January 6, 2026

Presentation Overview

WebScanPro: AI-Driven Vulnerability Scanner

Problem Statement

- Traditional vulnerability scanners produce a high number of false positives
- Manual security testing is time-consuming and cannot keep pace with continuous deployment
- Existing tools lack intelligent risk classification and prioritization
- There is a strong need for an automated, accurate, and AI-driven vulnerability assessment solution

Project Overview

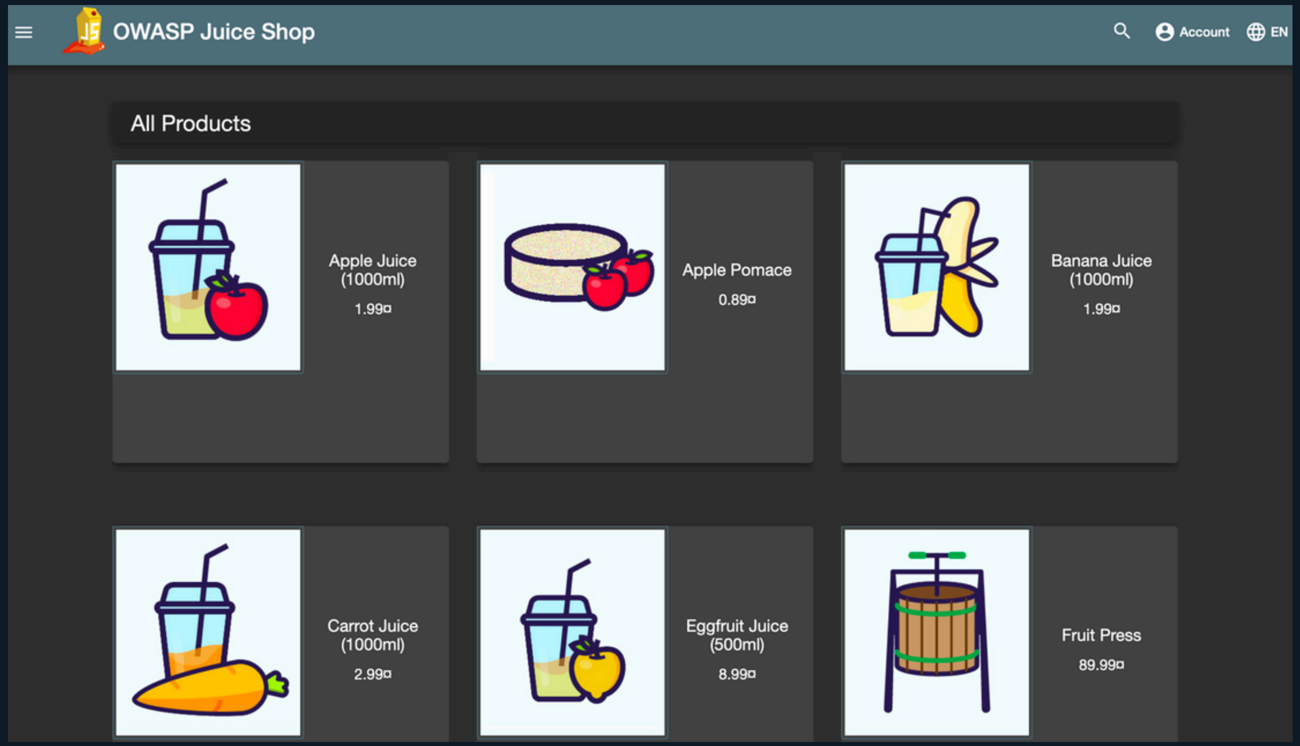
Introducing an AI-Driven vulnerability scanning solution

Executive Summary

- Project Name: WebScanPro: AI-Driven Automated Vulnerability Scanner.
- Core Purpose: A modern security auditing tool designed to identify, analyze, and report critical web vulnerabilities through an automated AI-driven pipeline.
- The Problem: Traditional security assessments are often slow and manual, failing to keep pace with rapid development cycles.

