ADDO

ALL DAY DEVOPS

NOVEMBER 6, 2019

Björn Kimminich

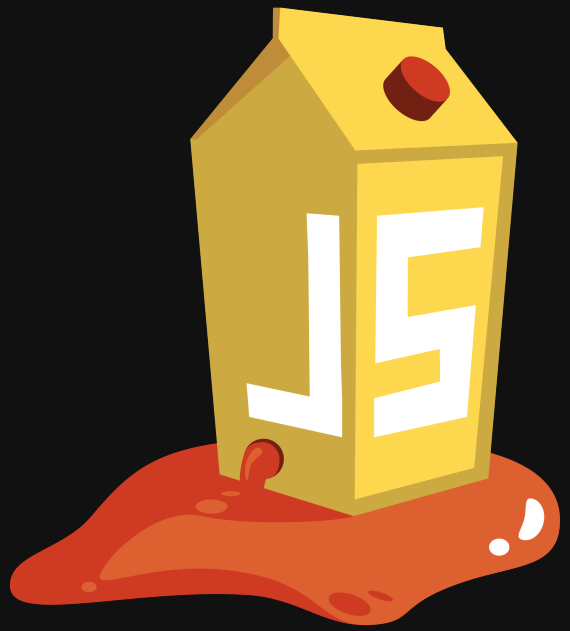
OWASP Juice Shop

The Ultimate All Vuln WebApp


Let us begin with a
happy path
shopping tour
like unsuspecting average Joe & Jane!

Wow, that was a perfectly fine shopping experience! No noteworthy errors, everything shiny & working as it should!

OWASP Juice Shop is looking forward to see you soon as a happy customer!



https://owasp-juice.shop

👋 That's it, thanks for watching!?!?

Let's take a look behind the curtain and explore why OWASP Juice Shop claims to be **"probably the most modern and sophisticated insecure web application!"**

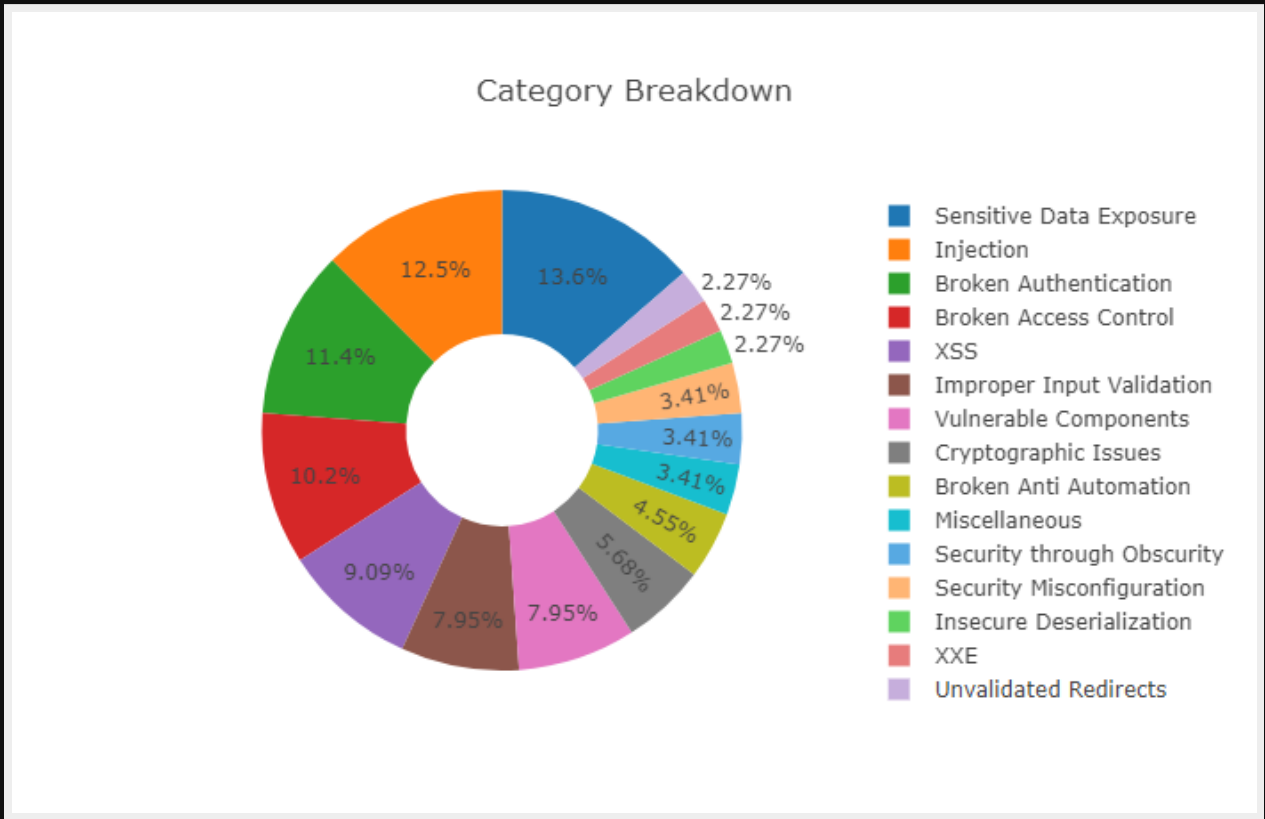
Why "Juice Shop"?!?

Translating "dump" or "useless outfit" into German yields "Saftladen" which is a compound word from "Saft" and "Laden". This reverse-translates into "juice" and "shop". Hence the project name.

