Product Requirements Document (PRD)

Overview

OWASP Juice Shop is a deliberately insecure web application designed for educational and training purposes. It replicates a real-world e-commerce site filled with security vulnerabilities. It is widely used by developers, penetration testers, and security enthusiasts to practice and improve their skills.

Goals

- Simulate common and advanced security vulnerabilities.
- Provide hands-on experience with web application security issues.
- Facilitate Capture the Flag (CTF) challenges and security workshops.
- Promote awareness and adoption of secure coding practices.

Features

- Fully functional e-commerce store simulation.
- Extensive vulnerabilities, including OWASP Top Ten and beyond.
- Built-in CTF mode with downloadable challenge sets.
- Gamification with progress tracking and scoreboard.
- REST API with security flaws for API security testing.
- Hint system for users needing assistance.
- Supports Docker, cloud deployment, and local installations.
- Multilingual interface.

Target Audience

- Developers and DevSecOps teams
- Penetration testers and security researchers

- Security educators and students

- Organizations conducting internal training

Functional Requirements

FR-1: Simulate browsing, purchasing, and user authentication flows

FR-2: Embed intentional vulnerabilities across functionalities

FR-3: Admin interface accessible through solving challenges

FR-4: Display progress through a dynamic scoreboard

FR-5: Provide CTF mode configuration

FR-6: REST APIs must have exploitable flaws

FR-7: Offer optional hints for challenges

FR-8: Allow Docker, Heroku, and local deployments

Non-Functional Requirements

NFR-1: Responsive design for desktop and mobile browsers

NFR-2: Quick setup and low entry barrier (easy installation)

NFR-3: Open-source under MIT License

NFR-4: Support internationalization (i18n)

NFR-5: Allow modular challenge additions

Assumptions

- Users are familiar with basic web application concepts.

- Organizations have local or cloud hosting capabilities.

Constraints

- Must intentionally retain insecure coding patterns.

- Should not be exposed to the public internet without disclaimers.

Milestones

- Deployment Setup (Docker, Local, Cloud): Immediate
- Enable CTF Mode and Testing: Within 1 week
- Conduct Security Training / Workshop: Within 1-3 months

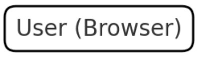
Risks

- Risk of misuse if publicly exposed.
- Potential confusion for beginners due to high vulnerability density.

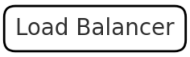
Architecture Diagrams

Basic Architecture:

Docker Deployment Architecture:



Kubernetes Deployment Architecture:



References

- OWASP Juice Shop GitHub: https://github.com/juice-shop/juice-shop

- OWASP Juice Shop Documentation: https://owasp-juice.shop