



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

A vibrant illustration of a smoothie cup with the number '10' on it, surrounded by strawberries, a lime slice, and an apple against a starry night sky. The cup is filled with a yellow smoothie and topped with white whipped cream and two red straws. A red packet is attached to the side of the cup. The background is a dark blue night sky with yellow stars and white clouds. In the foreground, there are several strawberries, a slice of lime, and a green apple with a leaf.


The Idea

2008: Altoro Mutual




Stars 233



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



DEMO SITE ONLY

ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<p>PERSONAL</p> <ul style="list-style-type: none">Deposit ProductCheckingLoan ProductsCardsInvestments & InsuranceOther Services <p>SMALL BUSINESS</p> <ul style="list-style-type: none">Deposit ProductsLending ServicesCardsInsuranceRetirementOther Services <p>INSIDE ALTORO MUTUAL</p> <ul style="list-style-type: none">About UsContact UsLocationsInvestor RelationsPress RoomCareersSubscribe	<p>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.</p>  <p>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</p>	 <p>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.</p> <p>Retirement Solutions Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.</p>	<p>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.</p>  <p>Win a Samsung Galaxy S10 smartphone Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.</p>

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2023 Altoro Mutual, Inc. *This web application is open source! [Get your copy from GitHub](#) and take advantage of advanced features*

The Altoro Mutual 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/SW110>.

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

Server-side rendered demo app for a commercial vulnerability scanner

2010: Bodgeit Store Stars

The Bodgeit Store

We bodge it, so you dont have to! Guest user

[Home](#) [About Us](#) [Contact Us](#) [Login](#) [Your Basket](#) [Search](#)

[Doodahs](#)
[Gizmos](#)
[Thingamajigs](#)
[Thingies](#)
[Whatchamacallits](#)
[Whatsits](#)
[Widgets](#)

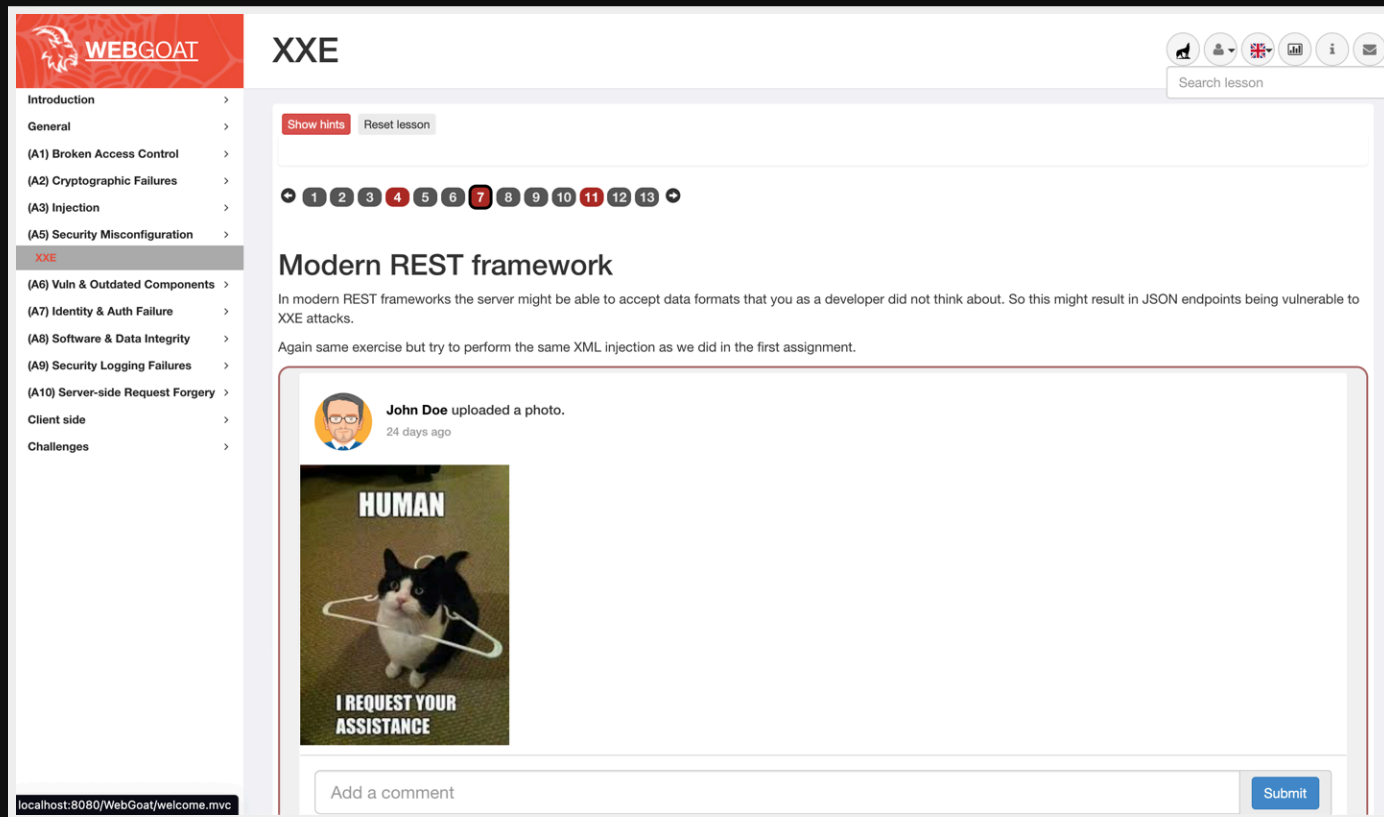
Our Best Deals!

Product	Type	Price
Thingie 2	Thingies	\$3.20
GZ ZX3	Gizmos	\$3.81
Thingie 2	Thingies	\$3.20
Thingie 5	Thingies	\$3.70
Thingie 4	Thingies	\$3.50
Thingie 4	Thingies	\$3.50
TGJ CCC	Thingamajigs	\$0.70
TGJ JJJ	Thingamajigs	\$0.80
Whatsit taste like	Whatsits	\$3.96
TGJ EFF	Thingamajigs	\$3.00

Server-side rendered demo app for the open source vulnerability scanner [Zed Attack Proxy](#)

