การประเมินจุดอ่อนด้านซอฟต์แวร์ของระบบเว็บเซอร์วิสโดยจำแนกความรุนแรงของความเสียหาย

นายกิตติศักดิ์ นิทาน

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2550

EVALUATION OF WEB SERVICES SOFTWARE VULNERABILITY BASED ON SEVERITY OF DAMAGE

Mr.Kittisak Nithan

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Computer Science
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2007

หัวข้อวิทยานิพนธ์	การประเมินจุดอ่อนด้านซอฟต์แวร์ของระบบเว็บเซอร์วิสโดยจำแนกความรุนแรงของความเสียหาย
โดย	นายกิตติศักดิ์ นิทาน
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษา	อาจารย์ ดร. ยรรยง เต็งอำนวย

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร.บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(อาจารย์ จารุมาตร ปิ่นทอง)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(อาจารย์ ดร.ยรรยง เต็งอำนวย)

..... กรรมการภายนอกมหาวิทยาลัย
(ดร.โกเมน พิบูลย์โรจน์)

..... กรรมการ
(อาจารย์ ดร.เกริก ภิรมย์โสภา)

กิตติศักดิ์ นิทาน : การประเมินจุดอ่อนด้านซอฟต์แวร์ของระบบเว็บเซอร์วิสโดยจำแนกความรุนแรงของความเสียหาย. (EVALUATION OF WEB SERVICES SOFTWARE VULNERABILITY BASED ON SEVERITY OF DAMAGE) อ.ที่ปรึกษา: อ.ดร.ยรรยง เต็งอำนวย , 121 หน้า.

งานวิจัยนี้ได้นำเสนอวิธีการประเมินจุดอ่อนด้านซอฟต์แวร์ของผลิตภัณฑ์เว็บเซอร์วิส โดยใช้รายการจุดอ่อนซีวีอี และได้นำเสนอวิธีการจำแนกความรุนแรงของผลกระทบที่ได้รับของความเสียหายที่เกิดขึ้น โดยแบ่งออกเป็น 3 ประเภทคือ การรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน โดยแยกจุดอ่อนของผลิตภัณฑ์เว็บเซอร์วิสเป็น 2 กลุ่มใหญ่ คือ จุดอ่อนของเครื่องมือที่ใช้ในการพัฒนาเว็บเซอร์วิส และจุดอ่อนของเครื่องมือที่ใช้ในการสนับสนุนการให้บริการ ในการประเมินได้มีการนำค่าของผลกระทบมาคำนวณหาค่าและเปรียบเทียบคะแนนความเสียหายของจุดอ่อนของแต่ละผลิตภัณฑ์

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต กิตติศักดิ์ นิทาน

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่ออาจารย์ที่ปรึกษา

ปีการศึกษา 2550

4971405121 : MAJOR COMPUTER SCIENCE

KEY WORD: SOFTWARE VULNERABILITY / WEB SERVICES / SEVERITY-BASED DAMAGE / CVE

KITTISAK NITHAN : EVALUATION OF WEB SERVICES SOFTWARE VULNERABILITY BASED ON SEVERITY OF DAMAGE. THESIS ADVISOR: YUNYONG TENG-AMNUAY, Ph.D., 121 pp.

This research assesses software vulnerability of web services products based on Common Vulnerability and Exposure (CVE) and classifies the damage of each vulnerability into confidentiality, integrity, and availability. The impact of each vulnerability type of web services products have been classified to development tools and runtime service tools. We use scores of impacts to compute severity of damage on web services products and compare each type of damage.

Department Computer Engineering Student's signature Kittisak Nithan

Field of study Computer Science Advisor's signature

Academic year 2007

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยดี เนื่องมาจากความช่วยเหลืออย่างดียิ่งของท่าน อ.ดร.ยรรงยง เต็งอำนวย อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่ได้สละเวลาให้คำปรึกษาแนะนำแนวทางเกี่ยวกับงานวิจัยอย่างดีตลอดมาจนเสร็จสมบูรณ์ และผู้วิจัยขอกราบขอบพระคุณคณะกรรมการสอบวิทยานิพนธ์ทุกท่านที่ได้ให้คำแนะนำ ข้อคิดเห็น ข้อเสนอแนะ และแนวทางในการพัฒนางานวิจัยนี้

ขอขอบคุณพี่ๆ เพื่อนๆ และน้องๆ ทุกคนที่ให้คำแนะนำและช่วยเหลือในส่วนข้อมูลของเว็บเซอร์วิส และการเก็บข้อมูลให้สำเร็จลุล่วงเป็นอย่างดี

สุดท้ายนี้ ขอกราบขอบพระคุณคุณพ่อและคุณแม่ที่สนับสนุนในด้านการศึกษาและเป็นกำลังใจที่ดีเสมอมา

สารบัญ

สารบัญตาราง

หน้า

สารบัญภาพ

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันเว็บเซอร์วิส (Web Services) มีการใช้งานอย่างแพร่หลาย เพราะสะดวกที่สามารถใช้ภาษาใดก็ได้ในการพัฒนาระบบ และใช้ระบบปฏิบัติการใดๆ ก็ได้ในการติดต่อสื่อสารและเชื่อมโยงข้อมูลกัน ความหลากหลายของรูปแบบต่างๆในการร่วมกันทำงานของเว็บเซอร์วิสเองทำให้เกิดจุดอ่อน (Vulnerability) ต่างๆ ตามมา ซึ่งจุดอ่อนส่วนใหญ่เกิดขึ้นทั้งในส่วนของเครื่องมือช่วยการพัฒนา (Development Tools) โดยมีจุดอ่อนในการสร้างเว็บเซอร์วิสขึ้นมาแล้วทำงานอย่างไม่มีเสถียรภาพ และในส่วนเครื่องมือสนับสนุนการให้บริการ (Runtime Service Tools) โดยมีจุดอ่อนในการให้บริการเว็บเซอร์วิสที่ผิดพลาด เช่น ไม่สามารถให้บริการได้ตลอดเวลาทำการหรือยอมให้บุคคลอื่นล่วงละเมิดเข้ามาแก้ไขข้อมูลที่ไม่ได้รับอนุญาต เป็นต้น ดังนั้นการพิจารณาเลือกผลิตภัณฑ์ของเว็บเซอร์วิสเพื่อนำมาใช้ในองค์กร ควรจะพิจารณาให้เหมาะสมกับการใช้งานและมีความปลอดภัยสูงจากการถูกโจมตีจากผู้ไม่หวังดี

งานวิจัยนี้จึงมีแนวความคิดที่จะประเมิน และเปรียบเทียบให้เห็นถึงความรุนแรงของความเสียหายต่อการโจมตีของระบบเว็บเซอร์วิสแบบต่างๆ แยกตามรายชื่อของผลิตภัณฑ์ที่ใช้ในการพัฒนาระบบเว็บเซอร์วิส โดยพิจารณาจากข้อมูลจุดอ่อนที่ได้มีการรวบรวมไว้ในรายการจุดอ่อนของซีวีอี [1] ซึ่งจะนำมาแบ่งประเภทตามกลุ่มของจุดอ่อนและผลิตภัณฑ์ที่เกี่ยวเนื่องกับเว็บเซอร์วิส มีการกำหนดระดับผลกระทบที่เกิดขึ้นตามแนวคิดวิธีการให้คะแนนค่าถ่วงน้ำหนัก [2] โดยจำแนกตามความเสียหายที่เกิดขึ้น ซึ่งจะเป็นประโยชน์ต่อการพิจารณาเลือกใช้เว็บเซอร์วิสได้อย่างเหมาะสม รวมถึงเป็นข้อมูลพื้นฐานเพื่อนำไปใช้ในการหาแนวทางการป้องกันสำหรับระบบเว็บเซอร์วิสที่มีใช้อยู่แล้วในองค์กร เพื่อเป็นการช่วยลดความเสี่ยงต่อการถูกโจมตีและป้องกันความเสียหายที่อาจเกิดขึ้นได้กับระบบ

1.2 วัตถุประสงค์ของการวิจัย

งานวิจัยนี้มีจุดประสงค์เพื่อวิเคราะห์ เปรียบเทียบ ประเมินผลกระทบของความเสียหายและความรุนแรงของจุดอ่อนด้านซอฟต์แวร์บนระบบเว็บเซอร์วิส โดยอาศัยการคัดกรองรายการจุดอ่อนที่เกี่ยวข้องกับเว็บเซอร์วิสจากซีวีอี

1.3 ขอบเขตของการวิจัย

1. รายการจุดอ่อนและคำสำคัญที่พบจากระบบ อ้างอิงจากชื่อจุดอ่อนจากรายการของซีวีอี (CVE) เวอร์ชั่น 20061101 โดยเลือกเฉพาะรายการจุดอ่อนด้านซอฟต์แวร์ที่เกิดขึ้นบนระบบเว็บเซอร์วิส
2. รูปแบบการประเมินระดับความรุนแรงและความเสียหายต่อระบบที่ใช้ในงานวิจัยอ้างอิงจากทฤษฎีการประเมินจุดอ่อนของเกียรติ [4]
3. เว็บเซอร์วิสผลิตภัณฑ์ที่ใช้ในงานวิจัยแบ่งเป็นส่วนเครื่องมือช่วยพัฒนาและส่วนเครื่องมือสนับสนุนการให้บริการ โดยคัดเลือกผลิตภัณฑ์ที่ได้รับความนิยม 10 อันดับแรกจากเว็บไซต์ [6,7]

1.4 ขั้นตอนการวิจัย

1. คัดเลือกข้อมูลจุดอ่อนด้านซอฟต์แวร์ที่เกิดขึ้นบนระบบเว็บเซอร์วิสจากรายการซีวีอี (CVE- Common Vulnerabilities and Exposures)
2. คัดเลือกและจัดกลุ่มจุดอ่อนด้านซอฟต์แวร์ของระบบเว็บเซอร์วิส โดยเลือกจากผลิตภัณฑ์ หรือส่วนประกอบที่เกี่ยวข้องกับระบบเว็บเซอร์วิสดังที่กล่าวมาแล้ว
3. สร้าง ปรับปรุงรูปแบบการประเมินจุดอ่อน ระดับความรุนแรงตามความเหมาะสม
4. คำนวณค่าระดับความเสียหายของรายการจุดอ่อนแต่ละรายการ
5. ประเมินผลการวิเคราะห์ระดับความรุนแรงและเสียหาย โดยแสดงผลออกมาในรูปเชิงปริมาณและกราฟแสดงผล
6. สรุปผลการวิจัย และจัดทำรายงานวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. สามารถนำรายการจุดอ่อนมาเป็นข้อมูลเบื้องต้นของการติดตั้งระบบเว็บเซอร์วิสของผู้ดูแลระบบเพื่อป้องกันการโจมตีจุดอ่อนจากแฮกเกอร์
2. สามารถนำข้อมูลจากงานวิจัยไปใช้เป็นข้อมูลช่วยสนับสนุนในการตัดสินใจเลือกใช้เครื่องมือที่ใช้ในการพัฒนาระบบเว็บเซอร์วิสที่เหมาะสมกับแต่ละองค์กร โดยสามารถเปรียบเทียบความปลอดภัยจากการโจมตีจุดอ่อนของเครื่องมือที่ใช้พัฒนาระบบเว็บเซอร์วิสต่างๆได้

1.6 โครงสร้างวิทยานิพนธ์

ในบทที่ 2 จะกล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้อง บทที่ 3 จะกล่าวถึงขั้นตอนการดำเนินการวิจัย บทที่ 4 จะกล่าวถึงผลการวิจัย ซึ่งเป็นผลที่ได้จากการเปรียบเทียบและการประเมินจุดอ่อนที่เกิดขึ้นของแต่ละผลิตภัณฑ์เว็บเซอร์วิส และทำการสรุปผลที่ได้รวมถึงข้อเสนอแนะต่างๆไว้ในบทที่ 5

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ทฤษฎีและงานวิจัยที่เกี่ยวข้องที่จำเป็นต้องศึกษาเพื่อใช้เป็นความรู้พื้นฐานในการทำงานวิจัยนี้ แบ่งออกได้เป็น 4 ส่วนด้วยกัน คือ ซีวีอี การจัดกลุ่มของจุดอ่อน การประเมินผลจุดอ่อน และงานวิจัยที่เกี่ยวข้อง ดังรายละเอียดต่อไปนี้

2.1 Common Vulnerabilities and Exposures

ซีวีอี (Common Vulnerability and Exposure (CVE)) [1] เป็นมาตรฐานการกำหนดชื่อที่เป็นของรายการจุดอ่อนที่เกิดขึ้นในระบบคอมพิวเตอร์ ซึ่งแต่เดิมจุดอ่อนที่เกิดขึ้นในระบบคอมพิวเตอร์มักจะถูกกำหนดชื่อเรียกแตกต่างกันออกไป ตามองค์กรหรือหน่วยงานที่แตกต่างกัน เช่น การอ้างอิงจุดอ่อนที่เกิดขึ้นกับโปรแกรมซีจีไอของระบบรายนามพีเอชเอฟ ในปี 1998 ดังรายละเอียดในตารางที่ 2.1

ตารางที่ 2.1 แสดงการอ้างอิงจุดอ่อนกับโปรแกรมซีจีไอของสมุดโทรศัพท์พีเอชเอฟ

หน่วยงาน	ชื่อจุดอ่อน
AXENT (now Symantec)	Phf CGI allows remote command execution
BindView	#107—cgi-phf
Bugtraq	PHF Attacks—fun and games for the whole family
CERIAS	http_escshellcmd
CERT	CA-96.06.cgi_example_code
Cisco Systems	HTTP—cgi-phf
CyberSafe	Network: HTTP ‘phf’ attack
DARPA	0x00000025 = HTTP PHF attack
IBM ERS	ERS-SVA-E01-1996:002.1
ISS	http—cgi-phf
Symantec	#180 HTTP server CGI example code compromises http server
Security Focus	#629—phf Remote Command Execution Vulnerability

การอ้างอิงถึงรายการจุดอ่อนระหว่างหน่วยงานต่างๆ แต่เดิมทำได้ยากเนื่องจากแต่ละหน่วยงานมีการอ้างอิงรายการจุดอ่อนโดยใช้ชื่อที่แต่ละหน่วยงานนั้นๆ เป็นผู้กำหนดขึ้น ทำให้การติดต่อสื่อสารกับหน่วยงานอื่นเมื่อต้องการอ้างถึงจุดอ่อนรายการเดียวกันเป็นเรื่องที่ยุ่งยากซับซ้อนโดยเฉพาะอย่างยิ่งเมื่อต้องการติดต่อกับหน่วยงานอื่นมากกว่า 2 หน่วยงานขึ้นไป การนำซีวีอีมาใช้ทำให้มีการอ้างรายการจุดอ่อนผ่านชื่อที่มีความเป็นมาตรฐาน ทำให้การอ้างอิงถึงรายการจุดอ่อนเดียวกันของแต่ละหน่วยงานทำได้ง่ายมากยิ่งขึ้นอย่างเช่นตัวอย่างที่กล่าวมาแล้วซีวีอีกำหนดชื่อไปเป็น

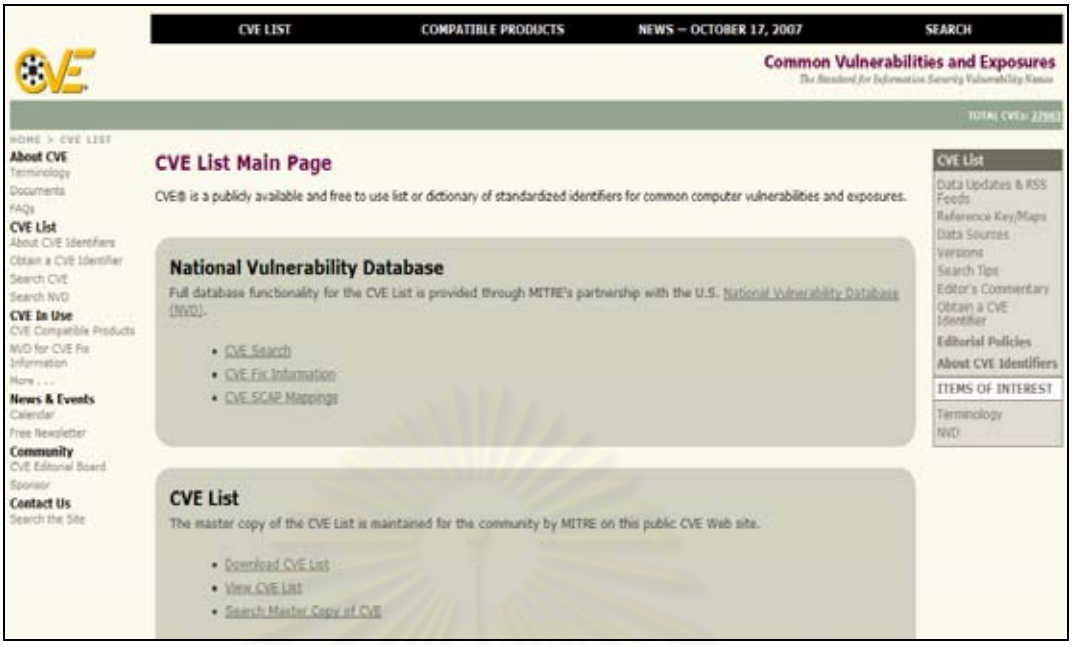
ข้อมูลจุดอ่อนที่ปรากฏอยู่ในรายการซีวีอี มีองค์ประกอบอยู่ 3 ส่วนด้วยกัน ได้แก่

1. ชื่อรายการจุดอ่อน เป็นการตั้งชื่อเพื่อให้เป็นมาตรฐานในการอ้างอิงถึงข้อมูลจุดอ่อน โดยมีรูปแบบคือ CVE- YYYY-NNNN โดยที่ YYYY เป็นปีที่ออกหมายเลข และ NNNN คือ ลำดับที่ของรายการซีวีอีที่ออกในปีนั้น เช่น CVE-2000-1001
2. คำอธิบาย เป็นคำอธิบายสั้นๆ ว่าเป็นจุดอ่อนที่เกี่ยวข้องกับเรื่องใด
3. แหล่งข้อมูลอ้างอิง บอกถึงแหล่งข้อมูลอื่นๆ ที่สามารถนำไปใช้ในการค้นหาข้อมูลรายละเอียดของจุดอ่อนนั้นๆ เพิ่มเติมได้

ตารางที่ 2.2 แสดงตัวอย่างข้อมูลจุดอ่อนที่ปรากฏในรายการซีวีอี

ชื่อรายการซีวีอี	คำอธิบาย	แหล่งข้อมูลอ้างอิง
CVE-2000-1001	Add_2_basket asp in.Element InstantShop allows remote attackers to modifly price information via the “price” hidden form variable.	BUGTRAQ:20001024 Price modification in Element InstantShop.XF:instantshop-modifly-price,OSVDB:6787

ตารางที่ 2.2 แสดงตัวอย่างของข้อมูลจุดอ่อนในรายการซีวีอี พร้อมทั้งรูปแบบการตั้งชื่อ คำอธิบายและแหล่งข้อมูลอ้างอิงต่างๆ ส่วนรูปที่ 2.1 แสดงข้อมูลของแหล่งอ้างรายการซีวีอีที่สามารถค้นหาได้ผ่านอินเทอร์เน็ตโดยสามารถเข้าถึงได้ที่ http://cve.mitre.org/cve/index.html



รูปที่ 2.1 หน้าเว็บเพจของแหล่งอ้างอิงรายการซีวีอี

2.2 การจัดกลุ่มของจุดอ่อน

การจัดกลุ่มของจุดอ่อนหรือข้อบกพร่องที่เกิดขึ้น เพื่อใช้ในการเปรียบเทียบผลกระทบที่เกิดขึ้นบนเว็บเซอร์วิสผลิตภัณฑ์ว่ามีจุดอ่อน ณ ตำแหน่งใดเกิดขึ้นมากที่สุด และจุดอ่อนนั้นสามารถสร้างความเสียหายให้กับระบบเว็บเซอร์วิสได้มากน้อยเพียงใด ซึ่งมีงานวิจัยที่เกี่ยวข้อง ดังนี้

แลนเวอร์ และคณะ [3] ได้จัดกลุ่มของข้อบกพร่องออกเป็น 3 กลุ่ม ตามลักษณะการเกิด เวลาที่เกิด และสถานที่เกิด

รัศมีทิพย์ [2] ปรับการจัดกลุ่มของจุดอ่อนของแลนเวอร์ โดยตัดเวลาที่เกิดข้อบกพร่องออก และได้เสริมลักษณะความเสียหายและระดับความรุนแรงเข้าไป เพื่อนำไปวิเคราะห์กับรายการในซีวีอี ซึ่งงานวิจัยนี้ได้ทดลองทำการประเมินค่าระดับความเสียหายของจุดอ่อนสำหรับระบบลินุกซ์

เจียงซุก [4] นำเสนอรูปแบบการจัดกลุ่มของจุดอ่อน ให้เหมาะสมกับระบบเว็บเซอร์วิสเพื่อนำมาใช้ในการพัฒนาระบบ ไอดีเอส (IDS-Intrusion Detection System) ซึ่งใช้เป็นแนวทางในการค้นหาจุดบกพร่องของเว็บเซอร์วิสในรายการของซีวีอี เพื่อนำมาวิเคราะห์และเปรียบเทียบต่อไป

2.3 การประเมินคะแนนจุดอ่อน

การประเมินคะแนนของจุดอ่อนเพื่อดูผลกระทบต่อระบบ ใช้คะแนนที่ได้มาของแต่ละจุดอ่อนในการบ่งบอกถึงระดับความเสียหายที่เกิดขึ้น ในงานวิจัยนี้จำเป็นที่ต้องหาวิธีที่ใช้ในการประเมินเพื่อให้เกิดประสิทธิภาพสูงสุดในการประเมินผล ซึ่งจะมีงานวิจัยที่เกี่ยวข้องมีดังนี้

เกียรติ [4] เป็นการวัดระดับผลกระทบของจุดบกพร่องที่สามารถคำนวณได้โดยการใช้ผลรวมคะแนนของระดับความเสียหายแต่ละประเภทที่เกิดขึ้น ได้แก่ การรักษาความลับ (Confidentiality) บูรณภาพ (Integrity) และสภาพพร้อมใช้งาน (Availability)

งานวิจัยที่ได้กล่าวมา เป็นแนวทางในการคิดคำนวณความรุนแรงของความเสียหายแต่และประเภท รวมถึงแนวทางในการวิเคราะห์และประเมินผลจุดอ่อนที่เกิดขึ้น

2.4 การค้นหาจุดอ่อนของระบบ

การค้นหาจุดอ่อนของระบบเว็บเซอร์วิสเป็นกระบวนการที่สำคัญที่จะได้มาของข้อมูลจุดอ่อนที่จะนำไปใช้ในงานวิจัย จากการศึกษาพบว่ามีงานวิจัยที่เกี่ยวข้องดังนี้

เดมเชนโก้ และคณะ [8] เสนอภาพรวมและรูปแบบการป้องกันจุดอ่อนของเว็บเซอร์วิสและกริด งานวิจัยนี้อธิบายหลักการเบื้องต้นของการป้องกันการโจมตีเข้ามาทางการให้บริการต่างๆ ของเว็บเซอร์วิสเองและการป้องกันการโจมตีแบบหลายชั้นตามต้นแบบของโครงสร้างเอสโอเอ (SOA-Service Oriented Architecture) สุดท้ายงานวิจัยนี้แสดงการวิเคราะห์และนำเสนอรูปแบบพื้นฐานของการพัฒนาเพื่อให้รับรู้จุดอ่อนต่างๆ จนถึงหลักการออกแบบการรักษาความปลอดภัยจากการให้บริการซึ่งได้รับการรับรองแล้ว

โฮลเกอซัน และ โซเดอร์สตอม [9] มุ่งประเด็นไปที่จุดอ่อนของระบบเว็บเซอร์วิส การคุกคามและบุกรุกเข้ามาในการนำเว็บเซอร์วิสที่ใช้ในอยู่ทั่วไปบนระบบเครือข่ายที่ไม่มีความปลอดภัยเพียงพอ ซึ่งจะใช้มาตรฐานของ WS-Security โดยกำหนดคุณสมบัติเพิ่มเติมดังนี้ คือ WS-Policy, WS-Trust, WS-Privacy, WS Secure Conversation, WS-Dederation และ WS-Authorization

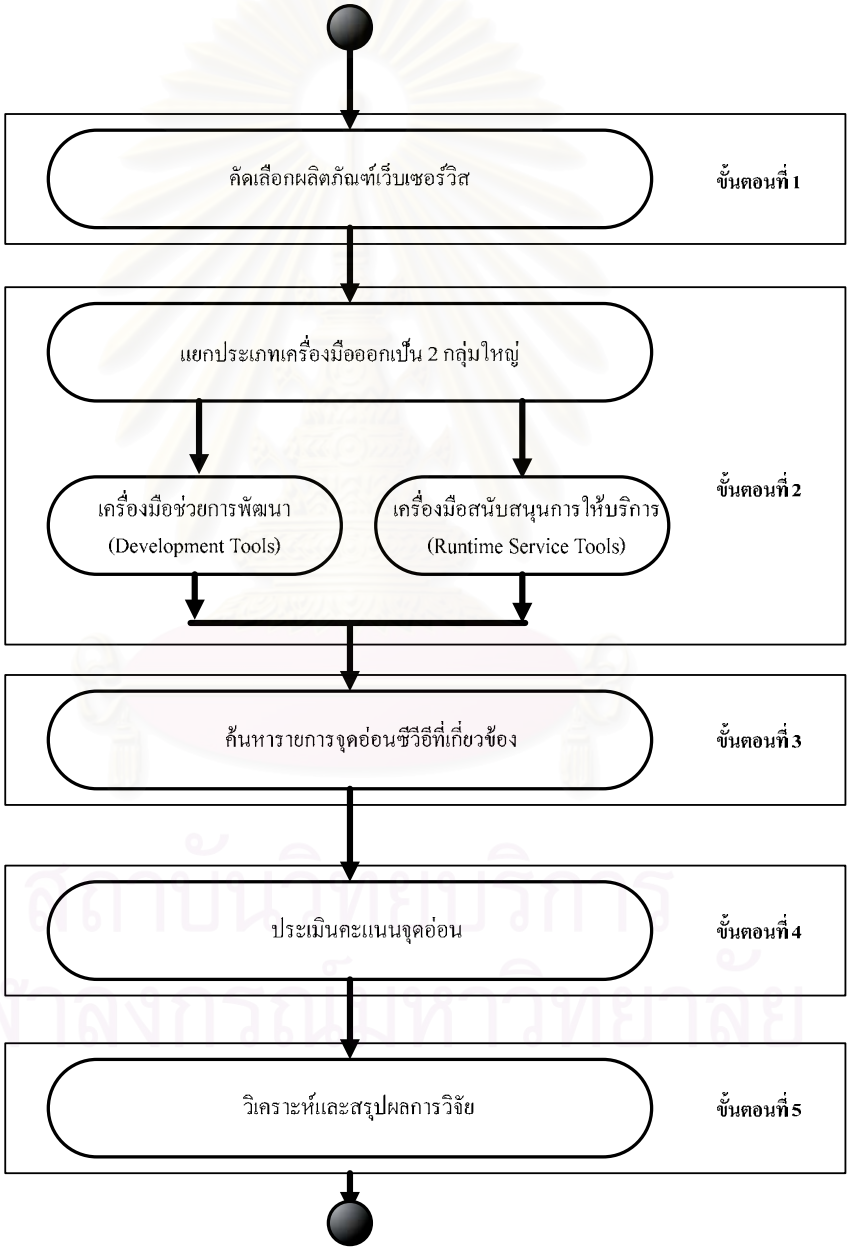
คารอส กูเตียเรสและคณะ [10] นำเสนอรูปแบบของการรักษาความปลอดภัยของเว็บเซอร์วิส โดยมีกระบวนการ PWSSec (Process for Web Service Security) 3 ขั้นตอน คือ ขั้นตอนที่ 1 WsSecReq (Web service Security Requirements) ขั้นตอนที่ 2 WsSecArch (Web Service Security Architecture) และ ขั้นตอนที่ 3 WsSecTech (Web Service Security

