

# OWASP Juice Shop

## 10TH ANNIVERSARY: Is it still fresh?

<https://owasp-juice.shop>

Copyright (c) 2014-2024 Björn Kimminich | @bkimminich | infosec.exchange/@bkimminich

@jannik@infosec.exchange

# OWASP Juice Shop

10TH ANNIVERSARY: Is it still fresh?

<https://owasp-juice.shop>

Copyright (c) 2014-2024 Björn Kimminich | @bkimminich | infosec.exchange/@bkimminich

@jannik@infosec.exchange

# The Idea



# 2008: Altoro Mutual

Stars 233

**AltoroMutual**

[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search  Go

**ONLINE BANKING LOGIN**

**PERSONAL**

- [Deposit Product](#)
- [Checking](#)
- [Loan Products](#)
- [Cards](#)
- [Investments & Insurance](#)
- [Other Services](#)

**SMALL BUSINESS**

- [Deposit Products](#)
- [Lending Services](#)
- [Cards](#)
- [Insurance](#)
- [Retirement](#)
- [Other Services](#)

**INSIDE ALTORO MUTUAL**

- [About Us](#)
- [Contact Us](#)
- [Locations](#)
- [Investor Relations](#)
- [Press Room](#)
- [Careers](#)
- [Subscribe](#)

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2023 Altoro Mutual, Inc.

**PERSONAL**

**Online Banking with FREE Online Bill Pay**  
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.



**Real Estate Financing**  
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it

**SMALL BUSINESS**

**Business Credit Cards**  
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.



**Retirement Solutions**  
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

**INSIDE ALTORO MUTUAL**

**Privacy and Security**  
The 2000 employees of Altoro Mutual are dedicated to protecting your [privacy](#) and [security](#). We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.



**DEMO SITE ONLY**

**This web application is open source!** Get your copy from [GitHub](#) and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SWI10>.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

Server-side rendered demo app for a commercial vulnerability scanner

# 2010: Bodgelt Store

Stars 263

The screenshot shows a web application interface. At the top, a light blue header bar contains the title "The Bodgelt Store". Below it, a message reads "We bodge it, so you dont have to!" and a "Guest user" link. A navigation menu with links for Home, About Us, Contact Us, Login, Your Basket, and Search is visible. On the left, a sidebar menu lists categories: Doodahs, Gizmos, Thingamajigs, Thingies, Whatchamacallits, Whatsits, and Widgets. The main content area features a section titled "Our Best Deals!" with a table displaying ten products. The table has columns for Product, Type, and Price.

Product	Type	Price
<a href="#">Thingie 2</a>	Thingies	\$3.20
<a href="#">GZ ZX3</a>	Gizmos	\$3.81
<a href="#">Thingie 2</a>	Thingies	\$3.20
<a href="#">Thingie 5</a>	Thingies	\$3.70
<a href="#">Thingie 4</a>	Thingies	\$3.50
<a href="#">Thingie 4</a>	Thingies	\$3.50
<a href="#">TGJ CCC</a>	Thingamajigs	\$0.70
<a href="#">TGJ JJJ</a>	Thingamajigs	\$0.80
<a href="#">Whatsit taste like</a>	Whatsits	\$3.96
<a href="#">TGJ EFF</a>	Thingamajigs	\$3.00

Server-side rendered demo app for the open source vulnerability scanner Zed Attack Proxy

# OWASP WebGoat

Stars 7k

## (Honorable Mention)

The screenshot shows the OWASP WebGoat interface for the XXE lesson. The left sidebar contains a navigation menu with categories like Introduction, General, and various Axx vulnerabilities. The 'XXE' category is currently selected. The main content area is titled 'XXE' and 'Modern REST framework'. It includes a note about modern REST frameworks accepting unexpected data formats, which can lead to JSON endpoint vulnerabilities. Below this is a note about performing XML injection. A photo of a black and white cat sitting on a hanger is displayed, with the text 'HUMAN' above it and 'I REQUEST YOUR ASSISTANCE' below it. At the bottom, there's a comment input field and a 'Submit' button.

localhost:8080/WebGoat/welcome.mvc

Server-side rendered and lesson-based training application

# 2014: Juice Shop

The screenshot shows a web application interface for the OWASP Juice Shop. At the top, there is a navigation bar with links for 'Login', 'English', 'Search...', 'Contact Us', and 'About Us'. A GitHub link is also present on the right side of the header. Below the header, the title 'All Products' is displayed. A table lists various products with their descriptions and prices. The products listed are:

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.	0.89
Banana Juice (1000ml)	Monkeys love it the most.	1.99
Eggfruit Juice (500ml)	Now with even more exotic flavour.	8.99
Fruit Press	Fruits go in. Juice comes out. Pomace you can send back to us for recycling purposes.	89.99
Green Smoothie	Looks poisonous but is actually very good for your health! Made from green cabbage, spinach, kiwi and grass.	1.99
Lemon Juice (500ml)	Sour but full of vitamins.	2.99
OWASP Juice Shop Hoodie	Mr. Robot-style apparel. But in black. And with logo.	49.99
OWASP Juice Shop Mug	Black mug with logo on each side! Your colleagues will envy you!	21.99
OWASP Juice Shop T-shirt	You want to put one of these beauties on your laptop. You definitely want	2.99

Rich Internet Application (RIA) designed for realism, manual exploration and hacking w/ or w/o pentesting tools

# 2014: Juice Shop

Juice Shop v1.0.0      Login      Search      Submit      Contact Us      About Us

## All Products

Product	Description	Price	
Apple Juice (1000ml)	The all-time classic.	1.99	<input checked="" type="checkbox"/>
Orange Juice (1000ml)	Made from oranges hand-picked by Uncle Dittmeyer.	2.99	<input checked="" type="checkbox"/>
Eggfruit Juice (500ml)	Now with even more exotic flavour.	8.99	<input checked="" type="checkbox"/>
Raspberry Juice (1000ml)	Made from blended Raspberry Pi, water and sugar.	4.99	<input checked="" type="checkbox"/>
Lemon Juice (500ml)	Sour but full of vitamins.	2.99	<input checked="" type="checkbox"/>
Banana Juice (1000ml)	Monkeys love it the most.	1.99	<input checked="" type="checkbox"/>
Lemon Juice (500ml)	Sour but full of vitamins.	2.99	<input checked="" type="checkbox"/>
Juice Shop T-Shirt (3XL)	Real fans wear it 24/7!	24.99	<input checked="" type="checkbox"/>
OWASP SSL Advanced Forensic Tool (O-Saft)	O-Saft is an easy to use tool to show information about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations. <a href="#">More...</a>	0.01	<input checked="" type="checkbox"/>

Fork me on GitHub

Actually, THIS was the original look-and-feel

# 2014: Personal "Pet Project"

## Juice Shop

An intentionally insecure webapp suitable for pentesting and security awareness trainings written in Node, Express and Angular.

 Download .zip

 Download .tar.gz

 View on GitHub

## Juice Shop

An intentionally insecure webapp suitable for pentesting and security awareness trainings written in Node, Express and Angular. Inspired by the "classic" [Bodgelt Store](#) by [@psiilon](#).

Translating "dump" or "useless outfit" into German yields "Saftladen" which can be reverse-translated word by word into "juice shop". Hence the name of this project.

You may find it easier to find vulnerabilities using a pen test tool. I strongly recommend [Zed Attack Proxy](#) which is open source and very powerful, yet beginner friendly.

### Features

- Easy to install: Just requires [node.js](#)
- Self contained: Additional dependencies will be resolved and downloaded automatically
- No external DB: A simple file based SQLite database is used which is wiped and regenerated on server startup
- Open source: No hidden costs or caveats

# 2016: Juice Shop joins OWASP

This site is the archived OWASP Foundation Wiki and is no longer accepting Account Requests.  
To view the new OWASP Foundation website, please visit <https://owasp.org>

## OWASP Juice Shop Project

Revision as of 08:35, 9 May 2017 by Bjoern Kimminich (talk | contribs) (*Update logo with facelifted version*)  
(diff) ← Older revision | Latest revision (diff) | Newer revision → (diff)

Main Acknowledgements Road Map and Getting Involved

# INCUBATOR new projects

### OWASP Juice Shop Tool Project

*The most trustworthy online shop out there.* (dschadow)

OWASP Juice Shop is an intentionally insecure webapp for security trainings written entirely in Javascript which encompasses the entire OWASP Top Ten and other severe security flaws.

