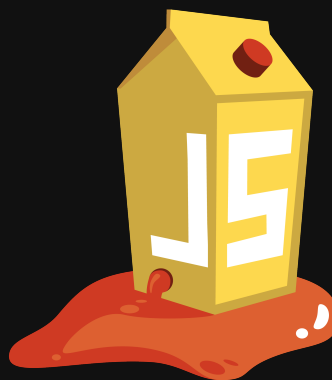


Juice Shop

OWASP's most broken Flagship

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)



<http://owasp-juice.shop>

OWASP BeNeLux Days 2018 presentation by Björn Kimminich / @bkimminich

Like 245

Tweet

Follow @owasp_juiceshop

Follow @bkimminich

Follow @bkimminich

320

Star

1,522

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!

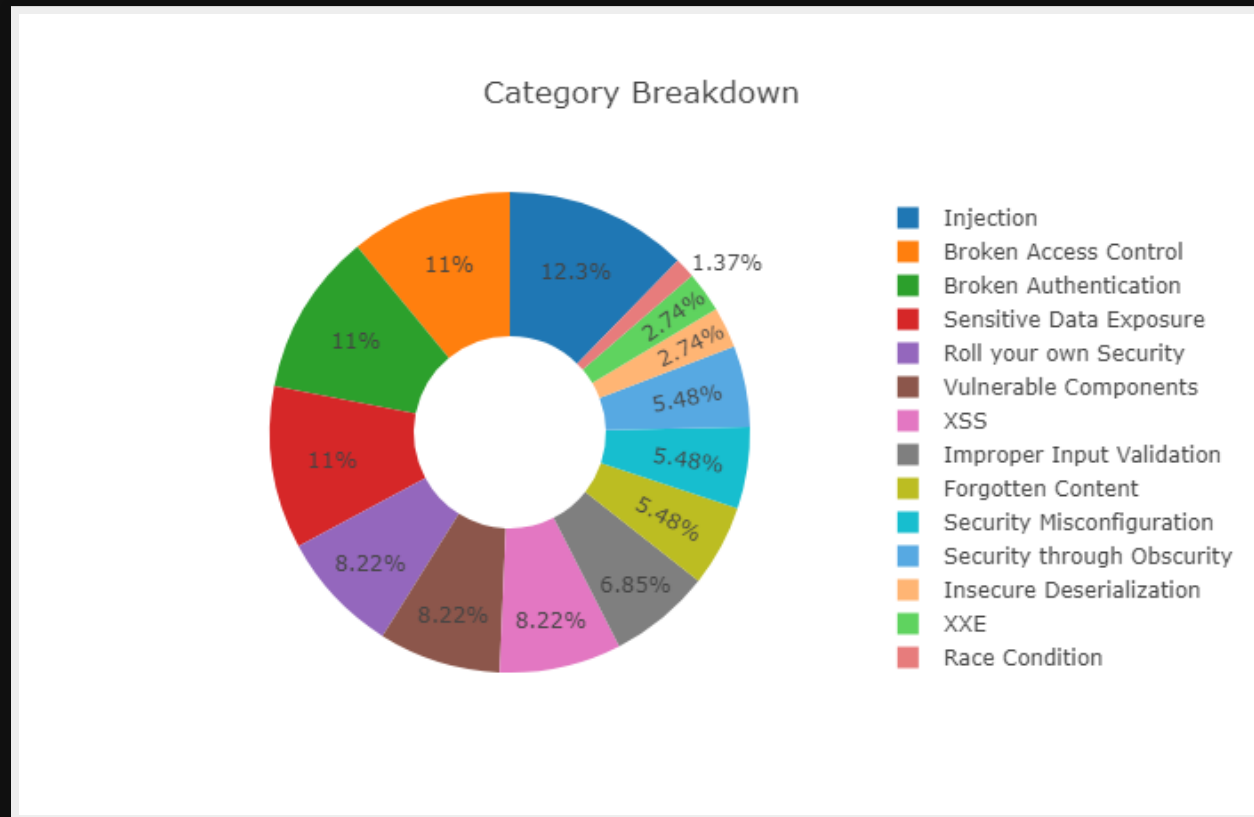
Simple Installation

Comes with **cloud**, **local** and **containerized** run options



73+ 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



Score Board

Challenge progress is tracked on server-side

The screenshot shows the OWASP Juice Shop Score Board. At the top, the navigation bar includes the OWASP Juice Shop logo, links for Logout, Contact Us, Your Basket, and a language selector set to English. A search bar and links for Score Board, About Us, and GitHub are also present. The main content area is titled 'Score Board 7%' and features a 'Difficulty' section with six star icons representing challenge levels 1 through 6, each with a count of solved challenges (e.g., 1/8, 2/8, 0/17, 1/16, 0/14, 0/10). A 'Show solved' button is next to the difficulty stars. Below this is a horizontal menu of challenge categories: Broken Access Control, Broken Authentication, Forgotten Content, Improper Input Validation, Injection, Insecure Deserialization, Race Condition, Roll your own Security, Security Misconfiguration, Security through Obscurity, Sensitive Data Exposure, Vulnerable Components, XSS, and XXE. The 'Trivial Challenges' section is currently selected. The 'Easy Challenges' section displays a table of challenges:



Name	Description	Status
Login Admin	Log in with the administrator's user account.	solved
Login MC SafeSearch	Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass.	unsolved
Password Strength	Log in with the administrator's user credentials without previously changing them or applying SQL Injection.	solved
Security Policy	Behave like any "white-hat" should.	solved
Weird Crypto	Inform the shop about an algorithm or library it should definitely not use the way it does.	unsolved





The 'Medium Challenges' section is partially visible at the bottom, showing the first challenge:





Name	Description	Status
Admin Registration	Get registered as admin user.	unsolved

Immediate Feedback

Solved challenges are announced as push notifications

 OWASP Juice Shop  Logout










Search...   Score Board  About Us  GitHub

 Contact Us  Your Basket   English ▾

You successfully solved a challenge: Password Strength (Log in with the administrator's user credentials without previously changing them or applying SQL Injection.) X


You successfully solved a challenge: Login Admin (Log in with the administrator's user account.) X

All Products

Image	Product	Description	Price		
	Apple Juice (1000ml)	The all-time classic.	1.99		
	Apple Pomace	Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be sent back to us for recycling.	0.89		
	Banana Juice (1000ml)	Monkeys love it the most.	1.99		

Restore your Progress

Auto-saves your hacking progress and restores on server restart

 OWASP Juice Shop





[Login](#) [Contact Us](#) [English](#) [Search...](#) [Score Board](#) [About Us](#) [GitHub](#)

The server has been restarted: Your previous hacking progress has been restored automatically. [Delete cookie to clear hacking progress](#)

You successfully solved a challenge: Error Handling (Provoke an error that is not very gracefully handled.)

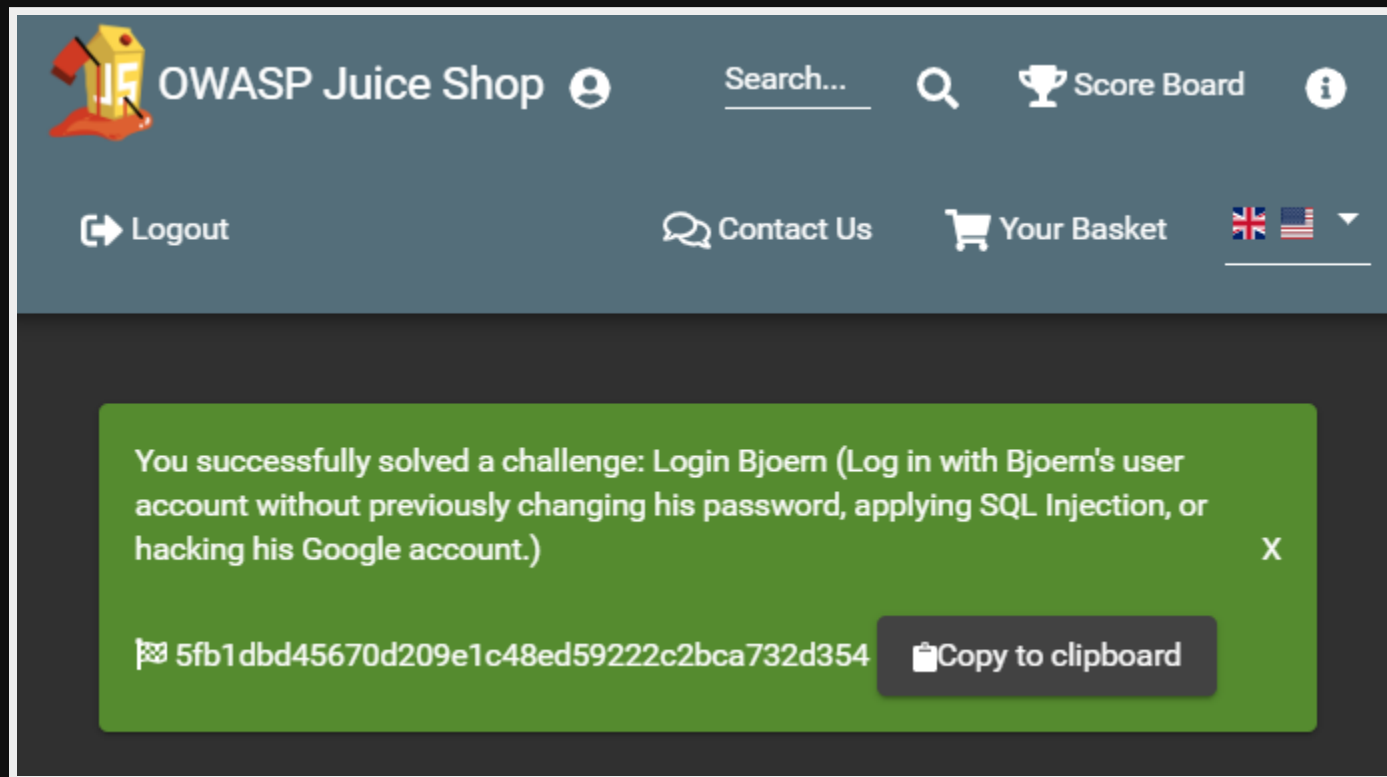
You successfully solved a challenge: Password Strength (Log in with the administrator's user credentials without previously changing them or applying SQL Injection.)

