

ADDO[®]

ALL DAY DEVOPS

NOVEMBER 6, 2019

Björn Kimminich

OWASP Juice Shop

The Ultimate
All Vuln WebApp



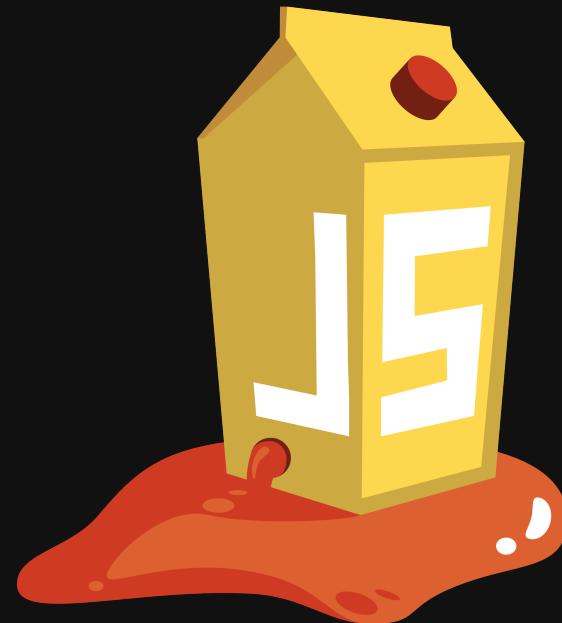


Let us begin with a
happy path
shopping tour

like unsuspecting average Joe & Jane!

Wow, that was a perfectly fine shopping experience! No noteworthy errors, everything shiny & working as it should!

**OWASP Juice Shop is looking forward to
see you soon as a happy customer!**



<https://owasp-juice.shop>



That's it, thanks for watching!?!?



Let's take a look behind the curtain and explore why OWASP Juice Shop claims to be "**probably the most modern and sophisticated insecure web application!**"

Why "Juice Shop"?!?

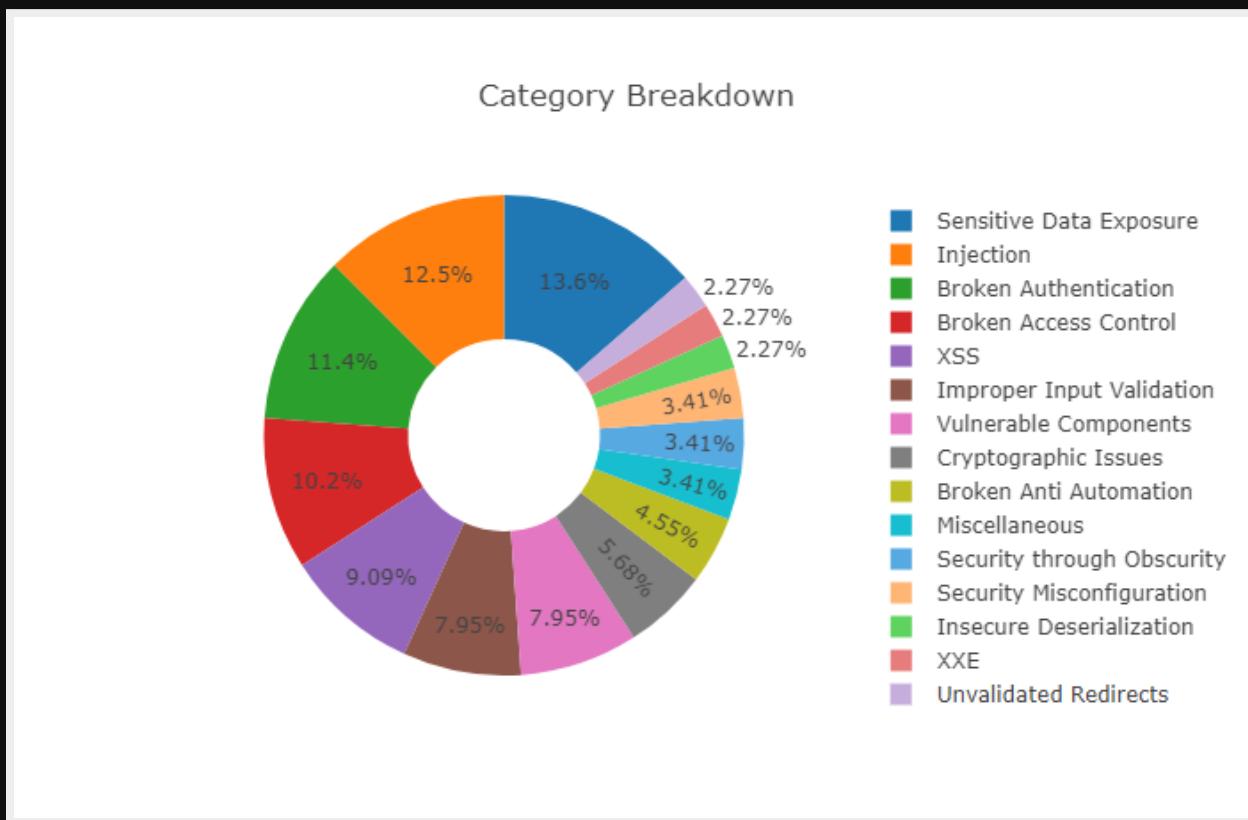
Translating "dump" or "useless outfit" into German yields "Saftladen" which is a compound word from "Saft" and "Laden". This reverse-translates into "juice" and "shop". Hence the project name.



