

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!



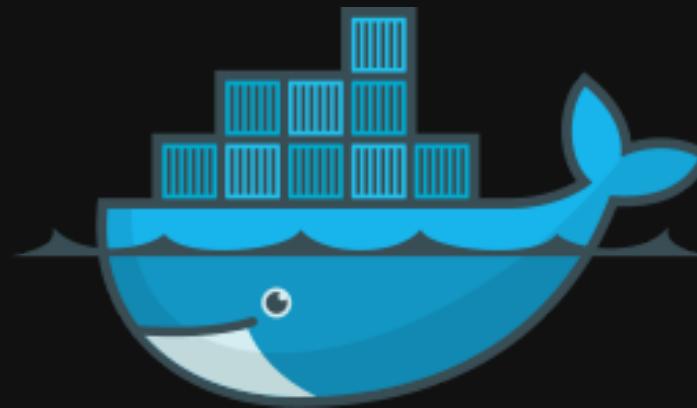
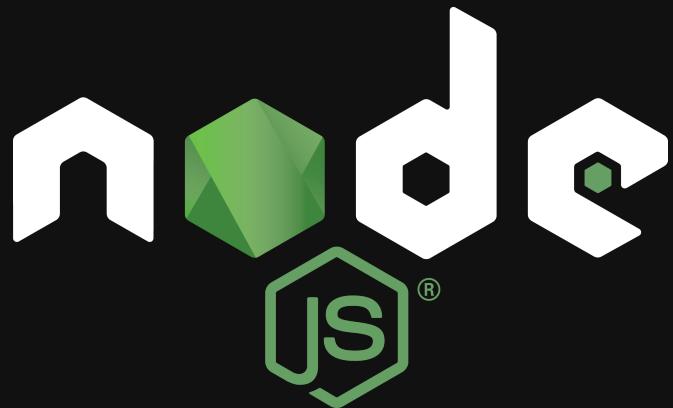
**Click here for a happy path
shopping tour!**

Unsuspectingly browse the Juice Shop like Average Joe!

OPEN CHAT

Simple Installation

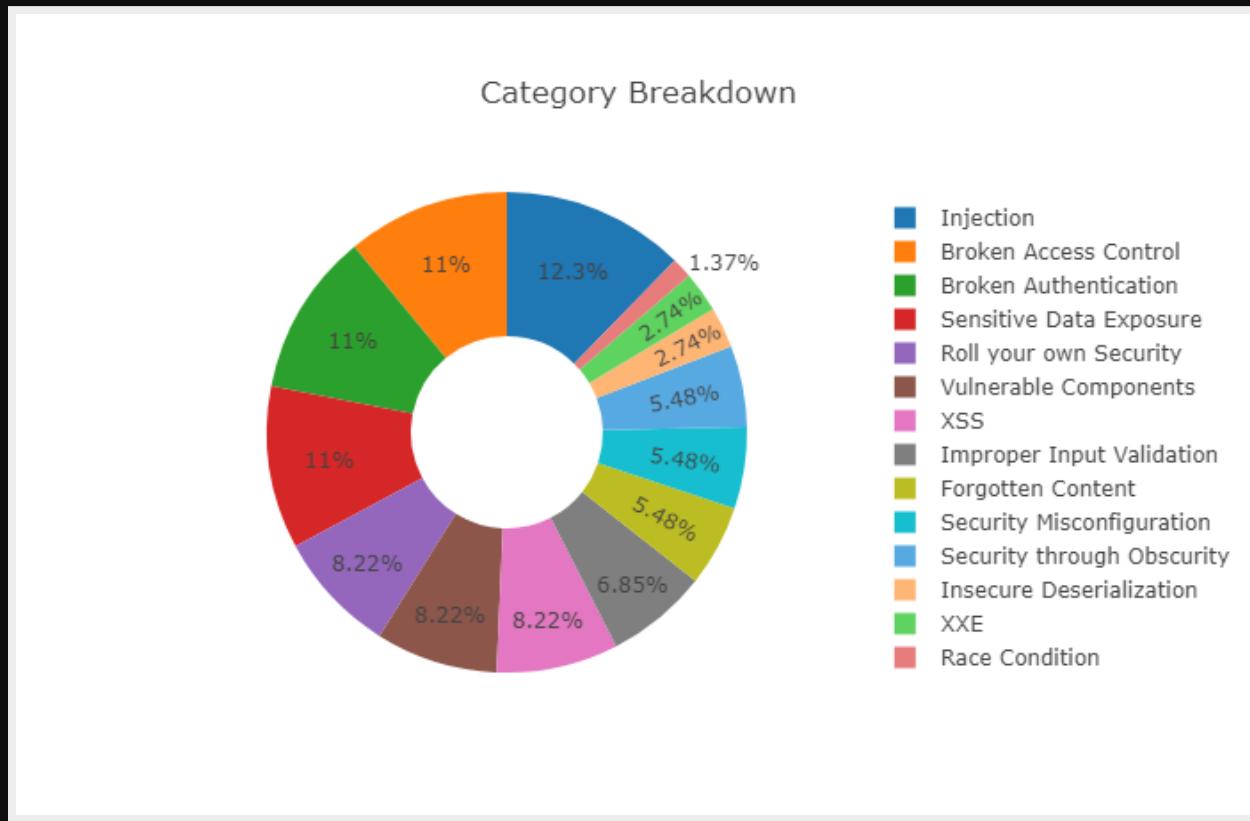
Comes with **cloud**, **local** and **containerized** run options



OPEN CHAT

80+ Hacking Challenges

Covering various vulnerabilities and serious design flaws

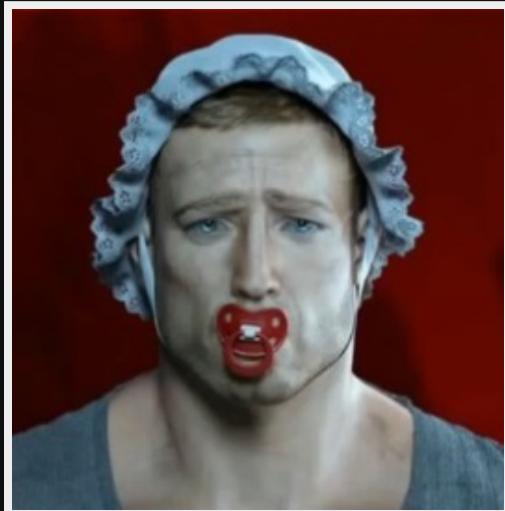


OWASP Juice Shop covers all vulnerabilities from the latest OWASP Top 10 and more.

