เครื่องมือช่วยบริหารความปลอดภัยโดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด

นายปฏิญญา จันฤาชัย

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2547

ISBN 974-53-1998-8

SECURITY ADMINISTRATIVE TOOL BASED ON OPEN SOURCE VULNERAIBLITY DATABASE

Mr. Patinya Janluechai

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 974-53-1998-8

หัวข้อวิทยานิพนธ์	เครื่องมือช่วยบริหารความปลอดภัยโดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด
โดย	นายปฏิญญา จันฤาชัย
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษา	อาจารย์ ดร.ยรรยง เต็งอำนวย

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

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

คณะกรรมการสอบวิทยานิพนธ์

…… ประธานกรรมการ
(อาจารย์ ธงชัย โรจน์กังสดาล)

……... อาจารย์ที่ปรึกษา
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

……กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา)

……กรรมการ
(นางสาว รัศมีทิพย์ วิตา)

ปฏิญญา จันฤาชัย : เครื่องมือช่วยบริหารความปลอดภัยโดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด. (SECURITY ADMINISTRATIVE TOOL BASED ON OPEN SOURCE VULNERABILITY DATABASE) อ. ที่ปรึกษา: อ.ดร.ยรรยง เต็งอำนวย, 54 หน้า. ISBN 974-53-1998-8.

ซอฟต์แวร์ต่างๆที่ถูกพัฒนาและใช้งานกันอยู่ในปัจจุบันนี้ โดยส่วนใหญ่จะมีจุดอ่อนอยู่ในตัวของซอฟต์แวร์เอง จากจุดอ่อนของซอฟต์แวร์ที่มีอยู่นี้ ผู้บุกรุกหรือแฮกเกอร์สามารถนำมาใช้เป็นช่องทางในการเข้าไปก่อให้เกิดความเสียหายกับระบบคอมพิวเตอร์ในรูปแบบต่างๆ เช่น เปลี่ยนแปลงข้อมูล ทำให้ข้อมูลสูญหาย ฝังตัวเองหรือแพร่ขยายตัวเองเพื่อก่อกวนระบบคอมพิวเตอร์ ทำให้ระบบคอมพิวเตอร์เกิดปัญหาในการทำงาน รวมถึงสามารถสร้างความเสียหายแก่ระบบเครือข่าย เป็นต้น

จากปัญหาจุดอ่อนของซอฟต์แวร์ที่กล่าวมา จึงมีการคิดค้นและพัฒนาเครื่องมือช่วยบริหารความปลอดภัยโดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด โดยได้นำเอาเทคโนโลยีเว็บเซอร์วิสและไมโครซอฟท์ดอทเน็ตมาพัฒนาเครื่องมือนี้ โดยเครื่องมือนี้สามารถสแกนรายการซอฟต์แวร์ที่มีอยู่ในเครื่องคอมพิวเตอร์ และจะเก็บข้อมูลที่สำคัญของซอฟต์แวร์คือ ชื่อและเวอร์ชันของซอฟต์แวร์ที่ต้องการตรวจสอบ จากนั้นทำการส่งข้อมูลที่ได้ผ่านระบบเครือข่ายทางเว็บเซอร์วิส เพื่อให้เครื่องศูนย์กลางนำข้อมูลนี้ไปค้นหาเปรียบเทียบกับฐานข้อมูลจุดอ่อนระบบเปิดว่ารายการซอต์ฟแวร์ของเครื่องคอมพิวเตอร์ที่ต้องการตรวจสอบนั้น มีจุดอ่อนรายการใดบ้าง ทำให้ผู้ดูแลระบบสามารถทราบรายการสรุปจุดอ่อนของแต่ละเครื่อง ทำการตรวจสอบรายการ ค้นหาจุดอ่อนของซอฟต์แวร์และป้องกัน แก้ไขจุดอ่อนที่จะเกิดขึ้นภายในเครื่องคอมพิวเตอร์และระบบเครือข่ายได้

เครื่องมือที่พัฒนานี้จึงเป็นอีกเครื่องมือหนึ่งที่ช่วยให้ผู้ดูแลระบบ สามารถดำเนินการตรวจสอบป้องกันและจัดการกับซอฟต์แวร์ในแต่ละเครื่องคอมพิวเตอร์และระบบเครือข่ายได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

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

4670358921 : MAJOR COMPUTER SCIENCE

KEY WORD: VULNERABILITY / OPEN SOURCE VULNERABILITY DATABASE / OSVDB / WEB SERVICE / SECURITY / ADMINISTRATIVE TOOL

PATINYA JANLUECHAI : SECURITY ADMINISTRATIVE TOOL BASED ON OPEN SOURCE VULNERABILTY DATABASE. THESIS ADVISOR : YUNYONG TENG-AMNUAY,Ph.D, 54 pp. ISBN 974-53-1998-8.

Software developed and used in present, mostly has its software vulnerability. Unauthorized users can use these software vulnerabilities to access and make a lot of damages to computer systems such as changing data, making data loss, distribute itself to other computers and interrupting their processes. Also, they damage computer networks.

The objective of this independent study is to research and implement a tool called "security administrative tool based on open source vulnerability database" to solve the above problems. This tool developed by using Web Service and Microsoft .Net technology. With this system, users can scan and find software lists installed in their computers. Each software list consists of the two important data are software name and version. Then users can send these data via network to web service. At web service server, these data are compared with the data contained in the Open Source Vulnerability Database to find their vulnerabilities. The result of this process is the software vulnerability lists. Later, users can use these software vulnerability lists to protect and handle the problems which may be caused by each software vulnerability.

Finally, this tool will be a useful tool to help system administrative to detect, problems and handle software in computers and networks.

Department.....Computer Engineering.....Student's signature.....

Field of study.....Computer Science.....Advisor's signature.....

Academic year ……2004……

กิตติกรรมประกาศ

วิทยานิพนธ์นี้จะไม่สามารถสำเร็จลุล่วงไปด้วยดี หากไม่ได้รับคำปรึกษาแนะนำอันเป็นประโยชน์ยิ่งจาก อาจารย์ ดร.ยรรยง เต็งอำนวย อาจารย์ที่ปรึกษาวิทยานิพนธ์ รวมถึง ผู้ช่วยศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา และ อาจารย์ ธงชัย โรจน์กังสดาล ขอขอบคุณ คุณรัศมี ทิพย์ วิตา และเพื่อนๆ ผู้ร่วมโครงการวิจัยเรื่อง Enterprise Information System ซึ่งคอยให้คำแนะนำและช่วยเหลือในด้านต่างๆ

ขอขอบคุณ คุณพ่อ คุณแม่ พี่และน้อง สำหรับแรงสนับสนุนและเป็นกำลังใจให้เสมอและขอขอบคุณสิ่งต่างๆ ที่ทำให้งานวิจัยสำเร็จลงได้ด้วยดี

สารบัญ

หน้า

บทที่ หน้า

สารบัญตาราง

ตาราง หน้า

สารบัญภาพ

ภาพประกอบ หน้า

แผนภาพ

แผนภาพ หน้า

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

จุดอ่อนของซอฟต์แวร์ (Software Vulnerabilities) เป็นปัญหาซึ่งมีผลกระทบต่อระบบคอมพิวเตอร์สามารถทำให้ระบบความปลอดภัยของเครื่องคอมพิวเตอร์ทำงานผิดพลาดและระบบเกิดความเสียหาย [1] ผู้บุกรุก (Attacker) สามารถใช้จุดอ่อนของซอฟต์แวร์ในการข้ามผ่านระบบการรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ ส่งผลให้เกิดการเปลี่ยนแปลงของข้อมูลหรือข้อมูลสูญหาย โปรแกรมที่สร้างความเสียหายเช่น ไวรัสซอฟต์แวร์ ใช้จุดอ่อนของระบบปฏิบัติการหรือจุดอ่อนของซอฟต์แวร์เข้าสู่ระบบได้และจะแพร่ขยายตัวเองสร้างความเสียหาย ข้อมูลจุดอ่อนของซอฟต์แวร์จึงเป็นสิ่งสำคัญต่อองค์กรและระบบเครือข่ายคอมพิวเตอร์ เพื่อเป็นแนวทางในการตรวจสอบและหลีกเลี่ยงซอฟต์แวร์ที่มีจุดอ่อนต่อไป

ฐานข้อมูลจุดอ่อน (Vulnerability Database) จะให้รายละเอียดต่างๆ เกี่ยวกับจุดอ่อนที่ค้นพบในระบบคอมพิวเตอร์ ฐานข้อมูลจุดอ่อนระบบเปิด (OSVDB: Open Source Vulnerability Database) [2] เป็นฐานข้อมูลที่ให้ข้อมูลเกี่ยวกับจุดอ่อนต่างๆที่เกิดขึ้นในระบบคอมพิวเตอร์ โดยไม่คิดค่าใช้จ่าย เปิดเผยโครงสร้างของฐานข้อมูล มีการปรับปรุงข้อมูลให้ทันสมัยอยู่เสมอ

การนำรายการข้อมูลของซอฟต์แวร์มาทำการตรวจสอบในฐานข้อมูลจุดอ่อนนั้นสามารถทำได้ สองแบบคือ แบบใช้มือ (Manual) และแบบอัตโนมัติ (Automated) [3] แบบใช้มือขึ้นอยู่กับผู้รับผิดชอบว่าสามารถทำงานได้ถูกต้องในระดับใด ต้องใช้เวลาและความละเอียดถี่ถ้วนเพราะข้อมูลที่ต้องการตรวจสอบทั้งหมดที่อยู่ในเครื่องคอมพิวเตอร์นั้นมีเป็นจำนวนมาก ซึ่งทำให้ง่ายต่อการเกิดความผิดพลาด แบบอัตโนมัติความถูกต้องจะมีมากขึ้นโดยจะใช้เครื่องมือในการค้นหาและทำการรวบรวมข้อมูลของเครื่องคอมพิวเตอร์ออกมาทำเป็นรายการ ในงานวิจัยชิ้นนี้จะใช้ซอฟต์แวร์ระบบเปิดในการทำรายการซอฟต์แวร์แบบอัตโนมัติ

เว็บเซอร์วิส (Web Service) เป็นเทคโนโลยีสำหรับการแลกเปลี่ยนข้อมูลบนระบบเครือข่ายโดยมีโครงสร้างพื้นฐานเป็นเทคโนโลยีระบบเปิดสามารถพัฒนาให้ทุกๆระบบปฏิบัติการสามารถใช้งานร่วมกันได้และไม่ขึ้นอยู่กับภาษาที่ใช้พัฒนา [4] ซึ่งถ้านำมาใช้ในการค้นหาจุดอ่อนของซอฟต์แวร์จะสามารถกระทำได้กับทุกๆระบบปฏิบัติการเพราะเมื่อรายการซอฟต์แวร์ที่ติดตั้งอยู่บนทุกระบบปฏิบัติการ ได้ข้อมูลจะสามารถส่งผ่านไปทางเว็บเซอร์วิสได้

งานวิจัยชิ้นนี้กล่าวถึง การนำรายการซอฟต์แวร์ที่เครื่องเป้าหมายซึ่งจะนำข้อมูลชื่อและเวอร์ชันของซอฟต์แวร์ ส่งข้อมูลผ่านทางเว็บเซอร์วิสอินเทอร์เฟส (WSI: Web Service Interface) เพื่อนำไปค้นหาที่เครื่องศูนย์กลาง เครื่องศูนย์กลางเรียกข้อมูลรายการซอฟต์แวร์ของเครื่องคอมพิวเตอร์เป้าหมายนำมาทำการค้นหาในฐานข้อมูลจุดอ่อนระบบเปิดแล้วสามารถบอกได้ถึงรายการซอฟต์แวร์ของเครื่องคอมพิวเตอร์เป้าหมายที่มีจุดอ่อนสรุปรายการซอฟต์แวร์ที่มีจุดอ่อนของแต่ละเครื่องทำเป็นรายงานให้ผู้ดูแลระบบติดตามและตรวจสอบ

1.2 วัตถุประสงค์ของการวิจัย

เป็นการพัฒนาเครื่องมือโดยใช้ฐานข้อมูลจุดอ่อนระบบเปิดเพื่อให้สามารถค้นหาจุดอ่อนของรายการซอฟต์แวร์บนเครื่องคอมพิวเตอร์โดยอัตโนมัติ ผ่านทางเว็บเซอร์วิส

1.3 ขอบเขตของการวิจัย

1.ใช้เว็บเซอร์วิสในการเชื่อมต่อการทำงานระหว่างฐานข้อมูลจุดอ่อนระบบเปิดและเครื่องเป้าหมาย

2.ระบบสามารถตั้งเวลาในการสแกนค้นหาจุดอ่อนของซอฟต์แวร์ได้

3.ระบบสามารถเก็บสถานะ และ ตรวจสอบการเปลี่ยนแปลง ทั้งฝั่งที่เป็นอุปกรณ์ของเครื่องเป้าหมาย และ ฝั่งที่เป็นฐานข้อมูลจุดอ่อน เพื่ออำนวยความสะดวกในการตรวจสอบ ลดความซ้ำซ้อน

4.ระบบสามารถตรวจสอบ เพื่อปรับปรุงเวอร์ชัน (Version) ใหม่ๆ ของฐานข้อมูลจุดอ่อนระบบเปิดได้

5.ระบบสามารถเพิ่มลดเครื่องเป้าหมายที่ต้องการตรวจสอบผ่านเว็บได้

6.ใช้ซอฟต์แวร์ระบบเปิด (Open Source Software) ทั้งทางฝั่งของ ฐานข้อมูลจุดอ่อนระบบเปิด และ เครื่องคอมพิวเตอร์เป้าหมาย

7.ข้อมูลและโครงสร้างของฐานข้อมูลจุดอ่อนระบบเปิด อย่างน้อยไม่เก่ากว่าเดือนตุลาคม พ.ศ. 2547

8. ใช้ภาษาวิชวลเบสิกดอทเน็ต (Visual Basic.NET) ในการพัฒนาโปรแกรมและไมโครซอฟท์แอคเซส (Microsoft Access) เป็นฐานข้อมูล

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1. สามารถใช้ประเมินรายการซอฟต์แวร์ที่มีจุดอ่อนของเครื่องคอมพิวเตอร์

2. สามารถทราบถึงวันที่ค้นพบจุดอ่อน คำอธิบายจุดอ่อน หมวดหมู่ของจุดอ่อน แนวทางการแก้ไขจุดอ่อน

3. เป็นการพัฒนาเครื่องมือที่ใช้ สำหรับค้นหาจุดอ่อน แบบอัตโนมัติ ผ่านทางเว็บเซอร์วิส ที่สามารถแสดงผลข้อมูลได้อย่างถูกต้อง รวดเร็ว สะดวกในการใช้งาน

1.5 วิธีดำเนินการวิจัย

1. วิเคราะห์และออกแบบ วิธีการรวบรวม รายการข้อมูลที่ต้องการจะตรวจสอบและอ้างอิง

2. ออกแบบและสร้างเว็บเซอร์วิสทั้งในส่วนของฐานข้อมูลจุดอ่อนระบบเปิดและเครื่องเป้าหมาย

3. ออกแบบในส่วนของการแสดงผล

4. ทดสอบวิธีการและโปรแกรมที่นำเสนอ

5. วิเคราะห์ผล

6. สรุปผลการวิจัย และเรียบเรียงวิทยานิพนธ์

1.6 โครงสร้างวิทยานิพนธ์

ในบทต่อไปของวิทยานิพนธ์นี้จะกล่าวถึงทฤษฎีที่นำมาประยุกต์ใช้และงานวิจัยที่เกี่ยวข้อง ส่วนในบทที่ 3 จะกล่าวถึงการออกแบบเครื่องมือการค้นหาจุดอ่อนของซอฟต์แวร์ ในบทที่ 4 จะกล่าวถึงการพัฒนาเครื่องมือค้นหาจุดอ่อนของซอฟต์แวร์ ในบทที่ 5 จะกล่าวถึงผลการวิจัย และในบทสุดท้ายจะเป็นการสรุปผลการวิจัยและข้อแนะนำในการพัฒนาต่อไป

บทที่ 2

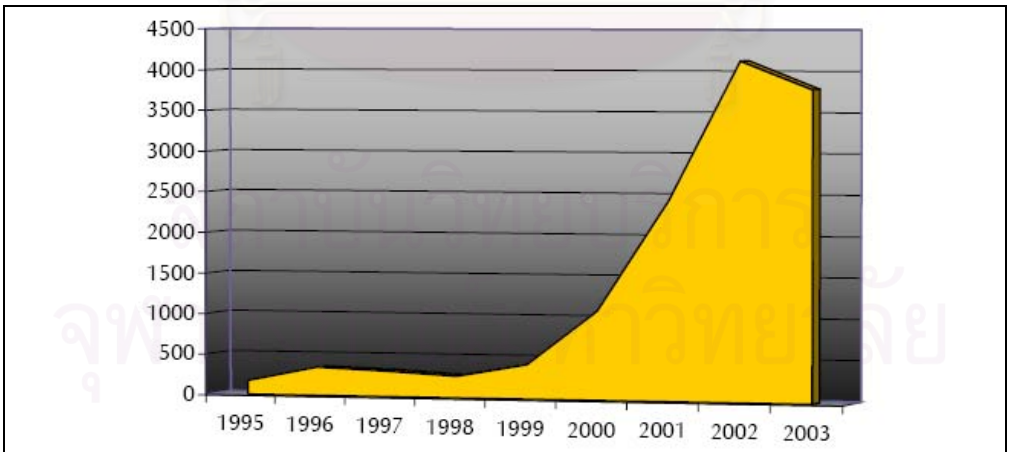
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดและทฤษฎี

จากการศึกษาเบื้องต้น พบว่าในงานวิจัยชิ้นนี้ จำเป็นต้องทำการศึกษาแนวคิดและทฤษฎีต่างๆ ซึ่งแบ่งออกเป็น 4 กลุ่มด้วยกันคือจุดอ่อนที่สามารถเกิดขึ้นในระบบ ฐานข้อมูลจุดอ่อน การค้นหาจุดอ่อนของซอฟต์แวร์ และเว็บเซอร์วิส ซึ่งในแต่ละกลุ่มมีรายละเอียดของแนวคิดและทฤษฎีดังต่อไปนี้

2.1.1 จุดอ่อนที่สามารถเกิดขึ้นในระบบ (Vulnerability and Exposure)

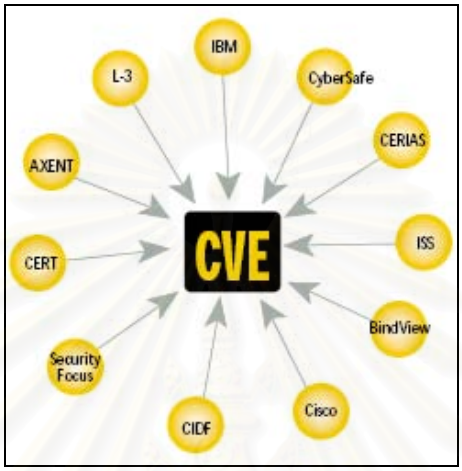
จุดอ่อนของซอฟต์แวร์เป็น ความผิดพลาดที่เกิดขึ้นภายในซอฟต์แวร์ทำให้ไวรัสหรือผู้ไม่หวังดี สามารถเข้าสู่ระบบโดยไม่ได้รับอนุญาต ก่อความเสียหายทำให้ระบบทำงานผิดพลาด ซึ่งระบบเครือข่ายภายในองค์กรควรคำนึงถึงในเรื่องนี้ด้วย จากสถิติของเซิร์ท (CERT) [5] ซึ่งดำเนินการโดย มหาวิทยาลัยคาเนกีเมลลอน (Carnegie Mellon University) ของประเทศสหรัฐอเมริกา ระบุว่า จำนวนจุดอ่อนที่เกิดขึ้นของระบบคอมพิวเตอร์ได้ทวีเพิ่มสูงขึ้นตั้งแต่ปี ค.ศ. 1995 ดังรูปที่ 2.1



	1995	1996	1997	1998	1999	2000	2001	2002	2003
Vuln's	171	345	311	262	417	1090	2437	4129	3784

รูปที่ 2.1 แผนภูมิแสดงจำนวนจุดอ่อนที่เกิดขึ้น

ซีวีอี (CVE: Common Vulnerabilities and Exposure) [6] ได้สร้างศูนย์กลางของการระบุ การค้น และแก้ไขจุดอ่อนให้มีความรวดเร็วและมีประสิทธิภาพ เนื่องจาก ฐานข้อมูลจุดอ่อนมีอยู่ด้วยกันหลากหลายฐานข้อมูล การตั้งชื่อจุดอ่อนของฐานข้อมูลจุดอ่อนแต่ละแห่งจะไม่เหมือนกัน จึงประสบปัญหาในการตั้งชื่อเรียกจุดอ่อน ซีวีอีไม่ใช่ฐานข้อมูลแต่จะเป็นเหมือนรายการข้อมูลซึ่งเป็นแหล่งอ้างอิงเพื่อค้นหารายละเอียดต่อไปในฐานข้อมูลจุดอ่อน แนวคิดรายการซีวีอีแสดงได้ดังรูปที่ 2.2