That the initials "JS" match with those of "JavaScript" was purely coincidental!

88+ 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

There's something to do for beginners and veterans alike



Score Board

Challenge progress is tracked on server-side

The screenshot shows the OWASP Juice Shop application's Score Board page. At the top, there is a navigation bar with a logo, the text "OWASP Juice Shop", a search icon, an account icon, a basket icon labeled "Your Basket", and a language switcher set to "EN". Below the navigation bar, the title "Score Board 2%" is displayed. Underneath the title, there is a row of six challenge cards, each with a star icon and a number from 1 to 6 followed by a slash and a number representing the current score. To the right of these cards are two buttons: "Show all" and "Show solved". Below the cards is a horizontal menu bar with categories: 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, XXE, and a "Hide all" button. The main content area displays a table of challenges:

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 graduation cap
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

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 a logo, a search icon, account information, a shopping cart 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". It 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 image of the product, a "Click for more information" link, and an "Add to Basket" button.

Product	Description	Price
Apple Juice (1000ml)	1.99	
Apple Pomace	0.89	
Banana Juice (1000ml)	1.99	
Carrot Juice (1000ml)	2.99	

Restore your Progress

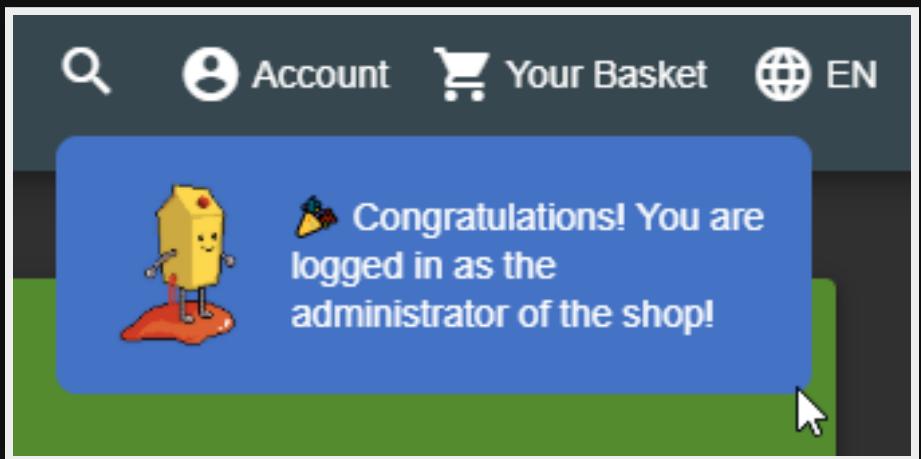
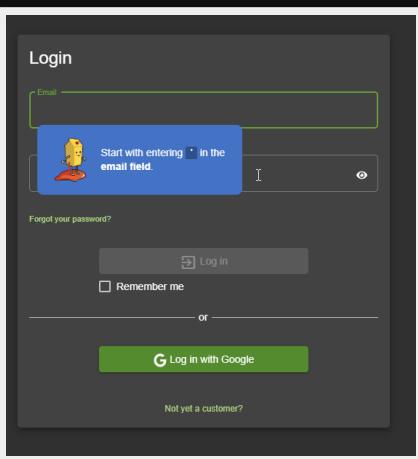
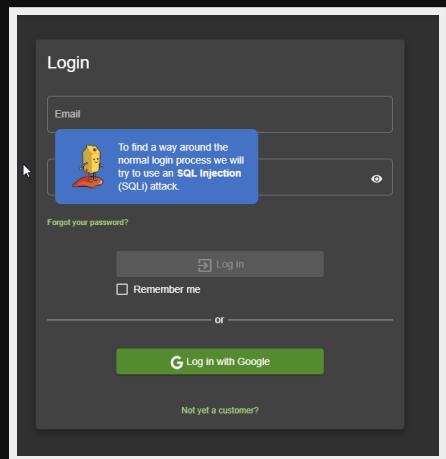
Auto-saves your hacking progress and restores on server restart