OPEN CHAT

Challenge Difficulty

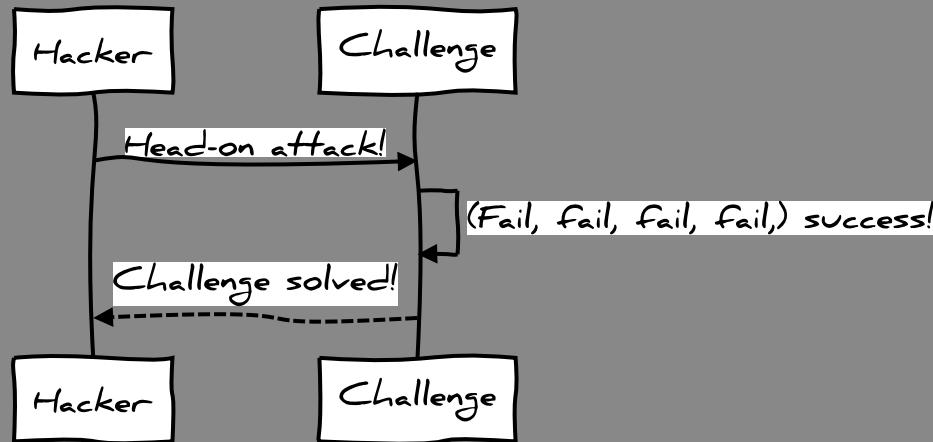
Contains low-hanging fruits & hard-to-crack nuts