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

88+ Hacking Challenges

Covering various vulnerabilities and serious design flaws



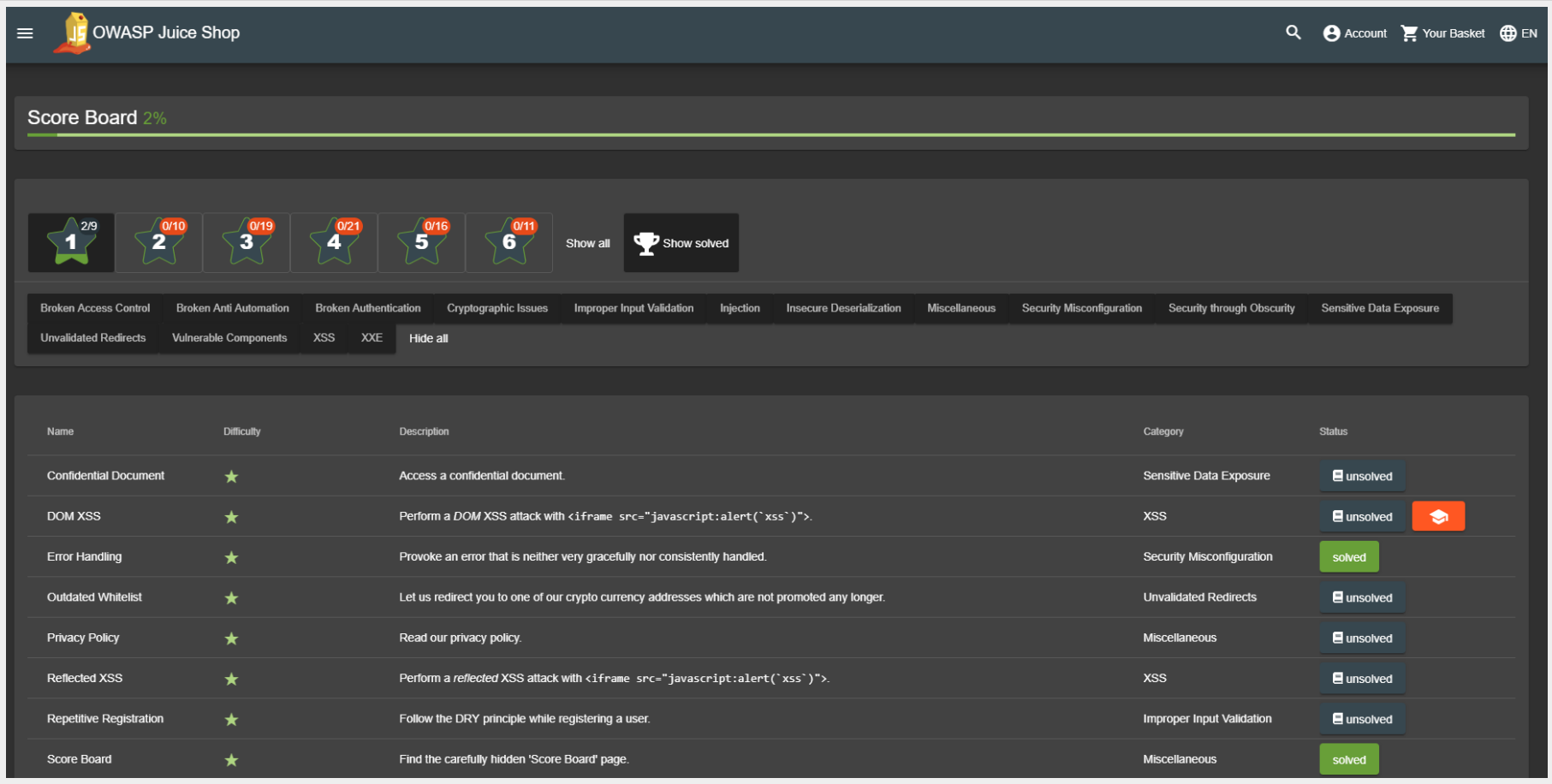
OWASP Juice Shop covers all vulnerabilities from the latest OWASP Top 10 and more.

