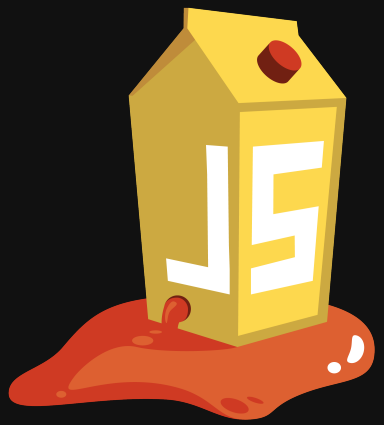
Fork me on GitHub

OWASP Juice Shop 8.x

~~An intentionally insecure JavaScript Web Application~~

The most trustworthy online shop out there (@dschadow) — The best juice shop on the whole internet! (@shehackspurple)
Actually the most bug-free vulnerable application in existence! (@vanderaj) — First you 😂😂 then you 😢 (@kramse)



http://owasp-juice.shop

Presentation by Björn Kimminich / @bkimminich

What is "OWASP"?!?

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software.

Why "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!

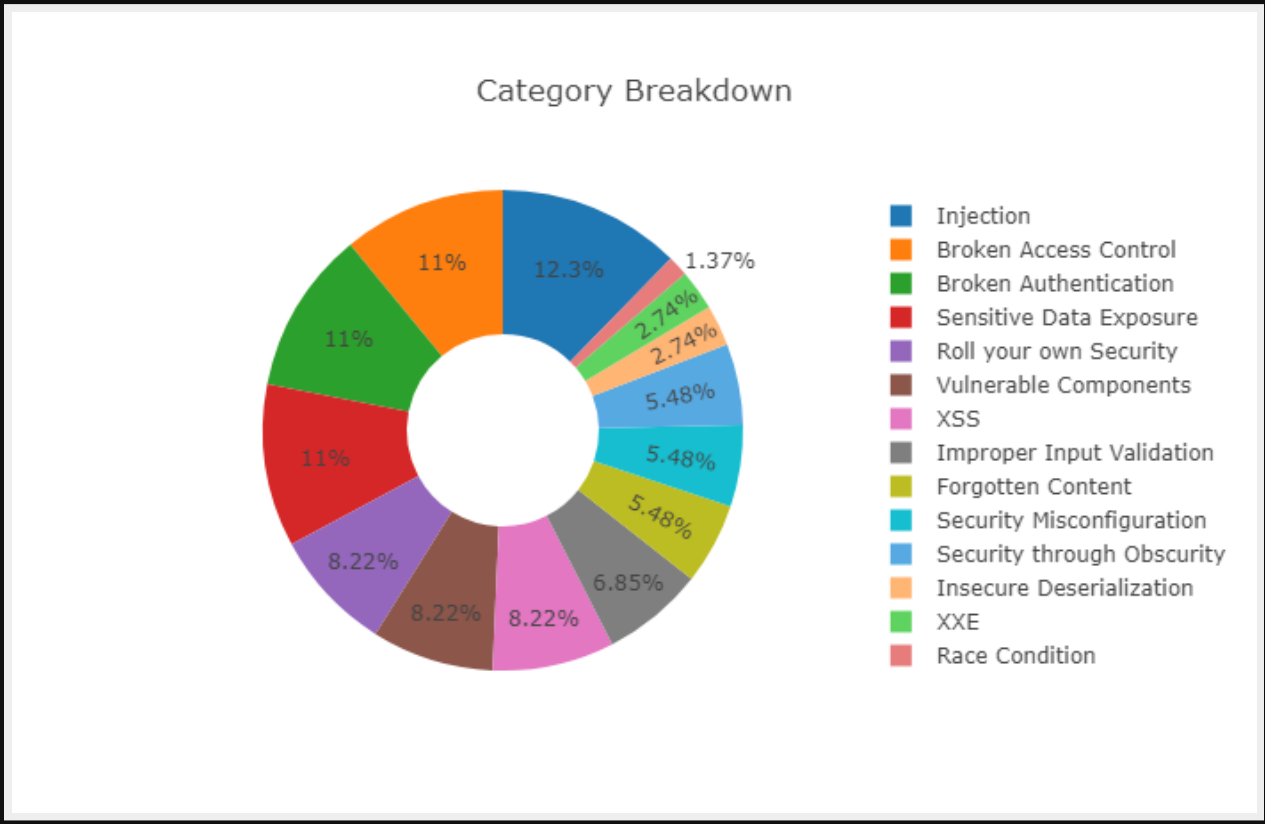

Click here for a happy path shopping tour!
Unsuspectingly browse the Juice Shop like Average Joe!
OPEN CHAT