OWASP WebGoat Stars

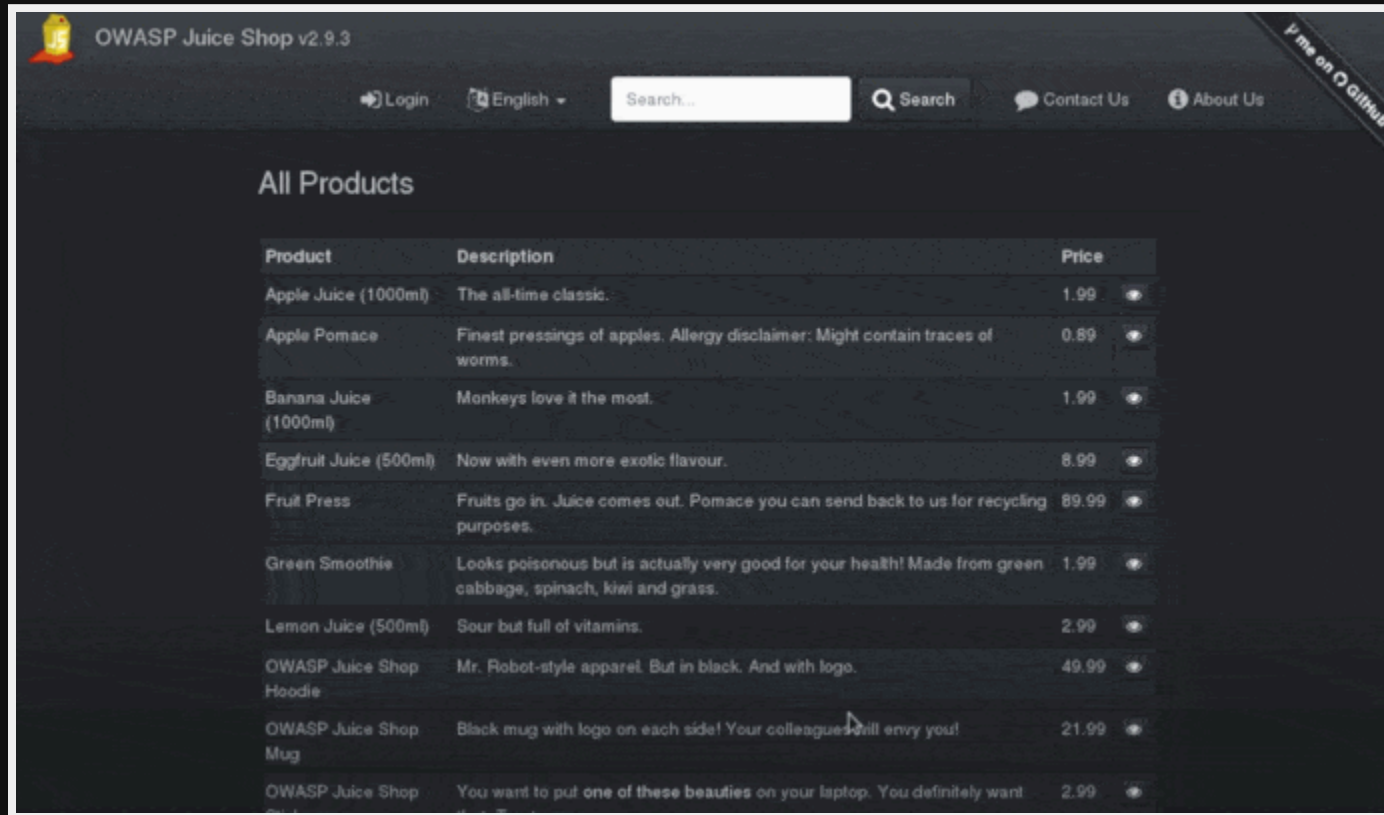
(Honorable Mention)



The screenshot displays the OWASP WebGoat application interface. On the left is a navigation menu with categories like Introduction, General, and various A01-A10 security topics. The main content area is titled "XXE" and features a "Show hints" button and a "Reset lesson" button. A progress indicator shows 13 lessons, with lesson 7 highlighted. The current lesson is "Modern REST framework", which explains that modern REST frameworks can accept data formats not considered by developers, making JSON endpoints vulnerable to XXE attacks. It includes a social media-style post from "John Doe" showing a cat with a hanger around its neck, with the text "HUMAN" and "I REQUEST YOUR ASSISTANCE". A "Submit" button is visible at the bottom right of the lesson content.

Server-side rendered and lesson-based training application

2014: Juice Shop



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](#) [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. More...	0.01	

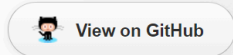
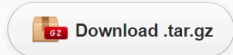
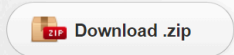
Fork me on GitHub

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.



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 [@psiinon](#).

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

- Home
- About OWASP
- Acknowledgements
- Advertising
- Books
- Brand Resources
- Careers
- Chapters
- Downloads
- Events
- Funding
- Governance
- Initiatives
- Mailing Lists
- Merchandise
- Presentations
- Press
- Projects
- Supporting Partners
- Video

- Reference
- Activities
- Attacks
- Code Snippets
- Controls
- Glossary
- How To...
- Java Project
- .NET Project
- Principles
- Technologies
- Threat Agents
- Vulnerabilities

- Tools
- What links here
- Related changes

Page Discussion Read View source View history Search

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

Watch 150 Star 8,560

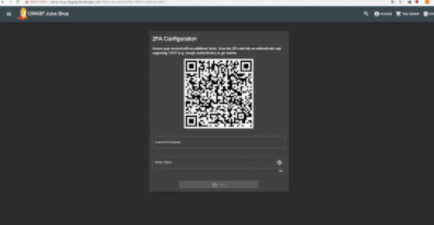
[Main](#) [Overview](#) [News](#) [Challenges](#) [Learning](#) [CTF](#) [Ecosystem](#) [Supporters](#)



owasp **flagship project** release **v15.0.0** GitHub **★ 8.6k** [Follow](#)

[CII Best Practices](#) Contributor Covenant **v2.0 adopted**

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](#)