#### Description



Juice Shop is written in Node.js, Express and AngularJS. It was the first application written entirely in JavaScript listed in the OWASP VWA Directory. The application contains more than 30 challenges of varying difficulty where the user is supposed to exploit the underlying vulnerabilities. The hacking progress is tracked on a score board. Finding this score board is actually one of the (easy) challenges! Apart from the hacker and awareness training use case, pentesting proxies or security scanners can use Juice Shop as a "guinea pig"-application to check how well their tools cope with Javascript-heavy application frontends and REST APIs.

*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!*

#### Main Selling Points

- Easy-to-install: Choose between node.js, Docker and Vagrant to run on Windows/Mac/Linux
- Self-contained: Additional dependencies are pre-packaged or will be resolved and downloaded automatically

**Donate**  


#### News

[29.04.17] juice-shop v3.0.1  
[21.04.17] juice-shop-ctf v1.0.1  
[20.04.17] juice-shop v2.26.0  
[01.04.17] juice-shop v2.25.0  
[22.02.17] juice-shop-ctf v0.3.1

#### Installation

Packaged Distributions  
Docker Image  
Online Demo (Heroku)

# 2018: Promoted to Flagship

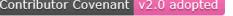
Please support the OWASP mission to improve software security through open source initiatives and community education. [Donate Now!](#) 

 [PROJECTS](#) [CHAPTERS](#) [EVENTS](#) [ABOUT](#)  [Member Login](#) [Store](#) [Donate](#) [Join](#)

## OWASP Juice Shop

[Main](#) [Overview](#) [News](#) [Challenges](#) [Learning](#) [CTF](#) [Ecosystem](#) [Supporters](#)

  
owasp   GitHub  8.6k 

CII Best Practices 

OWASP Juice Shop is probably the most modern and sophisticated insecure web application! It can be used in security trainings, awareness demos, CTFs and as a guinea pig for security tools! Juice Shop encompasses vulnerabilities from the entire [OWASP Top Ten](#) along with many other security flaws found in real-world applications!



### Description

Juice Shop is written in Node.js, Express and Angular. It was the first application written entirely in JavaScript listed in the [OWASP VWA Directory](#).

The application contains a vast number of hacking challenges of varying difficulty where the user is supposed to exploit the

**The OWASP® Foundation** works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

### Project Information

 **Flagship Project**

**Classification**

 **Tool**

**Audience**

 **Builder**  
 **Breaker**  
 **Defender**

**Installation**

**From Source**  
Packaged ([GitHub/SourceForge](#))  
[Docker Image](#)

**Sources**

[GitHub](#)  
[CTF Extension \(GitHub\)](#)

# The Challenges

19

# 2014: 23 Hacking Challenges

A screenshot of a GitHub commit page. The commit details are as follows:

- Date: Oct 21, 2014
- Author: bkimminich (represented by a profile icon)
- Commit message: Feature-complete version
- Branch: v0.3.0
- Commit ID: 25c40fb
- Compare link: Compare ▾

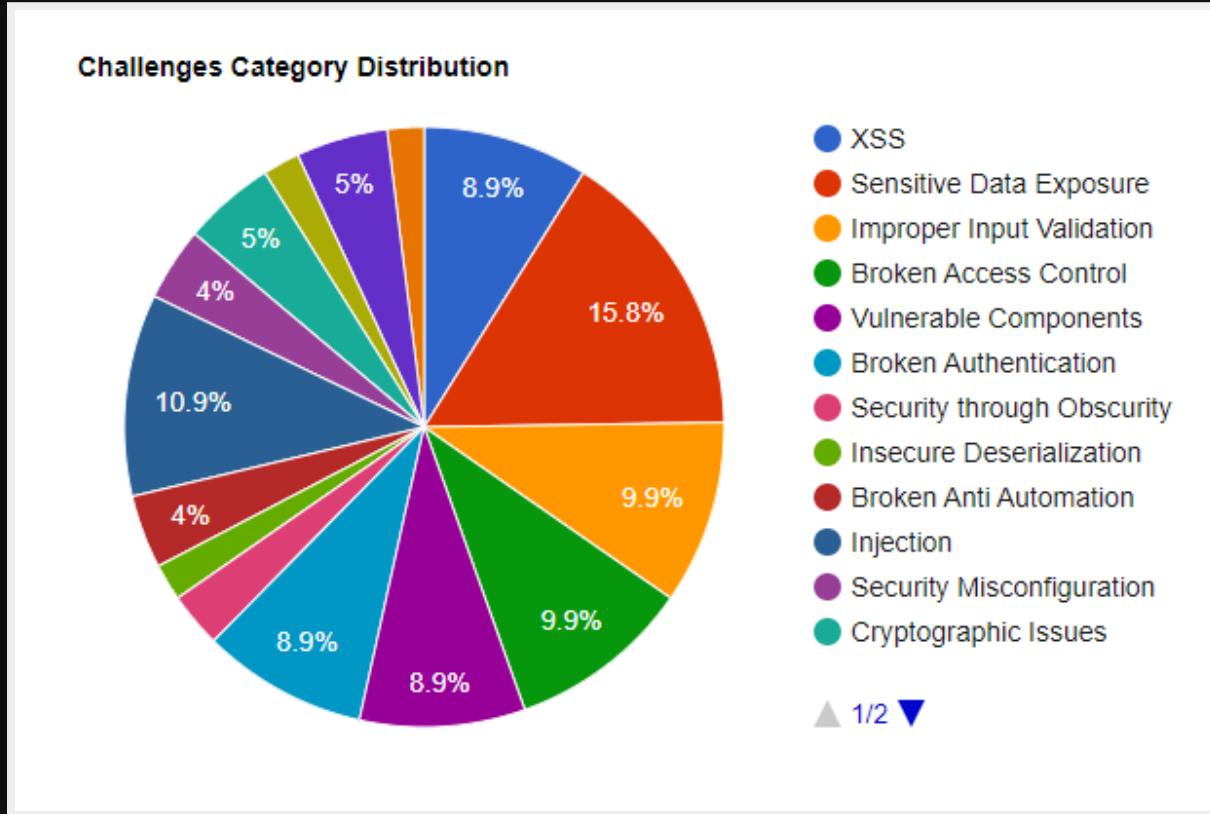
The commit message "Feature-complete version" is expanded to show the following list:

- complete feature-set of a small web-shop
- 23 security challenges featuring the entire [OWASP Top 10](#) and more
- complete server-side tracking of challenge progress (Warning: Resets on application restart!)
- almost full code coverage with client- and server-side tests

Below the commit message, there is a section titled "Assets" with a count of 2, accompanied by a smiley face icon.

Juice Shop v1.0.0 was released October 24th, 2014 with a mix of XSS, SQLi, Access Control and Information Leakage challenges

# Now: 107 Hacking Challenges



Challenges in Juice Shop are grouped into various categories mapped to official OWASP, CWE and WASC resources.

# 2014: Original Score Board

Juice Shop v1.0.0

Login Search Submit Contact Us About Us

## Score Board

Description	challenge	solved
Find the carefully hidden 'Score Board' page.	challenge	solved
Provoke an error that is not very gracefully handled.	challenge	open
Log in with the administrator's user account.	challenge	solved
Log in with Jim's user account.	challenge	open
Log in with Bender's user account.	challenge	open
XSS Tier 1: Perform a <i>reflected</i> XSS attack with <script>alert("XSS1")</script>.	challenge	open
XSS Tier 2: Perform a <i>persisted</i> XSS attack with <script>alert("XSS2")</script> bypassing a <i>client-side</i> security mechanism.	challenge	open
XSS Tier 3: Perform a <i>persisted</i> XSS attack with <script>alert("XSS3")</script> bypassing a <i>server-side</i> security mechanism.	challenge	open
XSS Tier 4: Perform a <i>persisted</i> XSS attack with <script>alert("XSS4")</script> without using the frontend application at all.	challenge	open
Retrieve a list of all user credentials via SQL Injection	challenge	solved
Log in with the administrator's user credentials without previously changing them or applying SQL Injection.	challenge	open
Get rid of all 5-star customer feedback.	challenge	open
Post some feedback in another users name.	challenge	open
Wherever you go, there you are.	challenge	open
Access someone else's basket.	challenge	open
Place an order that makes you rich.	challenge	open
Access a confidential document.	challenge	open
Access the administration section of the store.	challenge	open
Change Bender's password into <i>slurmCl4ssic</i> .	challenge	open
Change the link in the description of the O-Saft product to <a href="http://kimminich.de">http://kimminich.de</a> .	challenge	open
Inform the shop about a vulnerable library it is using. (Mention the exact library name and version in your complaint.)	challenge	open
Find the hidden easter egg.	challenge	open
Apply some advanced cryptanalysis to find the real easter egg.	challenge	open