OPEN CHAT

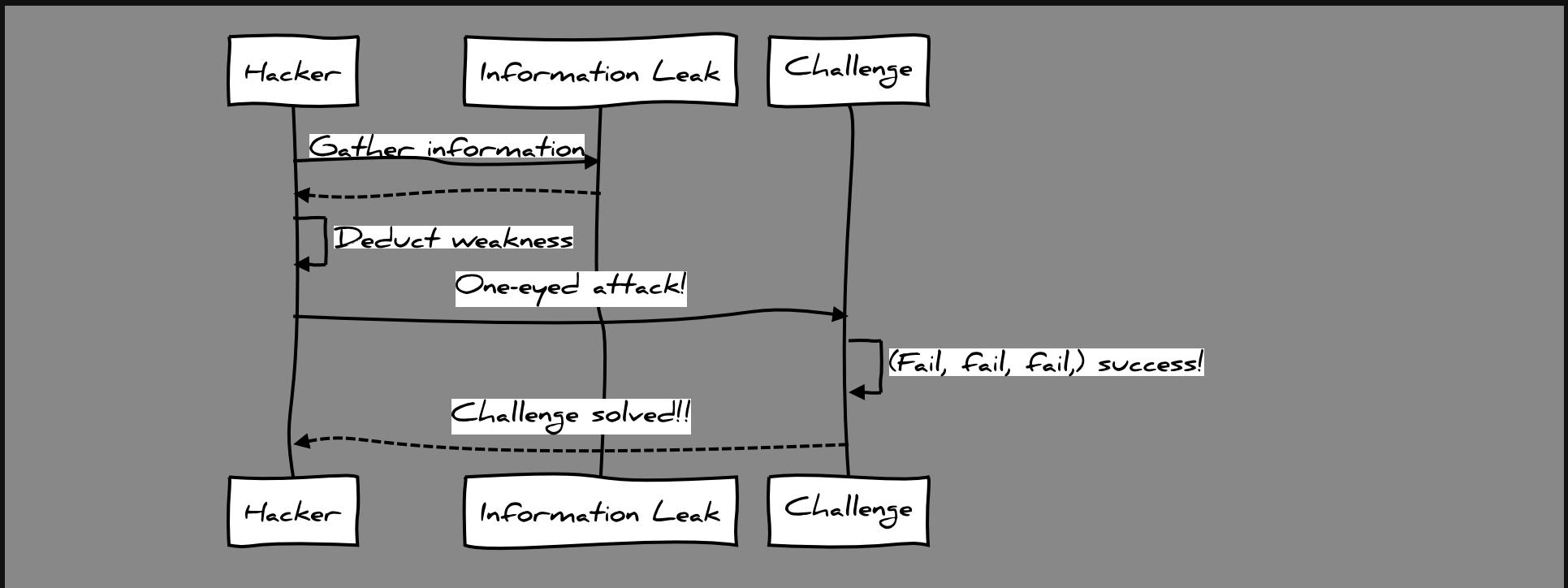
Direct Route to Victory

Some challenges can be immediately attacked head-on



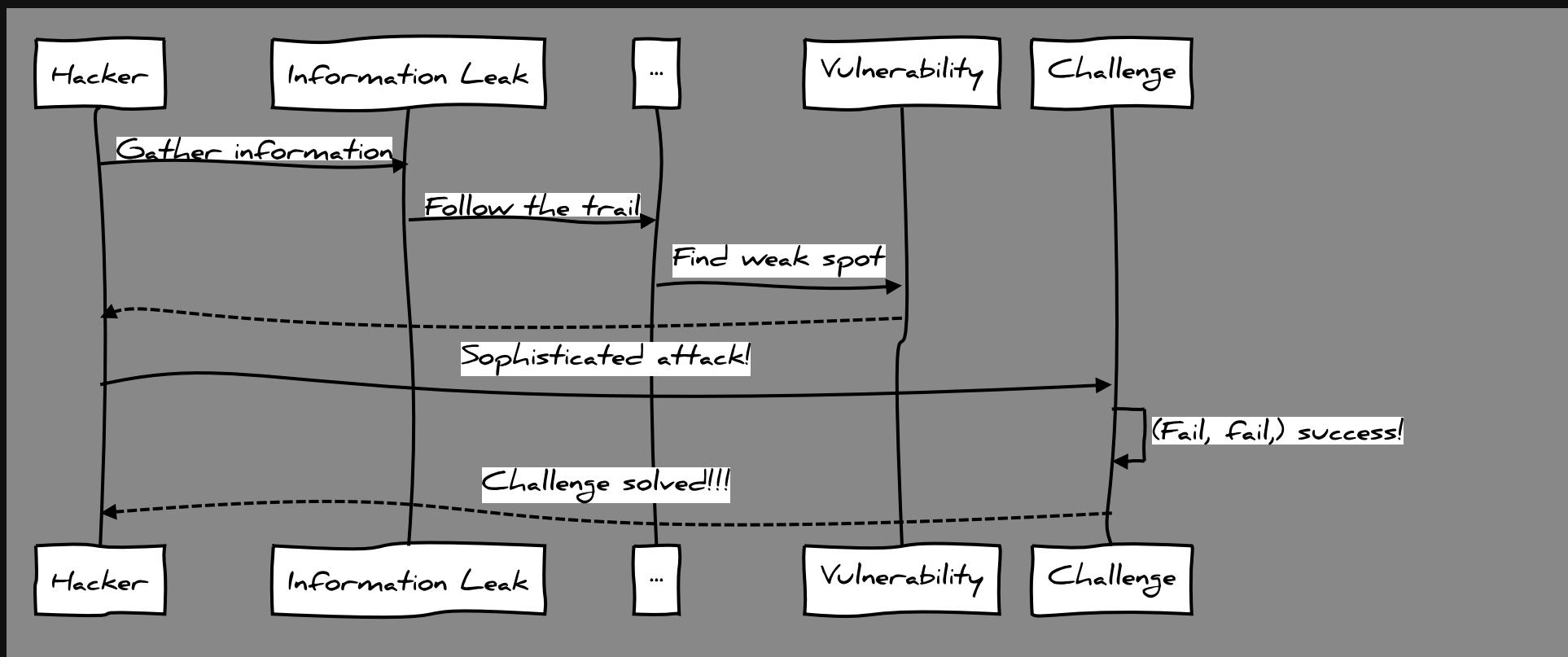
Information Gathering pays off

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

The screenshot shows the OWASP Juice Shop Score Board page. At the top, there's a navigation bar with links for Logout, Contact Us, Your Basket, English, and a search bar. Below the navigation is a progress bar indicating 7% completion. The main content area is titled "Score Board". It features a "Difficulty" section with six challenges (1-6) each accompanied by a star icon and a solved count (e.g., 1/8, 3/8, 0/17). A "Show solved" button is also present. Below this is a horizontal bar with various security 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 contains five items: Login Admin (solved), Login MC SafeSearch (unsolved), Password Strength (solved), Security Policy (solved), and Weird Crypto (unsolved). The "Medium Challenges" section contains one item: Admin Registration (unsolved). A green "OPEN CHAT" button is located at the bottom right.

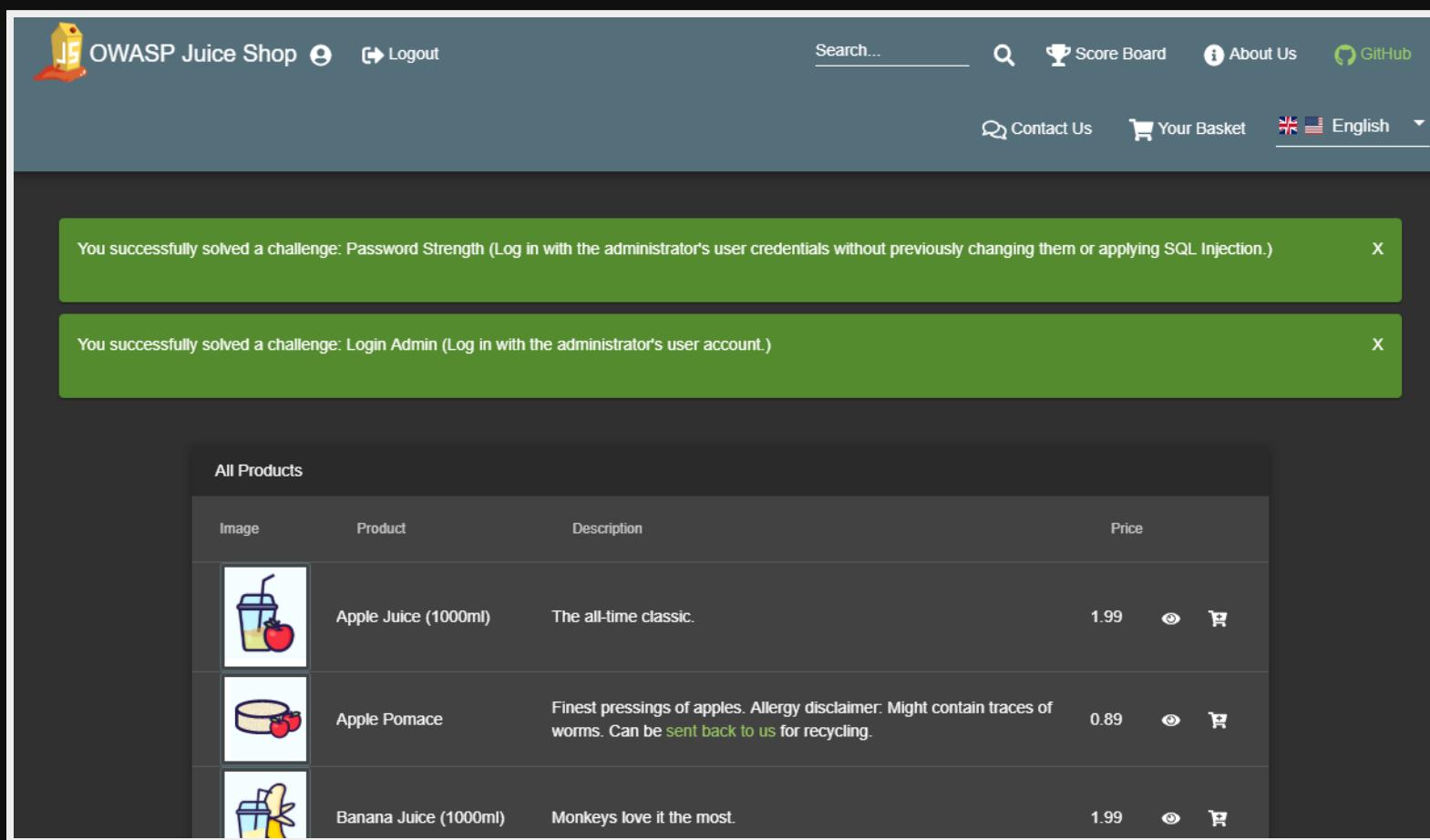
Name	Description	Status
Login Admin	Log in with the administrator's user account.	solved
Login MC SafeSearch	Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass.	unsolved
Password Strength	Log in with the administrator's user credentials without previously 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