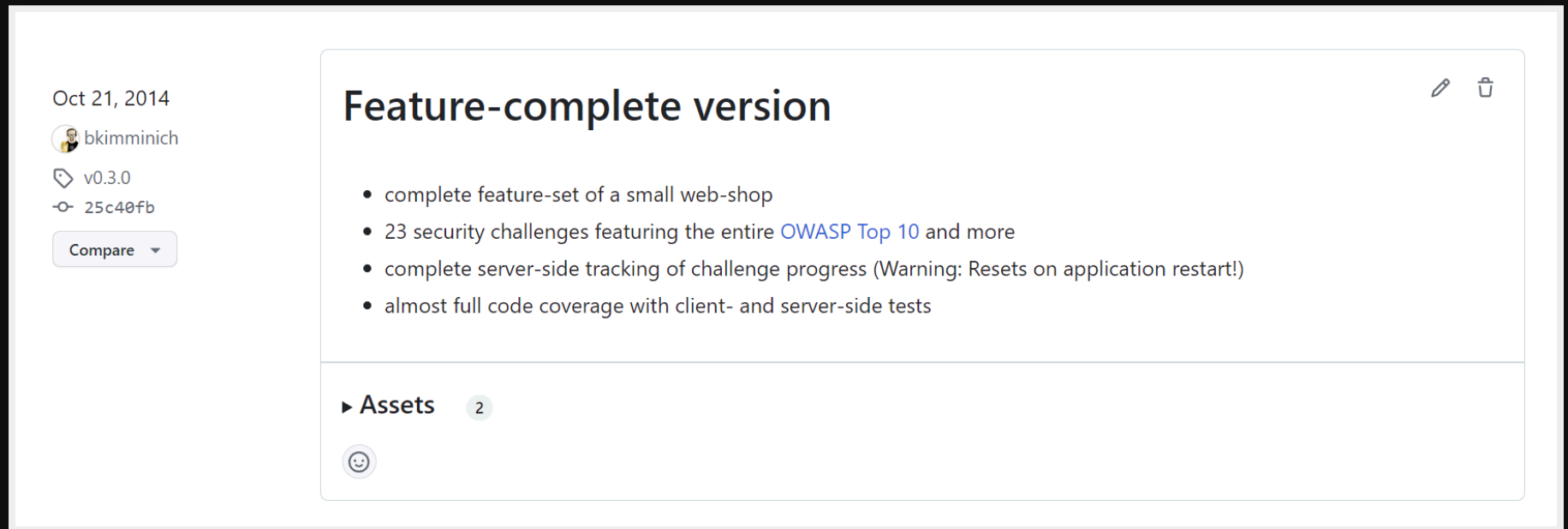
Sources

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





The Challenges


2014: 23 Hacking Challenges



Oct 21, 2014

 bkimminich

 v0.3.0


 25c40fb

Compare ▾

Feature-complete version

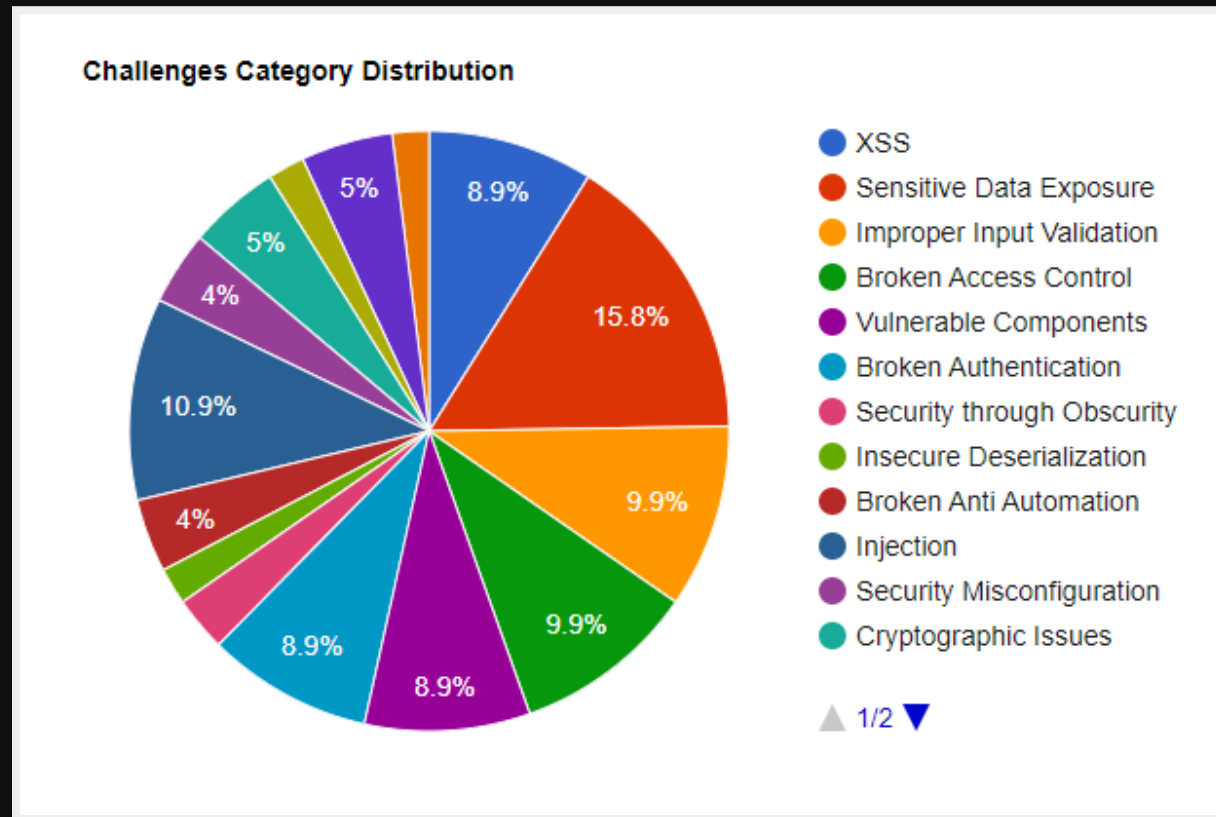
- complete feature-set of a small web-shop
- 23 security challenges featuring the entire [OWASP Top 10](#) and more
- complete server-side tracking of challenge progress (Warning: Resets on application restart!)
- almost full code coverage with client- and server-side tests

▶ Assets 2



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	
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 <code><script>alert("XSS1")</script></code> .	challenge open
XSS Tier 2: Perform a <i>persisted</i> XSS attack with <code><script>alert("XSS2")</script></code> bypassing a <i>client-side</i> security mechanism.	challenge open
XSS Tier 3: Perform a <i>persisted</i> XSS attack with <code><script>alert("XSS3")</script></code> bypassing a <i>server-side</i> security mechanism.	challenge open
XSS Tier 4: Perform a <i>persisted</i> XSS attack with <code><script>alert("XSS4")</script></code> 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>slurmC4ssic</i> .	challenge open
Change the link in the description of the <i>O-Saft</i> product to http://kimminich.de .	challenge open
Inform the <i>shop</i> about a vulnerable library it is using. (Mention the exact library name and version in your complaint.)	challenge open
Find the hidden <i>easter egg</i> .	challenge open
Apply some advanced cryptanalysis to find <i>the real</i> easter egg.	challenge open