Check me on GitHub

# 2021: Coding Challenges

Coding Challenge: DOM XSS

Find It

Fix It

```
1 filterTable () {
2     let queryParam: string = this.route.snapshot.queryParams.q
3     if (queryParam) {
4         queryParam = queryParam.trim()
5         this.dataSource.filter = queryParam.toLowerCase()
6         this.searchValue = this.sanitizer.bypassSecurityTrustHtml(queryParam)
7         this.gridDataSource.subscribe((result: any) => {
8             if (result.length === 0) {
9                 this.emptyState = true
10            } else {
11                this.emptyState = false
12            }
13        })
14    } else {
15        this.dataSource.filter = ''
16        this.searchValue = undefined
17        this.emptyState = false
18    }
19 }
```

close Submit

Coding Challenge: DOM XSS

Find It

Fix It

Fix 4

Fix 1

Fix 2

Fix 3

Fix 4

Differences (1)

Side by Side | Line by Line

Line	Code	Diff
1	filterTable () {	-
2	let queryParam: string = this.route.snapshot.queryParams.q	+ this.searchValue = this.sanitizer.bypassSecurityTrustScript(queryParam)
3	if (queryParam) {	- this.searchValue = this.sanitizer.bypassSecurityTrustHtml(queryParam)
4	queryParam = queryParam.trim()	- this.gridDataSource.subscribe((result: any) => {
5	this.dataSource.filter = queryParam.toLowerCase()	8 if (result.length === 0) {
6	this.searchValue = this.sanitizer.bypassSecurityTrustHtml(queryParam)	9 this.emptyState = true
7	this.gridDataSource.subscribe((result: any) => {	10 } else {
8	if (result.length === 0) {	11 this.emptyState = false
9	this.emptyState = true	12 }
10	} else {	13 })
11	this.dataSource.filter = ''	14 } else f
12	this.searchValue = undefined	
13	this.emptyState = false	
14	}	
15	}	

CSRF	★★★	Change the name of a user by performing Cross-Site Request Forgery from another origin.	Broken Access Control	unsolved
Confidential Document	★	Access a confidential document.	Sensitive Data Exposure	solved
DOM XSS	★	Perform a DOM XSS attack with <iframe src="javascript:alert('xss')">.	XSS	solved
Database Schema	★★★	Exfiltrate the entire DB schema definition via SQL Injection.	Injection	unsolved

Identify the underlying code flaw and select an appropriate fix. This is currently available as a follow-up task for 31 challenges

# 2023: Cluttered Score Board

Score Board 21% Coding Score 0%

10/13 4/13 6/22 1/25 0/18 6/11 Hide all Show solved Show tutorials only Show unavailable

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 Hide all

Name	Difficulty	Description	Category	Tags	Status	Feedback
Access Log	★★★★★	Gain access to any access log file of the server.	Sensitive Data Exposure		<span>unsolved</span>	<span>🔗</span>
Admin Registration	★★★	Register as a user with administrator privileges.	Improper Input Validation		<span>solved</span>	<span>🔗</span> <span>💡</span> <span>👎</span>
Admin Section	★★	Access the administration section of the store.	Broken Access Control	Good for Demos	<span>solved</span>	<span>🔗</span> <span>💡</span> <span>👎</span>
Allowlist Bypass	★★★★★	Enforce a redirect to a page you are not supposed to redirect to.	Unvalidated Redirects	Prerequisite	<span>solved</span>	<span>🔗</span> <span>💡</span> <span>👎</span>
Bjoern's Favorite Pet	★★★	Reset the password of Bjoern's OWASP account via the <a href="#">Forgot Password</a> mechanism with <i>the original answer</i> to his security question.	Broken Authentication	OSINT	<span>unsolved</span>	<span>🔗</span>
Blockchain Hype	★★★★★	Learn about the Token Sale before its official announcement.	Security through Obscurity	Code Analysis Contraption	<span>unsolved</span>	<span>🔗</span>
Bonus Payload	★	Use the bonus payload <iframe width="100%" height="166" scrolling="no" frameborder="no" all url="https://api.soundcloud.com/tracks/77198487&color=%23ff5500&auto_play=true&hide_reXSS</iframe> in the DOM XSS challenge.		Shenanigans Tutorial	<span>solved</span>	<span>🔗</span> <span>💡</span> <span>👎</span>
Bully Chatbot	★	Receive a coupon code from the support chatbot.	Miscellaneous	Brute Force Shenanigans	<span>solved</span>	<span>🔗</span> <span>💡</span> <span>👎</span>
CAPTCHA Bypass	★★★	Submit 10 or more customer feedbacks within 20 seconds.	Broken Anti Automation	Brute Force	<span>solved</span>	<span>🔗</span> <span>💡</span> <span>👎</span>
CSRF	★★★	Change the name of a user by performing Cross-Site Request Forgery from another origin.	Broken Access Control		<span>unsolved</span>	
Change Bender's Password	★★★★★	Change Bender's password into <i>slurmC1assic</i> without using SQL Injection or Forgot Password.	Broken Authentication		<span>unsolved</span>	
Christmas Special	★★★★★	Order the Christmas special offer of 2014.	Injection		<span>unsolved</span>	
Confidential Document	★	Access a confidential document.	Sensitive Data Exposure	Good for Demos	<span>solved</span>	<span>🔗</span> <span>💡</span> <span>👎</span>
Cross-Site Imaging	★★★★★	Stick cute cross-domain kittens all over our delivery boxes.	Security Misconfiguration	Contraption	<span>unsolved</span>	
DOM XSS	★	Perform a DOM XSS attack with <iframe src="javascript:alert('xss')">.	XSS	Good for Demos Tutorial	<span>solved</span>	<span>🔗</span> <span>💡</span> <span>👎</span>
Database Schema	★★★	Exfiltrate the entire DB schema definition via SQL Injection.	Injection		<span>unsolved</span>	<span>🔗</span>
Deluxe Fraud	★★★	Obtain a Deluxe Membership without paying for it.	Improper Input Validation		<span>unsolved</span>	
Deprecated Interface	★★	Use a deprecated B2B interface that was not properly shut down.	Security Misconfiguration	Contraption Prerequisite Contraption	<span>unsolved</span>	

# Now: Tile-based Score Board

The screenshot shows the OWASP Juice Shop application's score board interface. At the top, there are three progress bars: "Hacking Challenges" at 11%, "Coding Challenges" at 6%, and "Challenges Solved" at 14/156. Below the progress bars is a search bar and filters for "Difficulty", "Status", and "Tags". The main area displays challenges in a grid format:

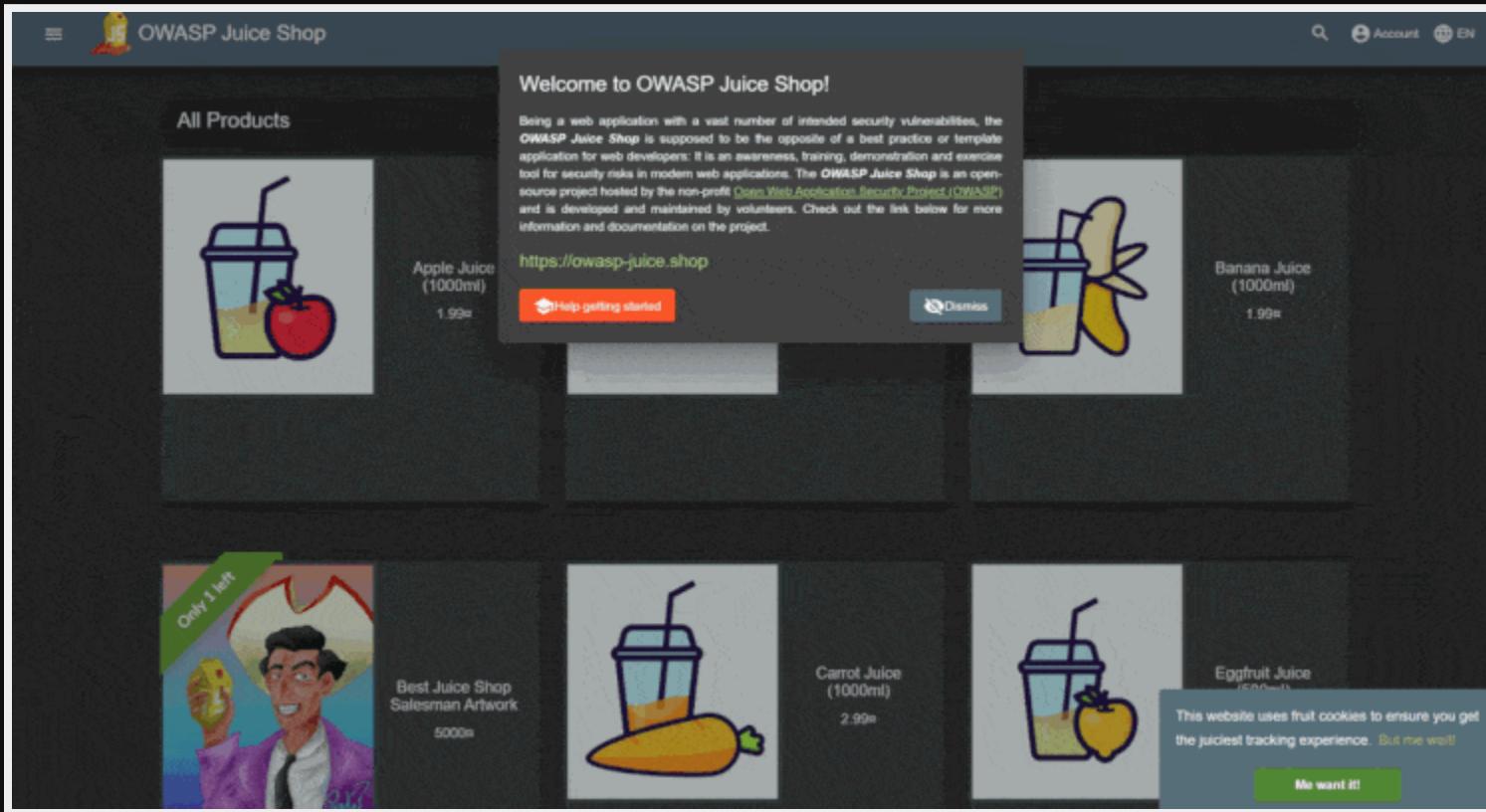
Vulnerability Type	Challenge Name	Difficulty	Status
XSS	API-only XSS	★★★	Pending
XSS	Bonus Payload	★	Pending
XSS	CSP Bypass	★★★★	Pending
XSS	Client-side XSS Protection	★★★	Pending
XSS	DOM XSS	★	Pending
XSS	HTTP-Header XSS	★★★★	Pending
XSS	Reflected XSS	★★	Pending
XSS	Server-side XSS Protection	★★★★★	Pending
XSS	Video XSS	★★★★★	Pending

Each challenge card includes a "Danger Zone" button, a "Tutorial" link, and a "Hint" button. A navigation bar at the bottom provides links to "Home", "About", "Contact", "Logout", and "Help".

# The Features

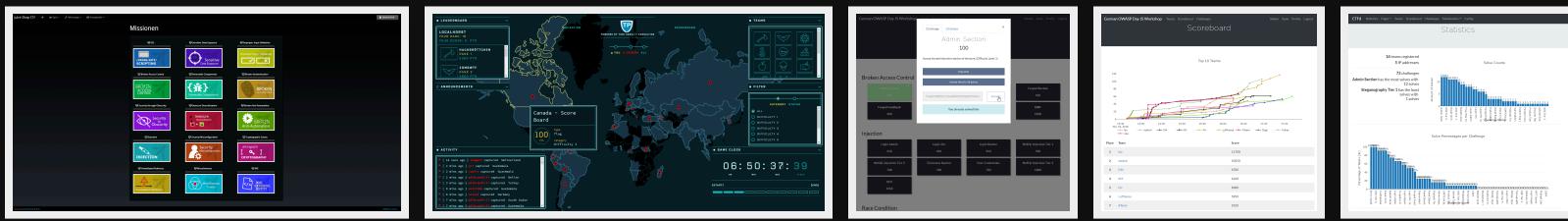
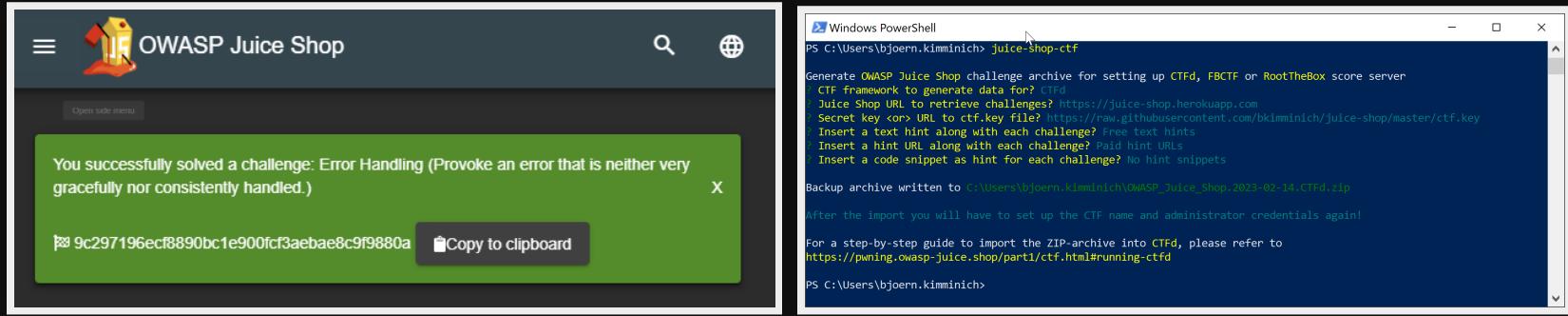


# Always: Real Fake Webshop



Juice Shop offers not only the full online shopping use case but also user profile management, 2FA, product reviews, customer services, chatbot assistance, user photo stories and much more

# 2016: Dedicated CTF-support



Built-in flag notifications and official juice-shop-ctf help setting up hacking events on CTFd, FBCTF or RootTheBox conveniently

# 2016: Companion Guide



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.



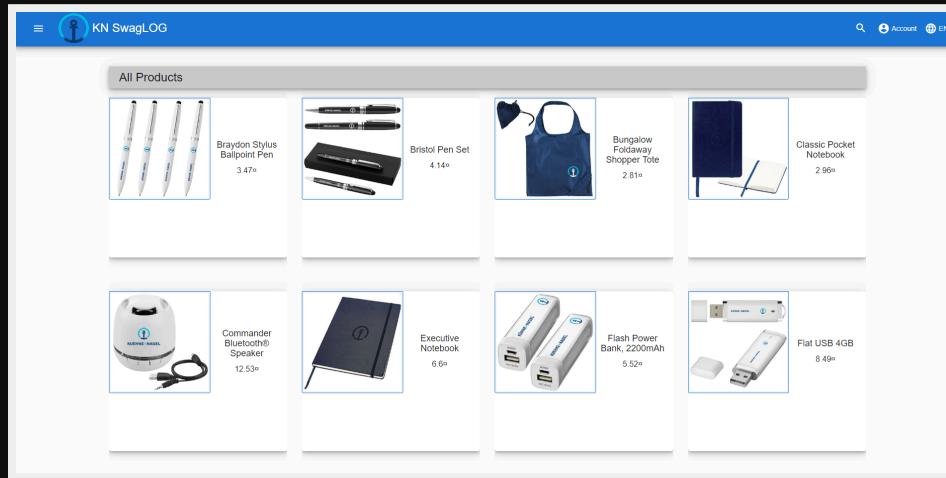
Pwning OWASP  
Juice Shop  
Björn Kimminich

Get It Free!