รูปที่ 2.2 แนวคิดของรายการซีวีอี

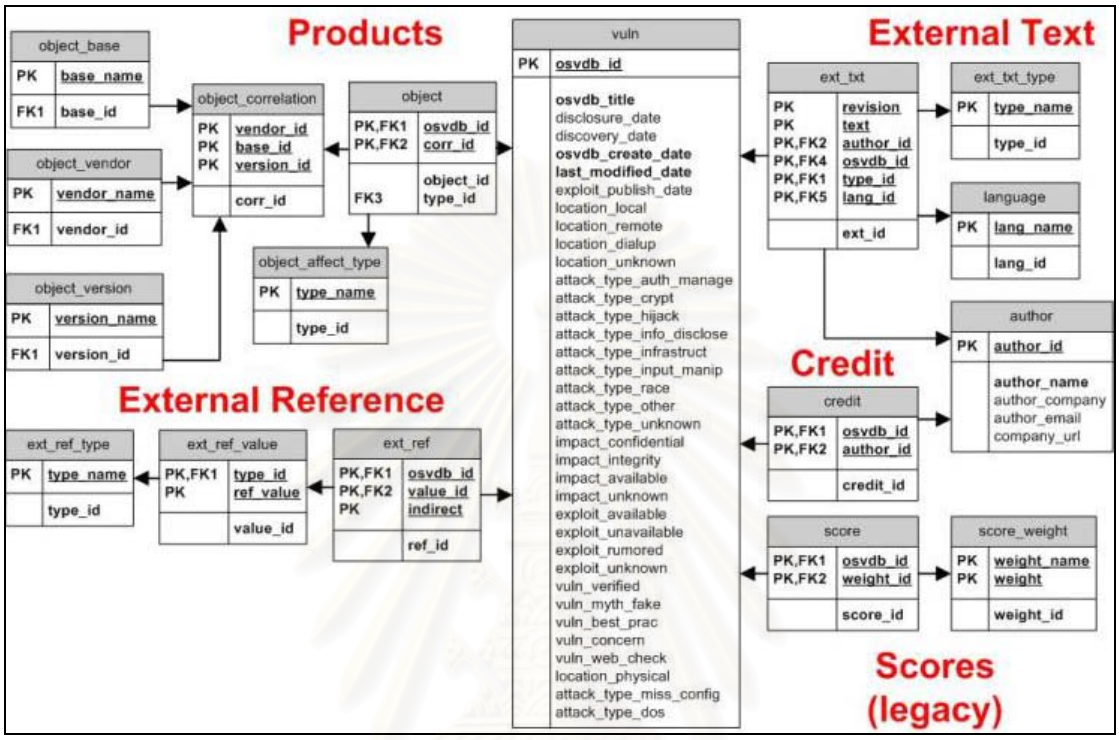
2.1.2 ฐานข้อมูลจุดอ่อน (Vulnerability Database)

ฐานข้อมูลจุดอ่อนเป็นการรวบรวมข้อมูลจุดอ่อนที่เกิดขึ้นได้ในระบบคอมพิวเตอร์ ซึ่งมีหลายหน่วยงานที่รวบรวมข้อมูลจุดอ่อนแล้วสร้างเป็นฐานข้อมูลจุดอ่อนขึ้นมา [7] ดังรูปที่ 2.3

Data base
CERT/CC Vulnerability Notes Database www.kb.cert.org/vuls
Coop VDB https://cirdb.cerias.purdue.edu/coopvdb/public/
ICAT Metabase icat.nist.gov
ISS X-Force http://www.iss.net/security_center/search.php
OSVDB www.osvdb.org
Scip Verletzbarkeitsdatenbank www.scip.ch/cgi-bin/smss/showadvf.pl
Security Focus www.securityfocus.com/bid

รูปที่ 2.3 ฐานข้อมูลจุดอ่อน

ฐานข้อมูลจุดอ่อนระบบเปิด (OSVDB: Open Source Vulnerability Database) ให้ข้อมูลเกี่ยวกับจุดอ่อนที่เกิดขึ้น โดยไม่คิดค่าใช้จ่าย ไม่มีการปิดบัง ซ่อนเร้นข้อมูล ฐานข้อมูลจุดอ่อนระบบเปิดจะมีโครงสร้าง ดังรูปที่ 2.4



รูปที่ 2.4 โครงสร้างของฐานข้อมูลจุดอ่อนระบบเปิด

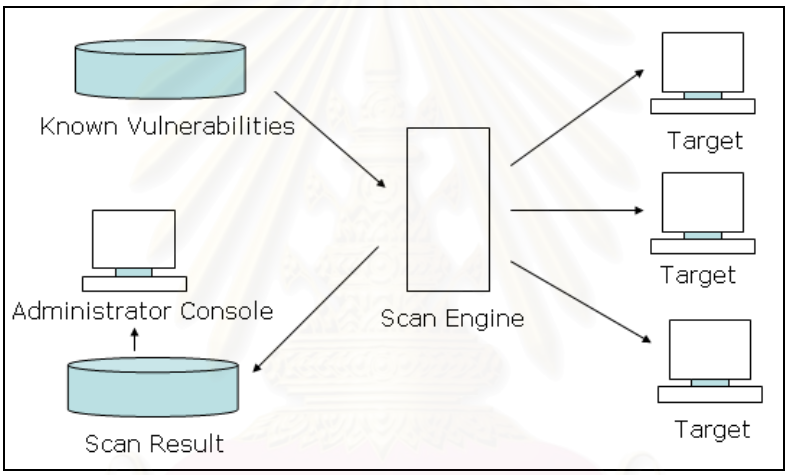
จากรูปที่ 2.4 พบว่าฐานข้อมูลประกอบด้วย 5 หมวดหมู่ คือ ผลิตภัณฑ์ (Product) ข้อมูลรายละเอียดจุดอ่อน (External Text) รายการอ้างอิง (External Reference) ผู้ค้นพบ (Credit) คะแนนและอัตราความเสี่ยง (Scores) โครงสร้างของฐานข้อมูลจุดอ่อนระบบเปิดจะมีตารางวัลน์ (Vuln) เก็บข้อมูลรายละเอียดจุดอ่อนหลักที่อยู่ในโครงสร้างของฐานข้อมูล

หมวดหมู่ของจุดอ่อนในฐานข้อมูลจุดอ่อนระบบเปิดสามารถแบ่งออกเป็น 5 กลุ่ม ได้แก่ **1. สถานที่** (Location) คือการเข้าสู่ระบบของผู้บุกรุก **2. การโจมตี** (Attack type) คือการกระทำอันประสงค์ร้ายต่อระบบ **3. ผลกระทบ** (Impact) คือ ความเสียหายที่เกิดขึ้นต่อระบบ **4. การประกาศ** (Exploit Availability) คือ ความสามารถที่จะทำการประกาศออกไปได้และ **5. เกี่ยวกับฐานข้อมูลโอเอสวีดีบี** (OSVDB) คือ เป็นข้อมูลซึ่งทางฐานข้อมูลจุดอ่อนระบบเปิดให้ข้อมูลเพิ่มเติมซึ่งหาไม่ได้จากฐานข้อมูลจุดอ่อนแห่งอื่น

2.1.3 การค้นหาจุดอ่อนของซอฟต์แวร์ (Software Vulnerability Detection)

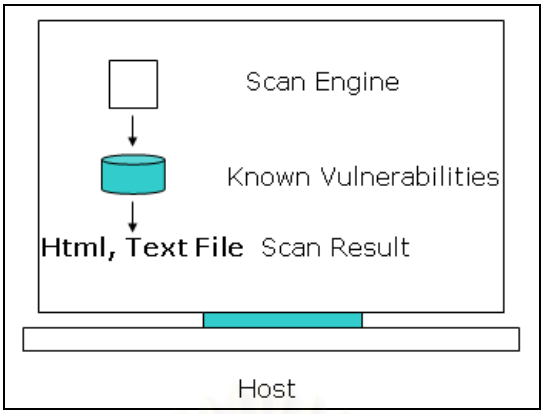
การค้นหาจุดอ่อนของซอฟต์แวร์เป็นการรวบรวมข้อมูลจุดอ่อนแล้วทำการประเมินเพื่อจัดการกับจุดอ่อนที่ค้นพบเหล่านั้น (Vulnerability Assessment and Management) [8] ซึ่งได้มีการพัฒนาเครื่องมือ (Tool) มีทั้งในลักษณะที่เป็น เน็ตเวิร์คสแกนเนอร์ (Network-Scanner) และโฮสต์สแกนเนอร์ (Host-Scanner)

เน็ตเวิร์คสแกนเนอร์ เป็นเครื่องมือที่ใช้ในการสแกนตรวจสอบจุดอ่อน โดยกระทำการติดตั้งจากเครื่องที่เป็นศูนย์กลางการตรวจสอบ จะกระทำได้จากการระบุช่วงหรือระยะ (Range) หมายเลขไอพีแอสเดรส (IP-Address) เครื่องที่ต้องการตรวจสอบ แล้วทำการค้นหา ดังรูปที่ 2.5



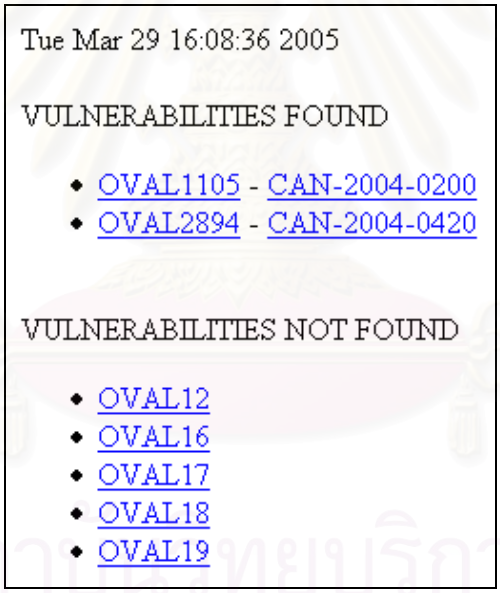
รูปที่ 2.5 ส่วนประกอบของเน็ตเวิร์คสแกนเนอร์

โฮสต์สแกนเนอร์ เป็นเครื่องมือที่จำเป็นจะต้องติดตั้งตัวโปรแกรมไว้ที่เครื่องที่ต้องการตรวจสอบ ตัวโปรแกรมจะทำการค้นหาจุดอ่อนและรายงานผล ไปที่ฐานข้อมูลส่วนกลางหรือเก็บข้อมูลไว้ที่เครื่องเพื่อใช้ในการตรวจสอบต่อไป ดังรูปที่ 2.6



รูปที่ 2.6 ส่วนประกอบของโฮสต์สแกนเนอร์

โปรแกรมโอวาล (OVAL: Open Vulnerability Assessment Language) [9] เป็นตัวอย่างของโฮสต์สแกนเนอร์ที่ทำการค้นหาจุดอ่อนของซอฟต์แวร์บนระบบปฏิบัติวินโดวส์และลีนุกซ์ อ้างอิงตามหมายเลขซีวีอี ผลลัพธ์จะได้ ดังรูปที่ 2.7



รูปที่ 2.7 ผลลัพธ์ที่ได้จากค้นหาโดยใช้โปรแกรมโอวาล

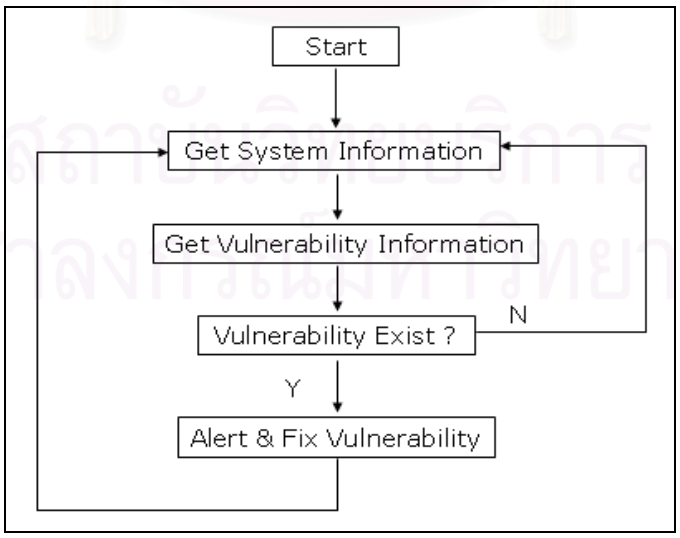
โปรแกรมไมโครซอฟท์เบสไลน์ (Microsoft Baseline Security Analyzer) [10] เป็นตัวอย่างของเน็ตเวิร์คสแกนเนอร์ที่บริษัทไมโครซอฟท์ได้พัฒนาขึ้นเพื่อทำการค้นหาจุดอ่อนของซอฟต์แวร์ของผลิตภัณฑ์ไมโครซอฟท์เอง แสดงดังรูปที่ 2.8

Score	Issue	Result
✗	SQL Server/MSDE Security Updates	Instance NETSDK: 1 critical security updates are missing. What was scanned Result details How to correct this
✱	Windows Security Updates	1 security updates could not be confirmed. What was scanned Result details How to correct this
✓	Microsoft VM Security Updates	No critical security updates are missing. What was scanned
✓	Office Security Updates	No critical security updates are missing. What was scanned
✓	IIS Security Updates	No critical security updates are missing. What was scanned
✓	MDAC Security Updates	No critical security updates are missing. What was scanned

รูปที่ 2.8 ผลลัพธ์ที่ได้จากค้นหาโดยใช้โปรแกรมไมโครซอฟท์เบสไลน์

การจัดการกับจุดอ่อนของระบบ ในทางทฤษฎีแล้วตรงไปตรงมา การเริ่มต้นจะมีขึ้นที่ระบบซึ่งไม่รู้ว่าตัวเองมีจุดอ่อน เมื่อเครื่องมือการตรวจสอบตรวจพบจุดอ่อน ก็จะทำการซ่อมแซมอย่างรวดเร็ว จุดอ่อนนั้นก็จะหายไป แต่ในทางปฏิบัติแล้ว การจัดการกับจุดอ่อนมีความยุ่งยาก อีกทั้งข้อมูลมีจำนวนมาก จึงเป็นเหตุผลหนึ่งที่ว่าไม่มีเครื่องมือที่สมบูรณ์แบบในการค้นหาจุดอ่อน

การจัดการกับจุดอ่อน [11] จะประกอบด้วย สี่ ขั้นตอน หลัก ได้แก่ การเก็บข้อมูลของระบบ การเก็บข้อมูลของจุดอ่อน ตรวจสอบ เตือนและซ่อมแซม ดังรูปที่ 2.9



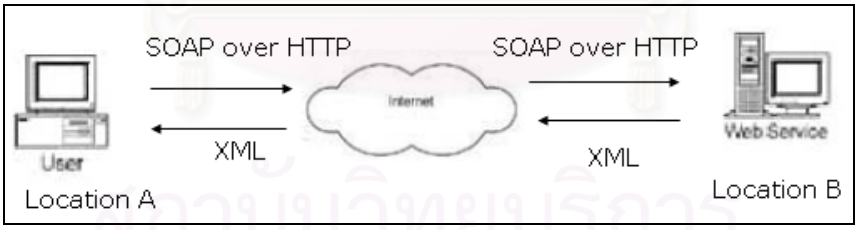
รูปที่ 2.9 กระบวนการในการจัดการกับจุดอ่อน

หลักการสำคัญอีกอย่างหนึ่งซึ่งขาดไม่ได้สำหรับการค้นหาจุดอ่อนของซอฟต์แวร์ คือความสอดคล้องกันของสตริง (String Matching) [12] เป็นหลักการที่มีความสำคัญในการรักษาความปลอดภัยของคอมพิวเตอร์ การออกแบบจะพัฒนาขึ้นเรื่อยๆไม่ว่าจะเป็นเรื่องของความเร็วหรือความถูกต้อง ซึ่งตัวอย่างที่เห็นได้ชัดเจนจะเป็นโปรแกรมชื่อว่า สนอร์ท (Snort) [13] เป็นเครื่องมือที่ใช้ตรวจจับการบุกรุกทางเครือข่าย (Network Intrusion Detection) หลักการความสอดคล้องกันของสตริงนี้จะนำมาใช้ในการค้นหาจุดอ่อนของซอฟต์แวร์ในงานวิจัยที่จะพัฒนาขึ้น

2.1.4 เว็บเซอร์วิส (Web Service)

ในการพัฒนาเครื่องมือเพื่อทำการค้นหาจุดอ่อนของซอฟต์แวร์ที่ใช้ในงานวิจัยชิ้นนี้ จะใช้เว็บเซอร์วิส ซึ่งเว็บเซอร์วิสเป็นการสร้างแอปพลิเคชัน ซึ่งสามารถทำงานผ่านทางเครือข่ายโดยใช้ภาษาเอ็กซ์เอ็มแอล (XML: eXtensible Markup Language) [14] เป็นพื้นฐานในการแลกเปลี่ยนข้อมูล เป็นเทคโนโลยีที่มีพื้นฐานเป็นระบบเปิดทำให้สามารถนำมาใช้งานได้ทุกระบบปฏิบัติการ และ ไม่จำกัดเรื่องภาษาที่จะนำมาใช้ในการพัฒนา

เว็บเซอร์วิสโดยพื้นฐานแล้วจะใช้การทำงานของ เอชทีทีพี (HTTP: Hypertext Transfer Protocol) และโซพ (SOAP: Simple Object Access Protocol) ในการทำให้ข้อมูลสามารถอยู่บนระบบเครือข่ายได้ โซพจะเรียกฟังก์ชันการทำงานข้ามเครือข่ายโดยผ่านทาง โปรโตคอลเอชทีทีพี [15] ดังรูปที่ 2.10



รูปที่ 2.10 ตัวอย่างรูปแบบการทำงานของเว็บเซอร์วิส

จากรูปที่ 2.10 ผู้ใช้ซึ่งอยู่ที่สถานที่ **เอ (A)** ได้ทำการเรียกฟังก์ชันการทำงานผ่านทางอินเตอร์เน็ตไปที่ เว็บเซอร์วิสที่ให้บริการซึ่งอยู่ที่สถานที่ **บี (B)** ผลลัพธ์ที่ได้จะอยู่ในรูปแบบข้อมูลไฟล์ เอ็กซ์เอ็มแอล เมื่อได้ผลลัพธ์เว็บเซอร์วิสจะส่งข้อมูลไฟล์เอ็กซ์เอ็มแอล กลับไปที่ผู้ใช้ซึ่งอยู่ที่สถานที่ **เอ (A)** ซึ่งในงานวิจัยที่พัฒนาขึ้นจะใช้วิธีในลักษณะเดียวกันนี้

2.2 เอกสารและงานวิจัยที่เกี่ยวข้อง

2.2.1 การวิจัยเรื่อง Sharing Vulnerability Information using a Taxonomically-correct, Web-based Cooperative Database [16]

L. Ma, S. Mandujano, G. Song และ P. Meunier จาก Center for Education and Research in Information Assurance and Security, Purdue University ได้นำเสนอแนวทางการออกแบบและจัดหมวดหมู่ของแต่ละชนิดของจุดอ่อนที่ค้นพบในระบบคอมพิวเตอร์ เพื่อสร้างเป็นระบบ ข้อมูลจะถูกเก็บไว้ในลักษณะของฐานข้อมูลเพื่อให้สามารถทำความเข้าใจได้ง่ายและข้อมูลมีความสัมพันธ์กัน การเข้าถึงข้อมูลสามารถกระทำได้โดยผ่านทางหน้าเว็บ (Web Interface) เพื่อสะดวกในการค้นหาข้อมูล

2.2.2 การวิจัยเรื่อง Integrating your information security vulnerability management capabilities through industry standards (CVE&OVAL) [17]

Robert A. Martin จาก Software Engineering Section Information Technology Directorate , The MITRE Corporation ได้แนะนำถึงซีวีอี (CVE: Common Vulnerabilities and Exposure) [13] ซึ่งเป็นมาตรฐานเกี่ยวกับข้อมูลจุดอ่อนของระบบ และโปรแกรมภาษา ที่มีชื่อว่าโอวาล (OVAL: Open Vulnerability Assessment Language) เป็นภาษาซึ่งใช้สำหรับในการประเมินเครื่องคอมพิวเตอร์ที่ได้รับการตรวจสอบ ซีวีอีให้ข้อมูลเป็นรายการข้อมูลของจุดอ่อน ที่เกิดขึ้นในระบบคอมพิวเตอร์ และโอวาลใช้ข้อมูลที่อ้างอิงได้จากรายการซีวีอีหารายละเอียดในการค้นหาข้อมูลภายในเครื่องคอมพิวเตอร์เพื่อสามารถบอกได้ว่าตามรายการซีวีอีพบซอฟต์แวร์รายการใดมีจุดอ่อน โอวาลมีเครื่องมือ (Tool) ซึ่งสามารถทำการติดตั้ง ค้นหาจุดอ่อนและรายงานผล การทำงานจะเป็นโฮตส์สแกนเนอร์ (Host-Scanner)

2.2.3 การวิจัยเรื่อง A Classification of Malicious Software Attacks [18]

Hanno Langweg และ Einar Snekkenes จาก NISlab Department of Computer Science and Media Technology, Gjøvik University College, Norway อธิบายถึงการจัดหมวดหมู่ของซอฟต์แวร์ที่ประสงค์ร้ายแก่ระบบคอมพิวเตอร์งานวิจัยชิ้นนี้จะมุ่งประเด็นไปที่ซอฟต์แวร์ที่ติดตั้งอยู่บนระบบปฏิบัติการแทนที่จะเป็นระบบปฏิบัติการ สิ่งที่แตกต่างระหว่างระบบปฏิบัติการและซอฟต์แวร์คือระบบปฏิบัติการจะมีฟังก์ชันการทำงานเป็นแบบทั่วๆไป ส่วนซอฟต์แวร์จะมีฟังก์ชันการทำงานที่พิเศษเพื่อติดตั้งบนระบบปฏิบัติการ ส่วนหนึ่งของการวิจัยจะเป็นการนำเอางานวิจัยอื่นๆ ที่เคยทำมาแล้วมาทำการเปรียบเทียบกัน ในการจัดหมวดหมู่ของโจมตีของงานวิจัยชิ้นนี้