The screenshot shows the OWASP Juice Shop interface. At the top, there is a navigation bar with the logo, "OWASP Juice Shop", a search icon, "Account", "Your Basket", and language selection ("EN"). A message banner at the top states: "The server has been restarted: Your previous hacking progress has been restored automatically." with a button to "Delete cookie to clear hacking progress". Below this, two green success messages are displayed: "You successfully solved a challenge: Error Handling (Provoke 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 lists five items:

Image	Name	Description	Price
	Apple Juice (1000ml)		1.99
	Apple Pomace		0.89
	Banana Juice (1000ml)		1.99
	Carrot Juice (1000ml)		2.99

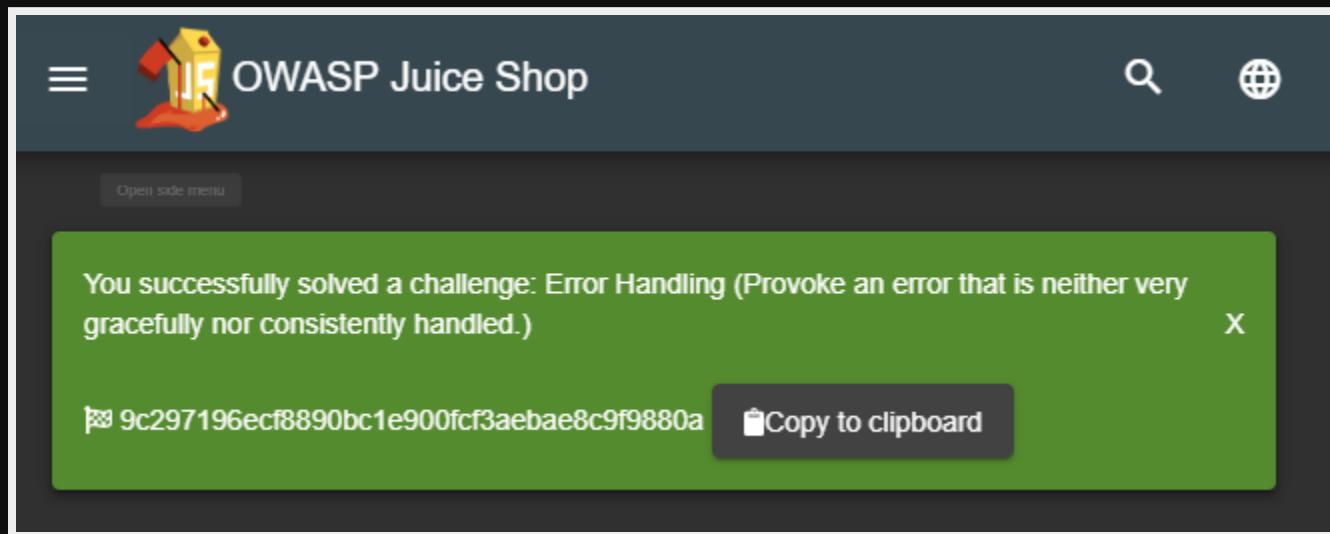
Hacking Instructor (¶)