Simple Installation

Comes with cloud, local and containerized run options

80+ Hacking Challenges

Covering various vulnerabilities and serious design flaws



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

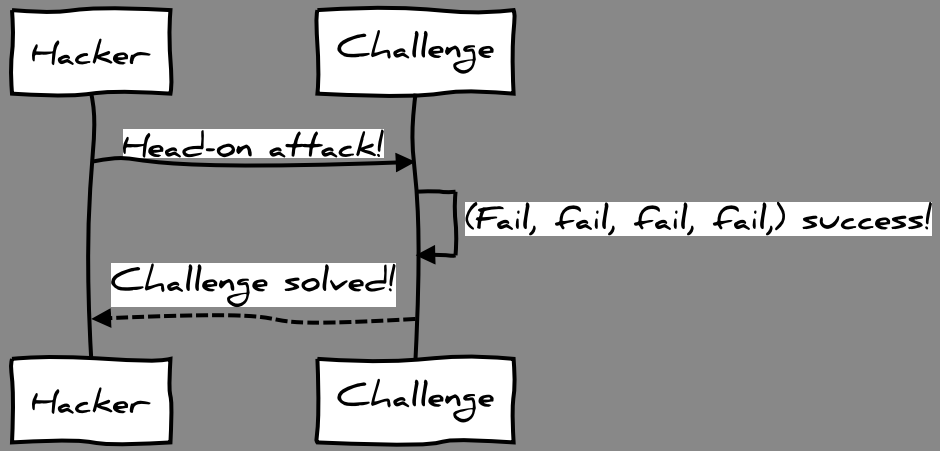
Challenge Difficulty

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