Minimum price: Free!  
Suggested price: \$10.99

The **free** official companion guide is available **on Leanpub** and can also be **read online**

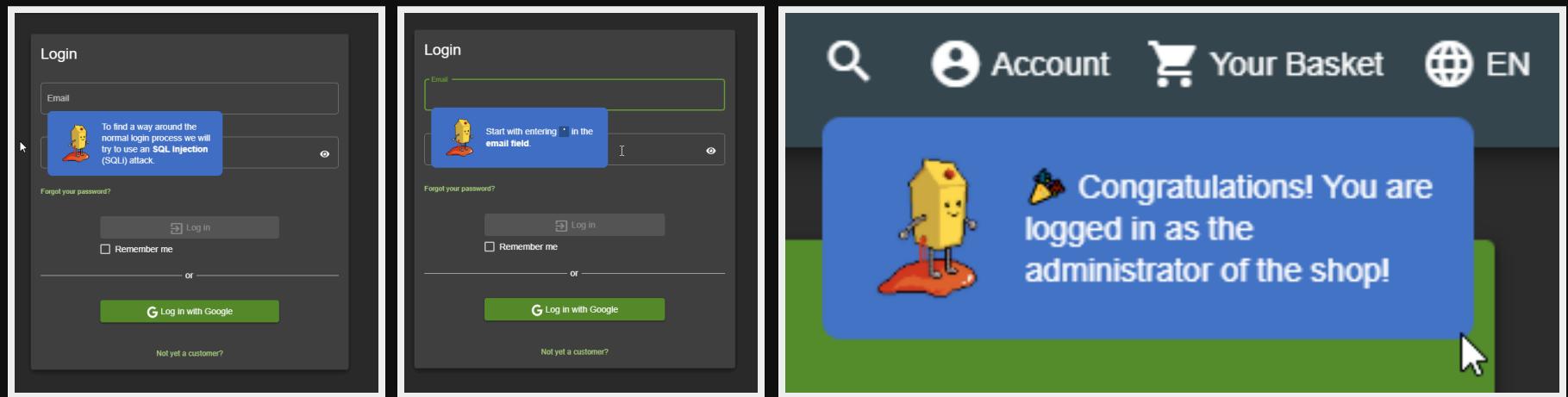
# 2017: Theming & Re-branding

Three screenshots of the KN SwagLOG website illustrating different user interactions:

- The first screenshot shows the "2FA Configuration" page, which includes a QR code for two-factor authentication, fields for "Please provide your current password" and "Initial Token", and a "Next Step" button.
- The second screenshot shows the "Your Basket" page for a user named "admin@kuehne-nagel.kn", listing items such as a Classic Softshell Jacket, a Latex Mattress, a Microfibre Towel, a Classic Pocket Notebook, and a Skin Support Pad, along with their prices and quantities.
- The third screenshot shows the "Customer Feedback" page, where a user has left a review with the text "WE CARE for security!", a rating of 5 stars, and a CAPTCHA field asking "What is 17+4?".

Fully customizable business context and look & feel for enhanced immersion in corporate trainings or awareness sessions

# 2019: Hacking Instructor



Several challenges come with an embedded interactive tutorial helping newcomers to get going

# 2019: MultiJuicer Platform

The image contains two side-by-side screenshots of the MultiJuicer platform interface.

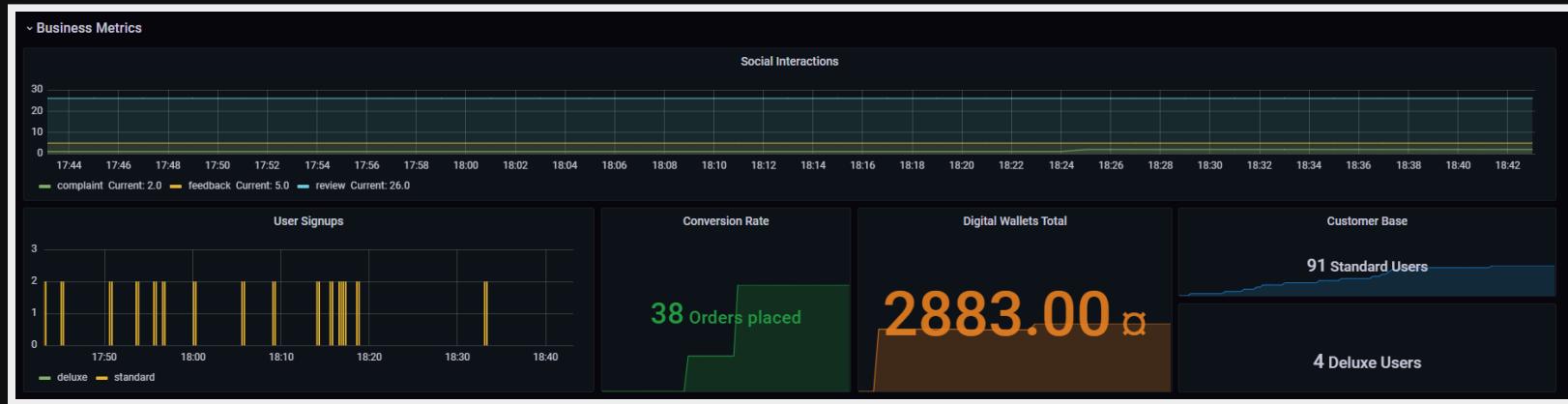
**Left Screenshot:** This is the "Team Created" page. At the top, it says "Logged in as four-point-zero" with "Log Out" and "Reset Passcode" buttons. Below that, a "Passcode" field shows a sequence of dots (••••••••). At the bottom, there's a green checkmark icon followed by "Juice Shop Instance Ready" and a large orange "Start Hacking" button. A small "Change Language" link is at the very bottom.

**Right Screenshot:** This is the "ScoreBoard" page. It features the MultiJuicer logo and the title "ScoreBoard". The table lists the following data:

#	NAME	SCORE
1	1337-hacker	50 points 4 solved challenges
2	localhorst	40 points 3 solved challenges
3	alpha	0 points 0 solved challenges
4	beta	0 points 0 solved challenges
5	delta	0 points 0 solved challenges
6	gamma	0 points 0 solved challenges

Originally an independent project, MultiJuicer became **the official platform** to run isolated Juice Shop instances for training or CTF participants on a central Kubernetes cluster in 2023

# 2020: Grafana Dashboard



JSON template allows to import a dashboard into Grafana consuming and displaying all metrics gathered via Prometheus

# 2020: Solution Webhook

```
{  
  "solution": {  
    "challenge": "localXssChallenge",  
    "cheatScore": 0,  
    "totalCheatScore": 0.15,  
    "issuedOn": "2020-12-15T18:24:33.027Z"  
  },  
  "ctfFlag": "b0d70dce...b85fac6785dba2349b",  
  "issuer": {  
    "hostName": "fv-az116-673",  
    "os": "Linux (5.4.0-1031-azure)",  
    "appName": "OWASP Juice Shop",  
    "config": "default",  
    "version": "12.3.0-SNAPSHOT"  
  }  
}
```

Sends a payload to a specified URL whenever a challenge is solved

# 2021: Cheat Detection

```
[0] info: Restored 'Fix It' phase of coding challenge localAssChallenge (Dom Ass)
[0] info: Restored 'Find It' phase of coding challenge scoreBoardChallenge (Score Board)
[0] info: Restored 'Fix It' phase of coding challenge scoreBoardChallenge (Score Board)
[0] info: Solved 'Find It' phase of coding challenge loginAdminChallenge (Login Admin)
[0] info: Accuracy for 'Find It' phase of coding challenge loginAdminChallenge: 0.5
[0] info: Cheat score for "Find it" phase of loginAdminChallenge solved in 1min (expected ~2min): 0.35365
[0] info: Solved 'Fix It' phase of coding challenge loginAdminChallenge (Login Admin)
[0] info: Accuracy for 'Fix It' phase of coding challenge loginAdminChallenge: 1
[0] info: Cheat score for "Fix it" phase of loginAdminChallenge solved in 1min (expected ~2min): 0.539975
[0] info: Solved 3-star loginJimChallenge (Login Jim)
[0] info: Cheat score for tutorial loginJimChallenge solved in 1min (expected ~3min) with hints allowed: 0.8261666666666667
[0] info: Solved 'Find It' phase of coding challenge loginJimChallenge (Login Jim)
[0] info: Accuracy for 'Find It' phase of coding challenge loginJimChallenge: 0.045454545454545456
[0] info: Cheat score for "Find it" phase of loginJimChallenge solved in 1min (expected ~2min): 0.6848083333333334
[0] info: Solved 'Fix It' phase of coding challenge loginJimChallenge (Login Jim)
[0] info: Accuracy for 'Fix It' phase of coding challenge loginJimChallenge: 0.1
[0] info: Cheat score for "Fix it" phase of loginJimChallenge solved in 0min (expected ~2min): 0.8438749999999999
```