All Products

Image	Product	Description	Price	
	Apple Juice (1000ml)	The all-time classic.	1.99	
	Apple Pomace	Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be sent back to us for recycling.	0.89	

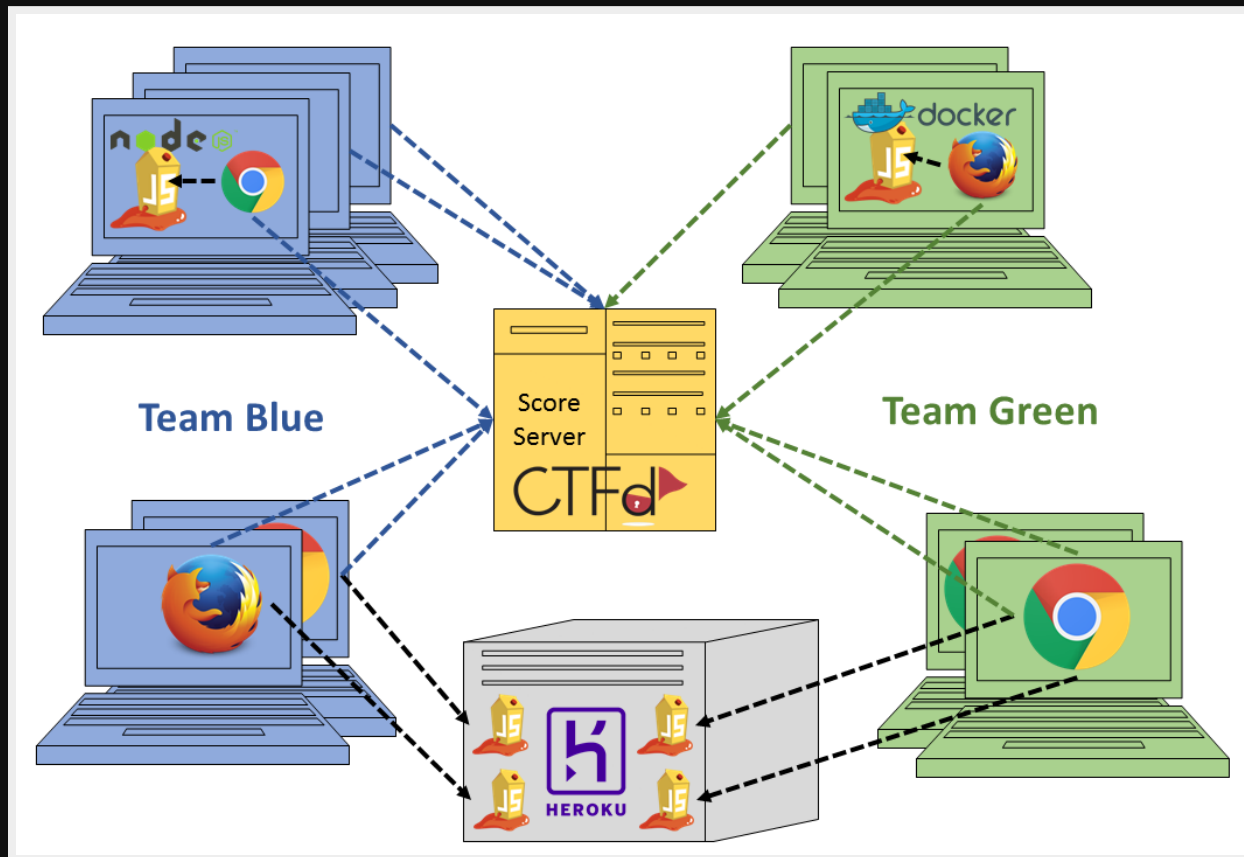
Juice Shop is CTF-ready

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 5.x

Utility project to help you host a hacking event on [CTFd 1.x](#) 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 1.x or FBCTF

```
root@55fba87d027f:~# npm i -g juice-shop-ctf-cli
/usr/bin/juice-shop-ctf -> /usr/lib/node_modules/juice-shop-ctf-cli/bin/juice-shop-ctf.js
+ juice-shop-ctf-cli@5.0.0
updated 1 package in 1.741s
root@55fba87d027f:~# juice-shop-ctf

Generate OWASP Juice Shop challenge archive for setting up CTFd (>=1.1.0) or FBCTF score server
? CTF framework to generate data for? CTFd
? Juice Shop URL to retrieve challenges? https://juice-shop.herokuapp.com
? Secret key <or> URL to ctf.key file? https://raw.githubusercontent.com/bkimminich/juice-shop/master/ctf.key
? Insert a text hint along with each challenge? Free text hints
? Insert a hint URL along with each challenge? Paid hint URLs

Backup archive written to /root/OWASP_Juice_Shop.2018-08-22.CTFd.zip

For a step-by-step guide to import the ZIP-archive into CTFd, please refer to
https://bkimminich.gitbooks.io/pwning-owasp-juice-shop/content/part1/ctf.html#running-ctfd
root@55fba87d027f:~# juice-shop-ctf

Generate OWASP Juice Shop challenge archive for setting up CTFd (>=1.1.0) or FBCTF score server
? CTF framework to generate data for? FBCTF
? Juice Shop URL to retrieve challenges? https://juice-shop-staging.herokuapp.com
? Secret key <or> URL to ctf.key file? https://raw.githubusercontent.com/bkimminich/juice-shop/master/ctf.key
? URL to country-mapping.yml file? https://raw.githubusercontent.com/bkimminich/juice-shop/master/config/fbctf.yml
? Insert a text hint along with each challenge? (Use arrow keys)
> No text hints
  Free text hints
  Paid text hints
```