Technologies) แต่ในงานวิจัยนี้นำเสนอและอธิบายเฉพาะ WsSecArch เพื่อเป็นพื้นฐานในการออกแบบโครงสร้างการรักษาความปลอดภัยบนระบบเว็บเซอร์วิส ซึ่งทำให้สะดวกในการแบ่งส่วนของการร้องขอของระบบการรักษาความปลอดภัย

ทฤษฎีและงานวิจัยที่ได้กล่าวมาในบทที่ 2 นี้ เป็นแนวทางในการจัดกลุ่มของจุดอ่อนและข้อผิดพลาดที่เกิดขึ้นในเว็บเซอร์วิส แนวทางในการแจกแจงคะแนนความเสียหาย รวมถึงแนวทางในการวิเคราะห์และประเมินผลจุดอ่อนที่เกิดขึ้น ซึ่งก่อนทำการจัดกลุ่มของจุดอ่อนจะต้องผ่านขั้นตอนในการคัดเลือกผลิตภัณฑ์ของเว็บเซอร์วิส และคัดเลือกรายการจุดอ่อนซีวีอีที่มีลักษณะตรงกับวัตถุประสงค์ของงานวิจัยนี้ก่อน ได้แก่จุดอ่อนที่เกิดขึ้นบนผลิตภัณฑ์ของเว็บเซอร์วิสทั้งในส่วนของเครื่องมือช่วยพัฒนา และเครื่องมือสนับสนุนการให้บริการ ในบทที่ 3 จะได้กล่าวถึงรายละเอียดของวิธีการคัดเลือกผลิตภัณฑ์ การคัดเลือกรายการจุดอ่อนและการจัดเก็บข้อมูลที่ได้จากการคัดเลือกต่อไป

บทที่ 3
วิธีดำเนินการวิจัย

บทนี้จะนำเสนอที่มาของจุดอ่อนด้านซอฟต์แวร์บนระบบเว็บเซอร์วิส การคัดเลือกจุดอ่อนที่มีอยู่ในรายการซีวีอี ตลอดจนการจัดเก็บข้อมูลเพื่อนำมาวิเคราะห์ เปรียบเทียบ และประเมินผลกระทบของความเสียหายและความรุนแรงของจุดอ่อนด้านซอฟต์แวร์บนระบบเว็บเซอร์วิส โดยมีขั้นตอนการดำเนินการวิจัย สามารถเขียนออกมาในรูปแผนผังลำดับงานได้ดังนี้



รูปที่ 3.1 แผนภาพแสดงขั้นตอนการวิจัย

รูปที่ 3.1 แสดงขั้นตอนการวิจัยเพื่อใช้ในการประเมินคะแนนจุดอ่อนของผลิตภัณฑ์เว็บเซอร์วิส ซึ่งมีขั้นตอนทั้งหมด 5 ขั้นตอน คือ ขั้นตอนที่ 1 คัดเลือกผลิตภัณฑ์เว็บเซอร์วิส ขั้นตอนที่ 2 แยกเครื่องมือออกเป็น 2 กลุ่มใหญ่ ขั้นตอนที่ 3 ค้นหารายการจุดอ่อนในรายการซีวีอีที่เกี่ยวข้อง ขั้นตอนที่ 4 ประเมินคะแนนจุดอ่อน และขั้นตอนสุดท้าย สรุปผลวิจัย

3.1 การคัดเลือกข้อมูลจุดอ่อนจากรายการซีวีอี

จุดอ่อนด้านซอฟต์แวร์บนระบบเว็บเซอร์วิสถูกนำมาจากรายการซีวีอีซึ่งแยกออกเป็นสองประเภท คือ

- เครื่องมือช่วยการพัฒนา (Development Tool)

  ในส่วนของเครื่องมือทางซอฟต์แวร์ประเภทนี้ผู้วิจัยได้เล็งเห็นความสำคัญของระบบที่อาจมีจุดอ่อนในการพัฒนาเว็บเซอร์วิสขึ้นมา แล้วทำให้การทำงานของเว็บเซอร์วิสไม่สามารถทำงานได้อย่างมีเสถียรภาพและประสิทธิภาพ หรือจุดอ่อนที่เกิดขึ้นขณะใช้โปรแกรมประยุกต์ในการพัฒนาทดสอบการทำงาน จึงทำให้เว็บเซอร์วิสเกิดปัญหาขณะพัฒนาแล้วไม่สามารถนำไปใช้งานได้จริง

- เครื่องมือสนับสนุนการให้บริการ (Runtime Service Tools)

  เครื่องมือทางซอฟต์แวร์ประเภทนี้ส่วนใหญ่มีจุดอ่อนในการให้บริการที่ผิดพลาด เช่น ไม่สามารถให้บริการได้ตลอดเวลาทำการ การยอมให้เกิดการโจมตีจากจุดอ่อนที่มีอยู่ หรือยอมให้บุคคลอื่นล่วงละเมิดเข้ามาแก้ไขข้อมูลที่ไม่ได้รับอนุญาต

ซึ่งเครื่องมือทั้งสองประเภทนี้ ผู้วิจัยได้ทำการค้นหาข้อมูลจากรายการซีวีอี โดยในรายการซีวีอีมีจำนวนของรายชื่อผลิตภัณฑ์ที่เกี่ยวข้องมากพอสมควร จึงได้มีการคัดเลือกข้อมูลของผลิตภัณฑ์เฉพาะที่มีนัยสำคัญ ซึ่งจะได้นำเสนอดังนี้

3.1.1 การคัดเลือกผลิตภัณฑ์เว็บซอร์วิส

การคัดเลือกผลิตภัณฑ์เว็บเซอร์วิสมาใช้ในงานวิจัยนี้ ทางผู้วิจัยได้ทำการแบ่งเป็น 2 ส่วนคือ

1. ข้อมูลรายชื่อผลิตภัณฑ์ก่อนการนำไปค้นหาข้อมูลในรายการซีวีอี

ผู้วิจัยได้ทำการศึกษาหาข้อมูลของรายชื่อผู้ผลิตซอฟต์แวร์เว็บเซอร์วิสของแต่ละผลิตภัณฑ์ และได้นำรายชื่อเครื่องมือของแต่ละผลิตภัณฑ์มาค้นหาข้อมูลในรายการซีวีอี ซึ่งได้ข้อมูลรายชื่อผลิตภัณฑ์ 10 ตัว รายชื่อเครื่องมือ 20 ตัว โดยแบ่งเป็นเครื่องมือช่วยการพัฒนาจำนวน 6 ตัวและเครื่องมือสนับสนุนการให้บริการจำนวน 13 ตัว ดังแสดงในตารางที่ 3.1

ตารางที่ 3.1 ตารางแสดงข้อมูลรายชื่อผลิตภัณฑ์เว็บเซอร์วิสที่นำไปค้นหาในรายการซีวีอี

ลำดับ	บริษัท	Development Tools	Runtime Service Tools
1	Apache.org	ไม่พบ Entry ในซีวีอี	- jUDDI - Tomcat
2	BEA	ไม่พบ Entry ในซีวีอี	-Web Logic Server UDDI Registry
3	IBM	- Web Sphere Studio Application Developer	- HTTPs
4	Microsoft	- Microsoft UDDI Software Developers Kit - Microsoft Visual Studio .NET 2003 and 2005	- Internet Information Services (IIS)
5	Novell	ไม่พบ Entry ในซีวีอี	-Novell Nsure UDDI Server
6	Oracle	- JDeveloper	-OracleAS -Oracle Enterprise Manager
7	SAP	ไม่พบ Entry ในซีวีอี	-SAP Web Application Server
8	SOA Software	ไม่พบ Entry ในซีวีอี	-Registry Manager
9	Sun Microsystems	- NetBeans IDE - eclipse	-Java Web Services Developer Pack -Sun Java Enterprise
10	JBOSS	ไม่พบ Entry ในซีวีอี	-JBoss Application Server (JBoss AS)

จากข้อมูลในตารางที่ 3.1 ไม่พบรายการในซีวีอีสำหรับบางตัว และในการตรวจพบเบื้องต้นผลิตภัณฑ์บางตัวมีข้อมูลในรายการซีวีอีไม่เกิน 5 รายการเท่านั้น

2. การคัดกรองรายชื่อผลิตภัณฑ์

เนื่องจากบางผลิตภัณฑ์ไม่สามารถนำมาใช้งานได้ เช่น ข้อมูลน้อยเกินไป ในการวิจัยนี้ได้กำหนดว่าต้องมีจุดอ่อนเกิน 5 รายการ ดังนั้นผู้วิจัยจึงขอนำเสนอข้อมูลเฉพาะที่ค้นหาพบในรายการซีวีอีและมีข้อมูลมากกว่า 5 รายการขึ้นไปเท่านั้น ซึ่งก็จะเหลือรายชื่อผลิตภัณฑ์จำนวน 7 ผลิตภัณฑ์ที่ใช้ในงานวิจัยดังแสดงในตารางที่ 3.2

ตารางที่ 3.2 ตารางแสดงข้อมูลรายชื่อผลิตภัณฑ์ที่นำมาใช้ในงานวิจัยเตามประเภทเครื่องมือ

ลำดับ	บริษัท	Development Tools	Runtime Service Tools
1	BEA	ไม่พบ Entry ในซีวีอี	-Web Logic Server UDDI Registry
2	IBM	- Web Sphere Studio Application Developer	ไม่พบ Entry ในซีวีอี
3	Microsoft	- Microsoft Visual Studio .NET 2003 and 2005	- Internet Information Services (IIS)
4	Oracle	ไม่พบ Entry ในซีวีอี	-OracleAS
5	SAP	ไม่พบ Entry ในซีวีอี	-SAP Web Application Server
6	Sun Microsystems	ไม่พบ Entry ในซีวีอี	-Sun Java Enterprise
7	JBOSS	ไม่พบ Entry ในซีวีอี	-JBoss Application Server (JBoss AS)

3.1.2 การคัดเลือกรายการซีวีอีของผลิตภัณฑ์ที่เกี่ยวข้องกับเว็บเซอร์วิส

จุดอ่อนในรายการซีวีอีที่เกี่ยวข้องกับผลิตภัณฑ์เว็บเซอร์วิสมีจำนวนมาก ผู้วิจัยต้องทำการคัดเลือกรายการจุดอ่อนที่เกี่ยวข้องกับเว็บเซอร์วิสเท่านั้น การคัดเลือกรายการซีวีอีที่เกี่ยวข้องจะใช้การกำหนดเงื่อนไขของเนื้อหาดังนี้

- เกี่ยวข้องกับองค์ประกอบเว็บเซอร์วิส ได้แก่
  - WSDL (Web Service Description Language)
  - UDDI (Universal Description, Discovery and Integration)
  - SOAP (Simple Object access Protocol)

- เกี่ยวข้องกับรูปแบบการโจมตีเว็บเซอร์วิส [5,8] แบ่งเป็น

    1. บัฟเฟอร์โอเวอร์โฟล (Buffer Overflow) คือการใส่ข้อมูลลงให้มากกว่าที่ระบบรองรับได้ เพื่อให้ระบบล่มแล้วผู้บุกรุกจึงเข้ายึดครอง ในกรณีของเว็บเซอร์วิสนั้น ผู้บุกรุกจะพยายามใส่ค่า Input String ที่มาขนาดใหญ่มากเกินกว่าที่เซอร์วิสปลายทางจะรับได้

    2. ดีนาย อ็อฟ เซอร์วิส (Denial Of Service) คือการทำให้ระบบนั้นทำงานหนักจนไม่สามารถรับงานอื่นได้อีก วิธีที่แพร่หลายคือการ Flood ซึ่งสามารถทำได้โดยการส่งแพ็กเก็ตจำนวนมากไปยังเว็บเซอร์วิสปลายทางจนไม่สามารถประมวลผลได้ทัน และอาจส่งผลให้เซอร์วิสตัวนั้นต้องล่มไปในที่สุดหรืออย่างน้อยที่สุดก็คือ ไม่สามารถให้บริการการร้องขอตัวอื่นๆ ได้

    3. เอสคิวแอล อินเจคชั่น (SQL Injection) คือ การแทรกสอดโปรแกรมโดยผู้บุกรุกต้องมีความรู้เกี่ยวกับการทำงานภายในของระบบที่จะโจมตีพอสมควร ซึ่งผู้บุกรุกเองต้องมีการเก็บข้อมูลกันก่อนว่าเว็บเซอร์วิสตัวนี้ทำงานอย่างไร มีระบบเชื่อมต่ออย่างไรบ้าง ซึ่งโดยทั่วไปนั้นแฟ้มสามารถค้นข้อมูลเกี่ยวกับเว็บเซอร์วิสนั้นๆ ได้จากแหล่งทั่วไปในอินเทอร์เน็ต

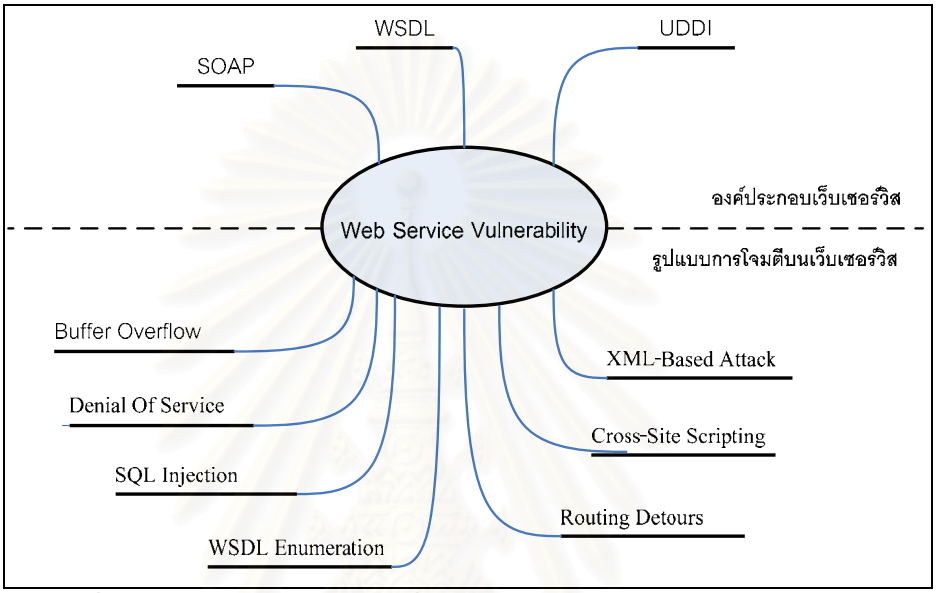
    4. ดับเบิ้ลยูเอสดีแอล อีนูเมอเรชั่น (WSDL Enumeration) แฟ้มดับเบิ้ลยูเอสดีแอลมีความสำคัญมาก เพราะเปิดเผยข้อมูลสำคัญๆในระบบ ข้อมูลต่างๆ เหล่านี้จำเป็นสำหรับผู้บุกรุกในการทำความเข้าใจกับระบบเพื่อเตรียมความพร้อมที่จะเจาะระบบในที่สุด

    5. เร้าติ้ง เดทัวร์ (Routing Detours) คือ แท้ที่จริงแล้วก็คืออีกรูปแบบหนึ่งของการโจมตีแบบแมนอินเดอะมิดเดิ้ล (Man-in-the-middle) ที่เรารู้จักกันดีอยู่แล้วนั่นเอง ในกรณีเว็บเซอร์วิสนั้นก็คือ การเปลี่ยนเส้นทางการวิ่งของข้อมูลเสียใหม่ ไปเป็นที่ที่แฮกเกอร์ต้องการแทน

    6. ครอสไซต์สคริปปิ้ง (Cross-Site Scripting) หรือที่บางคนเรียกว่า เอ็กเอ็มแอล เอ็นแคปซูเรชั่น (XML Encapsulation) จะอาศัยการใส่ข้อมูลลงในส่วนที่บ่งชี้ว่าข้อมูลส่วนใดของข้อความที่ไม่ต้องประมวลผล ดังนั้นจึงทำให้ผู้บุกรุกสามารถส่งโปรแกรมแปลกปลอมหรือหลอกลวงมาพร้อมกับข้อความได้

7. เอ็กเอ็มแอลเบสแอทแทค (XML-Based Attack) คือ การโจมตีที่จุดอ่อนของเอ็กเอ็มแอลพาซเซอร์ (XML Parser) ที่จัดการกับข้อความโซป

ซึ่งรูปแบบต่างๆ ที่กล่าวมาเป็นรูปแบบการโจมตีเว็บเซอร์วิส ซึ่งเป็นผลให้เกิดความเสียหาย ก็จะนับว่าเป็นส่วนที่เกี่ยวข้องกับการโจมตีและจะนำรายการที่มีเนื้อหาจุดอ่อนดังกล่าวมาใช้ในงานวิจัยดังแสดงในรูปที่ 3.2



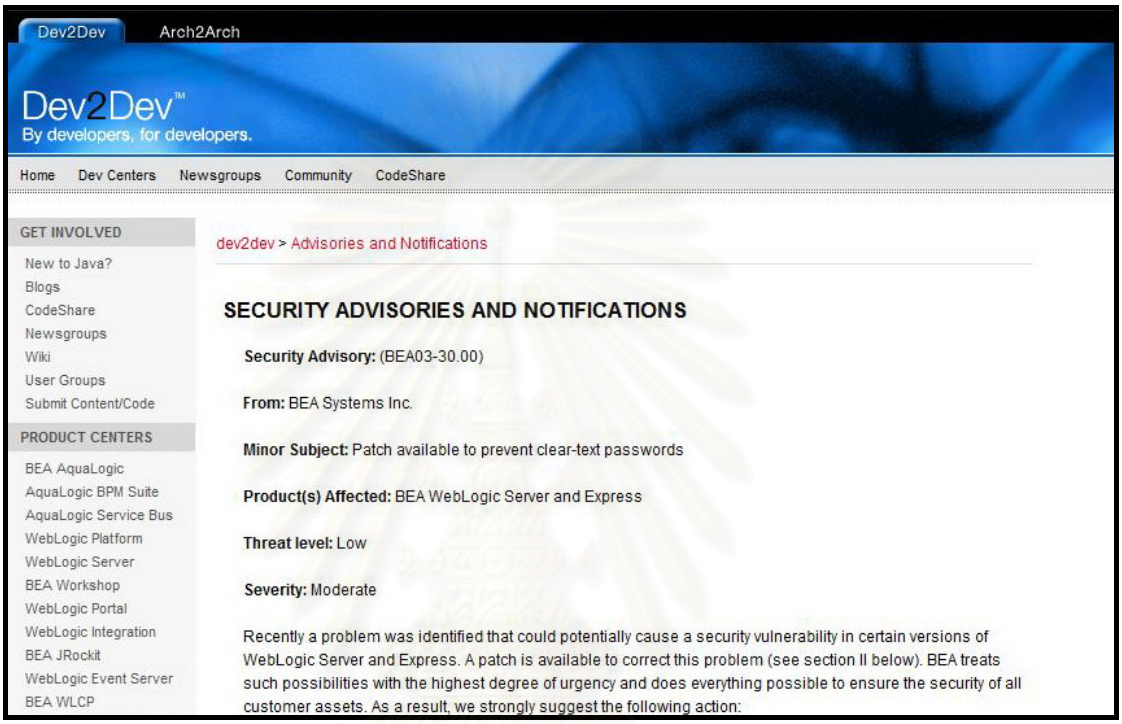
รูปที่ 3.2 รูปแสดงแผนผังข้อมูลที่ใช้ในการคัดเลือกจุดอ่อนจากรายการซีวีอี

ตารางที่ 3.3 รายการจุดอ่อนซีวีอีของผลิตภัณฑ์ BEA

รายการซีวีอี	CVE-0652-2004
รายละเอียด	The default CredentialMapper for BEA Web Logic Server and Express 7.0 and 7.0.0.1 stores passwords in cleartext on disk, which allows local users to extract passwords.
รายการอ้างอิง	BEA:BEA03-30.00 | URL:http://dev2dev.bea.com/pub/advisory/22 | BID:7563 | URL:http://www.securityfocus.com/bid/7563

จากข้อมูลรายการซีวีอีในตารางที่ 3.3 ดูจากคำอธิบายแล้วยังไม่สามารถสรุปได้ชัดเจนว่าเป็นจุดอ่อนในส่วนของเว็บเซอร์วิสหรือไม่ ดังนั้นผู้วิจัยจึงจำเป็นต้องค้นหาข้อมูลเพิ่มเติม

ตามแหล่งข้อมูลตามรายการอ้างอิงของซีวีอี เช่น ในรายการจุดอ่อน CVE-0652-2004 สามารถค้นหาข้อมูลเพิ่มเติมได้ที่เว็บไซต์ในรายการอ้างอิง เพื่อตรวจสอบรายการจุดอ่อนว่าเป็นข้อมูลที่เกี่ยวข้องกับเว็บเซอร์วิสตามในรายละเอียดที่กำหนดไว้ในรายการซีวีอีหรือไม่ ซึ่งแสดงดังรูปที่ 3.3 และ 3.4 ของเว็บไซต์ http://dev2dev.bea.com/pub/advisory/22 ของ Dev2Dev และ เว็บไซต์ http://www.securityfocus.com/bid/7563 ของ Security Focus

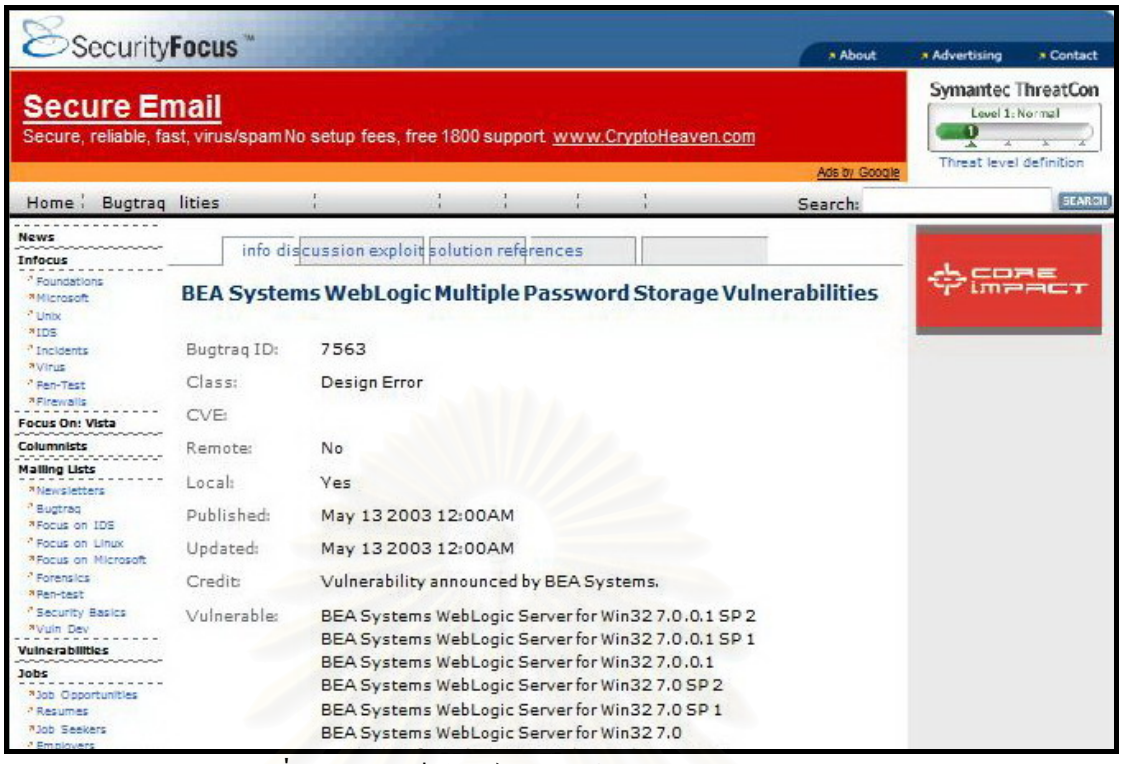


รูปที่ 3.3 แสดงเว็บไซต์รายการอ้างอิงของ BEA

รูปที่ 3.3 แสดงเว็บไซต์ของ BEA ที่ใช้ในการอ้างอิงจุดอ่อน โดยในเว็บไซต์มีเนื้อหาดังนี้

Security Advisories and Notifications

Security Advisory:	(BEA03-30.00)
From:	BEA Systems Inc.
Minor Subject:	Patch available to prevent clear-text passwords
Product(s) Affected:	BEA WebLogic Server and Express
Threat level:	Low
Severity:	Moderate



รูปที่ 3.4 แสดงเว็บไซต์รายการอ้างอิงของ Security Focus

รูปที่ 3.4 แสดงเว็บไซต์ของรายการอ้างอิงเลขที่ BID: 7563 เพื่อใช้ในการตรวจสอบจุดอ่อนจากแหล่งอ้างอิงของ Security โดยมีเนื้อหาในเว็บไซต์ดังนี้

BEA Systems WebLogic Multiple Password Storage Vulnerabilities

Bugtraq ID: 7563

Class: Design Error

CVE: CVE-0652-2004

Remote: No

Local: Yes

Published: May 13 2003 12:00AM

Updated: May 13 2003 12:00AM

Credit: Vulnerability announced by BEA Systems.

