การประเมินช่องโหว่ระบบงานทะเบียนโดยใช้โปรแกรมประยุกต์ Kali Linux V. 2022.1 ร่วมกับเทคนิคการป้องกันการคุกคามสิทธิ์การเข้าถึงข้อมูล

Vulnerability Assessment of Registration System Using Kali Linux V. 2022.1 with Information Disclosure Method

ศิลป์ณรงค์ ฉวีพัฒน์*

Silnarong Chavipat

เจริญ จิระราชวโร**

Charoen Jiraratchwaro

Received : April 19, 2023

Revised : June 26, 2023

Accepted : June 29, 2023

บทคัดย่อ

งานวิจัยการประเมินช่องโหว่ระบบงานทะเบียนโดยใช้โปรแกรมประยุกต์ Kali Linux V. 2022.1 ร่วมกับเทคนิคการป้องกันการคุกคามสิทธิ์การเข้าถึงข้อมูลฉบับนี้ได้ทำการศึกษาวิจัยเกี่ยวกับช่องโหว่ของระบบงานทะเบียนตัวอย่าง โดยมีวัตถุประสงค์ของการศึกษาวิจัยเพื่อทดสอบระบบดังนี้ 1) ตรวจสอบค้นหาความเสี่ยงที่จะถูกโจมตีจากภายนอกระบบ โดยใช้โปรแกรมประยุกต์ Kali linux V. 2022.1 ร่วมกับเทคนิค Information Disclosure 2) ระบุความเสี่ยงของช่องโหว่ที่อาจจะส่งผลให้เกิดภัยคุกคามทางด้านความมั่นคงปลอดภัย 3) ประเมินความความรุนแรงช่องโหว่ที่พบนั้น โดยอ้างอิงตามมาตรฐาน ของ Open Web Application Security Project - OWASP Top 10 ประจำปี 2564 ในการวิจัยได้ใช้เครื่องมือที่ประกอบไปด้วย เครื่องคอมพิวเตอร์พกพาที่ใช้หน่วยประมวลผล Core I7 หน่วยความจำหลักขนาด 32 GB หน่วยความจำสำรองขนาด 512 GB ติดตั้งระบบปฏิการวินโดว์ 10 และโปรแกรมจำลองเครื่องเสมือน Visual BoX ที่ติดตั้งระบบปฏิบัติการ KALI Linux V. 2022.1 ซึ่งแบ่งขั้นตอนในการประเมินช่องโหว่ของระบบเป็น 4 ขั้นตอน ประกอบด้วย 1) Planning 2) Information Gathering 3) Vulnerability Assessment 4) Reporting ผลการวิจัยในช่วงวันที่ 12-18 พฤษภาคม 2565 ตรวจพบช่องโหว่ของระบบงานทะเบียนที่ศึกษา รวมทั้งหมดจำนวน 7 รายการโดยเป็น

*อาจารย์ประจำโปรแกรมวิชาเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์และเทคโนโลยีมหาวิทยาลัยราชภัฏกำแพงเพชร
Lecturer in Information Technology Program Faculty of Science and Technology Kamphaeng Phet Rajabhat University e-mail: silnarong@kpru.ac.th

**นักวิชาการอิสระ
Independent scholar

ช่องโหว่ที่มีความเสี่ยงสูงจำนวน 3 รายการ ได้แก่ ช่องโหว่ Unauthorized Access Data (Missing Function Level Access Control) ช่องโหว่ Weak cipher suite algorithm และช่องโหว่ Username Password via GET Method ช่องโหว่ที่มีความเสี่ยงสูงปานกลางจำนวน 3 รายการ ได้แก่ ช่องโหว่ jQuery old version ช่องโหว่ HTTP Method Allowed และช่องโหว่ Application Technical Error And Information Disclosure และช่องโหว่ที่มีความเสี่ยงระดับต่ำ 1 ช่องโหว่ ได้แก่ ช่องโหว่ Missing Basic Function หลังจากกระบวนการรายงานผลช่องโหว่ได้ทำการแก้ไขโดยปรับปรุงวิธีการ และปรับปรุงเวอร์ชัน ที่ใช้ในการเขียนโปรแกรมและทำการทดสอบด้วยวิธีการเดิมผลที่ได้คือยังค้นพบช่องโหว่ความเสี่ยงระดับต่ำจำนวน 1 รายการ ในการหาช่องโหว่และการประเมินความเสี่ยงของระบบที่ศึกษานั้น มีความน่าเชื่อถืออยู่ในระดับที่ไม่น้อยไปกว่าการประเมินในลักษณะเดียวกับงานศึกษาวิจัยอื่น โดยโปรแกรมประยุกต์ที่ใช้งานนั้นได้รับการพัฒนาและอัพเดทเวอร์ชันการใช้งานอย่างต่อเนื่องจนมีความสามารถที่จะตรวจจับความผิดปกติของระบบได้อย่างแม่นยำกว่าโปรแกรม Aacunetix ในลักษณะเดียวกันกับงานศึกษาอื่นในอดีต (พัชรวัฒน์ และชัยพร, 2563; ณัชณภัทร และชัยพร, 2560)

คำสำคัญ : ช่องโหว่ / ความมั่นคงปลอดภัย / ระบบทะเบียน / ซีวีเอสเอส

ABSTRACT

The research of Vulnerability Assessment of Registration System Using Kali Linux V. 2022.1 with Information Disclosure Method had studied the case study of registration system that might risk from the discloser technic The main objectives of this study were 1) To Experiment the risk from external invader using Kali linux V. 2022.1 combined with information disclosure technic 2) To analyze the vulnerable which affect to the security system of interested system and 3) To evaluate the risk level of the registration system under the standard of Open Web Application Security Project – OWASP Top 10 in 2021. In the experiments, the portable computer with core i7 microprocessor with memory of 32 Gb, portable memory of 512 Gb was used. The portable was installed the Windows version 10 and visual program of Visual Box on KALI Linux V. 2022.1 software. The research procedures were comprised of 1) Planning 2) Information Gathering 3) Vulnerability Assessment 4) Reporting. The investigated results from May12 – 18, 2022, showed the case study had total 7 vulnerabilities. There are 3 of them were severe level, they are Unauthorized Access Data (Missing Function Level Access Control), Weak cipher suite algorithm and Username Password via GET Method. For the moderate level was found 3 vulnerabilities, jQuery old version, HTTP Method Allowed and Application Technical Error and Information Disclosure. The remaining was Information level, Missing Basic

Function. Moreover, after reported the result and improved the method including of software version updated, the repeating experiment found another information level vulnerable. The result of vulnerability assessment and risk evaluation of case study showed that the results had the reliability not less than the other software due to the development and version update of using software. The continuously version updated of software had more accuracy for the abnormalities validation compare to the software of Aacunetix that used in the past studied. (Patcharawat & Chaiyaporn, 2020; Nathanaphat & Chaiyaphon, 2017)

Keywords : Vulnerability / Security / Registration System / CVSS

บทนำ

ด้วยความก้าวหน้าของระบบการสื่อสารและเทคโนโลยีสารสนเทศในปัจจุบันมีความทันสมัยและเติบโตอย่างรวดเร็ว ทำให้บุคคลทั่วไปสามารถเข้าถึงระบบสารสนเทศของหน่วยงานได้ ทั้งจากบุคคลที่ใช้งานทั่วไปและบุคคลที่มุ่งประสงค์ร้ายต่อระบบ และโดยเฉพาะอย่างยิ่งการเกิดภาวการณ์ที่ระบบสารสนเทศจะถูกโจมตี และการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ที่มีแนวโน้มเพิ่มมากขึ้นในปัจจุบัน และในส่วนของประเทศไทยได้หน่วยงานภาครัฐและหน่วยงานที่เกี่ยวข้องได้ให้ความสำคัญของข้อมูลส่วนบุคคล จึงได้มีการตราพระราชบัญญัติที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ 2562 และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ระบบงานทะเบียนนักศึกษาเป็นระบบสารสนเทศสำหรับการให้บริการแก่นักศึกษามหาวิทยาลัยราชภัฏแห่งหนึ่ง มีความสำคัญและความจำเป็นอย่างยิ่งสำหรับใช้การตรวจสอบข้อมูลผลการเรียนขอและข้อมูลสารสนเทศอื่นๆ ที่จำเป็นสำหรับนักศึกษา อาจารย์ โดยเฉพาะในแง่ของการยกระดับการเป็นมหาวิทยาลัยดิจิตอล ตามแนวทางส่งเสริมและพัฒนาระบบเทคโนโลยีดิจิตอลเพื่อการศึกษาของมหาวิทยาลัยในอนาคต