แบ่งเป็น 3 ส่วนคือ 1.สถานที่ (Location) เทียบได้กับการนำข้อมูลเข้า 2.สาเหตุ (Cause) เทียบได้กับกระบวนการและ3.ผลกระทบ (impact) เทียบได้กับผลลัพธ์

2.2.4 การวิจัยเรื่อง Automated Vulnerability Management through Web Services [19]

H.T. Tian, L.S. Huang, J.L. Shan และ G.L. Chen จาก Department of Computer Science, University of Sci.&Tech. of China เสนอโครงร่างการทำงานที่นำเว็บเซอร์วิสเข้ามาช่วยในการค้นหาจุดอ่อน (Vulnerability) ของระบบ ฟังก์ชันการทำงานของเว็บเซอร์วิส ได้แก่ ผู้ประกาศ (issuer) ผู้ค้นหา (scanner) และผู้โจมตีระบบ (attacker) โดยการนำซีวีเอ็มแอล (CVML: Common Vulnerability Markup Language) [20] มาเป็นข้อมูลจุดอ่อนซึ่งจะอ้างอิงมาจากรายการซีวีอี (CVE) โดยการนำเว็บเซอร์วิสรันที่เครื่องให้บริการในการค้นหามีซอฟต์แวร์ตัวแทน (Agent) ทำหน้าที่ที่ร้องขอบริการจากเว็บเซอร์วิส ความแตกต่างของงานวิจัยคือ งานวิจัยชิ้นนี้เป็นการเพิ่มรายการซีวีอีให้มีโครงสร้างขึ้นและใช้ในการค้นหาจุดอ่อนผ่านเว็บเซอร์วิสแต่งานวิจัยที่จะทำขึ้นใช้ฐานข้อมูลจุดอ่อนโอเอสวีดีบีซึ่งเป็นโอเพนซอร์สและให้รายละเอียดดีกว่าการใช้เฉพาะรายการซีวีอีอย่างเดียว

2.2.5 การวิจัยเรื่อง Arm up Administrators: Automated Vulnerability Management [21]

H.T.Tian, L.S.Huang, Z.Zhou และ Y.L.Luo จาก Department of Computer Science, University of Sci.&Tech. of China เสนอแนวทางการจัดการกับจุดอ่อนของซอฟต์แวร์โดยใช้ ภาษาเอ็กซ์เอ็มแอล ได้แก่ ซีวีเอ็มแอล (CVML: Common Vulnerability Markup Language) เอสไอเอ็มแอล (SIML: System Information Markup Language) เอ็นเอสเอ็มแอล (NSML: Network System Markup Language) เป็นตัวกลางในการสื่อสารข้อมูลกับ ส่วนของการจัดการอีกสองส่วนคือ ตัวจัดการจุดอ่อนประจำเครื่อง (HVMs: Host Vulnerability Managers)และตัวจัดการจุดอ่อนประจำโดเมน (DVMs: Domain vulnerability managers)

บทที่ 3

การออกแบบเครื่องมือการค้นหาจุดอ่อนของซอฟต์แวร์

ในบทนี้จะกล่าวถึง ความต้องการโดยรวมของระบบ สถาปัตยกรรมของเครื่องมือในการค้นหาจุดอ่อนของซอฟต์แวร์โดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด ฟังก์ชันการทำงานของระบบ การค้นหาจุดอ่อนของซอฟต์แวร์ แผนที่เว็บไซต์ ฐานข้อมูลและแผนภาพกิจกรรมการทำงาน

3.1 ความต้องการโดยรวมของระบบ

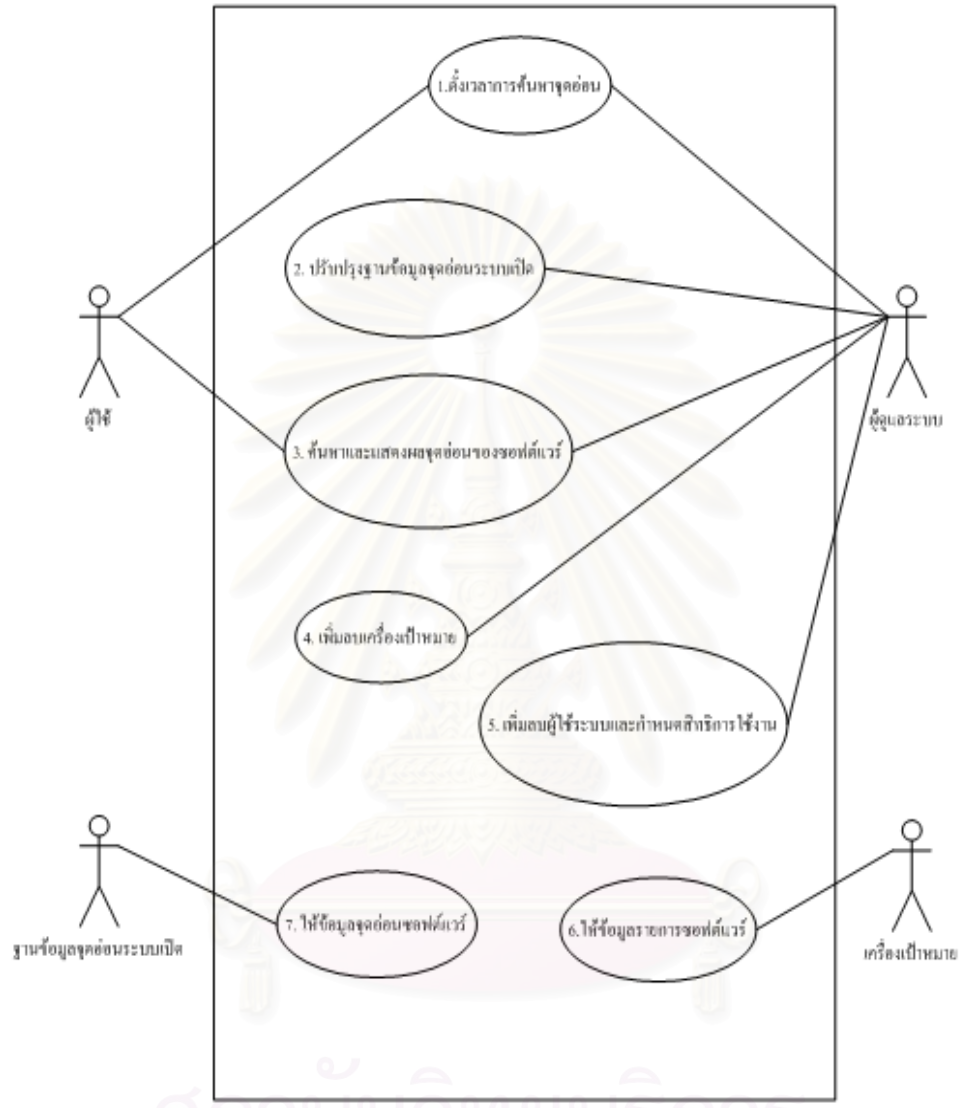
เครื่องมือในการค้นหาจุดอ่อนของซอฟต์แวร์โดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด เป็นระบบการค้นหาจุดอ่อนของซอฟต์แวร์โดยทำรายการชื่อซอฟต์แวร์และเวอร์ชันซอฟต์แวร์ที่เครื่องเป้าหมายแล้วนำข้อมูลมาให้เครื่องศูนย์กลางเพื่อค้นหากับฐานข้อมูลจุดอ่อนระบบเปิด โดยจะสรุปเป็นรายการชื่อซอฟต์แวร์ที่มีจุดอ่อนที่ค้นพบจากเครื่องเป้าหมาย ระบบสามารถทำงานได้ดีในสภาพแวดล้อมเครือข่ายภายในหรืออินทราเน็ต ความสามารถของระบบได้แก่ ค้นหารายการซอฟต์แวร์ที่มีจุดอ่อน ตั้งเวลาเพื่อค้นหาจุดอ่อนโดยอัตโนมัติ ปรับปรุงฐานข้อมูลจุดอ่อนระบบเปิด เพิ่ม/ลบเครื่องเป้าหมาย เพิ่ม/ลบผู้ใช้และกำหนดสิทธิ และ คำที่ไม่ต้องการค้น ผู้ใช้ระบบจะได้รับสิทธิการใช้งานในการเข้าใช้ระบบในส่วนต่างๆ ผู้ดูแลระบบเป็นผู้กำหนดสิทธิให้กับผู้ใช้

3.1.1 จากผลการวิเคราะห์สามารถสรุปเพื่อใช้สร้างแผนภาพยูสเคสได้ดังนี้

3.1.1.1 แอคเตอร์ (Actor) ได้แก่ ผู้ใช้ ผู้ดูแลระบบ ฐานข้อมูลจุดอ่อนระบบเปิด (โอเอสวีดีบี) และเครื่องเป้าหมาย

3.1.1.2 ยูสเคส (Use Case)ได้แก่ ตั้งเวลาการค้นหาจุดอ่อน ปรับปรุงฐานข้อมูลจุดอ่อนระบบเปิด ค้นหาและแสดงผลจุดอ่อนของซอฟต์แวร์ เพิ่มลบเครื่องเป้าหมาย เพิ่มลบผู้ใช้และกำหนดสิทธิ ให้ข้อมูลรายการซอฟต์แวร์และให้ข้อมูลจุดอ่อนของซอฟต์แวร์

เครื่องมือในการค้นหาจุดอ่อนของซอฟต์แวร์โดยปกติแล้วจะต้องทำการค้นหาในระดับรีจีสเตอร์ซึ่งซับซ้อนในการสร้างแอปพลิเคชันขึ้นมา งานวิจัยชิ้นนี้จะเป็นการนำเอาชื่อและเวอร์ชันของรายการซอฟต์แวร์มาทำการค้นหาซึ่งเป็นหลักการพื้นฐานทำให้สะดวกในการสร้างแอปพลิเคชัน การค้นหาจุดอ่อนของซอฟต์แวร์จะอ้างอิงกับฐานข้อมูลจุดอ่อนระบบเปิด ผู้ใช้จะทราบถึงรายการซอฟต์แวร์ที่มีจุดอ่อนและจำนวนรายการซอฟต์แวร์ที่มีจุดอ่อนโดยจะสามารถสรุปรายการซอฟต์แวร์ที่มีจุดอ่อนและไม่มีจุดอ่อน จุดอ่อนของซอฟต์แวร์ในกลุ่มใดที่มีมากที่สุดโดยอ้างอิงจากฐานข้อมูลจุดอ่อน การทำงานสามารถตั้งเวลาการสแกนแบบอัตโนมัติ ทำให้ได้แผนภาพยูสเคส ดังแสดงในแผนภาพที่ 3.1 และคำอธิบายยูสเคสอยู่ในตารางที่ 3.1



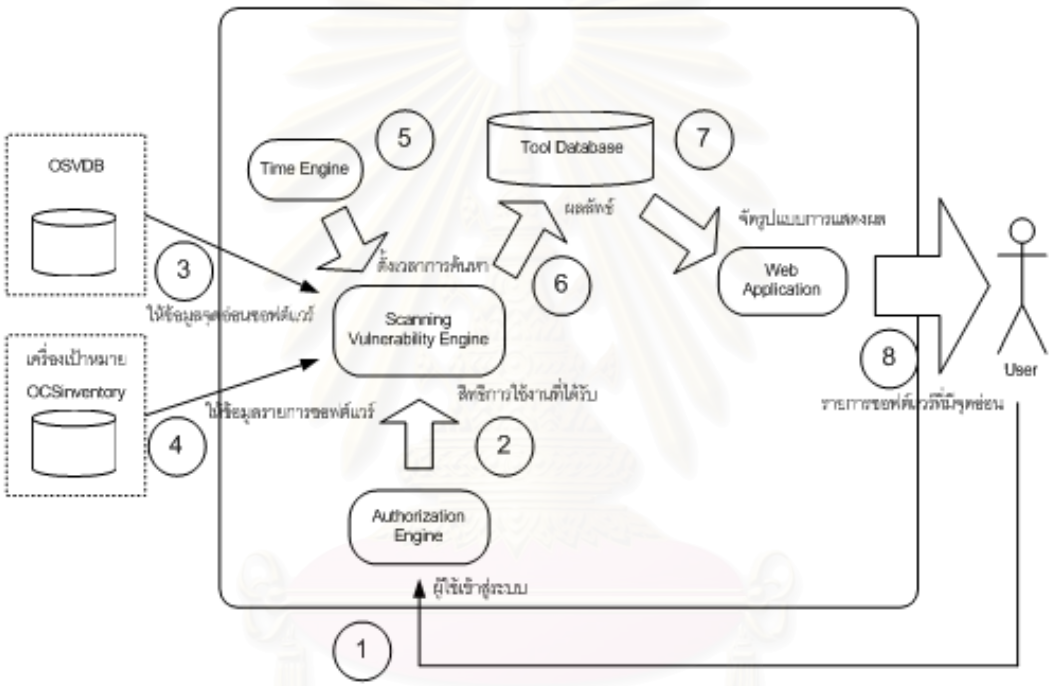
ชนิดของแผนภาพ : 3.1 ยูสเคส	**ชื่อระบบ**: ระบบค้นหาจุดอ่อนของซอฟต์แวร์โดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด	
ผู้จัดทำ: นายปฏิญญา จันฤาชัย	**เวอร์ชัน:** 1.00	**วันที่แก้ไขล่าสุด**: 14 เม.ย. 2548

ตารางที่ 3.1 อธิบายความหมายของแต่ละยูสเคส

ยูสเคส	คำอธิบาย
1. ตั้งเวลาค้นหาจุดอ่อนซอฟต์แวร์	กระทำโดยผู้ใช้หรือผู้ดูแลระบบ เพื่อกำหนดเวลาการค้นหาจุดอ่อนของซอฟต์แวร์ในแต่ละวัน
2. ปรับปรุงฐานข้อมูลจุดอ่อนระบบเปิด	กระทำโดยผู้ดูแลระบบ เพื่อปรับปรุงข้อมูลฐานข้อมูลจุดอ่อนระบบเปิดจากเว็บแอปพลิเคชัน
3. ค้นหาและแสดงผลจุดอ่อนของซอฟต์แวร์	กระทำโดยผู้ใช้หรือผู้ดูแลระบบ เพื่อค้นหาจุดอ่อนของซอฟต์แวร์ที่เครื่องเป้าหมาย
4. เพิ่มลบเครื่องเป้าหมาย	กระทำโดยผู้ดูแลระบบ เพื่อทำการเพิ่มหรือลบเครื่องเป้าหมายผ่านทางเว็บแอปพลิเคชัน
5. เพิ่มลบและกำหนดสิทธิผู้ใช้งานระบบ	กระทำโดยผู้ดูแลระบบ เพื่อกำหนดสิทธิการใช้งาน
6. ให้ข้อมูลรายการซอฟต์แวร์	กระทำโดยเครื่องเป้าหมายที่มีการติดตั้งเว็บเซอร์วิสอินเทอร์เฟสและโปรแกรมโอซีเอสอินเวนทอรี่
7. ให้ข้อมูลจุดอ่อนซอฟต์แวร์	กระทำโดยฐานข้อมูลจุดอ่อนระบบเปิด เพื่อให้ข้อมูลจุดอ่อนของซอฟต์แวร์

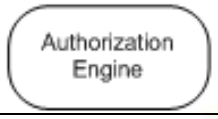
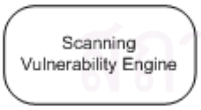
3.2 ภาพรวมของระบบ

3.2.1 สถาปัตยกรรมของงานวิจัยประกอบไปด้วยกระบวนการต่างๆ ดังแผนภาพที่ 3.2 และคำอธิบายสัญลักษณ์ในสถาปัตยกรรม อยู่ในตารางที่ 3.2



ชนิดแผนภาพ: 3.2 สถาปัตยกรรม	**ชื่อระบบ**: ระบบค้นหาจุดอ่อนของซอฟต์แวร์โดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด	
ผู้จัดทำ: นายปฏิญญา จันฤาชัย	**เวอร์ชัน**: 1.00	**วันที่แก้ไขล่าสุด**: 5 มี.ค. 2548

ตารางที่ 3.2 แสดงสัญลักษณ์และคำอธิบายสถาปัตยกรรม

สัญลักษณ์	อธิบาย
	ผู้ใช้หรือผู้ดูแลระบบกรอกข้อมูล ชื่อผู้ใช้และรหัสผ่าน เพื่อเข้าสู่ระบบ
	ส่วนตรวจสอบสิทธิการใช้งาน ถ้าเป็นผู้ดูแลระบบจะสามารถเข้าถึงได้ทุกส่วน
	ใช้โปรแกรมโอซีเอสอินเวนทอรี่ ในการสแกนเพื่อทำรายการซอฟต์แวร์เป็นข้อมูลให้กับเว็บเซอร์วิสอินเทอร์เฟสที่ติดตั้งอยู่บนเครื่องเป้าหมาย
	จุดอ่อนของซอฟต์แวร์ได้มาจากฐานข้อมูลจุดอ่อนระบบเปิดเป็นข้อมูลให้กับเว็บเซอร์วิสอินเทอร์เฟสเพื่อให้เครื่องศูนย์กลางเรียกข้อมูลมาใช้
	การตั้งเวลาที่ต้องการค้นหาจุดอ่อนซอฟต์แวร์ โดยจะมีรูปแบบเป็น 00:00 AM/PM
	การค้นหาจุดอ่อนของซอฟต์แวร์ซึ่งเป็นการอาศัยความสอดคล้องกันระหว่างชื่อซอฟต์แวร์และเวอร์ชัน ระหว่างรายการซอฟต์แวร์ที่อยู่ในฐานข้อมูลจุดอ่อนระบบเปิดและรายการซอฟต์แวร์ที่เครื่องเป้าหมาย
	ฐานข้อมูลส่วนกลางของระบบ
	เว็บแอปพลิเคชันสำหรับการใช้งานระบบ

กระบวนการทำงานโดยเบื้องต้นตามหมายเลขจากแผนภาพที่ 3.2 มีดังนี้

1. ผู้ใช้กระทำการกรอกข้อมูลได้แก่ ชื่อผู้ใช้และรหัสผ่าน เพื่อให้ระบบตรวจสอบข้อมูล

2. ตรวจสอบสิทธิการใช้งานของผู้ใช้ว่าสามารถเข้าใช้เมนูใดได้บ้าง

3. ฐานข้อมูลจุดอ่อนระบบเปิดให้ข้อมูลจุดอ่อนของซอฟต์แวร์ที่มีจุดอ่อน

4. โปรแกรมโอซีเอสอินเวนทอรี่ ให้ข้อมูลรายการซอฟต์แวร์ที่จะนำไปตรวจสอบ

5. การตั้งเวลาจากผู้ใช้

6. ส่วนของการเก็บข้อมูลผลลัพธ์ที่ฐานข้อมูลเครื่องศูนย์กลางเพื่อเก็บสถานะ

7. ข้อมูลที่ได้จากการตรวจสอบที่เก็บไว้ในฐานข้อมูลส่งไปยังส่วนของการแสดงผล

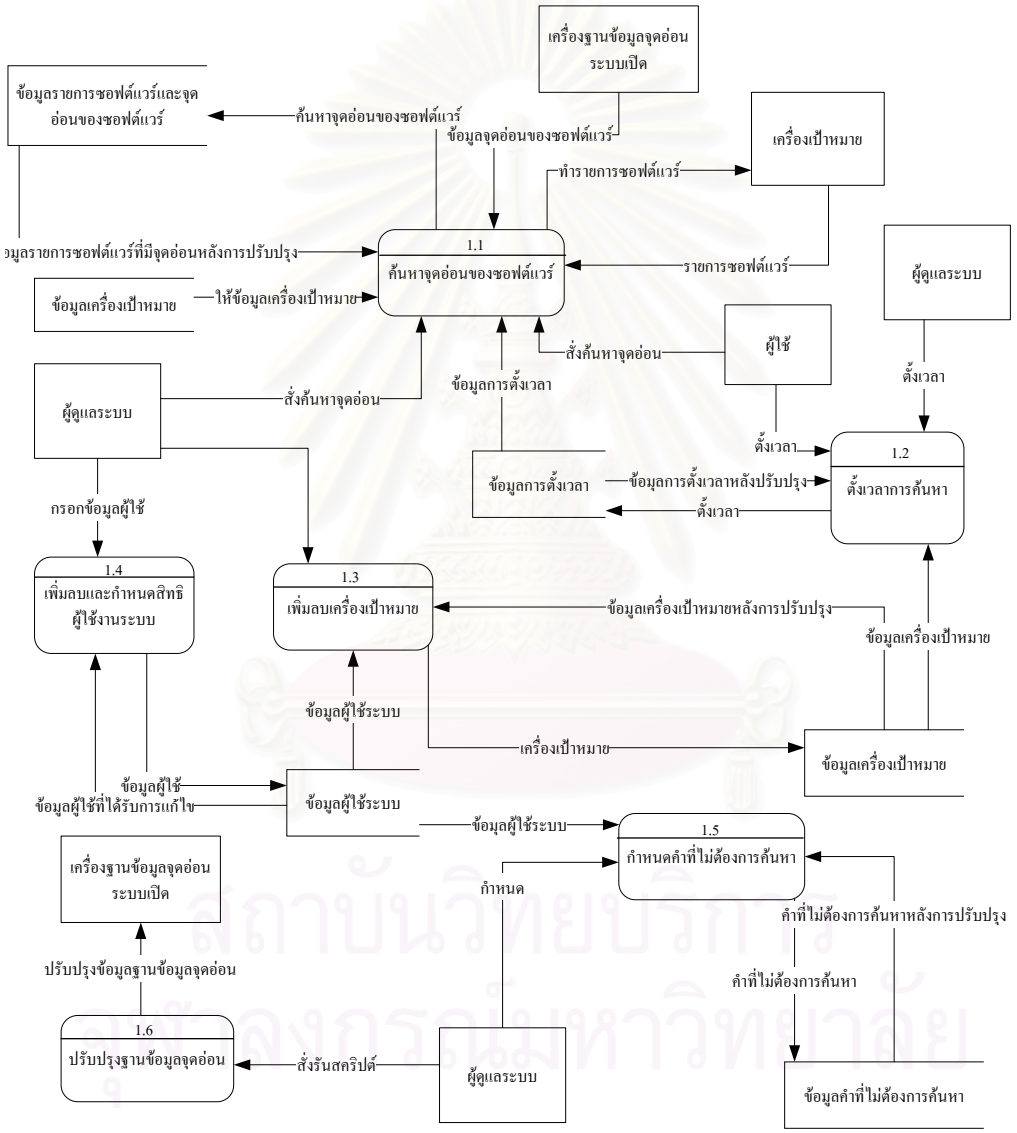
8. ส่วนของการแสดงผลลัพธ์ที่ได้จากการค้นหาผ่านทางเว็บแอปพลิเคชัน