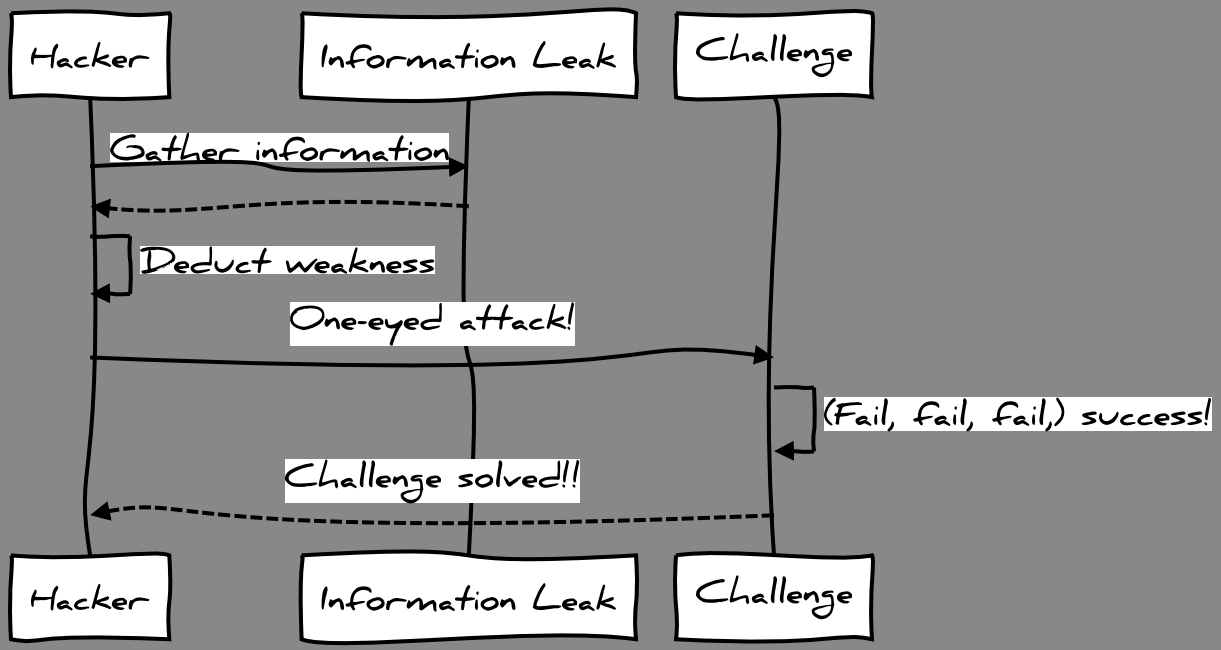
Direct Route to Victory

Some challenges can be immediately attacked head-on



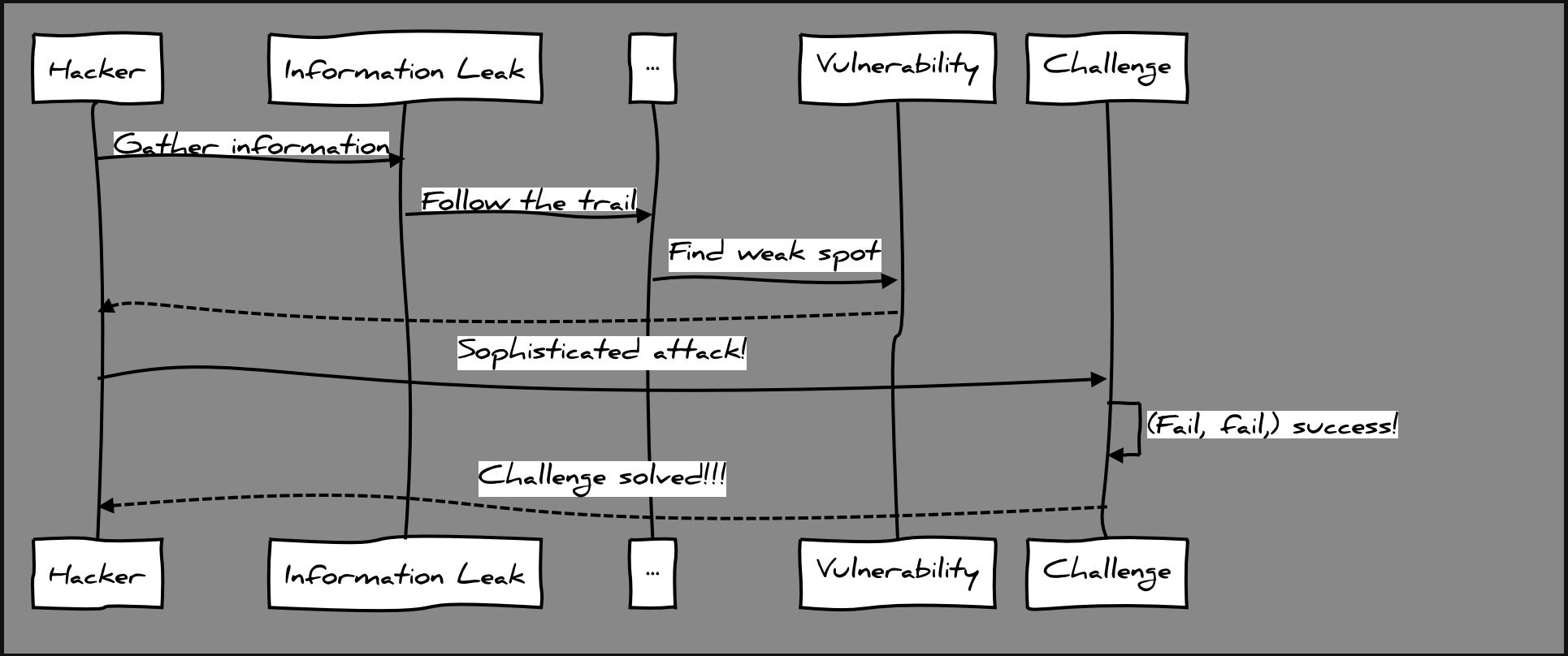
Information Gathering pays off

Most challenges are easier to solve after some research



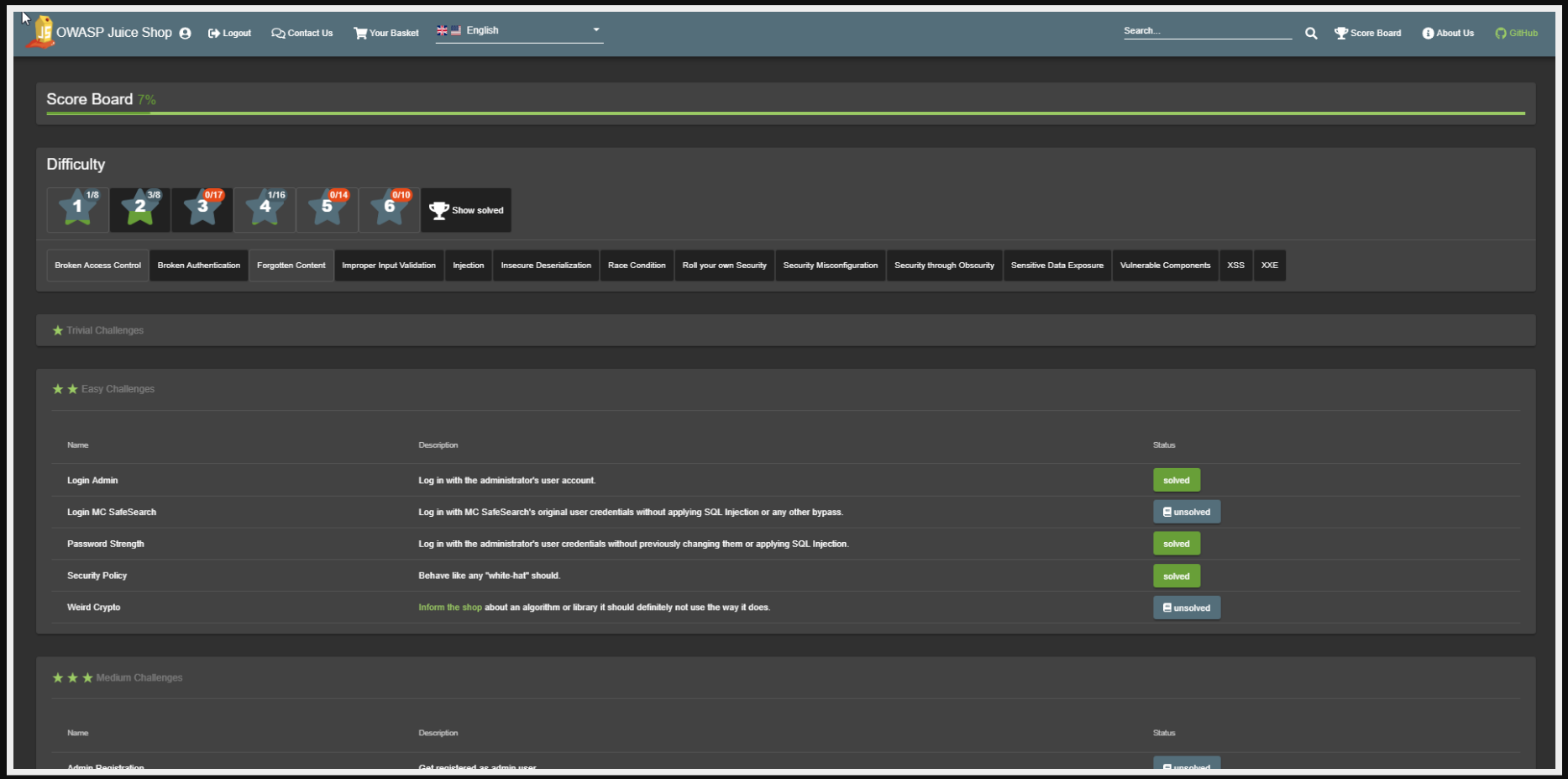
Multi-stage Attack Challenges

