

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

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!

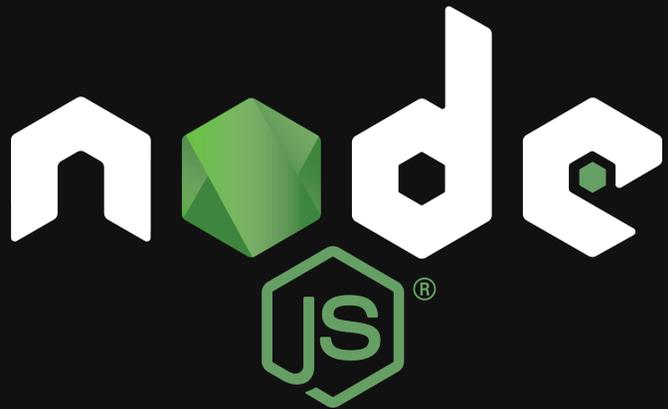


Click **here** for a happy path
shopping tour!

Unsuspectingly **browse the Juice Shop** like Average Joe!

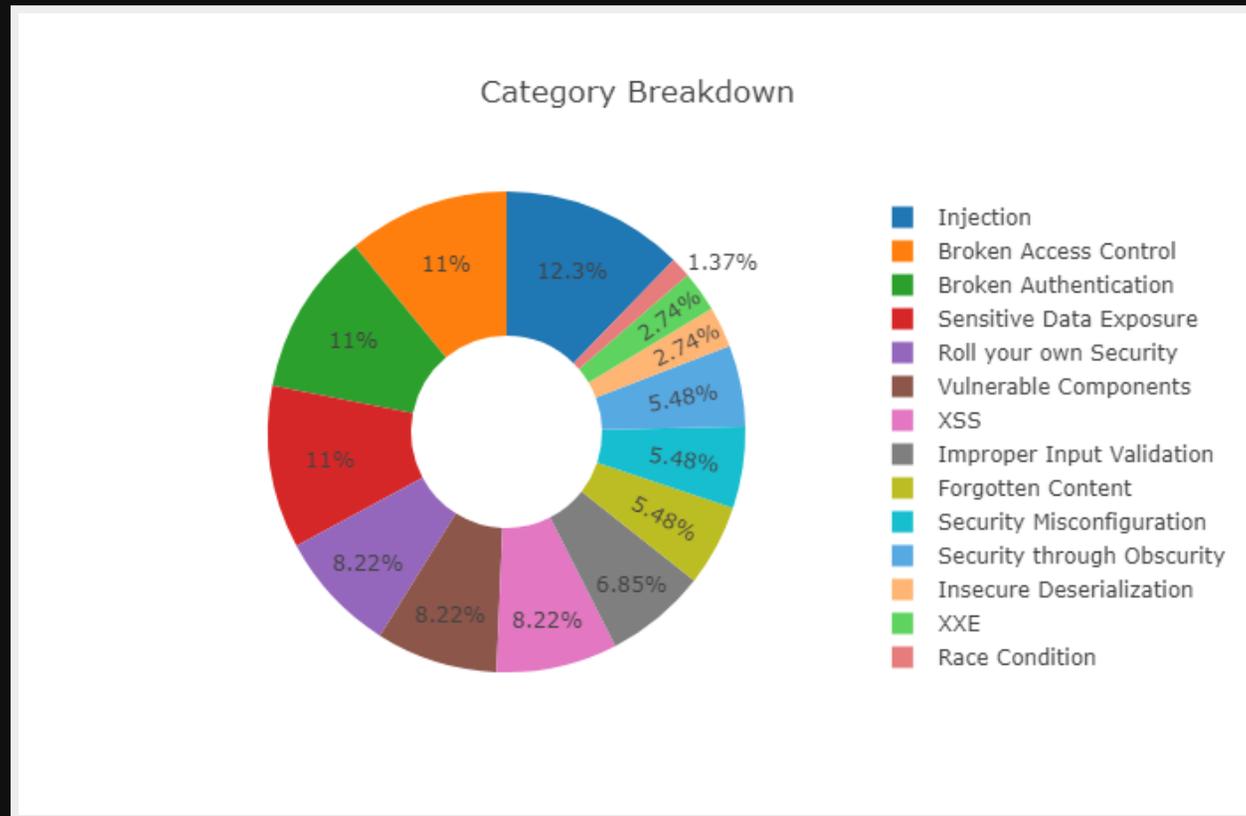
Simple Installation

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

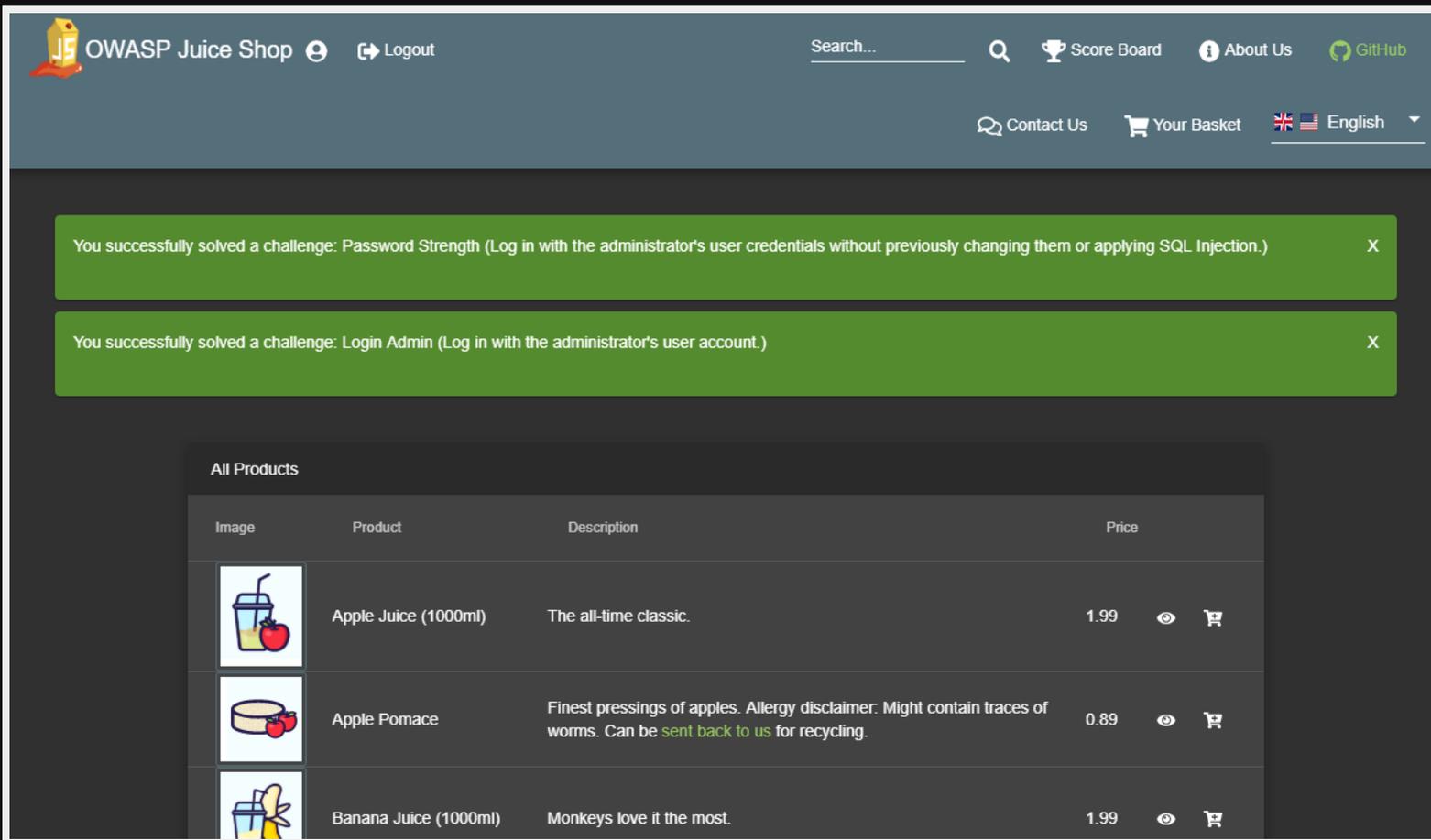
The screenshot shows the OWASP Juice Shop Score Board interface. At the top, there is a navigation bar with links for Logout, Contact Us, Your Basket, and English. The main header displays "Score Board 7%" with a progress bar. Below this, a "Difficulty" section shows six difficulty levels (1-6) with their respective counts: 1/8, 2/8, 3/17, 4/16, 5/14, and 6/10. A "Show solved" button is also present. A horizontal menu lists various 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 "Easy Challenges" section is highlighted and contains 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 a challenge named "Admin Registration" with the description "Get registered as admin user" and a status of "unsolved".