Challenge Difficulty

There's something to do for beginners and veterans alike

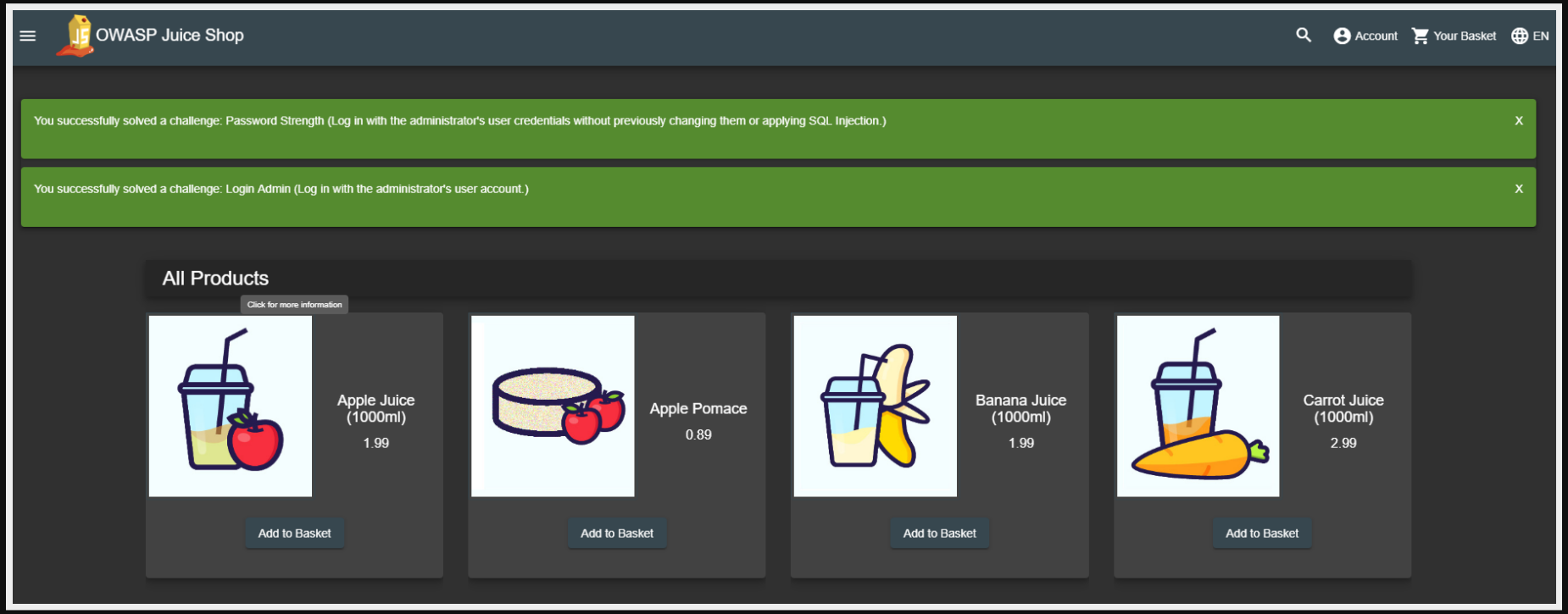
Score Board

Challenge progress is tracked on server-side



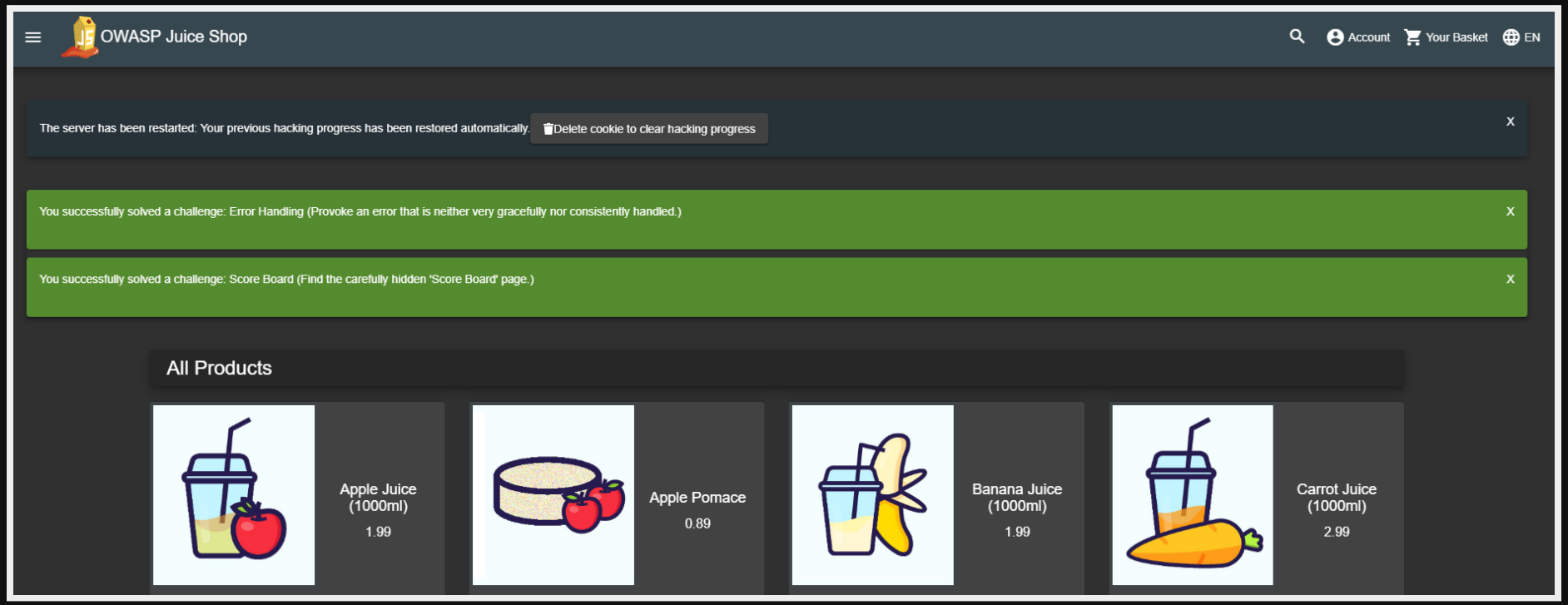
Immediate Feedback

Solved challenges are announced as push notifications



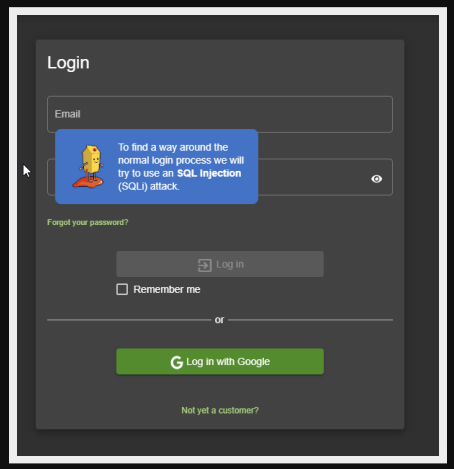
Restore your Progress

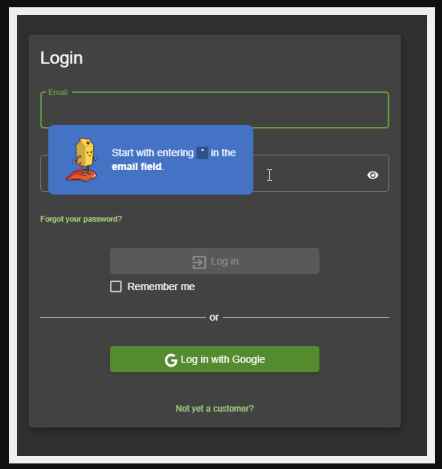
Auto-saves your hacking progress and restores on server restart

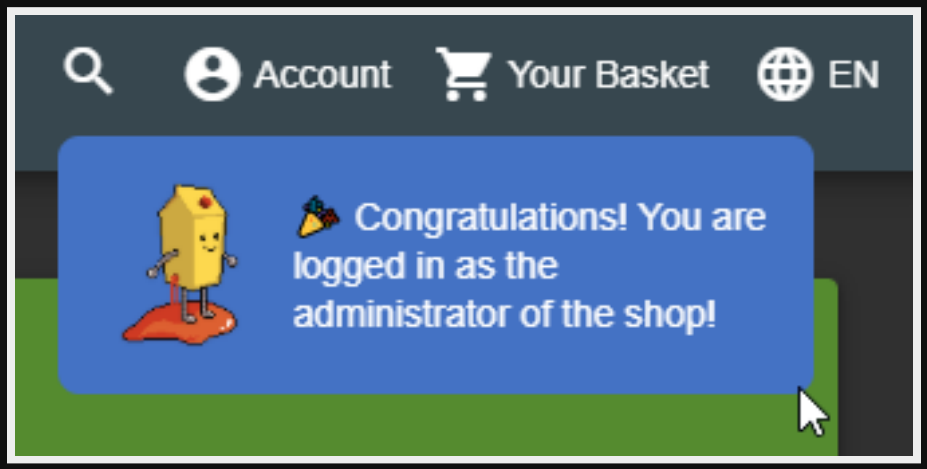


Hacking Instructor (🚧)