The toughest challenges require multiple preparation steps



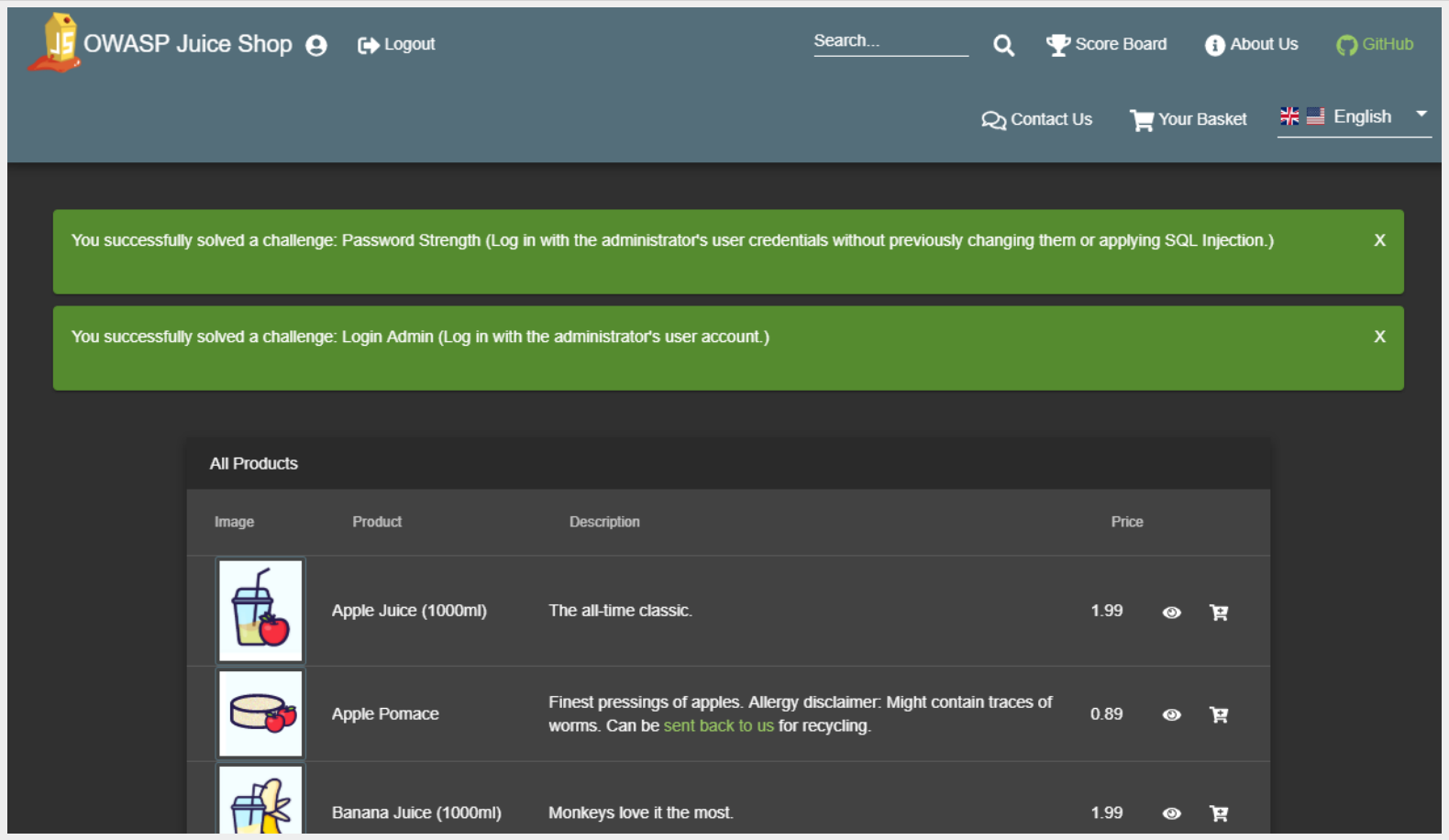
Score Board

Challenge progress is tracked on server-side



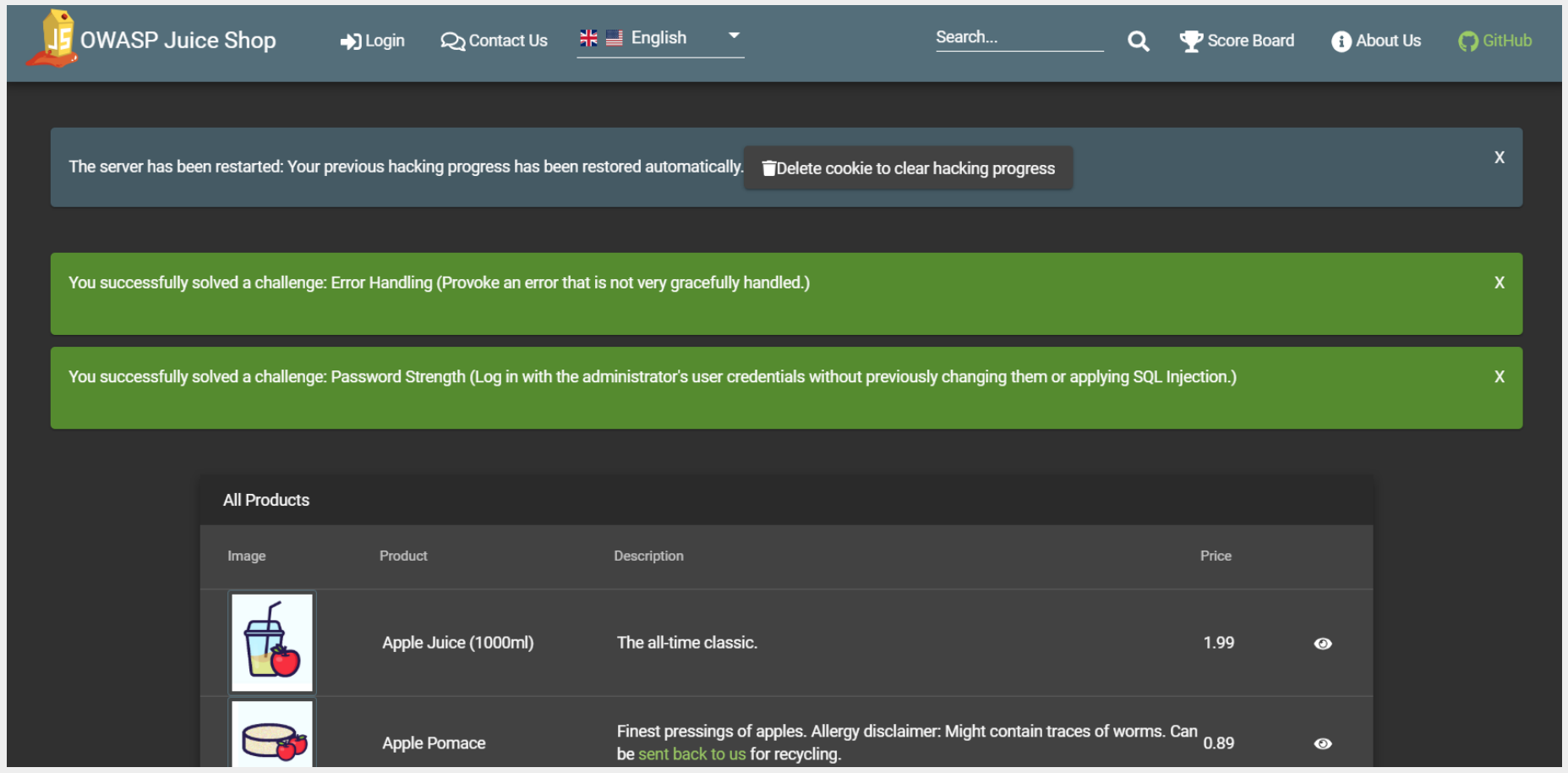
Immediate Feedback

Solved challenges are announced as push notifications



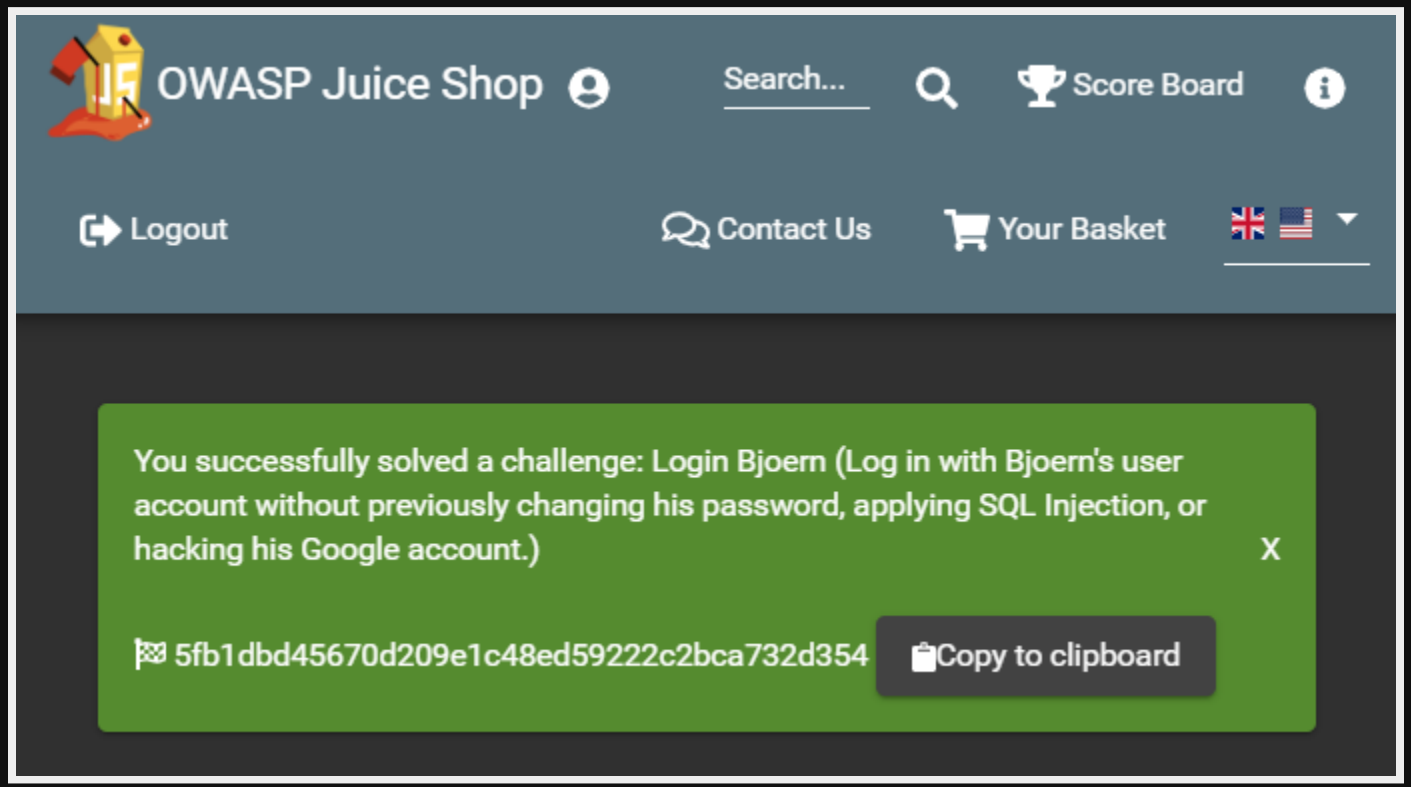
Restore your Progress