3.2.2 ฟังก์ชันการทำงานของระบบ

สำหรับแผนภาพที่ใช้อธิบายการทำงานต่างๆในระบบการค้นหาจุดอ่อนของซอฟต์แวร์โดยใช้ฐานข้อมูลจุดอ่อนระบบเปิดจะใช้แผนภาพแสดงทิศทางการไหลของข้อมูล (Data Flow Diagram) เพื่อให้เข้าใจถึงกระบวนการทำงานต่างๆ ของระบบ

ในการอธิบายการไหลของข้อมูลในลักษณะของลอจิคอล (Logical) แสดงได้ดังแผนภาพที่ 3.3การทำงานของระบบเริ่มจาก (กระบวนการที่ 1.3) ระบบทำการเพิ่มเครื่องเป้าหมายเข้าสู่ระบบเพื่อทำการเชื่อมต่อโดยที่เครื่องเป้าหมายนั้นจะต้องมีการติดตั้งซอฟต์แวร์ที่ใช้สำหรับสแกนรายการซอฟต์แวร์ เครื่องศูนย์กลางติดต่อกับเครื่องฐานข้อมูลจุดอ่อนระบบเปิดเพื่อนำข้อมูลมาใช้งานด้วย (กระบวนการที่ 1.1) ค้นหาจุดอ่อนของซอฟต์แวร์การทำงานจะเป็นการนำเอาข้อมูลรายการซอฟต์แวร์ที่เครื่องเป้าหมายมาค้นหาในฐานข้อมูลจุดอ่อนระบบเปิด เครื่องคอมพิวเตอร์ศูนย์กลางบันทึกรายการซอฟต์แวร์ของเครื่องเป้าหมายที่ฐานข้อมูลเครื่องคอมพิวเตอร์ศูนย์กลาง (กระบวนการที่ 1.2) การตั้งเวลาการค้นหาเป็นการกำหนดเวลาไว้เมื่อถึงเวลาฟังก์ชันการสแกนค้นหาจุดอ่อนของซอฟต์แวร์ที่เครื่องเป้าหมายจะทำงานโดยอัตโนมัติ และ (กระบวนการที่ 1.5) เนื่องจากการค้นหาแต่ละครั้งจะได้ชื่อซอฟต์แวร์ที่ซ้ำกันหรือเป็นโปรแกรมซ่อมแซมเล็กๆดังนั้นจึงจะต้องมีการกำหนดคำที่ไม่ต้องการจะนำมาค้นหาด้วยเพื่อให้การค้นหาสามารถข้ามผ่านซอฟต์แวร์เหล่านั้นได้ (กระบวนการที่ 1.4) สิทธิการใช้งานของผู้ใช้กำหนดจากผู้ดูแลระบบโดยทำการกรอกข้อมูลผู้ใช้เข้าสู่ระบบ (กระบวนการที่ 1.6) การปรับปรุงฐานข้อมูลจุดอ่อนระบบเปิดสามารถกระทำ

ได้จากเว็บแอปพลิเคชันซึ่งเป็นเหมือนการสั่งรันไฟล์สคริปต์ที่เครื่องฐานข้อมูลจุดอ่อนระบบเปิด ซึ่งสคริปต์ไฟล์ทางฐานข้อมูลจุดอ่อนระบบเปิดจะมีสคริปต์มาให้แล้วไม่ได้สร้างขึ้นมาเอง การรันสคริปต์แต่ละครั้งจะใช้เวลาประมาณสองถึงสามชั่วโมงในการปรับปรุงฐานข้อมูลจุดอ่อนระบบเปิด



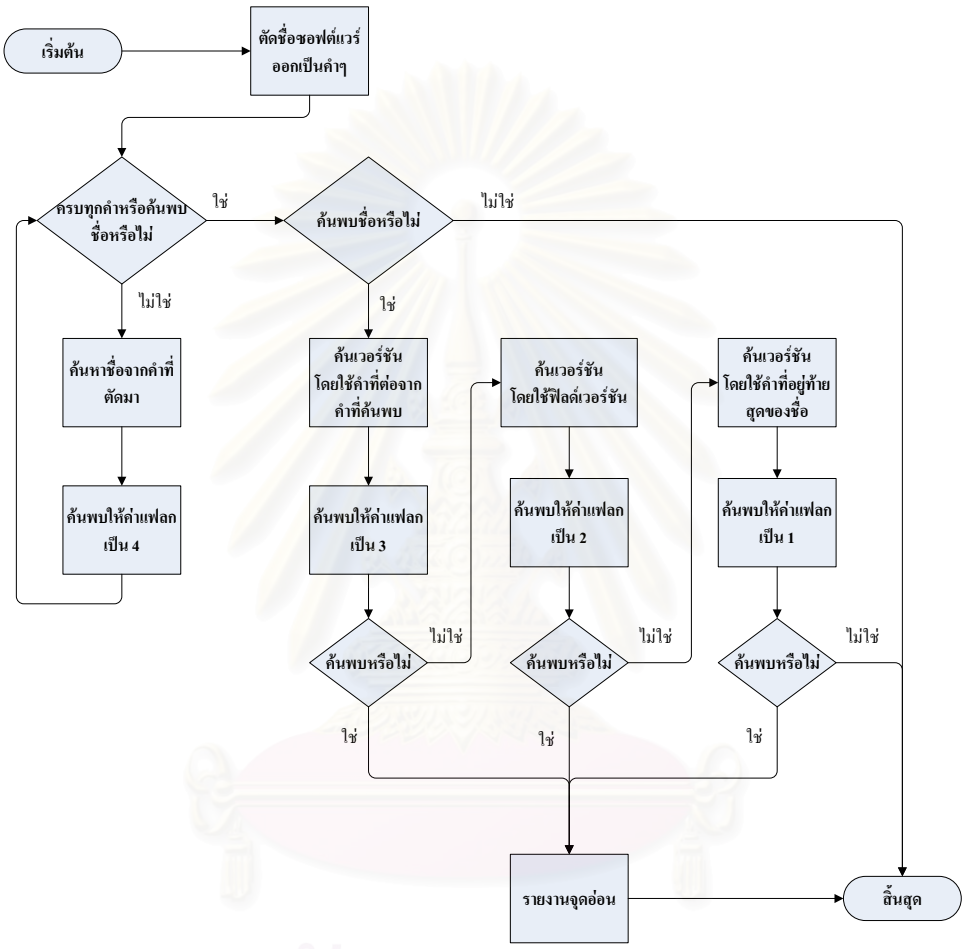
ชนิดของแผนภาพ : 3.3 แสดงการไหลของข้อมูลแบบลอจิคอล	**ชื่อระบบ**: ระบบค้นหาจุดอ่อนของซอฟต์แวร์โดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด	
ผู้จัดทำ: นายปฏิญญา จันฤาชัย	**เวอร์ชัน:** 1.00	**วันที่แก้ไขล่าสุด**: 8 มี.ค. 2548

3.2.3 การค้นหาจุดอ่อนของซอฟต์แวร์โดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด

การค้นหาจุดอ่อนของซอฟต์แวร์ของงานวิจัยที่จะทำขึ้นเป็นการนำชื่อและเวอร์ชันของซอฟต์แวร์มาค้นหาในฐานข้อมูลจุดอ่อนระบบเปิดคล้ายๆกับการกรองข้อมูลรายการซอฟต์แวร์จากข้อมูลทั้งหมด เพื่อให้สามารถระบุได้ว่าซอฟต์แวร์รายการที่มีจุดอ่อนจะใช้ลำดับขั้นตอน (Algorithm) ในการกรองข้อมูล

เนื่องจากลักษณะของข้อมูลซอฟต์แวร์ที่มีจุดอ่อน และลักษณะของข้อมูลที่ได้จากการค้นหาโดยใช้โปรแกรมโอซีเอส อินเวนทอรี่ จะได้ชื่อซอฟต์แวร์ซึ่งมีความยาวมากกว่าชื่อที่มีอยู่ในฐานข้อมูลจุดอ่อนระบบเปิด เช่น ซอฟต์แวร์ที่ค้นหามาได้ ชื่อ Apache HTTP Server 1.3.29 แต่ถ้าอยู่ในฐานข้อมูลจุดอ่อนระบบเปิด จะมีชื่อเป็น Apache เป็นต้น ดังนั้นจะต้องมี การตัดคำเพื่อให้สามารถนำไปค้นหาในฐานข้อมูลจุดอ่อนระบบเปิดได้

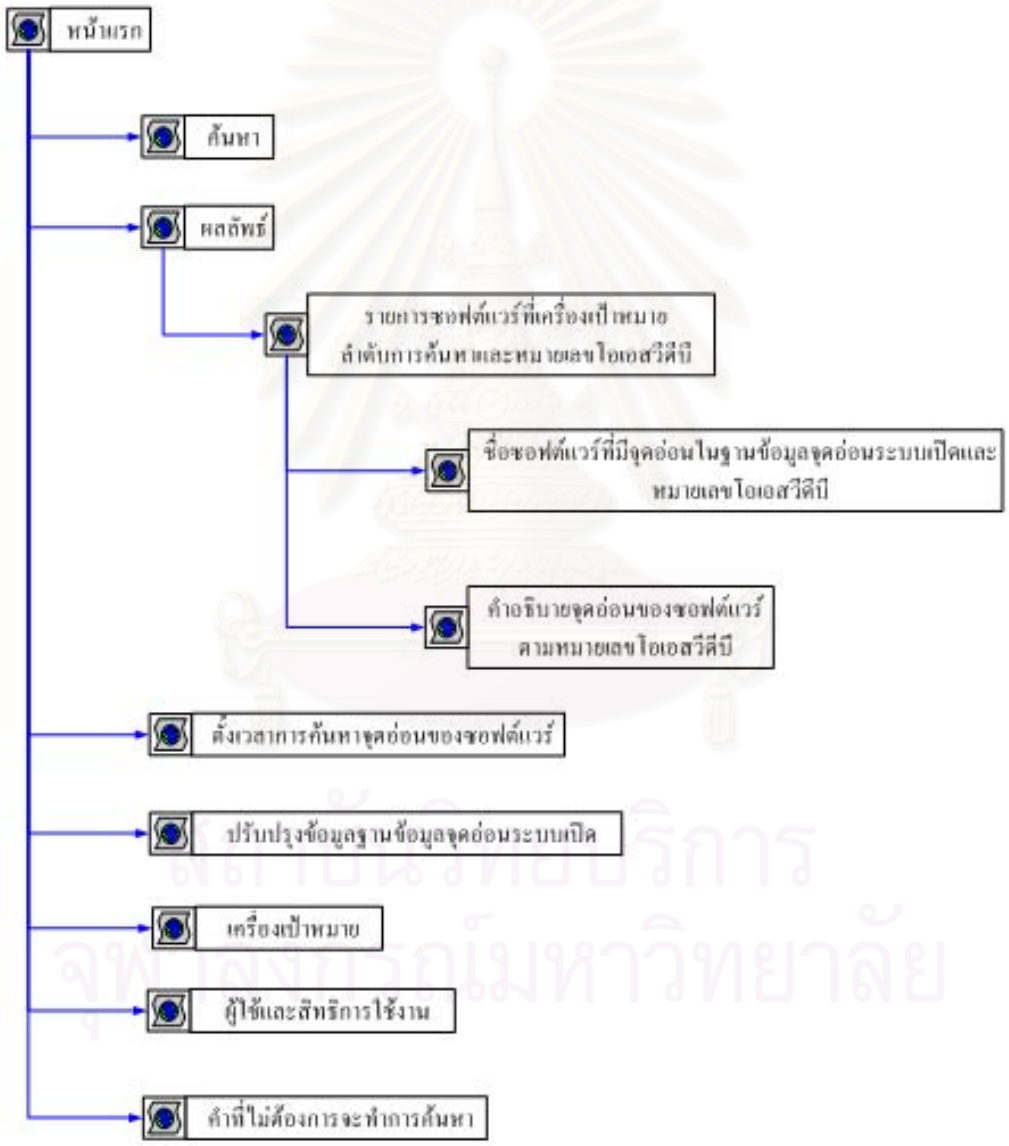
การค้นหาจุดอ่อนของรายการซอฟต์แวร์เริ่มที่การแบ่งชื่อซอฟต์แวร์ออกมาเป็นคำๆ เพื่อให้สามารถนำไปใช้ในการค้นกับฐานข้อมูลจุดอ่อนระบบเปิดได้ การแบ่งอาศัยช่องว่างระหว่างคำแล้วนำคำที่ได้ไปค้นหาในฐานข้อมูลจุดอ่อนระบบเปิดโดยลำดับแรก จะมีการตรวจสอบคำแต่ละคำที่แบ่งมาว่ามีในฐานข้อมูลจุดอ่อนหรือไม่ ถ้ามีผลลัพธ์เป็นใช่ (Yes) ถ้าไม่มีผลลัพธ์เป็นไม่ใช่ (No) ถ้าไม่มีก็ไม่ต้องทำการค้นหาเวอร์ชันแต่ถ้ามีก็จะทำการค้นเพื่อหาเวอร์ชันต่อไป โดยจะมีการกำหนดค่า แฟลก (Flag) ต่างๆ คือส่วนของ **การค้นชื่อ** หากค้นพบชื่อค่าแฟลกมีค่าเป็น สี่ (4) ส่วนของ **การค้นเวอร์ชัน** ถ้าพบโดยเป็นคำที่ต่อจากชื่อที่ค้นพบค่าแฟลกมีค่าเป็น สาม (3) ถ้าพบโดยเป็นฟิลด์เวอร์ชันค่าแฟลกมีค่าเป็น สอง (2) ถ้าพบโดยเป็นคำที่อยู่ท้ายสุดของชื่อซอฟต์แวร์ค่าแฟลกมีค่าเป็น หนึ่ง (1) และการค้นถ้าค้นชื่อไม่พบก็ไม่จำเป็นต้องค้นเวอร์ชันและค่าแฟลกจะมีค่าเป็น ศูนย์ (0) ซึ่งการกำหนดค่าแฟลกขึ้นมาก็เพื่อทำการเก็บสถิติเพื่อตรวจสอบความสอดคล้องกันระหว่างชื่อของซอฟต์แวร์ที่เครื่องเป้าหมายและชื่อที่ได้จากฐานข้อมูลจุดอ่อนระบบเปิดว่ามีความสอดคล้องกันอย่างไรแสดงได้ดังแผนภาพที่ 3.4



ชนิดของแผนภาพ : 3.4 ลำดับขั้นตอนในการหาความสัมพันธ์	**ชื่อระบบ**: ระบบค้นหาจุดอ่อนของซอฟต์แวร์โดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด	
ผู้จัดทำ: นายปฏิญญา จันฤาชัย	**เวอร์ชัน:** 1.00	**วันที่แก้ไขล่าสุด**: 8 มี.ค. 2548

3.3 แผนที่เว็บไซต์ (Web Site Map)

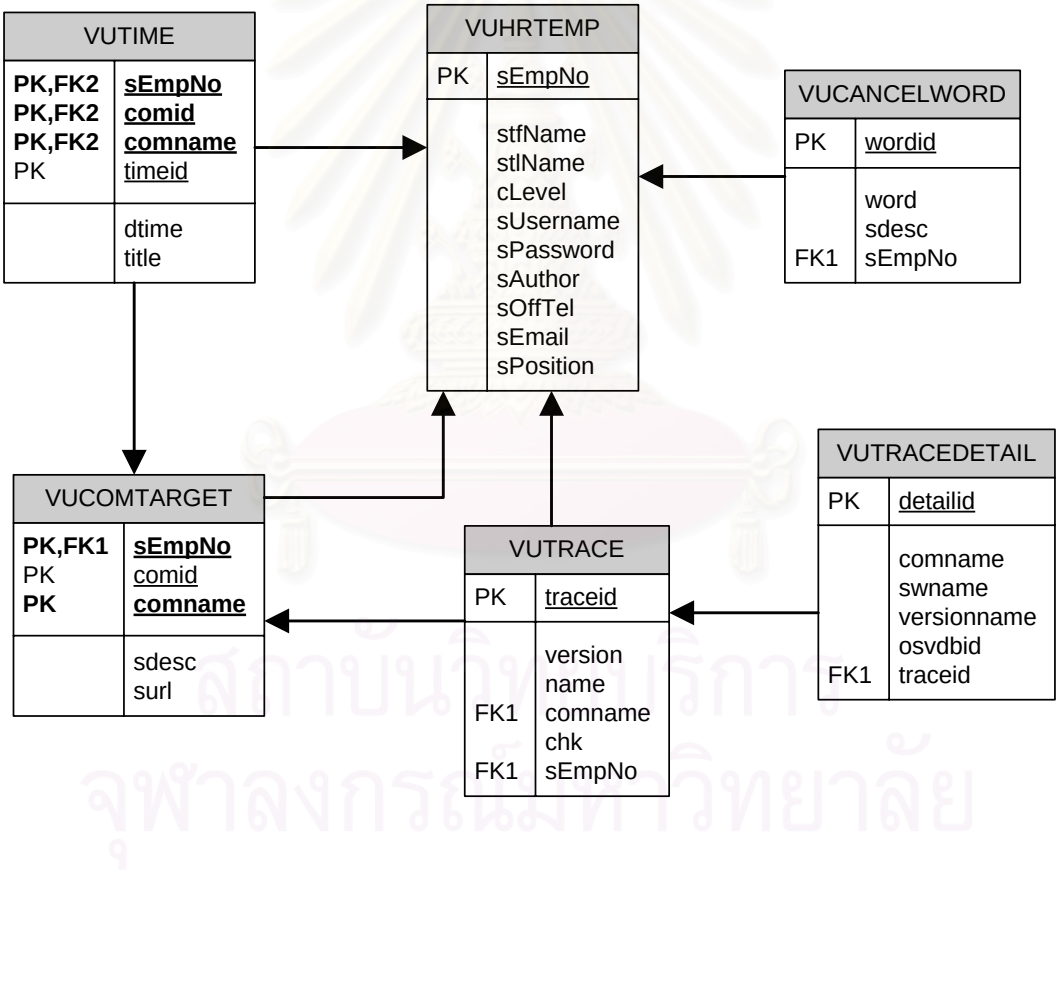
แผนที่เว็บไซต์ช่วยแสดงให้เห็นถึงภาพรวมของเว็บไซต์ทั้งหมดเมื่อผู้ใช้ต้องการทราบข้อมูลในเว็บไซต์ว่ามีอะไรบ้างเป็นสาระสำคัญ เว็บไซต์จะประกอบด้วยหน้าแรกเป็นหน้าหลักและเมนูการทำงานแยกเป็นลิงค์ต่างๆ ซึ่งในส่วนของผลลัพธ์จะแยกย่อยเพื่ออธิบายรายละเอียดในส่วนของจุดอ่อนที่ค้นพบ แสดงได้ดังแผนภาพที่ 3.4



ชนิดแผนภาพ: 3.5 แผนที่เว็บไซต์	**ชื่อระบบ**: ระบบค้นหาจุดอ่อนของซอฟต์แวร์โดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด	
ผู้จัดทำ: นายปฏิญญา จันฤาชัย	**เวอร์ชัน**: 1.00	**วันที่แก้ไขล่าสุด**: 5 มี.ค. 2548

3.4 ฐานข้อมูล

ในการทำงานของเครื่องมือการค้นหาจุดอ่อนซอฟต์แวร์โดยใช้ฐานข้อมูลจุดอ่อนระบบเปิดนั้น จำเป็นจะต้องมีการเก็บข้อมูลไว้ที่เครื่องคอมพิวเตอร์ศูนย์กลางเพื่อกำหนดเครื่องเป้าหมาย เก็บข้อมูลการตั้งเวลา เก็บข้อมูลสมาชิก และรายการซอฟต์แวร์ที่เครื่องเป้าหมาย สำหรับความสัมพันธ์ระหว่างตารางต่างๆ แสดงได้ ดังแผนภาพที่ 3.5 และคำอธิบายตารางอยู่ใน ตารางที่ 3.3