Some challenges come with an embedded interactive tutorial

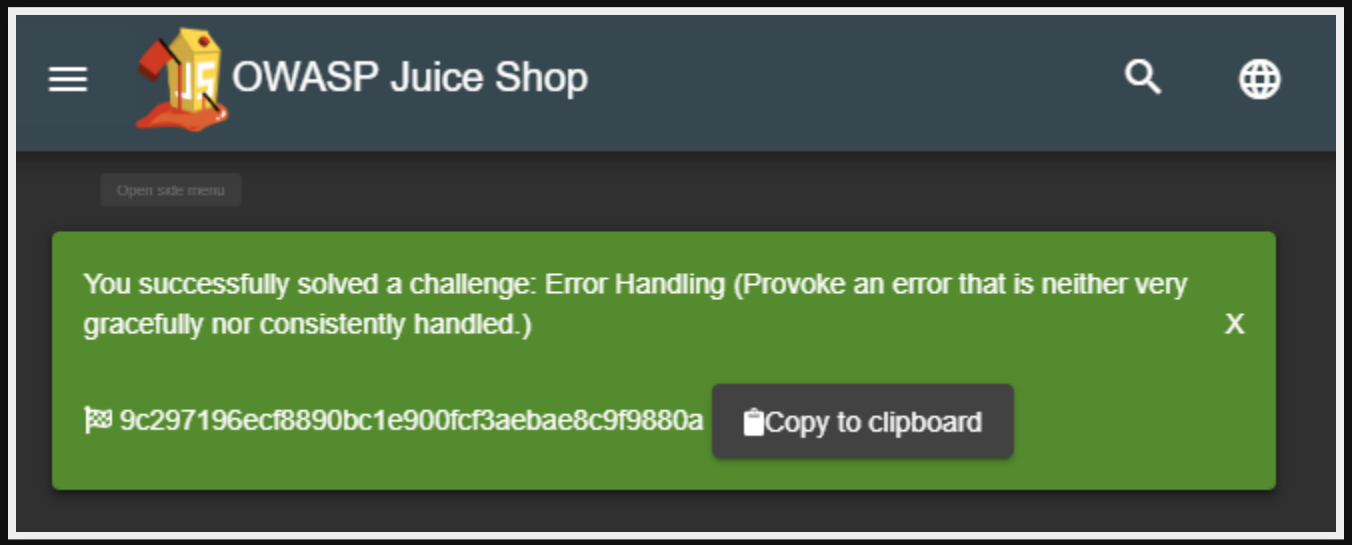






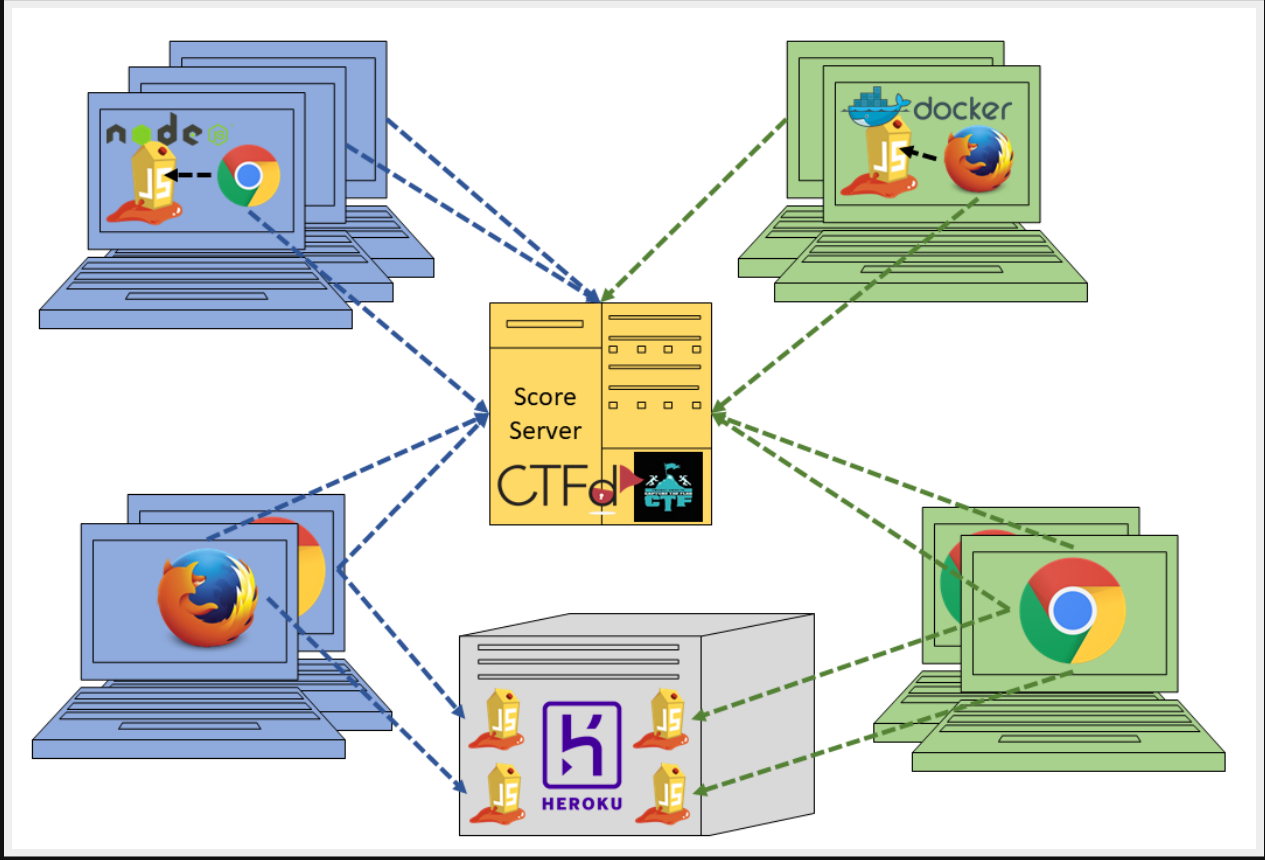
Juice Shop is CTF-ready

Flag codes can optionally be displayed for solved challenges



Frictionless CTF-Events