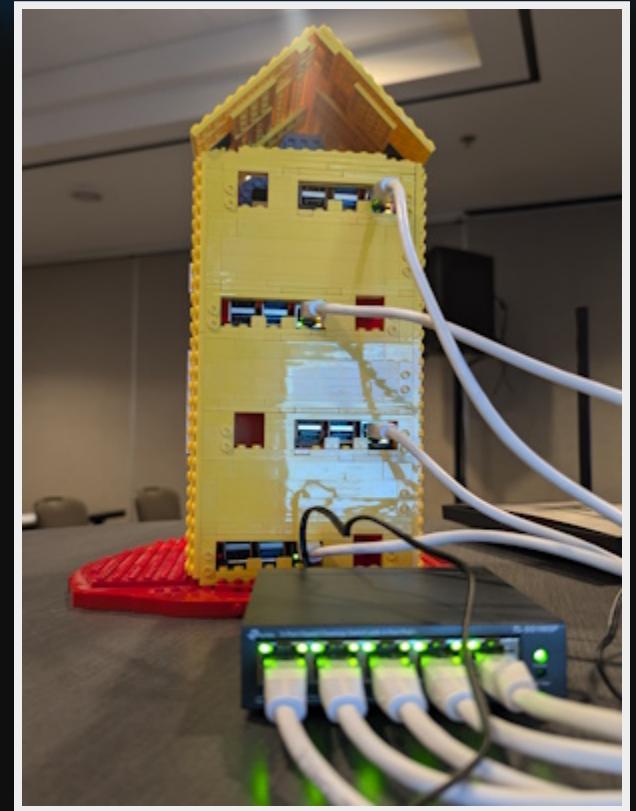
Solved challenges are rated based on cheating probability

# 2024: Juice Shop LEGO Tower



Huge kudos to Bram Patelski for the design & providing **all** necessary  
**source files** to build your own!

# 2024: MultiJuicer-To-Go



The LEGO case allows to bring a 4x Raspberry Pi cluster with PoE & cooling fans to any training and have MultiJuicer instances running literally out of the box! Also needed: PoE switch, WiFi router, and Internet uplink

# 2024: v1.0.0 Re-Release

**bkимminich/juice-shop** ★199  
By [bkимminich](#) · Updated about 1 hour ago  
OWASP Juice Shop: Probably the most modern and sophisticated insecure web application  
[IMAGE](#)

Manage Repository    Pulls 50M+

Overview Tags Dockerfile Builds

Sort by Newest Filter Tags Q    STATIC SCANNING ACTIVE

TAG
v1.0.0

Last pushed an hour ago by [bkимminich](#)

docker pull bkимminich/juice-shop:v1.0.0    Copy

Digest	OS/ARCH	Vulnerabilities	Last pull	Compressed Size
8bfd70cd6373	linux/amd64	20 54 52 6 0	an hour ago	252.31 MB

Juice Shop v1.0.0    Login Search Submit Contact Us About Us

All Products

Product	Description	Price
Apple Juice (1000ml)	The all-time classic.	1.99
Orange Juice (1000ml)	Made from oranges hand-picked by Uncle Dittmeyer.	2.99
Eggfruit Juice (500ml)	Now with even more exotic flavour.	8.99
Raspberry Juice (1000ml)	Made from blended Raspberry Pi, water and sugar.	4.99
Lemon Juice (500ml)	Sour but full of vitamins.	2.99
Banana Juice (1000ml)	Monkeys love it the most.	1.99
Lemon Juice (500ml)	Sour but full of vitamins.	2.99
Juice Shop T-Shirt (3XL)	Real fans wear it 24/7!	24.99
OWASP SSL Advanced Forensic Tool (O-Saft)	O-Saft is an easy to use tool to show information about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations. <a href="#">More...</a>	0.01

Fork me on GitHub

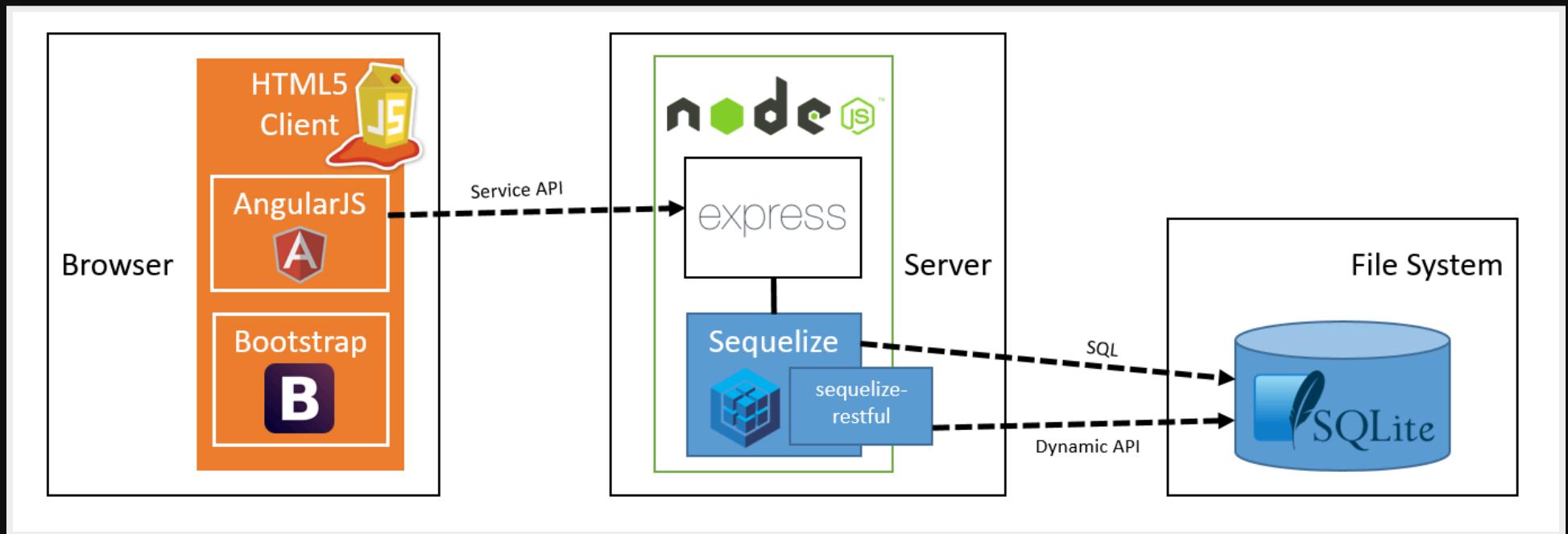
Docker images hadn't been introduced until v7.0.1 in 2017, but you can now experience the first ever Juice Shop with a hand-crafted v1.0.0 anniversary image available on DockerHub