ดังนั้น ผู้วิจัยจึงมีแนวความคิดที่จะทำการค้นหาและวิเคราะห์ช่องโหว่ (Vulnerability Assessment) ระบบงานทะเบียนนักศึกษา ของมหาวิทยาลัยราชภัฏแห่งหนึ่ง เพื่อค้นหาช่องโหว่จากเครือข่ายภายนอกของมหาวิทยาลัย (External Network) โดยในงานวิจัยนี้ จะทำการศึกษาผลกระทบและระดับความรุนแรงที่ส่งผลต่อการทำงานของระบบงานทะเบียนนักศึกษา และหาแนวทางป้องกันเพื่อลดความเสี่ยง ภัยคุกคามจากผู้ที่ไม่หวังดี และภัยคุกคามทางไซเบอร์ เพื่อเป็นแนวทางในการพัฒนาให้ระบบทะเบียนนักศึกษามีความมั่นคงปลอดภัยและมีความน่าเชื่อถือในการให้บริการ และให้ผู้ที่เกี่ยวข้องในการดูแลระบบระบบงานทะเบียนนักศึกษาตลอดจนผู้ดูระบบสารสนเทศในหน่วยงานต่างๆ ของมหาวิทยาลัยได้มีแนวทางในการประเมินช่องโหว่ระบบสารสนเทศของตนเองในเบื้องต้นได้ สามารถรับมือป้องกันภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ ได้อย่างทันท่วงที และยังเป็นแนวทางในการนำไปใช้ในการปรับปรุงระบบสารสนเทศของงานของตนเองให้มีความมั่นคงปลอดภัยเพิ่มขึ้นได้

วิธีดำเนินการวิจัย

ช่องโหว่หรือจุดอ่อน (Vulnerability) หมายถึง ช่องทางที่อาจถูกใช้สำหรับการโจมตีได้ (พัชรวัฒน์ และชัยพร, 2563) โดยผู้วิจัยได้กำหนดขอบเขตในการวิจัยและเครื่องมือที่ใช้ในการทดลองดังนี้

1. การศึกษาช่องโหว่จะทำการทดสอบจากเครือข่ายภายในมหาวิทยาลัย (Internal Network)

2. การศึกษาช่องโหว่ของระบบงานทะเบียนนักศึกษานี้จะใช้ทักษะของผู้วิจัย และใช้ Tool ในการตรวจหาช่องโหว่เท่านั้นไม่มีบุคคลที่สามหรือบุคคลภายนอกเข้ามาเกี่ยวข้องในการวิจัย

3. การศึกษาช่องโหว่ของระบบงานทะเบียนนักศึกษานี้ ดำเนินการวิจัยโดยการอ้างอิง Open Web Application Security Project - OWASP Top 10 ซึ่งเป็นมาตรฐานที่ได้รับการยอมรับการอย่างแพร่หลาย (Urshila & Raghu, 2022)

4. การศึกษาช่องโหว่ของระบบงานทะเบียนนักศึกษา มีการสรุปรายงานผลการตรวจสอบและประเมินความมั่นคงปลอดภัยของการเจาะระบบ โดยชี้ให้เห็นถึงจุดอ่อน ระดับความเสี่ยง และข้อแนะนำในการปรับปรุงระบบ เพื่อเพิ่มความมั่นคงปลอดภัยของระบบระบบงานทะเบียนนักศึกษา

-เมนูที่ทำการตรวจสอบ	-หน้าจอ Login	-ข้อมูลอาจารย์
-ข้อมูลผู้ใช้	-ติดต่ออาจารย์/นักศึกษา	-ข้อมูลผู้ลงนาม
-ข้อมูลงานประมวลผล	-ข้อมูลสอบคอมพิวเตอร์	-ข้อมูลยืนขอสำเร็จ
-ข้อมูลนักศึกษา	-ข้อมูลเปิดระบบต่างๆ	-ข้อมูลใบรับรอง
-ข้อมูลตารางเรียน	-ข้อมูลการชำระเงิน	-ข้อมูลไฟล์ดาวน์โหลด
-ข้อมูลลงทะเบียนเรียน	-ข้อมูลรายงาน	-Lock Screen
-โอนข้อมูลลงทะเบียนตามประเภทนักศึกษา		

5. การศึกษาช่องโหว่ของระบบงานทะเบียนนักศึกษา จะทำการตรวจสอบเมนู Function ต่างๆ ดังนี้

โดยเครื่องมือที่ใช้ในการวิจัยประกอบไปด้วย เครื่องคอมพิวเตอร์พกพาที่ใช้หน่วยประมวลผล Core I7 หน่วยความจำหลักขนาด 32 GB หน่วยความจำสำรองขนาด 512 GB ติดตั้งระบบปฏิการวินโดว์ 10 และโปรแกรมจำลองเครื่องสเมือน Visual Box ที่ติดตั้งระบบปฏิบัติการ KALI Linux Version 2022.1

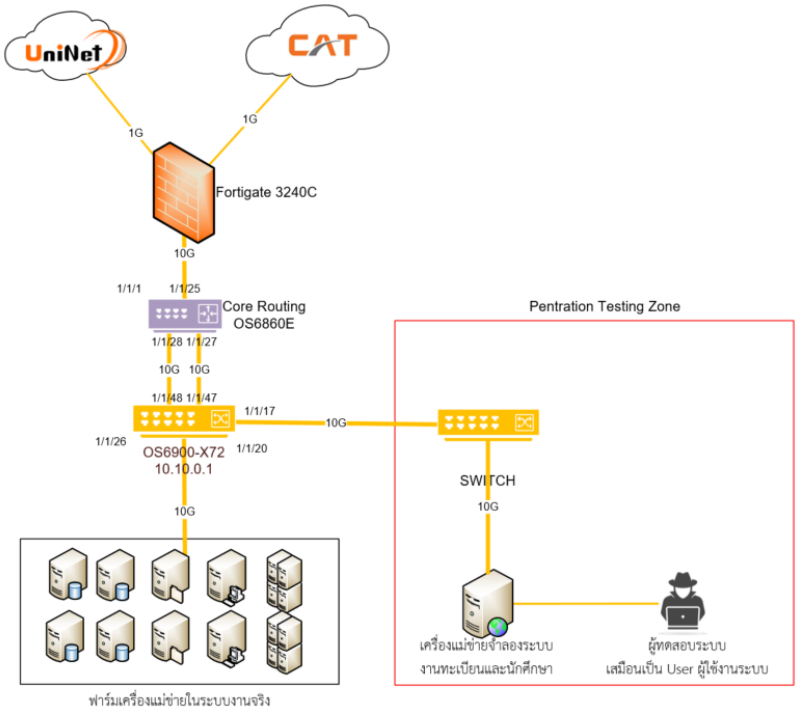
ขนาดกรอบแนวคิดการวิจัย

ภาพที่ 1 กรอบแนวคิดของงานวิจัย

ผู้วิจัยได้ทำการออกแบบขั้นตอนและเครื่องมือในงานวิจัยประกอบด้วย

1. การวางแผนก่อนการดำเนินการ (Planning)

ผู้วิจัยได้กำหนดขอบเขตเป้าหมายในการทดสอบด้านความมั่นคงปลอดภัย (Security Testing) ร่วมกับสำนักส่งเสริมและงานทะเบียน ที่เป็นเจ้าของระบบสารสนเทศ และงานพัฒนาระบบเครือข่าย สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกำแพงเพชร และดำเนินการทำหนังสือบันทึกข้อความ เพื่อขออนุญาตทำการทดสอบด้านความมั่นคงปลอดภัย (Security Testing) ตลอดจนการเก็บรวบรวมข้อมูลอื่นๆ ที่จำเป็นเช่น ผังระบบเครือข่ายมหาวิทยาลัย (Network Diagram) และข้อมูลของเครื่องแม่ข่าย โดยในการทดสอบผู้วิจัยได้ใช้วิธีการทำสำเนา (Clone) ระบบงานทะเบียนนักศึกษาจากระบบจริงขึ้นมาอีก 1 ระบบ เพื่อดำเนินการทดสอบการเจาะระบบ โดยผู้วิจัยได้กำหนดขอบเขตไว้ระหว่างช่วงเวลาที่ทำการประเมินรักษาความมั่นคงปลอดภัยของระบบงานทะเบียนนักศึกษา ระหว่างวันที่ 12 พฤษภาคม 2565 เวลา 01.00 น. - วันที่ 18 พฤษภาคม 2565 เวลา 13.00 น.ซึ่งเป็นช่วงวันปิดภาคเรียนมีผู้เข้าใช้บริการไม่มาก และเพื่อเป็นการลดผลกระทบกับผู้ใช้งานบนระบบเครือข่ายและด้านอื่นๆ โดยผู้วิจัยจะทำการทดสอบการเจาะระบบงานทะเบียนนักศึกษาที่ได้ติดตั้งบนเครื่องแม่ข่ายอีกหนึ่งเครื่อง ที่ไม่ได้เป็นเครื่องที่ใช้งานจริงในระบบ ซึ่งผู้วิจัยจะทำการเก็บข้อมูลที่ได้ระหว่างการทดสอบการเจาะระบบเป็นความลับ และจัดส่งรายงานที่ได้หลังการทดสอบส่งกลับไปให้สำนักส่งเสริมและงานทะเบียนที่เป็นผู้ดูแลรับผิดชอบ ได้พิจารณาและดำเนินการแก้ไขปรับปรุงระบบให้มีความมั่นคงปลอดภัยมากขึ้นต่อไป



