VulnX – Real-Time Web Threat Detection & Manual Vulnerability Scanner

Elevate Labs Cybersecurity Internship — Final Report
Intern Name: *Aditya Gudla*
GitHub: *https://github.com/aditya-gudla2005/VulnX-CyberDefender*

Introduction

VulnX is an integrated cybersecurity tool combining real-time packet sniffing and manual web vulnerability scanning into one unified dashboard. It detects XSS and SQL Injection attacks through live network monitoring and active payload injection, designed for lightweight, offline-compatible environments.

Abstract

Modern web applications often suffer from input injection vulnerabilities, which attackers exploit to compromise data, perform unauthorized actions, or execute malicious scripts. VulnX addresses this gap by providing:

- Live network sniffing using Scapy for detecting suspicious payloads in traffic.
- A manual vulnerability scanner that crawls websites and injects test payloads into form fields.
- A dashboard UI for real-time alert viewing, exportable reports, and optional Telegram bot alerts.

This project is built for practical use, especially by students, testers, or small orgs needing lightweight, offline-compatible tools.

Tools & Technologies Used

1) Python 3 for backend logic
2) Flask to serve the real-time dashboard
3) Scapy for live packet sniffing
4) BeautifulSoup + Requests for crawling and injection
5) Regex to detect XSS/SQLi in traffic
6) Chart.js for graph rendering
7) FPDF for exporting alerts as PDF
8) Telegram Bot API for instant alerts

Steps Involved in Building VulnX

1) **Sniffer Module:**

- Scapy captures live packets
- Decodes payloads with unquote()
- Matches against known XSS/SQLi patterns
- Logs to JSON and optionally alerts via Telegram

2) **Manual Scanner:**

- Crawls the site for forms/links
- Submits crafted payloads to test for reflection/errors
- Logs issues like:
    - XSS vulnerability on https://example.com
    - SQL Injection detected on ?id=' OR '1'='1

3) **Dashboard:**

- Displays alerts in real-time
- Filters by attack type (XSS/SQLi)
- Graph updates every 5s via Chart.js
- One-click PDF export of alerts & scan results

4) **Report Export:**

- Combined alerts.json + scan_results.json into a single PDF using fpdf
- Includes timestamps, types, and payload details for offline auditing

Conclusion

VulnX successfully demonstrates how real-time monitoring and manual testing can be combined into a seamless security toolkit. With a functional UI, real-time logging, export capabilities, and modular architecture, this project extends beyond internship expectations.

Note: While IP blocking was considered, it was skipped to avoid local self-blocking during testing. However, it can be easily added when deployed on a remote server.