Vulnerable: BEA Systems WebLogic Server for Win32 7.0 .0.1 SP 2

BEA Systems WebLogic Server for Win32 7.0 .0.1 SP 1

BEA Systems WebLogic Server for Win32 7.0 .0.1

BEA Systems WebLogic Server for Win32 7.0 SP 2

BEA Systems WebLogic Server for Win32 7.0 SP 1

BEA Systems WebLogic Server for Win32 7.0

เมื่อพิจารณาจากเนื้อหาในเว็บไซต์รายการอ้างอิง ซึ่งมีเนื้อหาที่เกี่ยวข้องกับรายการซีวีอี CVE0652-2004 และเกี่ยวข้องกับจุดอ่อนบนผลิตภัณฑ์ของ BEA WebLogic ซึ่งข้อมูลดังกล่าวสามารถอ้างอิงเพื่อยืนยันข้อมูลในรายการซีวีอีได้

3.2 การจัดกลุ่มจุดอ่อนของเว็บเซอร์วิส

ในส่วนการจัดกลุ่มจุดอ่อนอิงตามการจัดกลุ่มจุดอ่อนงานวิจัยของรัศมีทิพย์ [2] โดยทำการแบ่งจุดอ่อนออกเป็น 3 รูปแบบด้วยกัน ได้แก่ ประเภทของจุดอ่อน จุดที่เกิดจุดอ่อน และลักษณะความเสียหาย

3.2.1 ประเภทของจุดอ่อน

เป็นการจัดกลุ่มของความผิดพลาดที่มีในระบบโดยแบ่งออกได้เป็น 9 ประเภทดังนี้

1. การตรวจสอบข้อมูลนำเข้า (Input Validation)
2. ขอบเขตข้อมูล (Boundary Validation)
3. การตรวจสอบการเข้าถึง (Access Validation)
4. การเหลื่อมล้ำของการตรวจสอบสิทธิ (Serialization)
5. การปรับแต่งระบบ (Configuration)
6. สภาพแวดล้อม (Environmental)
7. การออกแบบระบบ (Design)
8. ชุดคำสั่งจัดการสิ่งผิดปกติ (Exception Handling)
9. อื่นๆ (Other)

ในงานวิจัยนี้จะกำหนดให้รายการจุดอ่อนแต่ละรายการมีประเภทของจุดอ่อนได้เพียง 1 ประเภทเพื่อความสะดวกในการจัดกลุ่มของจุดอ่อน

3.2.2 จุดที่เกิดจุดอ่อน

เป็นการแบ่งตามตำแหน่งที่เกิดจุดอ่อนว่าอยู่ส่วนใดของระบบ ซึ่งแบ่งได้ 8 ตำแหน่งดังนี้

1. ส่วนการเริ่มต้นระบบ (System Initiation)
2. ส่วนการจัดการหน่วยความจำ (Memory Management)
3. ส่วนการจัดการโปรเซส (Process Management)
4. ส่วนการจัดการอุปกรณ์ (Device Management)
5. ส่วนการจัดการแฟ้มข้อมูล (File Management)
6. ส่วนการพิสูจน์ตัวตน (Authentication)
7. ส่วนโปรแกรมที่สนับสนุนการทำงานระบบปฏิบัติการ (Support)
8. ส่วนโปรแกรมประยุกต์ (Application)

ในงานวิจัยนี้กำหนดรายการจุดอ่อนแต่ละรายการมีจุดที่เกิดได้เพียง 1 จุดเท่านั้น

3.2.3 ลักษณะความเสียหาย

การจัดกลุ่มจุดอ่อนจะจัดกลุ่มตามลักษณะความเสียหายที่เกิดขึ้น อาศัยพื้นฐานการรักษาความปลอดภัยทั่วๆไปของระบบ โดยอ้างอิงตามงานวิจัยของเกียรติ ภิรมย์โสภา [4] ประกอบด้วย

- ความลับ (Confidentiality)
- ความบูรณภาพ (Integrity)
- ความพร้อมใช้งาน (Availability)

3.2.4 ระดับความรุนแรง

เนื่องจากจุดอ่อนแต่ละรายการในทั้ง 3 รูปแบบที่กล่าวมาสามารถก่อความเสียหายมากน้อยไม่เท่ากัน จึงต้องแบ่งระดับความรุนแรงของความเสียหายที่เกิดขึ้นนั้น ออกเป็น 3 ระดับ ได้แก่

- ระดับสูง (High)
- ระดับกลาง (Medium)
- ระดับต่ำ (Low)

จากขั้นตอนการประเมินจุดอ่อนของเว็บเซอร์วิสดังที่กล่าวมาทั้งหมด ผู้วิจัยได้ทำการประเมินและคำนวณระดับคะแนนของผลกระทบของรายการจุดอ่อนตามซีวีอีทั้งหมด 416 รายการ โดยแยกเป็นเครื่องมือช่วยการพัฒนา จำนวน 54 รายการและเครื่องมือสนับสนุนการให้บริการ จำนวน 362 รายการ

3.3 การประเมินคะแนนจุดอ่อน

การแจกแจงคะแนนของรายการจุดอ่อนจะให้คะแนนจำแนกตามความเสียหาย โดยการใช้ระดับความรุนแรงอ้างอิงจากตารางที่ 3 เป็นรูปแบบที่ใช้ในการประเมินคะแนน โดยการแจกแจงคะแนนจะประกอบด้วย 2 ส่วน คือ

- การกำหนดคะแนนระดับความรุนแรง
- การประเมินระดับผลกระทบ

ประเภทของความเสียหายที่เกิดขึ้น ได้แก่ การรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน [2 , 4] ดังตารางที่ 3.4

ตารางที่ 3.4 แสดงเงื่อนไขในการกำหนดระดับผลกระทบแยกตามความเสียหาย

ระดับความรุนแรง			
ระดับสูง	ระดับกลาง	ระดับต่ำ	ไม่มีผลกระทบ
สูญเสียความลับ (Confidential)			
- เรียกดูข้อมูล โดยใช้สิทธิ์ของผู้ใช้งานสูงสุด	- เรียกดูข้อมูลโดยใช้สิทธิของระดับผู้ใช้งานที่สามารถเข้าถึงได้	- เรียกดูข้อมูลในระบบโดยใช้สิทธิ์ผู้ใช้งานทั่วไป	- ผู้มีสิทธิสามารถเรียกดูข้อมูลที่เปิดเผยแก่บุคคลทั่วไป
สูญเสียบูรณภาพ (Integrity)			
- แก้ไขข้อมูลโดยใช้สิทธิของผู้ใช้งานสูงสุด	- แก้ไขข้อมูลโดยใช้สิทธิของระดับผู้ใช้งานที่สามารถแก้ไขข้อมูลได้	- แก้ไขข้อมูลโดยใช้สิทธิของผู้ใช้งานทั่วไป	- แก้ไขข้อมูลตามสิทธิที่ได้รับเท่านั้น
สูญเสียความพร้อมใช้งาน (Available)			
- ทำให้ผู้ใช้งานระบบไม่สามารถใช้บริการระบบได้	- หยุดการให้บริการบางส่วนของระบบ	- สร้างข้อมูลจำนวนมากในระบบแต่ระบบยังสามารถให้บริการได้ปกติ	- สามารถใช้บริการของระบบได้ตามสิทธิที่ได้รับเท่านั้น

3.3.1 การกำหนดคะแนนระดับความรุนแรง

การประเมินผลจุดอ่อนคำนวณได้โดยการใช้ผลรวมคะแนนของระดับความเสียหายแต่ละประเภท โดยกำหนดคะแนนไว้ดังนี้ [2]

ตารางที่ 3.5 การกำหนดคะแนนระดับความรุนแรง

ประเภทความเสียหาย	ระดับความรุนแรง			
	สูง	กลาง	ต่ำ	ไม่มีผลกระทบ
การรักษาความลับ	3	2	1	0
บูรณภาพ	3	2	1	0
สภาพพร้อมใช้งาน	3	2	1	0

3.3.2 การประเมินระดับผลกระทบ

การประเมินระดับผลกระทบของจุดอ่อนที่สามารถคำนวณได้โดยการใช้ผลรวมคะแนนของระดับความเสียหายแต่ละประเภทที่เกิดขึ้น ได้แก่ การรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน คิดได้จากสมการดังนี้ [5]

$$W_i = WC_i + WI_{i+} WA_i \quad \text{----------(1)}$$

โดยที่

W_i คือ ระดับผลกระทบของจุดอ่อนใดๆ

WC_i คือ ระดับผลกระทบของจุดอ่อนใดๆ ที่ส่งผลต่อการรักษาความลับ

WI_i คือ ระดับผลกระทบของจุดอ่อนใดๆ ที่ส่งผลต่อการบูรณภาพ

WA_i คือ ระดับผลกระทบของจุดอ่อนใดๆ ที่ส่งผลต่อสภาพพร้อมใช้งาน

i คือ ลำดับของซีวีอี

โดยให้ค่าของผลกระทบที่ส่งผลต่อการรักษาความลับ (C) ต่อบูรณภาพ (I) และต่อสภาพพร้อมใช้งาน (A) แต่ละประเภทมีค่าเป็น 1 และผลกระทบแบ่งเป็น 4 ระดับ คือ ส่งผล

กระทบสูงมีคะแนนเป็น 3 ส่งผลกระทบปานกลางมีคะแนนเป็น 2 ส่งผลกระทบต่ำมีคะแนนเป็น 1 และไม่มีผลกระทบ มีคะแนนเป็น 0 แล้วจึงคำนวณโดยใช้สมการ $\sum_{i=1}^{n} W_i$ เพื่อคำนวณคะแนนผลกระทบโดยรวมของจุดอ่อนออกมา

ดังนั้นจุดอ่อนต่างๆ สามารถมีค่าผลกระทบได้สูงสุดคือ 3 + 3 + 3 = 9 และมีค่าผลกระทบต่ำสุดคือ 0 + 0 + 0 = 0 หรือไม่มีผลกระทบต่อความมั่นคงของระบบนั่นเอง ดังแสดงตามตารางที่ 5 ซึ่งค่าระดับผลกระทบนั้นแสดงถึงระดับความเสียหายที่เกิดขึ้นจากจุดอ่อนนั้นๆ โดยหากจุดอ่อนใดมีค่าระดับผลกระทบสูง หมายถึงจุดอ่อนนั้นสามารถสร้างความเสียหายให้แก่องค์กรได้มากกว่าจุดอ่อนที่ระดับผลกระทบ ต่ำกว่า

3.4 การจัดเก็บข้อมูลจุดอ่อน

งานวิจัยนี้ได้ทำการจัดเก็บข้อมูลลงบนโปรแกรมไมรโครซอฟต์เอ็กเซล (Microsoft Excel) เพราะโปรแกรมสามารถนำข้อมูลไปสร้างข้อมูลประเภทกราฟ และนำไปวิเคราะห์ข้อมูลในเชิงสถิติได้ง่าย ตารางที่ 3.6 แสดงตารางการจัดเก็บข้อมูลที่ใช้ในการประเมินคะแนนจุดอ่อน ซึ่งข้อมูลที่จัดเก็บลงในตารางมีคำอธิบายและรายละเอียดเพื่อใช้ในการจัดเก็บข้อมูลตามตารางที่ 3.7

ตารางที่ 3.6 ตารางการจัดเก็บข้อมูลของจุดอ่อนโดยใช้ไมรโครซอฟต์เอ็กเซล

Name	Description	Vulnerabilities and Explosures																								
		Type		Vulnerability Type									Location								Loss Type			Score
		Runtime Tools	Develop Tools	Input Validation Error	Boundary Overflow	Access Validation Error	Serialization	Configuration Error	Environmanetal Error	Design Error	Exceptional Condition	Others	System Initiation	Memory Management	Process Management	Device Management	File Management	Authentication	Support	Application	Confidentiality	Integrity	Availability	
Total		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

ตารางที่ 3.7 คำอธิบายตารางจัดเก็บข้อมูลจุดอ่อน

ชื่อหัวข้อ	**คำอธิบาย**
NAME	ชื่อรายการซีวีอี
Description	คำอธิบายจุดอ่อนว่าเกิดขึ้น ณ จุดใด เพราะอะไร
Type	ประเภทครื่องมือ แสดงในรูปของจำนวนของรายการซีวีอี
Vulnerability Type	ประเภทของจุดอ่อน แบ่งออกเป็น 8 ประเภท โดยการบันทึกข้อมูลจะกำหนดให้สามารถระบุประเภทของประเภทจุดอ่อนที่เกิดขึ้นได้เพียง 1 ประเภทเท่านั้น
Location	ตำแหน่งที่เกิดจุดอ่อน แบ่งเป็น 8 แห่ง โดยการบันทึกจะกำหนดให้ 1 รายการซีวีอีสามารถระบุตำแหน่งได้เพียง 1 ตำแหน่งที่เกี่ยวข้องเท่านั้น
Loss Type	ประเภทของความเสียหายที่เกิดขึ้น แบ่งเป็น 3 ประเภท โดยการบันทึกคะแนนความเสียหายของจุดอ่อนที่เกิดขึ้นของข้อมูล การกำหนดคะแนนใช้เกณฑ์ตามกำหนดเพื่อระบุถึงค่าความเสียหายที่อาจเกิดขึ้นกับผลิตภัณฑ์

จากหลักเกณฑ์การคัดเลือกข้อมูลจุดอ่อน การรวบรวมข้อมูลจุดอ่อนต่างๆ ทำการจัดกลุ่มของจุดอ่อน และจัดเก็บข้อมูลจุดอ่อนที่ได้ หลังจากเสร็จสิ้นกระบวนการต่างๆในขั้นตอนเหล่านี้แล้ว ในขั้นตอนต่อไป จะเป็นการคำนวณปริมาณจุดอ่อนที่เกิดขึ้นบนแยกตามประเภทของเครื่องมือ และการคำนวณคะแนนความเสียหายของจุดอ่อนที่มีอยู่ในรายการซีวีอี

3.5 การคำนวณและแจกแจงคะแนนความเสียหายจากข้อมูลจุดอ่อน

ขั้นตอนการคำนวณและแจกแจงคะแนนของจุดอ่อนในรายการซีวีอีเพื่อนำมาใช้ในการวิเคราะห์และประเมินผลจุดอ่อนของแต่ละผลิตภัณฑ์มีขั้นตอนดังต่อไปนี้

3.5.1 การนับจำนวนรายการจุดอ่อน

การนับจำนวนรายการจุดอ่อนจากงานวิจัยนี้ ใช้การนับรายการจุดอ่อนซีวีอี 1 รายการเป็น 1 จุดอ่อน กรณีที่รายการจุดอ่อนของผลิตภัณฑ์ใดที่มีเวอร์ชั่นต่างกัน แต่เกิดตำแหน่งของจุดอ่อนที่พบเดียวกันจะนับว่าเป็นรายการจุดอ่อนคนละรายการ

3.5.2 ตัวอย่างการคำนวณและการแจกแจงคะแนน

เมื่อผู้วิจัยทำการประเมินคะแนนจากรูปแบบและสูตรการคำนวณดังที่กล่าวมา ข้อมูลแต่ละรายการจะถูกจัดเก็บในตารางเก็บข้อมูล ซึ่งสามารถอธิบายข้อมูลได้ดังตัวอย่างในตารางที่ 3.8

ตารางที่ 3.8 แสดงการคำนวณคะแนนจุดอ่อน

Name	Description	Vulnerabilities and Explosures																								
		Type		Vulnerability Type									Location								Loss Type			Score
		Runtime Tools	Develop Tools	Input Validation Error	Boundary Overflow	Access Validation Error	Serialization	Configuration Error	Environmental Error	Design Error	Exceptional Condition	Others	System Initiation	Memory Management	Process Management	Device Management	File Management	Authentication	Support	Application	Confidentiality	Integrity	Availability	
CVE-2004-0205	Buffer overflow in Microsoft Internet Information Server (IIS) 4.0 allows local users to execute arbitrary code via the redirect function.	X			X															X	2	2	0	4

จากตารางที่ 3.8 สามารถอธิบายรายการจุดอ่อนที่อยู่ในตารางได้ดังนี้

ชื่อรายการจุดอ่อน CVE-2004-0205

รายละเอียด Unknown vulnerability in an ISAPI plugin for ISS Server Sensor 7.0 XPU 20.16, 20.18, and possibly other versions before 20.19, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code in Internet Information Server (IIS) via a certain URL through SSL.

ประเภทเครื่องมือ เครื่องมือสนับสนุนการให้บริการ (Runtime Service Tools)

ประเภทของจุดอ่อน Serialization

จุดที่เกิดจุดอ่อน File Management

คะแนนความเสียหาย 4 คะแนน (2+ 2+ 0)

สามารถคำนวณคะแนนความเสียหายได้ดังนี้

คำนวณคะแนนความเสียหายได้จากสมการที่ (1) ดังนี้

$$\text{คะแนนความเสียหาย} = \sum_{i=1}^{n} W_i$$

ความเสียหาย : 2 + 2 + 0 = 4

ผลลัพธ์ได้เป็นดังนี้

1. CVE-2004-0205 มีประเภทจุดอ่อนที่ Serialization
2. CVE-2004-0205 สามารถเกิดจุดอ่อนได้ที่ File Management
3. CVE-2004-0205 มีคะแนนความรุนแรงทั้งหมดเท่ากับ 4 คะแนน
4. CVE-2004-0205 มีคะแนนความเสียหายและระดับความรุนแรงดังนี้

   Confidentiality = 2 คะแนน ความรุนแรงระดับปานกลาง

   Integrity = 2 คะแนน ความรุนแรงระดับปานกลาง

   Availability= 0 คะแนน ไม่มีผลกระทบต่อความเสียหาย

ในบทที่ 3 นี้เป็นขั้นตอนและวิธีการ ในการคำนวณคะแนนความเสียหายของจุดอ่อนที่เกิดขึ้นของแต่ละซีวีอีที่เกี่ยวข้องกับผลิตภัณฑ์เว็บเซอร์วิส ซึ่งในบทต่อไป คือ บทที่ 4 จะเป็นผลการวิจัย และการวิเคราะห์และเปรียบเทียบผลลัพธ์ที่ได้จากการคำนวณ

บทที่ 4
ผลการวิเคราะห์ข้อมูล

ในงานวิจัยนี้ทำการค้นหารายการจุดอ่อนบนรายการซีวีอีเวอร์ชั่น 20061101 จำนวน 21,516 รายการ แต่มีจุดอ่อนที่เกี่ยวข้องกับผลิตภัณฑ์เว็บเซอร์วิสทั้งเจ็ดตัวจำนวน 416 รายการ โดยแยกเป็นเครื่องมือช่วยการพัฒนาจำนวน 54 รายการและเครื่องมือสนับสนุนการให้บริการจำนวน 362 รายการ ผลลัพธ์จากการประเมินและเปรียบเทียบจุดอ่อนสามารถแบ่งออกเป็นกลุ่มข้อมูลดังนี้

- รายชื่อผลิตภัณฑ์
- ประเภทที่เกิดจุดอ่อน
- จุดที่เกิดจุดอ่อน
- ลักษณะความเสียหาย

4.1 ผลลัพธ์แยกตามรายชื่อผลิตภัณฑ์

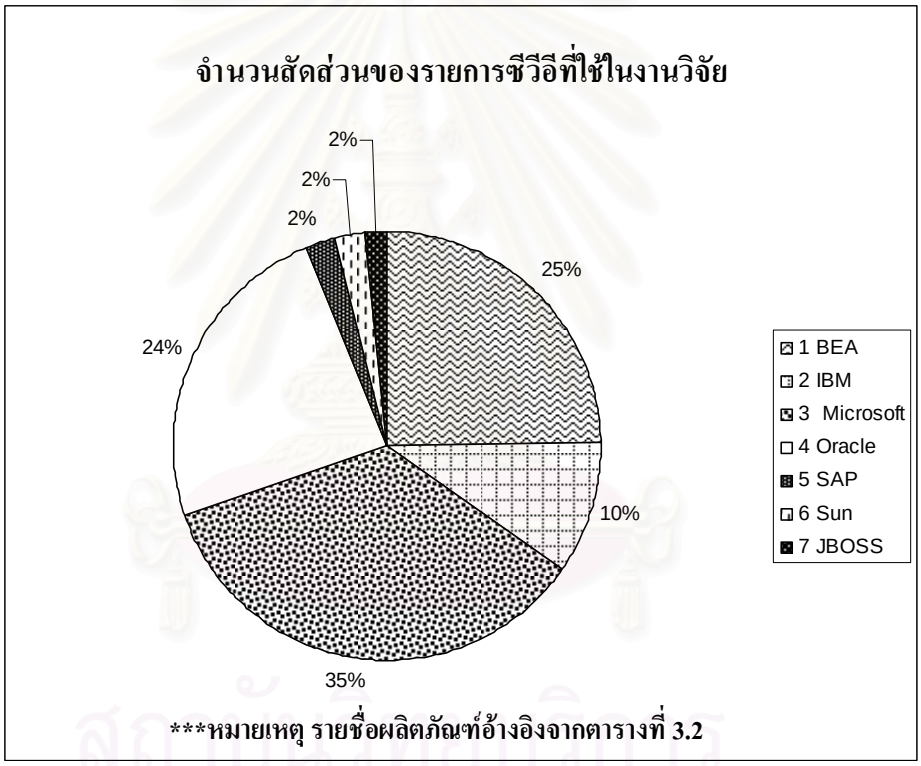
ข้อมูลผลิตภัณฑ์เว็บเซอร์วิสแบ่งออกเป็น 2 กลุ่มคือ เครื่องมือสนับสนุนการให้บริการ (Runtime Service Tools) และเครื่องมือช่วยการพัฒนา (Development Tools) ซึ่งผลลัพธ์แสดงดังตารางที่ 4.1

ตารางที่ 4.1 จำนวนรายการซีวีอีของแต่ละผลิตภัณฑ์โดยแยกตามเครื่องมือ

No.	Product	Runtime Service Tools	Development Tools	Total
1	BEA	103	0	103
2	IBM	0	42	42
3	Microsoft	142	3	145
4	Oracle	101	0	101
5	SAP	9	0	9
6	Sun	0	9	9
7	JBOSS	7	0	7
	TOTAL	362	54	416
***หมายเหตุ รายชื่อผลิตภัณฑ์อ้างอิงจากตารางที่ 3.2				

กลุ่มของเครื่องมือสนับสนุนการให้บริการ เครื่องมือที่มีรายการจุดอ่อนซีวีอีมากที่สุด คือ ผลิตภัณฑ์ของ Microsoft มีจำนวน 142 รายการ และเครื่องมือที่มีรายการจุดอ่อนน้อยที่สุด คือ ผลิตภัณฑ์ของ IBM และ SUN มีจำนวน 0 รายการ (กรณีจำนวนรายการจุดอ่อนมีค่าเท่ากับ 0 แสดงว่าไม่พบรายการจุดอ่อนของผลิตภัณฑ์ดังกล่าวปรากฏในซีวีอี)

และกลุ่มของผลิตภัณฑ์กลุ่มเครื่องมือช่วยการพัฒนาเว็บเซอร์วิส ผลิตภัณฑ์ที่มีรายการจุดอ่อนซีวีอีมากที่สุด คือ ผลิตภัณฑ์ของ IBM มีจำนวน 42 รายการ และผลิตภัณฑ์ที่มีรายการจุดอ่อนน้อยที่สุด คือ ผลิตภัณฑ์ของ BEA, Oracle, SAP และ JBOSS มีจำนวน 0 รายการ (กรณีจำนวนรายการจุดอ่อนมีค่าเท่ากับ 0 แสดงว่าไม่พบรายการจุดอ่อนของผลิตภัณฑ์ดังกล่าวปรากฏในซีวีอี)



รูปที่ 4.1 สัดส่วนรายการจุดอ่อนซีวีอีแยกตามผลิตภัณฑ์

รูปที่ 4.1 แสดงอัตราสัดส่วนของรายการจุดอ่อนซีวีอีที่ใช้ในงานวิจัยโดยแยกตามรายชื่อผลิตภัณฑ์ เมื่อดูจากสัดส่วนแล้วผลิตภัณฑ์ที่พบจุดอ่อนในรายการซีวีอีเรียงลำดับจากมากไปน้อยที่สุดดังนี้

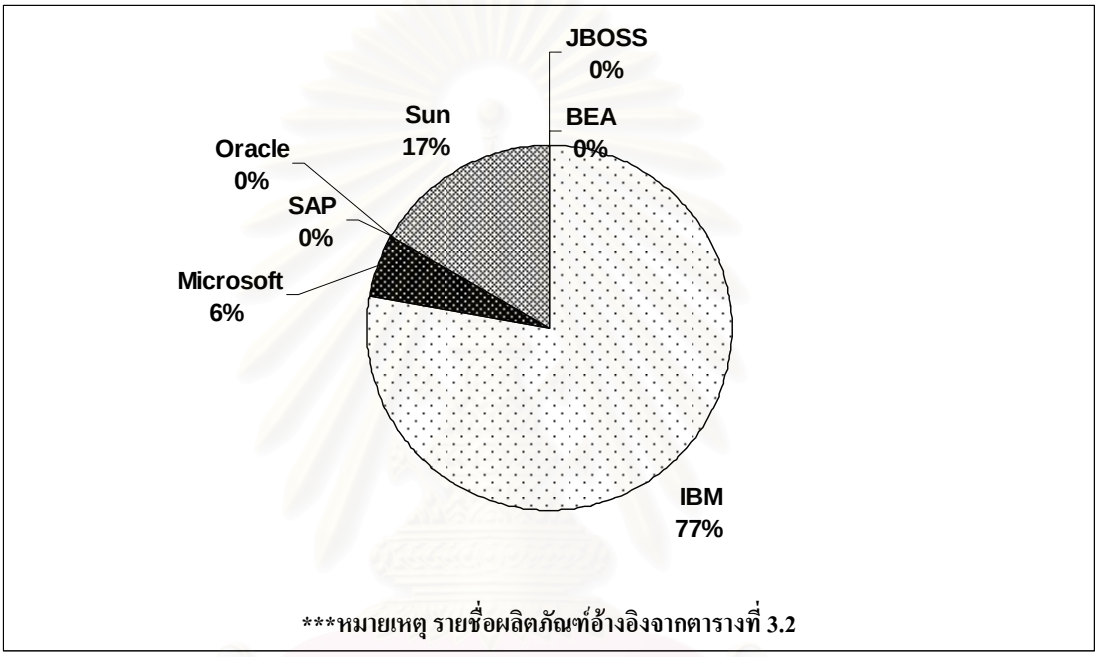
1. Microsoft จำนวน 35 %
2. BEA จำนวน 25%

3. Oracle จำนวน 24 %

4. IBM จำนวน 10 %

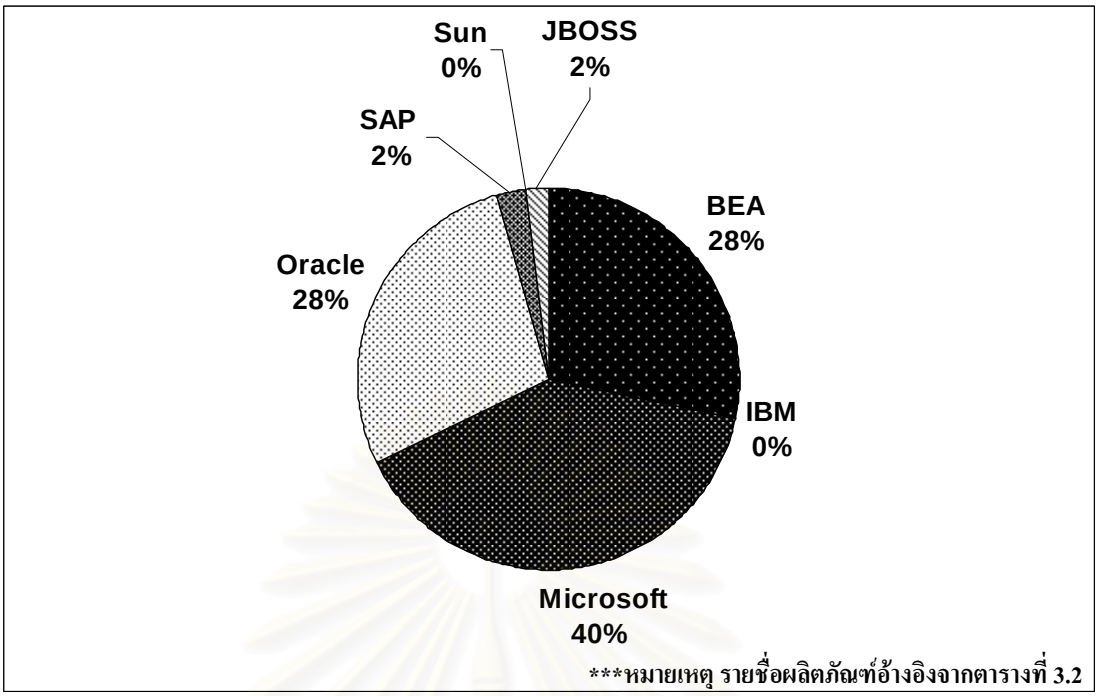
5. SAP , SUN Microsystems และ JBOSS จำนวน 2 %