Some challenges come with an embedded interactive tutorial



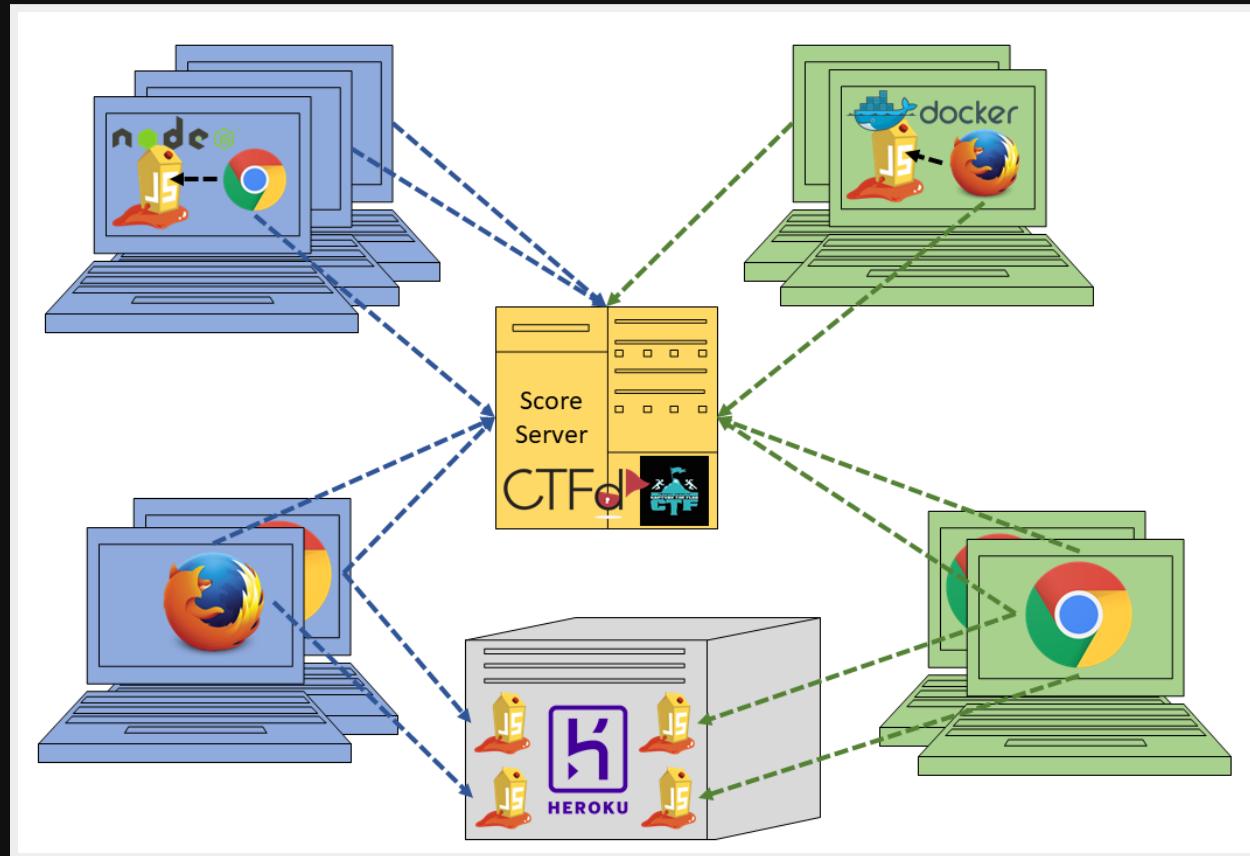
Juice Shop is CTF-ready

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.