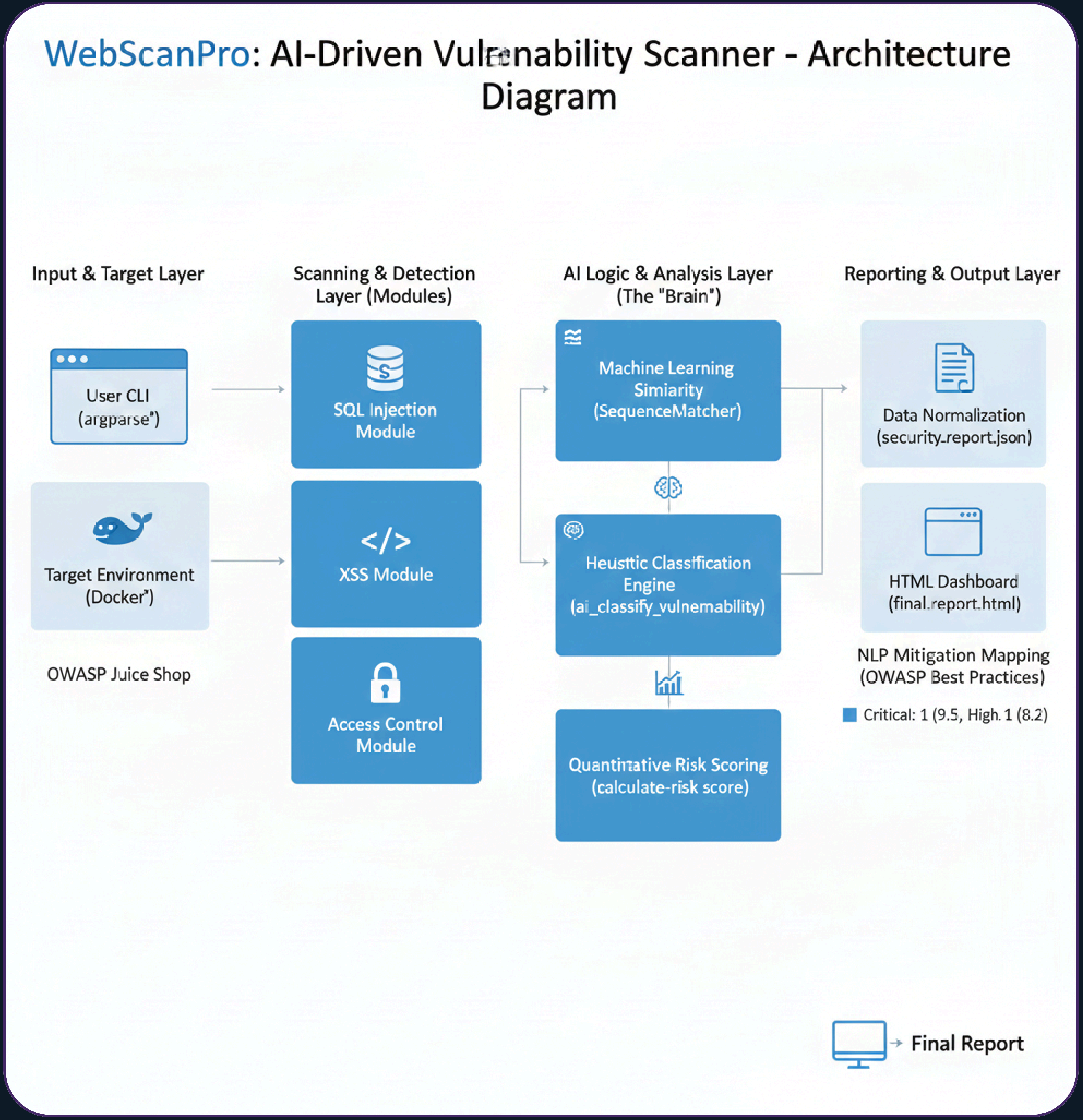
Technologies /ToolsUsed

- Python – Core programming language used to build the vulnerability scanner and AI logic
- Docker – Provides an isolated and secure environment for deploying the test application
- OWASP Juice Shop – Vulnerable web application used for security testing and validation
- HTML & CSS – Used to design the final security report dashboard
- Git & GitHub – Used for version control and project management
- AI / Machine Learning (Similarity Analysis) – Used to compare server responses and reduce false positives