Work me on GitHub

2021: Coding Challenges

Coding Challenge: DOM XSS

Find It Fix It 🔒

```
1 filterTable () {
2   let queryParams: string = this.route.snapshot.queryParams.q
3   if (queryParams) {
4     queryParams = queryParams.trim()
5     this.dataSource.filter = queryParams.toLowerCase()
6     this.searchValue = this.sanitizer.bypassSecurityTrustHtml(queryParams)
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

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

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	Good for Demos solved
DOM XSS	★	Perform a DOM XSS attack with <code><iframe src="javascript:alert(`xss`)"></code> .	XSS	Good for Demos Tutorial 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 **1** 4/13 **2** 6/22 **3** 1/25 **4** 0/13 **5** 0/11 **6**

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		unsolved	
Admin Registration	★★★	Register as a user with administrator privileges.	Improper Input Validation		solved	👍👎
Admin Section	★★	Access the administration section of the store.	Broken Access Control	Good for Demos	solved	👍👎
Allowlist Bypass	★★★★	Enforce a redirect to a page you are not supposed to redirect to.	Unvalidated Redirects	Prerequisite	solved	👍👎
Biorn's Favorite Pet	★★★	Reset the password of Biorn's OWASP account via the <i>Forgot Password</i> mechanism with the <i>original</i> answer to his security question.	Broken Authentication	OSINT	unsolved	
Blockchain Hype	★★★★★	Learn about the Token Sale before its official announcement.	Security through Obscurity	Code Analysis Contraption	unsolved	
Bonus Payload	★	Use the bonus payload <code><iframe width="100%" height="166" scrolling="no" frameborder="no" all url=https%3A//api.soundcloud.com/tracks/771984076&color=23ff500&auto_play=true&hide_reXSS /></code> in the <i>DOM XSS</i> challenge.		Shenanigans Tutorial	solved	👍👎
Bully Chatbot	★	Receive a coupon code from the support chatbot.	Miscellaneous	Brute Force Shenanigans	solved	👍👎
CAPTCHA Bypass	★★★	Submit 10 or more customer feedbacks within 20 seconds.	Broken Anti Automation	Brute Force	solved	👍👎
CSRF	★★★	Change the name of a user by performing Cross-Site Request Forgery from <i>another origin</i> .	Broken Access Control		unsolved	
Change Bender's Password	★★★★★	Change Bender's password into <i>slurmC4ssic</i> without using SQL Injection or <i>Forgot Password</i> .	Broken Authentication		unsolved	
Christmas Special	★★★★	Order the Christmas special offer of 2014.	Injection		unsolved	
Confidential Document	★	Access a confidential document.	Sensitive Data Exposure	Good for Demos	solved	👍👎
Cross-Site Imaging	★★★★★	Slick <i>cute cross-domain kittens</i> all over our delivery boxes.	Security Misconfiguration	Contraption	unsolved	
DOM XSS	★	Perform a <i>DOM XSS</i> attack with <code><iframe src="javascript:alert('xss')"></code> .	XSS	Good for Demos Tutorial	solved	👍👎
Database Schema	★★★	Exfiltrate the entire DB schema definition via SQL Injection.	Injection		unsolved	
Deluxe Fraud	★★★	Obtain a Deluxe Membership without paying for it.	Improper Input Validation		unsolved	
Deprecated Interface	★★	Use a deprecated B2B interface that was not properly shut down.	Security Misconfiguration	Contraption Prerequisite Contraption	unsolved	

Now: Tile-based Score Board

The screenshot displays the OWASP Juice Shop score board in a browser window. The page title is "OWASP Juice Shop" and the URL is "localhost:3000/#score-board-preview?categories=XSS". The interface features a dark theme and a navigation bar with a search icon, "Account", "Your Basket", and "EN" language selector.

At the top, there are three summary tiles:

