

OWASP Juice Shop 10.x

Probably the most modern and sophisticated insecure 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)
But this doesn't have anything to do with juice (@coderPatros' wife)

<https://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 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!



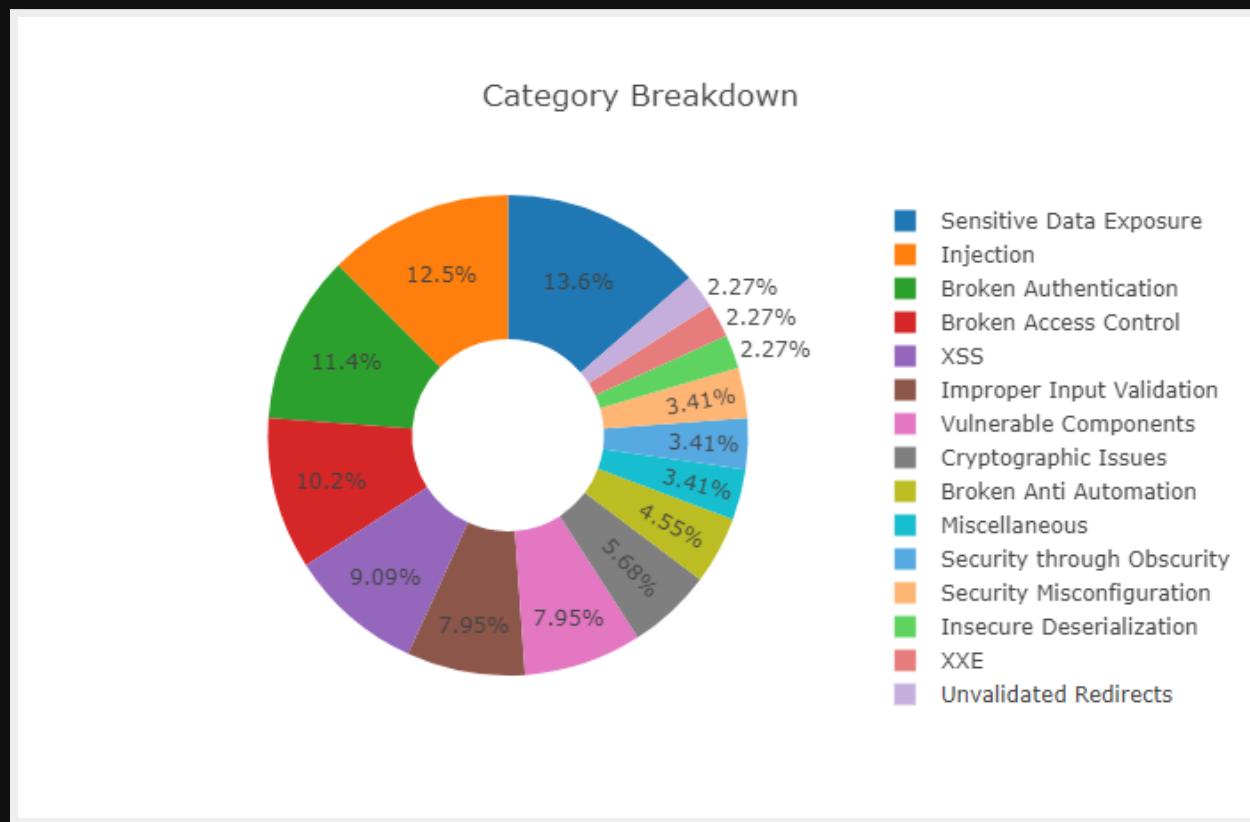
**Click here for a happy path
shopping tour!**

Unsuspectingly browse the Juice Shop like Average Joe!

OPEN CHAT

91+ 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

There's something to do for beginners and veterans alike



OPEN CHAT

Score Board

Challenge progress is tracked on server-side

The screenshot shows the OWASP Juice Shop Score Board page. At the top, there are six challenges represented by stars with numbers: 1 (2/9), 2 (0/10), 3 (0/19), 4 (0/21), 5 (0/16), and 6 (0/11). Below these are buttons for 'Show all' and 'Show solved'. A navigation bar at the bottom includes categories like Broken Access Control, Broken Anti Automation, Broken Authentication, Cryptographic Issues, Improper Input Validation, Injection, Insecure Deserialization, Miscellaneous, Security Misconfiguration, Security through Obscurity, Sensitive Data Exposure, Unvalidated Redirects, Vulnerable Components, XSS, and XXE. The main table lists challenges with columns for Name, Difficulty, Description, Category, and Status. Some challenges have orange 'solved' status indicators.

Name	Difficulty	Description	Category	Status
Confidential Document	★	Access a confidential document.	Sensitive Data Exposure	unsolved
DOM XSS	★	Perform a DOM XSS attack with <iframe src="javascript:alert('xss')">.	XSS	unsolved
Error Handling	★	Provoke an error that is neither very gracefully nor consistently handled.	Security Misconfiguration	solved
Outdated Whitelist	★	Let us redirect you to one of our crypto currency addresses which are not promoted any longer.	Unvalidated Redirects	unsolved
Privacy Policy	★	Read our privacy policy.	Miscellaneous	unsolved
Reflected XSS	★	Perform a reflected XSS attack with <iframe src="javascript:alert('xss')">.	XSS	unsolved
Repetitive Registration	★	Follow the DRY principle while registering a user.	Improper Input Validation	unsolved
Score Board	★	Find the carefully hidden 'Score Board' page.	Miscellaneous	solved

OPEN CHAT

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 a logo, a search icon, account information, a basket icon labeled "Your Basket", and a language selector set to "EN". Below the navigation bar, two green notification boxes are displayed, each containing a message about solving a challenge: "You successfully solved a challenge: Password Strength (Log in with the administrator's user credentials without previously changing them or applying SQL Injection.)" and "You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)". Both notifications have a close button ("X") in the top right corner. Below the notifications, the main content area is titled "All Products" and displays four product cards: "Apple Juice (1000ml)" priced at 1.99, "Apple Pomace" priced at 0.89, "Banana Juice (1000ml)" priced at 1.99, and "Carrot Juice (1000ml)" priced at 2.99. Each card features an "Add to Basket" button at the bottom.

