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

- B
- Angular
- Node.js
- Express
- SQLite
SIMPLE INSTALLATION

Works in local and containerized environment

![JavaScript](js.png) ![Docker](docker.png) ![Amazon Web Services](aws.png)
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
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!
COPYRIGHT (C) 2015 BJÖRN KIMMINICH
Licensed under the MIT license.

Created with reveal.js - The HTML Presentation Framework