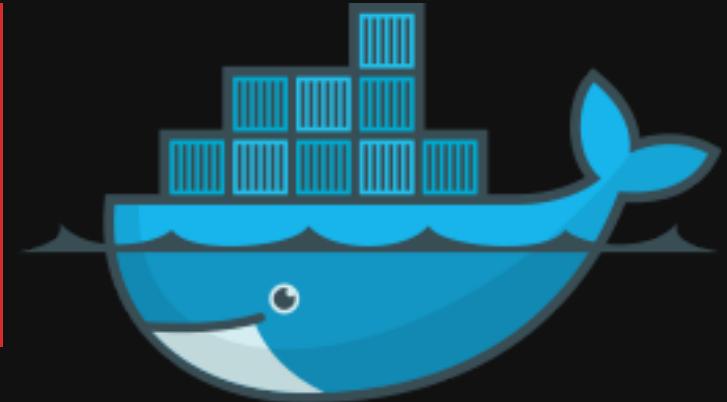
CTF Extension 6.x

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

```
root@2268d9451e23:/# juice-shop-ctf

Generate OWASP Juice Shop challenge archive for setting up CTFd 1.x, CTFd 2.x or FBCTF score server
? CTF framework to generate data for? CTFd 2.x
? Juice Shop URL to retrieve challenges? https://juice-shop.herokuapp.com
? Secret key <or> URL to ctf.key file? https://raw.githubusercontent.com/bkrimminich/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 /OWASP_Juice_Shop.2019-05-08.CTFd2.zip

You can dismiss the potential Internal Server Error alert popup after import.
Simply restart CTFd and set up CTF name and administrator credentials again.

For a step-by-step guide to import the ZIP-archive into CTFd 2.x, please refer to
https://bkrimminich.gitbooks.io/pwning-owasp-juice-shop/content/part1/ctf.html#running-ctfd
root@2268d9451e23:/#
```



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

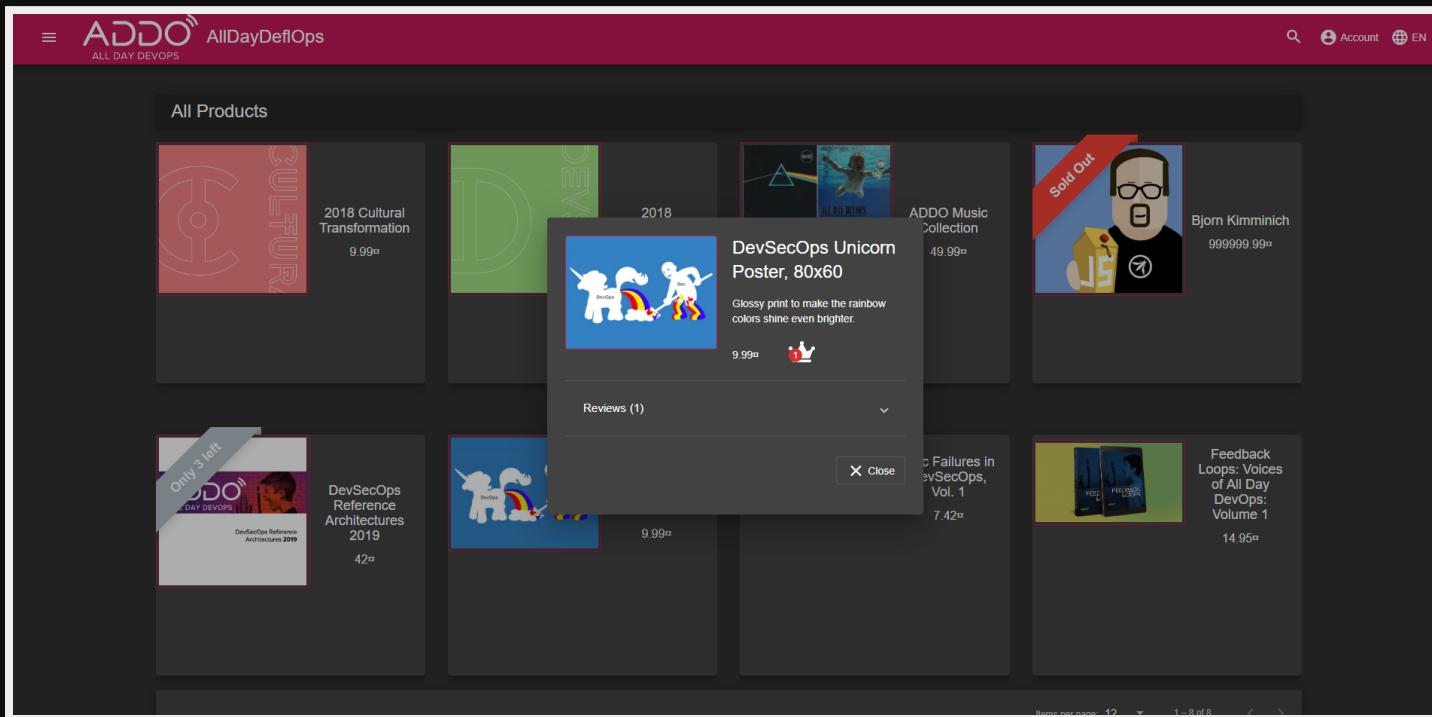
13:30 14:00 14:30 15:00 15:30 16:00 16:30 17:00 17:30
Nov 19, 2018