ซึ่งพิจารณาจากข้อมูลจะพบว่าจุดอ่อนส่วนใหญ่เกิดจากผลิตภัณฑ์ที่มีความนิยมในการใช้งานสูงและมีการใช้งานอย่างกว้างขวางกว่าผลิตภัณฑ์ที่ไม่เป็นที่นิยม



รูปที่ 4.2 สัดส่วนรายการจุดอ่อนของเครื่องมือช่วยการพัฒนาแยกตามผลิตภัณฑ์

รูปที่ 4.2 แสดงสัดส่วนของรายการซีวีอีแยกตามรายชื่อผลิตภัณฑ์ในกลุ่มของเครื่องมือช่วยการพัฒนาเว็บเซอร์วิสโดยเรียงลำดับตามสัดส่วนจากมากไปน้อย IBM จำนวน 77%, SUN Microsystems จำนวน 16 %, Microsoft จำนวน 7%, Oracle, SAP, BEA และ JBOSS จำนวน 0 % (กรณีจำนวนรายการจุดอ่อนมีค่าเท่ากับ 0 % แสดงว่าไม่พบรายการจุดอ่อนของผลิตภัณฑ์ดังกล่าวปรากฏในซีวีอี) เมื่อพิจารณาแล้วจะเห็นได้ว่ากลุ่มผลิตภัณฑ์เครื่องมือช่วยพัฒนาที่มีผู้ใช้งานเป็นนิยมอย่างกว้างขวางจะมีรายการจุดอ่อนมากกว่าแบบที่ไม่เป็นที่นิยมของเครื่องมือ



รูปที่ 4.3 สัดส่วนจุดอ่อนของเครื่องมือสนับสนุนการให้บริการแยกตามผลิตภัณฑ์

รูปที่ 4.3 แสดงสัดส่วนของรายการซีวีอีแยกตามเครื่องมือสนับสนุนการให้บริการเว็บเซอร์วิสโดยเรียงลำดับตามสัดส่วนจากมากไปน้อย ผลที่ได้คือ Microsoft จำนวน 40%, BEA และ Oracle จำนวน 28%, JBOSS และ SAP จำนวน 2%, SUN และ IBM จำนวน 0% (กรณีจำนวนรายการจุดอ่อนมีค่าเท่ากับ 0 % แสดงว่าไม่พบรายการจุดอ่อนของผลิตภัณฑ์ดังกล่าวปรากฏในซีวีอี)

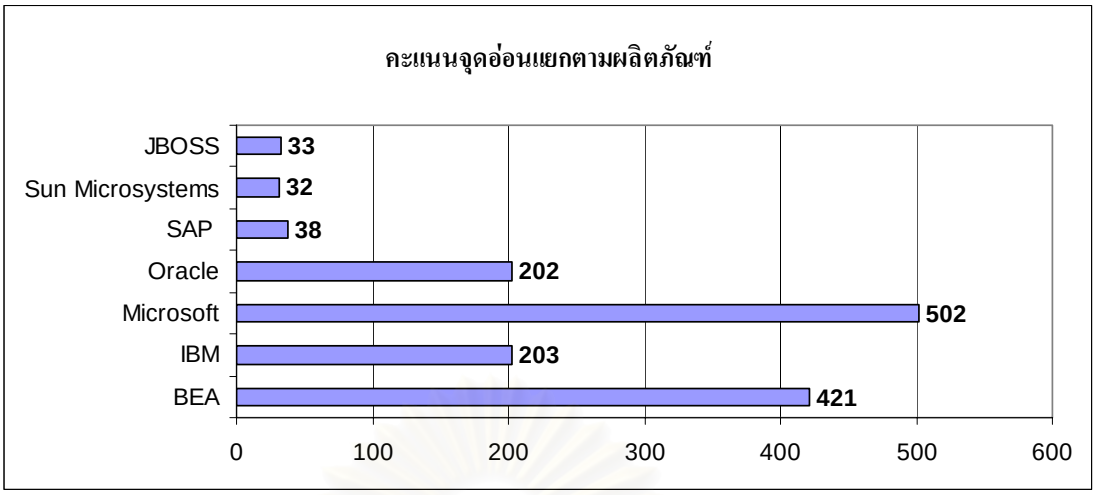
ตารางที่ 4.2 แสดงคะแนนที่ได้จากการประเมินของแต่ละผลิตภัณฑ์ ซึ่งการคำนวณคะแนนนี้เป็นไปตามแนววิธีในหัวข้อ 3.3 โดยข้อมูลของคะแนนจุดอ่อนรวมทั้งหมดมีค่าคะแนนเท่ากับ 1,431 คะแนน ที่มีค่าคะแนนสูงที่สุดคือ ผลิตภัณฑ์ของ Microsoft 502 คะแนน อันดับที่ 2 คือ BEA 421 คะแนน อันดับที่ 3 คือ IBM 203 คะแนน และต่ำสุดคือผลิตภัณฑ์ของ SUN 32 คะแนน

ตารางที่ 4.2 แสดงข้อมูลคะแนนจุดอ่อนของแต่ละผลิตภัณฑ์

No.	Product	Runtime Service Tools	Development Tools	Total
1	BEA	421	0	421
2	IBM	0	203	203
3	Microsoft	481	21	502
4	Oracle	202	0	202
5	SAP	38	0	38
6	Sun	0	32	32
7	JBOSS	33	0	33
	Total	1175	256	1431
*****หมายเหตุ รายชื่อผลิตภัณฑ์อ้างอิงจากตารางที่ 3.2**				

โดยคะแนนจุดอ่อนของกลุ่มเครื่องมือช่วยการพัฒนา ผลิตภัณฑ์ที่มีคะแนนสูงที่สุดคือ IBM 203 คะแนน อันดับที่ 2 คือ SUN Microsystems 32 คะแนน อันดับที่ 3 คือ Microsoft 21 คะแนน และต่ำสุดคือ BEA, Oracle, SAP และ JBOSS 0 คะแนน และคะแนนจุดอ่อนของกลุ่มเครื่องมือสนับสนุนการให้บริการ ผลิตภัณฑ์ที่มีคะแนนสูงที่สุดคือ Microsoft 481 คะแนน อันดับที่ 2 คือ BEA 421 คะแนน อันดับที่ 3 คือ Oracle 202 คะแนน และต่ำสุดคือ IBM และSUN Microsystems 0 คะแนน

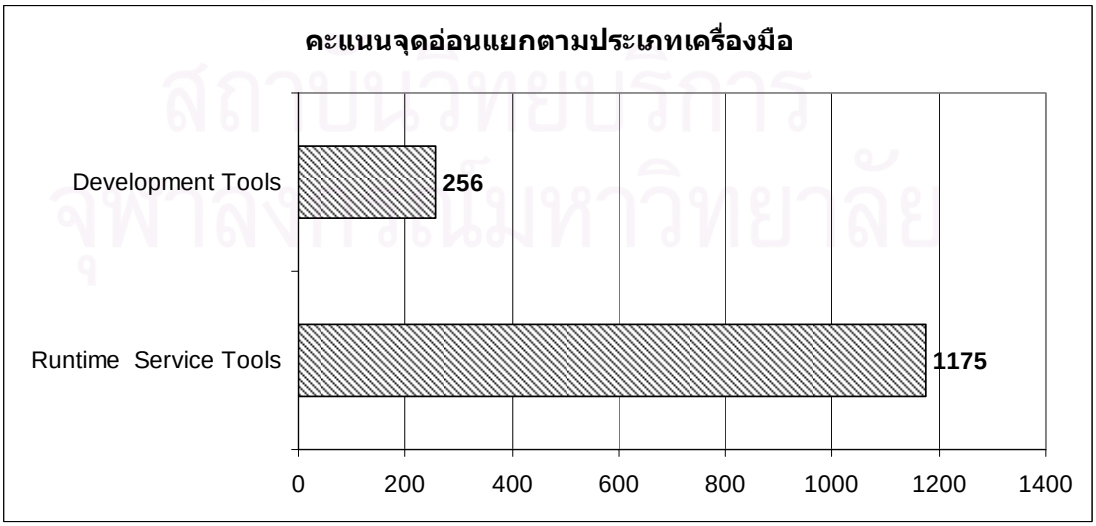
เมื่อพิจารณาจากคะแนนที่ได้มาจากการประเมินแล้ว จะสังเกตุได้ว่ารายชื่อผลิตภัณฑ์ที่มีคะแนนสูงจะเป็นกลุ่มของผลิตภัณฑ์ที่มีชื่อเสียงและได้รับความนิยมในการใช้งานสูง อาจเป็นเพราะการใช้งานเป็นที่แพร่หลายจึงอาจมีผู้ค้นพบจุดอ่อนได้มากกว่ากลุ่มผลิตภัณฑ์ที่ไม่ค่อยเป็นที่นิยม และส่วนใหญ่จุดอ่อนนั้นพบโดยผู้ผลิต ผู้ใช้งาน หรือนักวิจัย ซึ่งเมื่อมองจากคะแนนจุดอ่อนที่ได้มา อาจประเมินได้ว่าผลิตภัณฑ์ใดมีจุดอ่อนและช่องโหว่ของเว็บเซอร์วิสผลิตภัณฑ์มากที่สุด จากจุดนี้เองสามารถบ่งบอกว่าคะแนนที่ได้มาแสดงถึงความนิยมในการใช้งาน



***หมายเหตุ รายชื่อผลิตภัณฑ์อ้างอิงจากตารางที่ 3.2

รูปที่ 4.4 คะแนนรวมจุดอ่อนของแต่ละผลิตภัณฑ์

รูปที่ 4.4 แสดงกราฟคะแนนจุดอ่อนจากการประเมินของแต่ละผลิตภัณฑ์ ผลที่ได้คือ Microsoft มีคะแนนสูงสูดเป็น 502 คะแนน อันดับที่ 2 คือ ผลิตภัณฑ์ BEA ได้ 421 คะแนน อันดับที่ 3 คือ ผลิตภัณฑ์ IBM ได้ 203 คะแนน และผลิตภัณฑ์ที่มีคะแนนจุดอ่อนต่ำที่สุด คือ ผลิตภัณฑ์ SUN ได้ 32 คะแนน โดยเมื่อพิจารณาจากคะแนนของแต่ละผลิตภัณฑ์ สรุปได้ว่าผลิตภัณฑ์ที่มีคะแนนสูงก็จะมีจุดอ่อนมากสุดตามไปด้วย แต่เมื่อพิจารณาจากรายชื่อของผลิตภัณฑ์ที่มีคะแนนสูง สังเกตได้ว่าผลิตภัณฑ์ดังกล่าวจะมีความนิยมในการใช้งาน เช่น Microsoft, IBM,BEA และ Oracle ซึ่งเป็นเพราะการใช้งานมากของผู้ใช้งานอาจทำให้ค้นพบจุดอ่อนต่างๆ ได้มากกกว่าผลิตภัณฑ์ที่ไม่ค่อยเป็นที่นิยม จึงมีจำนวนรายการซีวีอีมากกว่าและเป็นผลให้มีคะแนนจุดอ่อนมากตามไปด้วย



รูปที่ 4.5 เปรียบเทียบคะแนนจุดอ่อนแยกตามกลุ่มของประเภทเครื่องมือ

รูปที่ 4.5 กราฟแสดงการเปรียบเทียบคะแนนจุดอ่อนระหว่างเครื่องมือสนับสนุนการให้บริการ (Runtime Service Tools) และเครื่องมือช่วยการพัฒนา (Development Tools) ผลลัพธ์ที่ได้คือ เครื่องมือสนับสนุนการให้บริการมีคะแนนทั้งหมด 1175 คะแนนและเครื่องมือช่วยการพัฒนามีคะแนนทั้งหมด 256 คะแนน ซึ่งเมื่อพิจารณาคะแนนแล้วสามารถสรุปได้ว่าเครื่องมือสนับสนุนการให้บริการมีจุดอ่อนมากกว่า และส่งผลกระทบทำให้เกิดความเสียหายกับระบบเว็บเซอร์วิสได้มากกว่าเครื่องมือช่วยการพัฒนา

4.2 ผลลัพธ์แยกตามประเภทที่เกิดของจุดอ่อน

ตารางที่ 4.3 แสดงข้อมูลจำนวนรายการซีวีอีแยกตามประเภทจุดอ่อน ซึ่งได้แบ่งออกเป็น 9 ประเภท ดังต่อไปนี้

ตารางที่ 4.3 แสดงจำนวนรายการซีวีอีแยกตามประเภทจุดอ่อนและรายชื่อผลิตภัณฑ์

No	Location	BEA	IBM	Microsoft	Oracle	SAP	Sun	JBOSS	Total
1	Input Validation	6	2	29	15	4	2	1	**59**
2	Boundary Validation	15	7	33	5	2	3	1	**66**
3	Access Validation	16	12	34	11	2	1	0	**76**
4	Serialization	17	9	10	6	0	3	2	**47**
5	Configuration	17	2	13	14	1	0	2	**49**
6	Environmental	7	0	5	1	0	0	0	**13**
7	Design	19	7	15	33	0	0	1	**75**
8	Exception Handling	4	1	4	0	0	0	0	**9**
9	Other	2	2	2	16	0	0	0	**22**
	Total	**103**	**42**	**145**	**101**	**9**	**9**	**7**	**416**
*****หมายเหตุ รายชื่อผลิตภัณฑ์อ้างอิงจากตารางที่ 3.2**									

จากตารางจะเห็นว่าประเภทที่เกิดจุดอ่อนมากที่สุดคือ การตรวจสอบการเข้าถึง (Access Validation) จำนวน 76 รายการ อันดับที่ 2 คือ การออกแบบระบบ (Design) จำนวน 75 รายการ อันดับที่ 3 คือ ขอบเขตข้อมูล (Boundary Validation) จำนวน 66 รายการ และประเภทที่มีจุดอ่อนน้อยที่สุด คือ ชุดคำสั่งจัดการสิ่งผิดปกติ (Exception Handling) จำนวน 9 รายการ ซึ่งผลที่ได้ของประเภทจุดอ่อนสามารถแจกแจงได้ดังต่อไปนี้

จุดอ่อนประเภทความผิดพลาดการตรวจสอบข้อมูลนำเข้า (Input Validation) มากที่สุดคือ Microsoft จำนวน 29 รายการ อันดับที่ 2 คือ Oracle จำนวน 15 รายการ อันดับที่ 3 คือ BEA จำนวน 6 รายการ

จุดอ่อนประเภทความผิดพลาดขอบเขตข้อมูล (Boundary Validation) มากที่สุดคือ Microsoft จำนวน 33 รายการ อันดับที่ 2 คือ BEA จำนวน 15 รายการ อันดับที่ 3 คือ IBM จำนวน 7 รายการ และน้อยที่สุด คือ JBOSS จำนวน 1 รายการ

จุดอ่อนประเภทความผิดพลาดการตรวจสอบการเข้าถึง (Access Validation) มากที่สุดคือ Microsoft จำนวน 34 รายการ อันดับที่ 2 คือ BEA จำนวน 16 รายก่าร อันดับที่ 3 คือ IBM จำนวน 12 รายการ และเกิดจุดอ่อนประเภทนี้น้อยที่สุด คือ JBOSS จำนวน 0 รายการหรือไม่มีจุดอ่อนประเภทนี้เกิดขึ้นเลย

จุดอ่อนประเภทความผิดพลาดเหลื่อมล้ำการตรวจสอบสิทธิ (Serialization) มากที่สุดคือ BEA จำนวน 17 รายการ อันดับที่ 2 คือ Microsoft จำนวน 10 รายการ อันดับที่ 3 คือ IBM จำนวน 9 รายการ และผลิตภัณฑ์ที่เกิดจุดอ่อนประเภทนี้น้อยที่สุดคือ SAP จำนวน 0 รายการ

จุดอ่อนประเภทความผิดพลาดการปรับแต่งระบบ (Configuration) มากที่สุดคือ BEA จำนวน 17 รายการ อันดับที่ 2 คือ Oracle จำนวน 14 รายการ อันดับที่ 3 คือ Microsoft จำนวน 13 รายการ และผลิตภัณฑ์ที่เกิดจุดอ่อนประเภทนี้น้อยที่สุดคือ SUN จำนวน 0 รายการ

จุดอ่อนประเภทความผิดพลาดจากสภาพแวดล้อม (Environmental) มากที่สุดคือ BEA จำนวน 7 รายการ อันดับที่ 2 คือ Microsoft จำนวน 5 รายการ อันดับที่ 3 คือ Oracle จำนวน 1 รายการ และผลิตภัณฑ์ที่เกิดจุดอ่อนประเภทนี้น้อยที่สุดคือ IBM, SAP, SUN และ JBOSS จำนวน 0 รายการเท่ากัน

จุดอ่อนประเภทความผิดพลาดจากการออกแบบระบบ (Design) มากที่สุดคือ Oracle จำนวน 33 รายการ อันดับที่ 2 คือ BEA จำนวน 19 รายการ อันดับที่ 3 คือ Microsoft จำนวน 15 รายการ และผลิตภัณฑ์ที่เกิดจุดอ่อนประเภทนี้จำนวนน้อยที่สุดคือ SAP และ SUN จำนวน 0 รายการ

จุดอ่อนประเภทความผิดพลาดจากชุดคำสั่งจัดการสิ่งผิดปกติ (Exception Handling) มากที่สุดคือ BEA และ Microsoft จำนวน 4 รายการเท่ากัน อันดับที่ 2 คือ IBM จำนวน 1 รายการ และผลิตภัณฑ์ที่เกิดจุดอ่อนประเภทนี้น้อยที่สุดคือ Oracle, SAP, SUN และ JBOSS จำนวน 0 รายการเท่ากัน

และจุดอ่อนประเภทความผิดพลาดอื่นๆ (Other) มากที่สุดคือ Oracle จำนวน 16 รายการ อันดับที่ 2 คือ BEA, IBM และ Microsoft จำนวน 2 รายการเท่ากัน และผลิตภัณฑ์ที่มีจุดอ่อนประเภทนี้เกิดขึ้นน้อยที่สุดคือ SAP, SUN และ JBOSS จำนวน 0 รายการเท่ากัน

ตารางที่ 4.4 จำนวนจุดอ่อนแยกตามประเภทและกลุ่มเครื่องมือ

No	Location	Runtime Service Tools	Development Tools	Total
1	Input Validation	55	4	**59**
2	Boundary Validation	55	11	**66**
3	Access Validation	63	13	**76**
4	Serialization	35	12	**47**
5	Configuration	46	3	**49**
6	Environmental	13	0	**13**
7	Design	67	8	**75**
8	Exception Handling	8	1	**9**
9	Other	20	2	**22**
	Total	**362**	**54**	**416**

ตารางที่ 4.4 แสดงข้อมูลเปรียบเทียบประเภทของจุดอ่อนที่เกิดขึ้นระหว่างเครื่องมือสนับสนุนการให้บริการ (Runtime Service Tools) และเครื่องมือช่วยการพัฒนา (Development Tools) ซึ่งผลที่ได้จากการประเมินคือ

- การตรวจสอบข้อมูลนำเข้า (Input Validation) เครื่องมือสนับสนุนการให้บริการมีจำนวนจุดอ่อน 55 รายการมากกว่าเครื่องมือช่วยการพัฒนาที่มีจุดอ่อนจำนวน 4 รายการ
- ขอบเขตข้อมูล(Boundary Validation) เครื่องมือสนับสนุนการให้บริการมีจุดอ่อนจำนวน 55 รายการมากกว่าเครื่องมือช่วยการพัฒนาที่มีจุดอ่อนจำนวน 11 รายการ
- การตรวจสอบการเข้าถึง(Access Validation) เครื่องมือสนับสนุนการให้บริการมีจุดอ่อนจำนวน 63 รายการมากกว่าเครื่องมือช่วยการพัฒนาที่มีจุดอ่อนจำนวน 13 รายการ

- การเหลื่อมล้ำของการตรวจสอบสิทธิ (Serialization) เครื่องมือสนับสนุนการให้บริการมีจุดอ่อนจำนวน 35 รายการมากกว่าเครื่องมือช่วยการพัฒนาที่มีจุดอ่อนจำนวน 12 รายการ
- การปรับแต่งระบบ (Configuration) เครื่องมือสนับสนุนการให้บริการมีจุดอ่อนจำนวน 46 รายการมากกว่าเครื่องมือช่วยการพัฒนาที่มีจุดอ่อนจำนวน 3 รายการ
- สภาพแวดล้อม (Environmental) เครื่องมือสนับสนุนการให้บริการมีจุดอ่อนจำนวน 13 รายการมากกว่าเครื่องมือช่วยการพัฒนาที่มีจุดอ่อนจำนวน 0 รายการ
- การออกแบบระบบ (Design) เครื่องมือสนับสนุนการให้บริการมีจุดอ่อนจำนวน 67 รายการมากกว่าเครื่องมือช่วยการพัฒนาที่มีจุดอ่อนจำนวน 8 รายการ
- ชุดคำสั่งจัดการสิ่งผิดปกติ (Exception Handling) เครื่องมือสนับสนุนการให้บริการมีจุดอ่อนจำนวน 8 รายการมากกว่าเครื่องมือช่วยการพัฒนาที่มีจุดอ่อนจำนวน 1 รายการ
- อื่นๆ (Other) เครื่องมือสนับสนุนการให้บริการมีจุดอ่อนจำนวน 20 รายการมากกว่าเครื่องมือช่วยการพัฒนาที่มีจุดอ่อนจำนวน 2 รายการ

เมื่อพิจารณาจากผลลัพธ์ที่ได้ สรุปได้ว่าเครื่องมือสนับสนุนการให้บริการมีจุดอ่อนมากกว่าเครื่องมือช่วยการพัฒนาเมื่อแยกตามประเภทของจุดอ่อนทั้ง 9 ประเภท

4.3 ผลลัพธ์แยกตามจุดที่เกิดของจุดอ่อน

ข้อมูลจำนวนรายการซีวีอีแยกตามจุดที่เกิดจุดอ่อน ซึ่งจุดที่เกิดของจุดอ่อนสามารถก่อให้เกิดความเสียหายต่างๆ บนเว็บเซอร์วิสได้แตกต่างกัน ซึ่งจะได้แสดงข้อมูลดังต่อไปนี้

ตารางที่ 4.5 จำนวนจุดอ่อนแยกตามจุดที่เกิดจุดอ่อนแยกตามรายชื่อผลิตภัณฑ์

No	Location	BEA	IBM	Microsoft	Oracle	SAP	Sun	JBOSS	Total
1	System Initiation	13	2	10	40	0	0	0	65
2	Memory Management	15	5	31	9	2	2	1	65
3	Process Management	23	8	22	14	1	1	3	72
4	Device Management	0	0	1	0	0	0	0	1
5	File Management	4	11	32	10	1	1	0	59
6	Authentication	38	14	24	12	1	1	3	93
7	Support	2	1	2	0	0	0	0	5
8	Application	8	1	23	16	4	4	0	56
	SUM	103	42	145	101	9	9	7	416
***หมายเหตุ รายชื่อผลิตภัณฑ์อ้างอิงจากตารางที่ 3.2									

ตารางที่ 4.5 แสดงจำนวนรายการซีวีอีแยกตามจุดที่เกิดจุดอ่อนและรายชื่อผลิตภัณฑ์ ผลที่ได้ คือ รายการซีวีอีจำนวน 416 รายการ จุดที่เกิดจุดอ่อนส่วนใหญ่เกิดจากปัญหาการพิสูจน์ตัวตน(Authentication) โดยมีจำนวนสูงสุดเท่ากับ 93 รายการ อันดับที่ 2 คือ ปัญหาการจัดการโปรเซส (Process Management) มีจำนวนเท่ากับ 72 รายการ อันดับที่ 3 คือ ปัญหาการจัดการหน่วยความจำ (Memory Management) และ การเริ่มต้นระบบ (System Initiation) มีจำนวน 65 รายการเท่ากัน และจุดอ่อนที่เกิดขึ้นน้อยที่สุด คือ ปัญหาที่เกิดจากการจัดการอุปกรณ์ (Device Management) มีจำนวน 1 รายการ ซึ่งปัญหาที่เกิดโดยรวมจำเป็นต้องหาวิธีป้องกันเพื่อจะได้ไม่เกิดความเสียหายตามมา

จุดที่เกิดจุดอ่อนส่วนการเริ่มต้นระบบ (System Initiation) ผลที่ได้คือผลิตภัณฑ์ Oracle มีจุดอ่อนมากที่สุดจำนวน 40 รายการ อันดับที่ 2 คือ ผลิตภัณฑ์ BEA มีจำนวน 13 รายการ อันดับที่ 3 คือผลิตภัณฑ์ Microsoft มีจำนวน 10 รายการ และอันดับสุดท้ายมีจุดอ่อนในส่วนการเริ่มต้นระบบน้อยที่สุดคือผลิตภัณฑ์ SAP, SUN และ JBOSS จำนวน 0 รายการ

จุดอ่อนที่เกิดจากการจัดการหน่วยความจำ (Memory Management) ผลที่ได้คือ ผลิตภัณฑ์ที่มีจุดอ่อนส่วนการจัดการหน่วยความจำมากที่สุดคือ Microsoft จำนวน 31 รายการ อันดับที่ 2 คือ BEA จำนวน 15 รายการ อันดับที่ 3 คือ Oracle จำนวน 9 รายการ และอันดับสุดท้ายที่มีจุดอ่อนที่เกิดขึ้นในส่วนการจัดการหน่วยความจำน้อยที่สุดคือ JBOSS จำนวน 1 รายการ

จุดอ่อนที่เกิดจากส่วนการจัดการโปรเซส (Process Management) ผลที่ได้คือ ผลิตภัณฑ์ที่มีจุดอ่อนจากการจัดการโปรเซสมากที่สุดคือ BEA จำนวน 23 รายการ อันดับที่ 2 คือ Microsoft จำนวน 22 รายการ อันดับที่ 3 คือ Oracle จำนวน 14 รายการ และอันดับสุดท้ายที่มีจุดอ่อนที่เกิดขึ้นในส่วนการจัดการโปรเซสน้อยที่สุดคือ SAP และ SUN จำนวน 1 รายการ

จุดอ่อนที่เกิดจากส่วนการจัดการอุปกรณ์ (Device Management) ผลที่ได้คือ ผลิตภัณฑ์ที่มีจุดอ่อนในส่วนการจัดการอุปกรณ์มากที่สุด คือ Microsoft จำนวน 1 รายการ และผลิตภัณฑ์ที่ไม่มีจุดอ่อนที่เกิดจากการจัดการอุปกรณ์ คือ BEA, IBM, Oracle, SAP, SUN และ JBOSS จำนวน 0 รายการ นับเป็นจุดที่เกิดของจุดอ่อนที่ไม่ค่อยเกิดขึ้นในระบบเว็บเซอร์วิส

จุดอ่อนที่เกิดจากการจัดการแฟ้มข้อมูล (File Management) บนระบบเว็บเซอร์วิส ผลิตภัณฑ์ ผลที่ได้คือ ผลิตภัณฑ์ที่มีจุดอ่อนที่เกิดจากการจัดการแฟ้มข้อมูลมากที่สุด คือ Microsoft จำนวน 32 รายการ อันดับที่ 2 คือ IBM จำนวน 11 รายการ อันดับที่ 3 คือ Oracle จำนวน 10 รายการ และผลิตภัณฑ์ที่มีจุดอ่อนเกิดขึ้นที่ส่วนการจัดการแฟ้มข้อมูลน้อยที่สุดคือ JBOSS มีจำนวน 0 รายการ