OPEN CHAT

Restore your Progress

Auto-saves your hacking progress and restores on server restart

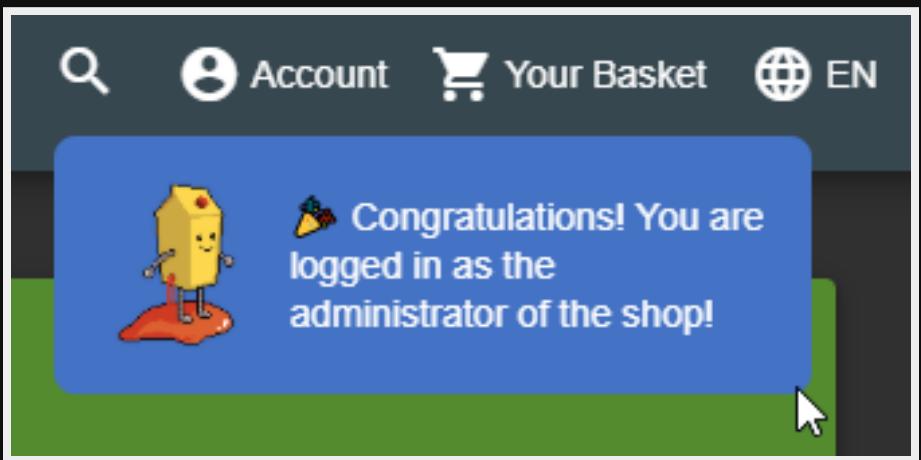
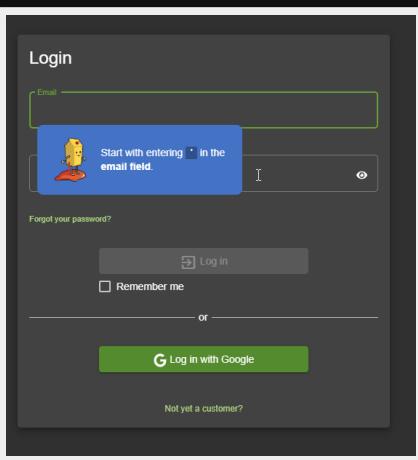
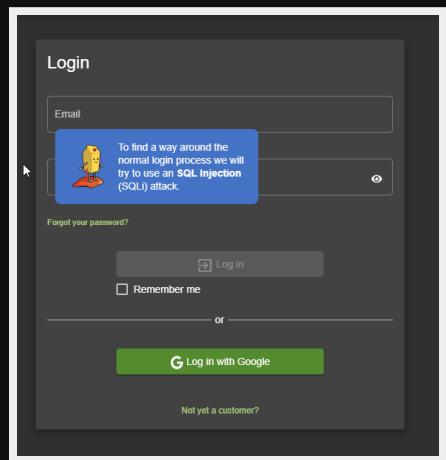
The screenshot shows the OWASP Juice Shop interface. At the top, there's a navigation bar with a logo, a search icon, account information, a shopping basket icon, and language selection (EN). A message banner at the top states: "The server has been restarted: Your previous hacking progress has been restored automatically." Below it, two green success messages appear: "You successfully solved a challenge: Error Handling (Provoked an error that is neither very gracefully nor consistently handled.)" and "You successfully solved a challenge: Score Board (Find the carefully hidden 'Score Board' page.)". The main content area is titled "All Products" and displays five items in cards:

- Apple Juice (1000ml)** - Price: 1.99
- Apple Pomace** - Price: 0.89
- Banana Juice (1000ml)** - Price: 1.99
- Carrot Juice (1000ml)** - Price: 2.99

OPEN CHAT

Hacking Instructor

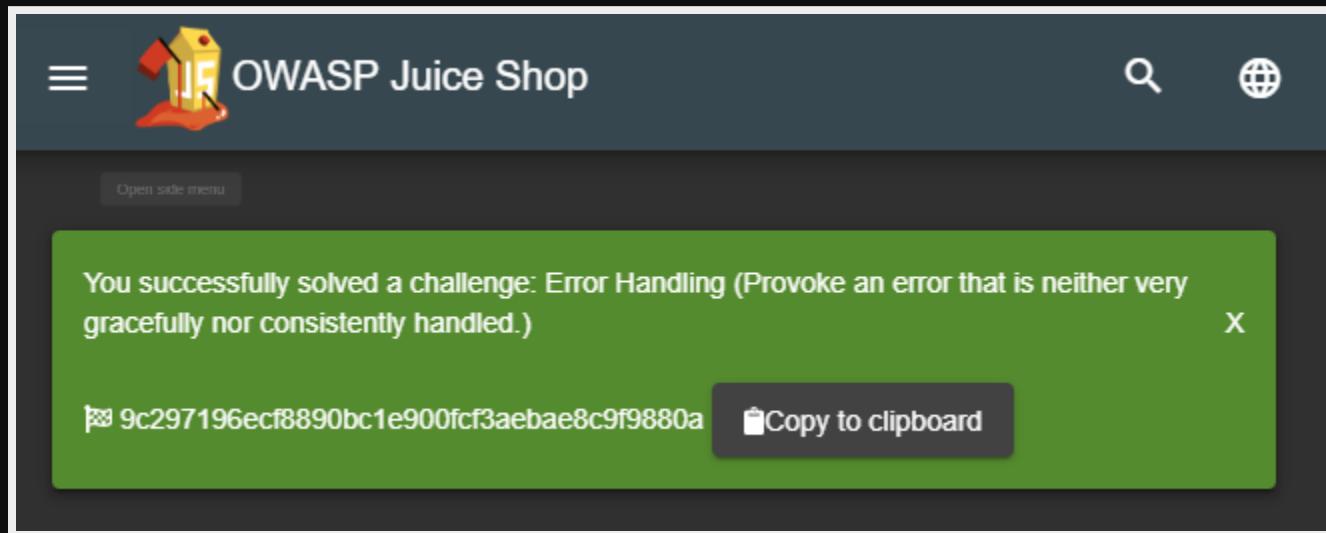
Some challenges come with an embedded interactive tutorial