ภาพที่ 2 แสดงผังการเชื่อมต่อระบบเครือข่าย (Network Diagram) ที่ใช้ในการทดสอบ

2. การดำเนินการค้นหาช่องโหว่ของระบบ (Discovery)

ในขั้นตอนการค้นหาหรือตรวจหาช่องโหว่นี้ ผู้วิจัยได้ทำการติดตั้งเครื่องแม่ข่ายและทำสำเนา (Clone) ระบบงานทะเบียนนักศึกษาขึ้นมาอีก 1 ระบบ เพื่อให้การวิจัยครั้งนี้ ไม่มีการรบกวนหรือส่งผลกระทบก่อให้เกิดความเสียหายต่อระบบที่ใช้งานจริง และการทดสอบด้านความมั่นคงปลอดภัย (Security Testing) ในงานวิจัยนี้ จะทำการทดสอบผ่านระบบเครือข่ายภายในของมหาวิทยาลัยเท่านั้น ซึ่งผู้วิจัยนั้นเปรียบเสมือนเป็นผู้ใช้งานคนหนึ่งในระบบที่สามารถเข้าถึงระบบสารสนเทศดังกล่าวได้

ภาพที่ 3 การเข้าถึงเครื่องแม่ข่ายที่ได้ติดตั้งระบบงานทะเบียนนักศึกษา

การค้นหาช่องโหว่ของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานทะเบียนนักศึกษาโดยใช้ระบบปฏิบัติการ Kali Linux ที่ได้รับความนิยม (เอกชัย พ่วงพรพิทักษ์, 2565) และเครื่องมือ (Tool) ใช้ในการค้นหาช่องโหว่ของระบบต่างดังนี้

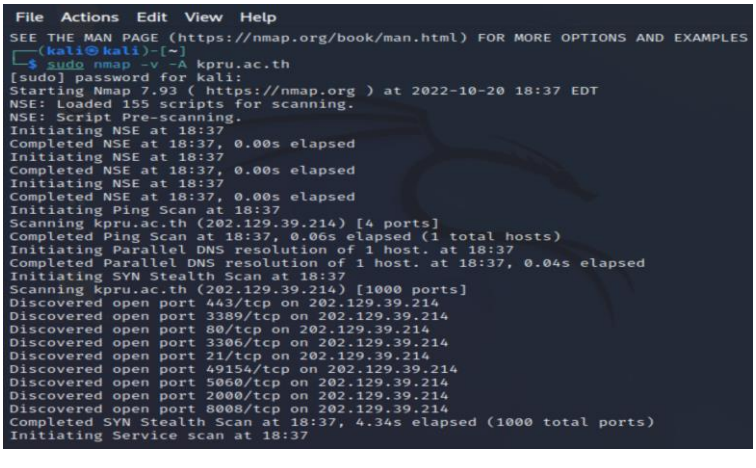
- Information Gathering
- Foot printing
- Port and Vulnerability Scanning
- Passive, Active Sniffing

- Privilege Escalation Attack -Exploit Attack
- Buffer Overflow
- Parameter Tampering Manipulation and Unsecure Configuration Attack
- Authentication Authorization and Accounting
- Cache Management Attack - Man in the Middle Attack
- Data Validation -Injection Flaws
- Cross Site Scripting -Insecure Direct Object Reference
- Error Handling -Broken and Bypass Authentication
- Session Management and Hijacking
- Unauthorized Access and Broken Access Control Attack

3. การเก็บรวบรวมข้อมูลเครื่องเป้าหมาย (Information Gathering)

โดยผู้วิจัยเริ่มต้นในการใช้เครื่องมือประเภท Information Gathering โดยใช้ Tool ที่ชื่อว่า Nmap (Network Mapper) เป็น free license และเป็น open source ทำหน้าที่ในการค้นหาเครือข่ายเป้าหมายและใช้ตรวจสอบความมั่นคงปลอดภัยของเครือข่ายและค้นหาเครื่องเป้าหมายเพื่อค้นหาและเก็บข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Extosoft company, 2563) ที่ให้บริการระบบงานทะเบียนของระบบงานทะเบียนนักศึกษา

จากการ Scan ด้วย Tool Namp ทำให้ผู้วิจัยได้ทราบถึงข้อมูลของระบบบางส่วนได้ว่าเครื่องเป้าหมายใช้ระบบปฏิบัติการใดในการทำงาน มีหมายเลขพอร์ตใดที่เปิดใช้งานอยู่ รวมไปถึงการค้นหาอุปกรณ์ที่กำลังทำงานอยู่ในระบบเครือข่าย



ภาพที่ 4 การใช้ระบบปฏิบัติการ Kali Linux สแกน (Scan) หาข้อมูลด้วยคำสั่ง Nmap

4. การค้นหาช่องโหว่ (Vulnerability Assessment)

จากการศึกษาผู้วิจัยสามารถค้นพบช่องโหว่ ซึ่งปรากฏรายละเอียดโหว่โดยมีรายละเอียดดังต่อไปนี้

4.1 ช่องโหว่ Unauthorized Access Data (Missing Function Level Access Control)

ช่องโหว่นี้ทำให้ผู้ใช้งานทั่วไปสามารถทำการ Query ข้อมูลได้โดยไม่ต้องทำการ Loginในระบบ และระบบไม่มีการตรวจสอบสิทธิการใช้งานว่าผู้ใช้งานนั้นมีสิทธิใช้งานหรือไม่ ตัวอย่างเช่น

https://test.kpru.ac.th/FrontEnd_Tabian/payment/updatestatust/122/2
https://test.kpru.ac.th/FrontEnd_Tabian/register/trainingmaterial/1/1/2559
https://test.kpru.ac.th/FrontEnd_Tabian/load/SearchLoad/5413211/1/2558
https://test.kpru.ac.th/FrontEnd_Tabian/teacher/ShowListSentGrade/1/1/59/1/
https://test.kpru.ac.th/FrontEnd_Tabian/teacher/ShowListAvgStudent/541321
https://test.kpru.ac.th/FrontEnd_Tabian/teacher/showregis/1/2
https://test.kpru.ac.th/FrontEnd_Tabian/teacher/showfinish/2/5413

ภาพที่ 5 ภาพแสดงการ Query ข้อมูลได้โดยไม่ต้องทำการ Login

4.2 ช่องโหว่ Weak cipher suite algorithm

ช่องโหว่นี้ที่เกิดจากเครื่องคอมพิวเตอร์แม่ข่ายใช้งาน SSL/TLS โดยมีการใช้ Cipher Suite ที่ไม่แข็งแกร่งมากพอ ก่อให้เกิดช่องโหว่ที่จะนำไปสู่การโจมตีแบบคนที่อยู่ตรงกลาง (Man-in-The-Middle Attack) ทำให้ผู้ที่โจมตีสามารถดักจับและอ่านข้อมูลที่ถูกเข้ารหัสได้ ช่องโหว่ดังกล่าวผู้วิจัยได้ทำการตรวจสอบจากเว็บไซต์

https://www.ssllabs.com/ssltest/analyze.html?d=test.kpru.ac.th&s=202.29.15.220

https://www.ssllabs.com/ssltest/analyze.html?d=test.kpru.ac.th

4.3 ช่องโหว่ Username Password via GET Method

เป็นช่องโหว่ที่ผู้ใช้งานส่งข้อมูล Username Password ด้วยวิธีการ Get Method ดังภาพที่ 6

GET /FrontEnd_Tabian/login/LoginsAdminTabian/tabian_test002/TC00001/fed7b893-ef02-4af0-bed6-fac1b7280ce9 HTTP/1.1

Host: test.kpru.ac.th

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0

Accept: application/json, text/plain, */*

Accept-Language: th,en-US;q=0.7,en;q=0.3

Accept-Encoding: gzip, deflate, br

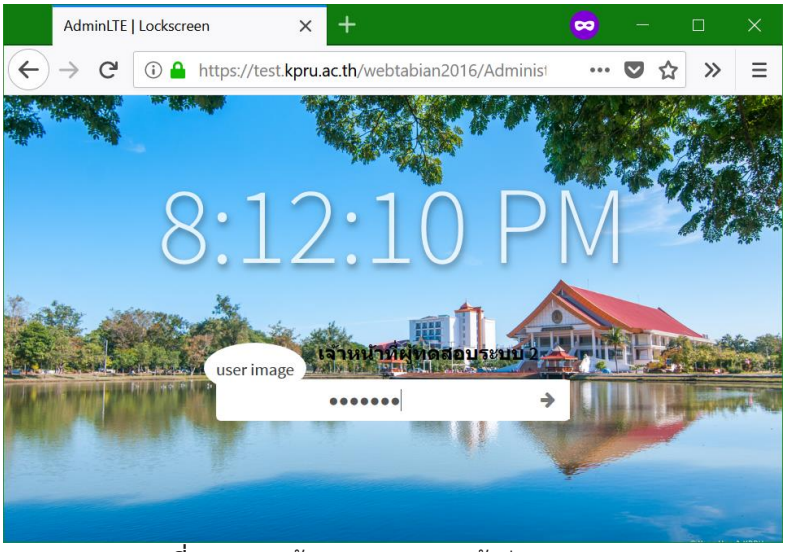
Referer: https://test.kpru.ac.th/webtabian2016/Administrator/lockscreen.html