All participants use individual Juice Shop instances anywhere, sharing only the flag code-`ctfKey` and a central score server.



CTF Extension 6.x

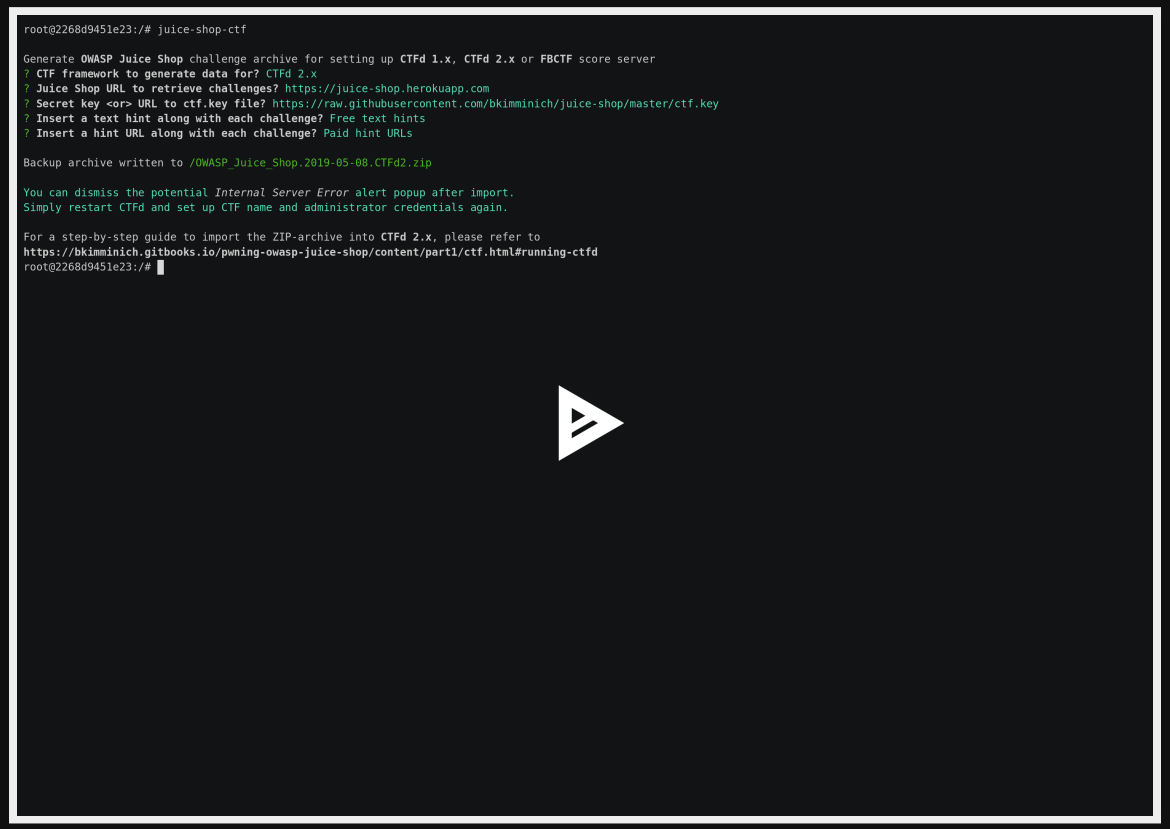
Utility project to help you host a hacking event on CTFd or FBCTF