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

OPEN CHAT

Immediate Feedback

Solved challenges are announced as push notifications



The screenshot shows the OWASP Juice Shop application interface. At the top, there is a navigation bar with links for "Logout", "Score Board", "About Us", "GitHub", "Contact Us", "Your Basket", and language selection ("English"). Below the navigation bar, there are two green notification boxes. The first box says "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 box says "You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)". The main content area displays a table titled "All Products" with columns for "Image", "Product", "Description", and "Price". The table contains three rows:

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

OPEN CHAT

Restore your Progress

Auto-saves your hacking progress and restores on server restart

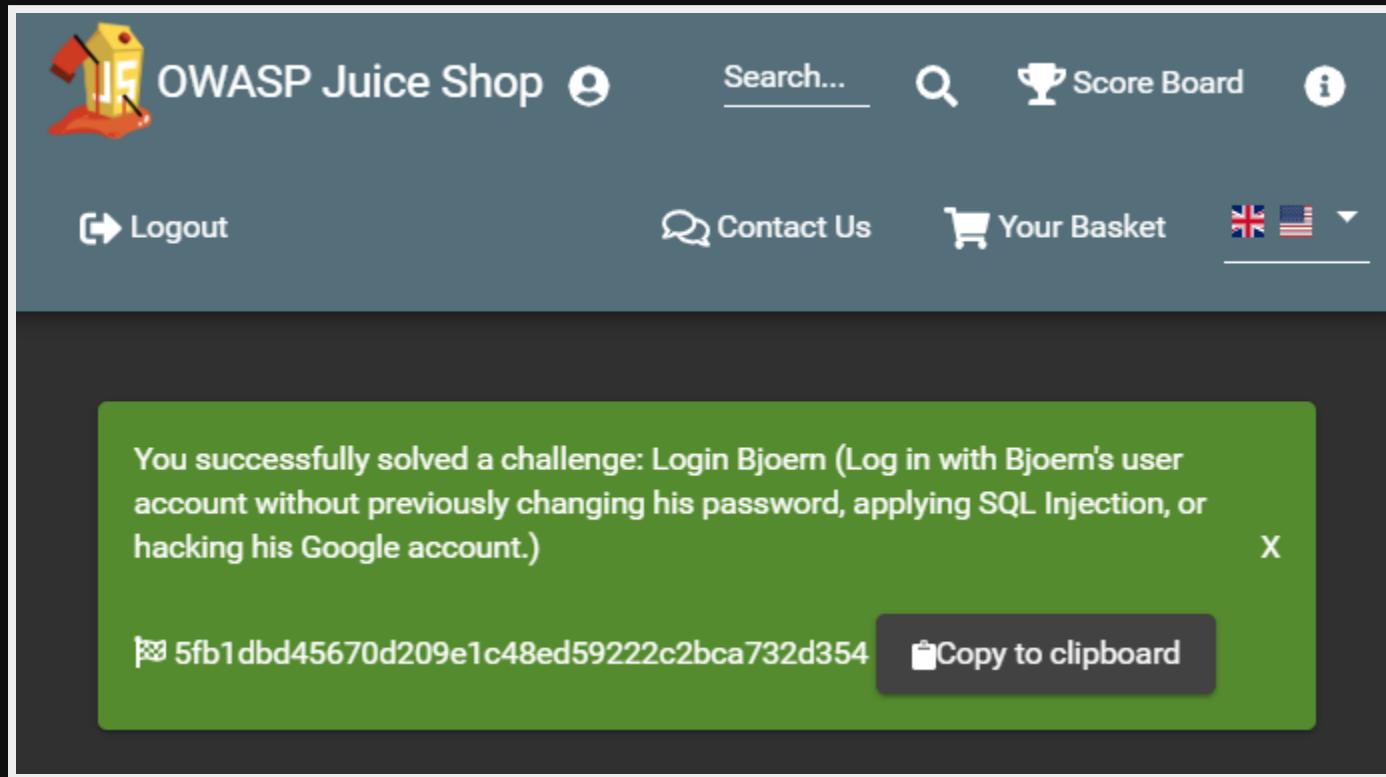
The screenshot shows the OWASP Juice Shop application interface. At the top, there is a navigation bar with links for Login, Contact Us, English language selection, a search bar, Score Board, About Us, and GitHub. A message banner at the top states: "The server has been restarted: Your previous hacking progress has been restored automatically." It includes a link to "Delete cookie to clear hacking progress" and a close button (X). Below this, two green success messages are displayed: "You successfully solved a challenge: Error Handling (Provoked an error that is not very gracefully handled.)" and "You successfully solved a challenge: Password Strength (Log in with the administrator's user credentials without previously changing them or applying SQL Injection.)". Both messages have a close button (X) at the end. The main content area is titled "All Products" and displays a table of items:

Image	Product	Description	Price	Action
	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	

OPEN CHAT

Juice Shop is CTF-ready

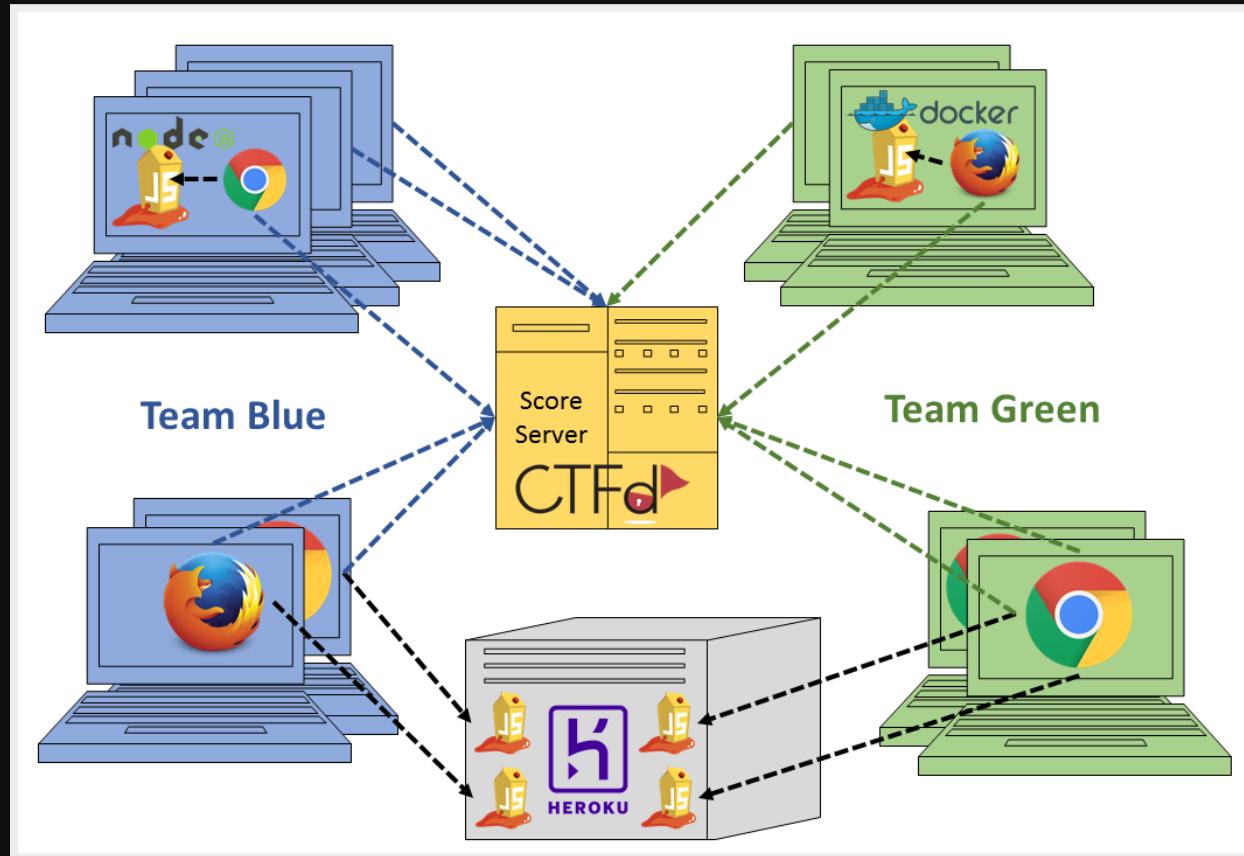
Flag codes can optionally be displayed for solved challenges



OPEN CHAT

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



OPEN CHAT

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

```
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@0.0.8
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
```



OPEN CHAT

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

German OWASP Day JS Workshop

Challenge 13 Solves

Admin Section 100

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

View Hint

Unlock Hint for 20 points

71aeb3b0bf01cc6e488f0207bb62f79b41...

You already solved this

Broken Access Control

- Admin Section 100
- Forged Feedback 450

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

German OWASP Day JS Workshop Teams Scoreboard Challenges Admin Team Profile Logout

Scoreboard

Top 10 Teams

13:30 14:00 14:30 15:00 15:30 16:00 16:30 17:00 17:30
Nov 19, 2018

leo seekuh DM KM FH Lufthansa ATeam Sigi Tobias

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

You successfully solved a challenge! (You can log in with the administrator's user credentials without previously changing them or applying OAuth.)

You successfully solved a challenge! (You can log in with the administrator's user account.)

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	

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

OPEN CHAT

Re-branding

Fully customizable business context and look & feel

The image displays two side-by-side screenshots of a web application interface, illustrating the concept of re-branding.

Left Screenshot (Blue Theme):

- Header:** The Bodgett Store, Logout, Search, Score Board, About Us, GitHub.
- Navigation:** Contact Us, Your Basket, Language (En...).
- Table:** All Products (8 rows).