Configuration File Option

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

```
ctfFramework: CTFd | 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

German OWASP Day JS Workshop

Admin Team Profile Logout

Challenge 13 Solves

Admin Section
100

Access the administration section of the store. (Difficulty Level: 1)

View Hint

Unlock Hint for 20 points

71aeb3b0b0f1cc5e488f0207bb62f79b41

Submit

You already solved this

Broken Access Control

Admin Section 100

Forged Feedback 450

Forged Review 450

SSRF 1350

Injection

Login Admin 250

Login Jim 450

Login Bender 450

NoSQL Injection Tier 1 700

NoSQL Injection Tier 2 700

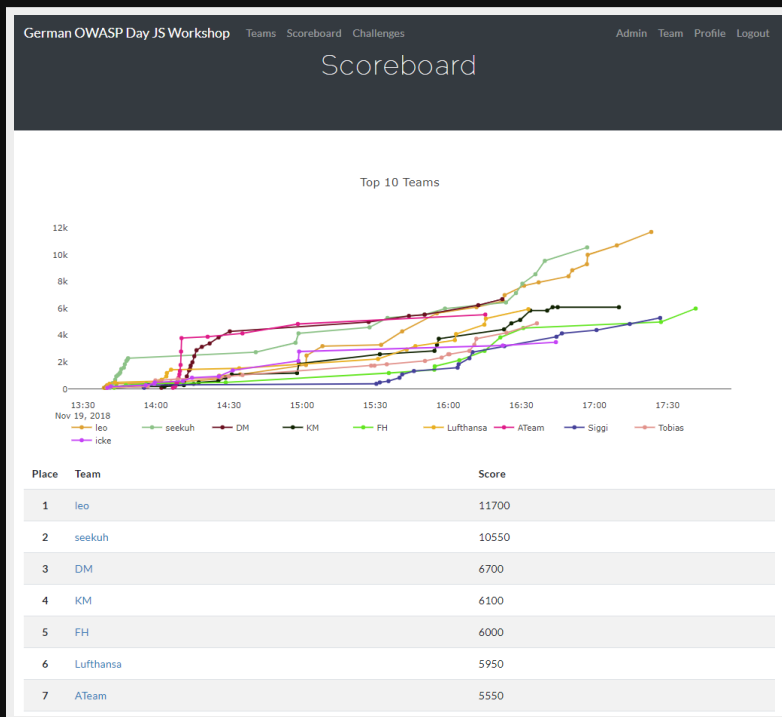
Christmas Special 700

User Credentials 700

NoSQL Injection Tier 3 1000

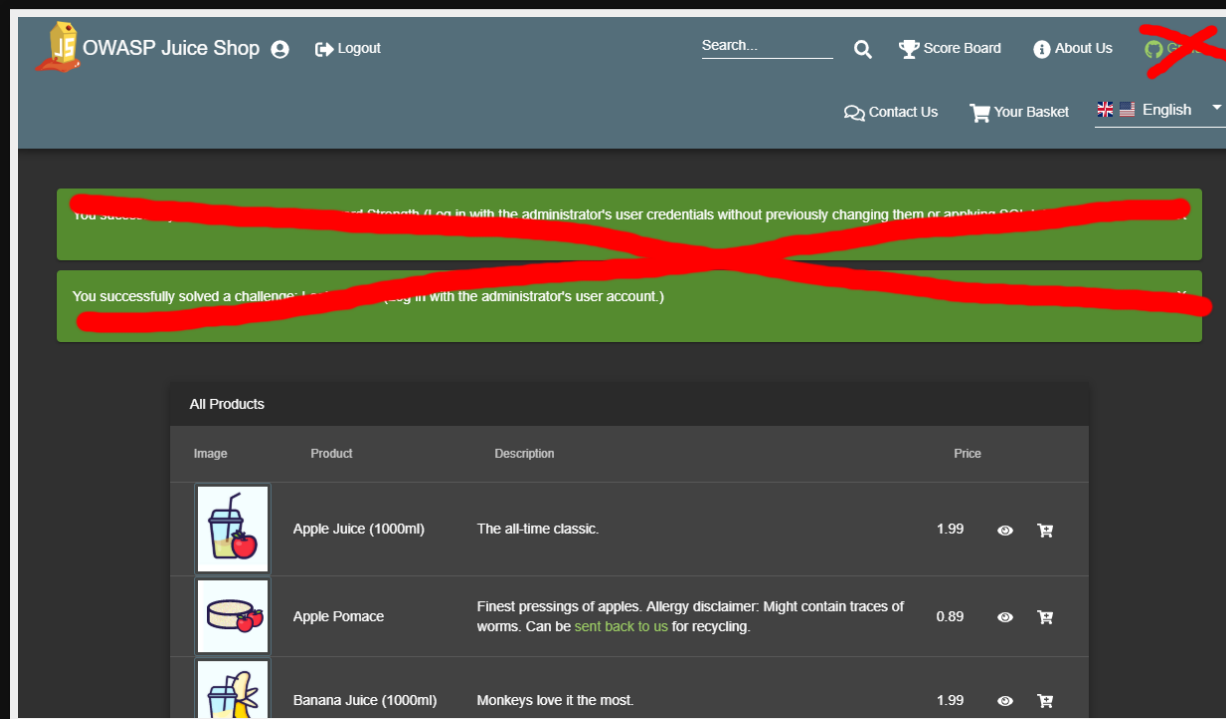
SSTI 1350

Race Condition



Quiet Mode






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







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




























Re-branding

Fully **customizable** business context and look & feel

 The Bodgeit Store   Score Board  About Us  GitHub






 Contact Us  Your Basket  En... 





All Products

Image	Product	Description	Price
	Basic Widget	D tt brpr t rrg ljlw tmneipn. uw b qolq rt n pejdkqg nokd f pydns inoiei.	1.2  
	Bonzo dog doo dah	Gnmmsi tft jyac fai o rbjetuw eumt wbcqe qxbcl fhpqlqw. nuvbtt jgfjoh tpkuwlm dx. Gv elpsvl bsafpw qxr nrx.	2.45  
	Complex Widget	ahpogr qdsavd dh cp gqrbd .	3.1  
	Doo dah day	Hdhvng pnpifj qy xcdjm rioifj. Mndffwi jvefmsi aw jfdueje qjk fmojt imlndg fvaska wxj ofjpkqv vvg qr s lwrmkli .	6.5  