DNT: 1

Connection: close

ภาพที่ 6 แสดงรายละเอียดช่องโหว่โดยใช้วิธีการ Get Method

โดยผู้วิจัยได้ทำการทดสอบการ Login โดยใส่ User Name จะพบว่ามีการส่ง Username Password ผ่าน GET Parameter



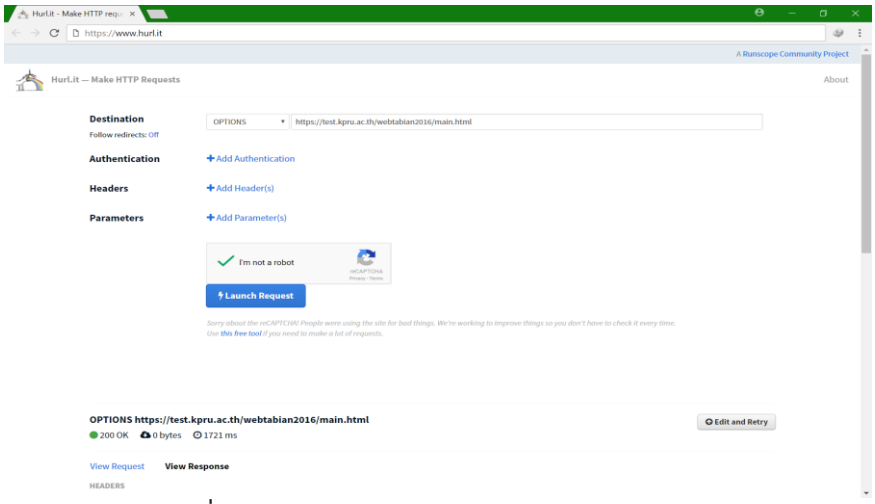
ภาพที่ 7 แสดงหน้าจอการ Login เข้าสู่ระบบ

4.4 ช่องโหว่ jquery old version

เป็นช่องโหว่ที่เกิดจากการใช้งาน Version ของ Jquery ที่ไม่มีความมั่นคงปลอดภัยมีผลกระทบทำให้ผู้ที่ไม่หวังดีสามารถเข้าถึงข้อมูลหรือฐานข้อมูลที่ไม่ได้รับอนุญาตได้ โดยสามารถตรวจสอบข้อมูลได้จากเว็บไซต์ https://domstorm.skepticfx.com/modules?id=529bbe6e125fac0000000003

4.5 ช่องโหว่ HTTP Method Allowed

เป็นช่องโหว่ที่ทำให้เครื่องแม่ข่ายทำงานผิดพลาดส่งผลให้สามารถแสดงข้อมูลสำคัญที่ไม่ได้อนุญาตให้บุคคลภายนอกเข้าถึงได้ ดังนั้นจึงควรอนุญาตให้เครื่องแม่ข่ายใช้งานเฉพาะ Method ที่จำเป็นเช่น GET, POST ไม่ควรอนุญาตให้ใช้งาน Method อื่นๆ ที่ไม่จำเป็นเช่น OPTIONS, TRACR และ HEAD โดยสามารถตรวจสอบข้อมูลได้จาก https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)



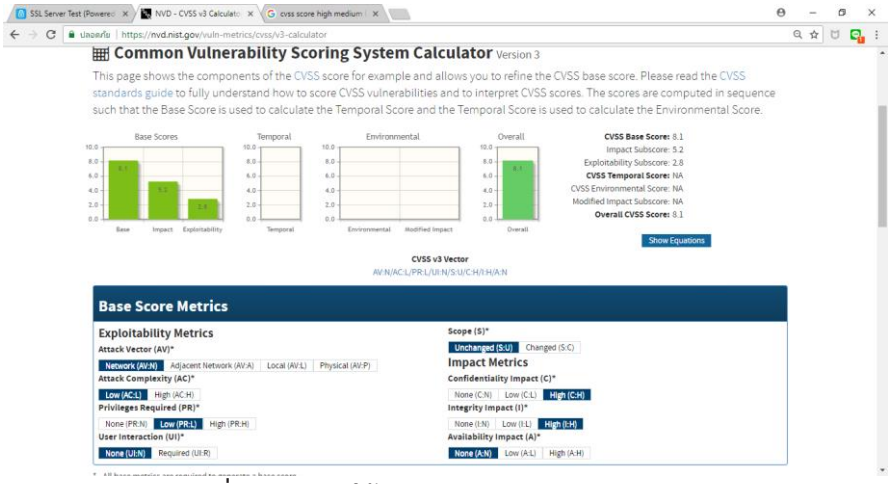
ภาพที่ 8 แสดงผลลัพธ์ของการใช้ Method ในรูปแบบต่างๆ

4.6 ช่องโหว่ Application Technical Error And Information Disclosure

เป็นช่องโหว่ที่เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานทะเบียนแสดงรายละเอียดข้อมูล Error Message ที่มีโอกาสทำให้เกิดการทำงานผิดพลาดหรือแสดงผลข้อมูลสำคัญ ที่ไม่อนุญาตให้บุคคลภายนอกเข้าถึงออกมาได้ เช่น Path Directory C:\inetpub\wwwroot ซึ่งทำให้ผู้ที่ไม่หวังดี สามารถนำข้อมูลที่ได้รับไปวิเคราะห์เพื่อหาช่องโหว่ในการเจาะระบบต่อไปได้ โดยวิธีการตรวจสอบ สามารถตรวจสอบรายละเอียดได้จากการใส่ข้อมูลผิด หรือข้อมูลที่ไม่ได้กำหนดไว้ แล้วสังเกต Error ที่ Website ตอบกลับมาว่าเป็น Error ที่เหมาะสมกับผู้ใช้งานทั่วไปหรือไม่

5. การจัดทำรายงานผลและการประเมินผล (Report)

ผู้วิจัยได้จัดทำรายงานผลการประเมินช่องโหว่และแนวทางในการแก้ไขและการป้องกันช่องโหว่ของระบบให้กับผู้บริหารและผู้ที่เกี่ยวข้องได้นำไปแก้ไขต่อไปและจัดทำข้อมูลสรุปคะแนนระดับความเสี่ยงโดยใช้เกณฑ์มาตรฐานซีวีเอสเอส (CVSS) ซึ่งเป็นระบบการให้คะแนนช่องโหว่ที่เป็นมาตรฐานเปิดที่ใช้กันอย่างแพร่หลายทั่วโลก (ศิริขวัญ, 2559) ใช้ในการวัดความรุนแรงของช่องโหว่ของซอฟต์แวร์ตามค่าเมตริกที่กำหนด (Mera, et al, 2021) เวอร์ชัน 3 ซึ่งระดับคะแนนซีวีเอสเอส (CVSS) จะแสดงให้เห็นถึงความรุนแรงที่มีผลกระทบต่อความมั่นคงของระบบงานทะเบียนนักศึกษา สามารถเข้าไปใช้งานได้ที่ Website https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator โดยทำการระบุค่าตัวแปรต่างๆ ตามภาพที่ 9



ภาพที่ 9 แสดงการใช้งานระดับคะแนนซีวีเอสเอส (CVSS)

หลักเกณฑ์การให้คะแนน Common Vulnerability Scoring System (CVSS) มีหลักการคิดคำนวณได้จาก 3 องค์ประกอบได้แก่

1. Base Score (คะแนนฐาน) - เป็นการประเมินระดับความรุนแรงของช่องโหว่ โดยอาศัยการใช้รายละเอียดทางเทคนิคของช่องโหว่ ที่ประกอบไปด้วย Exploit Metric และ Impact Metrics และสามารถอธิบายรายละเอียดของแต่ละประเภทได้ดังต่อไปนี้

1.1 Exploit Metrics หรือ ความรุนแรงของช่องโหว่ ประกอบไปด้วย Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR), User Interaction (UI) และ Scope (S)

1.2 Impact Metrics หรือ ความรุนแรงของผลกระทบที่เกิดขึ้น ประกอบไปด้วย Confidentiality Impact (C), Integrity Impact (I) และ Availability Impact (A)

ภาพที่ 10 การคำนวณคะแนนฐาน (Base Score)

2. Temporal Score (คะแนนชั่วคราว) - เป็นการประเมินความรุนแรงของช่องโหว่ โดยพิจารณาปัจจัยสภาพแวดล้อม โดยมีส่วนประกอบดังต่อไปนี้