OPEN CHAT

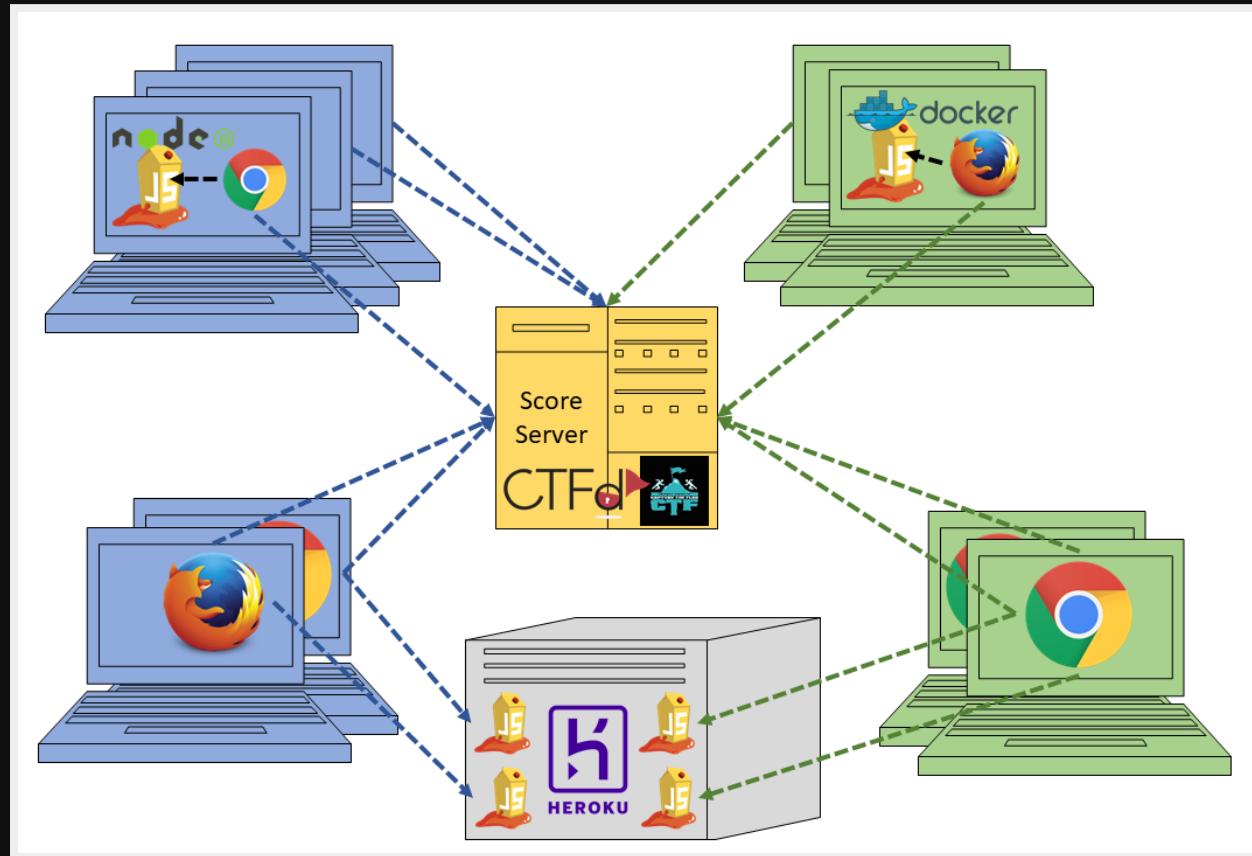
Juice Shop is CTF-ready

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 7.x

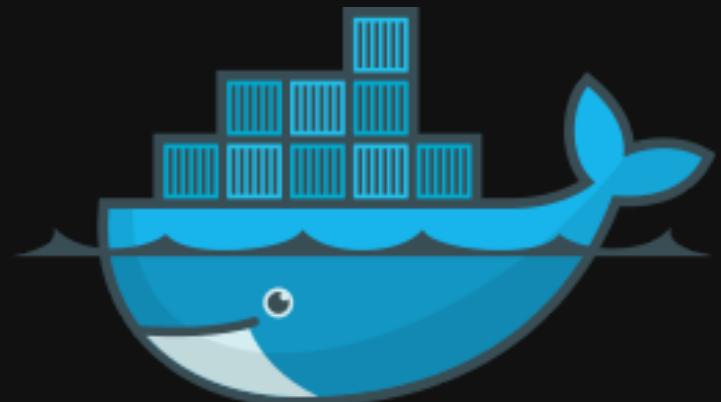
Utility project to help you host a hacking event on CTFd, FBCTF or RootTheBox



