JUICE SHOP

An intentionally insecure Javascript Web Application

https://github.com/bkimminich/juice-shop

Created by Björn Kimminich / @bkimminich

WHY THE NAME "JUICE SHOP"?!?

Translating "dump" or "useless outfit" into German yields "Saftladen" which can be reverse-translated word by word into "juice shop". Hence the project name.

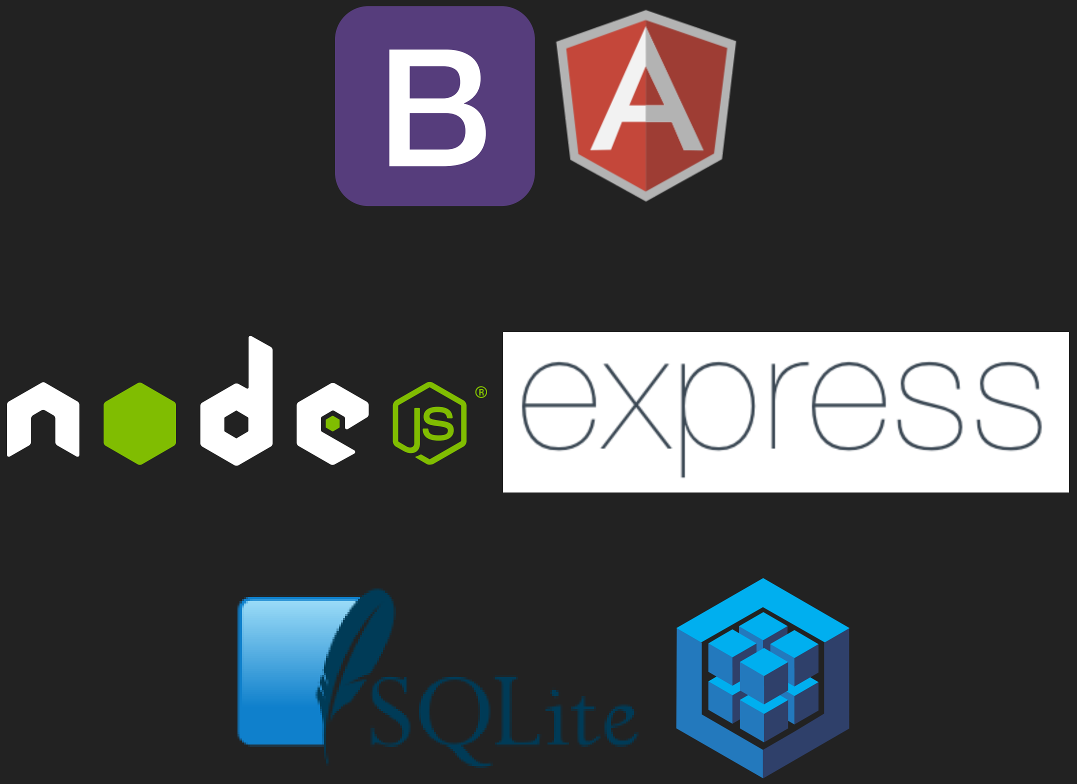
That the initials "JS" match with those of "Javascript" was purely coincidental!

WHY ANOTHER BROKEN WEBAPP?!?

Juice Shop is the first application written entirely in Javascript listed in the OWASP VWA Directory. It also seems to be the first broken webapp that uses the currently popular architecture of an SPA/RIA frontend with a RESTful backend.

TECHNOLOGY STACK

Javascript all the way from UI to REST API



SIMPLE INSTALLATION

Works in local and containerized environment

JS
TM
docker
amazon
web services

LIVE DEMO

Let's enjoy the Juice Shop like an average happy shopper...