Simple Installation

Locally via `npm i -g juice-shop-ctf-cli` or as Docker container

Setup Wizard

Run `juice-shop-ctf` on the command line and let a wizard create a data-backup archive to conveniently import into CTFd or FBCTF



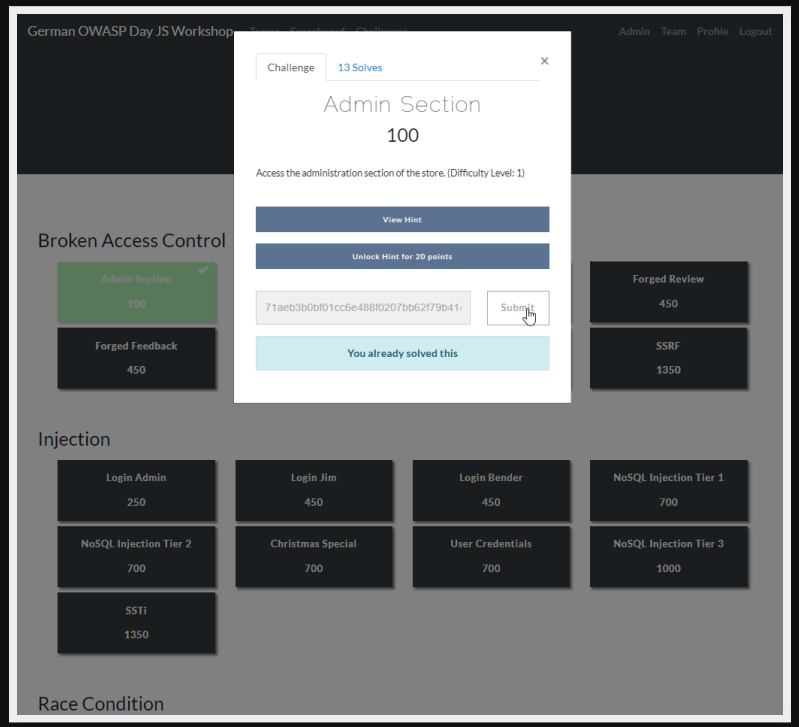
Configuration File Option

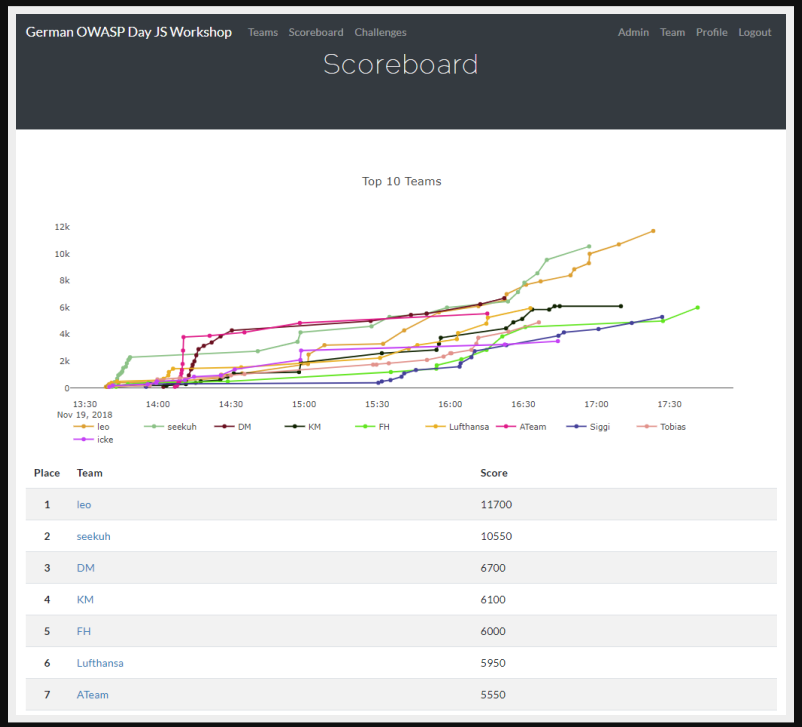
Run `juice-shop-ctf --config myconfig.yml` to use non-interactive mode passing in configuration via YAML file

```
ctfFramework: CTFd 2.x | CTFd 1.x | FBCTF
juiceShopUrl: https://juice-shop.herokuapp.com
ctfKey: https://raw.githubusercontent.com/bkimminich/juice-shop/master/ctf.key
countryMapping: https://raw.githubusercontent.com/bkimminich/juice-shop/master/config/f
insertHints: none | free | paid
insertHintUrls: none | free | paid
```