OPEN CHAT

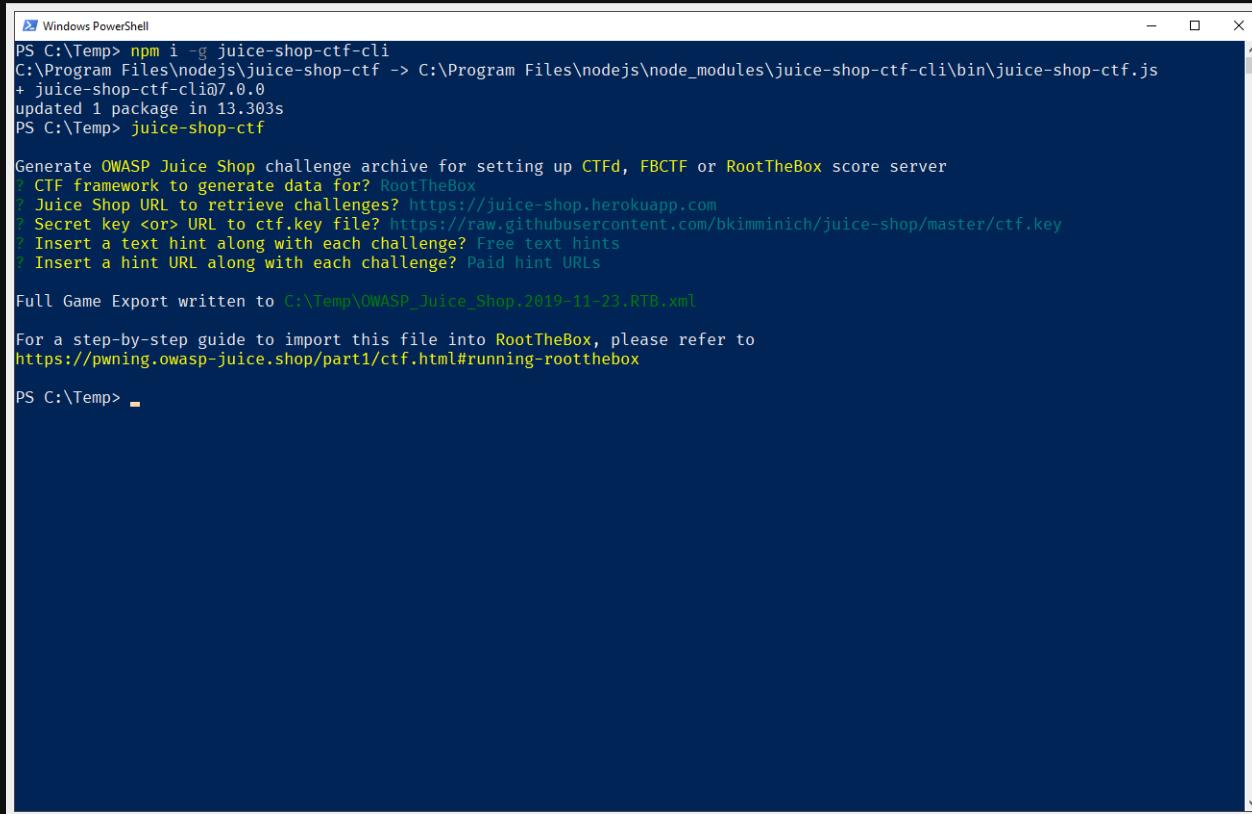
Simple Installation

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-dump to conveniently import into CTFd, FBCTF or RootTheBox



```
PS C:\Temp> npm i -g juice-shop-ctf-cli
C:\Program Files\nodejs\juice-shop-ctf -> C:\Program Files\nodejs\node_modules\juice-shop-ctf-cli\bin\juice-shop-ctf.js
+ juice-shop-ctf-cli@7.0.9
updated 1 package in 13.303s
PS C:\Temp> juice-shop-ctf

Generate OWASP Juice Shop challenge archive for setting up CTFd, FBCTF or RootTheBox score server
? CTF framework to generate data for? RootTheBox
? 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

Full Game Export written to C:\Temp\OWASP_Juice_Shop.2019-11-23.RTB.xml

For a step-by-step guide to import this file into RootTheBox, please refer to
https://pwning.owasp-juice.shop/part1/ctf.html#running-rootthebox

PS C:\Temp> -
```

OPEN CHAT

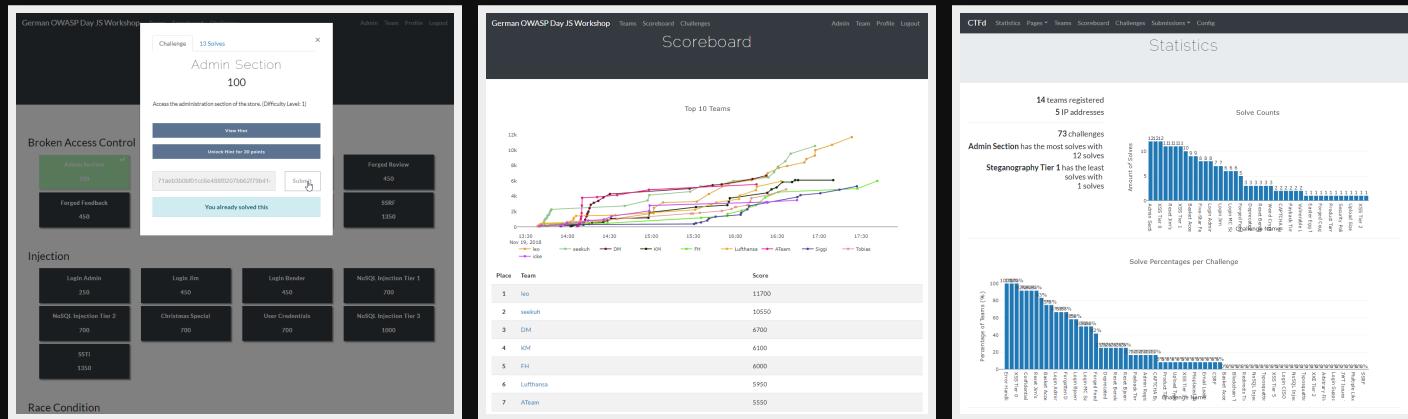
Configuration File Option

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

```
ctfFramework: CTFd | FBCTF | RootTheBox
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/
insertHints: none | free | paid
insertHintUrls: none | free | paid
```

Screenshots from CTF games

Your CTF score server instance will be ready-to-play in <5min



OPEN CHAT

MultiJuicer Platform 3.x

3rd party project to run separate Juice Shop instances for training or CTF participants on a central Kubernetes cluster



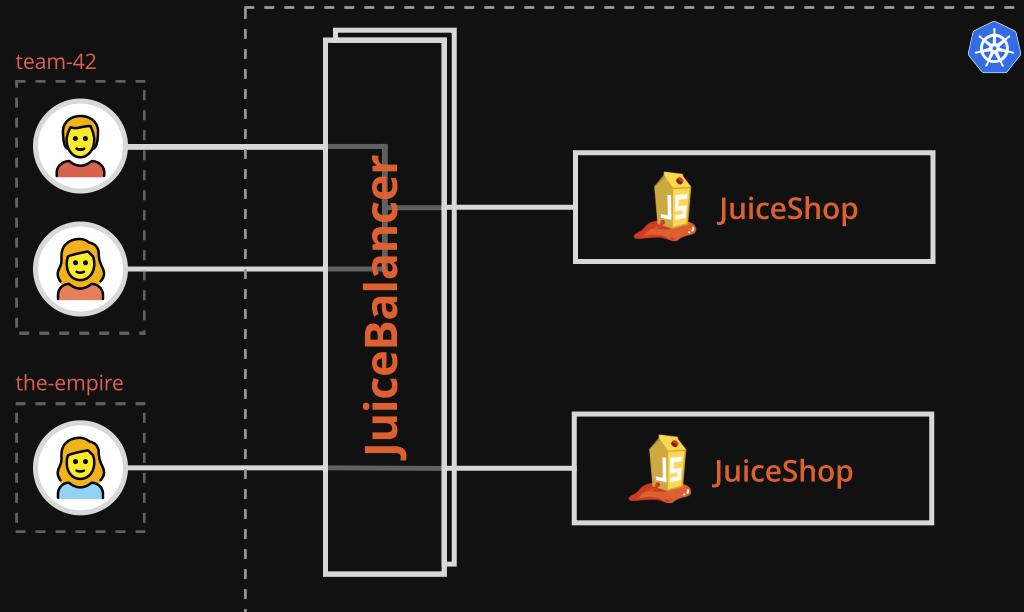
MultiJuicer

Multi User Plattform for OWASP Juice Shop

OPEN CHAT

Custom JuiceBalancer

Restricts number of users to team members and protects against illicit cross-team instance access



Re-branding

Fully customizable business context and look & feel

The screenshot shows a rebranded e-commerce website with a dark orange header. The header includes a menu icon, the text "Mozilla CTF" with the Firefox logo, a search icon, "Account", "Your Basket", and a language switcher set to "EN". Below the header is a grid of nine product cards labeled "All Products". Each card contains an image, the product name, price, and an "Add to Basket" button.