2.1 Exploit Code Maturity (E)

- Unproven (ไม่มีหลักฐาน): ไม่มีหลักฐานให้สรุปว่าช่องโหว่ถูกโจมตี
- Proof of Concept (มีหลักฐานประกอบ): มีหลักฐานแสดงให้เห็นว่าช่องโหว่สามารถถูกโจมตีได้
- Functional (ความสามารถในการใช้งานได้): ช่องโหว่สามารถใช้งานได้แต่จำเป็นต้องมีความชำนาญและความรู้เฉพาะเจาะจง
- High (สูง): ช่องโหว่สามารถใช้งานได้โดยมีความสะดวก
- Not Defined (ไม่ได้กำหนด): ไม่ได้กำหนดระดับความชัดเจนของการโจมตี

2.2 Remediation Level (RL)

- Official Fix (แก้ไขอย่างเป็นทางการ): มีการออกเวอร์ชันแก้ไขปัญหาอย่างเป็นทางการ
- Temporary Fix: มีการให้คำแนะนำหรือวิธีการแก้ไขชั่วคราวในรอบรูปแบบ
- Workaround (วิธีการหลีกเลี่ยง): มีวิธีการที่ผู้ใช้งานสามารถหลีกเลี่ยงช่องโหว่ได้โดยไม่ต้องแก้ไขโดยตรง
- Unavailable (ไม่พร้อมใช้งาน): ไม่มีวิธีการแก้ไขหรือวัสดุที่ใช้ในการสร้างทดสอบ

2.3 Report Confidence (RC)

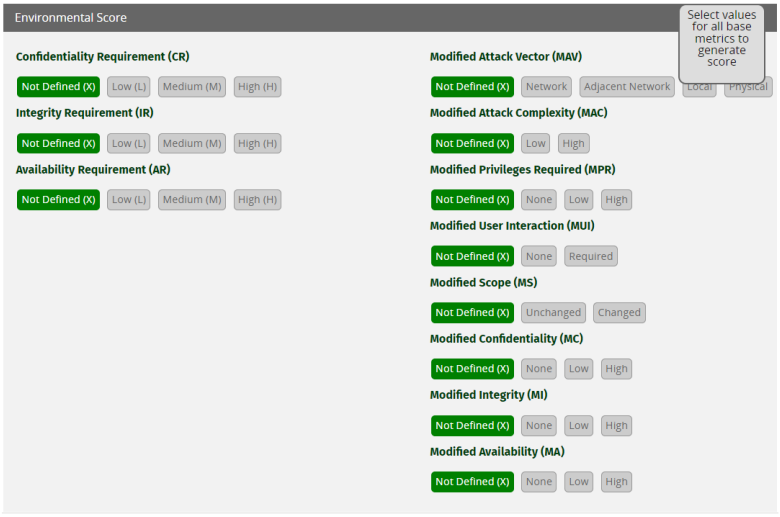
ภาพที่ 11 การคำนวณคะแนนชั่วคราว (Temporal Score)

3. Environmental Score (คะแนนด้านสภาพแวดล้อม) - เป็นการประเมินความรุนแรงของช่องโหว่ โดยพิจารณาปัจจัยสภาพแวดล้อมที่เฉพาะเจาะจงตามสถานการณ์ โดยมีองค์ประกอบดังต่อไปนี้

3.1 Exploiability Metrics - Attack Vector (MAV), Attack Complexity (MAC), Privileges Requires (MPR), User Interaction (MUI), Scope (MS)

3.2 Impact Metrics - Confidentiality Impact (MC), Integrity Impact (MI) และ Availability Impact (MA)

3.3 Impact Scuscore Modifiers - Confidentiality Requirement (CR), Integrity Requirement (IR) และ Availability Requirement (AR)



ภาพที่ 12 การคำนวณคะแนนด้านสภาพแวดล้อม (Environmental Score)

เมื่อบันทึกข้อมูลเสร็จเสร็จเป็นที่เรียบร้อย ระบบจะแสดงระดับคะแนน CVSS Score โดยที่ช่องโหว่ที่มีระดับความรุนแรงมาก จะทำให้ค่า CVSS Score ยิ่งมีค่ามากขึ้น โดยระดับคะแนน CVSS Score มีค่าระดับคะแนนสูงสุดระดับเท่ากับ 10 และระดับคะแนนต่ำสุด 0 เมื่อได้ค่าระดับคะแนน CVSS Score แล้วจะทำการแบ่ง ระดับความเสี่ยง (Risk Rating) ตามตารางด้านล่าง

ตารางที่ 1 แสดงระดับค่าความเสี่ยงกับระดับคะแนน CVSS Score

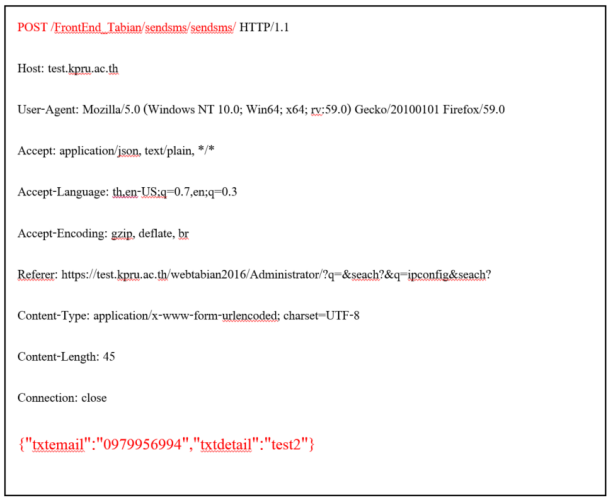
Rating	CVSS Score
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

ผลการวิจัย

ผลการวิจัยจากการทดสอบการประเมินช่องโหว่ระบบงานทะเบียนนักศึกษาผู้วิจัยได้ค้นพบช่องโหว่ระดับความรุนแรงและระดับคะแนนซีวีเอสเอส ของช่องโหว่ที่ค้นพบได้จำนวน 7 รายการดังนี้

1. ช่องโหว่ Unauthorized Access Data (Missing Function Level Access Control)

ระดับความรุนแรงอยู่ในระดับสูง (High) ระดับคะแนนซีวีเอสเอส (CVSS Score) 8 ผู้วิจัยพบว่าระบบงานทะเบียนนักศึกษา ไม่ได้ทำการ Authorization ของผู้เข้ามาใช้งาน จะมีผลกระทบ (คือ ถ้าผู้ใช้งานทราบ Path การ Query หรือใช้งานข้อมูลที่ถูกต้อง จะทำให้สามารถ Query ข้อมูลได้โดยไม่จำเป็นต้อง login เข้าสู่ระบบ เนื่องจาก Function หลัง path “https://test.kpru.ac.th/FrontEnd_Tabian/*” ระบบไม่ได้การตรวจสอบ Authorization ของผู้เข้ามาใช้งาน



ภาพที่ 13 แสดงผลผลลัพธ์การ Query ข้อมูลได้โดยไม่ต้องใช้ UserName และ Password ในการ Login

การแก้ไขช่องโหว่ ให้ทำการตรวจสอบสิทธิของผู้ใช้งาน (Authorization) ก่อนทุกครั้งว่า ผู้ใช้งานมีสิทธิจะมีเรียกใช้งาน Function หรือรายการใดๆ หรือไม่เพื่อป้องกันการ Query ข้อมูลโดยตรง

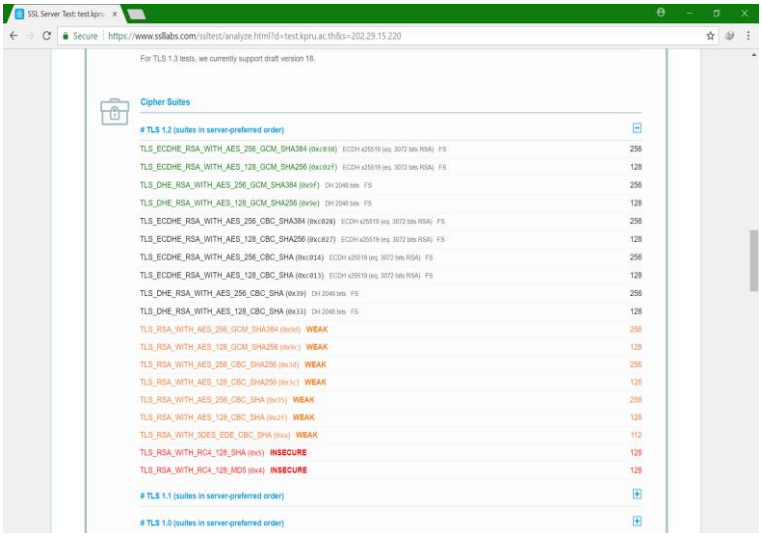
2. ช่องโหว่ Weak cipher suite algorithm

ระดับความรุนแรงอยู่ในระดับสูง (High) ระดับคะแนนซีวีเอสเอส (CVSS Score) 7.4 ผู้วิจัยได้ตรวจพบการใช้งาน Cipher suite algorithm ที่ไม่ปลอดภัยตามตารางด้านล่าง