CTFd for OWASP Juice Shop

Your CTFd instance will be ready-to-hack in <5min

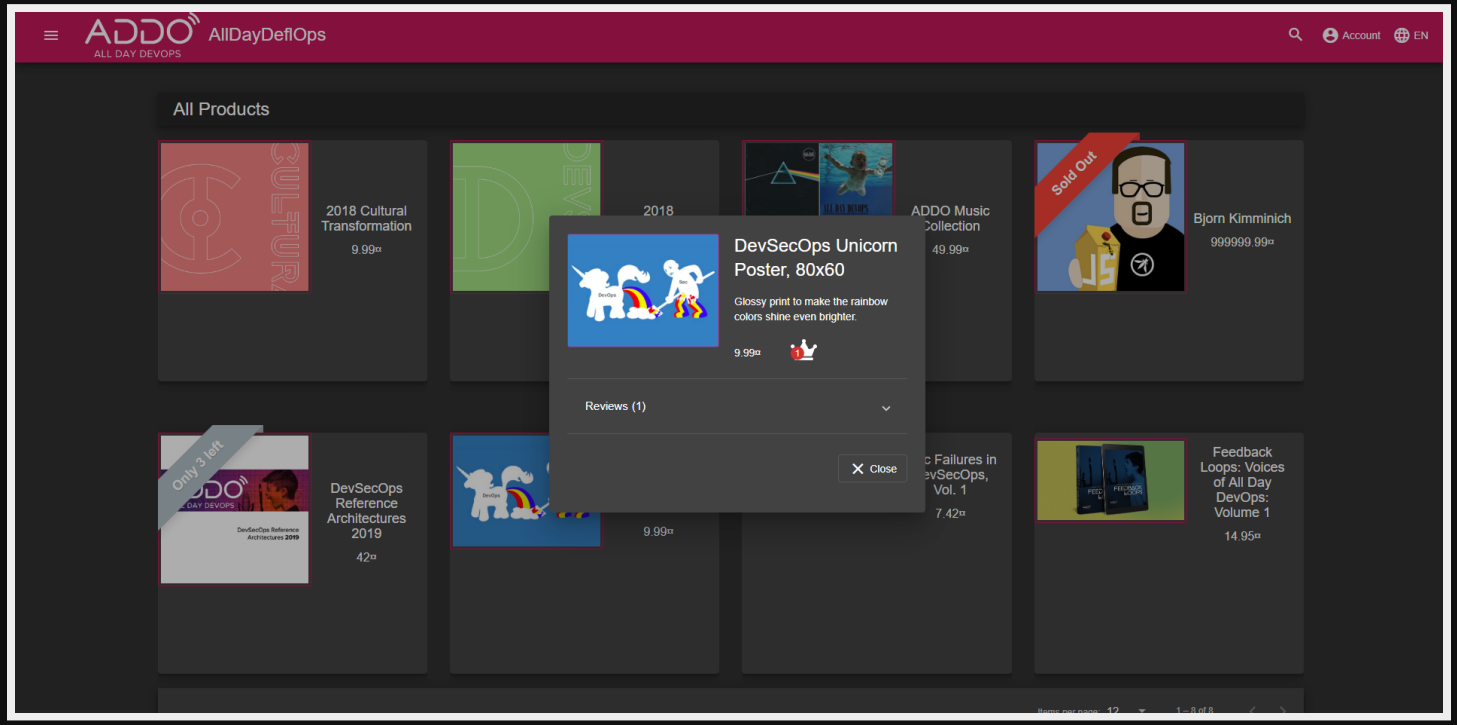




Place	Team	Score
1	leo	11700
2	seekuh	10550
3	DM	6700
4	KM	6100
5	FH	6000
6	Lufthansa	5950
7	ATeam	5550

Re-branding

Fully customizable business context and look & feel



Configurative Customization

Customize the application via a simple YAML file

```yaml
application:
  domain: ad.do
  name: 'AllDayDeflOps'
  logo: 'https://www.alldaydevops.com/[...]/2019%20Logo%20Files/ADDO_Logo_2019_White.sv
  favicon: 'https://www.sonatype.com/hubfs/ADDO-2018/ADDO_fav4.png'
  theme: pink-bluegrey
  showGitHubLinks: false
  twitterUrl: 'https://twitter.com/AllDayDevOps'
  facebookUrl: 'https://www.facebook.com/AllDayDevOps/'
  [...]
```

Choose your own inventory

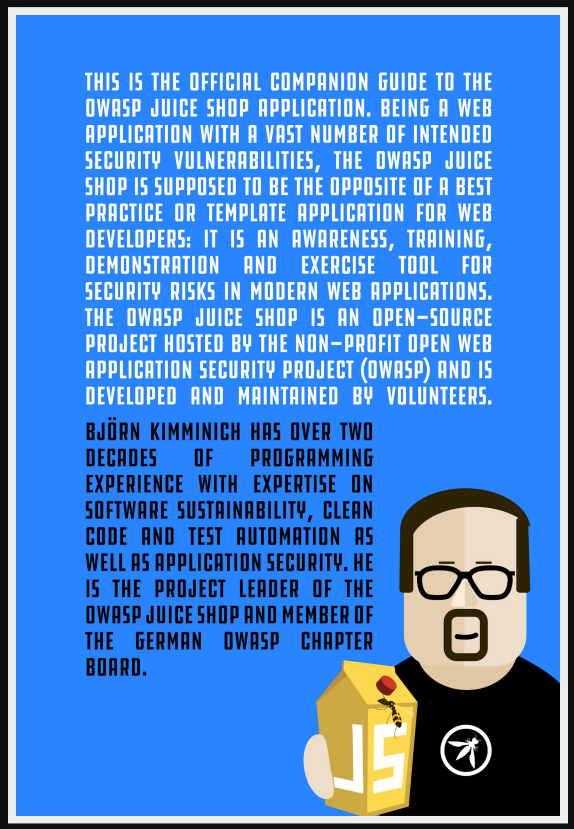
The YAML configuration allows you to override all products

```yaml
products:
  [...]
  - name: 'DevSecOps Reference Architectures 2019'
    description: 'Gloriously referential! Whitepaperesquely architectural!'
    price: 42.00
    quantity: 3
    image: 'https://www.alldaydevops.com/hubfs/2019-ADDO/[...]/Untitled%20design%20(3).
    urlForProductTamperingChallenge: 'http://bit.ly/2YIjdt7'
  - name: 'DevSecOps Reference Architectures 2018'
    description: 'Very referential! Mildly architectural!'
    price: 21.00
    image: undefined.jpg
    useForChristmasSpecialChallenge: true
  [...]
```