- 11% Hacking Challenges**: Represented by a green progress bar.
- 6% Coding Challenges**: Represented by a green progress bar.
- 14/156 Challenges Solved**: Represented by a grid of 6 stars, with the first 14 stars filled and the remaining 142 empty.

Below the summary tiles is a search bar and filter options for "Difficulty", "Status", and "Tags". A horizontal menu of category buttons is visible, including "All", "XSS", "Sensitive Data Exposure", "Improper Input Validation", "Broken Access Control", "Unvalidated Redirects", "Vulnerable Components", "Broken Authentication", "Security through Obscurity", "Insecure Deserialization", "Miscellaneous", "Broken Anti Automation", "Injection", "Security Misconfiguration", "Cryptographic Issues", and "XXE".

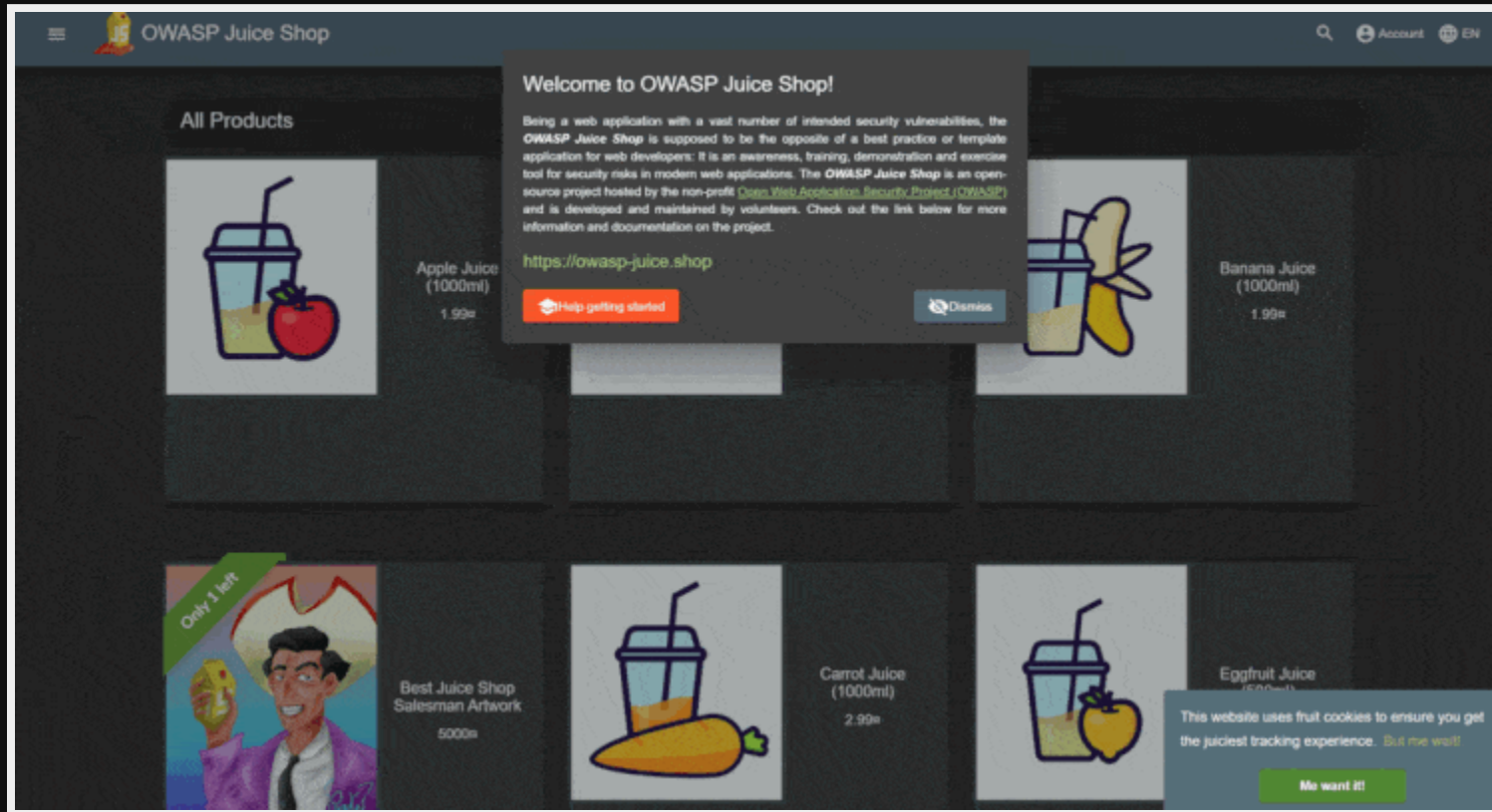
The main content area displays a grid of challenge tiles for the "XSS" category. Each tile includes the challenge name, difficulty rating (stars), a brief description, and a "Danger Zone" button. The tiles shown are:

- API-only XSS** (★★★): Perform a *persisted* XSS attack with `<iframe src='javascript:alert('xss')'>` without using the frontend application at all.
- Bonus Payload** (★): `hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true"></iframe>` in the DOM XSS challenge.
- CSP Bypass** (★★★★★): Bypass the Content Security Policy and perform an XSS attack with `<script>alert('xss')</script>` on a legacy page within the application.
- Client-side XSS Protection** (★★★): Perform a *persisted* XSS attack with `<iframe src='javascript:alert('xss')'>` bypassing a *client-side* security mechanism.
- DOM XSS** (★): Perform a *DOM* XSS attack with `<iframe src='javascript:alert('xss')'>`.
- HTTP-Header XSS** (★★★★★): Perform a *persisted* XSS attack with `<iframe src='javascript:alert('xss')'>` through an HTTP header.
- Reflected XSS** (★★):
- Server-side XSS Protection** (★★★★★):
- Video XSS** (★★★★★★):

The Features

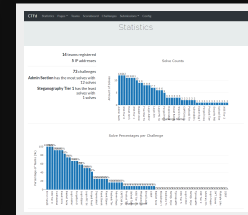
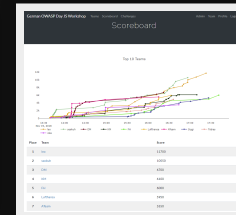
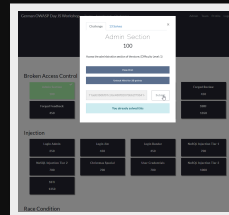
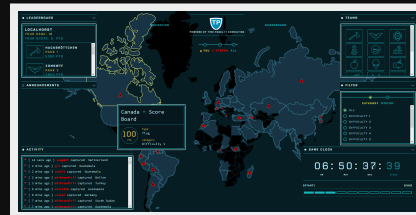
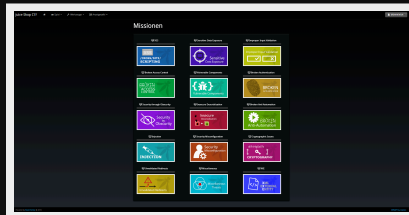
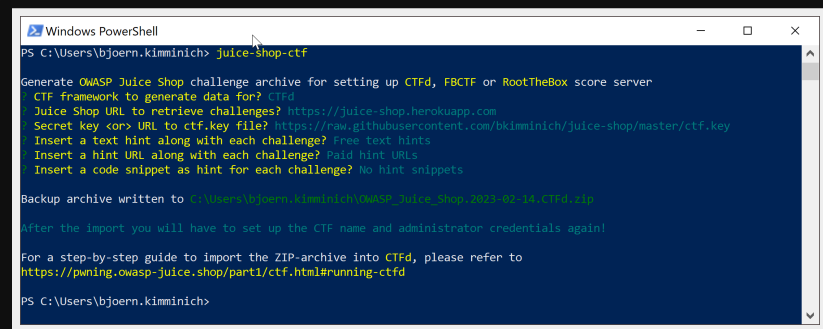
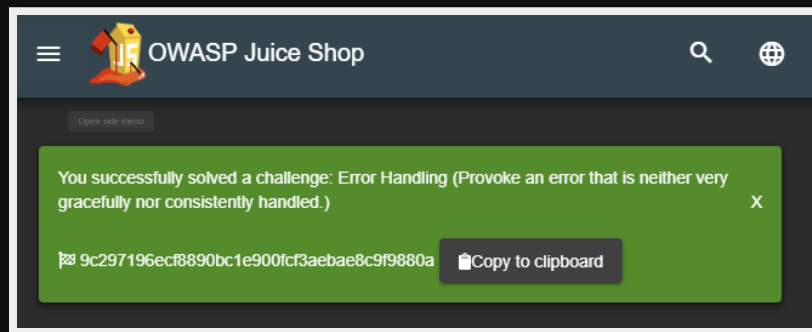


Always: Real Fake Webshop



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-cli** 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.



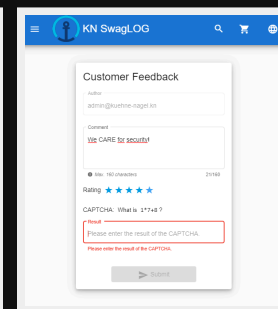
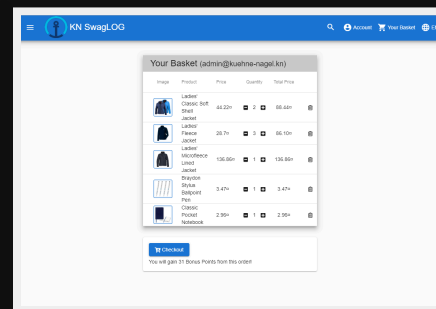
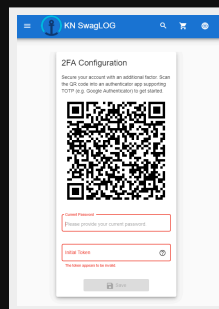
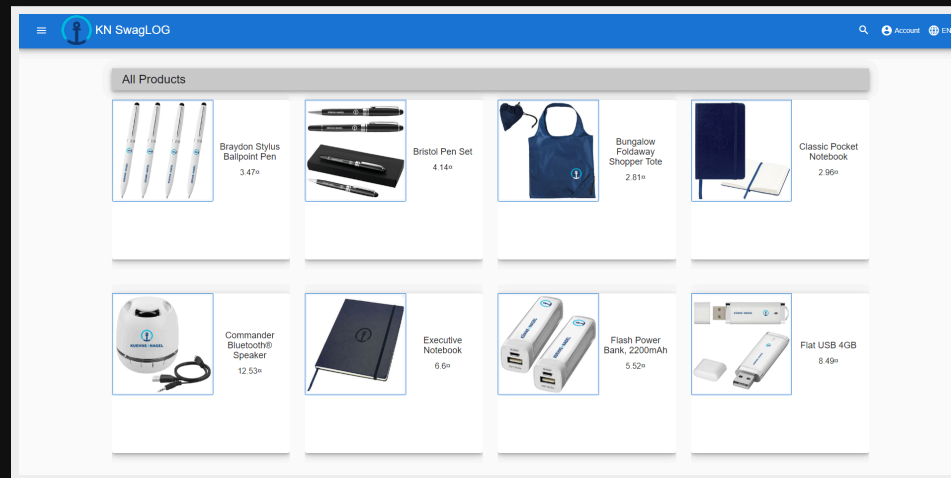
Pwning OWASP
Juice Shop
Björn Kimminich

Get It Free!

Minimum price: Free!
Suggested price: \$10.99

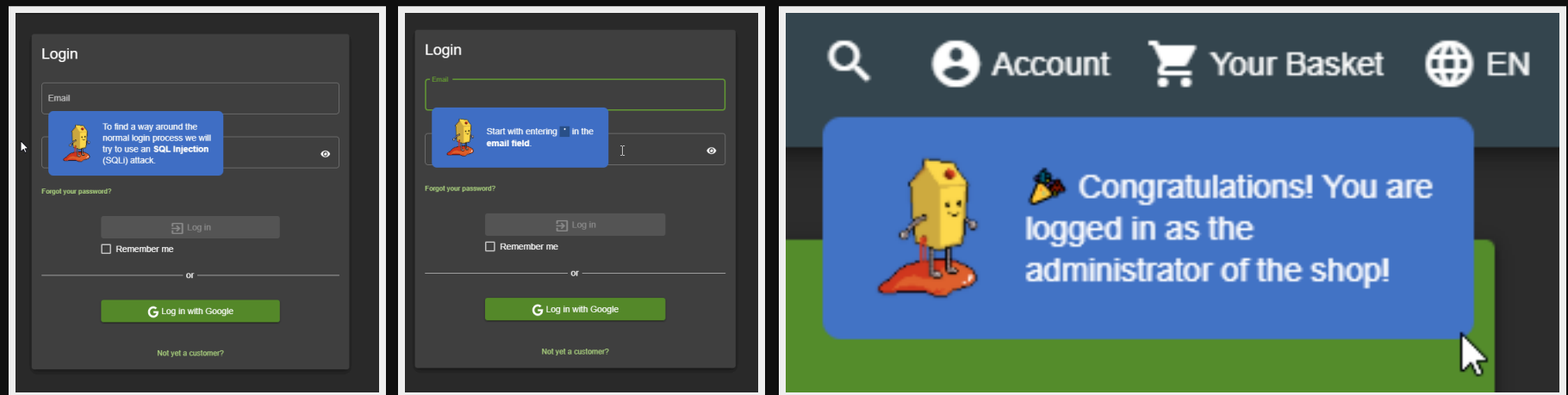
The **free** official companion guide is available **on Leanpub** and can also be **read online**

2017: Theming & Re-branding



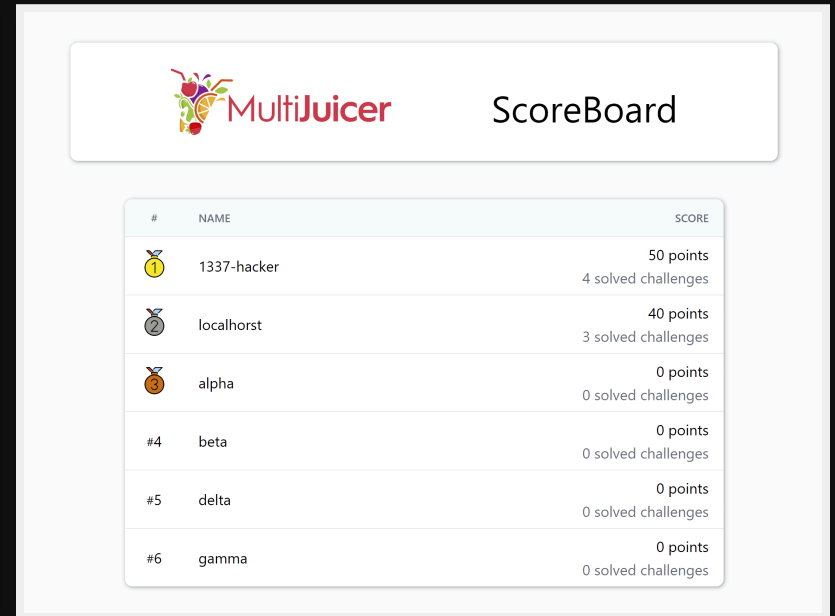
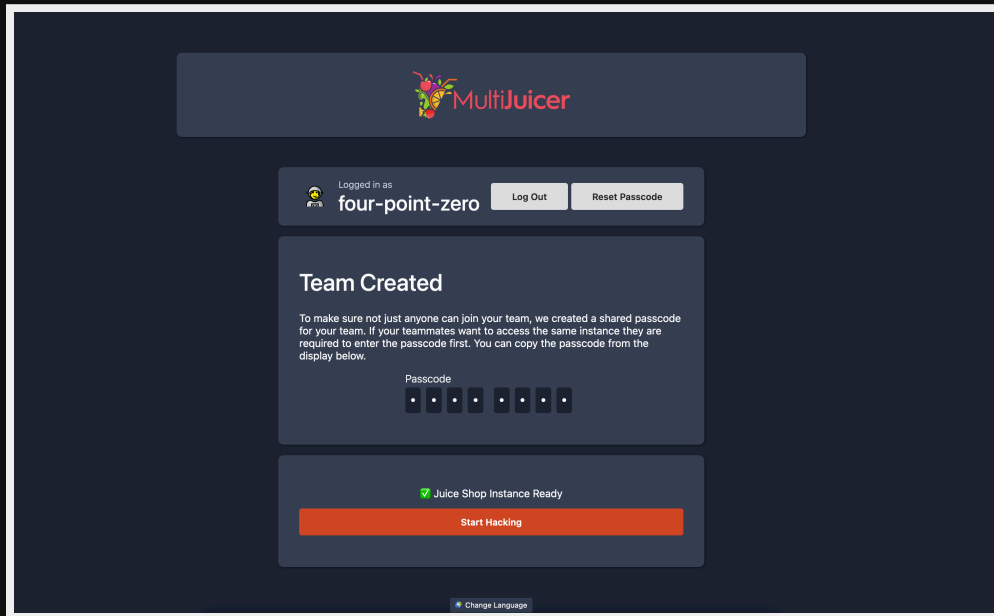
Fully **customizable** business context and look & feel for enhanced immersion in corporate trainings or awareness sessions

2019: Hacking Instructor



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

2019: MultiJuicer Platform



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: 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 localXSSChallenge (DOM XSS)
[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 lmin (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 lmin (expected ~2min): 0.539975
[0] info: Solved 3-star loginJimChallenge (Login Jim)
[0] info: Cheat score for tutorial loginJimChallenge solved in lmin (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 lmin (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
```