27 CHALLENGES

Covering various vulnerabilities and design flaws

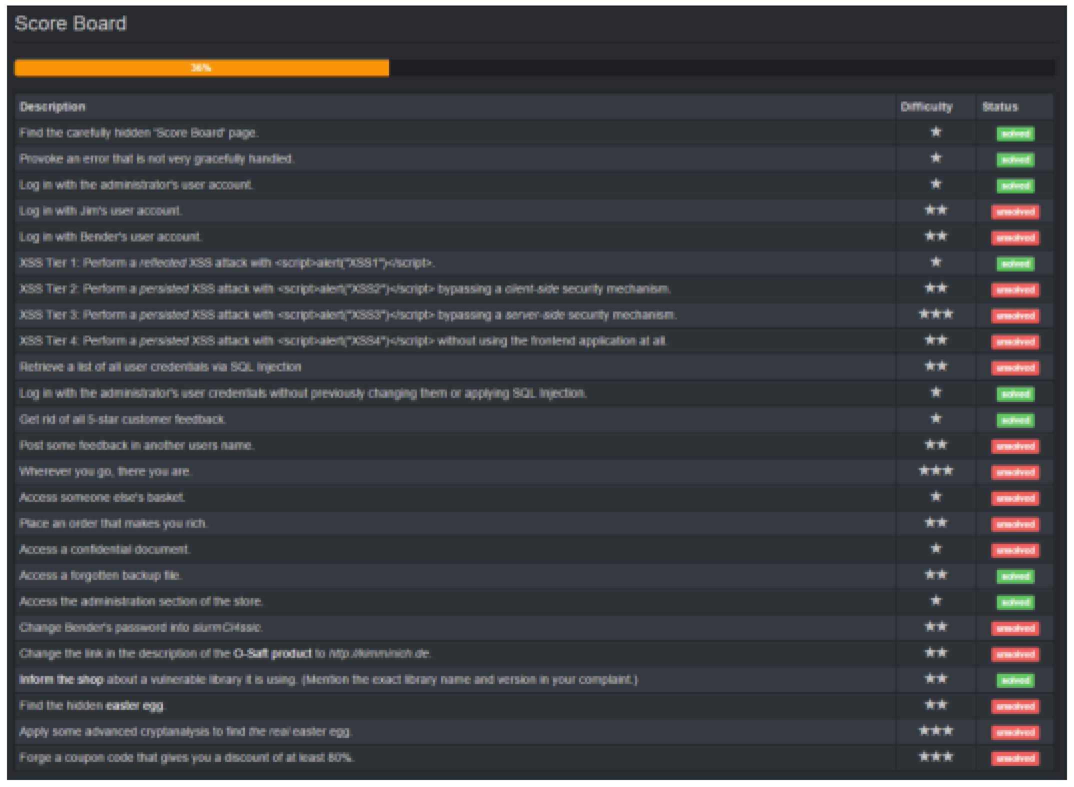
Juice Shop covers all vulnerabilities from the latest OWASP Top 10 and more.

CHALLENGE DIFFICULTY

Contains low-hanging fruits & hard-to-crack nuts

SCORE BOARD

Challenge progress is tracked on server-side



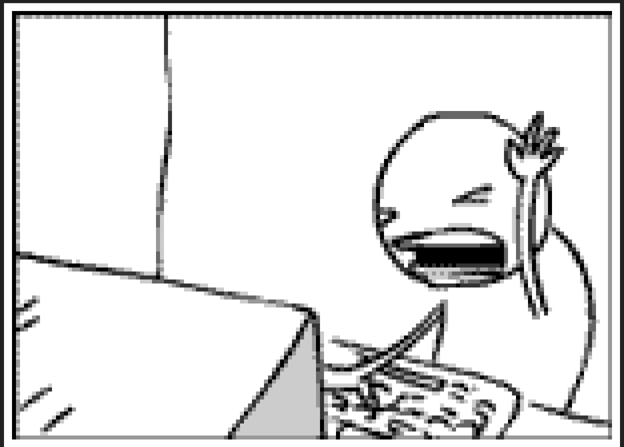
Score Board

36%

Description	Difficulty	Status
Find the carefully hidden 'Score Board' page.	★	solved
Provoke an error that is not very gracefully handled.	★	solved
Log in with the administrator's user account.	★	solved
Log in with Jim's user account.	★★	unsolved
Log in with Bender's user account.	★★	unsolved
XSS Tier 1: Perform a *reflected* XSS attack with <script>alert("XSS1")</script>.	★	solved
XSS Tier 2: Perform a *persisted* XSS attack with <script>alert("XSS2")</script> bypassing a *client-side* security mechanism.	★★	unsolved
XSS Tier 3: Perform a *persisted* XSS attack with <script>alert("XSS3")</script> bypassing a *server-side* security mechanism.	★★★	unsolved
XSS Tier 4: Perform a *persisted* XSS attack with <script>alert("XSS4")</script> without using the frontend application at all.	★★	unsolved
Retrieve a list of all user credentials via SQL Injection	★★	unsolved
Log in with the administrator's user credentials without previously changing them or applying SQL Injection.	★	solved
Get rid of all 5-star customer feedback.	★	solved
Post some feedback in another users name.	★★	unsolved
Wherever you go, there you are.	★★★	unsolved
Access someone else's basket.	★	unsolved
Place an order that makes you rich.	★★	unsolved
Access a confidential document.	★	unsolved
Access a forgotten backup file.	★★	solved
Access the administration section of the store.	★	solved
Change Bender's password into *slurmCl4ssic*.	★★	unsolved
Change the link in the description of the **O-Saft product** to *http://kimminich.de*.	★★	unsolved
Inform the shop about a vulnerable library it is using. (Mention the exact library name and version in your complaint.)	★★	solved
Find the hidden **easter egg**.	★★	unsolved
Apply some advanced cryptanalysis to find *the real* easter egg.	★★★	unsolved
Forge a coupon code that gives you a discount of at least 80%.	★★★	unsolved

SORRY, THIS IS A LIGHTNING TALK

I will not live-hack even a single challenge for you!



E2E HACKING TESTSUITE VIDEO

I will instead show you a prerecorded execution of the testsuite automatically hacking all 27 challenges!

For details on the testsuite implementation and CI-integration check out my Guest Post: Proving that an application is as broken as intended on The SauceLabs Blog.

DO YOU ACCEPT THE CHALLENGE?

Breakers Try to hack all the challenges!

Defenders Let loose all your fancy tools!

Builders Learn from my silly mistakes!

Bonus challenge: Contribute to Juice Shop by reporting bugs or helping to fix issues!

Created with reveal.js - The HTML Presentation Framework