SQL Injection Playground with Detection Engine

Introduction

The SQL Injection Playground with Detection Engine is a web-based application developed to simulate SQL Injection (SQLi) vulnerabilities for educational and testing purposes. This project aims to help cybersecurity enthusiasts understand SQLi attacks and implement detection techniques in a controlled environment. It allows users to execute common SQLi patterns on a vulnerable web interface while monitoring logs and detection alerts.

Abstract

SQL Injection remains one of the most critical web security vulnerabilities. This project creates a safe playground to demonstrate how SQLi attacks work and how they can be detected using a Python-based detection engine. Built using Flask and MySQL, the platform provides a simple login form vulnerable to SQLi, alongside a detection script that monitors queries for attack patterns. This setup aids both learning and testing of basic SQLi prevention mechanisms.

Tools Used

- Frontend: HTML (Jinja2 Templates)
- Backend: Python (Flask Framework)
- Database: MySQL
- Detection Engine: Python (Custom Detection Script)
- Utilities: MySQL-Connector-Python, Flask

Steps Involved in Building the Project

1. Environment Setup: Installed Flask and MySQL-Connector-Python to facilitate backend development and database connectivity.
2. Database Configuration: Manually created a sqli_demo database with a users table in MySQL, pre-loaded with sample data.
3. Vulnerable Application Development: Developed a basic Flask web app (app.py) with a login form intentionally designed to be vulnerable to SQLi attacks.
4. Detection Engine Implementation: Created a Python script (detector.py) to monitor query patterns and detect potential SQL Injection attempts by analyzing user inputs.
5. Interface & Logging: Designed simple frontend templates and added logging functionality (logs.txt) to track all login attempts and SQLi detection alerts.
6. Testing & Demonstration: Deployed the application locally and performed multiple SQLi test cases to validate detection engine accuracy.

Conclusion

The SQL Injection Playground with Detection Engine successfully provides a hands-on environment to understand SQLi vulnerabilities and detection techniques. It serves as an effective tool for security practitioners, educators, and students to learn about SQL Injection in a practical, controlled manner. The modular design of the project allows further enhancement, including advanced SQLi attack detection and preventive measures.