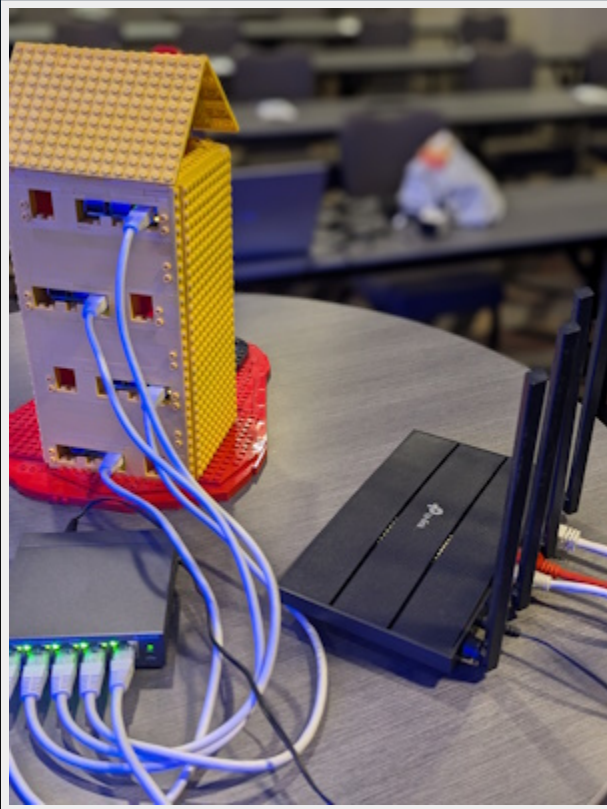
Solved challenges are rated based on cheating probability