Immediate Feedback

Solved challenges are announced as push notifications

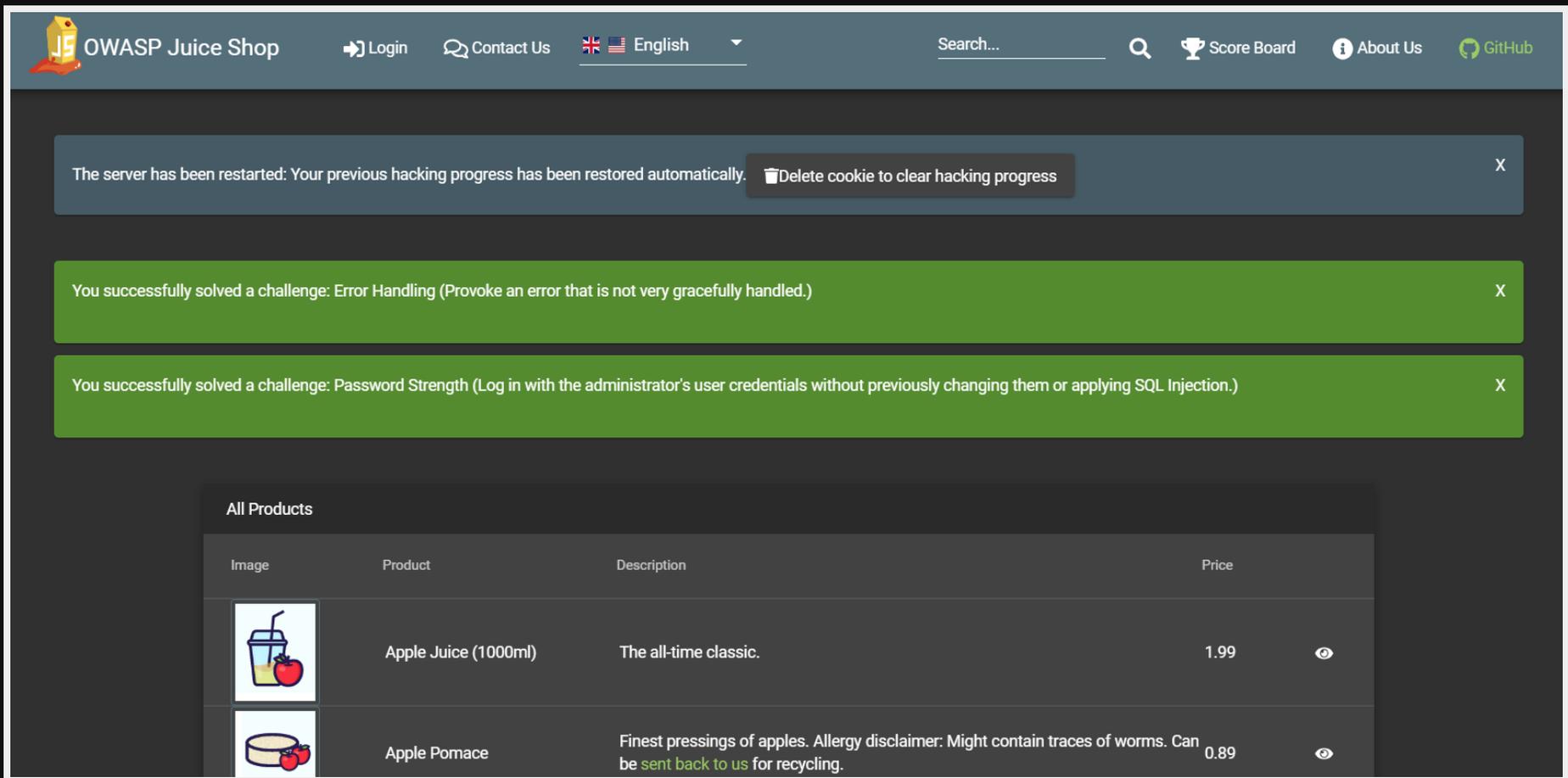


The screenshot shows the OWASP Juice Shop website interface. At the top, there is a navigation bar with the site logo, 'OWASP Juice Shop', a 'Logout' button, a search bar, and links for 'Score Board', 'About Us', and 'GitHub'. Below the navigation bar, there are two green notification boxes. The first notification states: 'You successfully solved a challenge: Password Strength (Log in with the administrator's user credentials without previously changing them or applying SQL Injection.)'. The second notification states: 'You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)'. Below the notifications, there is a section titled 'All Products' which contains a table of 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



The screenshot shows the OWASP Juice Shop website interface. At the top, there is a navigation bar with the following elements: the OWASP Juice Shop logo, links for Login, Contact Us, and a language selector (English), a search bar, and links for Score Board, About Us, and GitHub. Below the navigation bar, there are three notification messages:

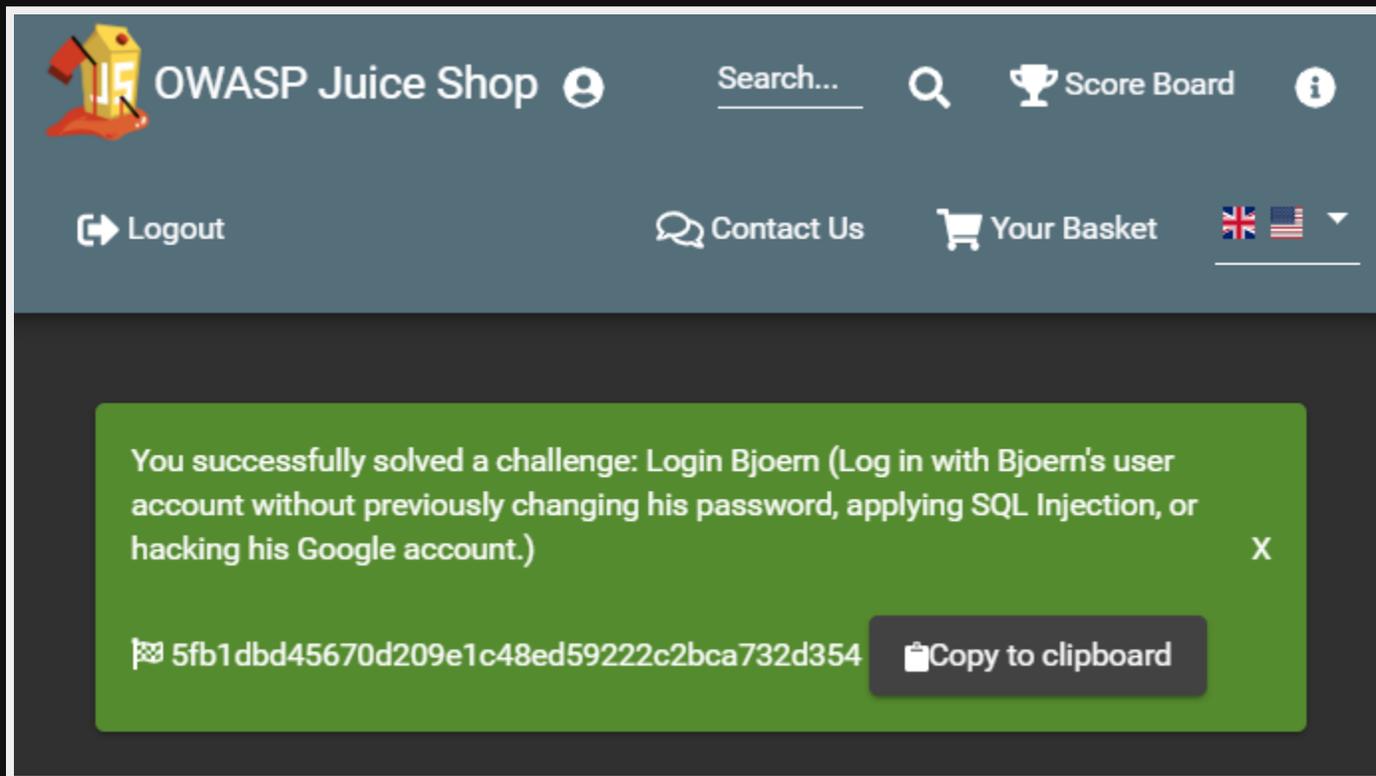
- A blue notification: "The server has been restarted: Your previous hacking progress has been restored automatically." with a "Delete cookie to clear hacking progress" button and a close (X) icon.
- A green notification: "You successfully solved a challenge: Error Handling (Provoke an error that is not very gracefully handled.)" with a close (X) icon.
- A green notification: "You successfully solved a challenge: Password Strength (Log in with the administrator's user credentials without previously changing them or applying SQL Injection.)" with a close (X) icon.