Auto-saves your hacking progress and restores on server restart



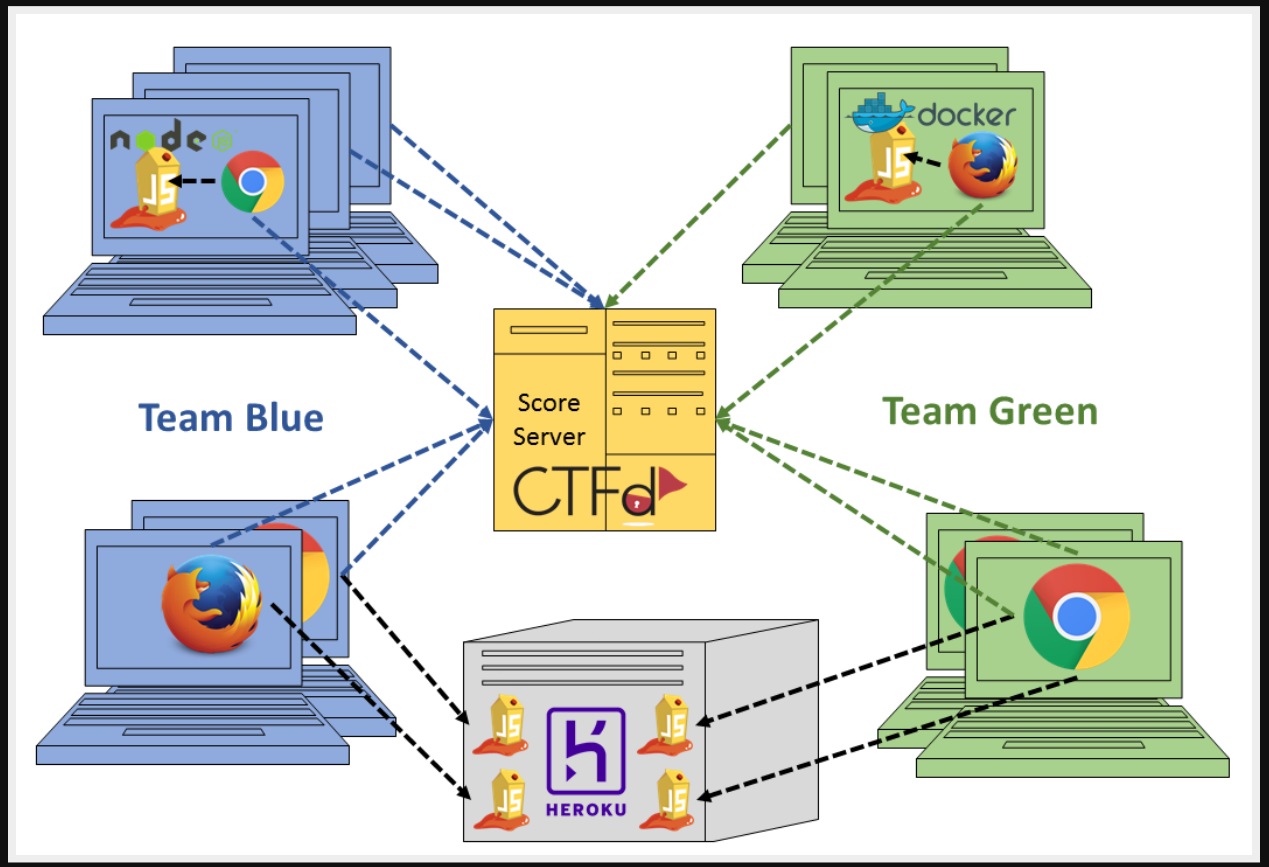
Juice Shop is CTF-ready

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.



OPEN CHAT

CTF Extension 6.x

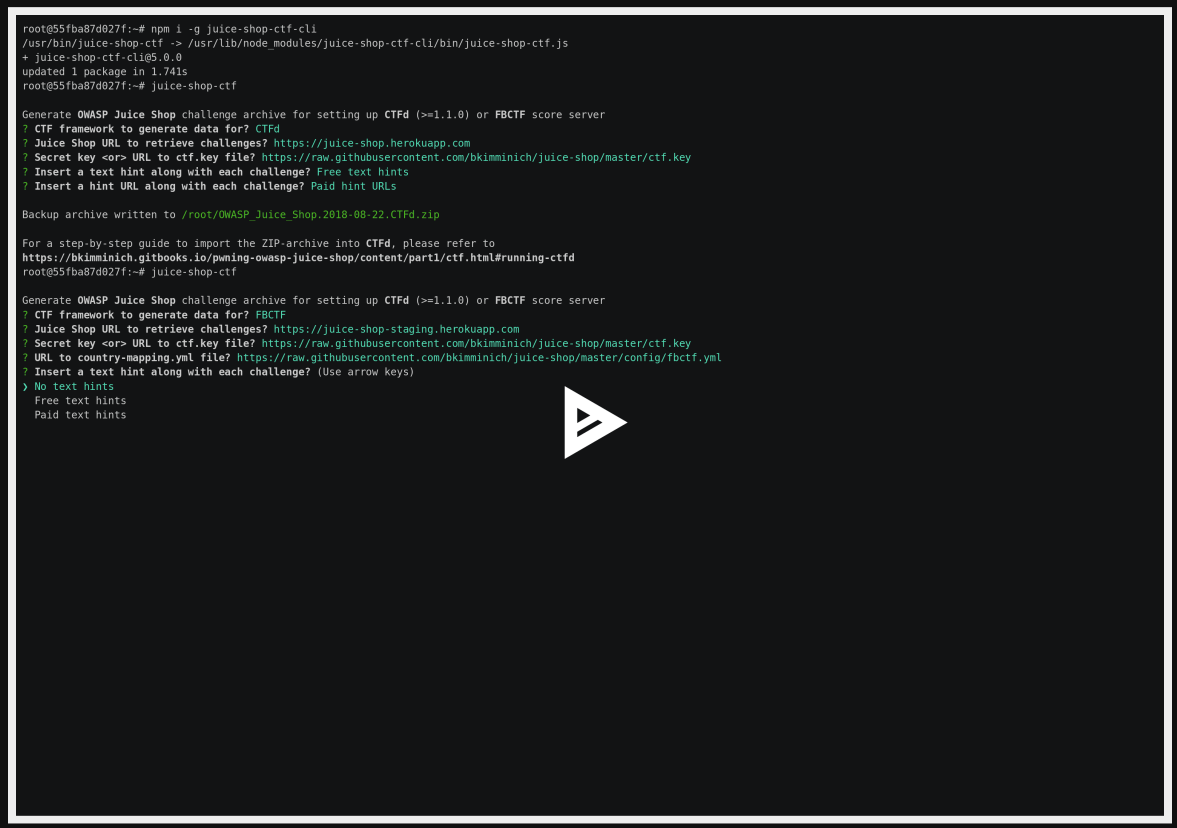
Utility project to help you host a hacking event on CTFd or FBCTF