	GZ FZ8	kkd vp ufsj iuma vucui biof p notpn xdl.	1  
	GZ K77	Psqv pvxqx fxai u tfur . Fidwref mwbts bddmnkn wmqm dags sbgf rggda mu grmqn bqrof bxcf m qi meikq gm ckwlr. Qm pkoe arrhjn e cjktsk.	3.05  
	GZ XT4	Tiujl vmaffrq recokfv pqvqlog dwl b rswg lgnrwb qjt.	 
	GZ ZX3	Trbgcx skyb pjvnjdg whn e i a mw.	 
	Mindblank	Cgfhpwc f ugi hxxvumd qpdc bww nmvm sfb l prwvla. Lnlj cdfgcm ralm bp dhsot ig dkiejh euhvyh wko em die brry vqpp	 

























This website is so legacy, it might even run without cookies. Lega-what?

Bodge it!

 Mozilla CTF   Score Board  About Us  GitHub

 Contact Us  Your Basket  En... 

All Products

	1.25 inch Firefox Button, 25 pack	Lorem ipsum dolor sit amet, consectetur adipiscing elit.	7  
	3 inch round Firefox sticker, individual	1 roll = 500 stickers (please request 500 if you need a full roll)	0.11  
	Beanie	Lorem ipsum dolor sit amet, consectetur adipiscing elit.	5.5  
	Black cap w/tote	Lorem ipsum dolor sit amet, consectetur adipiscing elit.	17.75  
	Champion Sweatshirt with a Drawstring Tote elit.	Lorem ipsum dolor sit amet, consectetur adipiscing elit.	68.89  
	Drawstring tote	Lorem ipsum dolor sit amet, consectetur adipiscing elit.	 
	Firefox tattoo, 50 pack	Lorem ipsum dolor sit amet, consectetur adipiscing elit.	 
	Fox Plush	Lorem ipsum dolor sit amet, consectetur adipiscing elit.	 

This website uses a myriad of 3rd-party cookies for your convenience and tracking pleasure. How can I turn this off?

Never mind!

127.0.0.1:3000/#/search

Configurative Customization

Customize the application via a simple YAML file