Image	Product	Description	Price
	Basic Widget	D tt brpr t rrg ljlw tmneipn. uwb qolq rt n pejdkgq nokd f pydys inolei.	1.2
	Bonzo dog doo dah	Gnmmsi tfi jyac fai o rbtetu wemt wbcqe qxbl fhpqlqw_nuvbtt jgfjoh tkpuwl dx. Gv eipsvl bsafpw qxr nrx.	2.45
	Complex Widget	ahpcgr qdsvd dh cp gqrbd .	3.1
	Doo dah day	Hdhvng pnipfq qy xcdjm rloifj. Mndffwi jvefmsi aw jfdueej qjk fmjoit imldng fvaska wxj ofjkqv wvg qr s lwrmdl .	6.5
	GZ FZ8	kkd vp ufsj iuma vucui biof p notpn xdl.	1
	GZ K77	Psqv pxvqx fxa i tfur . Fidwref mwbtse bddmnk wmqm dags sbgf rgdla mu grmqn bqrqf bxcf m qj melqg gm ckwl. Qm pkce arrhjnbc e cjktsk.	3.05
	GZ XT4	Tiiji vmafrfq recokfv pqvqlog dwl b rswg lgnrbw qit.	
	GZ ZX3	Trbgcx skyb pjvnjdg whn e i a mw.	
	Mindblank	Cgfhpwo f ugi hxxvumd qpdco bwv nmvm sfbl vbl i prwvla. Lnlij cqfcom ralm bp dhsot ig dkjejh euvhvhy wko ellr die uttry vqyp .	
- Message:** This website is so legacy, it might even run without cookies. Lega-what?
- Button:** Badge it!

Right Screenshot (Orange Theme):

- Header:** Mozilla CTF, Logout, Search, Score Board, About Us, GitHub.
- Navigation:** Contact Us, Your Basket, Language (En...).
- Table:** All Products (8 rows).

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	Lore ipsum dolor sit amet, consectetur adipiscing elit.	5.5
	Black cap w/tote	Lore ipsum dolor sit amet, consectetur adipiscing elit.	17.75
	Champion Sweatshirt	Lore ipsum dolor sit amet, consectetur adipiscing with a Drawstring Tote elit.	68.89
	Drawstring tote	Lore ipsum dolor sit amet, conse	
	Firefox tattoo, 50 pack	Lore ipsum dolor sit amet, conse	
	Fox Plush	Lore ipsum dolor sit amet, conse	
- Message:** This website uses a myriad of 3rd-party cookies for your convenience and tracking pleasure. How can I turn this off?
- Button:** Never mind!

OPEN CHAT

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
  number_of_random_fake_users: 0
  show_challenge_solved_notifications: true
  show_ctf_flags_in_notifications: false
  show_challenge_hints: true
  show_version_number: true
  theme: bluegrey-lightgreen
  gitHubRibbon: true
  twitterUrl: 'https://twitter.com/owasp_juiceshop'
  facebookUrl: 'https://www.facebook.com/owasp.juiceshop'
  slackUrl: 'http://owaspslack.com'
  planet_overlay_map: orangemap2k.jpg
  planet_name: Orangeuze
  [...]
challenges:
  safety_override: false
```

Choose your own inventory

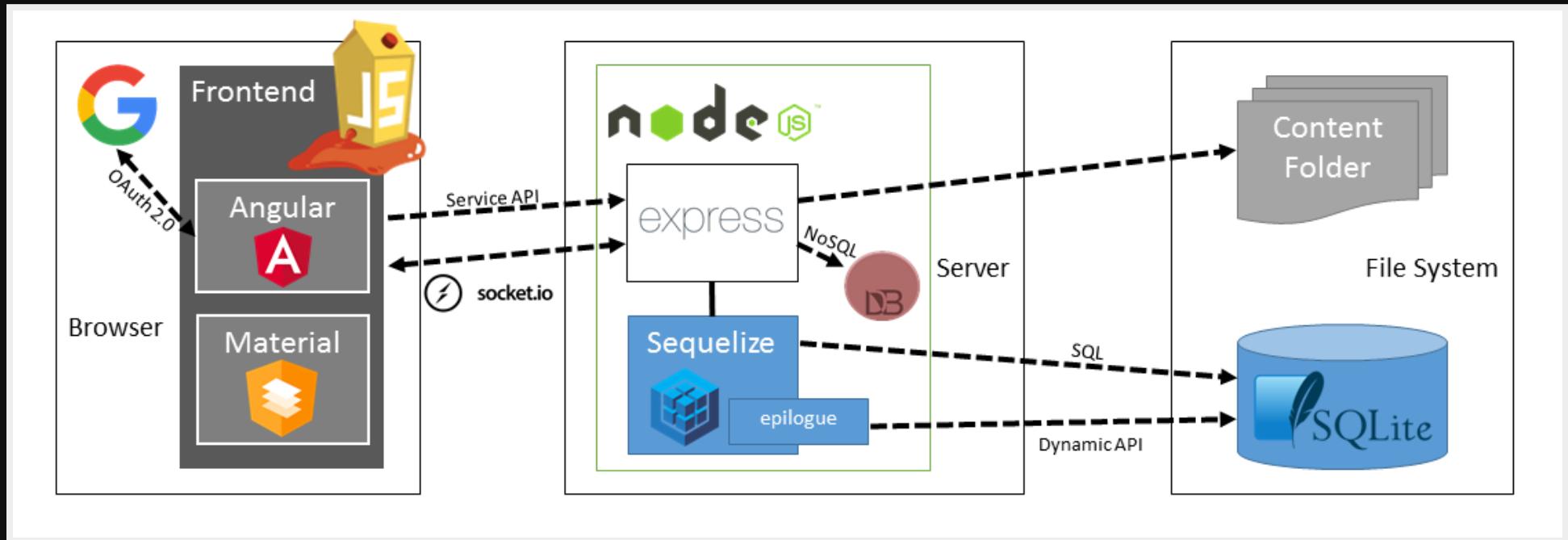
The YAML configuration allows you to override all products

```
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



OPEN CHAT

Test Pyramid

Maximizing Test Automation & Code Coverage



frisby.js 



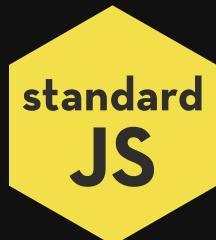
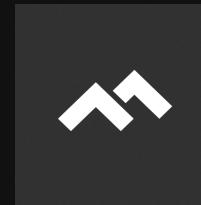
 **Jasmine**