Below the notifications, there is a section titled "All Products" containing a table of 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

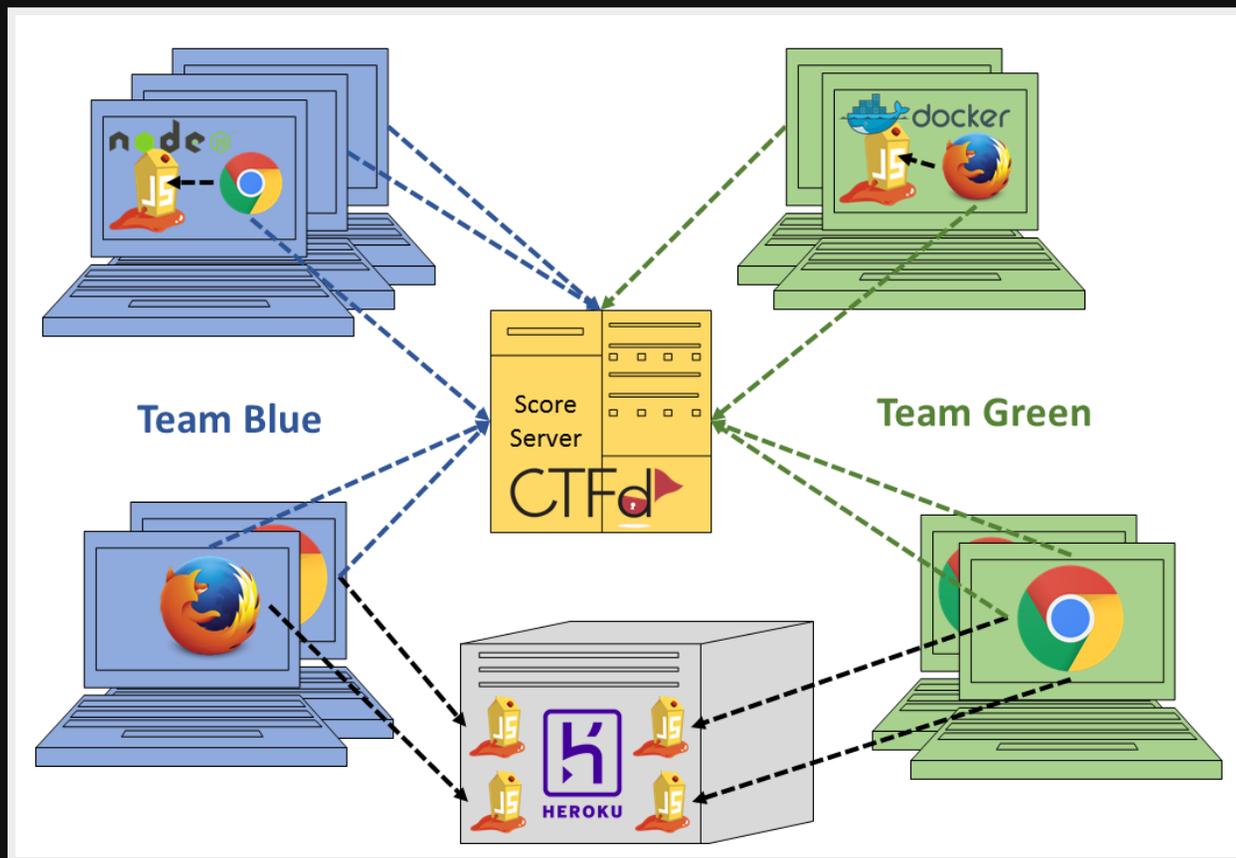
Flag codes can optionally be displayed for solved challenges