จุดอ่อนที่เกิดจากส่วนการพิสูจน์ตัวตน (Authentication) บนเว็บเซอร์วิสผลิตภัณฑ์ ผลที่ได้คือ ผลิตภัณฑ์ที่มีจุดอ่อนจากการพิสูจน์ตัวตนมากที่สุดคือ BEA จำนวน 38 รายการ อันดับที่ 2 คือ Microsoft จำนวน 24 รายการ อันดับที่ 3 คือ IBM จำนวน 14 รายการ และผลิตภัณฑ์ที่มีจุดอ่อนเกิดขึ้นส่วนการพิสูจน์ตัวตนน้อยที่สุดคือ SAP และ SUN ซึ่งมีจำนวน 1 รายการ

จุดอ่อนที่เกิดจากโปรแกรมที่สนับสนุนการทำงานระบบปฏิบัติการ (Support) บนเว็บเซอร์วิสผลิตภัณฑ์ ผลที่ได้คือ ผลิตภัณฑ์ที่มีจุดอ่อนเกิดขึ้นจากโปรแกรมที่สนับสนุนการทำงานระบบปฏิบัติการมากที่สุดคือ BEA และ Microsoft จำนวน 2 รายการ อันดับที่ 2 คือ IBM จำนวน 1 รายการ และ ผลิตภัณฑ์ที่มีจุดอ่อนที่เกิดขึ้นที่ส่วนนี้น้อยที่สุดมี 4 ผลิตภัณฑ์คือ Oracle, SAP, SUN และ JBOSS มีจำนวน 0 รายการ

และจุดอ่อนที่เกิดจากส่วนโปรแกรมประยุกต์ (Application) ผลที่ได้คือ ผลิตภัณฑ์ที่มีจุดอ่อนเกิดขึ้นมากที่สุดที่ส่วนนี้คือ Microsoft จำนวน 23 รายการ อันดับที่ 2 คือ Oracle จำนวน

16 รายการ อันดับที่ 3 คือ BEA จำนวน 8 รายการ และผลิตภัณฑ์ที่มีจุดอ่อนเกิดขึ้นที่ส่วนนี้น้อยที่สุดคือ JBOSS จำนวน 0 รายการหรือไม่มีจุดอ่อนเลย

ตารางที่ 4.6 ข้อมูลจุดที่เกิดจุดอ่อนแยกตามประเภทของเครื่องมือ

No	Location	Runtime Service Tools	Development Tools	Total
1	System Initiation	63	2	**65**
2	Memory Management	57	8	**65**
3	Process Management	62	10	**72**
4	Device Management	1	0	**1**
5	File Management	46	13	**59**
6	Authentication	78	15	**93**
7	Support	4	1	**5**
8	Application	51	5	**56**
	Total	**362**	**54**	**416**

ตารางที่ 4.6 นำเสนอข้อมูลจุดที่เกิดของจุดอ่อนโดยแยกออกเป็นเครื่องมือสนับสนุนการให้บริการ และเครื่องมือช่วยการพัฒนา ผลที่ได้แยกตามจุดที่เกิดดังนี้

- ส่วนการเริ่มต้นระบบ (System Initiation) เครื่องมือสนับสนุนการให้บริการมีจำนวน 63 รายการ และเครื่องมือช่วยการพัฒนามีจำนวน 2 รายการ ดังนั้นเครื่องมือสนับสนุนการให้บริการมีจำนวนจุดอ่อนที่เกิดจากจุดนี้มีจำนวนมากกว่าเครื่องมือช่วยการพัฒนา
- ส่วนการจัดการหน่วยความจำ (Memory Management) เครื่องมือสนับสนุนการให้บริการมีจำนวน 57 รายการ และเครื่องมือช่วยการพัฒนามีจำนวน 8 รายการ ดังนั้นเครื่องมือสนับสนุนการให้บริการมีจำนวนจุดอ่อนที่เกิดจากจุดนี้เป็นจำนวนมากกว่าเครื่องมือช่วยการพัฒนา
- ส่วนการจัดการโปรเซส (Process Management) เครื่องมือสนับสนุนการให้บริการมีจำนวน 62 รายการ และเครื่องมือช่วยการพัฒนามีจำนวน 10 รายการ ดังนั้นเครื่องมือสนับสนุนการให้บริการมีจำนวนจุดอ่อนที่เกิดจากจุดนี้เป็นจำนวนมากกว่าเครื่องมือช่วยการพัฒนา
- ส่วนการจัดการอุปกรณ์ (Device Management) เครื่องมือสนับสนุนการให้บริการมีจำนวน 1 รายการ และเครื่องมือช่วยการพัฒนามีจำนวน 0 รายการ

ดังนั้นเครื่องมือสนับสนุนการให้บริการมีจำนวนจุดอ่อนที่เกิดจากจุดนี้เป็นจำนวนมากกว่าเครื่องมือช่วยการพัฒนา

- ส่วนการจัดการแฟ้มข้อมูล (File Management) เครื่องมือสนับสนุนการให้บริการมีจำนวน 46 รายการ และเครื่องมือช่วยการพัฒนามีจำนวน 13 รายการ ดังนั้นเครื่องมือสนับสนุนการให้บริการมีจำนวนจุดอ่อนที่เกิดจากจุดนี้เป็นจำนวนมากกว่าเครื่องมือช่วยการพัฒนา
- ส่วนการพิสูจน์ตัวตน (Authentication) เครื่องมือสนับสนุนการให้บริการมีจำนวน 78 รายการ และเครื่องมือช่วยการพัฒนามีจำนวน 15 รายการ ดังนั้นเครื่องมือสนับสนุนการให้บริการมีจำนวนจุดอ่อนที่เกิดจากจุดนี้เป็นจำนวนมากกว่าเครื่องมือช่วยการพัฒนา
- ส่วนโปรแกรมที่สนับสนุนการทำงานระบบปฏิบัติการ (Support) เครื่องมือสนับสนุนการให้บริการมีจำนวน 4 รายการ และเครื่องมือช่วยการพัฒนามีจำนวน 1 รายการ ดังนั้นเครื่องมือสนับสนุนการให้บริการมีจำนวนจุดอ่อนที่เกิดจากจุดนี้เป็นจำนวนมากกว่าเครื่องมือช่วยการพัฒนา
- ส่วนโปรแกรมประยุกต์ (Application) เครื่องมือสนับสนุนการให้บริการมีจำนวน 51 รายการ และเครื่องมือช่วยการพัฒนามีจำนวน 5 รายการ ดังนั้นเครื่องมือสนับสนุนการให้บริการมีจำนวนจุดอ่อนที่เกิดจากจุดนี้เป็นจำนวนมากกว่าเครื่องมือช่วยการพัฒนา

เมื่อพิจารณาจากข้อมูลที่ได้จากการประเมินแล้วสามารถเปรียบเทียบจุดที่เกิดของจุดอ่อนบนเว็บเซอร์วิสผลิตภัณฑ์ระหว่างเครื่องมือสนับสนุนการให้บริการและเครื่องมือช่วยการพัฒนา ซึ่งเมื่อสรุปตามคะแนนที่ได้จากการประเมินพบว่าเครื่องมือสนับสนุนการให้บริการจุดอ่อนที่สร้างความเสียหายได้มากกว่าเครื่องมือช่วยการพัฒนา

4.4 ผลลัพธ์แยกตามลักษณะความเสียหาย

ส่วนนี้นำเสนอข้อมูลของคะแนนจุดอ่อนที่แยกออกตามความเสียหายที่จุดอ่อนก่อให้เกิดความเสียหาย ทั้งในด้านการรักษาความลับ การสูญเสียบูรณภาพ และเสียความสภาพพร้อมใช้งาน โดยแยกเป็นรายชื่อเว็บเซอร์วิสผลิตภัณฑ์และประเภทของเครื่องมือ โดยมีรายละเอียดดังต่อไปนี้

ตารางที่ 4.7 คะแนนจุดอ่อนของแต่ละผลิตภัณฑ์แยกตามความเสียหายที่ส่งผลกระทบ

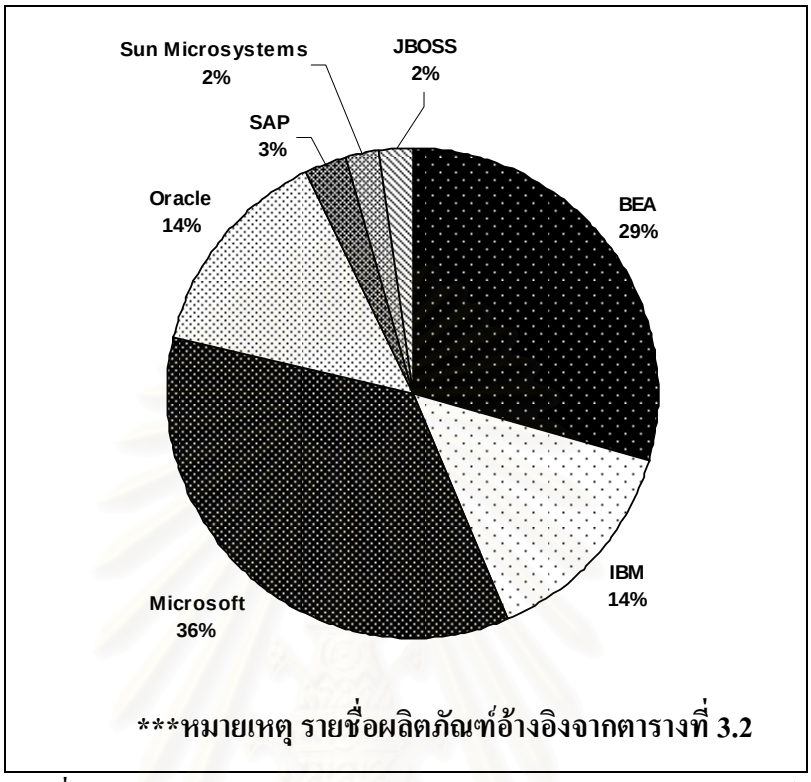
ผลิตภัณฑ์	การสูญเสียความลับ	การเสียบูรณภาพ	การเสียสภาพพร้อมใช้งาน	รวม
BEA	203	107	111	421
IBM	102	58	43	203
Microsoft	196	88	218	502
Oracle	129	20	53	202
SAP	14	7	17	38
Sun	11	6	15	32
JBOSS	13	11	9	33
รวมทั้งหมด	668	297	466	1431
*****หมายเหตุ รายชื่อผลิตภัณฑ์อ้างอิงจากตารางที่ 3.2**				

ตารางที่ 4.7 แสดงข้อมูลคะแนนโดยแยกออกตามความเสียหายทั้ง 3 รูปแบบ คือ การสูญเสียความลับ การสูญเสียบูรณภาพ และการสูญเสียสภาพพร้อมใช้งาน ซึ่งผลลัพธ์ที่ได้

- ความเสียหายด้านการสูญเสียความลับ ผลิตภัณฑ์ที่มีคะแนนจุดอ่อนสูงที่สุดในด้านการสูญเสียความลับ คือ BEA มี 203 คะแนน และผลิตภัณฑ์ SUN มีคะแนนจุดอ่อนในด้านการสูญเสียความลับน้อยที่สุด คือ 11 คะแนน
- ความเสียหายด้านการสูญเสียบูรณภาพ ผลิตภัณฑ์ที่มีคะแนนจุดอ่อนสูงที่สุดในด้านการสูญเสียบูรณภาพ คือ BEA มี 107 คะแนน และผลิตภัณฑ์ SUN มีคะแนนจุดอ่อนในด้านการสูญเสียบูรณภาพน้อยที่สุด คือ 6 คะแนน
- ความเสียหายด้านการสูญเสียสภาพพร้อมใช้งาน ผลิตภัณฑ์ที่มีคะแนนจุดอ่อนสูงที่สุดในด้านการสูญเสียสภาพพร้อมใช้งานคือ Microsoft มี 218 คะแนน และผลิตภัณฑ์ JBOSS มีคะแนนจุดอ่อนในด้านการสูญเสียสภาพพร้อมใช้งานน้อยที่สุด คือ 9 คะแนน

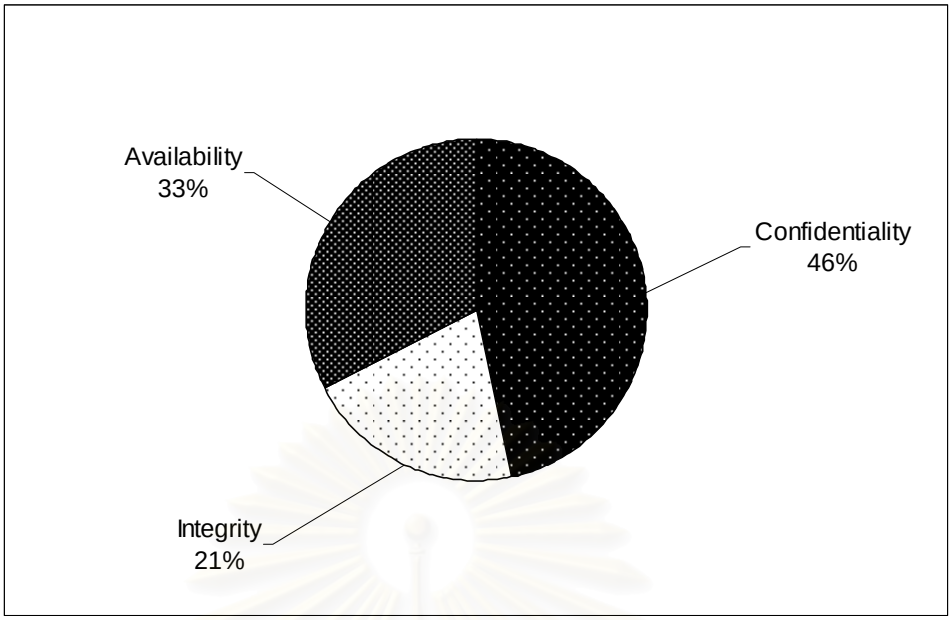
ในส่วนของคะแนนรวมทั้งหมดของความเสียหายทุกด้าน ผลิตภัณฑ์ที่มีคะแนนความเสียหายของจุดอ่อนสูงที่สุดคือ Microsoft จำนวน 502 คะแนน คะแนนสูงเป็นลำดับที่ 2 คือ ผลิตภัณฑ์ BEA จำนวน 421 คะแนน คะแนนสูงเป็นลำดับที่ 3 IBM จำนวน 203 คะแนน และผลิตภัณฑ์ที่มีคะแนนจุดอ่อนที่ต่ำที่สุด คือ ผลิตภัณฑ์ SUN จำนวน 32 ซึ่งเมื่อพิจารณาจากคะแนนที่ได้มาจากการประเมินผลแล้ว ปรากฏว่าผลิตภัณฑ์ที่เป็นที่นิยมในการใช้งานจะมีคะแนนจุดอ่อนที่

เกิดจากการโจมตีเว็บเซอร์วิสในปริมาณที่สูง เมื่อเปรียบเทียบกับผลิตภัณฑ์ที่มีผู้ใช้งานไม่ค่อยเป็นที่นิยม



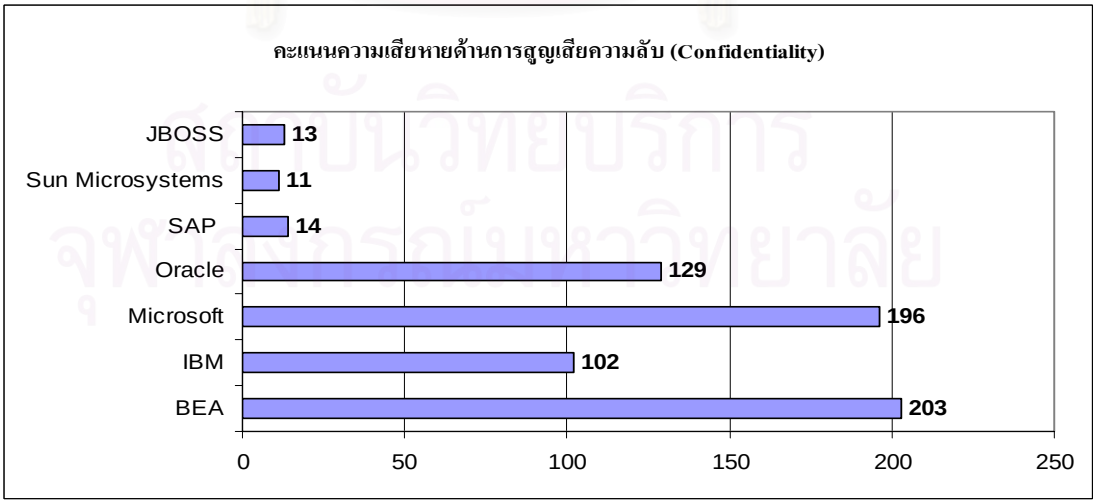
รูปที่ 4.6 กราฟเปรียบเทียบคะแนนความเสียหายจำแนกตามผลิตภัณฑ์

รูปที่ 4.6 แสดงกราฟเปรียบเทียบคะแนนความเสียหายที่จำแนกออกตามผลิตภัณฑ์ ซึ่งผลลัพธ์ที่ได้คือ Microsoft มีอัตราส่วนเป็นจำนวนที่มากที่สุด คือ 36 เปอร์เซนต์ และผลิตภัณฑ์ที่มีคะแนนเป็นอัตราส่วนน้อยที่สุดคือ SUN และ JBOSS คือ 2 เปอร์เซนต์



รูปที่ 4.7 เปรียบเทียบคะแนนจุดอ่อนแยกตามความเสียหายทั้งหมด

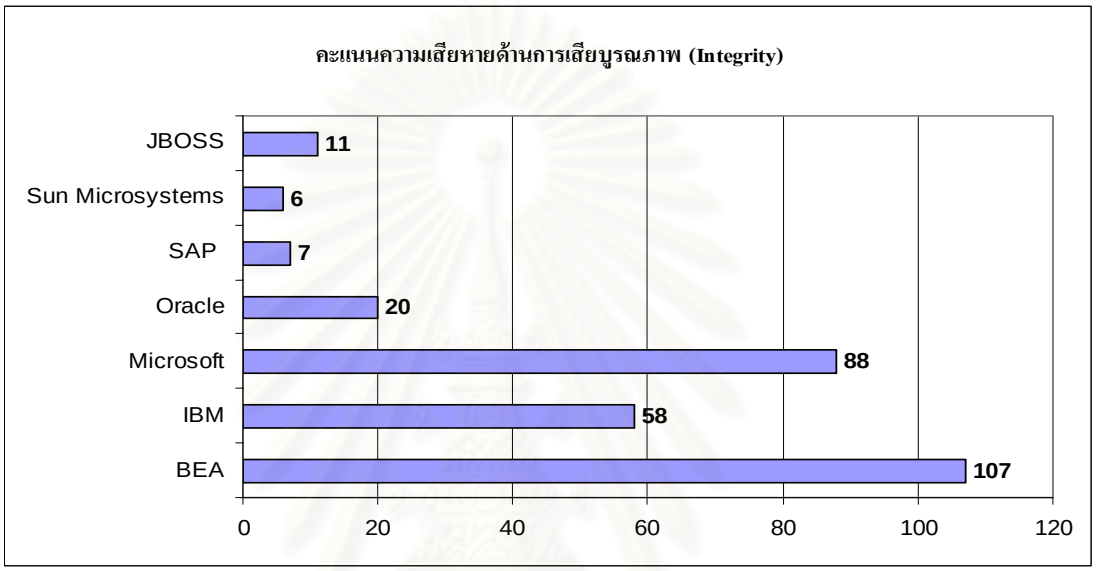
รูปที่ 4.7 แสดงอัตราส่วนของคะแนนจุดอ่อนแยกตามประเภทของความเสียหายทั้ง 3 ประเภทคือ การสูญเสียความลับ การสูญเสียบูรณภาพ การสูญเสียสภาพพร้อมใช้งาน ซึ่งผลที่ได้คือ ความเสียหายด้านการสูญเสียความลับมีคะแนนเป็นอัตราส่วนที่สูงที่สุด จำนวน 46 เปอร์เซนต์ อัตราส่วนคะแนนที่สูงเป็นลำดับที่ 2 คือ ความเสียหายด้านการสูญเสียสภาพพร้อมใช้งานมีอัตราส่วนจำนวน 33 เปอร์เซนต์ และความเสียหายด้านการสูญเสียบูรณภาพมีอัตราส่วนคะแนนจุดอ่อนน้อยที่สุดคือ 21 เปอร์เซนต์



***หมายเหตุ รายชื่อผลิตภัณฑ์อ้างอิงจากตารางที่ 3.2

รูปที่ 4.8 เปรียบเทียบคะแนนความเสียหายด้านการรักษาความลับ

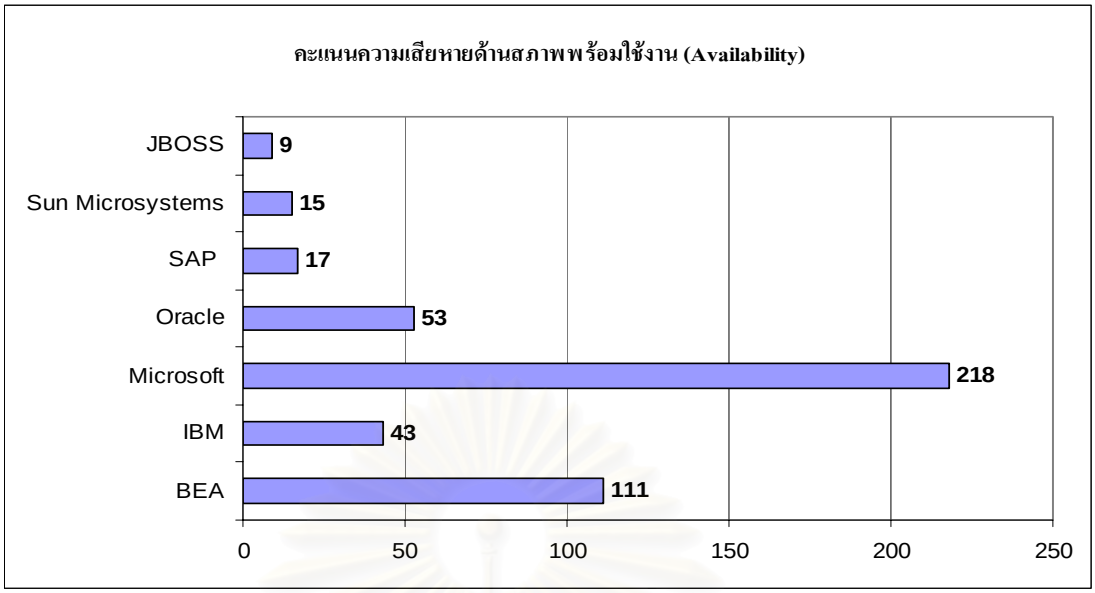
รูปที่ 4.8 แสดงกราฟเพื่อใช้เปรียบเทียบคะแนนความเสียหายด้านการสูญเสียความลับของแต่ละผลิตภัณฑ์ ซึ่งผลที่ได้คือ ผลิตภัณฑ์ BEA ได้รับคะแนนสูงสุดจากความเสียหายด้านการสูญเสียความลับเป็นจำนวน 203 คะแนน อันดับที่ 2 คือ Microsoft จำนวน 196 คะแนน อันดับที่ 3 คือ Oracle จำนวน 129 คะแนน และผลิตภัณฑ์ที่ได้มีคะแนนความเสียหายน้อยที่สุดคือ SUN ซึ่งมีคะแนนจำนวน 11 คะแนน



***หมายเหตุ รายชื่อผลิตภัณฑ์อ้างอิงจากตารางที่ 3.2

รูปที่ 4.9 เปรียบเทียบคะแนนความเสียหายด้านการสูญเสียบูรณภาพ

รูปที่ 4.9 แสดงกราฟเพื่อใช้เปรียบเทียบคะแนนความเสียหายด้านการเสียบูรณภาพของแต่ละผลิตภัณฑ์ ซึ่งผลที่ได้คือ ผลิตภัณฑ์ BEA ได้รับคะแนนสูงสุดจากความเสียหายด้านการเสียบูรณภาพเป็นจำนวน 107 คะแนน อันดับที่ 2 คือ Microsoft จำนวน 88 คะแนน อันดับที่ 3 คือ IBM จำนวน 58 คะแนน และผลิตภัณฑ์ที่ได้มีคะแนนความเสียหายน้อยที่สุดคือ SUN ซึ่งมีคะแนนจำนวน 6 คะแนน



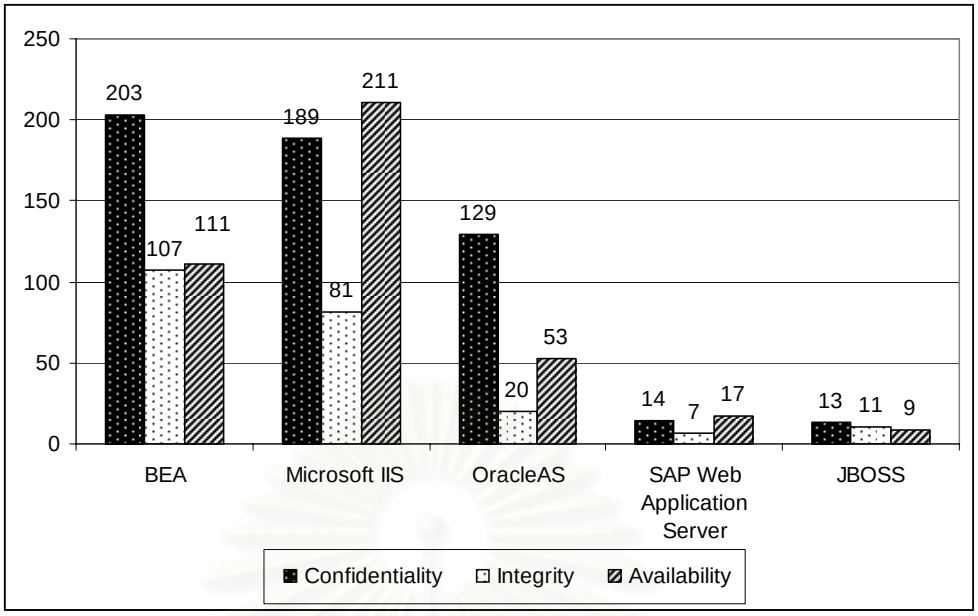
***หมายเหตุ รายชื่อผลิตภัณฑ์อ้างอิงจากตารางที่ 3.2

รูปที่ 4.10 เปรียบเทียบคะแนนความเสียหายด้านสภาพพร้อมใช้งาน

รูปที่ 4.10 แสดงกราฟเพื่อใช้เปรียบเทียบคะแนนความเสียหายด้านการสูญเสียสภาพพร้อมใช้งานของแต่ละผลิตภัณฑ์ ซึ่งผลที่ได้คือ ผลิตภัณฑ์ Microsoft ได้รับคะแนนสูงสุดจากความเสียหายด้านการสูญเสียสภาพพร้อมใช้งานเป็นจำนวน 218 คะแนน อันดับที่ 2 คือ BEA จำนวน 111 คะแนน อันดับที่ 3 คือ Oracle จำนวน 53 คะแนน และผลิตภัณฑ์ที่ได้มีคะแนนความเสียหายน้อยที่สุดคือ JBOSS ซึ่งมีคะแนนจำนวน 9 คะแนน