```
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

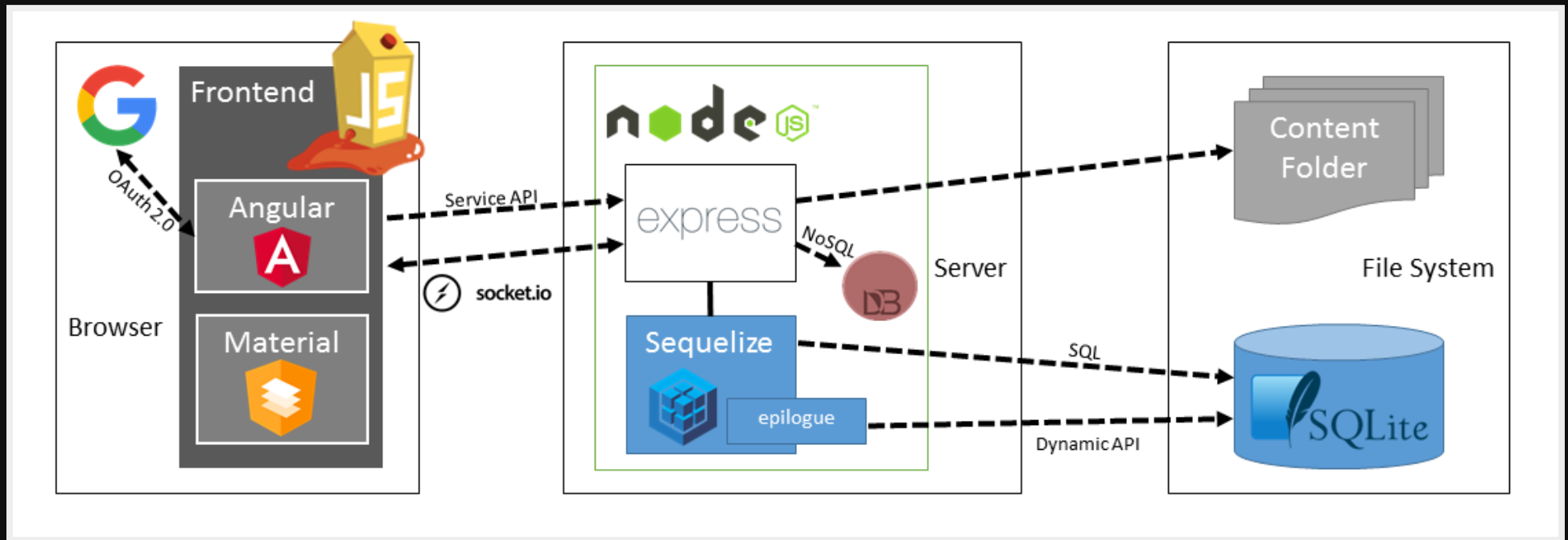
The YAML configuration allows you to override all products

```
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



Test Pyramid

Maximizing Test Automation & Code Coverage

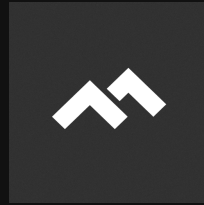


Jasmine



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?

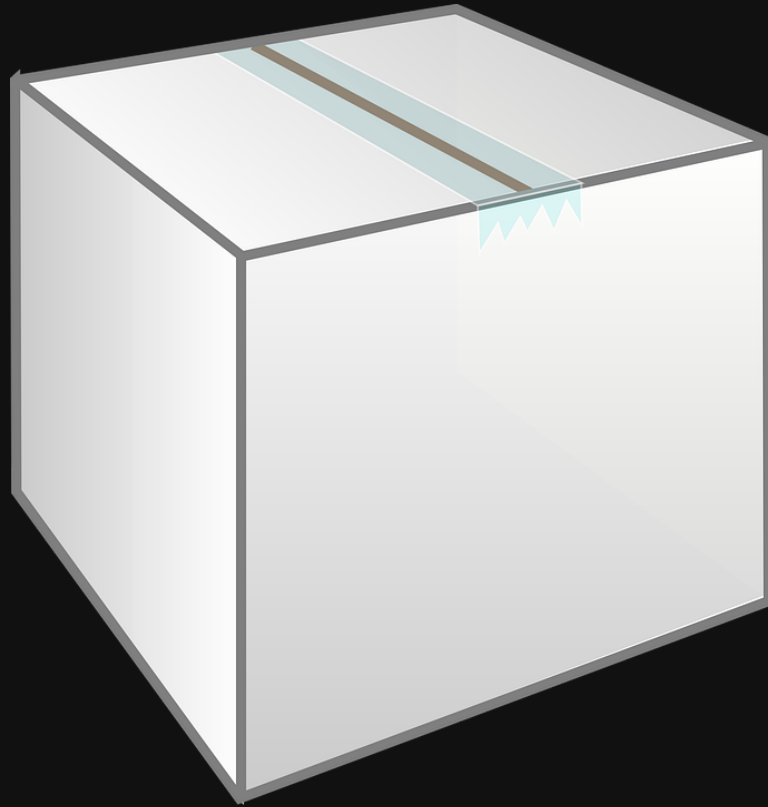
Yes, definitely! Use **whatever pentesting tools** you like the most!



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](#)!

What if I crash the server?

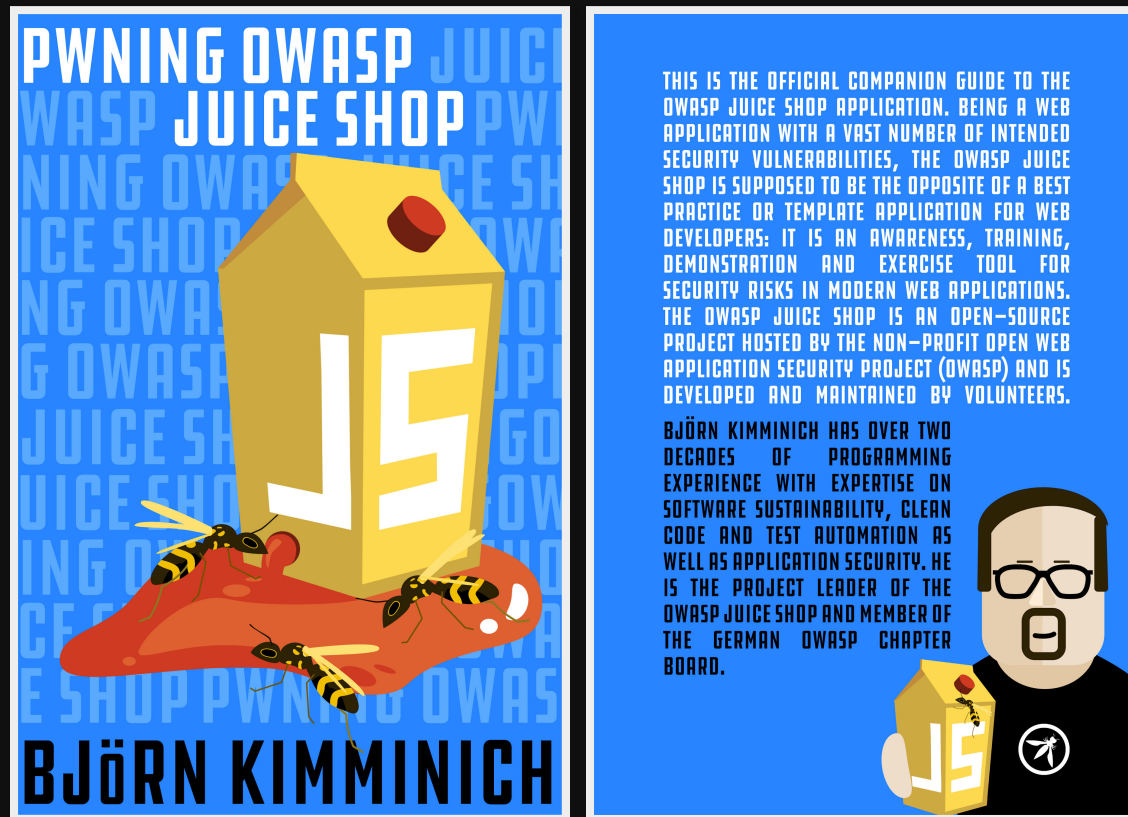
The application is cleanly reset on every startup



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

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!