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



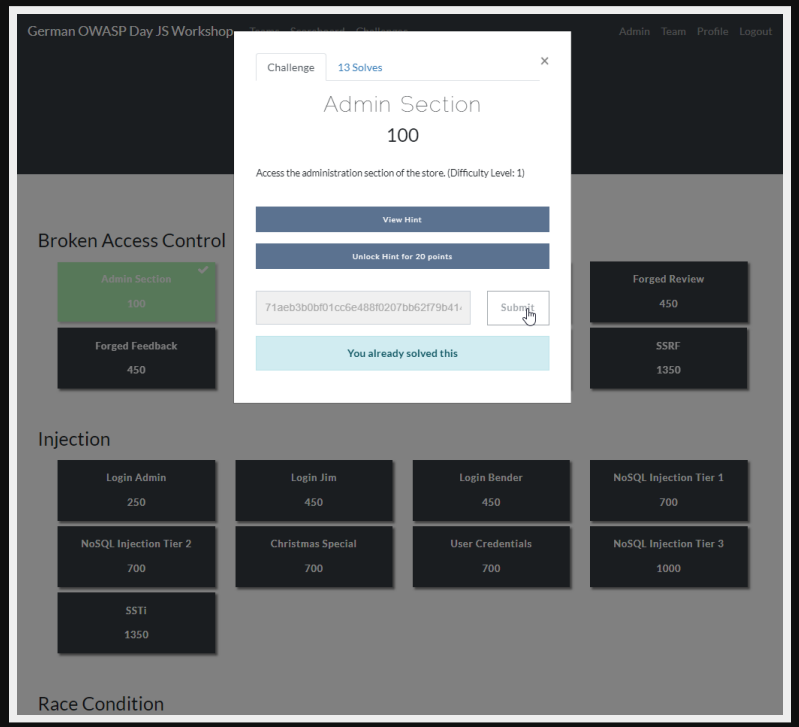
Configuration File Option

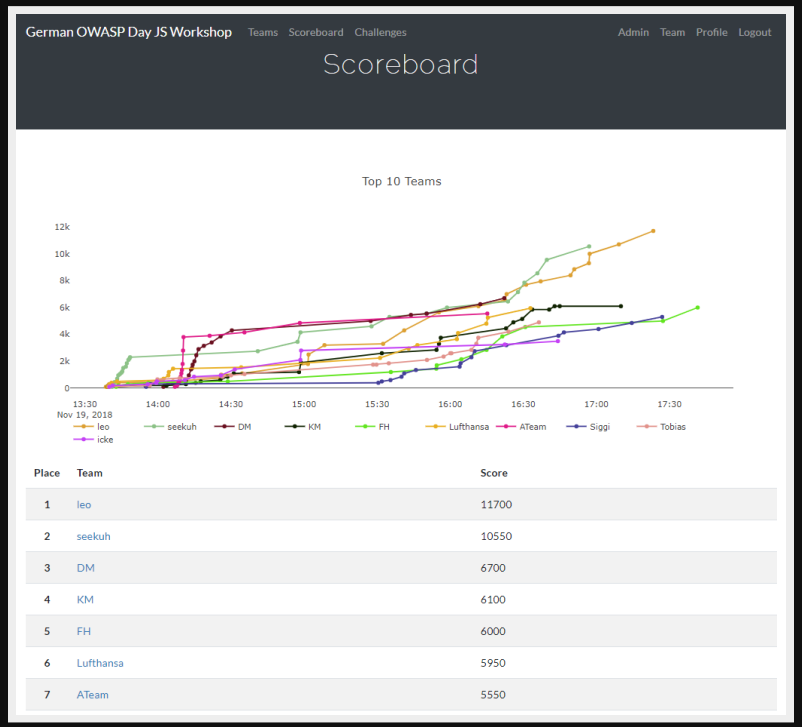
Run `juice-shop-ctf --config myconfig.yml` to use non-interactive mode passing in configuration via YAML file

```
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



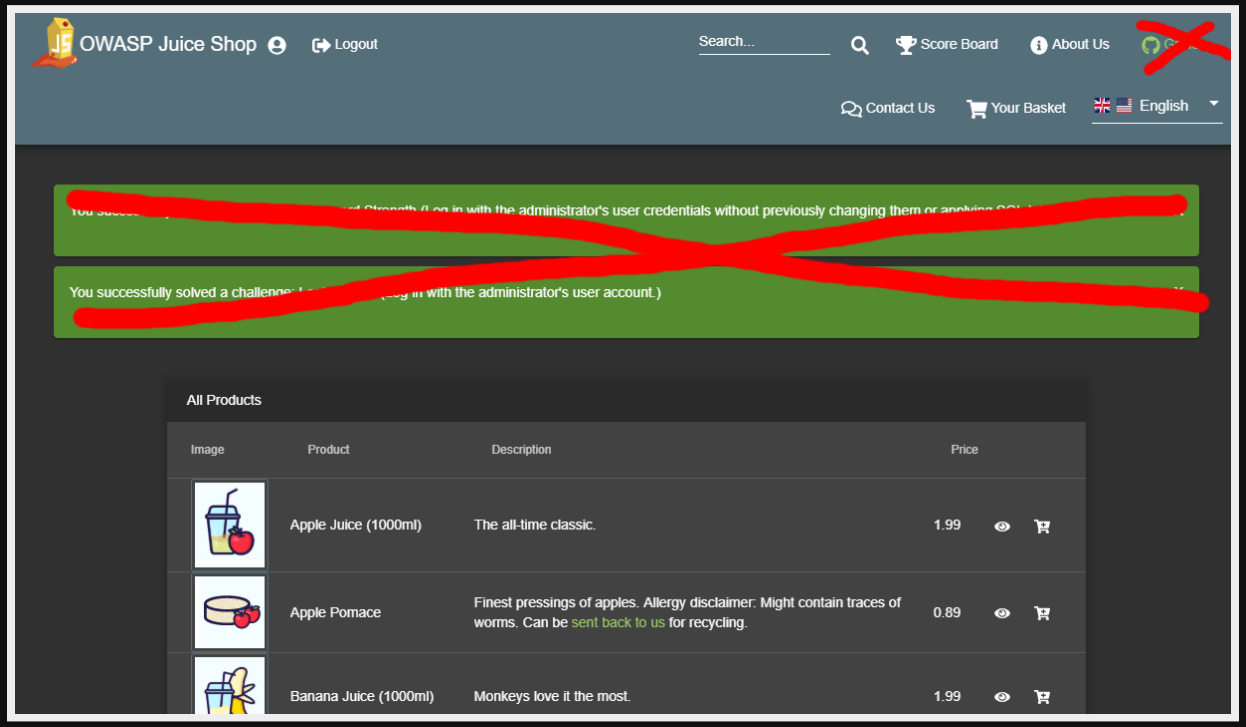


Place	Team	Score
1	leo	11700
2	seekuh	10550
3	DM	6700
4	KM	6100
5	FH	6000
6	Lufthansa	5950
7	ATeam	5550

OPEN CHAT

Quiet Mode

Hide ribbon & toasts for 0% distraction e.g. in awareness trainings

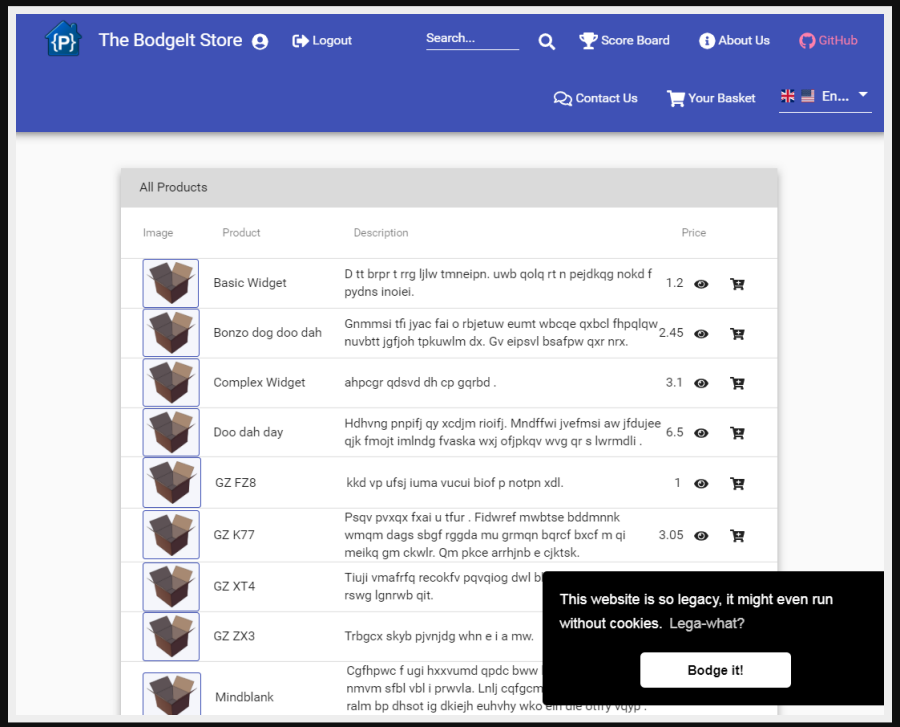


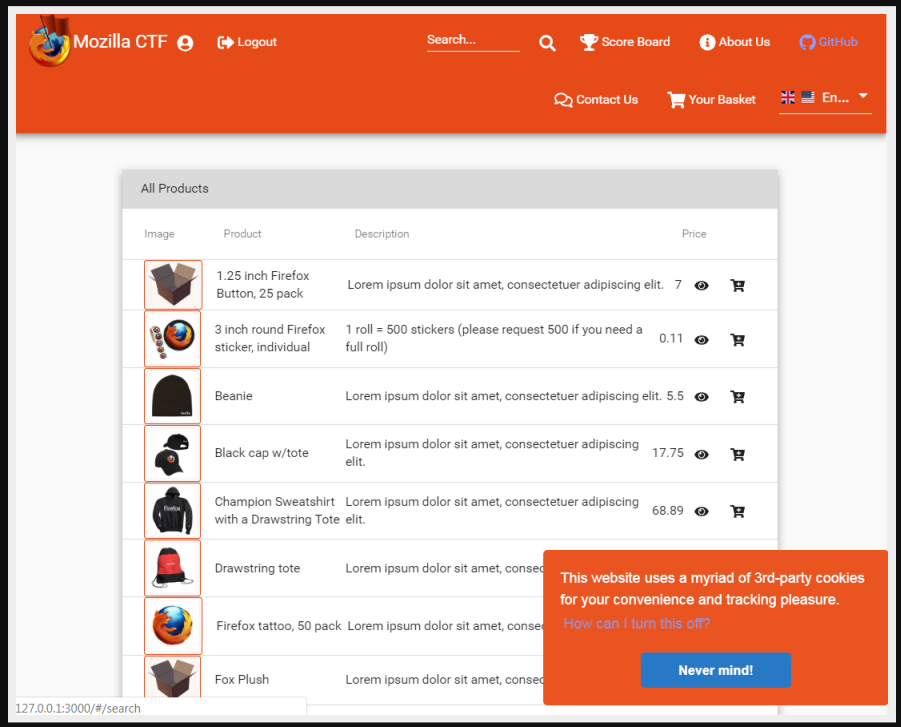
Simply start application with `NODE_ENV=quiet` environment variable defined!

OPEN CHAT

Re-branding

Fully customizable business context and look & feel





OPEN CHAT

Configurative Customization

Customize the application via a simple YAML file

