Web Application Intrusion Detection System (Web IDS)

1. ภาพรวมระบบ

ระบบ Web Application Intrusion Detection System (Web IDS) เป็นระบบตรวจจับการโจมตีที่เกิดกับ Web Application โดยใช้ Machine Learning ในการวิเคราะห์ payload ที่ถูกส่งเข้ามา เช่น SQL Injection และ Cross-Site Scripting (XSS). ระบบจะตรวจสอบ request ผ่าน API จากนั้นบันทึก log ลงฐานข้อมูลและแจ้งเตือนผ่าน Discord เมื่อพบพฤติกรรมที่เป็น Attack.

2. โครงสร้างการทำงานของระบบ

ลำดับการทำงานของระบบ:

1. Client ส่ง request payload ไปยัง API
2. Flask API รับ request ที่ endpoint /detect
3. Payload ถูกแปลงเป็น vector ด้วย CountVectorizer
4. Machine Learning Model (Logistic Regression) วิเคราะห์ payload
5. ระบบทำนายผลเป็น Attack หรือ Normal
6. ระบบบันทึกข้อมูลลงฐานข้อมูล SQLite
7. หากพบ Attack จะส่ง Notification ไปยัง Discord
8. Dashboard แสดงสถิติและข้อมูลการโจมตีล่าสุด

3. ซอฟต์แวร์ที่ต้องติดตั้งก่อนใช้งาน

- Python 3.10 หรือใหม่กว่า
- Postman (ใช้สำหรับทดสอบ API)
- Discord Account (ใช้รับการแจ้งเตือน)
- Visual Studio Code หรือโปรแกรม editor อื่น ๆ

4. การติดตั้งระบบ

1. เปิด Terminal หรือ Command Prompt
2. เข้าไปยังโฟลเดอร์โปรเจค
3. ติดตั้ง Library ที่จำเป็น:

```
pip install flask scikit-learn joblib requests
```

4. รันระบบด้วยคำสั่ง:

```
python app.py
```

5. การเข้าใช้งานระบบ

Dashboard:
http://127.0.0.1:5000/dashboard

Logs:
http://127.0.0.1:5000/logs

6. วิธีทดสอบระบบด้วย Postman

1. เปิด Postman
2. เลือก Method: POST
3. ใส่ URL: http://127.0.0.1:5000/detect
4. ไปที่ Body → raw → JSON
5. ใส่ payload ตัวอย่าง เช่น:

{ "payload": "<script>alert(1)</script>" }

6. กด Send เพื่อส่ง request
7. ระบบจะตอบกลับ prediction และบันทึก log

7. การแจ้งเตือนผ่าน Discord

เมื่อระบบตรวจพบ payload ที่ถูกจัดประเภทเป็น Attack ระบบจะส่ง Notification ไปยัง Discord Webhook เพื่อแจ้งเตือนผู้ดูแลระบบทันที.

8. คำแนะนำสำหรับการนำเสนอระบบ

ขั้นตอนที่แนะนำในการพรีเซนต์:

1. เปิด Dashboard เพื่อแสดงสถานะระบบ
2. ใช้ Postman ยิง payload ที่เป็น Attack
3. แสดงผล Prediction จาก API
4. เปิดหน้า Logs เพื่อดูการบันทึกข้อมูล
5. แสดง Discord Notification ที่แจ้งเตือน Attack

9. หมายเหตุสำคัญ

ผู้ใช้งานควรทดสอบระบบด้วยตนเองผ่าน Postman เพื่อให้เห็นลำดับการทำงานของระบบตั้งแต่การรับ request การตรวจจับด้วย Machine Learning การบันทึก log และการแจ้งเตือน.