cyber attack simulation

SC362006

Information and Communication Technology Security

อาจารย์ประจำวิชา **ศ. ดร.จักรชัย โสอินทร์**
ผศ. ดร.สาธิต กระเวนกิจ
อ. ดร.ชาติชาย ปุณริบูรณ์

หลักการและเหตุผล

ภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นทำให้การศึกษา ด้านความมั่นคงปลอดภัยมีความสำคัญมากขึ้น โครงงาน Cyber Attack Simulation จึงถูกพัฒนาเพื่อใช้เป็นสื่อการเรียนรู้ผ่านการ จำลองเหตุการณ์จริงในสภาพแวดล้อมเสมือน โดยเน้นการบันทึกเหตุการณ์ (Event Logging) และแสดงผลผ่าน Dashboard เพื่อให้เข้าใจกระบวนการตรวจจับและเฝ้าระวังได้อย่างเป็นรูปธรรม โดยไม่กระทบต่อระบบจริง

วัตถุประสงค์

- เพื่อสร้างความตระหนักรู้ด้านความปลอดภัยไซเบอร์
- เพื่อลดความเสี่ยงจากความผิดพลาดของมนุษย์ (Human Error)
- เพื่อใช้เป็นข้อมูลประกอบการวางแผนพัฒนาระบบรักษาความปลอดภัยในอนาคต
- เพื่อจำลองสถานการณ์การโจมตีเพื่อเป็นความรู้ในการศึกษาต่อๆไป
- เพื่อศึกษาผลกระทบของการโจมตีต่อระบบ เครือข่าย และข้อมูล

ขอบเขตการศึกษา

พัฒนาระบบเว็บแอปพลิเคชันสำหรับจำลองการโจมตีทางไซเบอร์ในสภาพแวดล้อมเสมือน (Virtual Machine) โดยไม่กระทบต่อระบบจริง ครอบคลุม 2 ส่วนหลัก ได้แก่

- Vulnerability — จำลองช่องโหว่ Web Application เช่น SQLi, XSS, CSRF, IDOR, Brute Force และ File Upload พร้อมเปรียบเทียบโค้ดระดับ Low ถึง Impossible
- Cyber Attack Simulation — จำลองสถานการณ์โจมตีจริง บันทึก Event Log (JSONL) ตรวจจับภัยคุกคาม และแสดงผลผ่าน Dashboard พร้อม Incident Timeline

สรุปผลการดำเนินงาน

โครงงาน Cyber Attack Simulation พัฒนาระบบเว็บสำเร็จตามวัตถุประสงค์ โดยสามารถ

- จำลองสถานการณ์ Web Attack และ Phishing ให้ผู้ใช้โต้ตอบได้จริงในสภาพแวดล้อมที่ปลอดภัย
- ตรวจจับและบันทึกเหตุการณ์ด้านความปลอดภัยลงฐานข้อมูลในรูปแบบ Event Log
- แสดงผลสถิติและ Incident Timeline ผ่านหน้า Dashboard
- สนับสนุนการเรียนรู้กระบวนการตอบสนองต่อเหตุการณ์ตามแนวทาง NIST SP 800-61

อ้างอิง

Digininja. DVWA. GitHub, https://github.com/digininja/DVWA
OWASP. WebGoat. GitHub,https://github.com/WebGoat/WebGoat