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

Re-branding

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



Configurative Customization

Customize the application via a simple YAML file

```
application:  
  domain: ad.do  
  name: 'AllDayDeflOps'  
  logo: 'https://www.alldaydevops.com/ [...] /2019%20Logo%20Files/ADDO_Logo_2019_White.svg'  
  favicon: 'https://www.sonatype.com/hubfs/ADDO-2018/ADDO_fav4.png'  
  theme: pink-bluegrey  
  showGitHubLinks: false  
  twitterUrl: 'https://twitter.com/AllDayDevOps'  
  facebookUrl: 'https://www.facebook.com/AllDayDevOps/'  
  [...]
```

Choose your own inventory

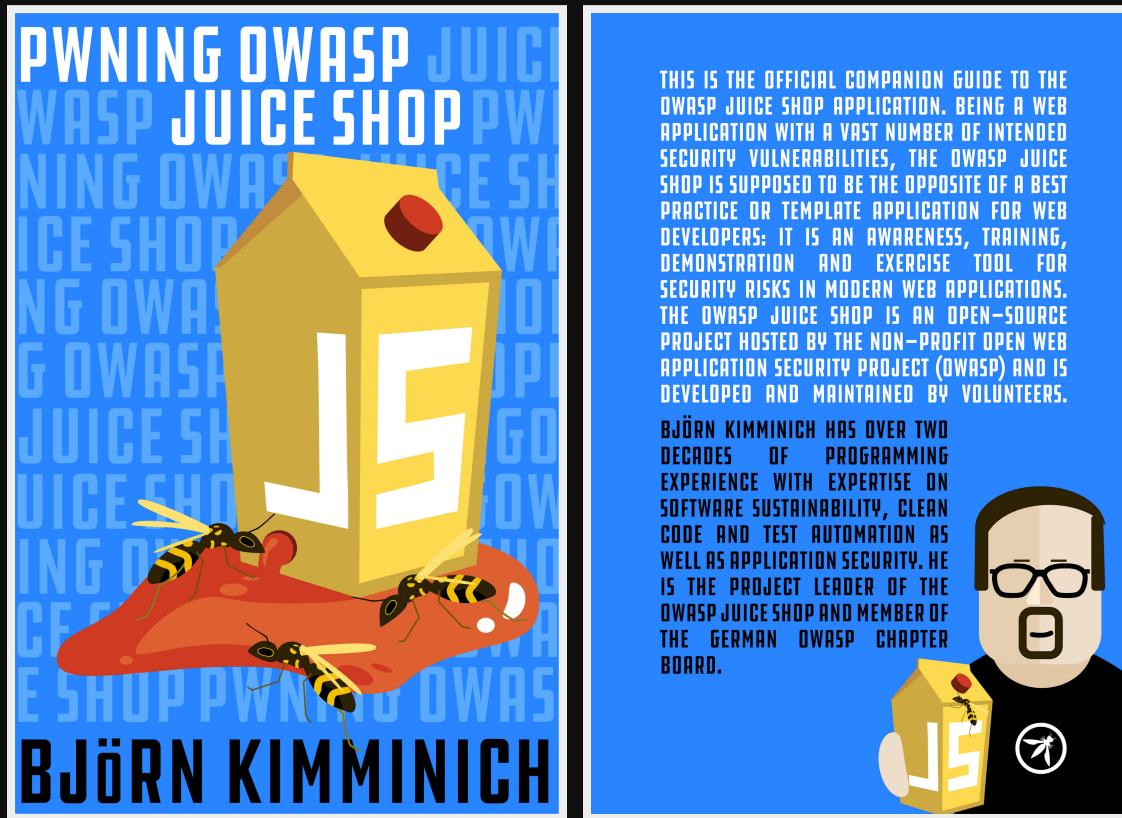
The YAML configuration allows you to override all products

```
products:  
  [...]  
  - name: 'DevSecOps Reference Architectures 2019'  
    description: 'Gloriously referential! Whitepaperesquely architectural!'  
    price: 42.00  
    quantity: 3  
    image: 'https://www.alldaydevops.com/hubfs/2019-ADDO/.../Untitled%20design%20(3).  
    urlForProductTamperingChallenge: 'http://bit.ly/2YIjdt7'  
  - name: 'DevSecOps Reference Architectures 2018'  
    description: 'Very referential! Mildly architectural!'  
    price: 21.00  
    image: undefined.jpg  
    useForChristmasSpecialChallenge: true  
  [...]
```