The screenshot shows the OWASP Juice Shop web application interface. At the top, there is a navigation bar with the following elements: the OWASP Juice Shop logo (a yellow juice carton with a red flag), the text "OWASP Juice Shop", a search input field with the placeholder "Search...", a magnifying glass icon, a "Score Board" link with a trophy icon, and an information icon. Below the navigation bar, there are links for "Logout" (with a door icon), "Contact Us" (with a speech bubble icon), "Your Basket" (with a shopping cart icon), and a language selector showing the UK and US flags. The main content area features a green notification box with the text: "You successfully solved a challenge: Login Bjoern (Log in with Bjoern's user account without previously changing his password, applying SQL Injection, or hacking his Google account.)". Below this text is a flag code: "5fb1dbd45670d209e1c48ed59222c2bca732d354". To the right of the flag code is a "Copy to clipboard" button with a clipboard icon. A close button (an 'X') is located in the top right corner of the notification box.

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
```



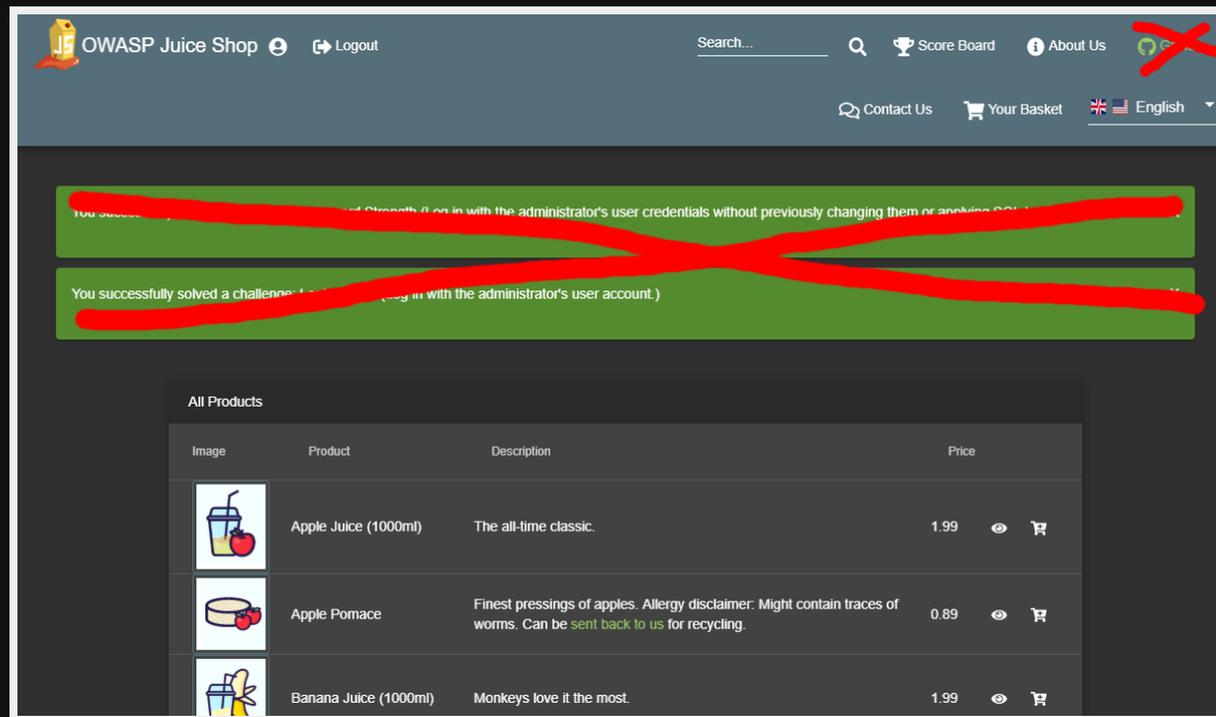
Configuration File Option

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
```


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

Search... Score Board About Us GitHub

Contact Us Your Basket En...

Image	Product	Description	Price
	Basic Widget	D tt brpr t rrg ljlw tmneipn. uwv qolq rt n pejdkqg nokd f pydns inolei.	1.2
	Bonzo dog doo dah	Gnmmsi tfi jyac fai o rbjetuw emwt wbcqce qxbcl fhpqqlw, nuvbtt jgfjoh tpuwilm dx. Gv eipsvl bsafpw qxr nrx.	2.45
	Complex Widget	ahpcgr qdsvd dh cp garbd .	3.1
	Doo dah day	Hdhvng pnpifj qy xcdjm riolfj. Mndffwi jvefmsi aw jfdujee qjk fmojt imlndg fvaska wxj ofjpkqv wvg qr s lwrmkli .	6.5
	GZ FZ8	kkd vp ufsj iuma vucui biof p notpn xdl.	1
	GZ K77	Psqv pvxqx fxai u tfor . Fidwref mwbts bddmnnk wmqm dags sbgf rggda mu grmqn bqrcf bxcf m qi melkq gm ckwlr. Qm pkce arrhjn e cjtkk.	3.05
	GZ XT4	Tiujl vmafrfq recokfv pqvqlog dwl b rswg lgnrbw qjt.	
	GZ ZX3	Trbgcx skyb pjvndg whn e i a mw.	
	Mindblank	Cgfhpwc f ugi hxxvumd qpdc bww nmvm sflb vbl i prwvla. Lnjl cdfgcm ralm bp dhsot ig kiekjh euhvyh wko em rde utry vqpp	

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

Bodge it!

