Project Report: Phishing Simulation Platform & Web Vulnerability Scanner

Introduction

This project combines two critical cybersecurity tools: a Phishing Simulation Platform and an AI-Powered Web Vulnerability Scanner. The phishing simulator helps organizations test employee awareness by simulating real-world phishing attacks, while the vulnerability scanner identifies security flaws in web applications, such as SQL Injection, XSS, and LFI. Both tools leverage AI to enhance detection and analysis.

Abstract

The Phishing Simulation Platform (phishing_ai.py) mimics phishing attacks by deploying a fake login page to capture user-submitted data, logging entries in an SQLite database. The Web Vulnerability Scanner (scanner_ai.py and scanner_ai_ultimate.py) crawls websites, injects malicious payloads, and detects vulnerabilities using AI-assisted analysis. The advanced version (scanner_ai_ultimate.py) integrates OpenAI for real-time cybersecurity guidance.

Tools Used

Python (Primary language for scripting)

Flask (For phishing web server)

SQLite (Storing phishing logs)

Requests & BeautifulSoup (Web crawling and form parsing)

OpenAI API (AI-powered pentesting assistance)

Rich & Colorama (Console formatting and UI)

Steps Involved in Building the Project

1. Phishing Simulation Platform

Developed a Flask-based web server (phishing_ai.py) hosting a fake "security alert" page.

Created an AI-generated phishing email template to lure users.

Implemented SQLite logging to store victim data (IP, email, timestamp, user agent).

Added a progress tracker and console UI for better interaction.

2. Web Vulnerability Scanner (Basic & Advanced)

Basic Scanner (scanner_ai.py)

Detects SQLi, XSS via predefined payloads.

Uses requests and BeautifulSoup for scanning forms.

Provides vulnerability explanations in a structured report.

Advanced Scanner (scanner_ai_ultimate.py)

Crawls entire websites to find hidden pages.

Detects SQLi, LFI, Command Injection, and missing security headers.

Integrates OpenAI for real-time cybersecurity advice.

Generates JSON reports for further analysis.

3. AI Integration

Used OpenAI’s GPT-4 to assist in vulnerability interpretation and ethical hacking guidance.

Added an interactive AI assistant for real-time queries.

Conclusion

This project successfully demonstrates how AI can enhance cybersecurity tools—both in simulating phishing attacks and detecting web vulnerabilities. The phishing simulator helps organizations train employees, while the scanner identifies critical security flaws before attackers exploit them. Future improvements could include automated remediation suggestions and multi-threaded scanning for efficiency.

Author: Abhijeet
Project: Phishing Simulation Platform & Web Vulnerability Scanner
Date: 20-06-2-25