2024: Juice Shop LEGO Tower



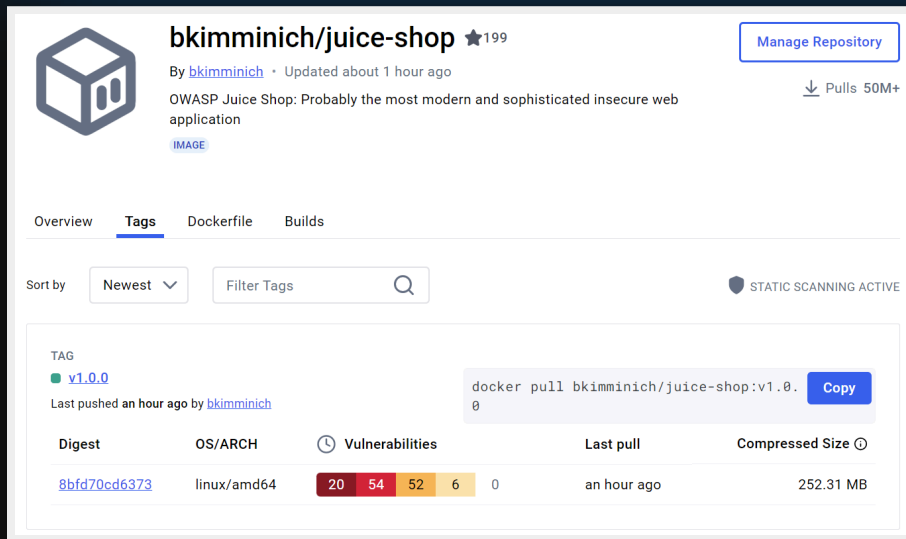
Huge kudos to Bram Patelski for the design & providing **all necessary source files** to build your own!

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



bkimminich/juice-shop ★199 [Manage Repository](#)

By [bkimminich](#) · Updated about 1 hour ago

OWASP Juice Shop: Probably the most modern and sophisticated insecure web application

↓ Pulls 50M+

Overview **Tags** Dockerfile Builds

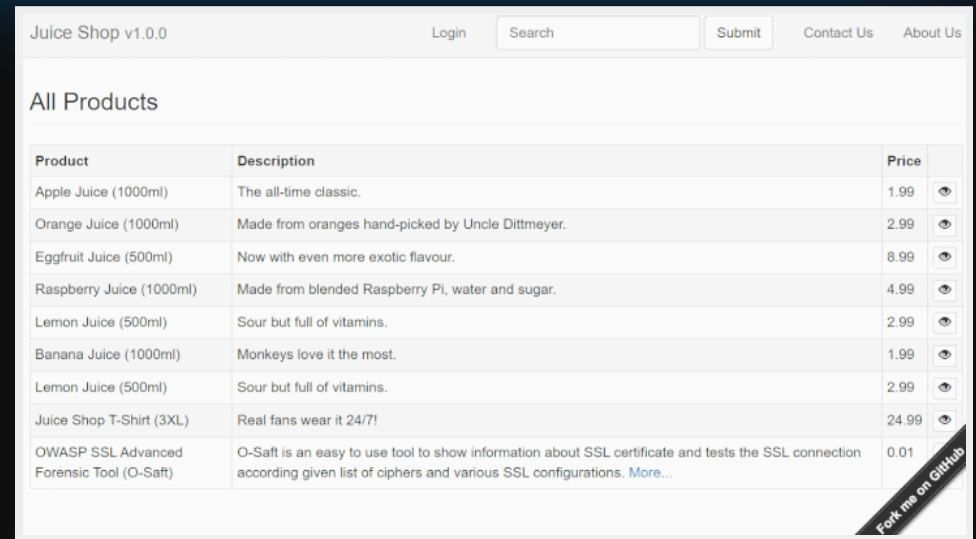
Sort by **Newest** Filter Tags STATIC SCANNING ACTIVE

TAG

v1.0.0 `docker pull bkimminich/juice-shop:v1.0.0` [Copy](#)

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

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](#) [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. More...	0.01

[Fork me on GitHub](#)