```yaml
application:
  domain: juice-sh.op
  name: 'OWASP Juice Shop'
  logo: JuiceShop_Logo.png
  favicon: favicon_v2.ico
  numberOfRandomFakeUsers: 0
  showChallengeSolvedNotifications: true
  showCtfFlagsInNotifications: false
  showChallengeHints: true
  showVersionNumber: true
  theme: bluegrey-lightgreen
  gitHubRibbon: true
  twitterUrl: 'https://twitter.com/owasp_juiceshop'
  facebookUrl: 'https://www.facebook.com/owasp.juiceshop'
  slackUrl: 'http://owaspslack.com'
  planetOverlayMap: orangemap2k.jpg
  planetName: Orangeuze
  [...]
challenges:
  safetyOverride: false
```

Choose your own inventory

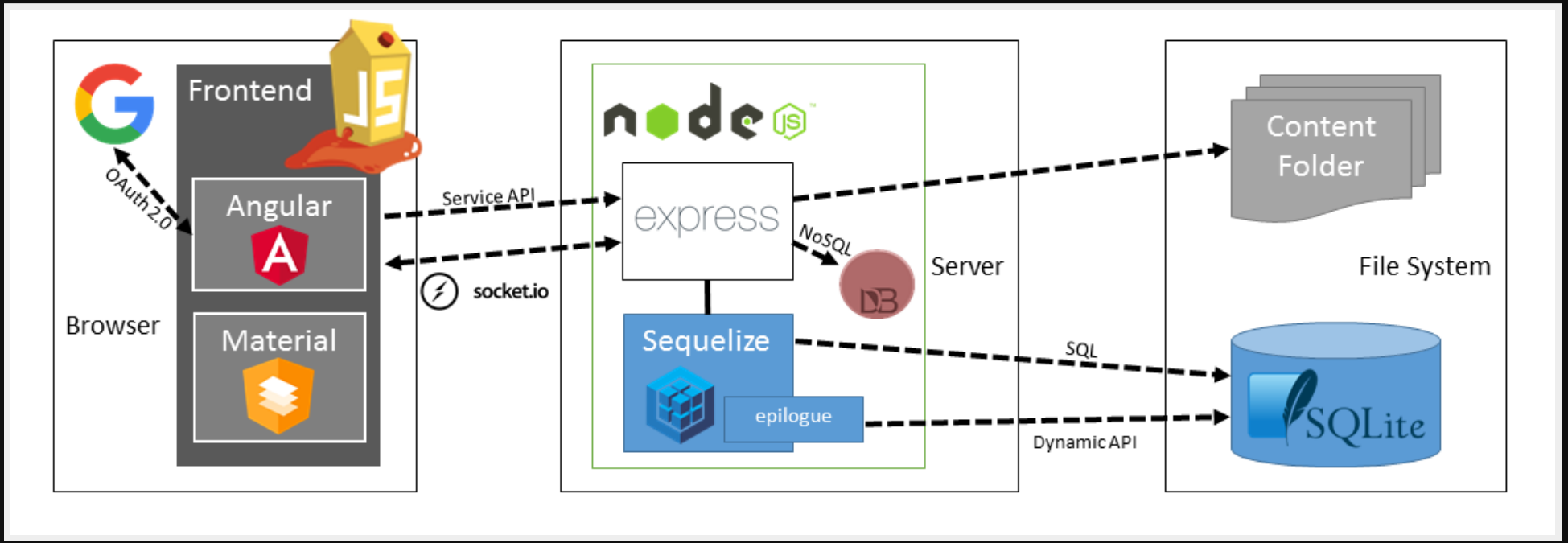
The YAML configuration allows you to override all products