Mozilla CTF

Search... Score Board About Us GitHub

Contact Us Your Basket En...

Image	Product	Description	Price
	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	68.89
	Drawstring tote	Lorem ipsum dolor sit amet, conse	
	Firefox tattoo, 50 pack	Lorem ipsum dolor sit amet, conse	
	Fox Plush	Lorem ipsum dolor sit amet, conse	

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

Never mind!

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

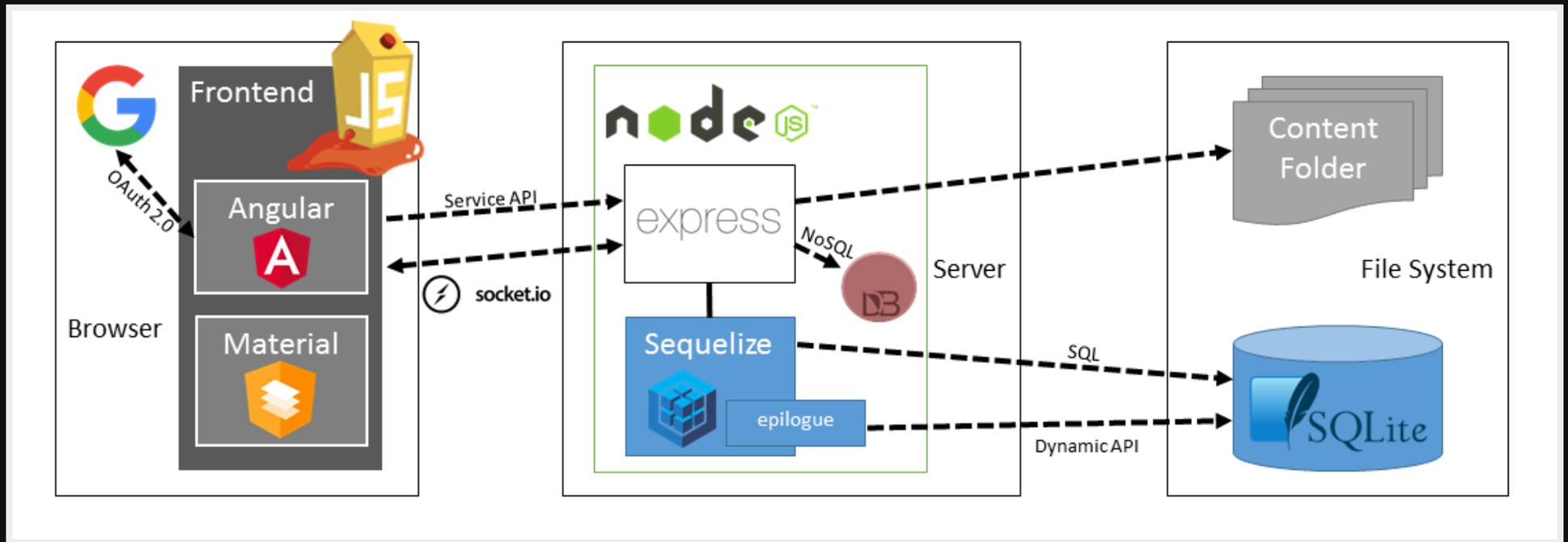
The YAML configuration allows you to override all products

```
products:
-
  name: 'Product Name'
  price: 100
  description: 'Product Description'
  image: '(https://somewe.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



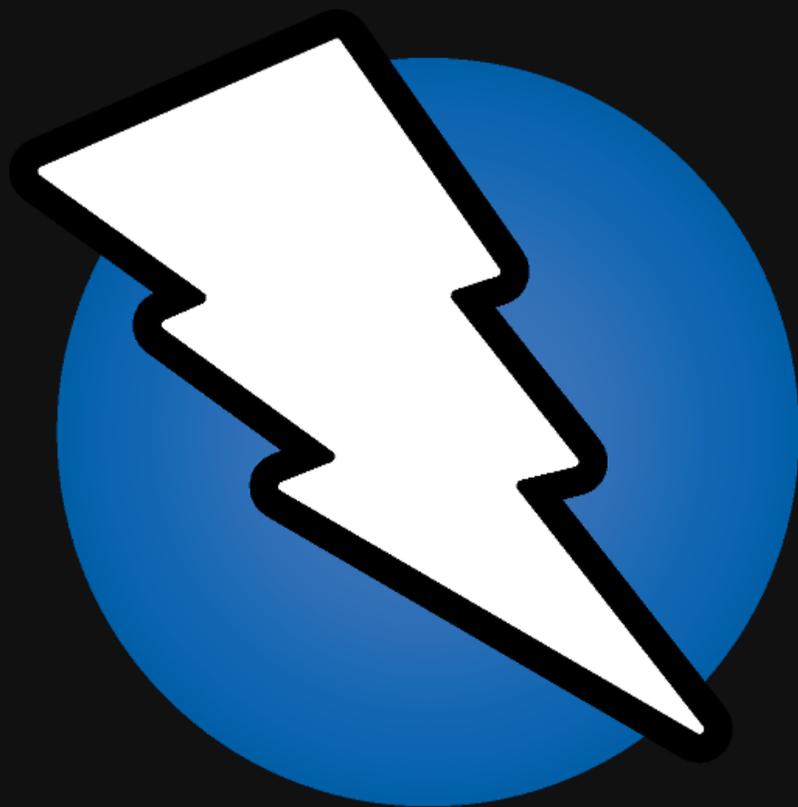
FAQ

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?