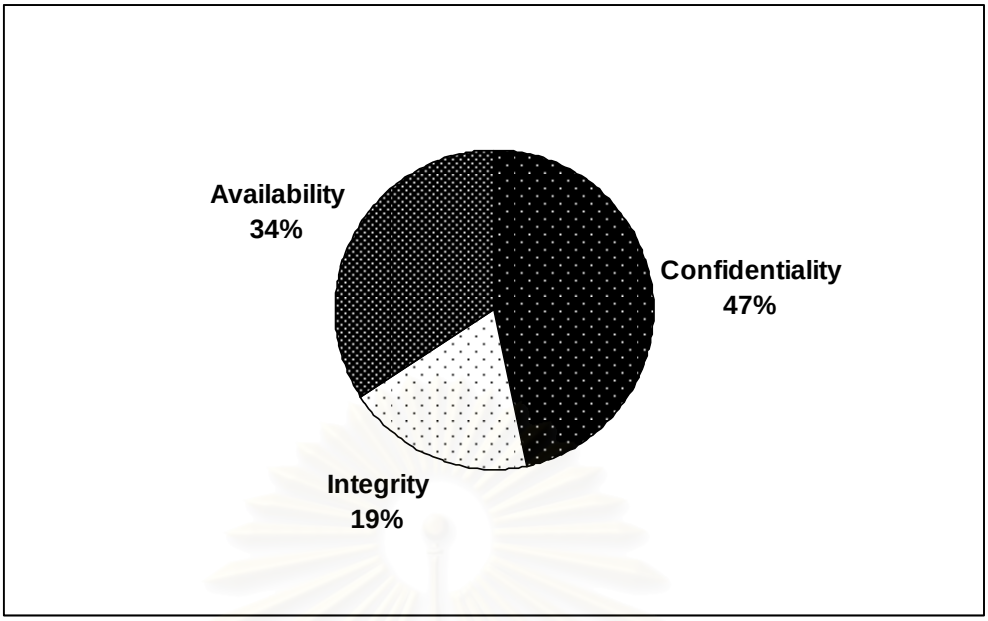
ตารางที่ 4.8 คะแนนจุดอ่อนแยกตามเสียหายของเครื่องมือสนับสนุนการให้บริการ

RUNTIME SERVICE TOOLS				
Product	Confidentiality	Integrity	Availability	SUM
BEA	203	107	111	421
Microsoft IIS	189	81	211	481
OracleAS	129	20	53	202
SAP Web Application Server	14	7	17	38
JBOSS	13	11	9	33
Total	548	226	401	1175



รูปที่ 4.11 คะแนนจุดอ่อนของความเสียหายแต่ละประเภทของเครื่องมือช่วยสนับสนุนการให้บริการ

ตารางที่ 4.8 และรูปที่ 4.11 เปรียบเทียบคะแนนจุดอ่อนของเครื่องมือสนับสนุนการให้บริการของแต่ละผลิตภัณฑ์และเครื่องมือ ผลที่ได้คือ เครื่องมือที่มีคะแนนจุดอ่อนมากที่สุดแยกแต่ละด้านของความเสียหายมีดังนี้ ความเสียหายด้านการสูญเสียความลับ คือ BEA Web logic จำนวน 203 คะแนน ด้านการสูญเสียบูรณภาพ คือ BEA จำนวน 107 คะแนน และความสูญเสียด้านสภาพพร้อมใช้งาน คือ Microsoft IIS จำนวน 211 คะแนน ซึ่งผลลัพธ์ของคะแนนที่ได้จากการประเมินแสดงให้เห็นถึงความเสียหายที่เกิดขึ้นของแต่ละเครื่องมือ ว่ามีความเสี่ยงต่อจุดอ่อนที่อาจเกิดขึ้นได้มากน้อยเพียงใดในแต่ละด้านของความเสียหาย

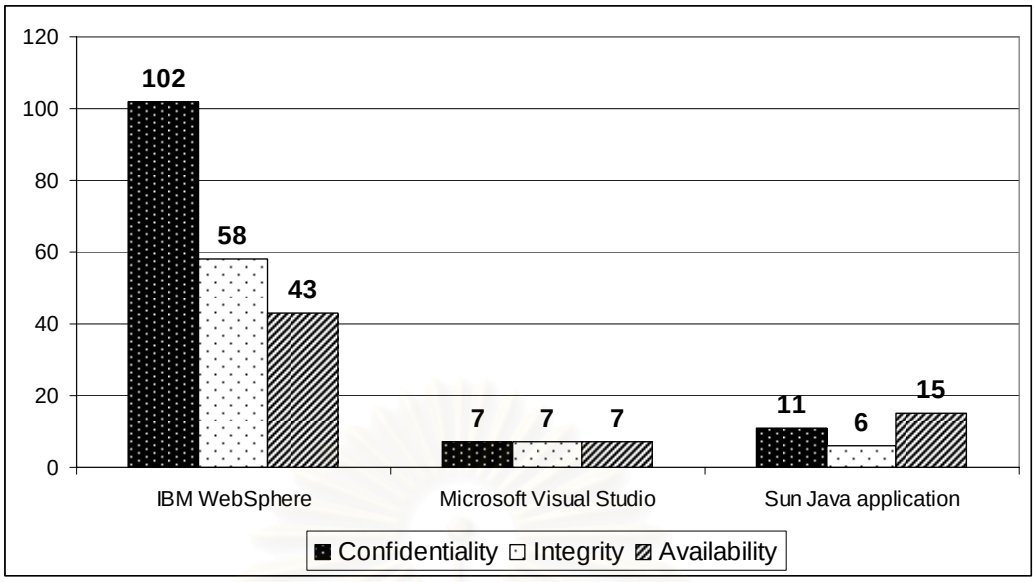


รูปที่ 4.12 สัดส่วนความเสียหายของเครื่องมือสนับสนุนการให้บริการ

รูปที่ 4.12 แสดงข้อมูลของอัตราส่วนของผลกระทบที่เกิดขึ้นจากจุดอ่อนทั้ง 3 ด้าน ของเครื่องมือสนับสนุนการให้บริการเว็บเซอร์วิส ซึ่งผลที่ได้เรียงลำดับจากมากไปน้อย คือ อัตราส่วนของความเสียหายด้านการสูญเสียความลับเท่ากับ 47 เปอร์เซ็นต์ รองลงมาคือความเสียหายด้านสภาพพร้อมใช้งานเท่ากับ 34 เปอร์เซ็นต์ และลำดับสุดท้ายคือ ความเสียหายด้านการสูญเสียบูณรภาพจำนวน 19 เปอร์เซ็นต์ ซึ่งคะแนนที่นำมาเปรียบเทียบเป็นอัตราส่วนนำมาจากตารางที่ 4.8

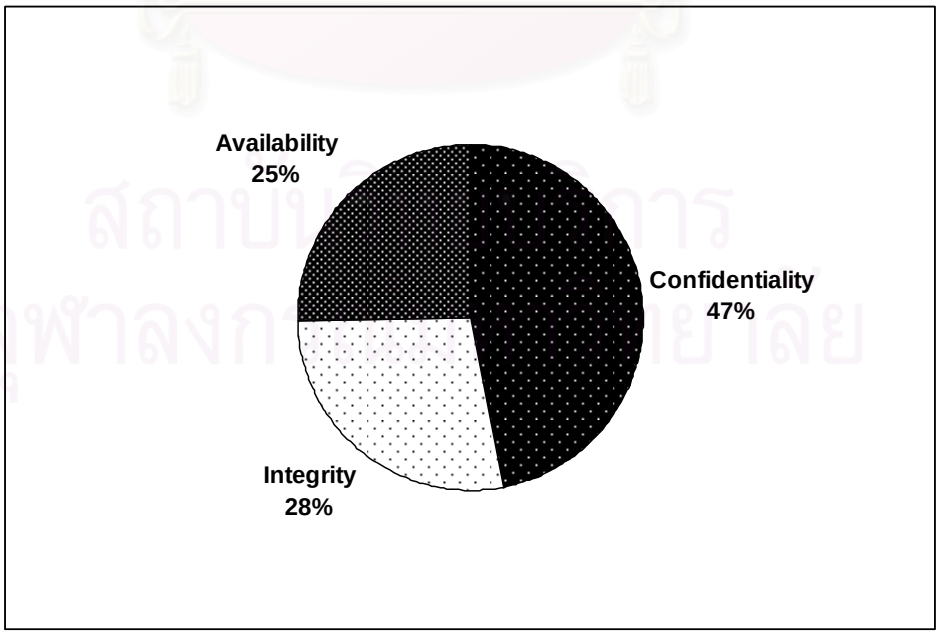
ตารางที่ 4.9 คะแนนจุดอ่อนแยกตามความเสียหายของเครื่องมือช่วยการพัฒนา

DEVELOPMENT TOOLS				
Product	**Confidentiality**	**Integrity**	**Availability**	**SUM**
IBM WebSphere	102	58	43	203
Microsoft Visual Studio	7	7	7	21
Sun Java application	11	6	15	32
Total	**120**	**71**	**65**	**256**



รูปที่ 4.13 คะแนนจุดอ่อนของความเสียหายแต่ละประเภทของเครื่องมือช่วยการพัฒนา

ตารางที่ 4.9 และ รูปที่ 4.13 แสดงข้อมูลเปรียบเทียบคะแนนที่ได้จากการประเมินของเครื่องมือช่วยการพัฒนาเว็บเซอร์วิส ผลที่ได้คือ ผลิตภัณฑ์ที่ได้รับคะแนนความเสียหายด้านการสูญเสียความลับมากที่สุดคือ IBM WebSphere จำนวน 102 คะแนน ผลิตภัณฑ์ที่ได้รับคะแนนความเสียหายด้านการสูญเสียบูรณภาพมากที่สุดคือ IBM WebSphere จำนวน 58 คะแนน และผลิตภัณฑ์ที่ได้รับคะแนนความเสียหายด้านการสูญเสียสภาพพร้อมใช้งานมากที่สุดคือ IBM WebSphere จำนวน 43 คะแนน

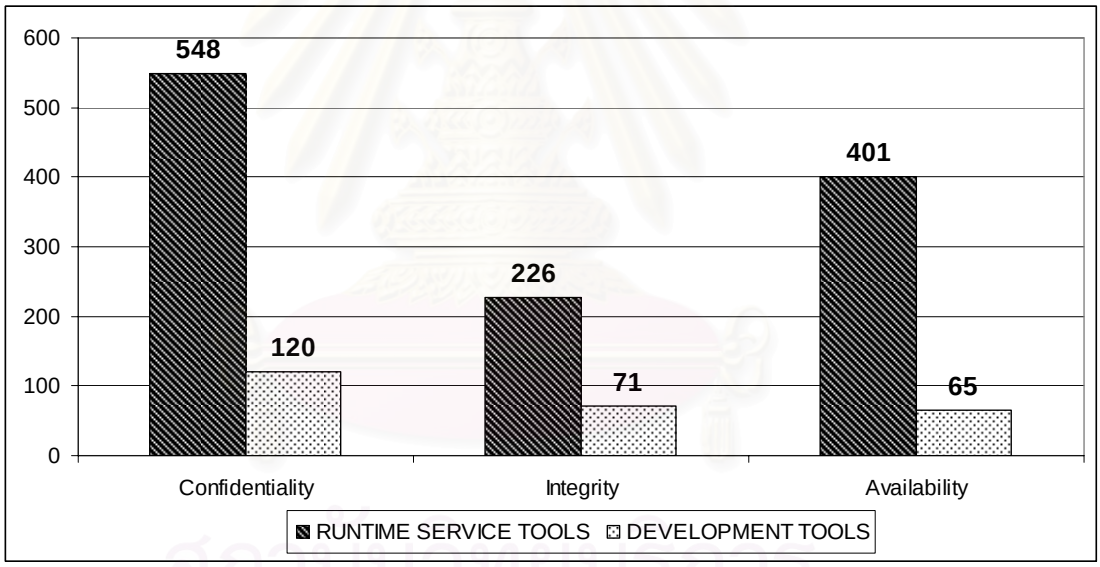


รูปที่ 4.14 สัดส่วนคะแนนความเสียหายของเครื่องมือช่วยการพัฒนา

รูปที่ 4.14 แสดงข้อมูลของอัตราส่วนของผลกระทบที่เกิดขึ้นจากจุดอ่อนทั้ง 3 ด้านของเครื่องมือช่วยการพัฒนาเว็บเซอร์วิส ซึ่งผลที่ได้เรียงลำดับจากมากไปน้อย คือ อัตราส่วนของความเสียหายด้านการสูญเสียความลับเท่ากับ 47 เปอร์เซ็นต์ รองลงมาคือความเสียหายด้านการสูญเสียบูณรภาพเท่ากับ 28 เปอร์เซ็นต์ และลำดับสุดท้ายคือ ความเสียหายด้านสภาพพร้อมใช้งานจำนวน 25 เปอร์เซ็นต์ ซึ่งคะแนนที่นำมาเปรียบเทียบเป็นอัตราส่วนนำมาจากตารางที่ 4.9

ตารางที่ 4.10 คะแนนของเครื่องมือแต่ละเครื่องมือแยกตามความเสียหาย

Product	Confidentiality	Integrity	Availability	SUM
Runtime Service Tools	548	226	401	1175
Development Tools	120	71	65	256
Total	**668**	**297**	**466**	**1431**



รูปที่ 4.15 คะแนนความเสียหายแต่ละด้านแยกตามเครื่องมือ

จากตารางที่ 4.10 และรูปที่ 4.15 แสดงข้อมูลเปรียบเทียบคะแนนจุดอ่อนของแต่ละเครื่องมือแยกตามความเสียหายทั้ง 3 ประเภท ผลลัพธ์ที่ได้คือ

- ความเสียหายด้านการสูญเสียความลับ
  เครื่องมือสนับสนุนการให้บริการมี 548 คะแนนและเครื่องมือช่วยการพัฒนา 120 คะแนน

- ความเสียหายด้านการสูญเสียบูรณภาพ
  เครื่องมือสนับสนุนการให้บริการมี 226 คะแนนและเครื่องมือช่วยการพัฒนา มี 71 คะแนน
- ความเสียหายด้านการเสียสภาพพร้อมใช้งาน
  เครื่องมือสนับสนุนการให้บริการมี 401 คะแนนและเครื่องมือช่วยการพัฒนา มี 65 คะแนน

ซึ่งเมื่อพิจารณาจากความเสียหายแต่ละประเภทจะพบว่าในแต่ละด้านเครื่องมือสนับสนุนการให้บริการจะมีคะแนนมากกว่าเครื่องมือช่วยการพัฒนา เนื่องจากสาเหตุที่เครื่องมือสนับสนุนการให้บริการมีรายการซีวีอีมากกว่าเครื่องมือช่วยการพัฒนา แต่เมื่อวิเคราะห์จากคะแนนของแต่ละรายการซีวีอีที่ได้จากการประเมินแล้ว สรุปว่าแต่ละรายการซีวีอีของเครื่องมือสนับสนุนการให้บริการจะมีคะแนนประเมินอยู่ในระดับคะแนนที่สูงกว่าเครื่องมือช่วยการพัฒนา

ในบทที่ 4 ที่ผ่านมาเป็นข้อมูลผลการวิจัย โดยผลที่ได้ ประกอบด้วยผลลัพธ์แยกตามรายชื่อผลิตภัณฑ์ ประเภทที่เกิดของจุดอ่อน จุดที่เกิดของจุดอ่อน และประเภทของความเสียหาย และในบทที่ 5 จะทำการสรุปผลการวิจัยที่ได้ และเสนอข้อเสนอแนะที่เกี่ยวข้องกับงานวิจัยต่อไป

บทที่ 5
สรุปผลการวิจัย

บทที่แล้วเป็นการประเมินจุดอ่อนที่เกิดขึ้นบนระบบเว็บเซอร์วิสสำหรับผลิตภัณฑ์เว็บเซอร์วิสทั้ง 2 กลุ่ม คือ เครื่องมือสนับสนุนการให้บริการและเครื่องมือช่วยการพัฒนา ซึ่งการทำงานในงานวิจัยนี้เน้นไปที่การคัดกรอง คัดเลือกรายการซีวีอีที่เกี่ยวข้องกับรายการจุดอ่อน เพื่อนำไปประเมินคะแนนของแต่ละผลิตภัณฑ์ โดยสามารถสรุปผลไว้ในบทนี้ได้ดังนี้

5.1 ผลจากการวิจัย

5.1.1 การคัดเลือกรายการซีวีอี

1. รายการซีวีอีเวอร์ชั่น 20061101 มีข้อมูลทั้งหมด 21,516 รายการ โดยคัดกรองให้เหลือเฉพาะรายการที่เกี่ยวข้องกับจุดอ่อนของผลิตภัณฑ์เว็บเซอร์วิสเป็นจำนวน 416 รายการ แยกเป็นเครื่องมือช่วยการพัฒนาจำนวน 54 รายการ และเครื่องมือสนับสนุนการให้บริการ 362 รายการ

2. การคัดเลือกรายชื่อผลิตภัณฑ์ที่มีอยู่ในรายการซีวีอี ขั้นตอนแรกได้ทำการคัดเลือกรายชื่อผลิตภัณฑ์เพื่อนำมาใช้ในงานวิจัยจำนวน 10 ตัว และมีเครื่องมือจำนวน 20 ตัว โดยแบ่งเป็นเครื่องมือช่วยการพัฒนาจำนวน 6 ตัวและเครื่องมือสนับสนุนการให้บริการจำนวน 13 ตัว และเมื่อนำรายชื่อผลิตภัณฑ์และเครื่องมือดังกล่าวมาทำการค้นหาในซีวีอี ปรากฏว่ารายชื่อผลิตภัณฑ์ที่ค้นพบในซีวีอีมีเพียงแค่ 7 ตัว และมีเครื่องมือจำนวน 8 ตัว แบ่งเป็นเครื่องมือช่วยการพัฒนาจำนวน 2 ตัวและเครื่องมือสนับสนุนการให้บริการจำนวน 6 ตัว ดังข้อมูลตารางที่ 3.2

3. วิธีการคัดกรองจุดอ่อนของผลิตภัณฑ์ที่เกี่ยวข้องกับเว็บเซอร์วิสในรายการซีวีอีมีเงื่อนไขดังนี้ รายละเอียดจุดอ่อนต้องเกี่ยวข้องกับองค์ประกอบเว็บเซอร์วิส และจุดอ่อนมีรูปแบบการถูกโจมตีที่เป็นรูปแบบการโจมตีเว็บเซอร์วิส ดังหัวข้อที่ 3.1.2

5.1.2 การหาวิธีคิดคะแนน

1. รูปแบบการประเมินคะแนน ใช้ตามหลักงานวิจัยของรัศมีทิพย์ วิตา ซึ่งจำแนกคะแนนตามประเภทของความเสียหาย 3 ประเภทคือ การสูญเสียความลับ การสูญเสียบูรณภาพ และการสูญเสียสภาพพร้อมใช้งาน

2. กำหนดให้มีค่าคะแนนความเสียหายของแต่ละจุดอ่อนออกเป็น 4 ระดับคือ สูง เท่ากับ 3 คะแนน ปานกลางเท่ากับ 2 ต่ำเท่ากับ 1 คะแนน และไม่มีผลกระทบ เท่ากับ 0
3. จุดที่เกิดและประเภทของจุดอ่อนใช้วิธีนับจำนวนของรายการจุดอ่อน ซึ่งจุดอ่อนแต่ละรายการจะกำหนดให้มีจุดที่เกิดและประเภทของจุดอ่อนอย่างละ 1 เท่านั้น
4. การคำนวณคะแนนจุดอ่อนของแต่ละผลิตภัณฑ์ ใช้วิธีนำคะแนนของแต่ละรายการมาบวกหาผลรวมทั้งหมด แล้วนำคะแนนของแต่ละผลิตภัณฑ์มาเปรียบเทียบจากผลของคะแนนรวม

5.1.3 ผลคะแนน

1. ผลิตภัณฑ์ที่พบรายการจุดอ่อนซีวีอีมากที่สุดคือ 5 อันดับแรก คือผลิตภัณฑ์ของ Microsoft จำนวน 145 รายการ BEA จำนวน 103 รายการ Oracle จำนวน 101รายการ IBM จำนวน 42 รายการและ JBOSS จำนวน 7 รายการ

2. เครื่องมือสนับสนุนการให้บริการมีคะแนนจุดอ่อนและความเสี่ยงต่อการโจมตีมากกว่าเครื่องมือช่วยการพัฒนา ซึ่งเครื่องมือสนับสนุนการให้บริการเป็นเครื่องมือที่ผู้ไม่หวังดีใช้ในการโจมตีมากกว่าเครื่องมือช่วยการพัฒนา

3. คะแนนจุดอ่อนของแต่ละผลิตภัณฑ์ที่มีคะแนนสูงสุดคือ Microsoft จำนวน 502 คะแนน และคะแนนต่ำสุดคือ SUN Microsystems จำนวน 32 คะแนน ซึ่งหมายความว่าผลิตภัณฑ์ของ Microsoft เกิดผลกระทบของความเสียหายในการใช้งานมากกว่าผลิตภัณฑ์อื่นๆ และผลิตภัณฑ์ของ SUN Microsystems มีผลกระทบจากความเสียหายเกิดขึ้นน้อยที่สุดกว่าผลิตภัณฑ์อื่น ๆ

4. ประเภทที่เกิดจุดอ่อนที่พบมากที่สุดคือ ความผิดพลาดของการตรวจสอบการเข้าถึง มีจำนวน 76 รายการ และผลิตภัณฑ์ที่มีจุดอ่อนประเภทนี้มากที่สุดคือไมโครซอฟต์ไอไอเอส ซึ่งมีจำนวนรายการจุดอ่อนที่เกิดจากจุดอ่อนประเภทนี้จำนวน 34 รายการ เมื่อพิจารณาจากประเภทเครื่องมือ ในส่วนเครื่องมือสนับสนุนการให้บริการมีจำนวน 63 รายการและเครื่องมือช่วยการพัฒนาจำนวน 13 รายการ

5. จุดที่เกิดจุดอ่อนมากที่สุดคือ ส่วนการพิสูจน์ตัวตน มีจำนวน 93 รายการ และผลิตภัณฑ์ที่มีจุดอ่อนเกิดที่จุดนี้มากที่สุดคือ BEA Web Logic ซึ่งมีจำนวนรายการจุดอ่อนที่เกิดจากจุดนี้จำนวน 38 รายการ เมื่อพิจารณาจากประเภทของเครื่องมือในส่วนของเครื่องมือสนับสนุนการให้บริการจะมีจำนวนเท่ากับ 78 รายการ และเครื่องมือช่วยการพัฒนามีจำนวน 15 รายการ

6. คะแนนจุดอ่อนเมื่อแยกตามผลกระทบของความเสียหายที่เกิดขึ้นมากที่สุด คือ การสูญเสียความลับ 688 คะแนน รองลงมาคือการสูญเสียสภาพพร้อมใช้งาน 466 คะแนน และการเสียบูรณภาพ 297 คะแนน

7. พิจารณาแยกเป็นกลุ่มเครื่องมือส่วนของเครื่องมือสนับสนุนการให้บริการและเครื่องมือช่วยการพัฒนา มีผลกระทบที่เกิดขึ้นมากที่สุดเหมือนกัน คือ การสูญเสียความลับ

5.1.4 วิเคราะห์ผลที่ได้

เมื่อพิจารณาจากข้อมูลของคะแนนที่ได้จากการประเมินสามารถวิเคราะห์ผลของแต่ละผลลัพธ์ได้ดังนี้

1. รายการจุดอ่อนของผลิตภัณฑ์ไมโครซอฟต์มีจำนวนรายการที่พบในซีวีอีมากที่สุด รวมทั้งคะแนนของผลิตภัณฑ์ไมโครซอฟต์ก็มีคะแนนจุดอ่อนสูงมากที่สุด เพราะจุดอ่อนที่เกิดขึ้นส่วนใหญ่มาจากโปรแกรมไอไอเอส(IIS) ซึ่งเป็นโปรแกรมประเภทสนับสนุนการให้บริการ เหตุผลเนื่องจากโปรแกรมนี้ติดตั้งง่ายและมีมาให้กับระบบปฏิบัติการวินโดว์ (Windows) ดังนั้นทำให้การใช้งานจึงเป็นที่นิยมเป็นอย่างมากของทั้งผู้พัฒนาโปรแกรม รวมทั้งการใช้งานจริง แต่โปรแกรมไมโครซอฟต์วิชวลสตูดิโอ (Microsoft Visual Studio) ซึ่งเป็นเครื่องมือช่วยการพัฒนา กลับเป็นไปในลักษณะตรงกันข้ามคือจะพบจุดอ่อนจากรายการซีวีอีไม่มาก และมีคะแนนไม่สูง ดังนั้นสรุปได้ว่าข้อมูลจากซีวีอีไมโครซอฟต์มีจุดอ่อนส่วนใหญ่เกิดขึ้นจากเครื่องมือช่วยสนับสนุนการให้บริการ
2. พิจารณาจากคะแนนจุดอ่อนของเครื่องมือสนับสนุนการให้บริการที่มีคะแนนสูงกว่าเครื่องมือช่วยการพัฒนา เป็นเพราะการโจมตีส่วนใหญ่ในปัจจุบันจะโจมตีจุดที่เข้าถึงได้ง่าย ซึ่งเครื่องมือสนับสนุนการให้บริการสามารถเข้าถึงได้ง่ายกว่า เนื่องจากเครื่องมือดังกล่าวทำงานภายใต้ระบบอินเทอร์เน็ต ซึ่ง

เปรียบเสมือนสถานที่สาธารณะที่ใครก็ตามสามารถเชื่อมต่อได้ก็สามารถเข้าถึงเพื่อโจมตีได้เช่นเดียวกัน แต่เครื่องมือช่วยการพัฒนาการโจมตีส่วนใหญ่จะโจมตีโดยการเข้าถึงในส่วนของช่วยการพัฒนา ซึ่งปัญหาดังกล่าวจะไม่ส่งผลกระทบต่อการใช้งานจริง ดังนั้นจากเหตุผลนี้ทำให้ข้อมูลจากรายการซีวีอีมีข้อมูลจากเครื่องมือสนับสนุนการให้บริการมากกว่า เพราะการใช้งานเว็บเซอร์วิสผู้ใช้งานส่วนใหญ่จะติดต่อกับเครื่องมือสนับสนุนการให้บริการมากกว่า ทำให้ข้อมูลดังกล่าวมีจำนวนมาก

3. ประเภทความผิดพลาดของการตรวจสอบการเข้าถึง เป็นประเภทที่พบมากที่สุดในจุดอ่อนบนผลิตภัณฑ์เว็บเซอร์วิส ซึ่งความผิดพลาดประเภทนี้เกิดขึ้นมากที่สุดเพราะเว็บเซอร์วิสทำงานบนระบบอินเทอร์เน็ตเป็นระบบเปิด ทำให้ผู้ไม่หวังดีอาศัยความผิดพลาดจากจุดนี้เข้าถึงระบบ
4. การพิสูจน์ตัวตนคือจุดที่เกิดจุดอ่อนมากที่สุด เนื่องจากจุดนี้เป็นส่วนเริ่มต้นของการใช้งานระบบทั่วๆไป รวมทั้งเว็บเซอร์วิสด้วย ซึ่งการโจมตีจะอาศัยการพยายามด้วยวิธีต่างๆ เพื่อเข้าใช้งานระบบ
5. จุดอ่อนที่มีประเภทจุดอ่อนเป็น อื่นๆ มีจำนวนมากถึง 16 รายการ ซึ่งเป็นของผลิตภัณฑ์ OracleAS ซึ่งมีเนื้อหาอธิบายจุดอ่อนว่า “ unknown impact and attack vectors “ ซึ่งทำให้การระบุประเภทไม่อยู่ในประเภทใดเลยอย่างชัดเจน เนื่องจากรายละเอียดและข้อมูลอ้างอิงจากรายการดังกล่าวให้ข้อมูลของการโจมตี และส่วนที่โดนโจมตีไม่เพียงพอ ดังนี้ผู้วิจัยจำเป็นต้องระบุประเภทจุดอ่อนเป็นประเภท อื่นๆ