All Products	
1.25 inch Firefox Button, 25 pack 7	3 inch round Firefox sticker, individual 0.11
Beanie 5.5	Black cap w/tote 17.75
Champion Sweatshirt with a Drawstring Tote 68.89	Drawstring tote 5.5
Firefox tattoo, 50 pack 4	Fox Plush 8.6

A cookie consent banner at the bottom right states: "This website uses a myriad of 3rd-party cookies for your convenience and tracking pleasure. How can I turn this off?". It has "Accept" and "Never mind!" buttons.

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_js.ico
  theme: bluegrey-lightgreen
  showVersionNumber: true
  showGitHubLinks: true
  numberofRandomFakeUsers: 0
  altcoinName: Juicycoin
  privacyContactEmail: donotreply@owasp-juice.shop
  customMetricsPrefix: juiceshop
  social:
    twitterUrl: 'https://twitter.com/owasp_juiceshop'
    facebookUrl: 'https://www.facebook.com/owasp.juiceshop'
    [...]
[...]
```

Choose your own inventory

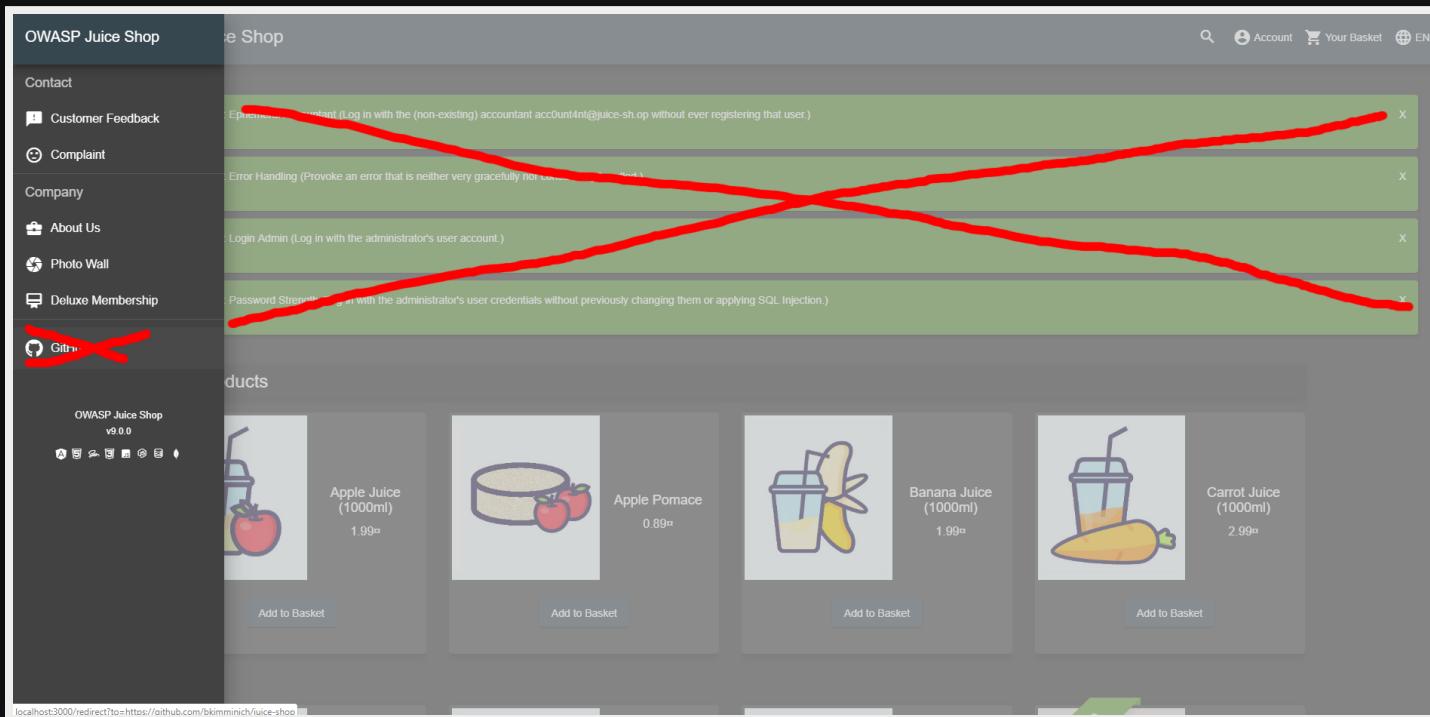
The YAML configuration allows you to override all products

```
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!