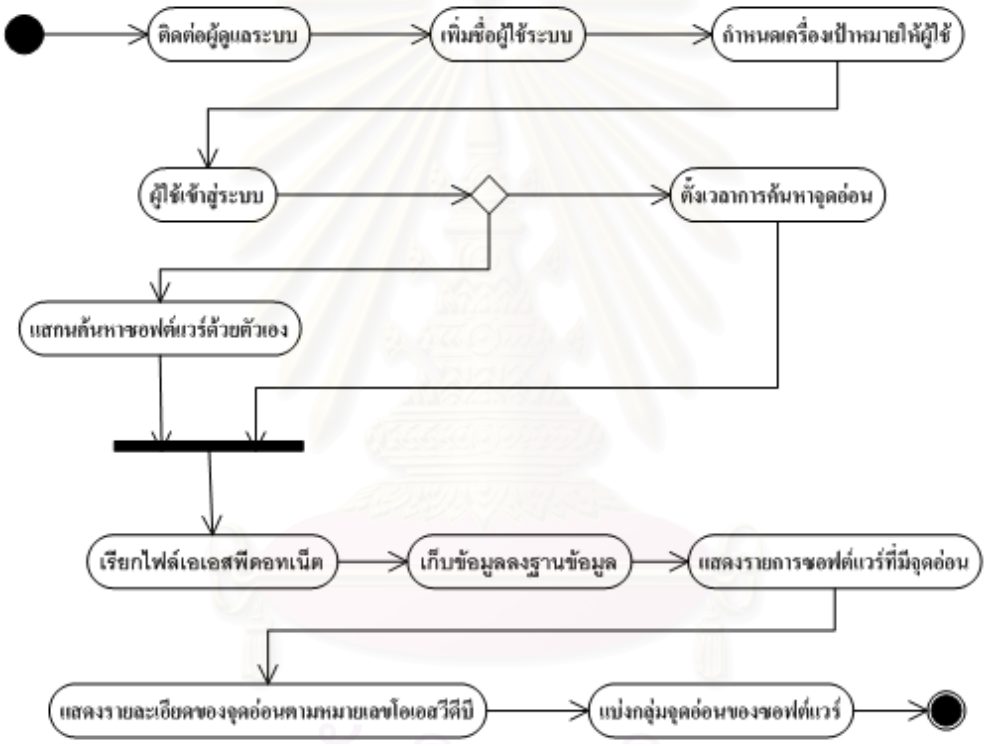
ชนิดของแผนภาพ : 3.6 ความสัมพันธ์ของตารางข้อมูล	**ชื่อระบบ**: ระบบค้นหาจุดอ่อนของซอฟต์แวร์โดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด	
ผู้จัดทำ: นายปฏิญญา จันฤาชัย	**เวอร์ชัน:** 1.00	**วันที่แก้ไขล่าสุด**: 8 มี.ค. 2548

ตารางที่ 3.3 แสดงคำอธิบายตารางข้อมูลที่เก็บในระบบจัดการฐานข้อมูล

ชื่อตาราง	คำอธิบาย
VUHRTEMP	เก็บข้อมูลผู้ใช้งานของระบบ ประกอบด้วย รหัสผู้ใช้ ชื่อ นามสกุล สถานะ ชื่อผู้ใช้ รหัสผ่าน สิทธิการใช้งาน หมายเลขโทรศัพท์ อีเมล์ ตำแหน่ง (ซึ่งข้อมูลผู้ใช้เป็นสิ่งสำคัญในการใช้งานระบบเพราะขั้นแรกต้องเพิ่มชื่อผู้ใช้ก่อน แล้วค่อยเพิ่มเครื่องเป้าหมายเพื่อให้ผู้ใช้สามารถเข้าไปสแกนรายการซอฟต์แวร์ที่มีจุดอ่อนเฉพาะเครื่องของตัวเอง)
VUCOMTARGET	เก็บข้อมูลเครื่องคอมพิวเตอร์เป้าหมาย ประกอบด้วย รหัสเครื่องเป้าหมาย ชื่อเครื่องเป้าหมายคำอธิบาย ยูอาร์แอลรายการอ้างอิงของเว็บเซอร์วิส และรหัสผู้ใช้ (จำเป็นที่จะต้องกำหนดเป็นคีย์หลัก เพราะจะใช้ชื่อในการตั้งชื่อไฟล์ซึ่งแต่ละไฟล์มีชื่อไม่ซ้ำกัน)
VUTIME	เก็บข้อมูลการตั้งเวลา ประกอบด้วย รหัส เวลา ผู้ตั้งเวลา รหัสเครื่องเป้าหมาย
VUCANCELWORD	เก็บข้อมูลคำที่ไม่ต้องการที่จะค้นหา ประกอบด้วย รหัส คำ ผู้กำหนด หมายเหตุ
VUTRACE	เก็บข้อมูลรายการซอฟต์แวร์ที่เครื่องเป้าหมายโดยบอกถึงรายการซอฟต์แวร์มีจุดอ่อน ประกอบด้วย รหัส เวอร์ชันของซอฟต์แวร์ ชื่อซอฟต์แวร์ ชื่อเครื่อง รหัส และชื่อผู้ใช้เพื่อแสดงผลเฉพาะผลลัพธ์ที่ผู้ใช้ได้ทำการค้นหา
VUTRACEDETAIL	เก็บข้อมูลชื่อซอฟต์แวร์และเวอร์ชันของซอฟต์แวร์โดยนำข้อมูลมาจากฐานข้อมูลจุดอ่อนระบบเปิด ประกอบด้วย รหัสคำอธิบาย ชื่อเครื่อง ชื่อซอฟต์แวร์ เวอร์ชัน และหมายเลขโอเอสวีดีบี

3.5 แผนภาพกิจกรรมการทำงาน (Activity Diagram)

เริ่มจากติดต่อผู้ดูแลระบบเพื่อนำข้อมูลผู้ใช้เข้าสู่ระบบและกำหนดเครื่องเป้าหมายให้กับผู้ใช้ เมื่อผู้ใช้เข้าสู่ระบบจะสามารถทำงานได้กับเฉพาะเครื่องของตนเอง ซึ่งสามารถสแกนรายการซอฟต์แวร์และตรวจสอบรายงานผลรายการซอฟต์แวร์ที่มีจุดอ่อนและสิ้นสุดการทำงาน ดังแผนภาพที่ 3.6



ชนิดของแผนภาพ : 3.7 กิจกรรมการทำงาน	**ชื่อระบบ**: ระบบค้นหาจุดอ่อนของซอฟต์แวร์โดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด	
ผู้จัดทำ: นายปฏิญญา จันฤาชัย	**เวอร์ชัน:** 1.00	**วันที่แก้ไขล่าสุด**: 8 มี.ค. 2548

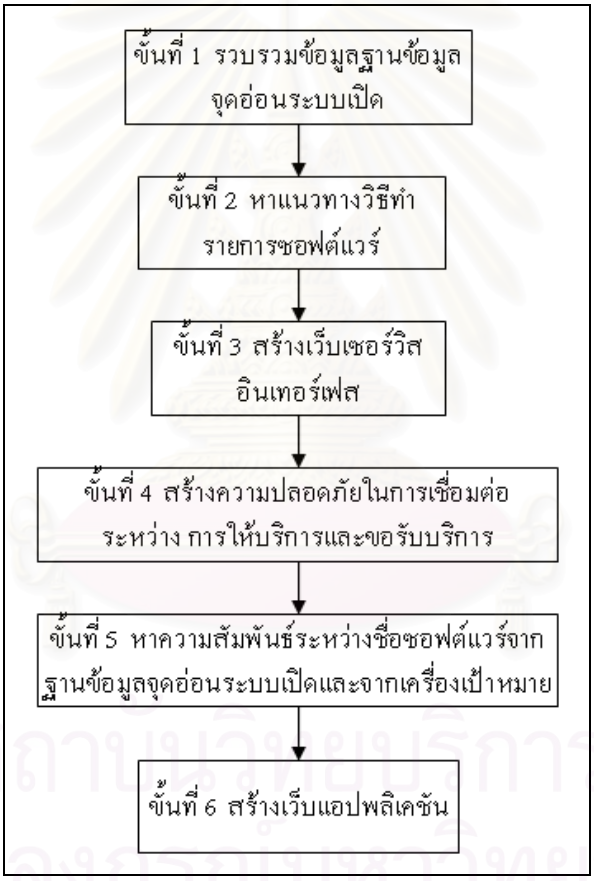
บทที่ 4

การพัฒนาเครื่องมือค้นหาจุดอ่อนของซอฟต์แวร์

ในบทนี้จะกล่าวถึงการพัฒนาเครื่องมือค้นหาจุดอ่อนของซอฟต์แวร์โดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด ที่พัฒนาขึ้นจากการออกแบบในบทที่ 3

4.1 ขั้นตอนการพัฒนาระบบ

ขั้นตอนในการพัฒนาระบบประกอบด้วย 6 ขั้นตอนดังรูปที่ 4.1



รูปที่ 4.1 ขั้นตอนในการพัฒนาระบบ

ขั้นที่ 1 รวบรวมข้อมูลจากฐานข้อมูลจุดอ่อนระบบเปิด

รวบรวมข้อมูลจากฐานข้อมูลจุดอ่อนระบบเปิดโดยจะทำการแยกเป็นหมวดหมู่และตรวจสอบรายละเอียดของฐานข้อมูลจุดอ่อนแล้วการสรุปเพื่อเลือกใช้คำสั่งในการค้นหาในฐานข้อมูล (SQL: Structure Query Language) เพื่อให้ค้นหาข้อมูลได้อย่างถูกต้อง โดยข้อมูลที่ได้ใน

เบื้องต้นแล้วจะเป็นข้อมูลที่เกี่ยวกับ ผลิตภัณฑ์ ข้อมูลรายละเอียดจุดอ่อน รายการอ้างอิง ผู้ค้นพบ แต่ยังไม่มีข้อมูลคะแนนและอัตราความเสี่ยง

ขั้นที่ 2 หาแนวทางวิธีทำรายการซอฟต์แวร์

ใช้ซอฟต์แวร์โอซีเอส อินเวนทอรี่ (OCS Inventory: Open Computer and Software Inventory) ค้นหาและรวบรวมรายการซอฟต์แวร์ บนระบบปฏิบัติการวินโดวส์ ซึ่งจะบันทึกข้อมูลรายละเอียดต่างๆที่ค้นพบเกี่ยวกับเครื่องคอมพิวเตอร์บันทึกไว้ที่ฐานข้อมูลไมโครซอฟท์แอคเซส (Microsoft Access) ศึกษารายละเอียดเพิ่มเติมได้ที่ภาคผนวก ก

ขั้นที่ 3 สร้างเว็บเซอร์วิสอินเทอร์เฟส

ทำการกำหนดและพัฒนาส่วนเชื่อมต่อของเว็บเซอร์วิสในส่วนของฐานข้อมูลจุดอ่อนระบบเปิด โดยระบุฟังก์ชันการค้นหาจุดอ่อน ที่มีผลกระทบกับซอฟต์แวร์ และเวอร์ชันที่กำหนด ส่งผลลัพธ์มาเป็นเอ็กซ์เอ็มแอลไฟล์ จากนั้นพัฒนาส่วนเชื่อมต่อเว็บเซอร์วิสในส่วนรายการซอฟต์แวร์ที่เครื่องเป้าหมายโดยระบุฟังก์ชันการตรวจสอบซอฟต์แวร์และส่งผลเป็นเอ็กซ์เอ็มแอลไฟล์ ในการสร้างเว็บเซอร์วิสจะมีฟังก์ชันการทำงานต่างๆ ดังตารางที่ 4.1 และ ตารางที่ 4.2

ตารางที่ 4.1 ชื่อและคำอธิบายของฟังก์ชันเว็บเซอร์วิสเครื่องฐานข้อมูลจุดอ่อนระบบเปิด

ชื่อฟังก์ชัน	อธิบาย
1.**GetDescOSVDBID**	เป็นฟังก์ชันที่ใช้สำหรับในการอธิบายข้อมูลของฐานข้อมูลจุดอ่อนระบบเปิด ซึ่งจะรับพารามิเตอร์เป็นหมายเลขรหัสโอเอสวีดีบี
2. **SRCsoftwarevuln**	เป็นฟังก์ชันที่ใช้สำหรับการค้นหาเวอร์ชันและชื่อของซอฟต์แวร์ที่มีจุดอ่อนโดยค่าที่ส่งกลับจะเป็นชื่อซอฟต์แวร์ เวอร์ชัน และ รายละเอียดของซอฟต์แวร์ในฐานข้อมูลจุดอ่อนระบบเปิด
3. **Findnameversion**	เป็นฟังก์ชันที่ใช้สำหรับการตรวจสอบชื่อและเวอร์ชันของซอฟต์แวร์โดยค่าที่ส่งกลับมาจะเป็น Yes (ค้นพบ) หรือ No (ค้นไม่พบ)

ตารางที่ 4.1 ชื่อและคำอธิบายของฟังก์ชันเว็บเซอร์วิสเครื่องฐานข้อมูลจุดอ่อนระบบเปิด (ต่อ)

ชื่อฟังก์ชัน	อธิบาย
4. **Findname**	เป็นฟังก์ชันที่ใช้สำหรับการตรวจสอบชื่อของซอฟต์แวร์โดยผลลัพธ์ที่ส่งกลับมาจะเป็นYes (ค้นพบ) หรือ No (ค้นไม่พบ)
5. **Edtosvdbupdate**	เป็นฟังก์ชันที่ใช้สำหรับในการปรับปรุงข้อมูลของฐานข้อมูลจุดอ่อนระบบเปิด

ตารางที่ 4.2 รายการชื่อและคำอธิบายของฟังก์ชันเว็บเซอร์วิสที่เครื่องเป้าหมาย

ชื่อฟังก์ชัน	อธิบาย
1. **Getinventory**	เป็นฟังก์ชันที่ใช้สำหรับในการเรียกข้อมูลจากฐานข้อมูลเครื่องเป้าหมายโดยจะทำการใส่ค่าพารามิเตอร์เป็นซอฟต์แวร์ เพื่อนำรายการซอฟต์แวร์จากเครื่องเป้าหมาย
2. **RunProcess**	เป็นฟังก์ชันที่ใช้สำหรับในการสั่งให้โปรแกรมโอซีเอสอินเวนทอรี่ ค้นหารายการซอฟต์แวร์ที่เครื่องเป้าหมาย

ขั้นที่ 4 สร้างความปลอดภัยในการเชื่อมต่อระหว่างการให้บริการและขอรับบริการ

จากการศึกษาพบว่า การสร้างความปลอดภัยของเว็บเซอร์วิส โดยการใช้ภาษาเอเอสพีดอทเน็ต (ASP.NET) [22] มีอยู่ด้วยกัน 3 แบบคือ 1.ใช้ไฟล์คอนฟิกของเว็บที่ชื่อว่า เว็บคอทคอนฟิก (Web.config) 2.ใช้เว็บเซิร์ฟเวอร์ และ 3.ใช้การเพิ่มเติมเข้าไปในส่วนหัวของโปรโตคอลโซพ (SOAPHeader) เพื่อให้การติดต่อระหว่างการให้บริการและขอรับบริการ มีความปลอดภัยซึ่งในงานวิจัยชิ้นนี้ จะใช้ไฟล์คอนฟิกของเว็บ (แบบที่1) เพราะสะดวกในการใช้งาน การให้สิทธิการใช้งานจะกระทำได้โดยการเพิ่ม แท็ก (Tag) <authorization> ในไฟล์เว็บคอทคอนฟิก (Web.config) ดังรูปที่ 4.2

```
<configuration>

  <system.web>
    <authentication mode="Windows"/>
  </system.web>

  <location path="secureservice.asmx">

    <system.web>
      <authorization>
        <allow users="Administrator"/>
        <allow users="DOMAIN\Bradley"/>
        <deny roles="BUILTIN\Power Users"/>
      </authorization>
    </system.web>

  </location>

</configuration>
```

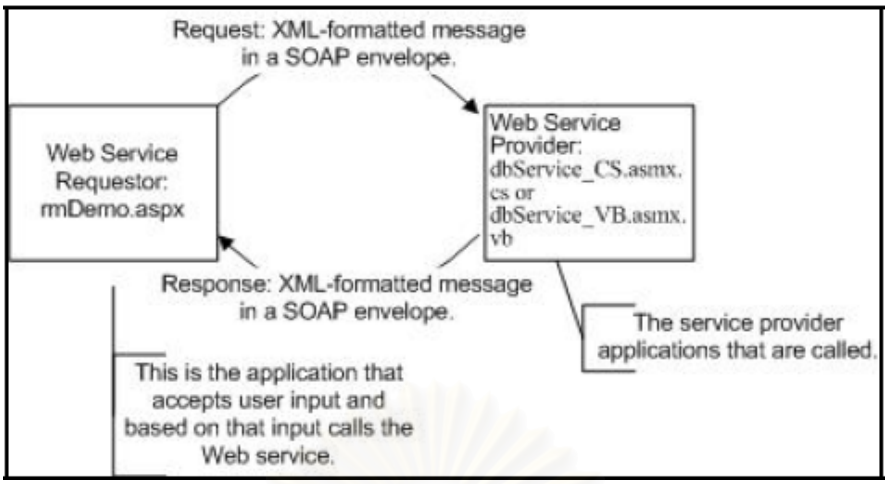
รูปที่ 4.2 กำหนดสิทธิการใช้งานเว็บเซอร์วิส

ขั้นที่ 5 หาความสัมพันธ์ระหว่างชื่อซอฟต์แวร์จากฐานข้อมูลจุดอ่อนระบบเปิดและชื่อซอฟต์แวร์ของเครื่องเป้าหมาย

ในการหาความสอดคล้องกันระหว่างชื่อซอฟต์แวร์จะใช้ลำดับขั้นตอนการหาความสัมพันธ์ที่ได้ออกแบบไว้ในบทที่ 3 การค้นหาจุดอ่อนของซอฟต์แวร์โดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด ข้อมูลที่ได้จะเป็นรายการซอฟต์แวร์เครื่องเป้าหมายที่มีจุดอ่อน ลำดับการค้นหา และหมายเลขโอเอสวีดีบี

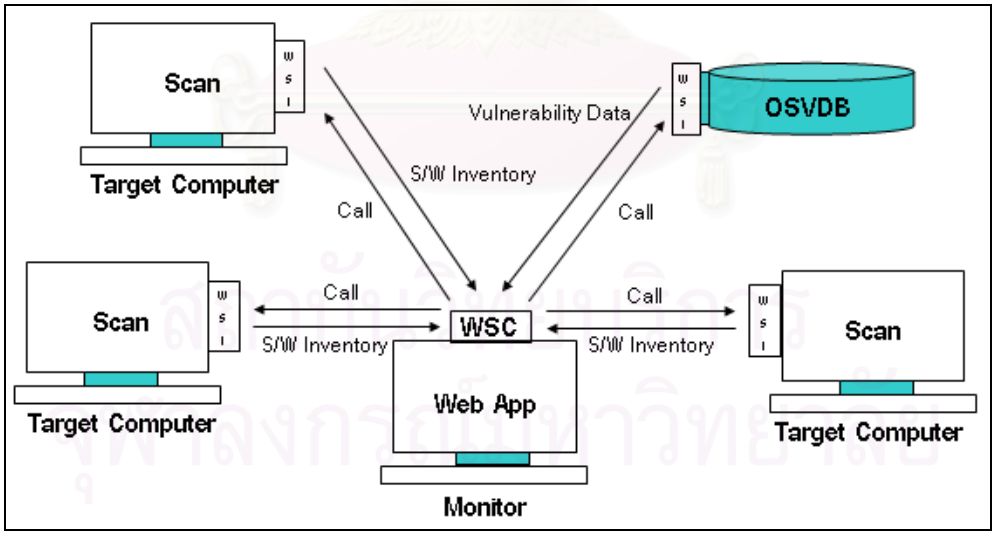
ขั้นที่ 6 สร้างเว็บแอปพลิเคชัน

การสร้างเป็นเว็บแอปพลิเคชันเมื่อเครื่องคอมพิวเตอร์ผู้ใช้ติดตั้งตัวเว็บบราวเซอร์ก็จะสามารถเข้าใช้งานได้ เครื่องเป้าหมายที่มีการเพิ่มเข้าสู่ระบบนั้นจะมีไฟล์เว็บแอปพลิเคชันหรือไฟล์เอเอสพีดอทเน็ต (ASP.net) ที่สร้างขึ้นเป็นไฟล์ประจำเครื่องของตัวเอง การสร้างไฟล์มีลักษณะการทำงานที่เป็นไดนามิก (Dynamic) คือสามารถสร้างตัวเองขึ้นมาใหม่จากไฟล์ต้นแบบได้เรื่อยๆ เมื่อมีการเพิ่มเครื่องเป้าหมายเข้าสู่ระบบจะทำการคัดลอกและเปลี่ยนชื่อไฟล์ต้นแบบเป็นชื่อเครื่องเป้าหมาย ไฟล์เว็บแอปพลิเคชันทั้งหมดที่ได้ทำการพัฒนาขึ้นจะเป็นการนำข้อมูลมาจากเว็บเซอร์วิสโดยการทำงานจะเป็นการร้องขอข้อมูลแล้วรอการตอบกลับมาของข้อมูล [23] มีลักษณะดังรูปที่ 4.3