5.1.5 ปัญหา อุปสรรค

จากการดำเนินการวิจัยนี้ มีปัญหาเกิดขึ้นดังนี้

1. โปรแกรมของบางผลิตภัณฑ์ค้นหาข้อมูลไม่พบในรายการซีวีอี ทั้งที่เป็นโปรแกรมที่มีชื่อเสียง [7] และได้รับความนิยมพอสมควร จึงทำให้โปรแกรมที่ต้องการนำมาใช้ในงานวิจัยตอนเริ่มแรก ไม่สามารถนำมาใช้ในงานวิจัยได้ จึงจำเป็นต้องตัดโปรแกรมดังกล่าวออกจากการวิจัย
2. การตรวจสอบความสัมพันธ์ของรายการซีวีอีกับจุดอ่อนที่เกี่ยวข้องกับเว็บเซอร์วิส เนื่องจากรายการจุดอ่อนที่เกี่ยวข้องจะมีรายละเอียดที่สัมพันธ์กับการทำงานของเว็บเซอร์วิส แต่ส่วนใหญ่ที่เกิดขึ้นมักไม่ค่อยเกี่ยวข้อง

3. การสืบค้นรายการอ้างอิงของรายการซีวีอีบางรายการ ไม่สามารถสืบค้นได้ เพราะเว็บไซต์บางส่วนไม่มีเสถียรภาพในการเข้าถึงข้อมูล ดังนั้นจึงต้องบันทึกหน้าเว็บเพจที่เกี่ยวข้องกับรายการจุดอ่อนนั้นๆ ไว้กรณีที่เข้าไปค้นหาข้อมูลไม่ได้
4. การประเมินคะแนนจุดอ่อนบางรายการที่ไม่มีข้อมูลจุดที่เกิดของจุดอ่อนและผลกระทบที่เกิดขึ้น โดยในรายการซีวีอีมีข้อความ “ unknown impact and attack vectors “ ซึ่งทำให้การประเมินยากลำบาก ไม่สามารถวิเคราะห์การให้คะแนนจากจุดที่ทำให้เกิดจุดอ่อนดังกล่าวได้ ทำให้ต้องวิเคราะห์จากรายการอ้างอิงที่เกี่ยวข้อง ซึ่งจะทำให้สามารถนำข้อมูลดังกล่าวมาประเมินคะแนนต่อไปได้ โดยที่จำนวนรายการซีวีอีที่มีปัญหาดังกล่าวมีจำนวน 23 รายการจากทั้งหมด 416 รายการ คิดเป็น 5.52 % ของจำนวนรายการซีวีอีที่ใช้ในงานวิจัยทั้งหมด

5.2 ข้อเสนอแนะ

จากการดำเนินการวิจัยจนได้ผลลัพธ์และข้อสรุปแล้วนั้น ได้มีจุดที่ควรคำนึงถึงในงานวิจัย ดังนี้

1. การวิเคราะห์ข้อมูลจุดอ่อนที่ได้เพียงอย่างเดียวอาจจะไม่เพียงพอ เพราะผลลัพธ์ที่ได้อาจจะไม่ใช่คำตอบที่ดีที่สุดก็เป็นได้หากผู้ที่ทำการวิเคราะห์นั้นขาดความรู้และประสบการณ์ที่มากพอ ดังนั้นหากมีผู้ที่มีความรู้ความสามารถหรือผู้ที่มีประสบการณ์ความชำนาญ ช่วยในการวิเคราะห์ข้อมูลก็จะยิ่งช่วยให้สามารถวิเคราะห์ข้อมูลที่เป็นทางเลือกที่ดีที่สุดได้มากยิ่งขึ้น
2. ผลจากงานวิจัยที่ได้สรุปผลออกมาในงานวิจัยนี้เป็นเพียงการวิเคราะห์มุมมองเพียงส่วนหนึ่งของข้อมูลที่จัดเก็บไว้เท่านั้น หากต้องการวิเคราะห์ข้อมูลให้มีความแม่นยำมากยิ่งขึ้น อาจจะจำเป็นต้องอาศัยมุมมองการวิเคราะห์ข้อมูลในมุมมองอื่นๆที่แตกต่างจากในงานวิจัยนี้ร่วมด้วยเพื่อให้เห็นลักษณะการเกิดจุดอ่อนที่ชัดเจนมากยิ่งขึ้น
3. มีรายการจุดอ่อนจำนวนมากที่ไม่สามารถระบุได้ว่า จุดอ่อนรายการนั้นๆ ส่งผลกระทบต่อระบบปฏิบัติการบนแพลตฟอร์มอะไร หรือส่งผลกระทบต่อระบบ ปฏิบัติการใดบ้าง ซึ่งหากสามารถศึกษาหรือค้นคว้าเพิ่มเติมจนทำให้สามารถระบุถึงประเภทของระบบปฏิบัติการหรือแพลตฟอร์มที่ได้รับผลกระทบจากรายการจุดอ่อนที่เกิดขึ้นในกลุ่มนี้ได้ ก็จะช่วยทำให้จุดอ่อนที่จัดอยู่ในกลุ่มนี้มีจำนวนลดลง และทำให้ได้ข้อมูลระบบปฏิบัติการที่ได้รับ

ผลกระทบจากจุดอ่อนนั้นๆมากขึ้น สามารถนำผลที่ได้ไปวิเคราะห์และประเมินผลได้อย่างถูกต้องมากยิ่งขึ้น

4. ประเด็นความล้าสมัยของเวอร์ชั่นเก่าและ Patch ที่ออกมาแก้จุดอ่อนของแต่ละเวอร์ชั่นในรายการซีวีอี เนื่องจากงานวิจัยนี้ไม่ได้สนใจในส่วนนี้ จึงจะนำประเด็นทั้งสองนี้ไปใช้ในงานวิจัยในอนาคต
5. ควรติดตามผลของจุดอ่อนตามรายการซีวีอีที่เกิดขึ้นในปี ค.ศ. 2007 และปี ค.ศ. 2008 เพราะเป็นปีที่เริ่มมีการใช้งานเว็บเซอร์วิสอย่างกว้างขวาง

5.3 งานวิจัยในอนาคต

จากงานวิจัยนี้ยังมีประเด็นที่สามารถนำมาทำการวิจัยต่อเนื่องได้ดังนี้

1. การประเมินคะแนนจุดอ่อนแยกตามจุดที่เกิดขึ้นกับส่วนต่างๆของระบบเว็บเซอร์วิส เช่น เว็บเซิร์ฟเวอร์ ฐานข้อมูล และเว็บเซอร์วิสอินเทอร์เฟส
2. การประเมินคะแนนจุดอ่อนของเว็บเซอร์วิสที่ใช้งานภายใต้ระบบปฏิบัติการต่างๆ เช่น ระบบปฏิบัติการวินโดว์ ระบบปฏิบัติการลีนุกต์ ระบบปฏิบัติการยูนิกต์ เป็นต้น
3. การประเมินคะแนนจุดอ่อนของเว็บเซอร์วิสโดยพิจารณาเฉพาะเวอร์ชั่นปัจจุบันและรายการซีวีอีที่ยังไม่มี Patch
4. การประเมินคะแนนจุดอ่อนที่เกิดขึ้นกับเว็บเซอร์วิสในเชิงลึก

รายการอ้างอิง

[1] CVE List. [Online]. Available from: http://www.cve.mitre.org/cve. [2006,December 31]

[2] รัศมีทิพย์ วิตา. การประเมินและเปรียบเทียบการป้องกันจุดอ่อนของระบบลินุกซ์โดยการเพิ่มความแข็งแกร่งกับการใช้แอลเอสเอ็ม. วิทยานิพนธ์ปริญญามหาบัณฑิต ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2546.

[3] Landwehr, C.E., et al. A Taxonomy of Computer Program Security Flaws. ACM Computing Surveys (CSUR) 1994 : 26.

[4] เกียรติ ภิรมย์โสภา. การประเมินความเสี่ยงเว็บเซิร์ฟเวอร์โดยการจำแนกระดับผลกระทบของความเสียหาย. วิทยานิพนธ์ปริญญามหาบัณฑิต ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2547.

[5] Jeongseok S, Han-Sung K, Sanghyun C, Sungdeok C. Web server attack categorization Based on root causes and their locations. Proceedings of International Conference on Information Technology, Coding and Computing (ITCC 2004) 2004 : 157-163.

[6] UDDI Products and Components. [Online]. Available from: http://uddi.org/solutions.html [2007, January 20]

[7] Web services development. [Online]. Available from:http://searchwebservices.techtarget.com/ [2006, December 30]

[8] Demchenko Y, Gommans L, de Laat C, Oudenaarde B. Web services and grid security vulnerabilities and threats analysis and model. Grid Computing The 6th IEEE/ACM International Workshop 2005 : 6.

[9] Holgersson J, Soderstrom E. Web service security - vulnerabilities and threats within the context of WS-security. Grid Computing Workshop 2005 : 138-146.

[10]Carlos Gutiérrez,Eduardo Fernández-Medina,Mario Piattini. Web services enterprise security architecture: a case study their locations. ACM Press 2005 : 10-19.

ภาคผนวก

ภาคผนวก ก
รายการซีวีอี

ผลิตภัณฑ์ BEA Web Logic จำนวน 103 รายการ

CVE-2000-0499	CVE-2003-1226	CVE-2005-2680	CVE-2006-0422	CVE-2000-1238
CVE-2000-0500	CVE-2003-1290	CVE-2005-4704	CVE-2006-0423	CVE-2003-0733
CVE-2000-0681	CVE-2004-0470	CVE-2005-4705	CVE-2006-0424	CVE-2005-2092
CVE-2000-0682	CVE-2004-0471	CVE-2005-4749	CVE-2006-0425	
CVE-2000-0683	CVE-2004-0652	CVE-2005-4750	CVE-2006-0426	
CVE-2000-0684	CVE-2004-0711	CVE-2005-4751	CVE-2006-0427	
CVE-2000-0685	CVE-2004-0712	CVE-2005-4752	CVE-2006-0428	
CVE-2001-0098	CVE-2004-0713	CVE-2005-4753	CVE-2006-0429	
CVE-2002-0106	CVE-2004-0715	CVE-2005-4754	CVE-2006-0430	
CVE-2002-1030	CVE-2004-1755	CVE-2005-4755	CVE-2006-0431	
CVE-2002-2141	CVE-2004-1756	CVE-2005-4756	CVE-2006-0432	
CVE-2002-2142	CVE-2004-1757	CVE-2005-4757	CVE-2006-1351	
CVE-2002-2177	CVE-2004-1758	CVE-2005-4758	CVE-2006-1352	
CVE-2003-0151	CVE-2004-2320	CVE-2005-4759	CVE-2006-1358	
CVE-2003-0624	CVE-2004-2321	CVE-2005-4760	CVE-2006-2461	
CVE-2003-0640	CVE-2004-2424	CVE-2005-4761	CVE-2006-2462	
CVE-2003-1093	CVE-2005-0432	CVE-2005-4762	CVE-2006-2464	
CVE-2003-1094	CVE-2005-1742	CVE-2005-4763	CVE-2006-2466	
CVE-2003-1095	CVE-2005-1743	CVE-2005-4764	CVE-2006-2467	
CVE-2003-1220	CVE-2005-1744	CVE-2005-4765	CVE-2006-2468	
CVE-2003-1221	CVE-2005-1745	CVE-2005-4766	CVE-2006-2469	
CVE-2003-1222	CVE-2005-1746	CVE-2005-4767	CVE-2006-2470	
CVE-2003-1223	CVE-2005-1747	CVE-2006-0419	CVE-2006-2471	
CVE-2003-1224	CVE-2005-1748	CVE-2006-0420	CVE-2006-2472	
CVE-2003-1225	CVE-2005-1749	CVE-2006-0421	CVE-2006-2546	

ผลิตภัณฑ์ IBM Web Sphere จำนวน 42 รายการ

CVE-1999-0852	CVE-2001-1189	CVE-2005-4413	CVE-2006-2435	CVE-2006-6135
CVE-1999-0944	CVE-2002-1153	CVE-2006-1093	CVE-2006-2436	CVE-2006-6136
CVE-2000-0497	CVE-2004-0684	CVE-2006-1619	CVE-2006-3231	
CVE-2000-0652	CVE-2004-2558	CVE-2006-2342	CVE-2006-3232	
CVE-2000-0848	CVE-2005-0425	CVE-2006-2429	CVE-2006-4136	

CVE-2001-0122	CVE-2005-1112	CVE-2006-2430	CVE-2006-4137
CVE-2001-0312	CVE-2005-1872	CVE-2006-2431	CVE-2006-4222
CVE-2001-0446	CVE-2005-2091	CVE-2006-2432	CVE-2006-4223
CVE-2001-0824	CVE-2005-3498	CVE-2006-2433	CVE-2006-5323
CVE-2001-0962	CVE-2005-3760	CVE-2006-2434	CVE-2006-5324

ผลิตภัณฑ์ Microsoft Internet Information Services (IIS) จำนวน 142 รายการ

CVE-2004-1312	CVE-1999-0738	CVE-2000-0630	CVE-2001-0709	CVE-2002-1718
CVE-2005-0871	CVE-1999-0739	CVE-2000-0631	CVE-2001-0902	CVE-2002-1744
CVE-2005-1118	CVE-1999-0777	CVE-2000-0649	CVE-2001-1186	CVE-2002-1745
CVE-2005-2089	CVE-1999-0861	CVE-2000-0746	CVE-2001-1243	CVE-2002-1790
CVE-2005-2678	CVE-1999-0867	CVE-2000-0770	CVE-2001-1510	CVE-2002-1876
CVE-2005-4047	CVE-1999-0874	CVE-2000-0778	CVE-2001-1511	CVE-2002-1895
CVE-2005-4360	CVE-1999-1011	CVE-2000-0858	CVE-2002-0071	CVE-2002-1908
CVE-2005-4734	CVE-1999-1035	CVE-2000-0884	CVE-2002-0072	CVE-2002-1992
CVE-2006-0026	CVE-1999-1148	CVE-2000-0886	CVE-2002-0073	CVE-2003-0105
CVE-2006-0704	CVE-1999-1223	CVE-2000-0951	CVE-2002-0074	CVE-2003-0109
CVE-2006-1394	CVE-1999-1233	CVE-2000-0970	CVE-2002-0075	CVE-2003-0223
CVE-1999-0154	CVE-1999-1376	CVE-2000-1090	CVE-2002-0079	CVE-2003-0224
CVE-1999-0191	CVE-1999-1397	CVE-2000-1104	CVE-2002-0147	CVE-2003-0225
CVE-1999-0229	CVE-1999-1451	CVE-2000-1147	CVE-2002-0148	CVE-2003-0226
CVE-1999-0233	CVE-1999-1537	CVE-2001-0004	CVE-2002-0149	CVE-2003-0227
CVE-1999-0253	CVE-1999-1538	CVE-2001-0096	CVE-2002-0150	CVE-2003-0349
CVE-1999-0278	CVE-1999-1544	CVE-2001-0146	CVE-2002-0224	CVE-2003-0702
CVE-1999-0281	CVE-2000-0024	CVE-2001-0151	CVE-2002-0364	CVE-2003-0718
CVE-1999-0348	CVE-2000-0025	CVE-2001-0241	CVE-2002-0419	CVE-2003-0904
CVE-1999-0349	CVE-2000-0071	CVE-2001-0333	CVE-2002-0421	CVE-2003-1102
CVE-1999-0360	CVE-2000-0115	CVE-2001-0334	CVE-2002-0422	CVE-2004-0205
CVE-1999-0407	CVE-2000-0126	CVE-2001-0335	CVE-2002-0862	CVE-2004-0928
CVE-1999-0412	CVE-2000-0167	CVE-2001-0336	CVE-2002-0869	
CVE-1999-0448	CVE-2000-0226	CVE-2001-0337	CVE-2002-1180	
CVE-1999-0449	CVE-2000-0246	CVE-2001-0500	CVE-2002-1181	
CVE-1999-0450	CVE-2000-0258	CVE-2001-0506	CVE-2002-1182	
CVE-1999-0561	CVE-2000-0304	CVE-2001-0507	CVE-2002-1309	
CVE-1999-0725	CVE-2000-0408	CVE-2001-0508	CVE-2002-1310	
CVE-1999-0736	CVE-2000-0413	CVE-2001-0544	CVE-2002-1694	
CVE-1999-0737	CVE-2000-0457	CVE-2001-0545	CVE-2002-1717	

ผลิตภัณฑ์ Microsoft Visual Studio จำนวน 3 รายการ

CVE-2001-0341	CVE-2004-0204	CVE-2006-0187

ผลิตภัณฑ์ Oracle Application Server (OracleAS) จำนวน 101 รายการ

CVE-2000-1235	CVE-2002-0571	CVE-2005-3448	CVE-2006-0435	CVE-2006-5361
CVE-2000-1236	CVE-2002-0842	CVE-2005-3449	CVE-2006-3706	CVE-2006-5362
CVE-2001-0326	CVE-2002-0947	CVE-2005-3450	CVE-2006-3707	CVE-2006-5363
CVE-2001-0419	CVE-2002-1630	CVE-2005-3451	CVE-2006-3708	CVE-2006-5364
CVE-2001-1216	CVE-2002-1631	CVE-2005-3452	CVE-2006-3709	CVE-2006-5365
CVE-2001-1217	CVE-2002-1632	CVE-2005-3453	CVE-2006-3710	CVE-2004-1368
CVE-2001-1371	CVE-2002-1635	CVE-2005-4549	CVE-2006-3711	CVE-2005-1383
CVE-2001-1372	CVE-2002-1636	CVE-2005-4550	CVE-2006-3712	CVE-2005-3445
CVE-2002-0102	CVE-2002-1637	CVE-2006-0273	CVE-2006-3713	CVE-2005-3446
CVE-2002-0103	CVE-2002-1638	CVE-2006-0274	CVE-2006-3714	CVE-2005-3447
CVE-2002-0386	CVE-2002-1641	CVE-2006-0275	CVE-2006-3719	CVE-2004-0543
CVE-2002-0559	CVE-2002-1858	CVE-2006-0282	CVE-2006-3720	CVE-2004-2115
CVE-2002-0560	CVE-2002-2153	CVE-2006-0283	CVE-2006-3721	CVE-2006-5346
CVE-2002-0561	CVE-2003-1193	CVE-2006-0284	CVE-2006-5353	CVE-2006-5347
CVE-2002-0562	CVE-2004-0385	CVE-2006-0285	CVE-2006-5354	CVE-2006-5348
CVE-2002-0563	CVE-2004-1362	CVE-2006-0286	CVE-2006-5355	CVE-2006-5349
CVE-2002-0564	CVE-2004-1877	CVE-2006-0287	CVE-2006-5356	CVE-2006-5350
CVE-2002-0565	CVE-2004-2244	CVE-2006-0288	CVE-2006-5357	
CVE-2002-0566	CVE-2005-2093	CVE-2006-0289	CVE-2006-5358	
CVE-2002-0568	CVE-2005-2291	CVE-2006-0290	CVE-2006-5359	
CVE-2002-0569	CVE-2005-2292	CVE-2006-0291	CVE-2006-5360	

ผลิตภัณฑ์ SAP Web Application Server จำนวน 9 รายการ

CVE-2005-3633	CVE-2005-3635	CVE-2006-1039	CVE-2006-5785	CVE-2001-0366
CVE-2005-3634	CVE-2005-3636	CVE-2006-5784	CVE-2006-6011	

ผลิตภัณฑ์ SUN Java Enterprise จำนวน 9 รายการ

CVE-2004-2216	CVE-2005-0742	CVE-2005-4804	CVE-2006-2501	CVE-2006-5654
CVE-2004-1816	CVE-2005-4046	CVE-2005-4805	CVE-2006-3921	

ผลิตภัณฑ์ JBoss Application Server (JBoss AS) จำนวน 7 รายการ

CVE-2003-0845	CVE-2005-2158	CVE-2005-4709	CVE-2006-5750
CVE-2005-2006	CVE-2005-3583	CVE-2006-3733	

ภาคผนวก ข
ผลงานตีพิมพ์

งานประชุมทางวิชาการวิทยาการคอมพิวเตอร์ และวิศวกรรมคอมพิวเตอร์แห่งชาติ ครั้งที่ 11 (National Computer Science and Engineering Conference (NCSEC 2007)) ระหว่างวันที่ 19 - 21 พฤศจิกายน 2550 ณ โรงแรม Miracle Grand Convention Hotel ประเทศไทย ในบทความเรื่อง การประเมินจุดอ่อนของผลิตภัณฑ์เว็บเซอร์วิสโดยจำแนกความรุนแรงของความเสียหาย ตีพิมพ์ในวารสาร การประชุมวิชาการวิทยาการคอมพิวเตอร์และวิศวกรรมคอมพิวเตอร์แห่งชาติ ครั้งที่ 11 (NCSEC2007)

การประเมินจุดอ่อนของผลิตภัณฑ์เว็บเซอร์วิสโดยจำแนกความรุนแรงของความเสียหาย

Vulnerability Assessment of Web Services Products Based on Severity of Damage

กิตติศักดิ์ นิทาน และ ดร.ยรรยง เต็งอำนวย
ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย กรุงเทพฯ 10330
อีเมล์ : Kittisak.N@Student.Chula.ac.th, Yunyong.T@Chula.ac.th

Abstract

This research assesses software vulnerability of web services products based on Common Vulnerability and Exposure (CVE) and classifies the damage of each vulnerability into confidentiality, integrity, and availability. The impact of each vulnerability type of web services products have been classified to development tools and runtime service tools. We use scores of impacts to compute severity of damage on web services products and compare each type of damage.

Keywords: Software Vulnerability, Web Services, Severity-Based Damage, CVE

บทคัดย่อ

งานวิจัยนี้ได้นำเสนอวิธีการประเมินจุดอ่อนด้านซอฟต์แวร์ของผลิตภัณฑ์เว็บเซอร์วิสโดยใช้รายการจุดอ่อนซีวีอี และได้นำเสนอวิธีการจำแนกความรุนแรงของผลกระทบที่ได้รับของความเสียหายที่เกิดขึ้น โดยแบ่งออกเป็น 3 ประเภท คือ การรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน โดยแยกจุดอ่อนของผลิตภัณฑ์เว็บเซอร์วิสเป็น 2 กลุ่มใหญ่ คือ จุดอ่อนของเครื่องมือที่ใช้ในการพัฒนาเว็บเซอร์วิสและจุดอ่อนของเครื่องมือที่ใช้ในการสนับสนุนการให้บริการ ในการประเมินได้มีการนำค่าของผลกระทบมาคำนวณหาค่าและเปรียบเทียบคะแนนความเสียหายของจุดอ่อนของแต่ละผลิตภัณฑ์

1. บทนำ

การโจมตีผ่านระบบเว็บเซอร์วิสเริ่มมีจำนวนเพิ่มมากขึ้น ส่วนใหญ่เกิดจากจุดอ่อนของการพัฒนาของแอพพลิเคชั่นที่ใช้ในการทำงานของเว็บเซอร์วิส ทั้งในส่วนเครื่องมือช่วยการพัฒนา (Development Tool) ซึ่งมีจุดอ่อนในการสร้างเว็บเซอร์วิสขึ้นมาแล้วทำงานอย่างไม่มีเสถียรภาพ และในส่วนเครื่องมือสนับสนุนการให้บริการ (Runtime Service Tools) ซึ่งมีจุดอ่อนในการให้บริการที่ผิดพลาด เช่น ไม่สามารถให้บริการได้ตลอดเวลาทำการ หรือยอมให้บุคคลอื่นล่วงละเมิดเข้ามาแก้ไขข้อมูลที่ไม่ได้รับอนุญาต เป็นต้น ดังนั้นการพิจารณาเลือกแอพพลิเคชั่นของเว็บเซอร์วิสเพื่อนำมาใช้ในองค์กร ควรจะพิจารณาให้เหมาะสมกับการใช้งานและมีความปลอดภัยสูงจากการถูกโจมตีจากผู้ไม่หวังดี

งานวิจัยนี้จึงมีแนวความคิดที่จะประเมินและเปรียบเทียบให้เห็นถึงความรุนแรงของความเสียหายต่อการโจมตีเว็บเซอร์วิสด้านซอฟต์แวร์ที่ใช้ในการพัฒนาระบบเว็บเซอร์วิส โดยพิจารณาจากข้อมูลจุดอ่อนที่ได้มีการรวบรวมไว้ในรายการจุดอ่อนของซีวีอี (Common Vulnerability and Exposure (CVE)) [1] ซึ่งจะนำมาแบ่งประเภทตามกลุ่มของจุดอ่อนและผลิตภัณฑ์ที่เกี่ยวเนื่องกับเว็บเซอร์วิส โดยจะมีการกำหนดระดับผลกระทบที่เกิดขึ้นตามแนวคิดวิธีการให้คะแนนค่าถ่วงน้ำหนัก [2] โดยจำแนกตามความเสียหายที่เกิดขึ้น ซึ่งจะเป็น

ประโยชน์ต่อการพิจารณาเลือกใช้เว็บเซอร์วิสได้อย่างเหมาะสม รวมถึงเป็นข้อมูลพื้นฐานเพื่อนำไปใช้ในการหาแนวทางการป้องกันสำหรับระบบเว็บเซอร์วิสที่มีใช้อยู่แล้วในองค์กร เพื่อเป็นการช่วยลดความเสี่ยงต่อการถูกโจมตีและป้องกันความเสียหายที่อาจเกิดขึ้นได้กับระบบ

2. งานวิจัยที่เกี่ยวข้อง

แลนด์เวอร์ และ คณะ [3] ได้จัดกลุ่มของจุดอ่อนออกเป็น 3 กลุ่มดังนี้ ตามลักษณะการเกิด เวลาที่เกิด และสถานที่ที่เกิด

รัศมีทิพย์ วิตา [2, 4] ปรับการจัดกลุ่มของแลนด์เวอร์ โดยตัดเวลาที่เกิดจุดอ่อนออก และเสริมลักษณะความเสียหายและระดับความรุนแรงเข้าไป เพื่อนำไปวิเคราะห์กับรายการในซีวีอี ซึ่งงานวิจัยนี้ได้ทดลองทำการประเมินค่าระดับความเสียหายของจุดอ่อนสำหรับระบบลีนุกซ์

เกียรติ ภิรมย์โสภา [5] วัดระดับผลกระทบของจุดอ่อน โดยการใช้ผลรวมคะแนนของระดับความเสียหายแต่ละประเภทที่เกิดขึ้น ได้แก่ การรักษาความลับ, บูรณภาพ และสภาพพร้อมใช้งาน

ส่วนในเรื่องของเว็บเซอร์วิสนั้น เจียงซอก [6] นำเสนอรูปแบบการจัดกลุ่มของจุดอ่อนให้เหมาะสมกับระบบเว็บเซอร์วิสเพื่อนำมาใช้ในการพัฒนาระบบ IDS (Intrusion Detection System) โดยการจัดกลุ่มการโจมตีแยกประเภทออกเป็นการโจมตีที่ Web Interface, Web Server, Preprocessor และ Database