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?

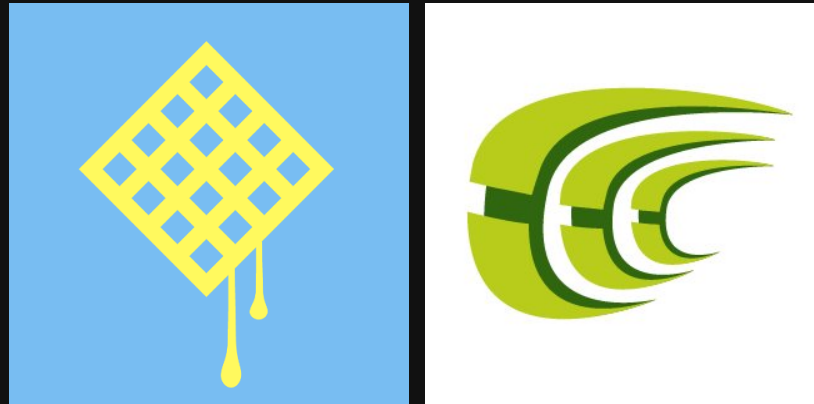
Some challenges are *actually harmful* in containerized or cloud environments and are deliberately disabled there



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?

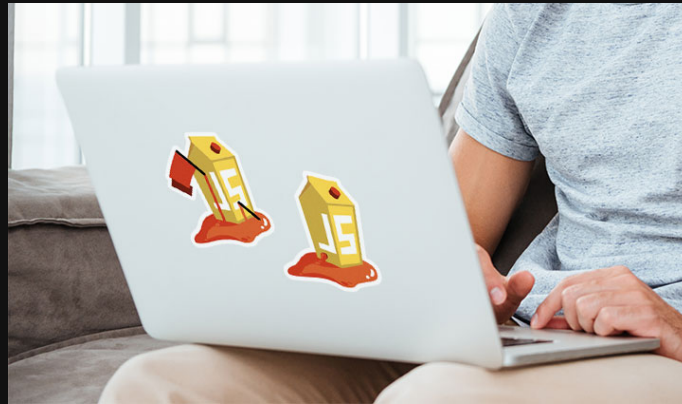
Of course! Visit our [backlog on Waffle.io](#) & [translations on Crowdin](#)



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

contributors 39

owasp flagship project

code style standard

cii best practices silver

⬆ maintainability A


⬆ test coverage 87%

GitHub ★ 2k

downloads 8k total

downloads 3k

docker pulls 3M



Seriously?

docker pulls

3M

No, really, seriously???

Project Roadmap

waffle