Quiet Mode

Hide origin & notifications for 0% distraction in awareness trainings

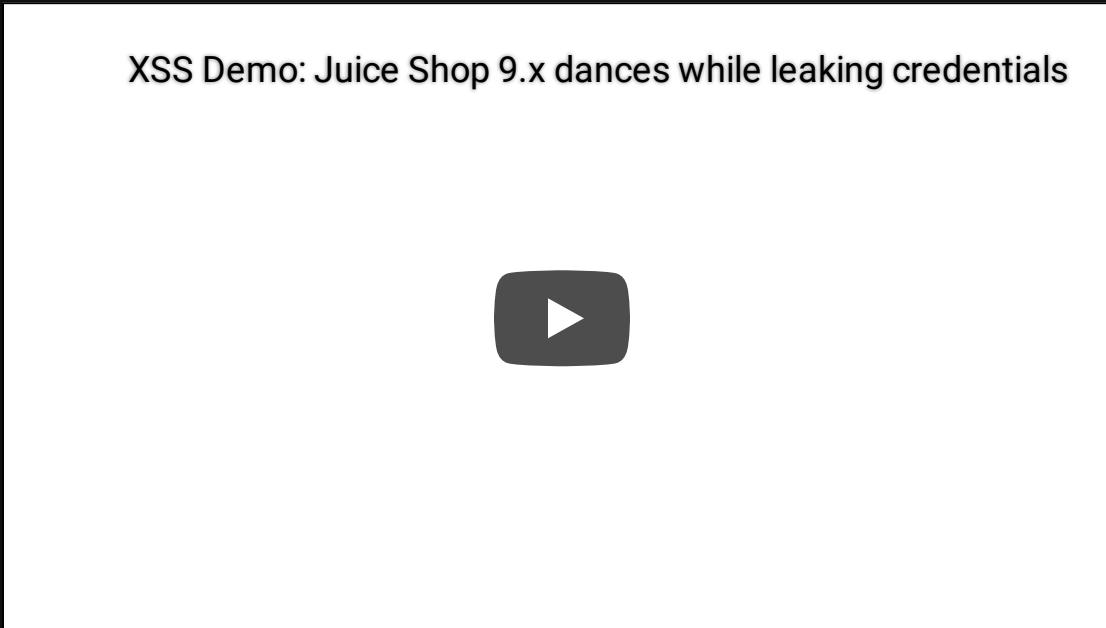


Simply start application with `NODE_ENV=quiet` environment variable defined!

OPEN CHAT

XSS/CSP Awareness Demo

Utility project to show the dangers of XSS holes combined with bad Content Security Policy using *Harlem Shake* and a Keylogger



Sophisticated Phishing Mail

*Dear valued {firstname} {lastname}, **you won** our big lottery which you might not even remembering to have participating in! Click on the following totall inconspicuous link to claim your prize now!*

CLICK HER NOW! FREE STUFF! YOU WON!

Sincerely yours, Bjorn Kimminich

(CEO/CIO/CISO/CISXP/CFM/SVP Marketing @ Juice Shop Inc.)

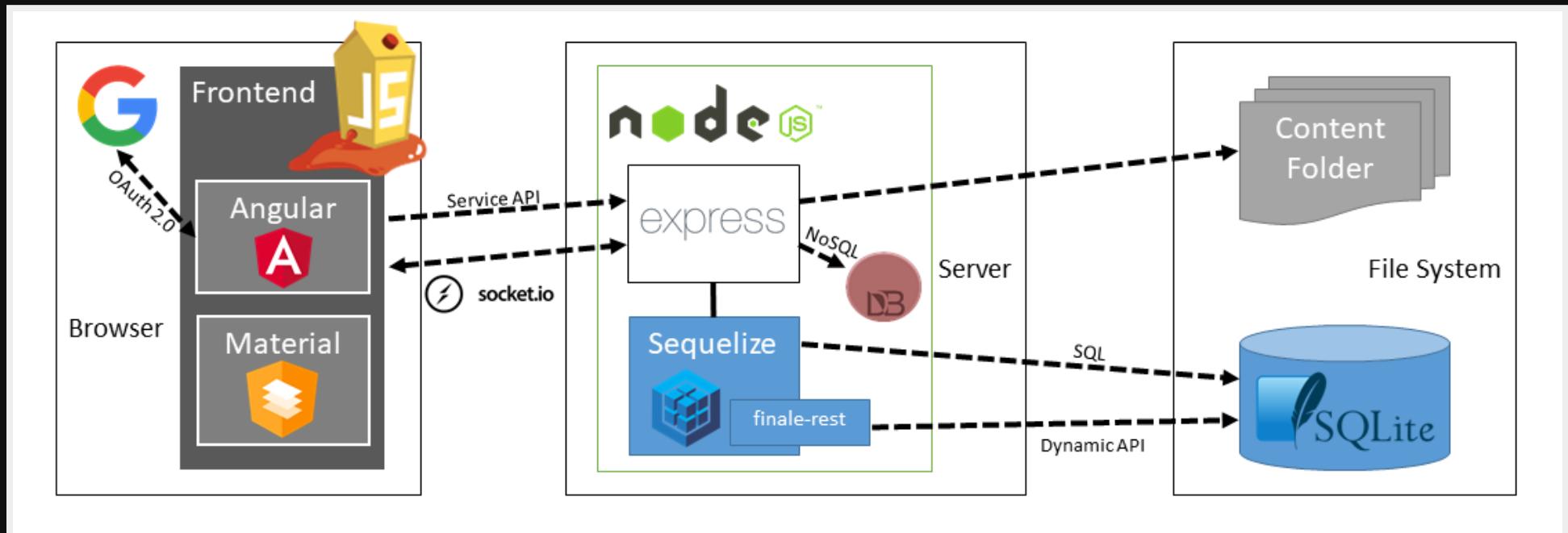
Juice Shop Inc. is registered as a bla bla bla bla yadda yadda lorem ipsum lirum larum lorum latido latido latidoooooooo and even more very assuring legal bla blubb. All logos and icons of which none is even in this lousy attempt of a phishing mail are registered trademarks of Juice Shop Inc. and finally we are throwing in an outdated Copyright (c) 2018 Juice Shop Inc.

Do you dare to click the link above? (Requires *shake-logger* to run locally!)

OPEN CHAT

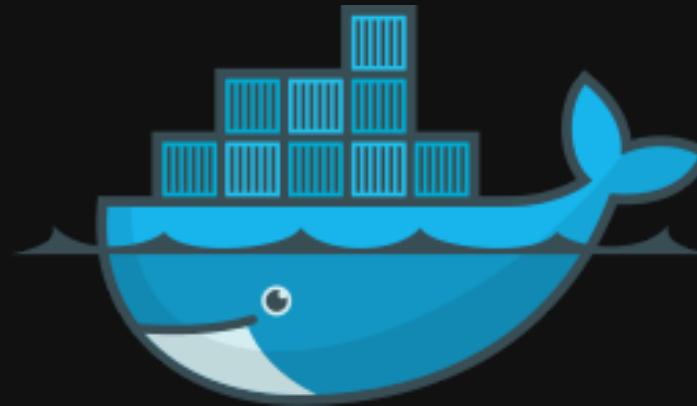
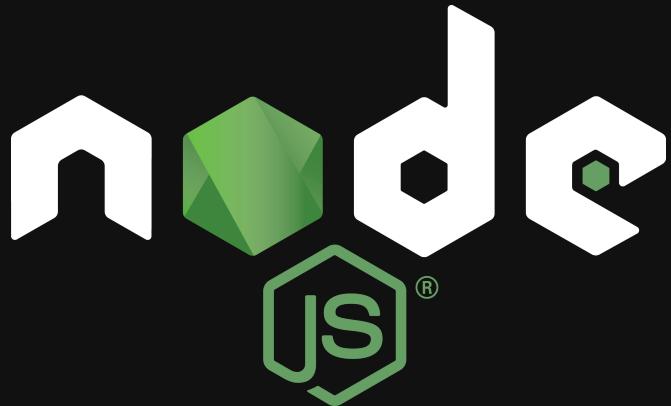
Modern Web-Architecture

