SENTINEL-X:CYBERSECURITY TOOLKIT

BY:-
AKANSH PANDEY
AKSHAYA TANWAR
KARTIKEYA
PALAK KASHYAP

INTRODUCTION

Cybersecurity Challenges: As our dependence on digital communication grows, so does the threat landscape—ranging from data breaches to unauthorized access.

Sentinel-X Solution: A unified platform providing end-to-end encryption, real-time scanning tools, and user-driven customization.

Key Features:

- ➢ Secure real-time communication
- ➢ Password strength checker
- ➢ Port and vulnerability scanners
- ➢ Modular and user-friendly design

OBJECTIVES

Secure Chat System: Implement AES encryption for encrypted messaging.

Port Scanner: Fast, real-time detection of open ports on a network.

Vulnerability Scanner: Scans web applications for vulnerabilities like SQLi and XSS.

Password Strength Checker: Helps users assess the strength of their passwords with breach pattern checks.

Scalability & Customization: Tools for both individuals and enterprises with adjustable settings.

User Control & Transparency: Full control over the security settings and configurations.

MODULES OVERVIEW

Secure Chatting Application

Tech Stack: Supabase, JavaScript, AES-GCM

Features:

End-to-end encryption

Typing indicators, friend search, online status

Hacker-themed UI for enhanced user experience

Vulnerability Scanner

Tech Stack: Flask, BeautifulSoup, Requests

Features:

Crawls websites for vulnerabilities

SQL Injection (SQLi) & Cross-Site Scripting (XSS) detection

Generates detailed reports for security auditing

Port Scanner

Tech Stack: Flask, Socket, threading

Features:

Multi-threaded, fast port scanning

Real-time feedback of scan results

Input-based targeting for customized scanning

Password Strength Checker

Tech Stack: HaveIBeenPwned API

Features:

Compares passwords with breached data

Provides suggestions to strengthen passwords

User-friendly interface

METHODOLOGY

Requirements Gathering:

Researching existing tools and CVE databases.

Identifying attack vectors, real-world threats, and user needs.

System Architecture:

Modular design: Flask for backend, Supabase for authentication, and frontend hosted on Vercel.

Encryption & Scanning:

AES-256 for encryption, real-time scanning using requests, socket, and BeautifulSoup.

Password analysis with regex and entropy checks.

Testing & Simulation:

Extensive unit and integration tests.

Real-time attack simulations for threat detection.

TECHNOLOGIES USED

Supabase: User authentication, real-time data, and chat functionality.

Flask: Backend for the port and vulnerability scanners, serving the API.

AES Encryption: Ensures that all messages within the chat are securely encrypted.

HaveIBeenPwned API: For password strength verification, checking passwords against a breach database.

Python Libraries:

Flask-CORS for handling CORS in web requests

Requests for HTTP requests

BeautifulSoup for web scraping and scanning

Deployment:

Frontend: Vercel for smooth hosting and scaling

Backend: Render for hosting Flask APIs

DEPLOYMENT STRATEGY

Frontend (Vercel):

HTML, CSS, and JavaScript files hosted under a single domain.

User-friendly interface with real-time feedback.

Backend (Render):

Flask APIs for real-time scanning and other backend functionalities.

Cross-Origin Resource Sharing (CORS):

Handled using Flask-CORS to allow secure communication between frontend and backend.

Continuous Updates:

Ongoing improvements to ensure compatibility with the latest security threats.

CONCLUSION

Sentinel-X is a comprehensive cybersecurity toolkit offering users full control, real-time adaptability, and robust defense mechanisms.

Key Features:

Secure chatting with AES encryption

Real-time port and vulnerability scanning

Password strength verification

Open-Source & Scalable:

Transparency and future extensibility for diverse user needs.

THANK YOU