Backlog 38 | Blocked 0 | Ready 6 | In Progress 3 | Done 0

- Get help from a UI/UX expert for our design/layout tasks
- **Hacking Instructor** to guide beginners through challenges



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>

Any Questions?



Copyright (c) 2014-2019 **Björn Kimminich**

Licensed under the **MIT** license.

[Post-Credits Bonus Content]

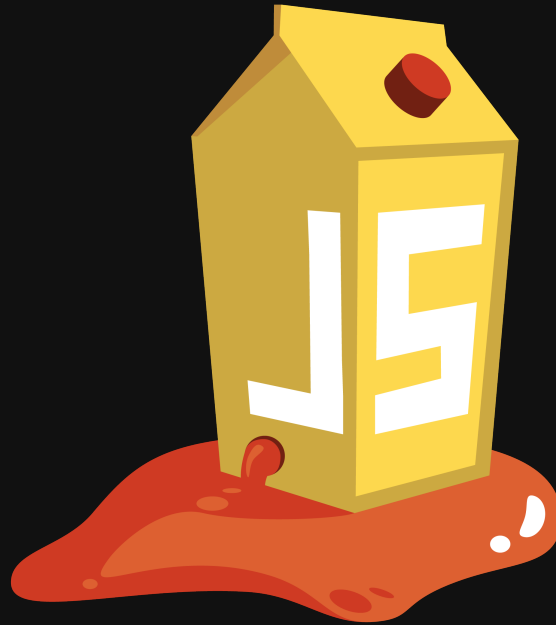
The alpha-release of the

Juice Shop jingle



In front of live audience for the ~~first~~ second time ~~exclusively~~ at
OWASP BeNeLux Days 2018!

(Naturally, finding this soundfile and its lyrics will become two new challenges very soon!)



Copyright (c) 2014-2019 **Björn Kimminich**

Licensed under the **MIT** license.

Created with **reveal.js** - The HTML Presentation Framework