JavaScript/TypeScript all the way from UI to REST API



Simple Installation

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



OPEN CHAT

Multi-language support

Crowd-sourced UI translations for 30+ languages



OPEN CHAT

I18N of Products & Challenges

Crowd-sourced translations available from v9.1.0 onward



OPEN CHAT

Test Pyramid

Maximizing Test Automation & Code Coverage



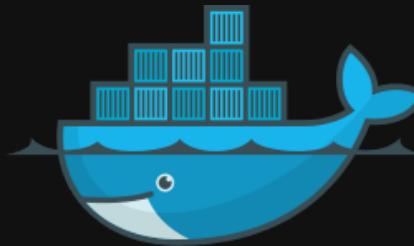
frisby.js 



OPEN CHAT

DevOps Pyramid

Automated Build, CI/CD & Code Analysis



OPEN CHAT

FAQ

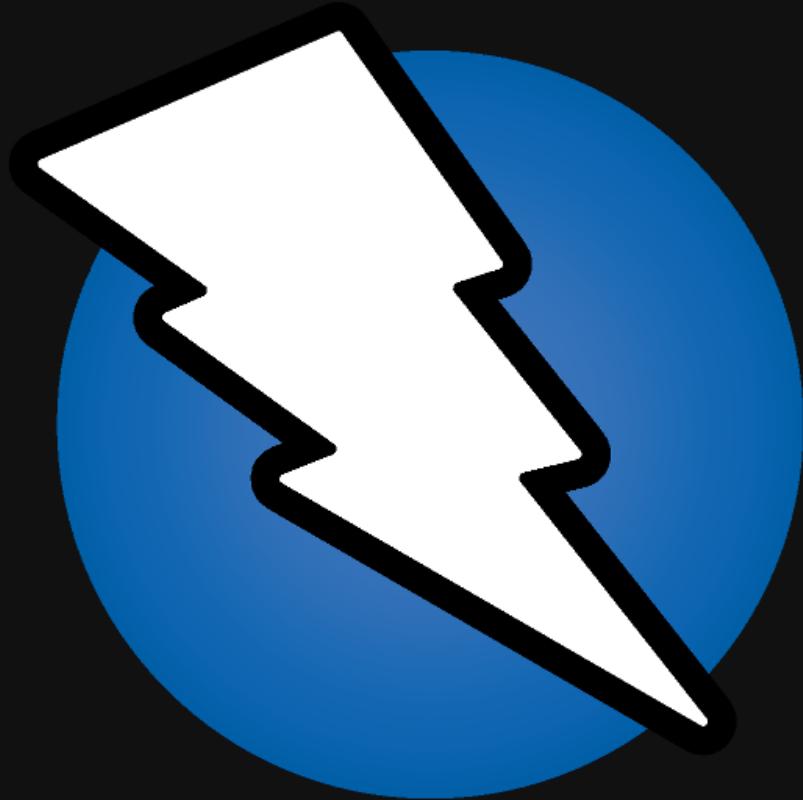
- Can I use my Pentesting toys?
- Can I do a white box pentest?
- Can I use the internet?
- Installation does not work!
- What if I crash the server?
- I'm stuck with a challenge!
- I found another vulnerability!
- Why are some challenges disabled?
- Can I contribute to the project?
- Is there a contribution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

If FAQ & README don't help, ask for help in the chat. Please refrain from using GitHub issues for support requests.

OPEN CHAT

Can I use my Pentesting toys?

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

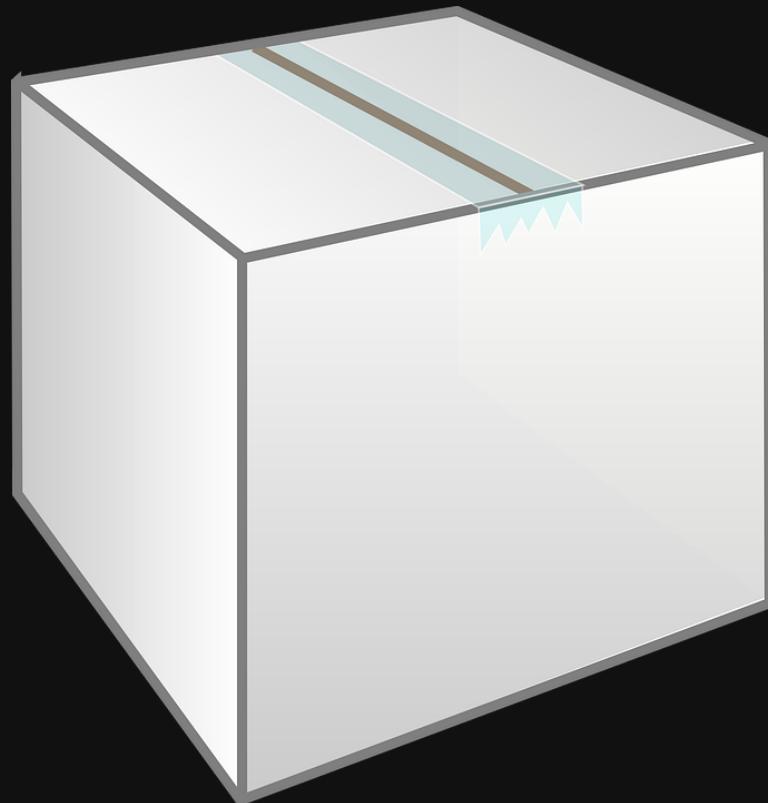


Proxies like OWASP ZAP or BurpSuite Free Edition can definitely be useful. Automatic tools like Arachni or Nikto might find some vulnerabilities but will obviously not be able to get the Score Board to 100% for you.