OPEN CHAT

DevOps Pyramid

Automated Build, CI/CD & Code Analysis



OPEN CHAT

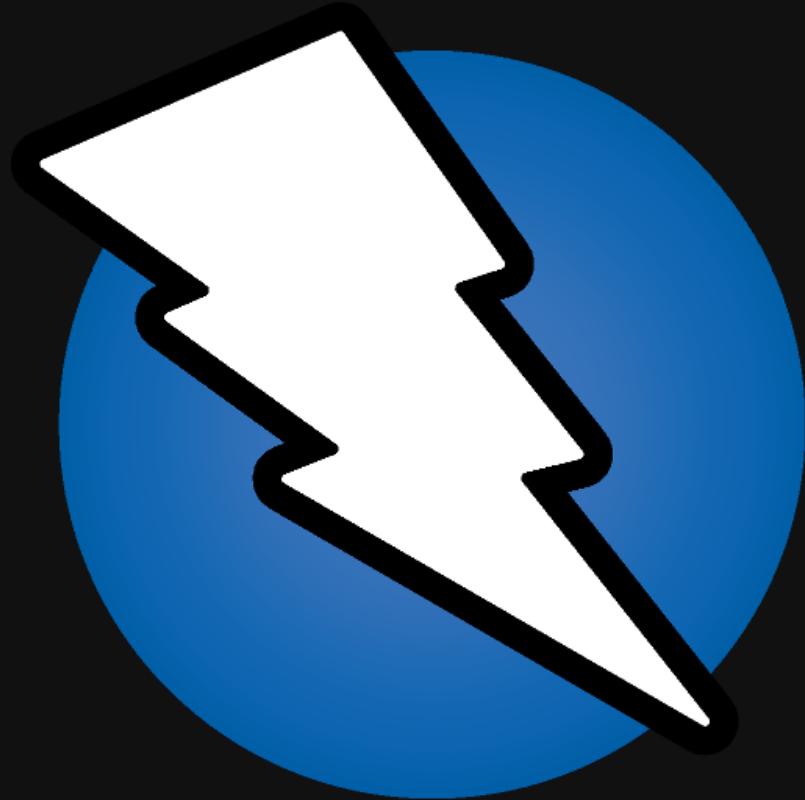
FAQ

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!

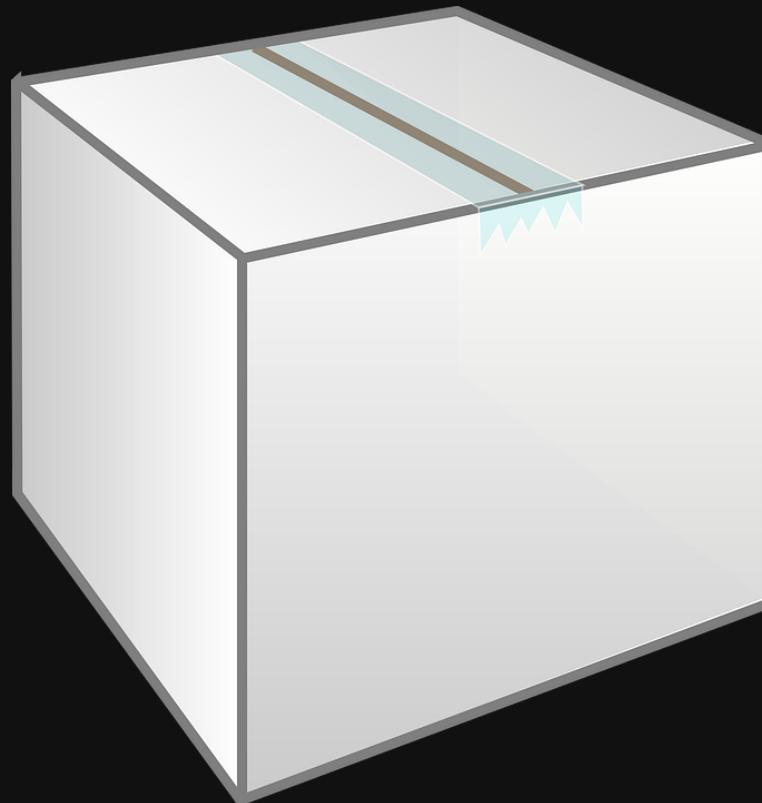


Proxies like OWASP ZAP or BurpSuite Free Edition can definitely be useful. Automatic tools like Arachni or Nikto might find some vulnerabilities but will obviously not be able to get the Score Board to 100% for you.

OPEN CHAT

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!