System Architecture

- The user provides the target URL using a command-line interface.
- The target application (OWASP Juice Shop) runs in a Docker environment for safe testing.
- The scanner checks the application using different vulnerability modules:
  - SQL Injection
  - Cross-Site Scripting (XSS)
  - Access Control / IDOR
- Each module sends test payloads and collects server responses.
- The AI logic layer analyzes responses to confirm real vulnerabilities.
- Vulnerabilities are classified based on severity and risk score.
- The system generates a final security report in HTML format.



WebScanPro: AI-Driven Vulnerability Scanner - Architecture Diagram

Input & Target Layer
Scanning & Detection Layer (Modules)
AI Logic & Analysis Layer (The "Brain")
Reporting & Output Layer
User CLI (argparse")
Target Environment (Docker')
OWASP Juice Shop
SQL Injection Module
XSS Module
Access Control Module
Machine Learning Simiarity (SequenceMatcher)
Heusttic Classfication Engine (ai_classify_vulnemability)
Quantinative Risk Scoring (calculate-risk score)
Data Normalization (security_report.json)
HTML Dashboard (final.report.html)
NLP Mitigation Mapping (OWASP Best Practices)
Critical: 1 (9.5, High. 1 (8.2)
Final Report

Project Milestones

Requirement Analysis

Completed initial project requirements and design specifications.

Defined scope based on OWASP Top 10

Core Engine

Developed the foundational code for WebScanPro functionality.