รูปที่ 4.3 การสร้างเว็บแอปพลิเคชันจากเว็บเซอร์วิส

จากรูปที่ 4.3 เป็นการสร้างไฟล์ เอเอสพีดอทเน็ต เพื่อให้สามารถเรียกใช้การบริการ (Service) จากเว็บเซอร์วิสโดยเว็บเซอร์วิสจะคอยรับการร้องขอเมื่อได้รับการร้องขอข้อมูลจะส่งข้อมูลกลับไปในลักษณะของเอ็กซ์เอ็มแอลไฟล์ แล้วให้ไฟล์เอเอสพีดอทเน็ต (ASP.NET) ซึ่งเป็นเว็บแอปพลิเคชันทำการจัดรูปแบบรายงานผลต่อไป เมื่อนำมาประยุกต์ใช้กับเครื่องมือในการค้นหาจุดอ่อนโดยใช้ฐานข้อมูลจุดอ่อนระบบเปิดเว็บแอปพลิเคชันที่สร้างขึ้นจะทำการร้องขอบริการจากเซอร์วิสที่ได้ทำการสร้างขึ้นเพื่อนำข้อมูลมาประมวลผล ดังรูปที่ 4.4



รูปที่ 4.4 การค้นหาจุดอ่อนของซอฟต์แวร์โดยใช้เว็บเซอร์วิส

จากรูปที่ 4.4 เป็นการแสดงลักษณะของการทำงานที่เชื่อมต่อระหว่างเว็บแอปพลิเคชันกับเว็บเซอร์วิส โดยเว็บแอปพลิเคชันจะเรียกใช้เว็บเซอร์วิสทางฝั่งของฐานข้อมูลจุดอ่อนระบบเปิดและเครื่องเป้าหมายเพื่อตรวจสอบรายการซอฟต์แวร์ที่มีจุดอ่อน

4.2 สภาพแวดล้อมที่ใช้ในการทดสอบ

4.2.1 ฮาร์ดแวร์

- เครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบการค้นหาจุดอ่อนของซอฟต์แวร์ จำนวน 1 เครื่อง Intel Pentium IV 2.5 MHz แรม 512 เมกะไบต์ ความจุฮาร์ดดิสก์ 40 กิกะไบต์

- เครื่องคอมพิวเตอร์ฐานข้อมูลจุดอ่อนระบบเปิด จำนวน 1 เครื่อง Intel Pentium IV 1.4 MHz แรม 256 เมกะไบต์ ความจุฮาร์ดดิสก์ 40 กิกะไบต์

- เครื่องคอมพิวเตอร์เป้าหมาย จำนวน 4 เครื่อง Intel Pentium IV 1.4 MHz แรม 256 เมกะไบต์ ความจุฮาร์ดดิสก์ 40 กิกะไบต์

4.2.2 ซอฟต์แวร์

- ไมโครซอฟต์ ด็อตเน็ต เฟรมเวิร์ค (Microsoft.Net Framework) รุ่น 1.0.3705

- ไอไอเอส (IIS: Internet Information Server) เวอร์ชัน 6.0 ซึ่งเป็นเครื่องบริการเว็บเซิร์ฟเวอร์ (Web Server) และเป็นส่วนหนึ่งของระบบปฏิบัติการวินโดวส์ด็อตเน็ตเอ็นเตอร์ไพรซ์ เซิร์ฟเวอร์

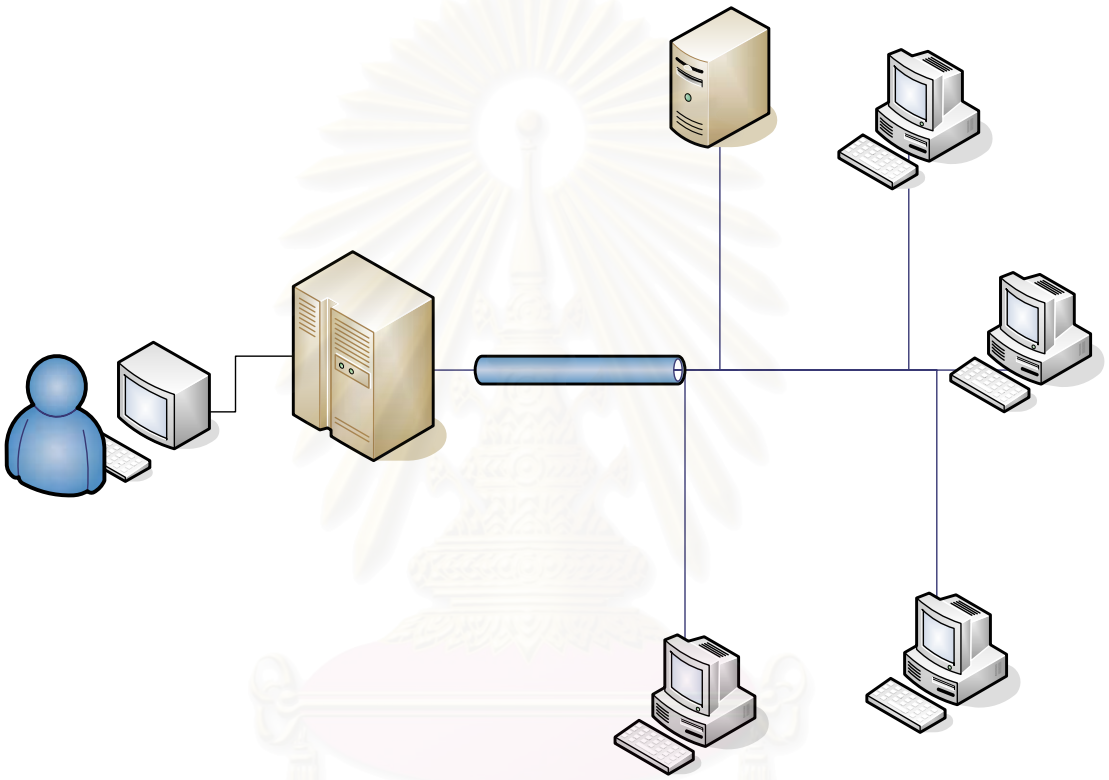
- อินเทอร์เน็ต เอ็กซ์พลอเรอร์ (Internet Explore) เวอร์ชัน 5.5 หรือสูงกว่าทำหน้าที่เป็นเว็บเบราว์เซอร์ (Web Browser)

- ฐานข้อมูลไมโครซอฟต์แอสเซส (Microsoft Access) เวอร์ชันเอ็กซ์พี (XP)

- ซอฟต์แวร์ โอซีเอส อินเวนทอรี่ (Open Computer and Software Inventory) เวอร์ชัน 3.00b3

- คอมโพเนนต์ แอคทีฟซอกเก็ต เน็ตเวิร์ค (Active Socket Network) เวอร์ชัน 2.3

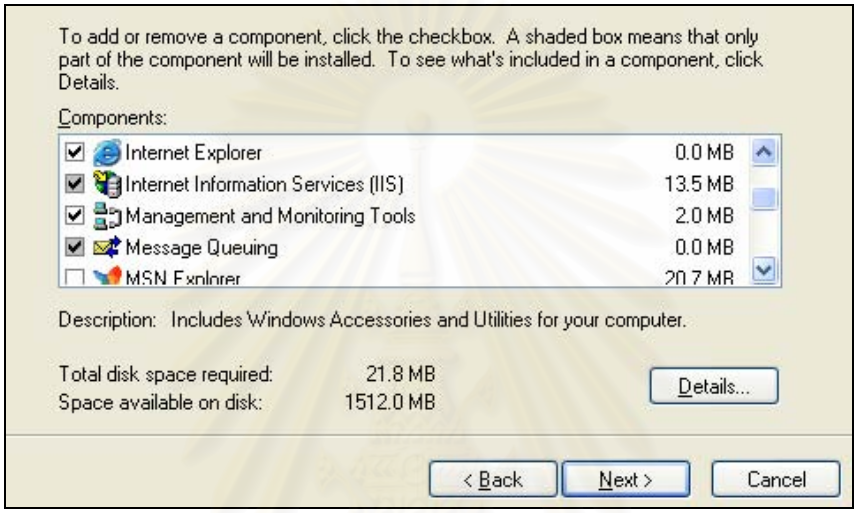
เริ่มจากการที่เครื่องศูนย์กลางเป็นผู้ร้องขอบริการผ่านทางเว็บเซอร์วิส เครื่องเป้าหมายทุกเครื่อง (Target1 - 4) เมื่อได้รับการร้องขอข้อมูลจะส่งข้อมูลไปให้เครื่องศูนย์กลางเป็นไฟล์เอ็กซ์เอ็มแอล (XML) เมื่อเครื่องศูนย์กลางได้รับไฟล์เอ็กซ์เอ็มแอลจะนำเอาชื่อและเวอร์ชันของซอฟต์แวร์ที่เครื่องเป้าหมายแต่ละเครื่องมาตัดคำเพื่อนำไปค้นกับเว็บเซอร์วิสของทางฐานข้อมูลจุดอ่อนระบบเปิด (OSVDB Server) เมื่อได้รับผลลัพธ์อย่างไรจะเก็บข้อมูลไว้ที่ฐานข้อมูลที่เครื่องศูนย์กลาง (Application Server) แสดงได้ดังแผนภาพที่ 4.1



ชนิดของแผนภาพ : 4.1 แผนผังการทดสอบ	**ชื่อระบบ**: ระบบค้นหาจุดอ่อนของซอฟต์แวร์โดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด	
ผู้จัดทำ:นายปฏิญญา จันฤาชัย	**เวอร์ชัน:** 1.00	**วันที่แก้ไขล่าสุด**: 8 มี.ค. 2548

4.3 การติดตั้งซอฟต์แวร์

4.3.1 สำหรับระบบปฏิบัติการวินโดวส์ (Windows) ที่จะนำมาทดสอบให้เพิ่มในส่วนของแอดออน คอมโพเนนต์ (Add-On Components) ในส่วนของไอไอเอส (IIS) เพื่อให้ระบบสามารถทำงานเป็นเว็บเซิร์ฟเวอร์ (Web Server) ได้ ซึ่งจะต้องทำการติดตั้งแก่เครื่องคอมพิวเตอร์ทั้งหมดได้แก่ เครื่องศูนย์กลาง เครื่องเป้าหมาย และเครื่องฐานข้อมูลจุดอ่อนระบบเปิด ดังรูปที่ 4.5



รูปที่ 4.5 การติดตั้งเว็บเซิร์ฟเวอร์

4.3.2 ทำการติดตั้งในส่วนของซอฟต์แวร์ที่จำเป็นต้องใช้ได้แก่

4.3.2.1 ดอทเน็ตเอฟเอ็กซ์ (dotnetfx) ซึ่งจะทำให้เครื่องสามารถรันระบบแอปพลิเคชันที่พัฒนาด้วยดอทเน็ตเฟรมเวิร์กได้ ซึ่งจะต้องทำการติดตั้งไว้ที่เครื่องศูนย์กลาง เครื่องเป้าหมาย และเครื่องฐานข้อมูลจุดอ่อนระบบเปิด

4.3.2.2 นำซอฟต์แวร์สแกนรายการซอฟต์แวร์โอซีเอสอินเวนทอรี่ ไปติดตั้งไว้ที่ เครื่องเป้าหมาย รายละเอียดเพิ่มเติมภาคผนวก ก

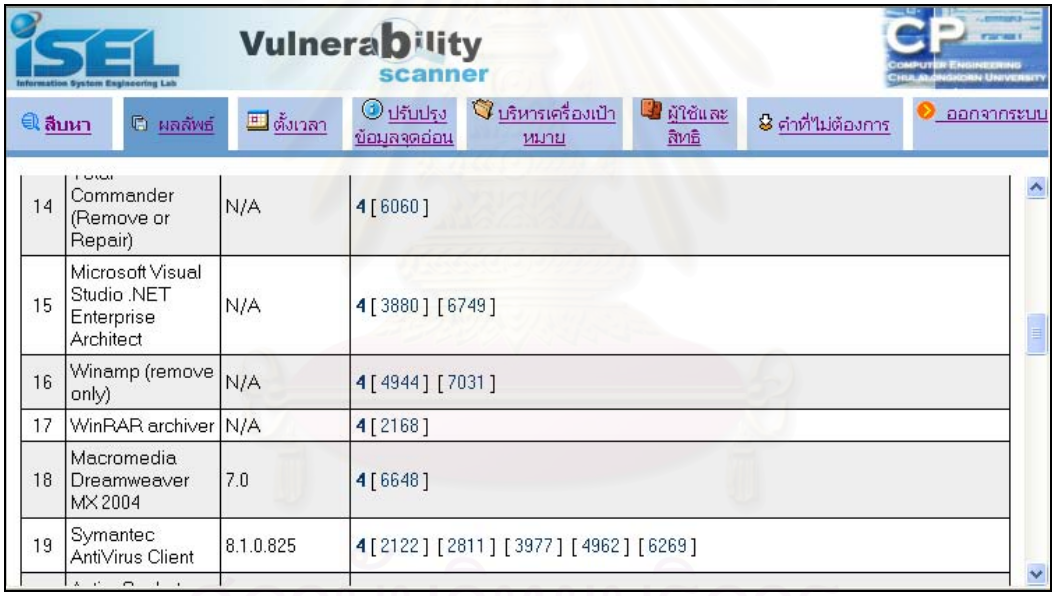
4.3.2.3 ติดตั้งซอฟต์แวร์ที่จะช่วยให้เครื่องเป้าหมายสามารถทำงานเป็นเว็บเซอร์วิสอินเทอร์เฟสให้บริการข้อมูลเมื่อได้รับการร้องขอข้อมูลจากเครื่องศูนย์กลางได้ ซอฟต์แวร์มีชื่อว่า ทาร์เก็ตเว็บเซ็ตอัพ (TargetWebSetup.msi)

4.3.3 ติดตั้งซอฟต์แวร์เครื่องมือการค้นหาจุดอ่อนของซอฟต์แวร์โดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด (ซอฟต์แวร์หลักในการทำงานและประมวลผล) ที่เครื่องคอมพิวเตอร์ศูนย์กลาง

4.3.4 รันโปรแกรมค้นหาจากการตั้งเวลาทำงานเพื่อโปรแกรมจะอ่านข้อมูลการตั้งเวลาแล้วทำการสแกนรายการซอฟต์แวร์เพื่อค้นหาจุดอ่อนของซอฟต์แวร์แบบอัตโนมัติ โปรแกรมจะต้องเปิดไว้ตลอดเวลาเพื่ออ่านข้อมูลการตั้งเวลา

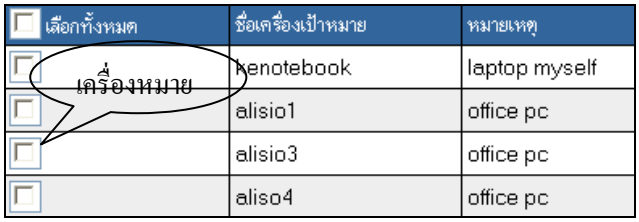
4.4 ส่วนติดต่อกับผู้ใช้

ในการใช้งานเครื่องมือการค้นหาจุดอ่อนของซอฟต์แวร์ ในส่วนของพื้นที่การใช้งานมีการแบ่งเป็น สองเฟรม (Flame) เฟรมแรกจะเป็นส่วนของโลโก้และเมนู เฟรมที่สองด้านล่างจะไว้สำหรับแสดงผลข้อมูลเมื่อข้อมูลมีจำนวนมากสามารถใช้สกรอล (Scroll Bar) เลื่อนดูข้อมูลการแสดงผลโดยที่เฟรมแรก (โลโก้และเมนู) ไม่ขยับทำให้ผู้ใช้ยังรู้อยู่ว่าตอนนี้อยู่เมนูใดแล้ว ลักษณะดังรูปที่ 4.6



รูปที่ 4.6 ส่วนติดต่อกับผู้ใช้

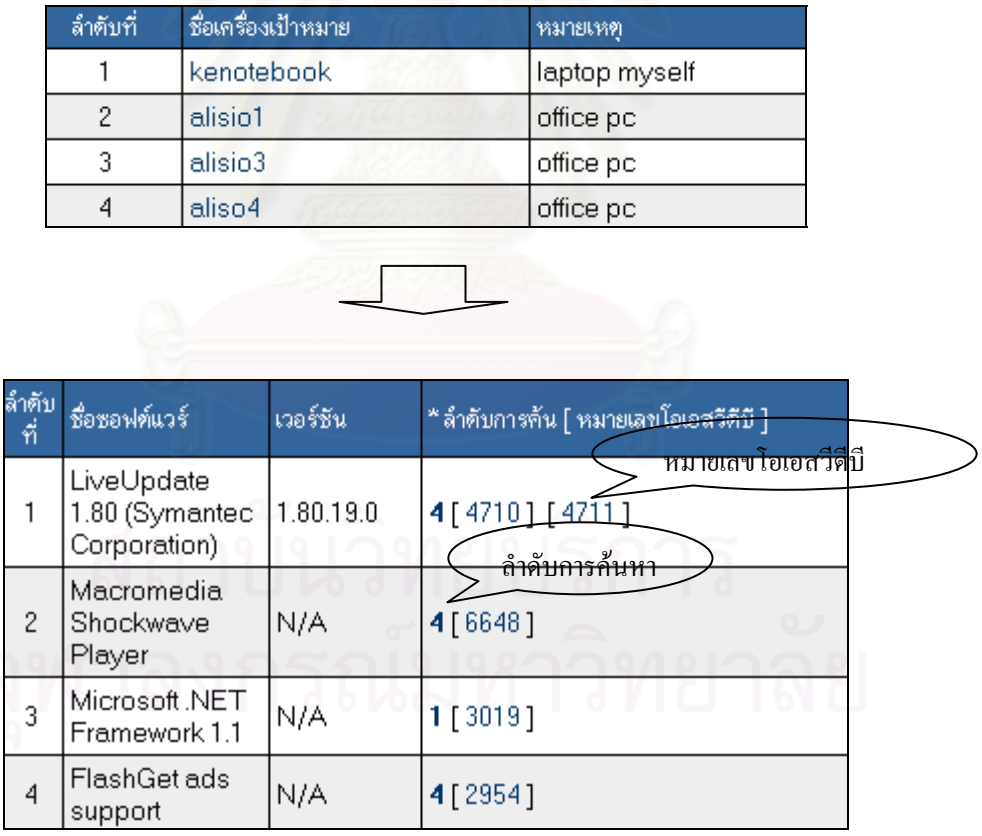
4.4.1 การค้นหา เป็นการระบุเครื่องที่ต้องการโดยให้ทำเครื่องหมายที่หน้าเครื่องที่จะกระทำการค้นหาจุดอ่อนของซอฟต์แวร์ซึ่งสามารถทำการค้นหาได้ทั้งหมดหรือระบุเฉพาะเครื่องที่ต้องการตรวจสอบเท่านั้น ดังรูปที่ 4.7



รูปที่ 4.7 ส่วนของการค้นหาจุดอ่อนของซอฟต์แวร์

เมื่อได้ทำการค้นหาจุดอ่อนของซอฟต์แวร์แล้วผลลัพธ์ที่ได้จะเก็บไว้ในฐานข้อมูลเพื่อสามารถนำผลลัพธ์มาวิเคราะห์ได้ในภายหลัง ซึ่งจะอยู่ในส่วนของการรายงานผลลัพธ์ที่ได้จากการค้นหาโดยใช้เครื่องมือค้นหาจุดอ่อนของซอฟต์แวร์

4.4.2 การรายงานซอฟต์แวร์ที่มีจุดอ่อน การรายงานผลสามารถกระทำได้โดยเลือกเครื่องเป้าหมายที่ต้องการตรวจสอบผลลัพธ์จะได้รายการซอฟต์แวร์ที่มีจุดอ่อนซึ่งจะมีหมายเลขโอเอสวีดีบี แสดงได้ดังรูปที่ 4.8



รูปที่ 4.8 รายงานผลลัพธ์จากการค้นหา

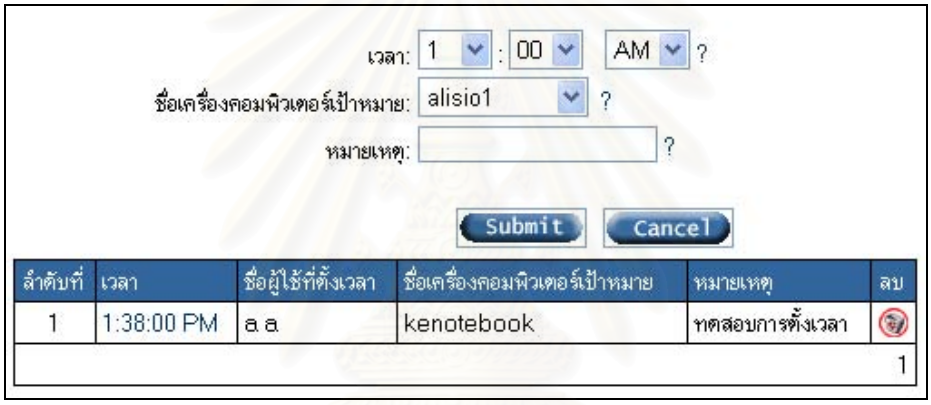
ในส่วนของรายการซอฟต์แวร์ที่มีจุดอ่อนประจำเครื่องนั้นจะประกอบด้วยชื่อซอฟต์แวร์และเวอร์ชันของซอฟต์แวร์ ลำดับการค้นหาโดยมีการกำหนดหมายเลขตั้งแต่หมายเลข

ศูนย์ถึงหมายเลขสี่ (ซึ่งได้ออกแบบลำดับการค้นหาไว้ในบทที่ 3) สุดท้ายเป็นหมายเลขโอเอสวีดีบีของจุดอ่อนเพื่อเชื่อมโยงไปสู่คำอธิบายอย่างละเอียดต่อไป