Your config is validated on server startup to prevent broken or unsolvable challenges!

Free Companion Guide

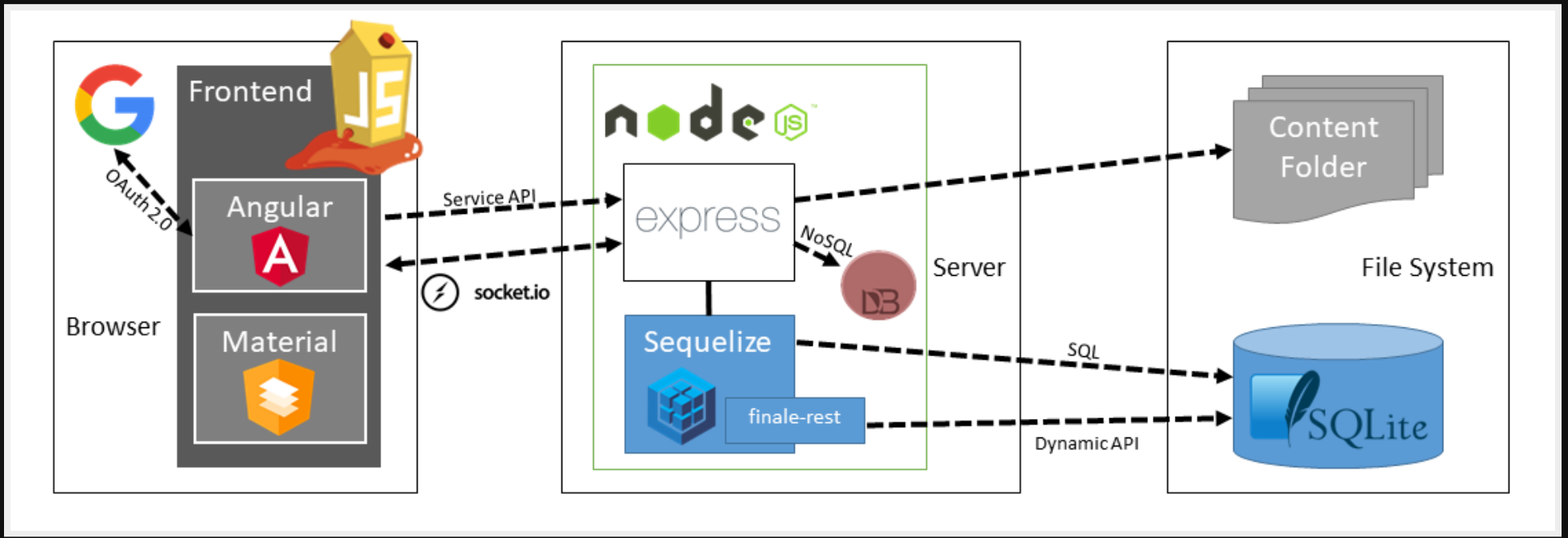
Contains all the setup documentation, hints & step-by-step solutions per challenge, contribution guidelines, trainers guide and more!



The eBook is available **for free** on Leanpub but also be read online.

Modern Web-Architecture

JavaScript/TypeScript all the way from UI to REST API



Simple Installation

Comes with cloud, local and containerized run options

Test Pyramid

Maximizing Test Automation & Code Coverage

Protractor
end to end testing for AngularJS

frisby.js

Jasmine

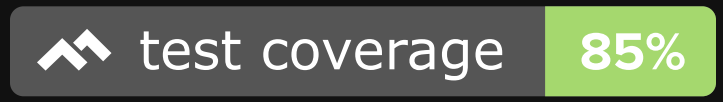
MOCHA

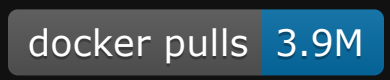
DevOps Pyramid

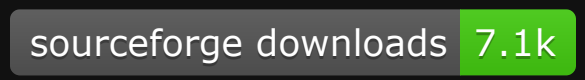
Automated Build, CI/CD & Code Analysis

Juice Shop Success Pyramid™

Some amazing facts & stats about the project







Additional Information

Official Site http://owasp-juice.shop

Sourcecode	https://github.com/bkimminich/juice-shop (MIT) https://github.com/bkimminich/juice-shop-ctf (MIT) https://github.com/bkimminich/pwning-juice-shop (CC-BY-NC-ND)

Bonus Material on Web Application Security

IT Security Lecture (CC-BY-SA)	https://github.com/bkimminich/it-security-lecture
Web Application Security in a Nutshell (CC-BY-SA)	http://webappsec-nutshell.kimminich.de

👋 That's it, thanks for watching!