Implemented SQL Injection, XSS, and Access Control detection

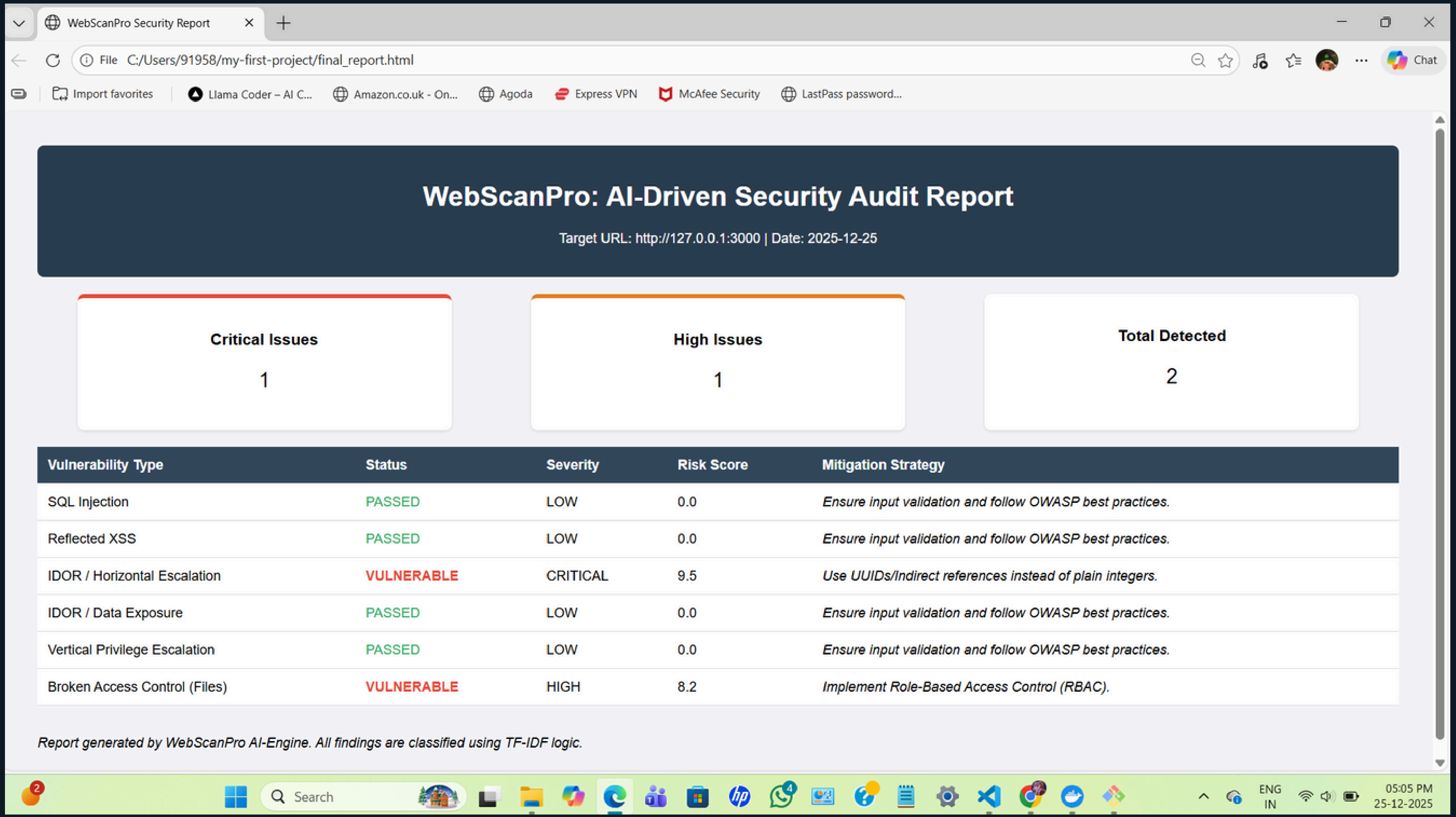
AI Integration

Implemented machine learning algorithms for enhanced scanning.

Integrated AI-based similarity analysis to reduce false positives

Results & Generated HTML Security Report

- The scanner successfully detected 2 confirmed vulnerabilities during execution
- A Critical IDOR vulnerability with a risk score of 9.5 was identified
- A High-risk Access Control vulnerability with a risk score of 8.2 was detected
- All findings were validated using AI-based logic to reduce false positives
- The results are automatically compiled into a professional HTML security report



WebScanPro: AI-Driven Security Audit Report

Target URL: http://127.0.0.1:3000 | Date: 2025-12-25

Critical Issues	High Issues	Total Detected
1	1	2

Vulnerability Type	Status	Severity	Risk Score	Mitigation Strategy
SQL Injection	PASSED	LOW	0.0	*Ensure input validation and follow OWASP best practices.*
Reflected XSS	PASSED	LOW	0.0	*Ensure input validation and follow OWASP best practices.*
IDOR / Horizontal Escalation	VULNERABLE	CRITICAL	9.5	*Use UUIDs/Indirect references instead of plain integers.*
IDOR / Data Exposure	PASSED	LOW	0.0	*Ensure input validation and follow OWASP best practices.*
Vertical Privilege Escalation	PASSED	LOW	0.0	*Ensure input validation and follow OWASP best practices.*
Broken Access Control (Files)	VULNERABLE	HIGH	8.2	*Implement Role-Based Access Control (RBAC).*

Report generated by WebScanPro AI-Engine. All findings are classified using TF-IDF logic.

The report includes:

- Executive summary for quick review
- Detailed vulnerability information with severity and risk score
- AI-assisted mitigation suggestions based on OWASP best practices

Conclusion

- WebScanPro successfully implements an AI-driven web vulnerability scanning system
- The project automates detection of security vulnerabilities based on OWASP Top 10 standards
- AI-based similarity analysis helps reduce false positives and improve detection accuracy
- The system effectively identified Critical IDOR and High-risk Access Control vulnerabilities
- Automatic generation of a professional HTML security report enhances usability
- Overall, the project demonstrates the practical application of AI in cybersecurity