3. การค้นหาจุดอ่อนในรายการซีวีอี

ซีวีอีเป็นการกำหนดชื่อมาตรฐานของรายการจุดอ่อนที่เกิดขึ้นในระบบคอมพิวเตอร์ ข้อมูลจุดอ่อนที่ปรากฏอยู่ในรายการซีวีอี มีองค์ประกอบอยู่ 3 ส่วนด้วยกัน ได้แก่ ชื่อรายการจุดอ่อน คำอธิบาย และแหล่งข้อมูลอ้างอิง

การค้นหารายชื่อจุดอ่อนในรายการซีวีอี ใช้วิธีการหาคำศัพท์ที่เกี่ยวข้องดังนี้

- ชื่อองค์ประกอบที่เกี่ยวข้องกับระบบเว็บเซอร์วิส
- ชื่อคำศัพท์เฉพาะของเว็บเซอร์วิส
- ชื่อผลิตภัณฑ์ที่ใช้ในการพัฒนาเว็บเซอร์วิส (Development Tools)
- ชื่อผลิตภัณฑ์ที่ใช้ในการให้บริการเว็บเซอร์วิส (Runtime Service Tools)

รวบรวมรายการจุดอ่อนจากรายการซีวีอีแล้ว คัดเลือกเฉพาะจุดอ่อนของเว็บเซอร์วิสดังตารางที่ 1 และคัดเลือกตามรายชื่อผลิตภัณฑ์และองค์ประกอบของเว็บเซอร์วิสที่เกี่ยวข้อง โดยแยกเป็นสองมิติของการค้นหาดังตารางที่ 2 ซึ่งรายชื่อผลิตภัณฑ์ที่คัดมาเป็นผลิตภัณฑ์เว็บเซอร์วิสที่ได้รับความนิยมในการใช้งานและเป็นที่รู้จักอย่างกว้างขวางของผู้ใช้งานทั่วไปจำนวน 10 ตัว โดยมีการแบ่งผลิตภัณฑ์เป็น 2 กลุ่มหลักคือส่วนการพัฒนา และส่วนการให้บริการ ข้อมูลที่ค้นหาได้มาจากการสืบค้นเว็บไซต์ [7, 8]

ตารางที่ : 1 รายการซีวีอีของผลิตภัณฑ์ BEA

รายการซีวีอี	CVE-2004-0652
รายละเอียด	The default CredentialMapper for BEA Web Logic Server and Express 7.0 and 7.0.0.1 stores passwords in cleartext on disk, which allows local users to extract passwords.
รายการอ้างอิง	BEA:BEA03-30.00 | URL:http://dev2dev.bea.com/pub/advisory/22 | BID:7563 | URL:http://www.securityfocus.com/bid/7563

ตารางที่ 2: แสดงรายชื่อผลิตภัณฑ์ที่ใช้ในงานวิจัย

	บริษัท	Development Tools	Runtime Service Tools
1	Apache	ไม่พบในซีวีอี	- jUDDI -Tomcat
2	BEA	ไม่พบในซีวีอี	-Web Logic Server
3	IBM	- Web Sphere Studio	- HTTPs
4	Micro Soft	- Microsoft Visual Studio	- IIS
5	Novell	ไม่พบในซีวีอี	-Novell Nsure UDDI Server
6	Oracle	- JDeveloper	-OracleAS
7	SAP	ไม่พบในซีวีอี	-SAP Web Application Server
8	SOA Software	ไม่พบในซีวีอี	-Registry Manager
9	Sun	- NetBeans - eclipse	-Sun Java Enterprise
10	JBOSS	ไม่พบในซีวีอี	- JBoss AS

4. การจัดกลุ่มจุดอ่อนของเว็บเซอร์วิส

ในส่วนการจัดกลุ่มจุดอ่อนของเว็บเซอร์วิส งานวิจัยนี้อาศัยหลักเกณฑ์อิงตามการจัดกลุ่มจุดอ่อนงานวิจัยของรัศมีทิพย์ [2, 4] โดยทำการแบ่งจุดอ่อนออกเป็น 3 รูปแบบด้วยกัน ได้แก่

- ประเภทของจุดอ่อน
- จุดที่เกิดจุดอ่อน
- ลักษณะความเสียหาย

4.1 ประเภทของจุดอ่อน

เป็นการจัดกลุ่มของลักษณะในการโจมตีระบบตามความผิดพลาด (Error) ที่มีในระบบโดยแบ่งความผิดพลาดออกได้เป็น 9 ประเภทดังนี้

- การตรวจสอบข้อมูลนำเข้า (Input validation)
- ขอบเขตข้อมูล(Boundary validation)
- การตรวจสอบการเข้าถึง (Access validation)
- การเหลื่อมล้ำของการตรวจสอบสิทธิ (Serialization)
- การปรับแต่งระบบ (Configuration)
- สภาพแวดล้อม (Environmental)
- การออกแบบระบบ (Design)
- ชุดคำสั่งจัดการสิ่งผิดปกติ (Exception Handling)
- อื่นๆ (Other)

ในงานวิจัยนี้จะกำหนดให้รายการจุดอ่อนแต่ละรายการมีประเภทของจุดอ่อนได้เพียง 1 ประเภท

4.2 จุดที่เกิดจุดอ่อน

เป็นการแบ่งตามตำแหน่งที่เกิดจุดอ่อนว่าอยู่ส่วนใดของระบบ ซึ่งแบ่งได้ 8 ตำแหน่งดังนี้

- ส่วนการเริ่มต้นระบบ (System Initiation)
- ส่วนการจัดการหน่วยความจำ (Memory Management)
- ส่วนการจัดการโปรเซส (Process Management)
- ส่วนการจัดการอุปกรณ์ (Device Management)
- ส่วนการจัดการแฟ้มข้อมูล (File Management)
- ส่วนการพิสูจน์ตัวตน (Authentication)
- ส่วนโปรแกรมที่สนับสนุนการทำงานระบบปฏิบัติการ (Support)
- ส่วนโปรแกรมประยุกต์ (Application)

ในงานวิจัยนี้กำหนดรายการจุดอ่อนแต่ละรายการมีจุดที่เกิดจุดอ่อนได้เพียง 1 จุดเท่านั้น

4.3 ลักษณะความเสียหาย

การจัดกลุ่มจุดอ่อนประเภทนี้ จะจัดกลุ่มตามลักษณะความเสียหายที่เกิดขึ้น อันจะนำไปสู่การเสียความเป็นความลับ การเสียบูรณภาพ และการเสียสภาพพร้อมใช้งาน

4.4 ระดับความรุนแรง

เนื่องจากจุดอ่อนแต่ละรายการในทั้ง 3 รูปแบบที่กล่าวมาสามารถก่อความเสียหายมากน้อยไม่เท่ากัน จึงต้องแบ่งระดับความรุนแรงของความเสียหายที่เกิดขึ้นนั้น ออกเป็น 3 ระดับ ได้แก่

- ระดับสูง (High)
- ระดับกลาง (Medium)
- ระดับต่ำ (Low)

จากขั้นตอนการประเมินจุดอ่อนของเว็บเซอร์วิสดังที่กล่าวมาทั้งหมด ผู้วิจัยได้ทำการประเมินและคำนวณระดับคะแนนของผลกระทบของรายการจุดอ่อนตามซีวีอีทั้งหมด 507 รายการ โดยแยกเป็นเครื่องมือช่วยการพัฒนา จำนวน 57 รายการและเครื่องมือสนับสนุนการให้บริการ จำนวน 450 รายการ

5. การแจกแจงคะแนน

การแจกแจงคะแนนของรายการจุดอ่อนจะให้คะแนนจำแนกตามความเสียหาย โดยการใช้ระดับความรุนแรงอ้างอิงจากตารางที่ 3 เป็นรูปแบบที่ใช้ในการประเมินคะแนน โดยการแจกแจงคะแนนจะประกอบด้วย 2 ส่วน คือ

- คะแนนระดับความรุนแรง
- การประเมินระดับผลกระทบ

5.1 คะแนนระดับความรุนแรง

การประเมินผลจุดอ่อนคำนวณได้โดยการใช้ผลรวมคะแนนของระดับความเสียหายแต่ละประเภทที่เกิดขึ้น ได้แก่ การรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน [2, 4] ดังตารางที่ 4

ตารางที่ 4: แสดงการคำนวณคะแนนระดับความรุนแรง

ประเภทความเสียหาย	ระดับความรุนแรง		
	ต่ำ	กลาง	สูง
การรักษาความลับ	1	2	3
บูรณภาพ	1	2	3
สภาพพร้อมใช้งาน	1	2	3

5.2 การประเมินระดับผลกระทบ

การประเมินระดับผลกระทบของจุดอ่อน [5] ที่สามารถคำนวณได้โดยการใช้ผลรวมคะแนนของระดับความเสียหายแต่ละประเภทที่เกิดขึ้น

ตารางที่ 3: แสดงเงื่อนไขในการกำหนดระดับผลกระทบแยกตามความเสียหาย

ระดับความรุนแรง			
ระดับสูง	ระดับกลาง	ระดับต่ำ	ไม่มีผลกระทบ
สูญเสียความลับ			
- เรียกดูข้อมูล โดยใช้สิทธิ์ของผู้ใช้งานสูงสุด	- เรียกดูข้อมูลโดยใช้สิทธิ์ของผู้ใช้งานระดับ USER ทั่วไป	- เรียกดูข้อมูลในระบบโดยใช้สิทธิ์ผู้ใช้งานทั่วไป	- ผู้มีสิทธิสามารถเรียกดูข้อมูลที่เปิดเผยแก่บุคคลทั่วไปตามสิทธิที่อนุญาต
สูญเสียบูรณภาพ			
- แก้ไขข้อมูลโดยใช้สิทธิของผู้ใช้งานสูงสุด	- แก้ไขข้อมูลโดยใช้สิทธิของผู้ใช้งานระดับ USER	- แก้ไขข้อมูลโดยใช้สิทธิของผู้ใช้งานทั่วไป	- แก้ไขข้อมูลตามสิทธิที่ได้รับเท่านั้น
สูญเสียความพร้อมใช้งาน			
- ทำให้ผู้ใช้งานระบบไม่สามารถใช้บริการระบบได้	- หยุดการให้บริการบางส่วนของระบบ	- สร้างข้อมูลจำนวนมากในระบบแต่ระบบยังสามารถให้บริการได้ปกติ	- สามารถใช้บริการของระบบได้ตามสิทธิที่ได้รับเท่านั้น

ได้แก่ การรักษาความลับ บูรณภาพ และสภาพพร้อมใช้งาน คิดได้จากสมการดังนี้

$$W_i = W_{C_i} + W_{I_{i+}} W_{A_i}$$

โดยที่

W_i คือ ระดับผลกระทบของจุดอ่อนใดๆ

W_{C_i} คือ ระดับผลกระทบของจุดอ่อนใดๆ ที่ส่งผลต่อการรักษาความลับ

W_{I_i} คือ ระดับผลกระทบของจุดอ่อนใดๆ ที่ส่งผลต่อการบูรณภาพ

W_{A_i} คือ ระดับผลกระทบของจุดอ่อนใดๆ ที่ส่งผลต่อสภาพพร้อมใช้งาน

i คือ ลำดับของซีวีอี

โดยให้ค่าของผลกระทบที่ส่งผลต่อการรักษาความลับ (C) ต่อบูรณภาพ (I) และต่อสภาพพร้อมใช้งาน (A) แต่ละประเภทมีค่าเป็น 1 และผลกระทบแบ่งเป็น 3 ระดับ คือ ส่งผลกระทบสูง มีคะแนนเท่ากับ 3 ส่งผลกระทบปานกลาง มีคะแนนเท่ากับ 2 และส่งผลกระทบต่ำ มีคะแนนเท่ากับ 1 แล้วจึงคำนวณโดยใช้สมการ $\sum_{i=1}^{n} W_i$ เพื่อคำนวณคะแนนผลกระทบโดยรวมของจุดอ่อนออกมา

ดังนั้นจุดอ่อนต่างๆ สามารถมีค่าผลกระทบได้สูงสุดคือ 3 + 3 + 3 = 9 และมีค่าผลกระทบต่ำสุดคือ 0 + 0 + 0 = 0 หรือไม่มีผลกระทบต่อความมั่นคงของระบบนั่นเอง ดังแสดงตามตารางที่ 5 ซึ่งค่าระดับผลกระทบนั้นแสดงถึงระดับความเสียหายที่เกิดขึ้นจากจุดอ่อนนั้นๆ โดยหากจุดอ่อนใดมีค่าระดับผลกระทบสูง หมายถึงจุดอ่อนนั้นสามารถสร้างความเสียหายให้แก่องค์กรได้มากกว่าจุดอ่อนที่ระดับผลกระทบต่ำกว่า

จากการคำนวณตามรูปแบบวิธีการประเมินจุดอ่อน ผลลัพธ์ที่ได้แยกตามประเภทของเครื่องมือดังตารางที่ 6 และแยกตามประเภทของจุดอ่อนตามตารางที่ 7 ถึง 10โดยเลือกมาพิจารณาเพียง 4 ผลิตภัณฑ์ที่มีค่าคะแนนสูง

ตารางที่ 5: แสดงการประเมินคะแนนรายการจุดอ่อน

	Confidentiality	Integrity	Availability	รวม
CVE-2006-5324	3	3	1	7
CVE-2006-3232	3	1	0	4
CVE-2006-4136	2	0	0	2

ตารางที่ 6: จำนวนจุดอ่อนแยกตามประเภทของเครื่องมือ

	ผลิตภัณฑ์	Development	Runtime	รวม
1	Apache	0	70	70
2	BEA	0	103	103
3	IBM	42	0	42
4	Microsoft	4	142	146
5	Novell	0	1	1
6	Oracle	0	110	110
7	SAP	0	8	8
8	SOA	0	1	1
9	Sun Micro Systems	11	8	19
10	JBOSS	0	7	7
	รวม	57	450	507

ตารางที่ 7: คะแนนจุดอ่อนแยกตามประเภท

ประเภทจุดอ่อน	BEA Web logic	IBM Web sphere	Sun Java Enterprise	JBoss Application Server
Input validation	6	2	2	1
Boundary validation	15	7	3	1
Access validation	16	12	1	0
Serialization	17	9	3	2
Configuration	17	2	0	2
Environment	6	0	0	0
Design	19	7	0	1
Exception handling	4	1	0	0
Other	2	2	0	0

ตารางที่ 8: คะแนนจุดอ่อนแยกตามจุดที่พบ

จุดที่เกิดจุดอ่อน	BEA Web logic	IBM Web sphere	Sun Java Enterprise	JBoss Application Server
System Initialization	13	2	0	0
Memory Management	15	5	3	1
Process Management Scheduling	22	8	1	3
Device Management	0	0	0	0
File Management	4	11	2	0
Identification/ Authentication	38	14	2	3
Support	2	1	0	0
Application	8	1	1	0

ตารางที่ 9: คะแนนแยกตามประเภทของความเสียหาย

	Confidentiality	Integrity	Availability	รวม
BEA	201	104	111	416
IBM	101	55	40	196
Sun Java Enterprise	11	6	15	32
JBoss AS	13	11	9	33
รวม	376	199	202	677

ตารางที่ 10: คะแนนรวมความรุนแรงแยกตามผลิตภัณฑ์

	BEA Web logic	IBM Web sphere	Sun Java Enterprise	JBoss Application Server
Overall Vulnerability	416	196	32	33

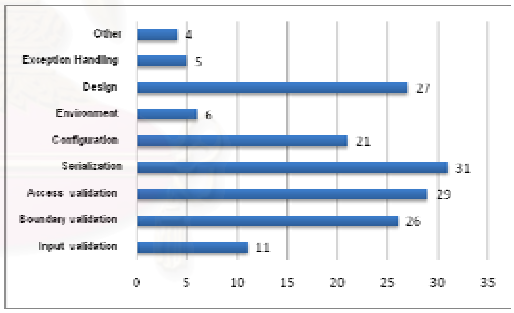
6. ผลการวิจัย

จากการวิเคราะห์และประเมินจุดอ่อนที่เกิดขึ้นบนเว็บเซอร์วิสของผลิตภัณฑ์ต่างๆ ทำให้สามารถสรุปได้ดังนี้

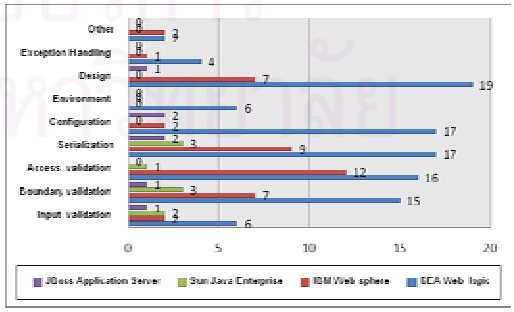
ผลิตภัณฑ์กลุ่มที่มีจุดอ่อนมากที่สุดได้แก่ แอพพลิเคชั่นประเภทเครื่องมือสนับสนุนการให้บริการ(450 รายการซีวีอี) เนื่องจากแอพพลิเคชั่นประเภทนี้เป็นกลุ่มเครื่องมือที่รองรับการบริการแก่ผู้ใช้เป็นจำนวนมาก สามารถเข้าถึงได้โดยง่ายผ่านช่องทางอินเตอร์เน็ต ที่เปรียบเสมือนเป็นที่สาธารณะที่เป็นที่รู้จักของบุคคลทั่วไปรวมไปทั้งผู้ที่ไม่หวังดีต่อระบบ อีกทั้งการโจมตีไปยังแอพพลิเคชั่นประเภทนี้ยังส่งผลกระทบต่อการให้บริการและการทำงานของผู้ใช้งานเป็นจำนวนมากกว่าแอพพลิเคชั่นแบบเครื่องมือช่วยการพัฒนา (57 รายการซีวีอี)

ประเภทจุดอ่อนที่พบมากที่สุดและเป็นช่องทางที่ใช้ในการโจมตีระบบได้แก่ จุดอ่อนที่เกิดจากความผิดพลาดของการเหลื่อมล้ำของการตรวจสอบสิทธิ และประเภทจุดอ่อนที่พบน้อยที่สุดคือ ประเภทจุดอ่อนอื่นๆ ซึ่งผลลัพธ์แสดงคะแนนรวมไว้ในรูปที่ 1 และแสดงคะแนนแยกตามประเภทของจุดอ่อนและผลิตภัณฑ์ในรูปที่ 2

รูปที่ 1: คะแนนรวมทั้งหมดแยกตามประเภทของจุดอ่อน



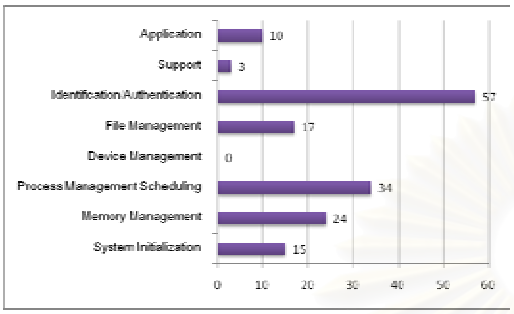
รูปที่ 2: คะแนนแยกตามประเภทของจุดอ่อนและผลิตภัณฑ์



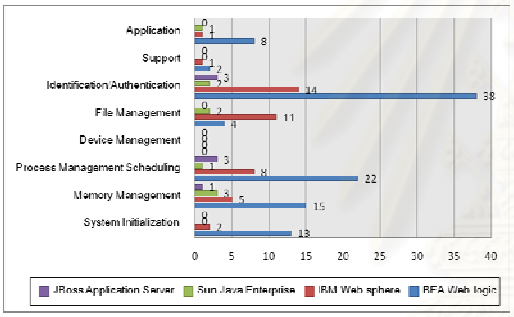
จุดที่มักพบจุดอ่อน ได้แก่ จุดอ่อนที่เกิดจากส่วนการพิสูจน์ตัวตน รองลงมาคือจุดอ่อนที่พบในส่วนการจัดการการประมวลผล และจุดที่พบ

จุดอ่อนน้อยที่สุดคือ ส่วนการจัดการอุปกรณ์ ซึ่งผลลัพธ์คะแนนรวมแสดงไว้ในรูปที่ 3 และแสดงคะแนนแยกตามจุดที่เกิดจุดอ่อนและผลิตภัณฑ์ในรูปที่ 4

รูปที่ 3: คะแนนรวมทั้งหมดแยกตามจุดที่เกิดจุดอ่อน

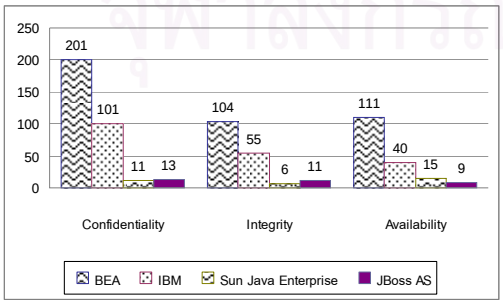


รูปที่ 4: คะแนนแยกตามจุดที่เกิดจุดอ่อนและผลิตภัณฑ์

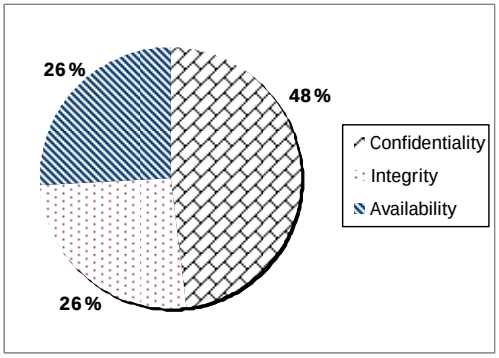


ลักษณะความเสียหายที่ได้รับคะแนนความเสียหายมากที่สุดคือ การรักษาความลับ รองลงมาคือ การส่งผลต่อสภาพพร้อมใช้งานและความเสียหายที่ส่งผลต่อบูรณภาพตามลำดับ ซึ่งผลลัพธ์แสดงไว้ในรูปที่ 5 และ รูปที่ 6

รูปที่ 5: แสดงคะแนนรวมความเสียหายของแต่ละผลิตภัณฑ์



รูปที่ 6: แสดงความเสียหายจุดอ่อนผลิตภัณฑ์ทั้งหมด



7. สรุป

จากจำนวนรายการจุดอ่อนทั้งหมด 507 รายการ เมื่อเปรียบเทียบจำนวนรายการจุดอ่อนของเครื่องมือช่วยการพัฒนาจำนวน 57 รายการ คิดเป็น 11.24 % และจำนวนรายการจุดอ่อนของเครื่องมือสนับสนุนการให้บริการจำนวน 450 รายการ คิดเป็น 88.76 % เป็นตัวบ่งชี้ว่าจุดอ่อนที่มักพบส่วนใหญ่ในการพัฒนาเว็บเซอร์วิสจะเกิดที่เครื่องมือสนับสนุนการให้บริการมากกว่า ซึ่งตัวเลขนี้สามารถใช้เป็นข้อมูลพื้นฐานในการติดตั้งหรือปรับแต่งเพื่อเสริมความแข็งแกร่งของระบบเว็บเซอร์วิสได้

ผลลัพธ์จากการประเมินจุดอ่อนของผลิตภัณฑ์เว็บเซอร์วิสที่นำเสนอในงานวิจัยนี้ผลของค่าคะแนนจุดอ่อนของการประเมินที่ได้มีดังนี้ BEA Web Logic 416 คะแนน ,IBM Web Spare 196 คะแนน ,JBoss As 33 คะแนน และ Sun JAVA Enterprise 32 คะแนน ซึ่งคะแนนที่ได้ทั้งหมดจากการประเมินสามารถนำไปใช้ในการเลือกและเปรียบเทียบผลิตภัณฑ์เว็บเซอร์วิสที่มีความปลอดภัยเหมาะสมในการใช้งานกับองค์กร พร้อมทั้งนำค่าคะแนนความเสียหายของแต่ละรายการซีวีอีไปวิเคราะห์ในการหาวิธีเสริมความแข็งแกร่งของจุดอ่อนที่พบในผลิตภัณฑ์ เพราะผู้ดูแลระบบจะได้ทราบว่าจุดอ่อนใดก่อความเสียหายมากก็พิจารณาให้มีความสำคัญมาก และจุดอ่อนใดมีคะแนนความเสียหายน้อยลงมาก็พิจารณาให้มีความสำคัญน้อยลง

มาเช่นกัน เพื่อใช้เป็นลำดับขั้นในการปรับแต่งเสริมความแข็งแกร่งให้กับผลิตภัณฑ์นั้นต่อไป

การใช้งานเว็บเซอร์วิสยังเป็นระบบที่ใหม่ต่อการใช้งาน การทำงานโดยรวมยังมีช่องโหว่และจุดอ่อนในผลิตภัณฑ์อยู่มากพอสมควร จึงต้องระมัดระวังเรื่องการถูกโจมตีและหาทางป้องกัน เช่น การลงซอฟต์แวร์แก้ไข (Patch) เพื่อปิดจุดอ่อนนั้น และหมั่นตรวจสอบการทำงานของระบบอยู่เสมอ เป็นต้น

8. กิตติกรรมประกาศ

งานวิจัยนี้เป็นส่วนหนึ่งของโครงการการวิศวกรรมซอฟต์แวร์แผนใหม่สำหรับวิสาหกิจโดยสถาปัตยกรรมเชิงบริการ (ระยะที่ 2) โดยได้รับการสนับสนุนจากสำนักงานส่งเสริมอุตสาหกรรมซอฟต์แวร์แห่งชาติ (องค์การมหาชน)

9. เอกสารอ้างอิง

[1] Get CVE [Online], Available from: http:// www.cve.mitre.org/cve [2006, December 5]

[2] Wita R, Teng-Amnuay Y. Vulnerability, Profile for Linux, IEEE, 2005.

[3] C. E. Landwehr, et al. A taxonomy of Computer Program security Flaws, ACM Computing Surveys (CSUR): ACM Press New York, NY, USA, 1994.

[4] รัศมีทิพย์ วิตา. การประเมินและเปรียบเทียบการป้องกันจุดอ่อนของระบบลินุกซ์โดยการเพิ่ม ความแข็งแกร่งกับการใช้แอลเอสเอ็ม. วิทยานิพนธ์ปริญญามหาบัณฑิต, ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย , 2003.

[5] เกียรติ ภิรมย์โสภา. การประเมินความเสี่ยงเว็บเซิร์ฟเวอร์โดยการจำแนกระดับผลกระทบของความเสียหาย. วิทยานิพนธ์ปริญญามหาบัณฑิต ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2004.

[6] Jeongseok S, Han-Sung K, Sanghyun C, Sungdeok C. Web server attack categorization Based on root causes and their locations, Proceedings of International Conference on Information Technology, Coding and Computing (ITCC 2004), 2004.

[7] UDDI Products and Components [Online]. Available from: http://uddi.org/solutions.html [2007, January 15].

[8] Web Services Development[Online]. Available from : http://searchwebservices.techtarget.com [2006, December 5].

ประวัติผู้เขียนวิทยานิพนธ์

นายกิตติศักดิ์ นิทาน เกิดเมื่อวันที่ 13 กุมภาพันธ์ พ.ศ. 2524 เรียนจบการศึกษาระดับปริญญาบัณฑิตที่มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา ในคณะครุศาสตร์ สาขาวิชาคอมพิวเตอร์ศึกษาในปี พ.ศ. 2547 และเข้าศึกษาต่อในหลักสูตรวิทยาศาสตร์มหาบัณฑิต ที่ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เมื่อ พ.ศ. 2549