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

Free Companion Guide

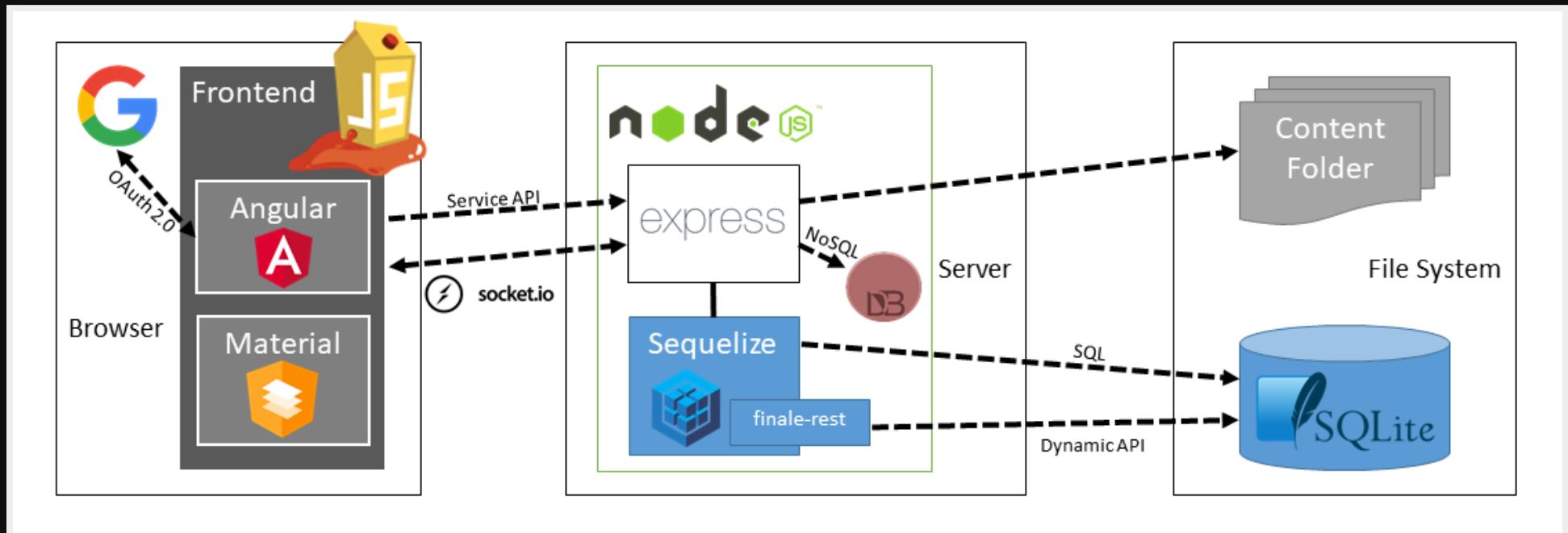
Contains all the setup documentation, hints & step-by-step solutions per challenge, contribution guidelines, trainers guide and more!



The eBook is available **for free** on Leanpub but also be **read online**.