4.5 ส่วนของการบริหารเครื่องมือค้นหาจุดอ่อนของซอฟต์แวร์

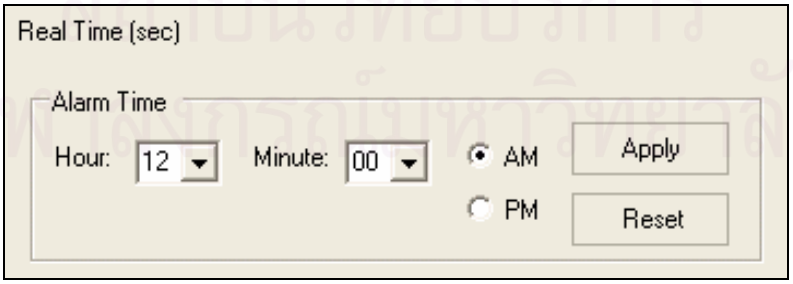
ส่วนของการบริหาร ทำหน้าที่ในการจัดการเกี่ยวกับคุณสมบัติของเครื่องมือ การเชื่อมต่อและความสามารถอื่นๆ ได้แก่

4.5.1 การตั้งเวลาเป็นการกำหนดเวลาการค้นหาจุดอ่อนของซอฟต์แวร์ผ่านทางเว็บ การกำหนดเวลาจะเป็น 00:00 AM/PM และต้องมีการระบุเครื่องที่ต้องการค้นหาจะต้องมีการรันโปรแกรมค้นหาจากการตั้งเวลาทำงานที่เครื่องคอมพิวเตอร์ศูนย์กลางเสมอ การตั้งเวลากำหนดได้ดังรูปที่ 4.9



รูปที่ 4.9 ส่วนของการตั้งเวลา

โปรแกรมค้นหาจากการตั้งเวลาทำงานนั้นจะมีลักษณะคล้ายกับโปรแกรมการแจ้งเตือนซึ่งเมื่อถึงเวลาที่กำหนด จะสามารถแจ้งให้ผู้ใช้ทราบ ดังรูปที่ 4.10



รูปที่ 4.10 โปรแกรมค้นหาจากการตั้งเวลา

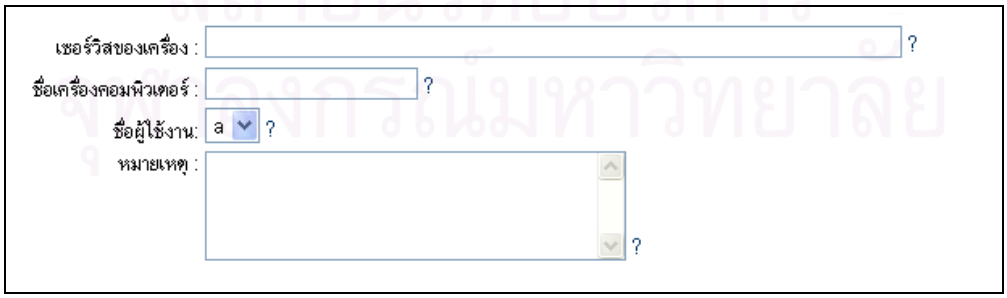
โดยโปรแกรมจะทำหน้าที่อ่านฐานข้อมูลและเมื่อถึงเวลาที่กำหนดไว้จะทำการค้นหาจุดอ่อนของซอฟต์แวร์ ซึ่งโปรแกรมจะต้องมีการเปิดบริการหรือรันโปรแกรมถึงจะสามารถทำให้การตั้งเวลาไว้ใช้งานได้

4.5.2 การปรับปรุงฐานข้อมูลจุดอ่อน มีปุ่มสำหรับการเรียกใช้คำสั่งไปที่เครื่องฐานข้อมูลจุดอ่อนระบบเปิด ดังรูปที่ 4.11

รูปที่ 4.11 ส่วนของการปรับปรุงข้อมูลฐานข้อมูลจุดอ่อน

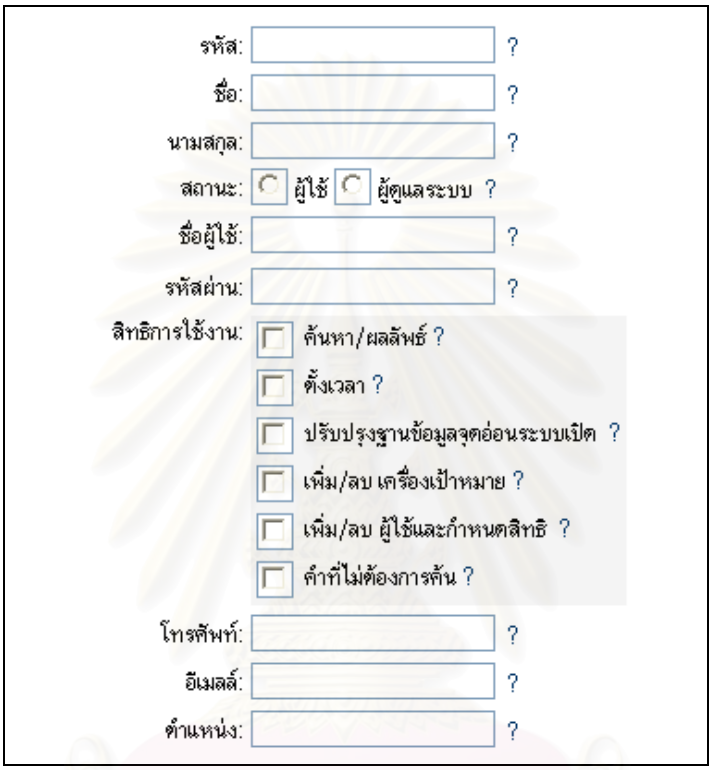
การปรับปรุงฐานข้อมูลจุดอ่อนจะเป็นการสั่งให้รันสคริปต์ไฟล์ที่เครื่องฐานข้อมูลจุดอ่อนระบบเปิดเพื่อนำเอาไฟล์เอ็กซ์เอ็มแอลของข้อมูลจุดอ่อนที่ได้จากทางเว็บไซต์โอเอสวีดีบีดอทโออาร์จี (OSVDB.org) ลงสู่ฐานข้อมูลจุดอ่อนระบบเปิด เพื่อปรับปรุงข้อมูลที่ใช้ในการอ้างอิงในการค้นหาจุดอ่อนของซอฟต์แวร์ของเครื่องคอมพิวเตอร์ (ใช้ในกรณีที่ต้องการปรับปรุงฐานข้อมูลผ่านทางเว็บแอปพลิเคชัน)

4.5.3 การเพิ่มลบเครื่องเป้าหมายจะเป็นการสร้างการติดต่อระหว่างเครื่องศูนย์กลางและเครื่องเป้าหมายเพื่อให้ระบบสามารถร้องขอข้อมูลจากเครื่องเป้าหมายได้ผ่านทางเว็บเซอร์วิส (Web Service) จะต้องมีการระบุยูอาร์แอลเว็บเซอร์วิสอินเทอร์เฟสที่ใช้อ้างอิงและชื่อเครื่องที่ถูกต้องโดยในการกำหนดชื่อเครื่องเป้าหมายจะต้องกำหนดไม่ให้ซ้ำกับชื่อเครื่องเป้าหมายที่เคยตั้งไว้อยู่แล้ว เพราะชื่อจะใช้เป็นชื่อไฟล์เว็บแอปพลิเคชันประจำเครื่องของเครื่องเป้าหมายแต่ละเครื่อง ดังรูปที่ 4.12



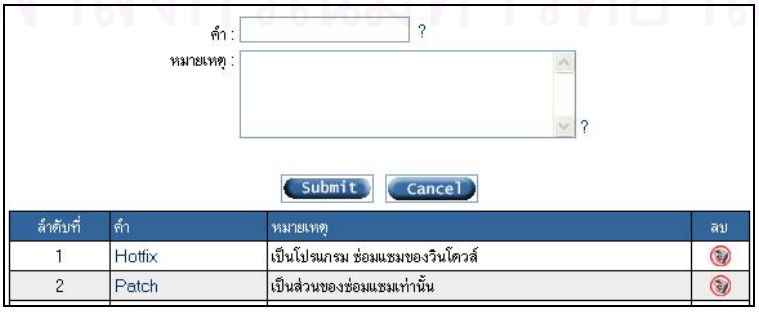
รูปที่ 4.12 ส่วนของการเพิ่มและลบเครื่องเป้าหมาย

4.5.4 การเพิ่มลบผู้ใช้และกำหนดสิทธิ จะเป็นการกำหนดสิทธิการใช้งานให้ผู้ใช้เมื่อเข้าสู่ระบบ ซึ่งถ้าเป็นซอฟต์แวร์เกี่ยวกับความปลอดภัยก็น่าที่จะมีระบบความปลอดภัยของตัวเองด้วย การเพิ่มผู้ใช้เข้าสู่ระบบและระบุสิทธิการใช้งานเป็นการทำงานขั้นตอนแรกของการเริ่มกิจกรรมการทำงานของระบบ สถานะจะมีทั้งผู้ใช้ และ ผู้ดูแลระบบ การเพิ่มผู้ใช้และกำหนดสิทธิสามารถกระทำได้ดังรูปที่ 4.13



รูปที่ 4.13 ส่วนของการเพิ่มและลบผู้ใช้ กำหนดสิทธิผู้ใช้

4.5.5 คำที่ไม่ต้องการค้นคือเมื่อมีรายชื่อซอฟต์แวร์ใดที่ซ้ำกันมากๆ หรือเป็นซอฟต์แวร์ที่ไม่น่าจะนำมาทำการค้นหาจะสามารถที่จะกำหนดให้โปรแกรมข้ามผ่านซอฟต์แวร์ที่มีคำเหล่านั้นได้ ดังรูปที่ 4.14



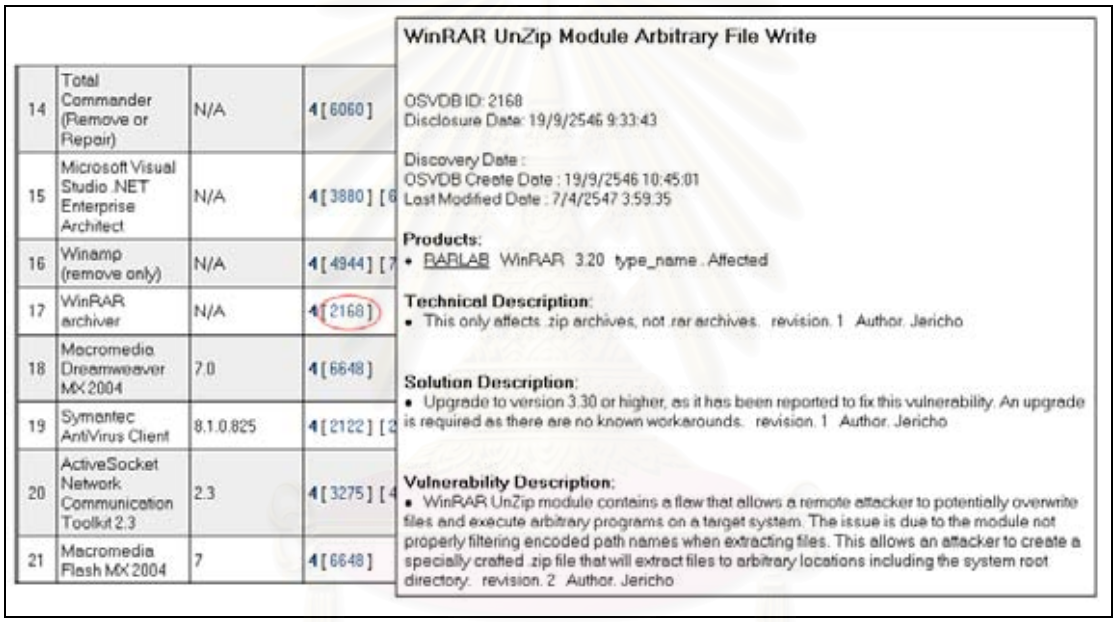
รูปที่ 4.14 ส่วนของการกำหนดคำที่ไม่ต้องการ

บทที่ 5

ผลการวิจัย

5.1 ผลการทดสอบ

5.1.1 จัดหมวดหมู่ของประเภทของซอฟต์แวร์ที่ค้นพบโดยทำการแยกผลของการค้นหาจุดอ่อนของซอฟต์แวร์ที่ได้ผลลัพธ์ถูกต้องและไม่ถูกต้อง แสดงได้ดังตารางที่ 5.1 โดยผลลัพธ์ในการการค้นหาแสดงได้ดังรูปที่ 5.1



14	Total Commander (Remove or Repair)	N/A	4 [6060]
15	Microsoft Visual Studio .NET Enterprise Architect	N/A	4 [3880] [6
16	Winamp (remove only)	N/A	4 [4944] [7
17	WinRAR archiver	N/A	4 [2168]
18	Macromedia Dreamweaver MX 2004	7.0	4 [6648]
19	Symantec AntiVirus Client	8.1.0.825	4 [2122] [2
20	ActiveSocket Network Communication Toolkit 2.3	2.3	4 [3275] [4
21	Macromedia Flash MX 2004	7	4 [6648]

รูปที่ 5.1 ผลลัพธ์ที่ได้จากการค้นหา

จากรูปที่ 5.1 แสดงรายการซอฟต์แวร์ที่มีจุดอ่อน ลำดับขั้นตอนการค้นและหมายเลขโอเอสวีดีบี และรายละเอียดตามหมายเลขโอเอสวีดีบี โปรแกรมจะต้องทำการประมวลผลในส่วนรายละเอียดจาก ไบนาริ่เป็นเป็นข้อความทำให้การแสดงรายละเอียดขึ้นมาต้องใช้เวลาสักพัก

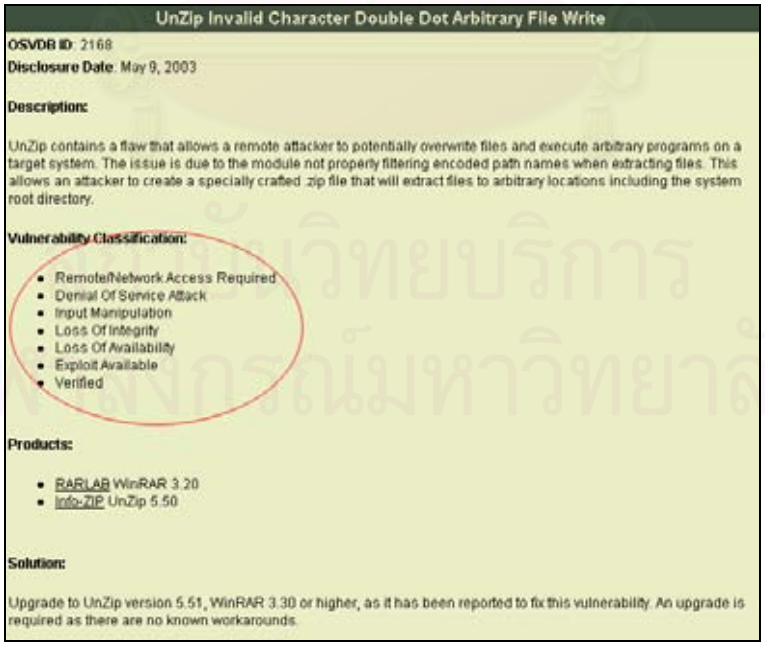
ผลลัพธ์ถูกต้องคือเป็นรายการซอฟต์แวร์ที่มีจุดอ่อนเมื่อตรวจสอบดูแล้วมีส่วนเกี่ยวข้องกับซอฟต์แวร์ในฐานข้อมูลจุดอ่อนระบบเปิด

ผลลัพธ์ไม่ถูกต้องคือไม่ใช่รายการซอฟต์แวร์ที่มีจุดอ่อนและไม่เกี่ยวข้องกับซอฟต์แวร์ที่มีจุดอ่อนที่ค้นพบ

ตารางที่ 5.1 ผลลัพธ์จากการค้นหาจุดอ่อนของซอฟต์แวร์

เครื่อง	ผลการค้นหา		รวม	%ความถูกต้อง
	ถูกต้อง	ไม่ถูกต้อง		
1. Target1 (kenotebook)	24	6	30	80%
2. Target2 (Alisio1)	11	15	26	42.30%
3. Target3 (Alisio2)	8	6	14	57.14%
4. Target4 (Alisio3)	10	8	18	55.55%
รวม	53	35	88	58.75%

นำผลการค้นหาที่ถูกต้องมาแยกเป็น 5 กลุ่มได้แก่สถานที่ (Location) การโจมตี (Attack type) ผลกระทบ (Impact) การประกาศ (Exploit Availability) และเกี่ยวกับฐานข้อมูลโอเอสวีดีบี (OSVDB) ผลลัพธ์แสดงไว้ในตารางที่ 5.1 - 5.6 โดยอ้างอิงจากทางเว็บไซต์ของโอเอสวีดีบีโดยตรง ซึ่งข้อมูลที่นำมาใช้อ้างอิง แสดงได้ดังรูปที่ 5.2



UnZip Invalid Character Double Dot Arbitrary File Write

OSVDB ID: 2168

Disclosure Date: May 9, 2003

Description:

UnZip contains a flaw that allows a remote attacker to potentially overwrite files and execute arbitrary programs on a target system. The issue is due to the module not properly filtering encoded path names when extracting files. This allows an attacker to create a specially crafted .zip file that will extract files to arbitrary locations including the system root directory.

Vulnerability Classification:

- Remote/Network Access Required
- Denial Of Service Attack
- Input Manipulation
- Loss Of Integrity
- Loss Of Availability
- Exploit Available
- Verified

Products:

- RARLAB WinRAR 3.20
- Info-ZIP UnZip 5.50

Solution:

Upgrade to UnZip version 5.51, WinRAR 3.30 or higher, as it has been reported to fix this vulnerability. An upgrade is required as there are no known workarounds.

รูปที่ 5.2 หมวดหมู่ของจุดอ่อนตามหมายเลขโอเอสวีดีบี

ตารางที่ 5.2 แยกเป็นกลุ่มสถานที่ (Location)

ประเภท	จำนวน	เปอร์เซ็นต์
กายภาพ (Physical)	-	0%
เฉพาะที่หรือภายใน (Local/Shell)	34	37.7%
รีโมทหรือเครือข่าย (Remote/Network)	53	60%
ระบบโทรศัพท์ (Telephony)	-	0%
ไม่ทราบ (Unknown)	3	3.3%

ตารางที่ 5.3 แยกเป็นกลุ่มประเภทการโจมตี (Attack type)

ประเภท	จำนวน	เปอร์เซ็นต์
การรับรองตัวตน (Authentication)	4	3.1%
การเข้ารหัส (Cryptographic)	1	0.9%
ไม่สามารถให้บริการได้ (Denial Of Service)	18	17.65%
ยึดข้อมูลในระหว่างส่งข้อมูล (Hijacking)	-	0%
ข้อมูลถูกเปิดเผย (Information Disclosure)	9	8.82%
โครงสร้าง (Infrastructure)	-	0%
การจัดการนำข้อมูลเข้า(Input Manipulation)	45	44.11%
การปรับแต่งที่ผิดพลาด (Misconfiguration)	5	4.9%
สภาพการแข่ง (Race Condition)	4	3.92%
อื่นๆ (Other) และไม่ทราบ	16	15.68%

ตารางที่ 5.4 แยกเป็นกลุ่มผลกระทบ (Impact)

ประเภท	จำนวน	เปอร์เซ็นต์
ไม่มีความเป็นส่วนตัว (Loss of Confidentiality)	20	17.85%
ไม่มีความน่าเชื่อถือ (Loss of Integrity)	62	55.35%
ไม่สามารถใช้งานได้ (Loss of Availability)	27	24.12%
ไม่ทราบ (Unknown)	3	2.68%

ตารางที่ 5.5 แยกเป็นกลุ่มการประกาศ (Exploit Availability)

ประเภท	จำนวน	เปอร์เซ็นต์
สามารถประกาศได้ (Available)	52	62.65%
ไม่สามารถประกาศออกไปได้ (Unavailable)	3	3.61%
ข่าวลือ (Rumored)	7	8.44%
ไม่ทราบ (Unknown)	21	25.3%

ตารางที่ 5.6 แยกเป็นกลุ่มเกี่ยวกับฐานข้อมูลโอเอสวีดีบี (OSVDB)

ประเภท	จำนวน	เปอร์เซ็นต์
ยืนยัน (Verified)	73	92.40%
หลอกลวง (Myth/Fake)	-	0%
กรณีตัวอย่าง (Best Practice)	1	1.26%
พิจารณา (Concern)	-	0%
ตรวจสอบ (Web Check)	5	6.34%

เป็นการวิเคราะห์ต่อจากผลที่ได้จากโปรแกรมการค้นหาจุดอ่อนระบบเปิดโดยใช้มือ (Manual) เพื่อสามารถประเมินได้ว่าจุดอ่อนลักษณะใดที่มีแนวโน้มสูงในผลการทดสอบครั้งนี้

5.1.2 ส่วนของลำดับการค้นหาที่ไว้ใช้หาความสัมพันธ์ระหว่างฐานข้อมูลจุดอ่อนระบบเปิดและรายการซอฟต์แวร์ที่เครื่องเป้าหมาย ลำดับการค้นหาหมายเลขที่ **4 คือ** ค้นหาชื่อแล้วพบ **3 คือ** ค้นเวอร์ชัน จากคำที่ต่อจากคำที่ค้นหาชื่อพบ **2 คือ** ค้นเวอร์ชันฟิลด์เวอร์ชัน **1 คือ** ค้นเวอร์ชันคำที่อยู่ท้ายสุดของชื่อซอฟต์แวร์ และ **0 คือ** ค้นหาแล้วไม่พบ โดยลำดับการค้นหาหมายเลข 1 จะมีความถูกต้องมากที่สุด สถิติลำดับการค้นหาแสดงได้ดังตารางที่ 5.7