`docker pull bkимminich/juice-shop:v1.0.0`

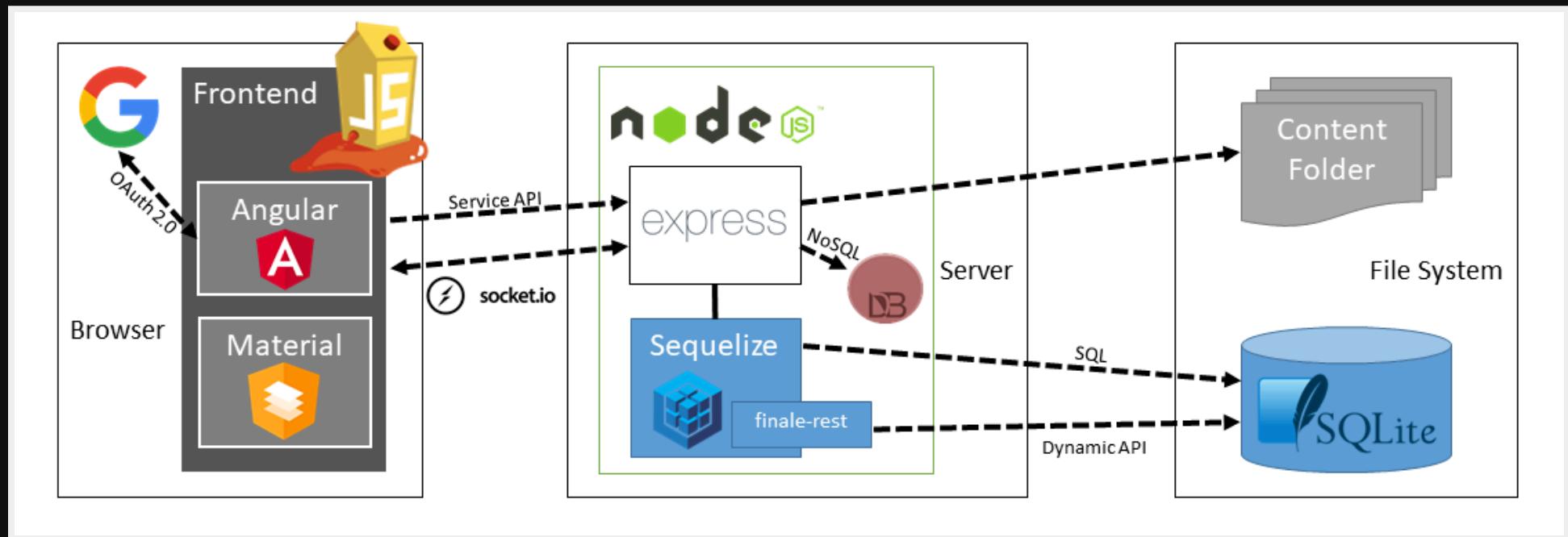
# The Technology



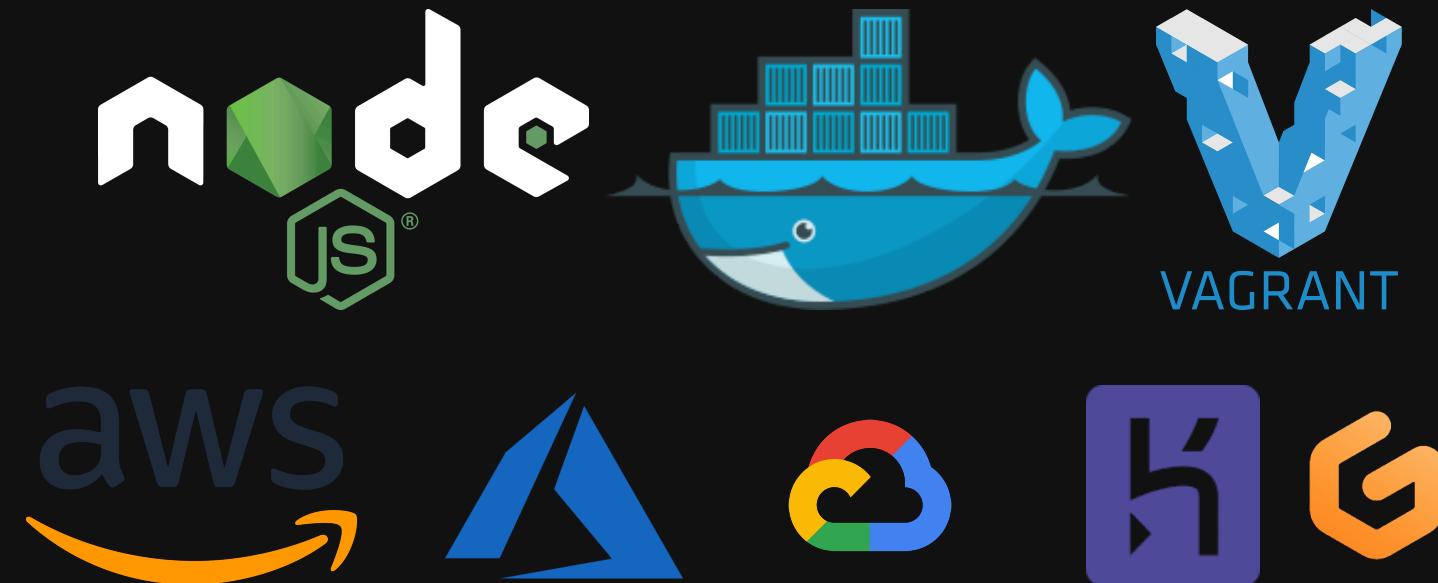
# 2014: "Bleeding-edge" Web-Architecture



