รายวิชา CP422031 | Introduction to Cybersecurity

อาจารย์ผู้สอน ศ.ดร.จักรชัย โสอินทร์ ผศ.ดร.สาธิต กระเวนกิจ และ อ. ดร.ชาติชาย ปุณริบูรณ์

Smart Shield Proxy

หลักการและเหตุผล

ปัจจุบันการโจมตีเว็บไซต์มีความซับซ้อนมากขึ้น ระบบป้องกันแบบเดิม เช่น WAF ที่ใช้กฎตายตัว มักตรวจจับการโจมตีรูปแบบใหม่หรือการดัดแปลงคำสั่งได้ยาก โปรเจกต์นี้จึงเสนอแนวคิด Hybrid Security โดยใช้ Machine Learning วิเคราะห์ Payload ร่วมกับ ModSecurity เพื่อเพิ่มความแม่นยำในการตรวจจับและตอบสนองต่อภัยคุกคามแบบ Real-time.

วัตถุประสงค์

1. พัฒนาระบบ Web Proxy อัจฉริยะ สำหรับกรองทราฟฟิกเว็บ
2. ใช้ Machine Learning เพื่อเพิ่มประสิทธิภาพการตรวจจับภัยคุกคาม
3. ใช้แนวคิด Defense-in-Depth เพื่อเสริมความปลอดภัยหลายชั้น
4. สร้างระบบ Real-time Monitoring สำหรับตรวจสอบและรายงานผล
5. จัดเตรียม Dataset เพื่อให้ระบบเรียนรู้และพัฒนาต่อเนื่อง

ขอบเขตระบบ

การตรวจจับ: เน้นตรวจจับ SQL Injection และ XSS ผ่าน HTTP
ระบบป้องกัน: 2 ชั้น — Layer 1: ML Model, Layer 2: ModSecurity
การตอบสนอง: บล็อกด้วย HTTP 403 Forbidden และบันทึก Log อัตโนมัติ
การแสดงผล: Dashboard แสดงสถิติการโจมตีและความแม่นยำของโมเดล

ขั้นตอนการทำงาน

1. Attacker ส่ง Request โจมตีมายัง Proxy (Port 8080)
2. ML Proxy ทำ Normalize และให้ ML Model วิเคราะห์
3. Layer 1 ถ้า ML ตรวจพบการโจมตี → Block และบันทึก Log
4. Layer 2 ถ้า ML ให้ผ่าน → ส่งไป Web Server (Port 80) ให้ ModSecurity ตรวจสอบซ้ำ
5. Monitoring ผู้ดูแลระบบดูผลผ่าน Dashboard

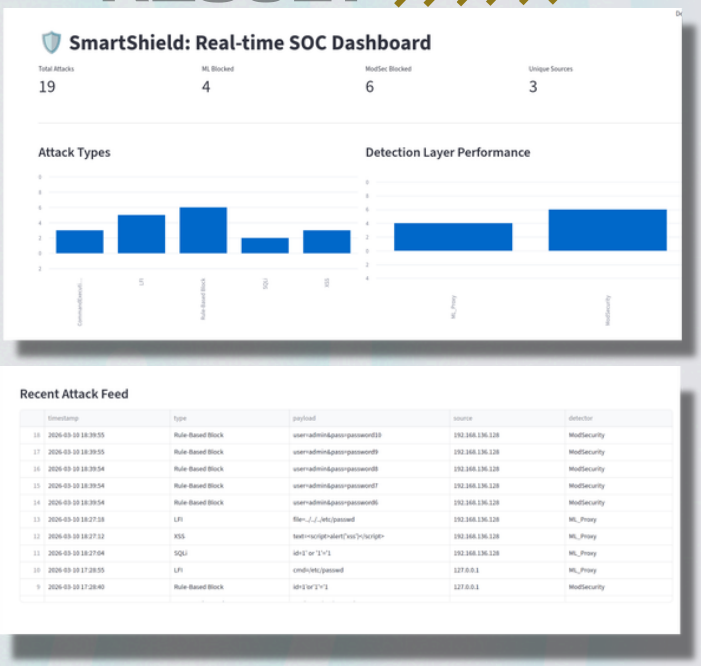
เครื่องมือที่ใช้

Streamlit

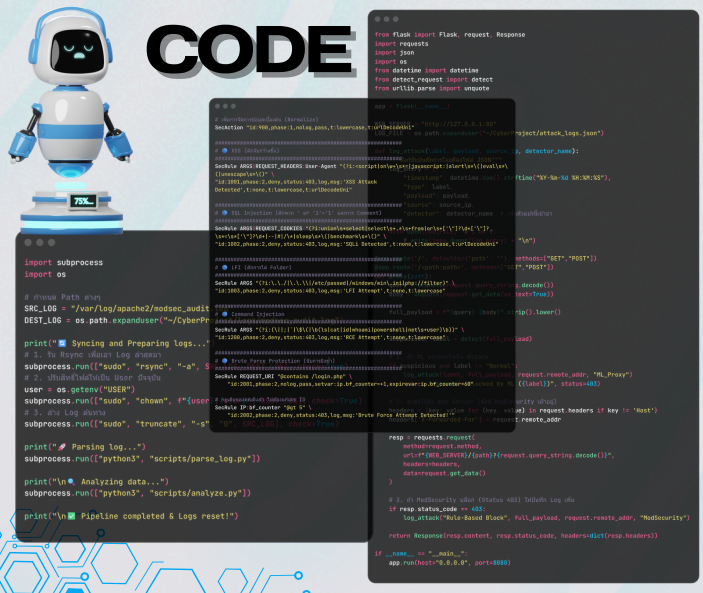
modsecurity

scikit learn

RESULT



CODE



สรุปผลการทำงาน

ระบบสามารถทำงานได้อย่างมีประสิทธิภาพตามสมมติฐาน โดย Machine Learning ช่วยให้การตรวจจับ Payload ที่มีความหลากหลายทำได้ดีขึ้น ในขณะที่ ModSecurity ช่วยเสริมความปลอดภัยในส่วนของกฎมาตรฐานสากล ผลการทดสอบพบว่าระบบสามารถบล็อกการโจมตีได้แบบ Real-time และช่วยให้ผู้ดูแลระบบมองเห็นภาพรวมของภัยคุกคามผ่าน Dashboard ได้อย่างชัดเจน พร้อมรองรับการอัปเดต Dataset เพื่อเพิ่มความฉลาดของโมเดลได้ในอนาคต

Member of Group 10 Sec 1

673380484-6 ภัทรภูมิ ไชยันโต
673380486-2 ยศพล สุกแสง
673380192-9 สิริมงคล ม่วงลาย
673380013-5 วณัฏฐนนท์ รือหาร
673380006-2 ชิดธรรม นาเมืองรักษ์