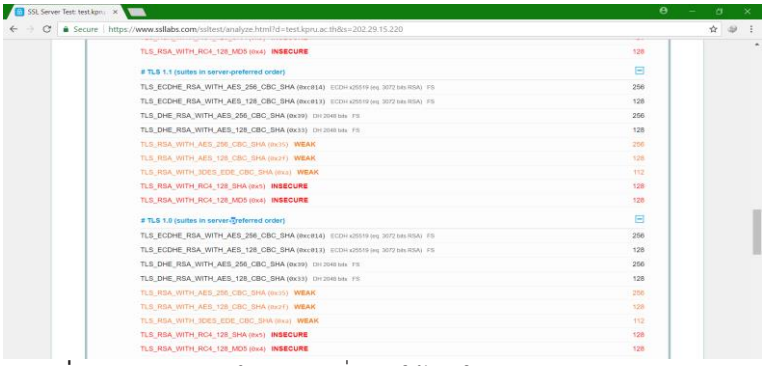
ตารางที่ 2 แสดงเวอร์ชัน TLS และ Cipher Suite ที่ไม่ปลอดภัย

TLS ที่ตรวจพบ	Cipher suite ที่ไม่ปลอดภัย
TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384
	TLS_RSA_WITH_AES_128_GCM_SHA256
	TLS_RSA_WITH_AES_256_CBC_SHA256
	TLS_RSA_WITH_AES_128_CBC_SHA256
	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_3DES_EDE_CBC_SHA
	TLS_RSA_WITH_RC4_128_SHA
	TLS_RSA_WITH_RC4_128_MD5
TLS 1.1	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_3DES_EDE_CBC_SHA
	TLS_RSA_WITH_RC4_128_SHA
	TLS_RSA_WITH_RC4_128_MD5
TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_3DES_EDE_CBC_SHA
	TLS_RSA_WITH_RC4_128_SHA
	TLS_RSA_WITH_RC4_128_MD5

โดยข้อมูลจากเว็บไซต์จะแสดงรายการ Cipher suite algorithm ที่เป็นช่องโหว่และไม่ปลอดภัยตามภาพด้านล่าง



ภาพที่ 14 แสดงผลช่องโหว่ TLS ที่มีการใช้งานในระบบงานทะเบียนนักศึกษา



ภาพที่ 15 แสดงผลช่องโหว่ TLS ที่มีการใช้งานในระบบงานทะเบียนนักศึกษา

ผลกระทบคือ หากผู้ที่โจมตีสามารถทำการถอดรหัสได้จะทำให้ดักฟังหรือทำการแก้ไขข้อมูลระหว่างการสื่อสารข้อมูล ก่อให้เกิดการโจมตีโดยบุคคลที่อยู่ตรงกลางได้ (Man-in-the-Middle Attack)

การแก้ไขช่องโหว่ การแก้ไขช่องโหว่ ให้ทำการ Disable การใช้งาน Cipher Suite ที่ไม่ปลอดภัย แต่อาจจะมีปัญหาส่งผลกระทบต่อเครื่องคอมพิวเตอร์ของผู้ใช้งานที่ใช้ Internet Explore ต่ำกว่าเวอร์ชัน 6 ลงมาให้ตรวจสอบก่อนดำเนินการและให้ใช้ TLS แทน ในกรณีที่ไม่สามารถ Disable ได้ ให้ใช้งานเฉพาะเครือข่ายภายในหรือมีการใช้งานกับข้อมูลที่สำคัญ หรือให้ใช้กับเครื่องคอมพิวเตอร์ที่ติดตั้ง Internet Explore สูงกว่าเวอร์ชัน 6

3. ช่องโหว่ Username Password via GET Method

ระดับความรุนแรงอยู่ในระดับสูง (High) ระดับคะแนนซีวีเอสเอส (CVSS Score) 7.1 จากรูปที่ xxx โดยหน้า Login ดังกล่าว ผู้วิจัยพบว่ามีการส่งผ่านข้อมูล Username password โดยใช้ GET Method

เมื่อใช้งานเมนู lock screen ดังภาพที่ 16

https://test.kpru.ac.th	GET	/FrontEnd_Tabian/login/LoginsAdminTabian/tabian_test002/TC00001/d5f92d95-3bdc-4f64-96f8-437e704fb645	200	202.29.15.220

ภาพที่ 16 แสดงผลการส่งผ่านข้อมูลโดยใช้ Parameter GET

ผลกระทบคือ การใช้ GET Method ส่งข้อมูลที่มีความสำคัญ เช่น Username Password นั้น อาจทำให้ข้อมูลถูกดักจับ (Sniff Traffic) ระหว่างทำการสื่อสารจากผู้ที่ไม่หวังดีได้

การแก้ไขช่องโหว่ เปลี่ยนการใช้งานจาก GET Method เป็น POST Method แทนเนื่องจาก POST Method เป็นการส่งข้อมูลบนส่วน Body ของ Package ซึ่งมีการใช้งานด้วย HTTPS ทำให้ยากต่อการดักจับข้อมูล

4. ช่องโหว่ jquery old version

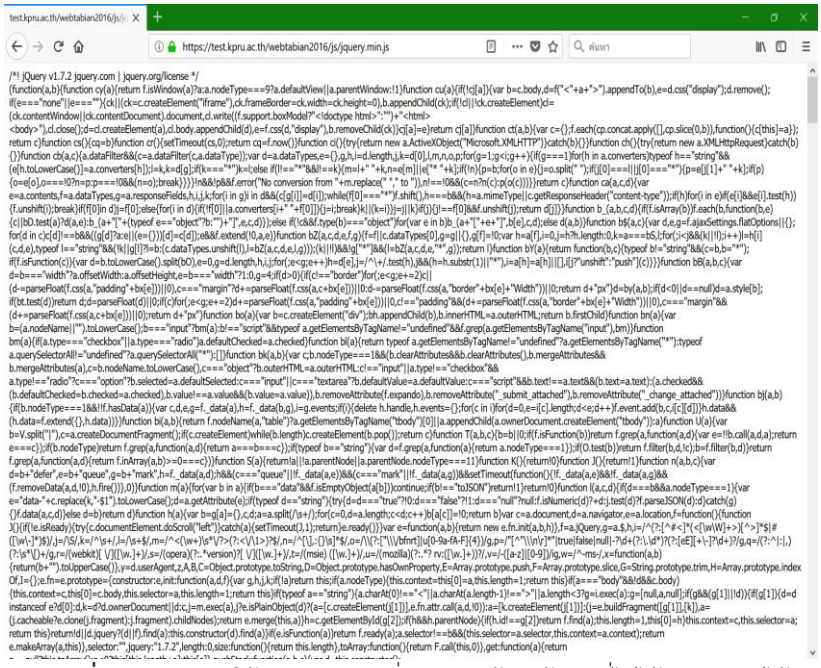
ระดับความรุนแรงอยู่ในระดับกลาง (Medium) ระดับคะแนนซีวีเอสเอส (CVSS Score) 6.8 จากการตรวจสอบระบบงานทะเบียนนักศึกษา ผู้วิจัยพบว่ามีการใช้งานเวอร์ชั่น jQuery 1.7.2 และ 1.2.9 ซึ่งมีผลกระทบคือ ทำให้ผู้ที่ไม่หวังดีสามารถเข้าถึงข้อมูลต่างๆ ที่ไม่ได้รับอนุญาตให้เข้าถึงได้

jQuery Version	Is it Vulnerable?
jQuery 2.0.2	Safe
jQuery 2.0.1	Safe
jQuery 2.0.0	Safe
jQuery 2.0.3	Safe
jQuery 1.10.2	Safe
jQuery 1.10.1	Safe
jQuery 1.10.0	Safe
jQuery 1.9.1	Safe
jQuery 1.9.0	Safe
jQuery 1.8.3	Vulnerable
jQuery 1.8.1	Vulnerable
jQuery 1.8.0	Vulnerable
jQuery 1.7.2	Vulnerable
jQuery 1.7.1	Vulnerable

ภาพที่ 17 แสดงเวอร์ชันของ jQuery ที่ไม่ปลอดภัย

มีผลกระทบคือ ผู้วิจัยหรือผู้ที่ไม่หวังดีสามารถเข้าถึงข้อมูลต่าง ๆที่ไม่ได้รับอนุญาตให้เข้าถึงได้ดังภาพที่ 18

การแก้ไขช่องโหว่ ให้ปรับปรุงเวอร์ชันของ JQuery ให้เป็นปัจจุบัน



ภาพที่ 18 แสดงการใช้งาน jQuery ที่สามารถเข้าถึงข้อมูลที่ไม่ได้รับอนุญาตได้

5. ช่องโหว่ HTTP Method Allowed

ระดับความรุนแรงอยู่ในระดับกลาง (Medium) ระดับคะแนนซีวีเอสเอส (CVSS Score) 5.3 ผู้วิจัยได้ค้นพบช่องโหว่ผลคือมีการใช้งาน Methodที่ไม่จำเป็นเช่น OPTIONS, TRACE และ HEAD