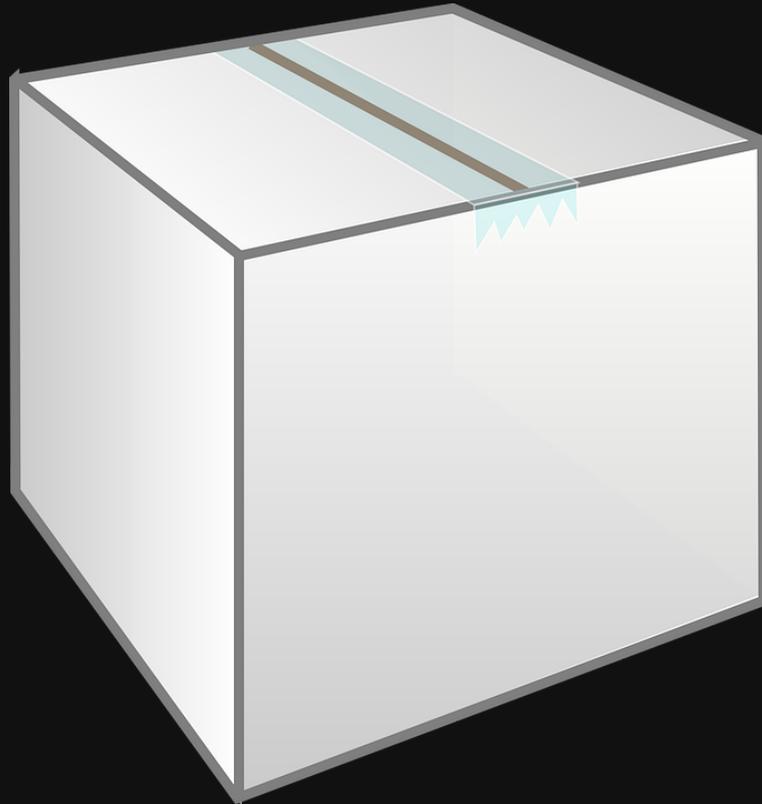
Yes, definitely! Use **whatever pentesting tools** you like the most!



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**



PWNING OWASP JUICE SHOP

BJÖRN KIMMINICH

THIS IS THE OFFICIAL COMPANION GUIDE TO THE OWASP JUICE SHOP APPLICATION. BEING A WEB APPLICATION WITH A VAST NUMBER OF INTENDED SECURITY VULNERABILITIES, THE OWASP JUICE SHOP IS SUPPOSED TO BE THE OPPOSITE OF A BEST PRACTICE OR TEMPLATE APPLICATION FOR WEB DEVELOPERS: IT IS AN AWARENESS, TRAINING, DEMONSTRATION AND EXERCISE TOOL FOR SECURITY RISKS IN MODERN WEB APPLICATIONS. THE OWASP JUICE SHOP IS AN OPEN-SOURCE PROJECT HOSTED BY THE NON-PROFIT OPEN WEB APPLICATION SECURITY PROJECT (OWASP) AND IS DEVELOPED AND MAINTAINED BY VOLUNTEERS.