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

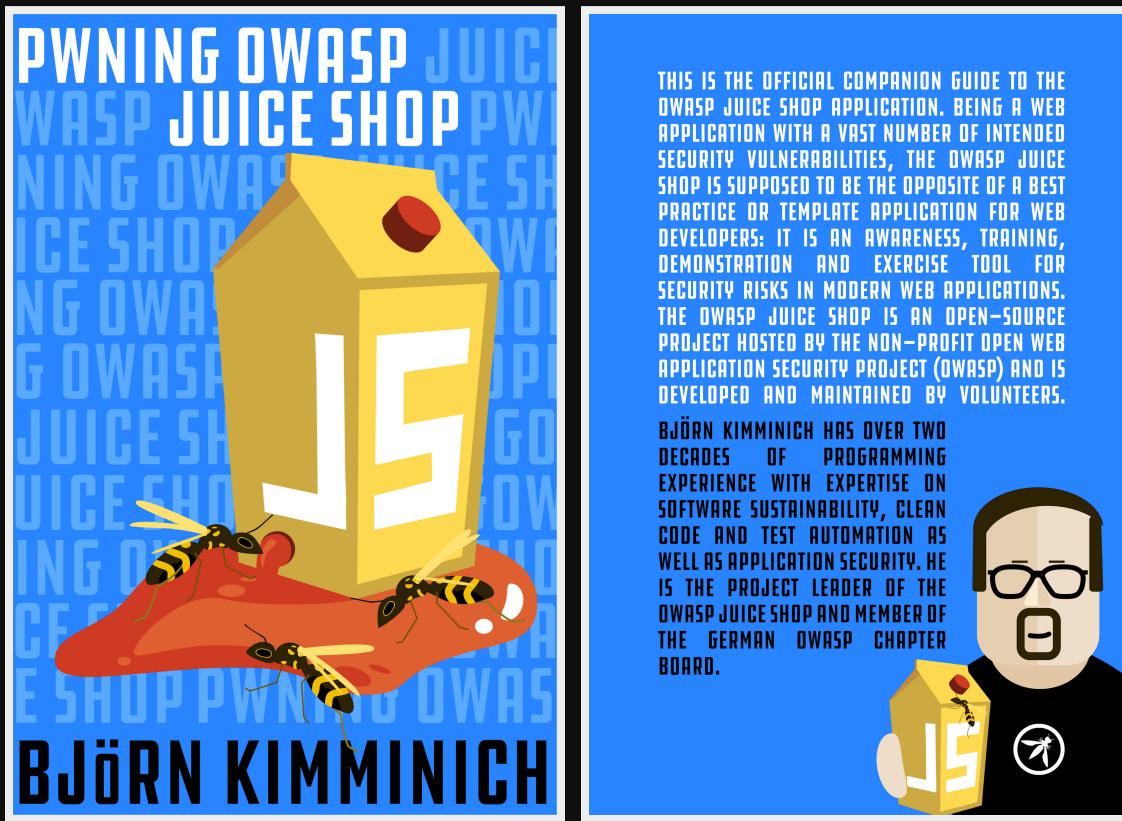


Your Score Board progress is **saved automatically** and will restore after server restart!

OPEN CHAT

I'm stuck with a challenge!

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



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**. 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, Deserialization and some NoSQLi challenges (as they could have unforeseeable side effects on the hosting platform).

Can I contribute to the project?

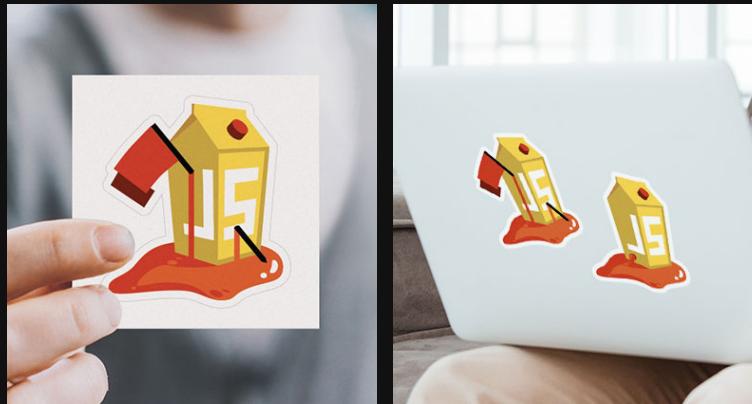
Of course! Visit our backlog on GitHub & translations on Crowdin



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 58

owasp flagship project

code style standard cii best practices gold

↗ maintainability A ↗ test coverage 86%

GitHub ★ 2.9k

downloads 28k

docker pulls 4M

sourceforge downloads 9.3k

OPEN CHAT

Project Roadmap

- Challenges in the pristine features added during GSoC 2019
- Receive amazing proposals from students for GSoC 2020
- Apply pressure to Brian to get the full Juice Shop jingle done



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

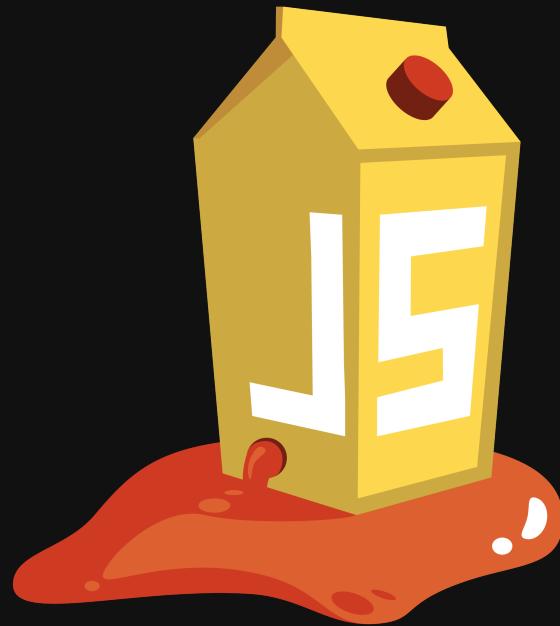
IT Security Lecture (CC-BY-SA)

<https://github.com/bkimminich/it-security-lecture>

Web Application Security in a Nutshell (CC-BY-SA)

<http://webappsec-nutshell.kimminich.de>

OPEN CHAT



Copyright (c) 2014-2020 Björn Kimminich

Licensed under the **MIT** license.

Created with reveal.js - The HTML Presentation Framework

OPEN CHAT