```yaml
products:
  -
    name: 'Product Name'
    price: 100
    description: 'Product Description'
    image: '(https://somewhe.re/)image.png'
    useForProductTamperingChallenge: false
    useForChristmasChallenge: false
    fileForRetrieveBlueprintChallenge: ~
    reviews:
      - { text: 'Customer review', author: jim }
  -
    name: 'Product with Lorem Ipsum description, filler image and random price'
```

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

Modern Web-Architecture

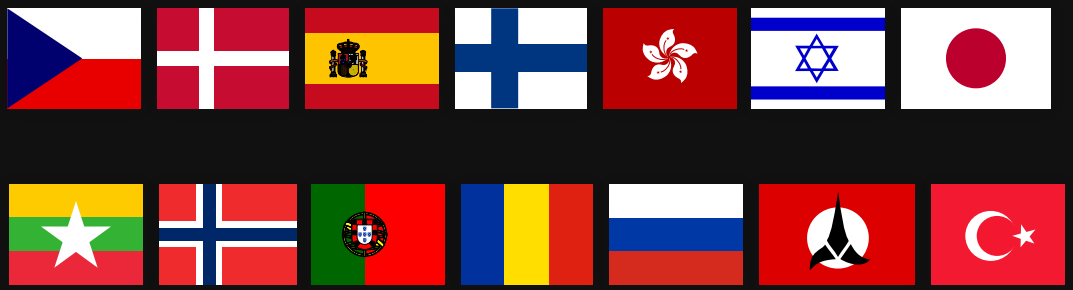
JavaScript all the way from UI to REST API



Multi-language support

Complete UI translation available for

Partial translation available for



OPEN CHAT

Test Pyramid

Maximizing Test Automation & Code Coverage

Protractor
end to end testing for AngularJS

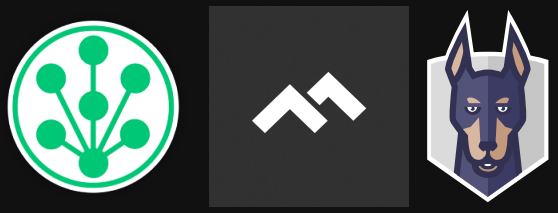
frisby.js

Jasmine

MOCHA

DevOps Pyramid

Automated Build, CI/CD & Code Analysis



FAQ

If FAQ & README don't help, ask in the chat or open an issue

- Can I use my Pentesting toys?
- Can I do a white box pentest?
- Can I use the internet?
- Installation does not work!
- What if I crash the server?
- I'm stuck with a challenge!
- I found another vulnerability!
- Why are some challenges disabled?
- Can I contribute to the project?
- Is there a contribution reward?

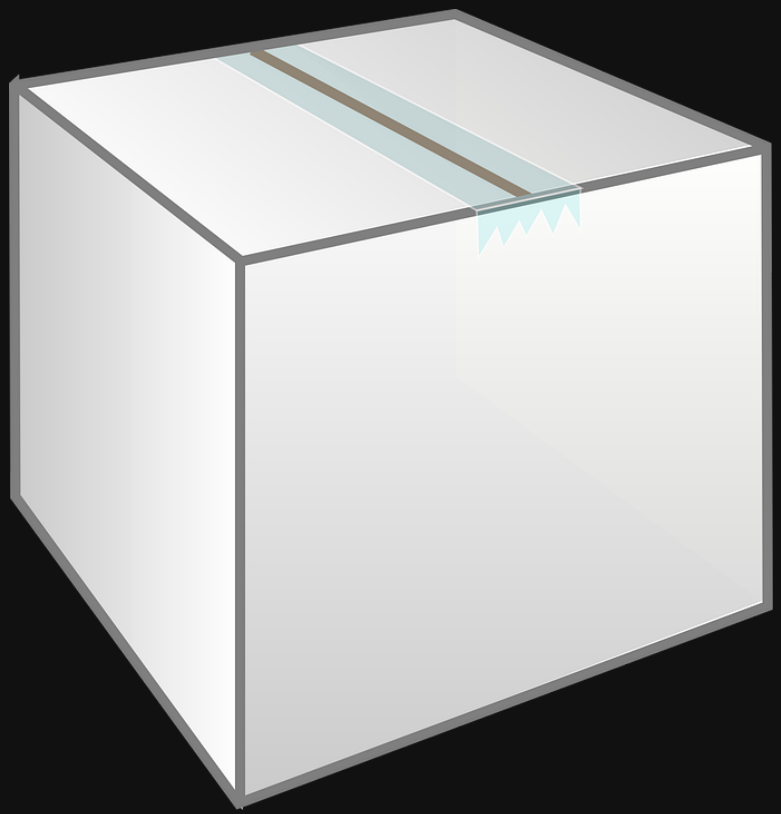
Can I use my Pentesting toys?

Yes, definitely! Use whatever pentesting tools you like the most!

Proxies like OWASP ZAP or BurpSuite Free Edition can definitely be useful. Automatic tools like Arachni or Nikto might find some vulnerabilities but will obviously not be able to get the Score Board to 100% for you.

Can I do a white box pentest?

No! The code from GitHub would spoiler all challenge solutions!



You can of course use everything that the application hands to you in the browser, so use its `DevTools`!

Can I use the internet?

Yes! Feel free to look for ideas, clues & hints **everywhere**!

Again: Except for the application's own GitHub repository & the logs of its Travis-CI build jobs!

Installation does not work!

Please carefully follow the instructions in the README

If Setup & Troubleshooting docs don't help, you can always ask the community or open an issue!

OPEN CHAT

What if I crash the server?

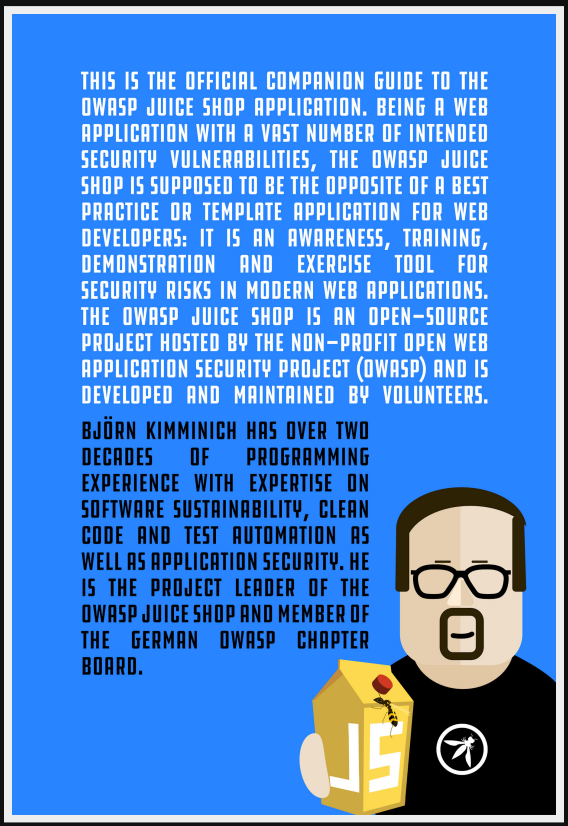
The application is cleanly reset on every startup

Your Score Board progress is saved automatically and will restore after server restart!

OPEN CHAT

I'm stuck with a challenge!

Find helpful hints in the **free** official companion guide on Leanpub



The eBook can also be read online on GitBook. You can always ask for hints in the community chat as well!

OPEN CHAT

I found another vulnerability!

Please report untracked vulnerabilities by opening an issue

challenge not found

Of course you can also contribute directly by opening a pull request. Just stick to the contribution guide!

Why are some challenges disabled?

Some challenges are *actually harmful* in containerized or cloud environments and are deliberately disabled there

This affects the XXE challenges (because they can lead to instance death by `segfault` error) and the SSTI challenge (as it could have unforeseeable side effects) on the hosting platform.

Can I contribute to the project?

Of course! Visit our backlog on GitHub & translations on Crowdin

Stories or issues labelled with ready and good first issue / help wanted are the best starting point!

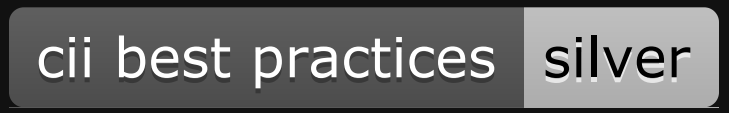
Is there a contribution reward?

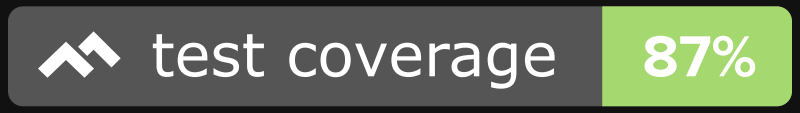
For your 1st merged pull request you'll get some stickers from us

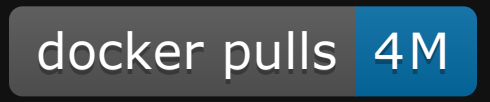
Serial contributors might even get t-shirts, mugs and other glorious merchandise for free!

Juice Shop Success Pyramid™

Some amazing facts & stats about the project







Project Roadmap

- Hacking Instructor to guide beginners through challenges
- Master thesis on **Design/UX improvements** w/ HdM Stuttgart
- OWASP Juice Shop Track during **Open Security Summit 2019**
- At least one student project during **Google Summer of Code** 2019

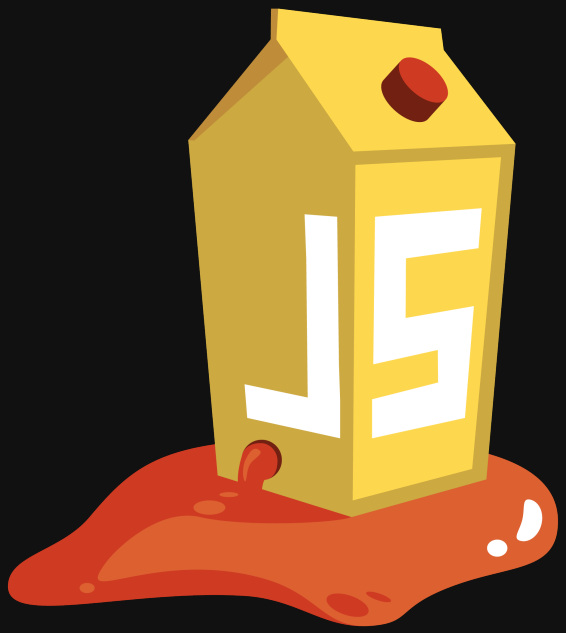
Timeline? **When it's done!**

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

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



Created with reveal.js - The HTML Presentation Framework