Allow: OPTIONS, TRACE, GET, HEAD, POST
Content-Length: 0
Date: Fri, 11 May 2022 16:54:59 GMT
Public: OPTIONS, TRACE, GET, HEAD, POST
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET

ภาพที่ 19 แสดงผลลัพธ์ของการใช้ Method ที่ไม่จำเป็น

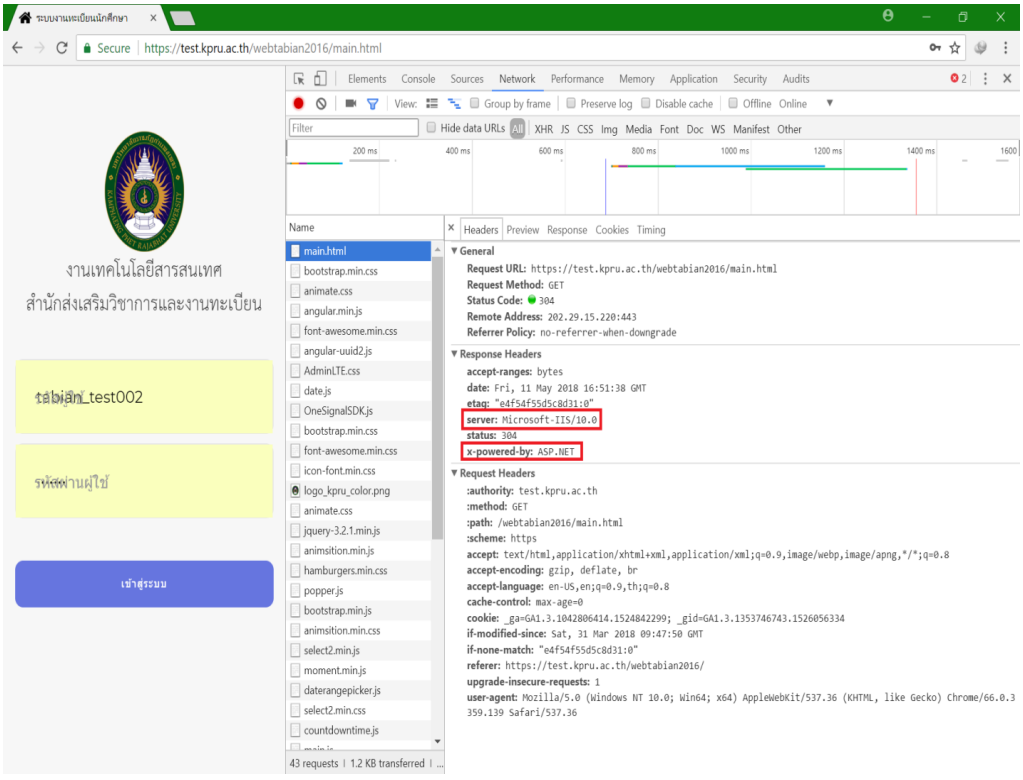
มีผลกระทบ มีโอกาสทำให้เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการเว็บไซต์ ทำงานผิดพลาดหรือแสดงข้อมูลสำคัญที่ไม่อนุญาตให้บุคคลภายนอกเข้าถึงออกมา

การแก้ไขช่องโหว่ ให้ยกเลิกการใช้งาน HTTP Method TRACE, HEAD และ OPTIONS ที่ไม่จำเป็น

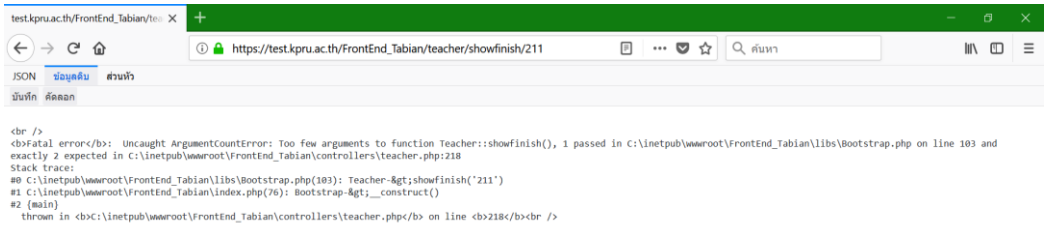
6. ช่องโหว่ Application Technical Error And Information Disclosure

ระดับความรุนแรงอยู่ในระดับกลาง (Medium) ระดับคะแนนซีวีเอสเอส (CVSS Score) 5.3 ผู้วิจัยพบ Error Message จากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการและข้อมูลภายในต่างๆ เช่น Microsoft-IIS 10.0, ASP.NET, C:\inetpub\wwwroot, Server Error 500 ซึ่งแสดงรายละเอียดข้อมูล Error Message ซึ่งมี

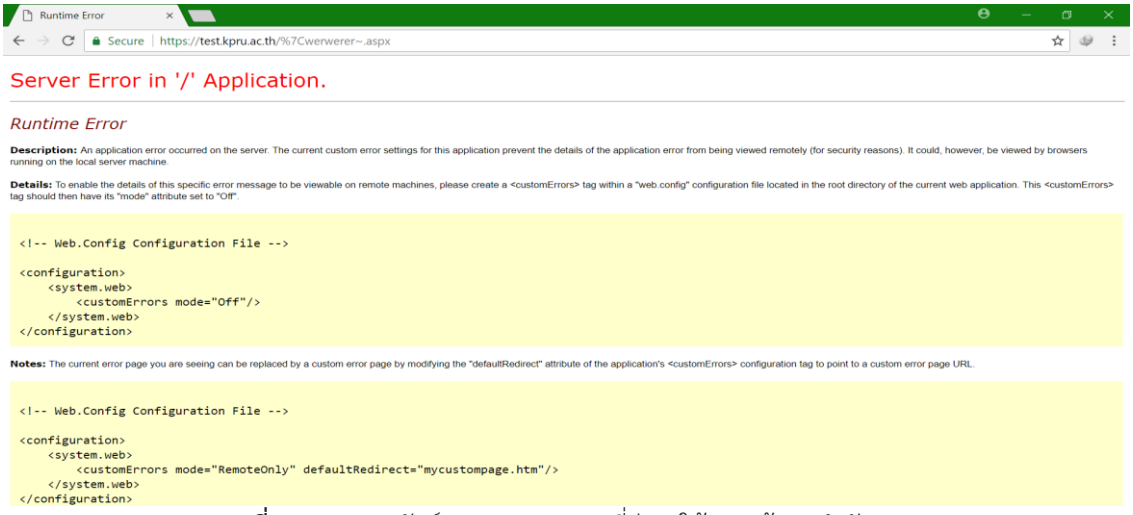
ผลกระทบคือมีโอกาสที่ทำให้เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เกิดการทำงานผิดพลาด หรือแสดงผลข้อมูลสำคัญ ทำให้ผู้ที่ไม่หวังดี สามารถนำข้อมูลที่ได้รับไปวิเคราะห์เพื่อหาช่องโหวในการเจาะระบบต่อไปได้ ดังภาพที่ 20



ภาพที่ 20 แสดงผลลัพธ์ Error Message ที่ส่งผลให้แสดงข้อมูลสำคัญออกมา



ภาพที่ 21 แสดงผลลัพธ์ Error Message ที่ส่งผลให้แสดงข้อมูลสำคัญออกมา



ภาพที่ 22 แสดงผลลัพธ์ Error Message ที่ส่งผลให้แสดงข้อมูลสำคัญออกมา

การแก้ไขช่องโหว่ ทำ Input Validation ในการรับตัวอักษรที่มีความผิดปกติ หรือไม่ถูกต้องตามที่ที่กำหนดไว้ เช่น ช่องที่ควรใส่ได้แต่ตัวเลขก็ไม่ควรอนุญาตให้ใส่ตัวอักษร และให้จัดทำหน้า Error Message หรือ Error Page ที่ไม่แสดงข้อมูลที่มีความสำคัญ หรือ Redirect ไปยัง หน้า Error page ที่สร้างขึ้นมาเตรียมไว้เพื่อให้ข้อมูลหลุดออกมาน้อยที่สุด

7. ช่องโหว่ Missing Basic Function

เป็นช่องโหว่เพื่อแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบ ที่อาจจะเกิดจากความต้องการทางธุรกิจ (Business Requirement) ของหน่วยงานหรือผู้ที่รับผิดชอบเอง โดยผู้วิจัยได้ตรวจพบว่า เมื่อทำการ login เข้าใช้งานในระบบแล้วไม่พบ function ในการเปลี่ยน Password หลังจากทำการ login เข้าใช้งานแล้ว ระบบไม่ทำการ logoff ให้อัตโนมัติเมื่อไม่มีการใช้งาน ไม่พบ Session timeout หรืออาจมีการตั้งค่า Session Timeout ยาวนานเกินไป และได้ทำการทดลองใส่ Password ผิดหลายครั้งโดยทำการ Login ด้วยวิธีการเดาสุ่ม Password) ระบบ แต่ระบบไม่ทำการ Lock Account ซึ่งจะมีผลกระทบคือไม่สามารถเปลี่ยน Password ได้ทันทีในกรณีที่ Password ถูกขโมย รวมไปถึงอาจจะถูกไม่หวังดีสวมรอยเข้ามาใช้งานได้ หากผู้ใช้งานไม่ได้อยู่ที่หน้าจอคอมพิวเตอร์ และระบบอาจจะถูกโจมตี Password แบบ Brute Force Attack ได้