# 2024: "Still-modern" Web-Architecture



# Always: Simple Installation



Comes with cloud, local and containerized run options

# The Community



# Core Team

Björn  
Kimminich



Jannik  
Hollenbach



Timo  
Pagel



Shubham  
Palriwala

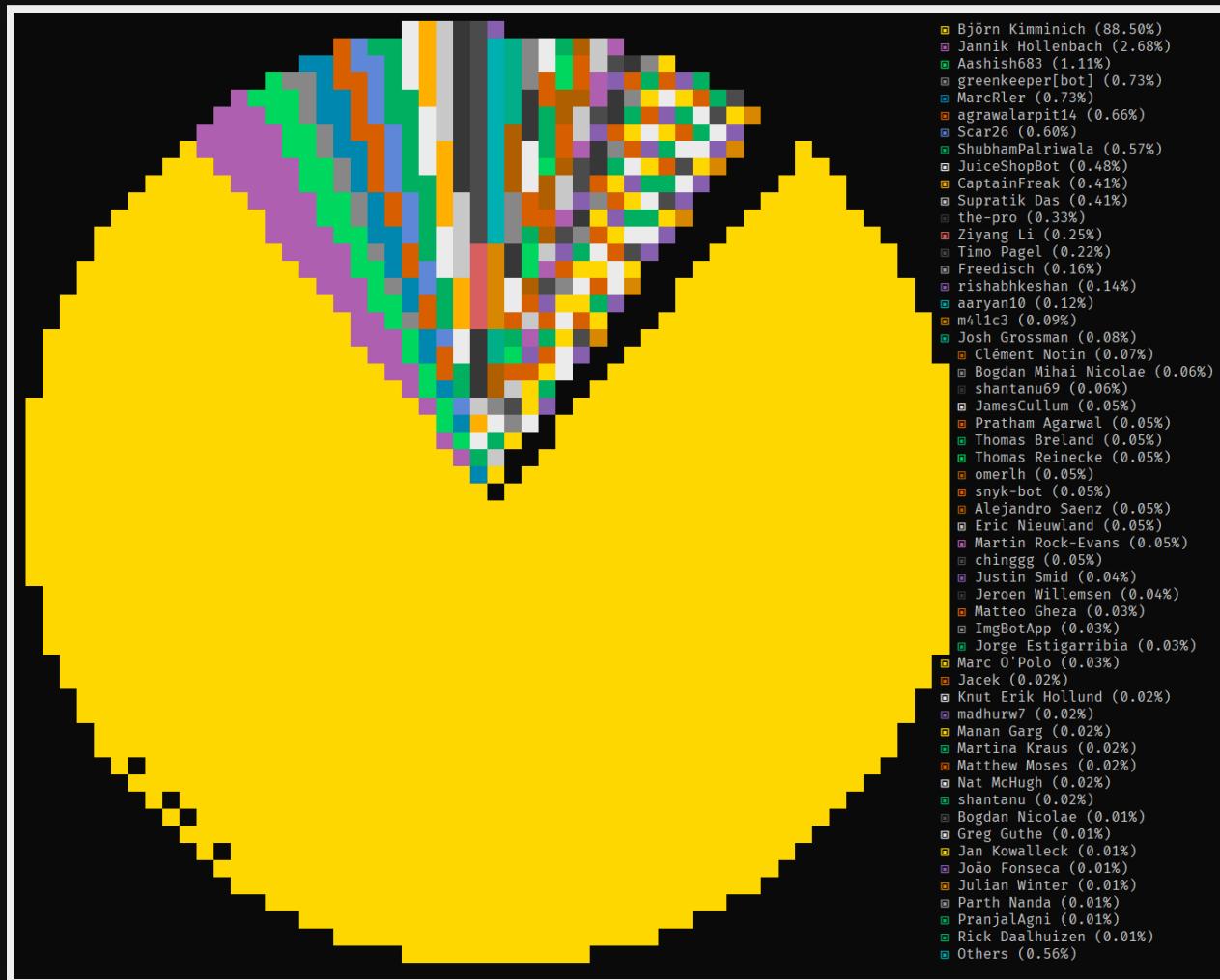


Björn Kimminich's GitHub Stats



Literally the **A-Team** behind the Juice Shop

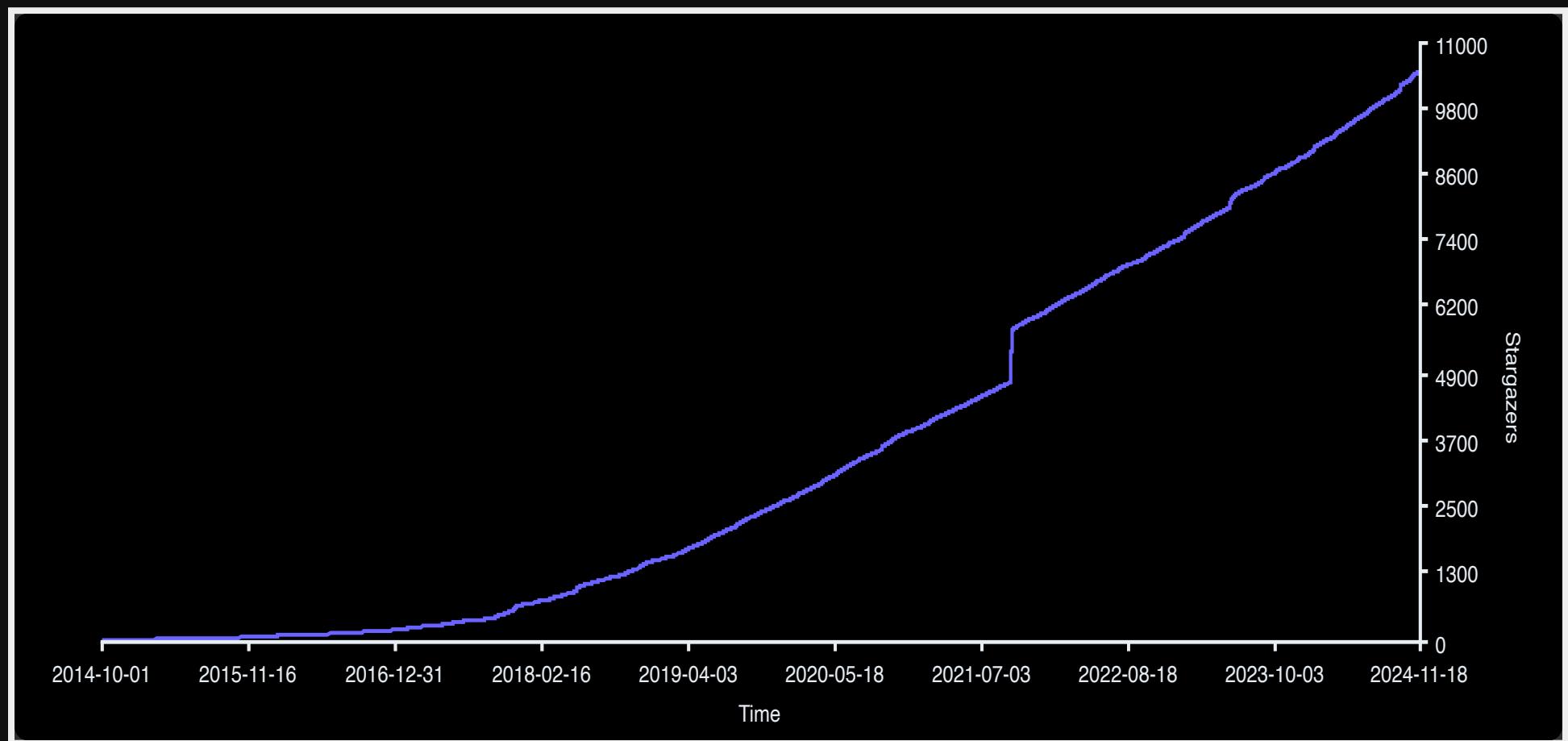
# Top 40+ Code Contributors



# Top 20+ I18N Contributors

Name	Languages	Translated ↓
 Björn Kimminich (bkimminich)	Dutch; German...	42 610
 tongsonghua (yolylight)	Chinese Simpli...	9689
 Derek Chan (ChanDerek)	Chinese Traditi...	5411
 D REMOVED_USER	Romanian	5009
 Yannick (yannickboy15)	Dutch	3872
 NCAA	Danish	3855
 Enrique Rossel (erossel)	Spanish	3416
 Simon Basset (simbas)	French	2933
 MortenHC	Danish	2597
 janestmae	Estonian	2594
 toshiaizawa	Japanese	2302
 mrtlgz	Turkish	2274
 schattenbaum	German, Switz...	2181
 Jean Novak (jeannovak)	Portuguese, Br...	2151
 ShahinF27 (Khan27)	Azerbaijani	2125
 Lang Mediator (lang.mediator)	Russian	1949
 Bogdan Mihai Nicolae (bogminic)	Romanian	1824
 htchen99	Chinese Traditi...	1664
 Timo Meriläinen (owasp.timo)	Finnish	1470
 Herisatry Lubaba (herisatry)	French	1465

# GitHub Stars over time



# 2020: Official Jingle



braimee

OWASP Juice Shop Jingle



SOUNDCLOUD

Share

[Privacy policy](#)

135K

braimee · OWASP Juice Shop Jingle

Thanks to podcaster-pentester-singer-songwriter-multi-talent Brian Johnson, Juice Shop is probably one of **very few** Open Source projects with its own official jingle

# 2018+: Google Summer of Code

- Student projects from [Google Summer of Code 2023](#)
  - [Companion Guide Tech Stack](#) by Parth Nanda (mentored by Jannik Hollenbach, Björn Kimminich and Shubham Palriwala)
  - [Hacking the Blockchain: Building Web3 Challenges for OWASP Juice Shop](#) by Rishabh Keshan (mentored by Shubham Palriwala and Björn Kimminich)
- Student project from [Google Summer of Code 2022](#)
  - [Replacement for Protractor end-to-end & Frisby API test suite to Cypress](#) by Shubham Palriwala (mentored by Jannik Hollenbach and Björn Kimminich)
- Student project from [Google Summer of Code 2021](#)
  - [Extending the features of the vulnerable code snippets](#) by Ayas Behera (mentored by Jannik Hollenbach and Björn Kimminich)
- Student project from [Google Summer of Code 2020](#)
  - [Juice-Shop ChatBot and general fixes](#) by Mohit Sharma (mentored by Jannik Hollenbach, Björn Kimminich and Timo Pagel)
- Student project from [Google Summer of Code 2019](#)
  - [OWASP Juice Shop: Feature Pack 2019](#) by Arpit Agrawal (mentored by Jannik Hollenbach, Björn Kimminich and Shoeb Patel)
- Student projects from [Google Summer of Code 2018](#)
  - [OWASP Juice Shop : Challenge Pack 2018](#) by Shoeb Patel (mentored by Jannik Hollenbach and Timo Pagel)
  - [OWASP Juice Shop : Frontend Technology Update](#) by Aashish Singh (mentored by Björn Kimminich)



# The Future

# Project Roadmap

Auction off up to ten unique anniversary NFT artworks to true Juice Shop fans

---

Complete the Angular 17 migration of the frontend

---

Re-write all MultiJuicer server components in Go (✓ completed. coming with upcoming 8.0.0 release)

---

Better MultiJuicer ScoreBoard listing solved challenges by team.

---

Pay back other accumulated technical debt and harmonize codebase overall

---

Bring overall test coverage back over 90%+



# The End...?



# Thank you for listening!

<https://owasp-juice.shop>

Copyright (c) 2014-2024 Björn Kimminich | @bkimminich | [@bkimminich@infosec.exchange](mailto:@bkimminich@infosec.exchange)

[@jannik@infosec.exchange](mailto:@jannik@infosec.exchange)