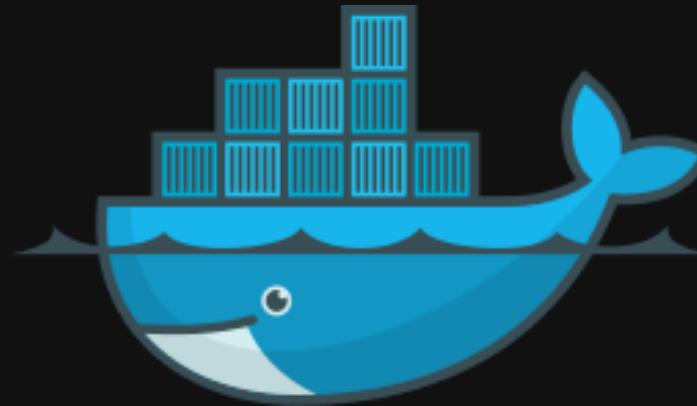
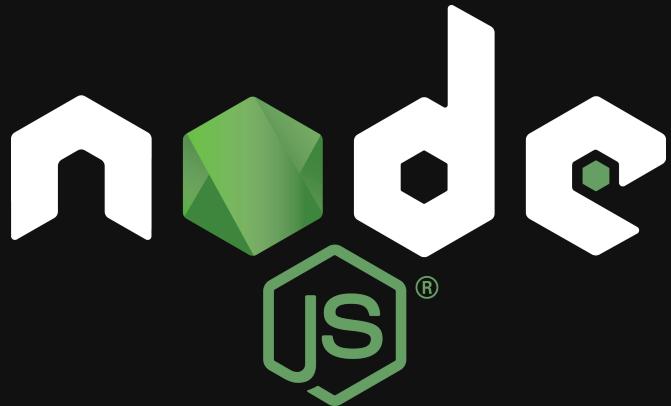
Modern Web-Architecture

JavaScript/TypeScript all the way from UI to REST API



Simple Installation

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



Test Pyramid

Maximizing Test Automation & Code Coverage

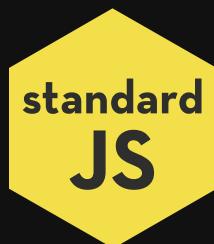
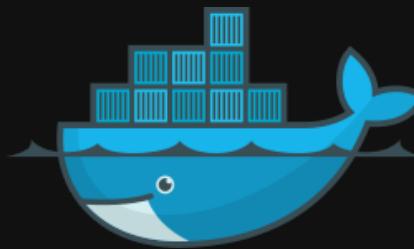


frisby.js 



DevOps Pyramid

Automated Build, CI/CD & Code Analysis



Juice Shop Success Pyramid™

Some amazing facts & stats about the project

contributors 57

owasp flagship project

code style standard cii best practices silver

↗ maintainability A

↗ test coverage 85%

pages 257

GitHub ★ 2.5k

downloads 23k

docker pulls 3.9M

sourceforge downloads 7.1k

sold 6561

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)

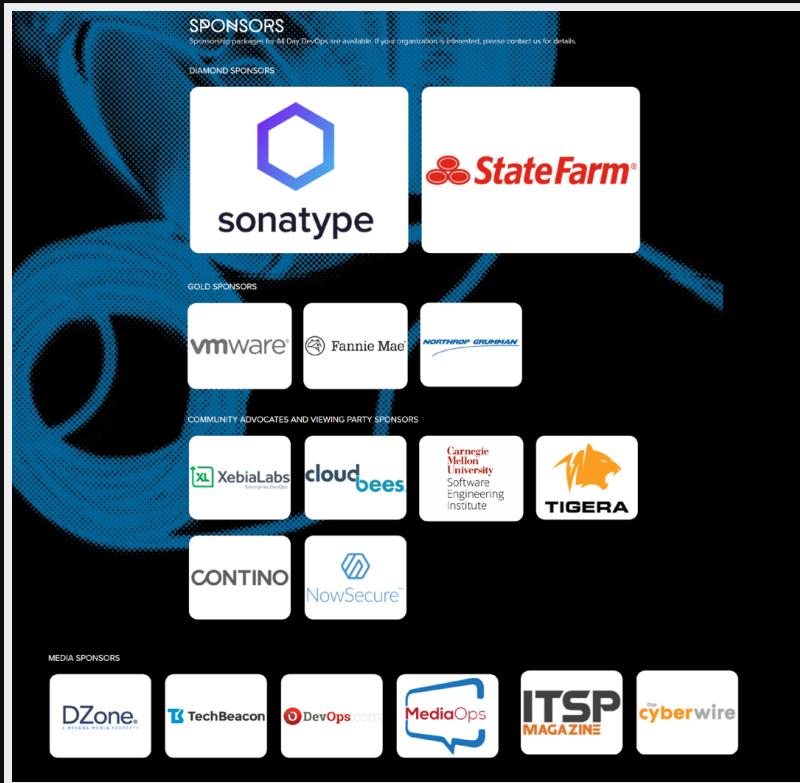
<https://github.com/bkimminich/it-security-lecture>

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

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



That's it, thanks for watching!



Copyright (c) 2014-2019 Björn Kimminich