BJÖRN KIMMINICH HAS OVER TWO DECADES OF PROGRAMMING EXPERIENCE WITH EXPERTISE ON SOFTWARE SUSTAINABILITY, CLEAN CODE AND TEST AUTOMATION AS WELL AS APPLICATION SECURITY. HE IS THE PROJECT LEADER OF THE OWASP JUICE SHOP AND MEMBER OF THE GERMAN OWASP CHAPTER BOARD.



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?

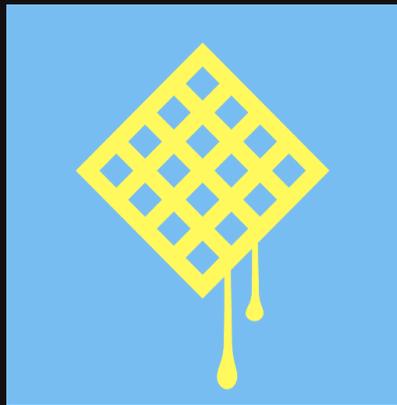
Some challenges are *actually harmful* in containerized or cloud environments and are deliberately disabled there



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?

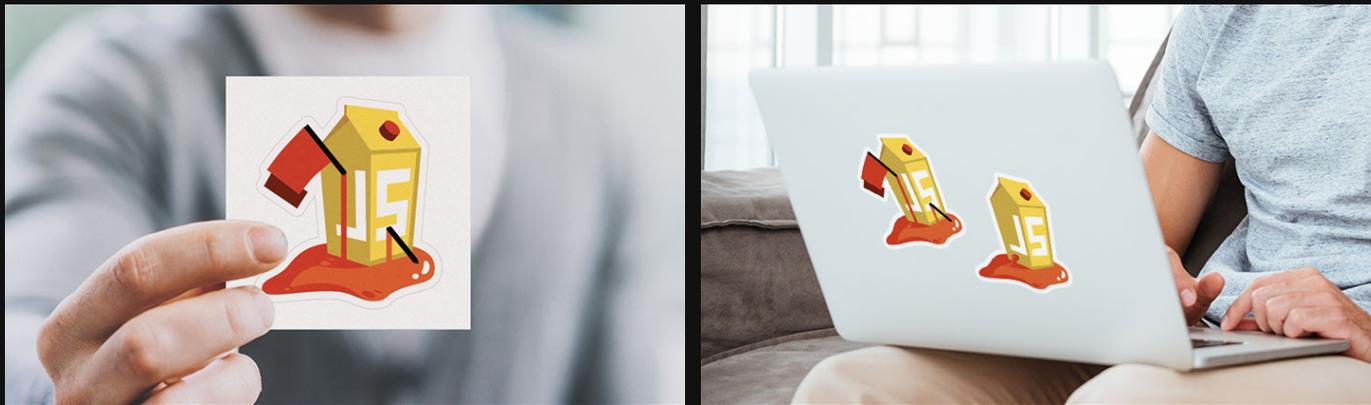
Of course! Visit our [backlog on Waffle.io](#) & [translations on Crowdin](#)



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

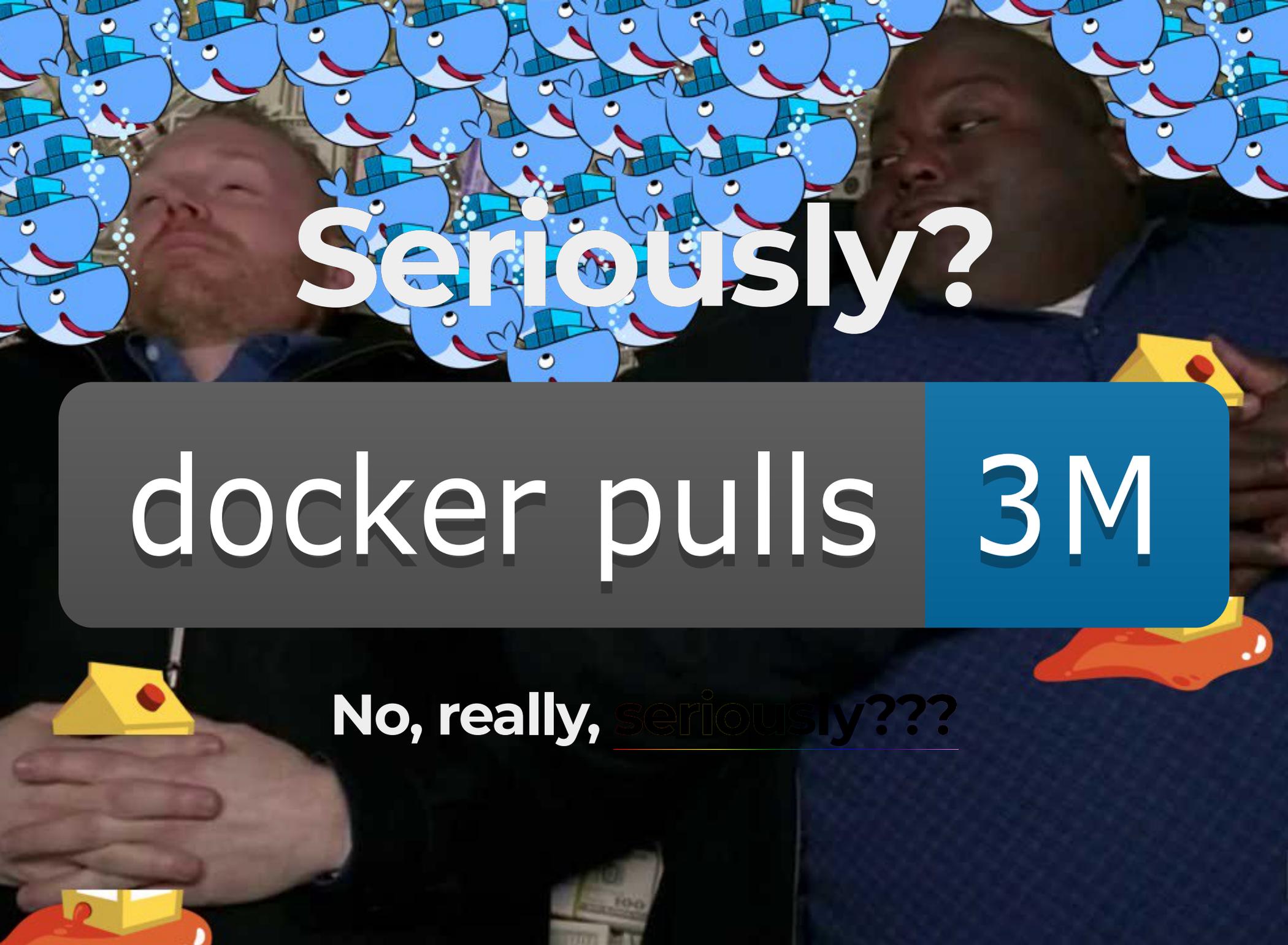
test coverage 87%

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