ซอฟต์แวร์ที่ใช้พัฒนา

Visual Studio Code · MySQL · HTML · PHP · JS

วิธีการใช้งาน

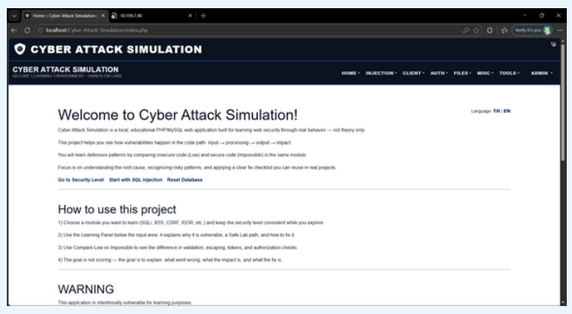
ส่วนที่ 1 — Vulnerability

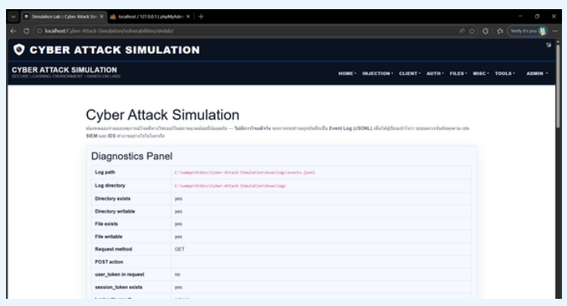
- เลือกบท ที่ต้องการ เช่น SQLi, XSS, CSRF, IDOR แล้วตั้ง Security Level
- ทดลองโจมตี ผ่านฟอร์ม แล้วอ่าน Learning Panel เพื่อทำความเข้าใจ Input Output Impact
- เปรียบเทียบโค้ด Low vs Impossible เพื่อดูวิธีป้องกันที่ถูกต้อง
- สรุป Fix Checklist เพื่อนำไปใช้กับงานพัฒนาจริง

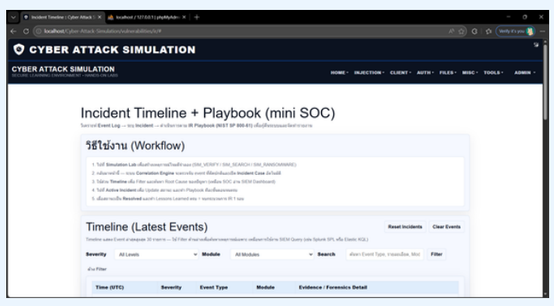
ส่วนที่ 2 — Cyber Attack Simulation

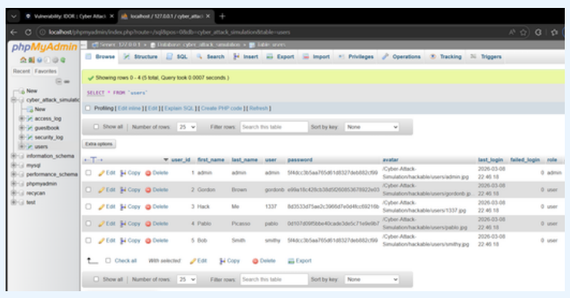
- เลือก Scenario จำลองการโจมตี เช่น Web Attack, Phishing ในสภาพแวดล้อมเสมือน
- ดู Event Log ที่ระบบบันทึกอัตโนมัติ (JSONL) เพื่อเรียนรู้การทำงานของ SIEM/IDS
- วิเคราะห์ Incident Timeline เรียงลำดับเหตุการณ์และระบุ attack phases
- จัดทำรายงาน ตาม IR Playbook (NIST SP 800-61) พร้อม Lessons Learned

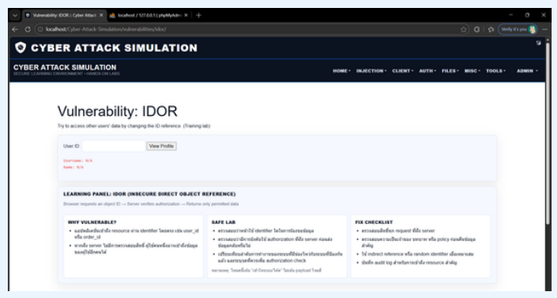
ตัวอย่างงาน











ผู้จัดทำ

ฐิติภัทร กันยาประสิทธิ์	673380214-5
นันท์นภัส กลมเกลี้ยง	673380224-2
พีรธัช ผันอากาศ	673380231-5
ศุภาฐิณี ซอสูงเนิน	673380245-4
สุรสีห์ วิไลจินดาพร	673380249-6

Group 7 Sec.1