WebScanPro – AI-Powered Web Application Security Testing Tool

By Deekshitha B R

deekshithabr.22aiml@saividya.ac.in

Introduction

- **What is WebScanPro?**
- WebScanPro is an automated web security testing tool
- Designed to detect vulnerabilities based on OWASP Top 10
- Combines rule-based scanning + AI/ML intelligence

- **Why it matters:**
- Web apps are frequent attack targets
- Manual testing is time-consuming and error-prone
- Need for intelligent, automated security testing

Problem Statement

- **Many web applications suffer from:**
- SQL Injection
- Cross-Site Scripting (XSS)
- Broken Authentication
- IDOR & Access Control flaws

- **Traditional scanners:**
- Produce false positives
- Miss logic-based vulnerabilities

- 👉Solution: WebScanPro with AI-driven analysis

Project Objectives

- Detect common web vulnerabilities automatically
- Simulate real-world attack scenarios
- Use AI/ML to:
- Reduce false positives
- Detect abnormal behavior
- Generate professional security reports
- Improve secure coding awareness

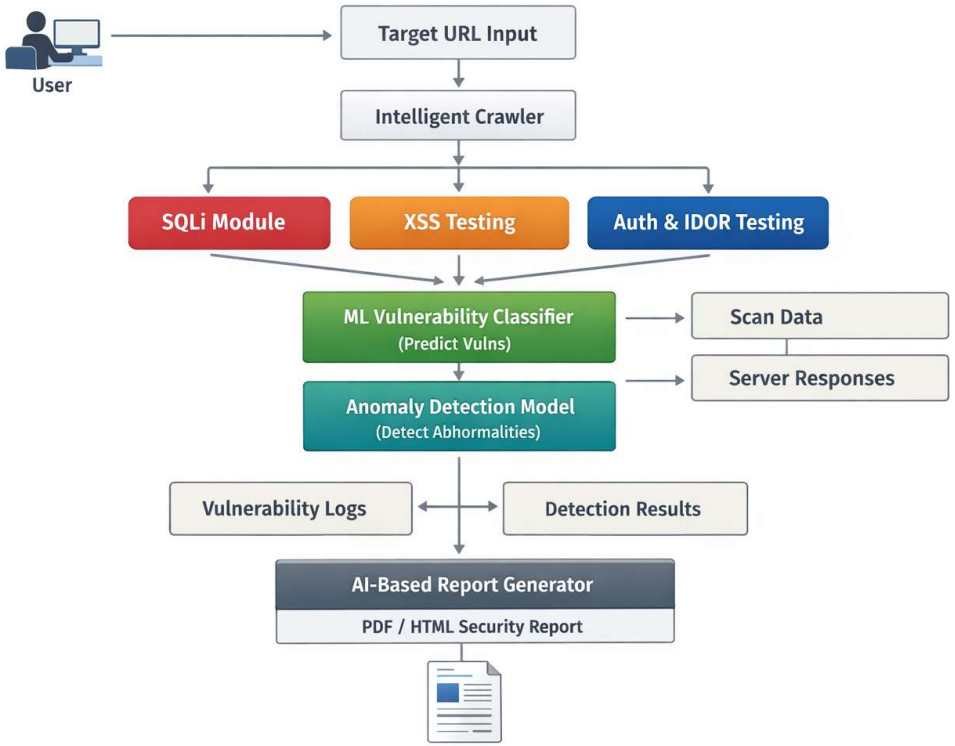
Technologies Used

- **Frontend:**
- HTML, CSS, JavaScript (or React)
- **Backend:**
- Python, Flask / FastAPI
- **Security Testing:**
- BeautifulSoup, Selenium
- **AI/ML:**
- Scikit-learn, NLP techniques, Anomaly Detection models
- **Testing Platforms:**
- DVWA, OWASP Juice Shop. bWAPP

System Architecture

- User inputs target URL
- Intelligent crawler discovers inputs
- Vulnerability modules test endpoints
- AI/ML analyzes responses
- Report generator produces final output

System Architecture



Overall Workflow

Step-by-step flow:

1. Load target URL
2. Run intelligent crawler
3. Discover pages & input fields
4. Generate AI-based payloads
5. Send requests & collect responses
6. ML classifier detects vulnerabilities
7. Anomaly detection for unknown issues
8. Generate AI-based report

Vulnerability Modules

Implemented Modules:

- SQL Injection Testing
- XSS Testing
- Authentication & Session Testing
- Access Control & IDOR Testing

Each module:

- Uses automated payload injection
- Analyzes server responses
- Logs vulnerabilities with evidence

SQL Injection Module

- Injects crafted SQL payloads
- Detects:
- Error-based SQLi
- Boolean-based SQLi
- Time-based SQLi
- Identifies vulnerable parameters
- Suggests parameterized queries as mitigation

XSS Testing Module

- Tests:
- Reflected XSS
- Stored XSS
- Injects JavaScript payloads
- Analyzes responses and DOM behavior
- Logs vulnerable endpoints

Authentication & Session Testing

- Weak/default credential testing
- Brute-force attack simulation
- Session cookie analysis:
- Secure
- HttpOnly
- SameSite
- Session hijacking & fixation testing

Access Control & IDOR Testing

- Identifies user roles (Admin, User, Guest)
- Tests:
- Horizontal privilege escalation
- Vertical privilege escalation
- Modifies object IDs (IDOR)
- Detects missing authorization checks

AI/ML Integration

- Why AI/ML?
- Traditional scanners are rule-based
- AI improves accuracy and adaptability
- AI Usage:
- ML classifiers for vulnerability prediction
- Anomaly detection for unknown flaws
- Intelligent payload generation
- AI-based severity scoring

Anomaly Detection

- Uses ML models like:
- Isolation Forest
- One-Class SVM
- Detects:
- Abnormal responses
- Logic flaws
- Unexpected access behavior
- Helps identify zero-day–like issues

AI-Based Report Generation

- Automatically generates:
- Vulnerability description
- Impact analysis
- Severity level
- Mitigation steps
- Formats:
- HTML
- PDF
- Professional, developer-friendly output

Results & Key Findings

- Successfully detected:
- SQL Injection vulnerabilities
- XSS issues
- Weak authentication flaws
- IDOR vulnerabilities
- Reduced false positives using AI logic
- Improved clarity in reporting

Suggested Mitigations

- Input validation & sanitization
- Parameterized queries
- Secure authentication practices
- RBAC / ABAC for access control
- Secure session handling
- Regular security testing

Limitations

- Designed for testing vulnerable applications
- AI models trained on limited datasets
- Dynamic JavaScript-heavy apps may need more tuning

Future Enhancements

- Support for more OWASP vulnerabilities
- Advanced deep learning models
- CI/CD pipeline integration
- Real-time monitoring dashboard
- Cloud-based deployment

Conclusion

- WebScanPro provides an intelligent approach to web security testing
- Combines automation with AI/ML
- Generates actionable, professional reports
- Helps developers build more secure applications

THANK YOU