OWASP

OWASP

- Open Web Application Security Project
  - Free and open software security community
  - 501(c)(3) Nonprofit organization
- Core purpose
  - Be the thriving global community that drives visibility and evolution in the safety and security of the world's software

OWASP Top 10 Builders Defenders

1	Injection	6	Security Misconfiguration
2	Broken Authentication	7	Cross-Site-Scripting (XSS)
3	Sensitive Data Exposure	8	Insecure Deserialization
4	XML External Entities	9	Using Components with Known Vulnerabilities
5	Broken Access Control	10	Insufficient Logging & Monitoring

Risk Rating Table

Threat Agents	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	SEVERE: 3	App / Business Specific
	AVERAGE: 2	COMMON: 2	AVERAGE: 2	MODERATE: 2	
	DIFFICULT: 1	UNCOMMON: 1	DIFFICULT: 1	MINOR: 1	

Based on the OWASP Risk Rating Methodology

OWASP Juice Shop

Builders Breakers Defenders

OWASP Juice Shop is probably the most modern and sophisticated insecure web application! It can be used in security trainings, awareness demos, CTFs and as a guinea pig for security tools! Juice Shop encompasses vulnerabilities from the entire OWASP Top Ten along with many other security flaws found in real-world applications!

Main Selling Points

- **Free and Open source**: Licensed under the MIT license with no hidden costs or caveats
- **Easy-to-install**: Choose between node.js, Docker and Vagrant to run on Windows/Mac/Linux
- **Self-contained**: Additional dependencies are pre-packaged or will be resolved and downloaded automatically
- **Beginner-friendly**: Hacking Instructor tutorial scripts guide users through several of the easier challenges while explaining the underlying vulnerabilities
- **Gamification**: The application notifies you on solved challenges and keeps track of successfully exploited vulnerabilities on a Score Board

- **Self-healing**: The simple SQLite and MarsDB databases are wiped and repopulated from scratch on every server startup
- **Re-branding**: Fully customizable in business context and look & feel to your own corporate or customer requirements
- **CTF-support**: Challenge notifications optionally contain a flag code for your own Capture-The-Flag events
- 

Official Companion Guide

> Pwning OWASP Juice Shop [...] will give you a complete overview of the vulnerabilities found in the application including hints how to spot and exploit them. In the appendix you will even find complete step-by-step solutions to every challenge. The ebook is continuously published under CC BY-NC-ND 4.0 and is online-readable **for free**. The latest officially released edition is available **for free** on LeanPub in PDF, Kindle and ePub format.

THIS IS THE OFFICIAL COMPANION GUIDE TO THE OWASP JUICE SHOP APPLICATION. BEING A WEB APPLICATION WITH A VAST NUMBER OF INTENDED SECURITY VULNERABILITIES, THE OWASP JUICE SHOP IS SUPPOSED TO BE THE OPPOSITE OF A BEST PRACTICE OR TEMPLATE APPLICATION FOR WEB DEVELOPERS: IT IS AN AWARENESS, TRAINING, DEMONSTRATION AND EXERCISE TOOL FOR SECURITY RISKS IN MODERN WEB APPLICATIONS. THE OWASP JUICE SHOP IS AN OPEN-SOURCE PROJECT HOSTED BY THE NON-PROFIT OPEN WEB APPLICATION SECURITY PROJECT (OWASP) AND IS DEVELOPED AND MAINTAINED BY VOLUNTEERS.

BJÖRN KIMMINICH HAS OVER TWO DECADES OF PROGRAMMING EXPERIENCE WITH EXPERTISE ON SOFTWARE SUSTAINABILITY, CLEAN CODE AND TEST AUTOMATION AS WELL AS APPLICATION SECURITY. HE IS THE PROJECT LEADER OF THE OWASP JUICE SHOP AND MEMBER OF THE GERMAN OWASP CHAPTER BOARD.

Exercise

Happy path shopping tour

1. Register a user account at your local Juice Shop
2. Browse the inventory and purchase some products
3. Try out all other functionality you find in the application

Exercise

Score Board

1. (🎓) Find the hidden *Score Board* in the Juice Shop (⭐)