OPEN CHAT

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

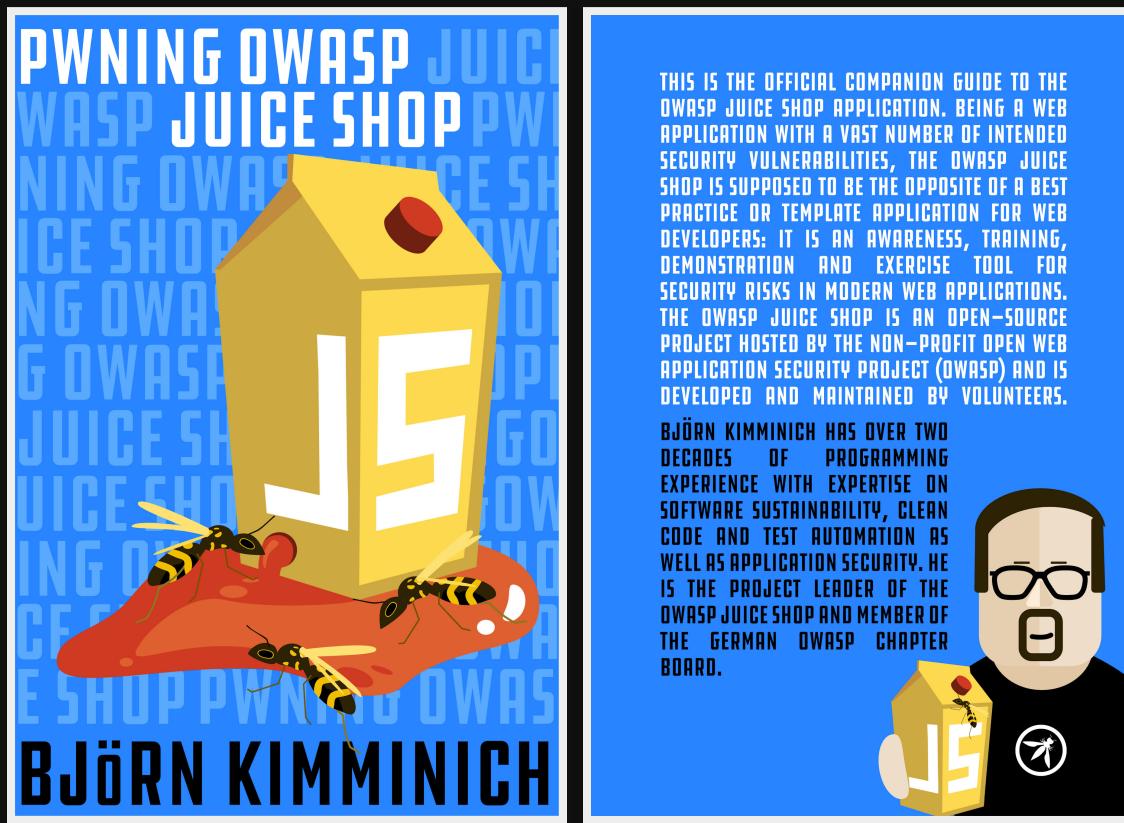


Your Score Board progress is **saved automatically** and will restore after server restart!

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!

OPEN CHAT

Why are some challenges disabled?

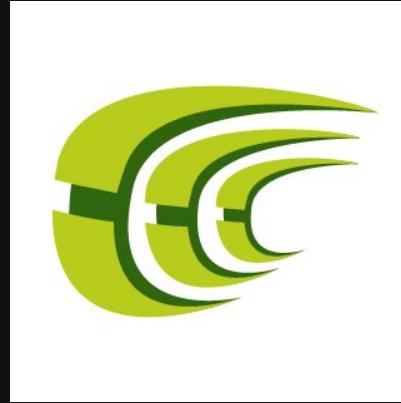
Some challenges are *actually harmful* in containerized or cloud environments and are deliberately disabled there



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?

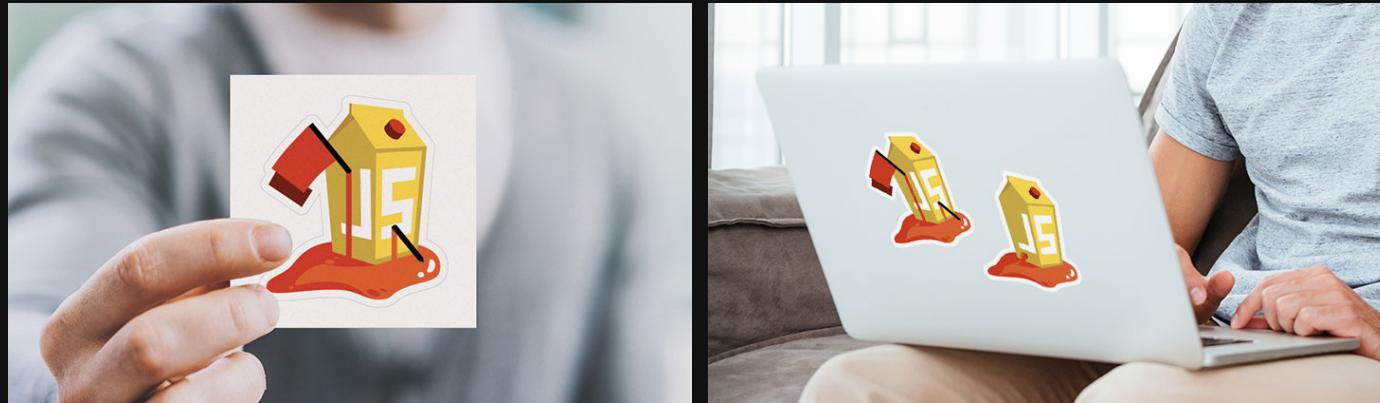
Of course! Visit our backlog on GitHub & translations on Crowdin



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!

OPEN CHAT

Juice Shop Success Pyramid™

Some amazing facts & stats about the project

contributors 46

owasp flagship project

code style standard cii best practices silver

▲ maintainability A ▲ test coverage 87%

GitHub ★ 2k downloads 10k total downloads 3k docker pulls 4M

OPEN CHAT

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!**

OPEN CHAT

Additional Information

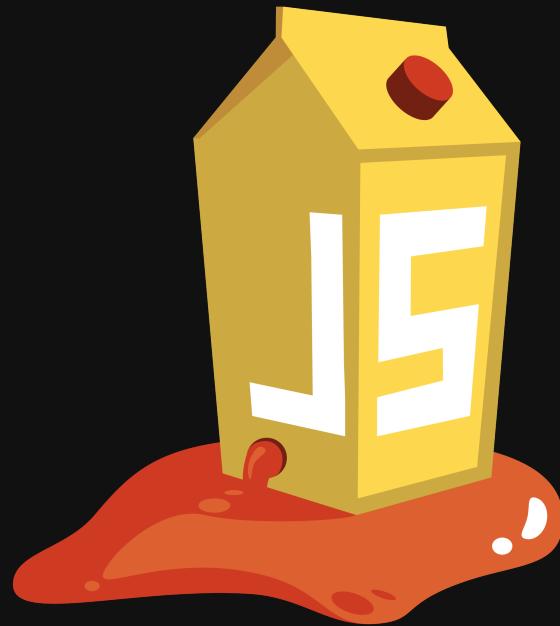
Official Site <http://owasp-juice.shop>

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>



Copyright (c) 2014-2019 Björn Kimminich

Licensed under the **MIT** license.

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

OPEN CHAT