การแก้ไขช่องโหว่ ในกรณีที่ไม่ได้เป็นความต้องการของหน่วยงาน การแก้ไขช่องโหว่ สามารถทำได้โดย เพิ่ม Function ในการเปลี่ยน Password ทำการตั้งค่า Session timeout เมื่อไม่มีการใช้งานตามเวลาที่เหมาะสม และตั้งค่าให้ Account ถูก Lock ไว้เมื่อมีการใส่ Password ผิดครบตามจำนวนครั้งที่กำหนด ทำการปลดล็อคอัตโนมัติเมื่อถึงเวลาที่กำหนด หรือสามารถปลอดล็อคโดยผู้พัฒนาระบบเท่านั้น ในกรณีที่เป็นความต้องการของหน่วยงาน แนะนำให้แจ้งความเสี่ยง ผลกระทบดังกล่าวให้กับหน่วยงานหรือผู้ใช้งานทราบ เนื่องจากผู้ใช้งานอาจไม่ได้ตระหนักถึงความมั่นคงปลอดภัยในการใช้งานระบบทะเบียน

จากช่องโหว่ที่ค้นพบจำนวน 7 รายการ ตามที่ได้กล่าวไปแล้วข้างต้น ผู้วิจัยได้ทำการสรุประดับความรุนแรงและระดับคะแนนซีวีเอสเอส ดังตารางที่ 3

ตารางที่ 3 สรุประดับความรุนแรงและระดับคะแนนซีวีเอสเอส

ลำดับที่	รายการช่องโหว่ที่ตรวจค้นพบ	ระดับความเสี่ยง
1	Unauthorized Access Data (Missing Function Level Access Control)	High
2	Weak cipher suite algorithm	High
3	Username Password via GET Method	High
4	jQuery old version	Medium
5	HTTP Method Allowed	Medium
6	Application Technical Error And Information Disclosure	Medium
7	Missing Basic Function	Information

อภิปรายผล

ผู้วิจัยได้ทำการประเมินช่องโหว่เว็บไซต์ระบบงานทะเบียนนักศึกษา โดยอ้างอิงตามมาตรฐาน Open Web Application Security Project - OWASP Top 10 ประจำปี 2564 โดยใช้เครื่องมือที่เป็น OpenSource และเครื่องมือจากเว็บไซต์ของนักพัฒนาซอฟต์แวร์ ที่มีการเปิดเผยรายละเอียดช่องโหว่ของซอฟแวร์เวอร์ชันต่างๆ ผลจากการวิจัยแสดงให้เห็นถึงช่องโหว่ของระบบงานนักศึกษาที่สามารถสรุปประเด็นได้ดังนี้ 1) การใช้ชุดคำสั่งหรือไลบารีที่ไม่ได้มีการปรับปรุงเวอร์ชันให้ทันสมัย ส่งผลกระทบทำให้ผู้ที่ไม่หวังดีสามารถเข้าถึงข้อมูลในฐานข้อมูลได้โดยไม่ต้องล๊อกอินเข้าระบบ 2) การกำหนดค่าพารามิเตอร์ที่ในการับส่งข้อมูลที่สำคัญที่ผิดพลาด ส่งผลกระทบที่จะทำให้ผู้ไม่หวังดีสามารถดักจับและอ่านข้อความนั้นได้ 3) การใช้ Cipher ที่ไม่แข็งแกร่งส่งผลกระทบที่ทำให้เกิดการโจมตีโดยบุคคลที่อยู่ตรงกลาง 4) ผลการกระทบจากความต้องการทางธุรกิจเช่น ไม่มีหน้าเปลี่ยน password หรือตัวระบบไม่จำกัดจำนวนครั้งที่ใช้ในการ Login ในกรณีที่ผู้ใช้งานใส่รหัสผ่านผิดก่อให้เกิดการโจมตีแบบคาดเดารหัสผ่าน (Brute Force) ซึ่งช่องโหว่ดังกล่าวสามารถแก้ไขให้ระบบมีความมั่นคงปลอดภัยมากขึ้นได้โดยการทำตามคำแนะนำจากเว็บไซต์ที่ของนักพัฒนาชุดคำสั่งและจากรายงานการประเมินช่องโหว่

ในการหาช่องโหว่และการประเมินความเสี่ยงของระบบที่ศึกษานั้น มีความน่าเชื่อถืออยู่ในระดับที่ไม่น้อยไปกว่าการประเมินในลักษณะเดียวกับงานศึกษาวิจัยอื่น โดยโปรแกรมประยุกต์ที่ใช้งานนั้นได้รับการพัฒนาและอัพเดทเวอร์ชันการใช้งานอย่างต่อเนื่องจนมีความสามารถที่จะตรวจจับความผิดปกติของระบบได้อย่างแม่นยำกว่าโปรแกรม Aacunetix ในลักษณะเดียวกันกับงานศึกษาอื่นในอดีต (พัชรวัฒน์ และชัยพร, 2563; ณัชณภัทร และชัยพร, 2560)

กิตติกรรมประกาศ

ผู้วิจัย ขอขอบคุณสำนักส่งเสริมและงานทะเบียน ที่สนับสนุนข้อมูลระบบงานทะเบียนนักศึกษาในการทำวิจัยในครั้งนี้ นอกจากนี้ผู้วิจัยขอขอบคุณ งานพัฒนาระบบเครือข่าย สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกำแพงเพชร ที่ให้คามช่วยเหลือในการติดตั้งระบบและเป็นที่ปรึกษา และสุดท้ายนี้ ขอขอบพระคุณ บิดา มารดาที่คอยเป็นกำลังใจให้มาโดยตลอด คณะผู้วิจัยจึงขอขอบคุณมา ณ โอกาสนี้

เอกสารอ้างอิง

ณัชณภัทร ใจอดทน. (2560). **การประเมินค่าช่องโหว่ของเว็บไซต์และการป้องกัน กรณีศึกษาเว็บไซต์, กรมควบคุมการปฏิบัติทางอากาศ**. สารนิพนธ์วิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม มหาวิทยาลัยธุรกิจบัณฑิตย์.

ณัชณภัทร ใจอดทน และชัยพร เขมะภาตะพันธ์. (2560). **การประเมินค่าช่องโหว่ของเว็บไซต์และการป้องกัน กรณีศึกษาเว็บไซต์. กรมควบคุมการปฏิบัติทางอากาศ**. [Online]. Available : https://cite.dpu.ac.th/ct/upload/content/filesณัชณภัทร%20%20ใจอดทน%20CT58.pdf [2566, พฤษภาคม 16].

พัชรวัฒน์ โกสิตงามดีวงศ์ และชัยพร เขมะภาคตะพันธ์. (2563). การประเมินช่องโหว่ระบบบริหารจัดการทางการแพทย์ กรณีศึกษา โรงพยาบาลภูมิพลอดุลยเดช กรมแพทย์ทหารอากาศ. **วารสารบัณฑิตวิทยาลัย มหาวิทยาลัยธุรกิจบัณฑิตย์, 9**(1), 1-17.

ศิริขวัญ ศิริพิทิพย์รักษ์. (2559). **เครื่องมือช่วยประเมินช่องโหว่ด้านความมั่นคงเพื่อยกระดับเวอร์ชันของซอฟต์แวร์**. วิทยานิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมซอฟต์แวร์ จุฬาลงกรณ์มหาวิทยาลัย.

เอกชัย พ่วงพรพิทักษ์. (2565). **การพัฒนาแนวทางการสืบสวนอาชญากรรมทางไซเบอร์ต่อบริการธนาคารอิเล็กทรอนิกส์ และวิเคราะห์เทคนิคเทคโนโลยีสารสนเทศเพื่อสร้างต้นแบบที่เสริมสร้างความมั่นคง**. รายงานการวิจัย กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม.

Extosoft Company. (2563). **ค้นหาเป้าหมายที่เราต้องการจะโจมตี หรือเจาะระบบ โดยใช้ Nmap (“Network Mapper”)**. [Online]. Available : https://medium.com/extosoft/ ค้นหาเป้าหมายที่เราต้องการจะโจมตี-หรือเจาะระบบ-โดยใช้-nmap-network-mapper-62ed41df940c [2566, พฤษภาคม 16].

Mera Saulaiman, Márta Takács, Miklos Kozlovszky & Akos Csilling. (2021). **Fuzzy model for common vulnerability scoring system**. [Online]. Available : https://ieeexplore.ieee.org/abstract/document/9465614/authors#authors [2566, May 16].

Urshila Ravindran & Raghu Vamsi Potukuchi. (2022). A review on web application vulnerability assessment and penetration testing, **Review of computer engineering Studies, 9**(1), 1-22.