ตารางที่ 5.7 สถิติลำดับการค้นหาที่กำหนดขึ้น

เครื่องเป้าหมาย	ลำดับการค้นหา					รวม
	4	3	2	1	0	
1. Target1 (kenotebook)	26	0	0	4	18	48
2. Target2 (Alisio1)	24	0	1	1	16	42
3. Target3 (Alisio3)	13	0	0	1	11	25
4. Target4 (Alisio4)	16	0	0	2	10	28
รวมทั้งหมด	79	0	1	8	55	143

5.2 การเปรียบเทียบกับเครื่องมืออื่นๆในการค้นหาจุดอ่อนของซอฟต์แวร์

5.2.1 ไมโครซอฟท์เบสไลน์ (Microsoft Baseline Security Analyzer)

โปรแกรมที่ได้จากการค้นหาโดยการใช้โปรแกรมไมโครซอฟท์เบสไลน์จะสามารถกระทำได้กับซอฟต์แวร์ซึ่งบริษัทไมโครซอฟต์ผลิตขึ้นมาเท่านั้นซึ่งถึงแม้จะมีโปรแกรมที่มีประสิทธิภาพมากแต่จะไม่สามารถบอกจุดอ่อนของซอฟต์แวร์ที่ผลิตจากผู้ผลิตรายอื่นๆได้เลย

5.2.2 โอวาล (OVAL: Open Vulnerability and Assessment Language)

โปรแกรมที่ได้จากการค้นหาโดยการใช้โอวาล เป็นการค้นหาที่สามารถกระทำได้ทั้งระบบปฏิบัติการวินโดวส์และลินุกซ์ โดยการอ้างอิงจากรายการซีวีอี ผู้ใช้จะต้องนำเอาตัวโปรแกรมโอวาล ลงไว้ที่เครื่องแล้วสั่งรัน โปรแกรมจะบันทึกผลลัพธ์ออกมาให้เป็นไฟล์ขนาดเล็กๆ การค้นหาจะเป็นแบบโฮสต์สแกนเนอร์ซึ่งข้อมูลจุดอ่อนจะติดไปกับตัวโปรแกรมทำให้ไม่ยืดหยุ่นในการปรับปรุงข้อมูลจุดอ่อนให้ทันสมัยอยู่เสมอ

5.2.3 การเปรียบเทียบระบบค้นหาจุดอ่อนของซอฟต์แวร์

จะเป็นการเปรียบเทียบโดยศึกษาจากการนำโปรแกรมมาติดตั้งและทดสอบการทำงานของโปรแกรมว่าสามารถทำอะไรในลักษณะใดได้บ้างซึ่งได้แก่โปรแกรมไมโครซอฟท์เบสไลน์ โอวาล และเครื่องมือที่ได้พัฒนาขึ้น ซึ่งสามารถทำได้ในลักษณะกว้างๆ คือเน้นประเด็นการนำไปใช้งานเช่นขึ้นอยู่กับระบบปฏิบัติการหรือไม่ การทำงานผ่านเครือข่าย และการค้นหาซอฟต์แวร์ได้หลากหลายหรือไม่

ตารางที่ 5.8 เปรียบเทียบการใช้งานเครื่องมือค้นหาจุดอ่อนของซอฟต์แวร์

เครื่องมือ	ระบบปฏิบัติการ		ทำงานผ่านเครือข่าย	ค้นหาได้กับซอฟต์แวร์จากหลายๆ ผู้ผลิต
	วินโดวส์	ลินุกซ์		
1. ไมโครซอฟท์เบสไลน์	ได้	ไม่ได้	ได้	ไม่ได้
2. โอวาล	ได้	ได้	ไม่ได้	ได้
3. เครื่องมือค้นหาจุดอ่อนของซอฟต์แวร์โดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด	ได้	ไม่ได้	ได้	ได้

บทที่ 6

สรุปผลการวิจัย และข้อเสนอแนะ

6.1 สรุปผลการวิจัย

จากการศึกษาและวิจัยเพื่อทำการออกแบบเครื่องมือสำหรับการค้นหาจุดอ่อนของซอฟต์แวร์โดยใช้ฐานข้อมูลจุดอ่อนระบบเปิด สามารถสรุปผลการวิจัยได้ดังต่อไปนี้

6.1.1 การนำรายชื่อซอฟต์แวร์แบ่งเป็นคำๆ เพื่อนำไปค้นหาในฐานข้อมูลจุดอ่อนระบบเปิดเพื่อให้สามารถบอกได้ว่ารายการซอฟต์แวร์รายการใดมีจุดอ่อนผลที่ได้ถือว่าเป็นพื้นฐานเบื้องต้นที่ดีในการค้นหารายการของซอฟต์แวร์ที่มีจุดอ่อนซึ่งเข้าใจได้ง่ายตรงไปตรงมา

6.1.2 การออกแบบระบบและพัฒนาให้เป็นเว็บแอปพลิเคชันผู้ใช้สามารถเข้าใช้งานระบบได้สะดวก รวดเร็ว

6.1.3 จากการทดสอบการใช้งานมีประสิทธิภาพพอสมควรสามารถค้นหารายการซอฟต์แวร์ที่มีจุดอ่อน แต่ยังคงมีในส่วนของซอฟต์แวร์ที่มีการค้นหาผิดพลาดอีกบ้าง จากผลที่ได้จากการทดสอบสามารถทำการแบ่งกลุ่มจุดอ่อนของซอฟต์แวร์ที่ค้นพบได้ในเครื่องคอมพิวเตอร์เป้าหมายซึ่งจะทำให้ทราบว่ากลุ่มจุดอ่อนของซอฟต์แวร์ประเภทใดที่มีอัตราส่วนมากกว่าประเภทอื่นๆในกลุ่มเดียวกันซึ่งสามารถสรุปได้ดังต่อไปนี้ จุดที่ใช้ในการโจมตีที่ต้องระวังมากที่สุดคือการรีโมทจากทางไกลเข้ามาที่เครื่องคอมพิวเตอร์ การโจมตีส่วนใหญ่จะเป็นการกรอกข้อมูลเข้ามาในระบบ สิ่งที่ส่งผลกระทบที่มากที่สุดคือระบบไม่ได้รับความน่าเชื่อถือ การแจ้งประกาศส่วนใหญ่จะสามารถหาได้จากที่อื่น จุดอ่อนของซอฟต์แวร์ที่ค้นพบส่วนมากได้รับการยืนยันแล้วจากฐานข้อมูลจุดอ่อนระบบเปิด

6.1.4. เนื่องจากซอฟต์แวร์ในปัจจุบันมีการพัฒนาเพิ่มมากขึ้นเรื่อยๆ ดังนั้นการควบคุมจุดอ่อนของซอฟต์แวร์จึงควรมีเครื่องมือสำหรับการค้นหาจุดอ่อนของซอฟต์แวร์ที่มีความสามารถที่หลากหลายดังนั้นการนำเอาเครื่องมือหรือวิธีการหลายๆอย่างเข้ามารวมกันจะทำให้การควบคุมจุดอ่อนของซอฟต์แวร์มีประสิทธิภาพมากยิ่งขึ้น

6.2 ปัญหาและข้อจำกัดของงานวิจัย

6.2.1 ระบบสามารถทำงานได้ในระบบปฏิบัติการวินโดวส์ (Windows) ซึ่งติดตั้งดอทเน็ตเฟรมเวิร์ค (Dotnet framework) ซึ่งเป็นการจำกัดในเรื่องของระบบปฏิบัติการ

6.2.2 การส่งข้อมูลข้ามไปมาบนเครือข่ายจะใช้การส่งผ่านทางโปรโตคอลเอชทีทีพี ดังนั้นทุกเครื่องจะต้องมีการติดตั้งอินเตอร์เน็ตอินฟอร์เมชันเซอร์วิส (IIS: Internet Information Service) ซึ่งอาจจะเป็นการไม่สะดวกสำหรับผู้ที่มีเว็บเซิร์ฟเวอร์ตัวอื่นอยู่แล้วเช่น อาปาเช่ (Apache)

6.2.3 ซอฟต์แวร์สแกนรายการซอฟต์แวร์โอซีเอสอินเวนทอรี่เป็นส่วนสำคัญของระบบสำหรับการทำรายการซอฟต์แวร์ถ้าผู้ใช้ลืมติดตั้งหรือตัวสแกนไม่สามารถทำงานได้จะทำให้ระบบก็ไม่สามารถทำงานได้

6.2.4 กำหนดผู้ใช้ เอเอสพีเน็ต (ASPNET) ไว้ที่กลุ่ม ผู้ดูแล (Administrator) ในเครื่องเป้าหมายซึ่งเกี่ยวกับเรื่องความปลอดภัยเพราะกลุ่มของผู้ดูแลเท่านั้นที่สามารถสแกนรายการซอฟต์แวร์ได้

6.2.5 ชื่อซอฟต์แวร์ที่จะนำมาทำการค้นหาในฐานข้อมูลจุดอ่อนระบบเปิดบางครั้งอาจจะไปตรงกับชื่อซอฟต์แวร์รายการอื่นๆอีกหลายรายการในฐานข้อมูลจุดอ่อนได้ เป็นปัญหาซึ่งทำให้เกิดการค้นหาผิดพลาด

6.2.6 ในการปรับปรุงข้อมูลของฐานข้อมูลจุดอ่อนระบบเปิดจะใช้เวลาอย่างน้อยประมาณ 2 ชั่วโมงครึ่ง เพราะต้องมีการรันสคริปต์ของทางฐานข้อมูลจุดอ่อนระบบเปิดให้ทำการปรับปรุงฐานข้อมูลโดยลบข้อมูลเก่าทั้งหมดออกก่อนแล้วนำข้อมูลใหม่เข้าสู่ฐานข้อมูล

6.3 ข้อเสนอแนะ

สำหรับแนวทางการวิจัยต่อในอนาคตนั้นแบ่งเป็น 3 แนวทางดังนี้

6.3.1 การเพิ่มความถูกต้องและความแม่นยำของระบบในการหาความสอดคล้องกันของข้อมูลโดยการนำลำดับขั้นตอนการหาความสอดคล้องที่มีประสิทธิภาพมากขึ้นหรือหาซอฟต์แวร์ที่ประมวลรายการซอฟต์แวร์แล้วได้ข้อมูลที่มีชื่อซอฟต์แวร์และเวอร์ชันใกล้เคียงกับข้อมูลในฐานข้อมูลจุดอ่อนระบบเปิด

6.3.2 ขยายการทำงานให้สามารถทำงานได้หลายๆ ระบบปฏิบัติการ ถ้า สามารถเปลี่ยนเป็นหลายๆระบบปฏิบัติการได้จะทำให้เครื่องมือที่พัฒนาสามารถนำไปใช้ได้ในวงกว้างมากขึ้น

6.3.3 การปรับปรุงประสิทธิภาพการทำงานให้รวดเร็วขึ้นในเรื่องของการปรับปรุงข้อมูลของฐานข้อมูลจุดอ่อนโดยสร้างสคริปต์ซึ่งสามารถอ่านและประมวลผลข้อมูลไฟล์เอ็กซ์เอ็มแอลได้รวดเร็วขึ้น โดยอาจใช้ภาษาซีในการพัฒนาสคริปต์แทนของภาษาเก่าที่เป็นภาษาเพิร์ล

รายการอ้างอิง

1. Software Vulnerability Control. [Online]. Available from: http://www.comptechdoc.org/independent/security/recommendations/secsoftwarev.html [2004, Dec 01]
2. Open Source Vulnerability Database. [Online]. Available from: http://www.osvdb.org [2004, Dec 01]
3. Open Computer and Software Inventory. [Online]. Available from: http://ocsinventory.sourceforge.net [2004, Dec 01]
4. G.Karlk. Web Services architecture overview. [Online]. Available from: http://www-106.ibm.com/developerworks/webservices/library/w-ovr/?dwzone=webservices [2000,Sep 01]
5. Warren A. S. Ward, Jacob L. Kouns. OSVDB White Paper Project Aims. [Online]. Available from: http://www.osvdb.org/OSVDB-Aims.pdf [2004, Mar 31]
6. Common Vulnerability and Exposure. [Online]. Available from: http://www.cve.mitre.org [2004, Dec 01]
7. CVE-Compatible Products and Services. [Online]. Available from: http://www.us-cert.gov/cve/compatible.html#current_compatible [2004, Dec 01]
8. Citadel Security Software. [Online]. Available from: https://hercules.citadel.com/docs/300VulGuide.pdf [2004, May]
9. Open Vulnerability Assessment Language. [Online]. Available from: http://oval.mitre.org [2004, Dec 01]
10. Microsoft Baseline Security Analyzer. [Online]. Available from: http://www.microsoft.com/technet/security/tools/mbsahome.mspx [2004, Dec 01]
11. eEye Digital Security . [Online]. Available from: http://www.eeye.com/html/ [2004, Dec 01]
12. Y. Bai, H. Kobayashi. New String Matching Technology for Network Security. Proceedings of the17th International Conference on Advanced Information Networking and Applications (AINA'03). 2003.
13. SNORT. [Online]. Available from: http://www.snort.org [2004, Dec 01]
14. Perfect XML. [Online]. Available from: http://www.perfectxml.com/XML.asp [2004, Dec 01]
15. P.Chris. 15 Seconds: Creating a .NET Web Service. [Online]. Available from: http://www.15seconds.com/issue/010430.htm [2001, Apr 30]

16. S. M. L. Ma, G. Song, P.Meunier. Sharing Vulnerability Information using a Taxonomically-correct, Web-based Cooperative Database. CERIAS Tech Report 2001-03. 2001.

17. R. A. Martin. Integrating your information security vulnerability management capabilities through industry standards (CVE&OVAL). IEEE. 2003.

18. H. L. a. E. Snekkenes. A Classification of Malicious Software Attacks. Proceedings of 23rd IEEE International Performance, Computing, and Communications Conference(2004): 827-832.

19. H.T. Tian, L.S. Huang, J.L. Shan,G.L. Chen. Automated Vulnerability Management through Web Services. Springer-Verlag Berlin Heidelberg (2003):1067 – 1070.

20. L. H. Haitao Tian, Zhi Zhou, and Hui Zhang. Common Vulnerability Markup Language. Springer-Verlag Berlin Heidelberg (2003): 228-240.

21. H.T. Tian, L.S. Huang, Z.Zhou, Y.L.Luo. Arm up Administrators: Automated Vulnerability Management. Proceedings of the 7th International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN'04). 2004.

22. ASP.NET Quick Start Tutorial. Security and XML Web Service. [Online]. Available from: http://www.asp.net/Tutorials/quickstart.aspx [2004, Dec 01]

23. A. VanLengen, D. Haney. Creating Web Services Using ASP.net. CCSC: Rocky Mountain Conference, JCSC 20,1 (October). 2004.

ภาคผนวก

ภาคผนวก ก
ซอฟต์แวร์โอซีเอสอินเวนทอรี่ (OCSinventory Software)

ก.1 คำอธิบาย

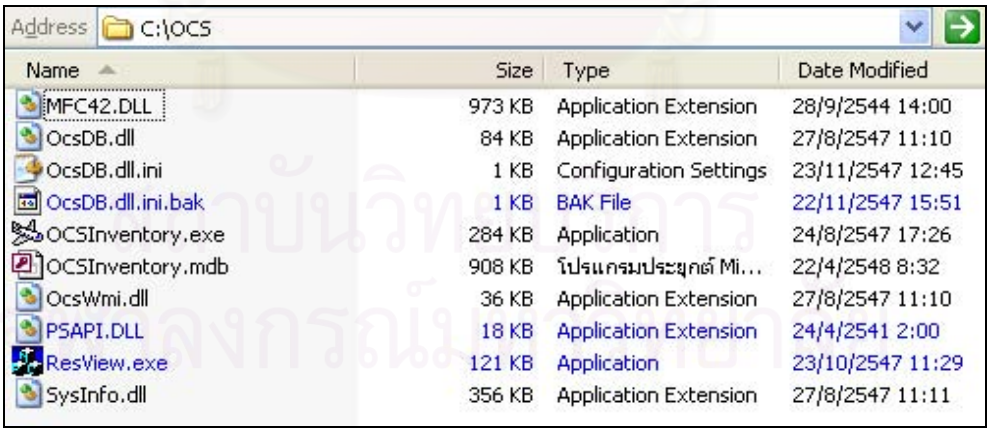
เป็นซอฟต์แวร์ที่ใช้สำหรับทำรายการซอฟต์แวร์ ซึ่งตัวโปรแกรมจะเก็บรายการซอฟต์แวร์ไว้ที่ฐานข้อมูล ไมโครซอฟท์แอคเสส (Microsoft Access) ในการเรียกใช้ให้ทำการ ตั้งค่าที่ไฟล์ OcsDB.dll.ini ซึ่งจะกำหนดพาท (path) ฐานข้อมูลในการเก็บข้อมูล

ตัวอย่าง

[OCS Inventory Database]

Database=Provider=Microsoft.Jet.OLEDB.4.0;Data Source=C:\OCS\OCSInventory.mdb;Persist Security Info=False

ในการสั่งให้โปรแกรมทำงานให้เรียกที่ไฟล์ OCSInventory.exe โปรแกรมจะทำการทำรายการซอฟต์แวร์และข้อมูลอื่นๆ เก็บข้อมูลไว้ที่ฐานข้อมูลที่ได้ตั้งค่าไว้ ไฟล์ของโอซีเอสอินเวนทอรี่ที่จะนำมาใช้เป็นตัวกระทำรายการซอฟต์แวร์จะวางไว้ที่ไดร์ฟซี แสดงได้รูปที่ ก1



รูปที่ ก1

นำมาใช้กับงานวิจัยในส่วนของการสแกนรายการซอฟต์แวร์ของเครื่องคอมพิวเตอร์เป้าหมายแล้วเก็บข้อมูลไว้ที่ฐานข้อมูลเพื่อให้เว็บเซอร์วิสอินเทอร์เฟสสามารถเรียกข้อมูลจากฐานข้อมูลได้

ภาคผนวก ข

คอมโพเนนต์ แอคทีฟซอกเก็ต เน็ตเวิร์ค (ActiveSocket Network)

ข.1 คำอธิบาย

การใช้งานจะเป็นการนำเอาคอมโพเนนต์มาทำการวางไว้ที่ไดเรกทอรี่บิน (Bin/) แล้วเรียกใช้ฟังก์ชันของคอมโพเนนต์ ตัวอย่างโค้ดโปรแกรมคือการเรียกไฟล์เอเอสพีดอทเน็ตซึ่งเป็นไฟล์ประจำเครื่องเป้าหมายแต่ละเครื่อง

```
Dim objHttp As ASOCKETLib.HttpClass
Dim strHost As String
Dim strData As String
objHttp = New ASOCKETLib.Http
strHost = "http://localhost/wsapp/vutarget_" & sname & ".aspx"
objHttp.Connect(strHost)
```

นำมาใช้ในงานวิจัยในส่วนของการตั้งเวลาเมื่อระบบทำการตั้งเวลาจะเป็นหน้าที่ของโปรแกรมค้นหาจากการตั้งเวลาทำงานโดยเป็นวินโดวส์แอปพลิเคชัน ซึ่งจะช่วยให้โปรแกรมสามารถเรียกใช้โปรโตคอลเอชทีทีพี (HTTP) ได้โดยที่ไม่ต้องเรียกใช้ ผ่านทางเว็บบราวเซอร์

ศึกษารายละเอียดเพิ่มเติม ได้ที่ http://www.activexperts.com/activsocket/

ภาคผนวก ค
การใช้งานเว็บเซอร์วิส

ค.1 คำอธิบาย

ในการใช้งานเว็บเซอร์วิสจะต้องมีการสร้างคลาสตัวแทน (Proxy Class) เพื่อเรียกใช้เว็บเซอร์วิสไว้ที่ผู้รับบริการ สำหรับวิชวลสตูดิโอด็อตเน็ต มีเครื่องมือที่เรียกว่า ดับเบิลยูเอสดีแอล (wsdl.exe) สำหรับสร้างคลาสตัวแทนดังกล่าว ซึ่งมีรูปแบบการใช้งาน

wsdl [*options*] *{URL* | path}

ตัวอย่างเช่น

wsdl /l:VB /out:class.vb http://localhost/wsosvdb/svosv.asmx?WSDL /n:nsclass

เป็นการสร้างคลาสตัวแทนจาก http://localhost/wsosvdb/svosv.asmx?WSDL

โดยกำหนดว่าจะสร้างคลาสตัวแทน class.vb กำหนดให้มี namespace ชื่อว่า nsclass

นำมาใช้ในงานวิจัยคือเมื่อเพิ่มเครื่องเป้าหมายเข้าสู่ระบบจะใช้การรันคำสั่งดังตัวอย่างข้างบน เพื่อทำการสร้างคลาสตัวแทนสำหรับเครื่องเป้าหมายซึ่งทุกเครื่องจะมีคลาสตัวแทนประจำเครื่องของตนเองซึ่งแตกต่างกัน

ประวัติผู้เขียนวิทยานิพนธ์

นายปฏิญญา จันฤาชัย เกิดเมื่อวันที่ 1 กรกฎาคม พ.ศ 2522 ที่จังหวัดอุดรธานี สำเร็จการศึกษาระดับปริญญาตรี วิทยาศาสตรบัณฑิต จากภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสถาบันราชภัฏอุดรธานี ในปีการศึกษา 2543 และ เข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิตภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เมื่อ พ.ศ. 2546