OWASP

OWASP

- **O**pen **W**eb **A**pplication **S**ecurity **P**roject
  - 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

Principles

- Free & Open
- Governed by rough consensus & running code
- Abide by a code of ethics
- Not-for-profit
- Not driven by commercial interests
- Risk based approach

OWASP Top 10

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

Top 10 Risk Factor Summary

Risk	Threat Agents	Attack Vectors (Exploitability)	Security Weakness (Prevalence)	Security Weakness (Detectability)	Impacts (Technical)	Impacts (Business)	Score
A1:2017-Injection	App Specific	EASY: 3	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	8.0
A2:2017-Broken Authentication	App Specific	EASY: 3	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A3:2017-Sensitive Data Exposure	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE: 2	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE: 2	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	6.0
A6:2017-Security Misconfiguration	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT: 1	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	MODERATE: 2	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE: 2	WIDESPREAD: 3	DIFFICULT: 1	MODERATE: 2	App Specific	4.0

OWASP Juice Shop

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!

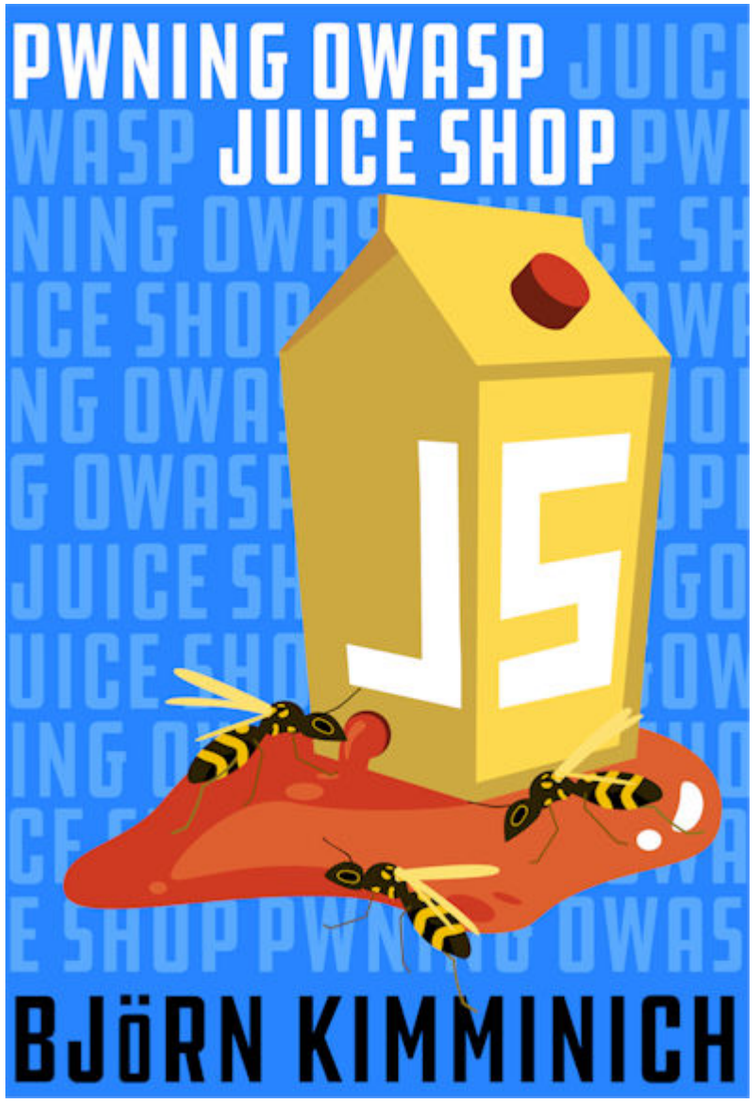
Main Selling Points

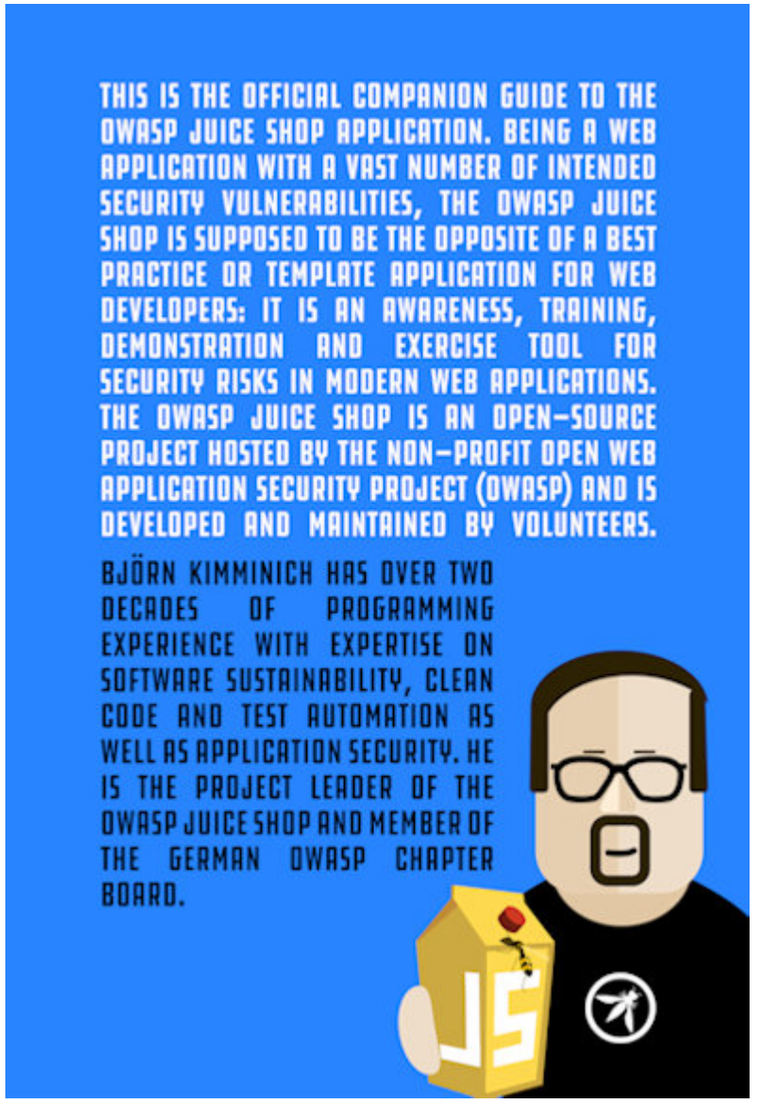
- **Easy-to-install**: Choose between node.js, Docker and Vagrant to run on Windows/Mac/Linux
- **Self-contained**: Additional dependencies are pre-packaged or will be resolved and downloaded automatically
- **Self-healing**: The simple SQLite database is wiped and regenerated from scratch on every server startup
- **Gamification**: The application notifies you on solved challenges and keeps track of successfully exploited vulnerabilities on a Score Board

- **CTF-support**: Challenge notifications contain a customizable flag code for your own Capture-The-Flag events
- **Re-branding**: Fully customizable business context and look & feel
- **Free and Open source**: Licensed under the MIT license with no hidden costs or caveats

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 published under CC BY-NC-ND 4.0 and is available **for free** as work-in-progress in HTML, PDF, Kindle and ePub format on GitBook. The latest officially released edition is available **for free** on LeanPub in PDF, Kindle and ePub format.





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 (⭐)