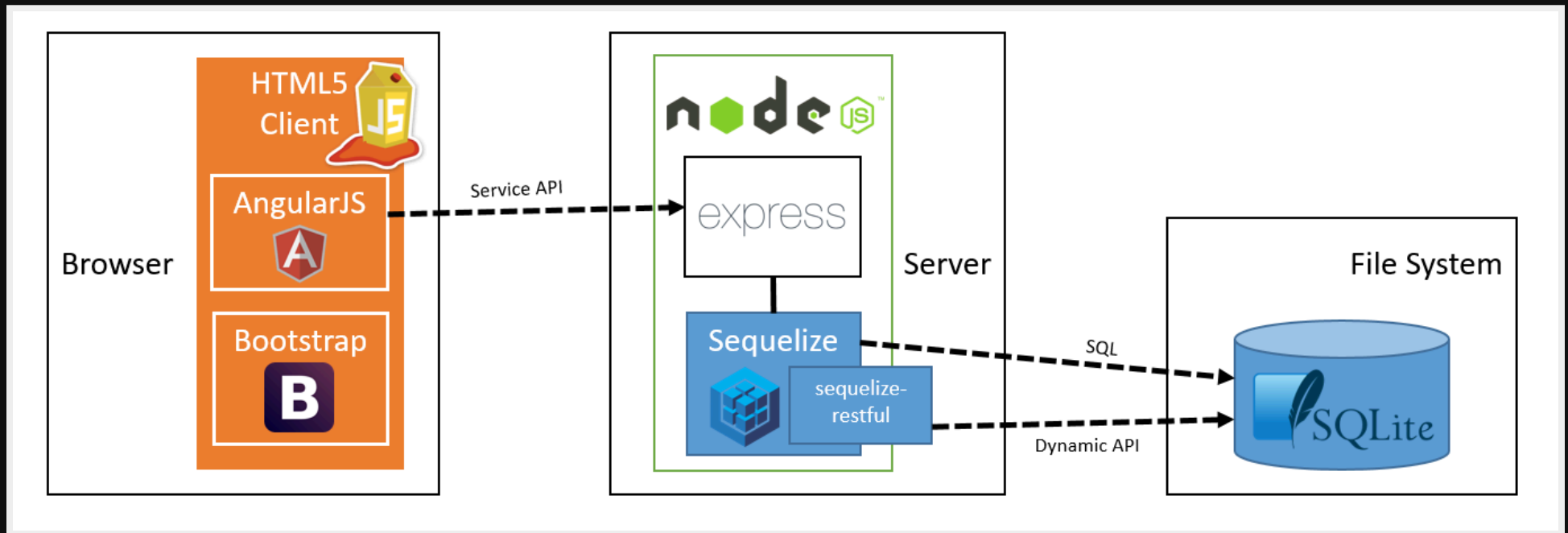
Docker images hadn't been introduced until v7.0.1 in 2017, but you can now experience the first ever Juice Shop with a hand-crafted v1.0.0 anniversary image available on DockerHub

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

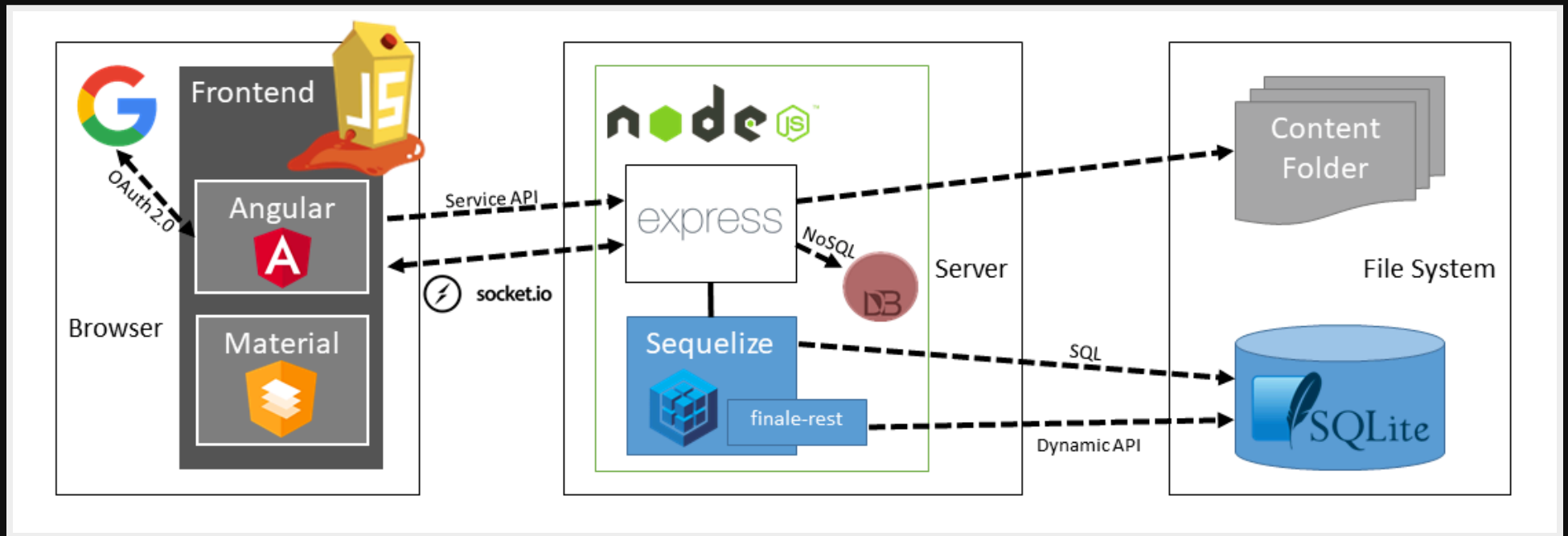


The Technology

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



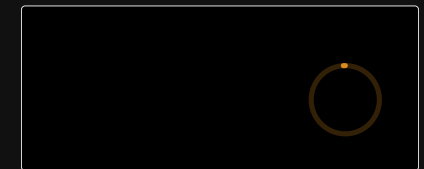
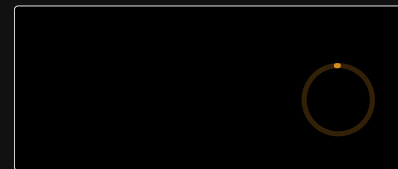
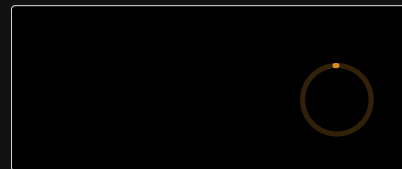
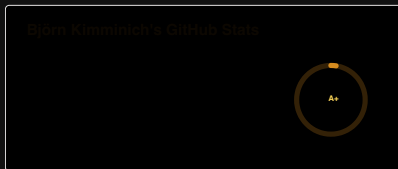
Jannik
Hollenbach



Timo
Pagel

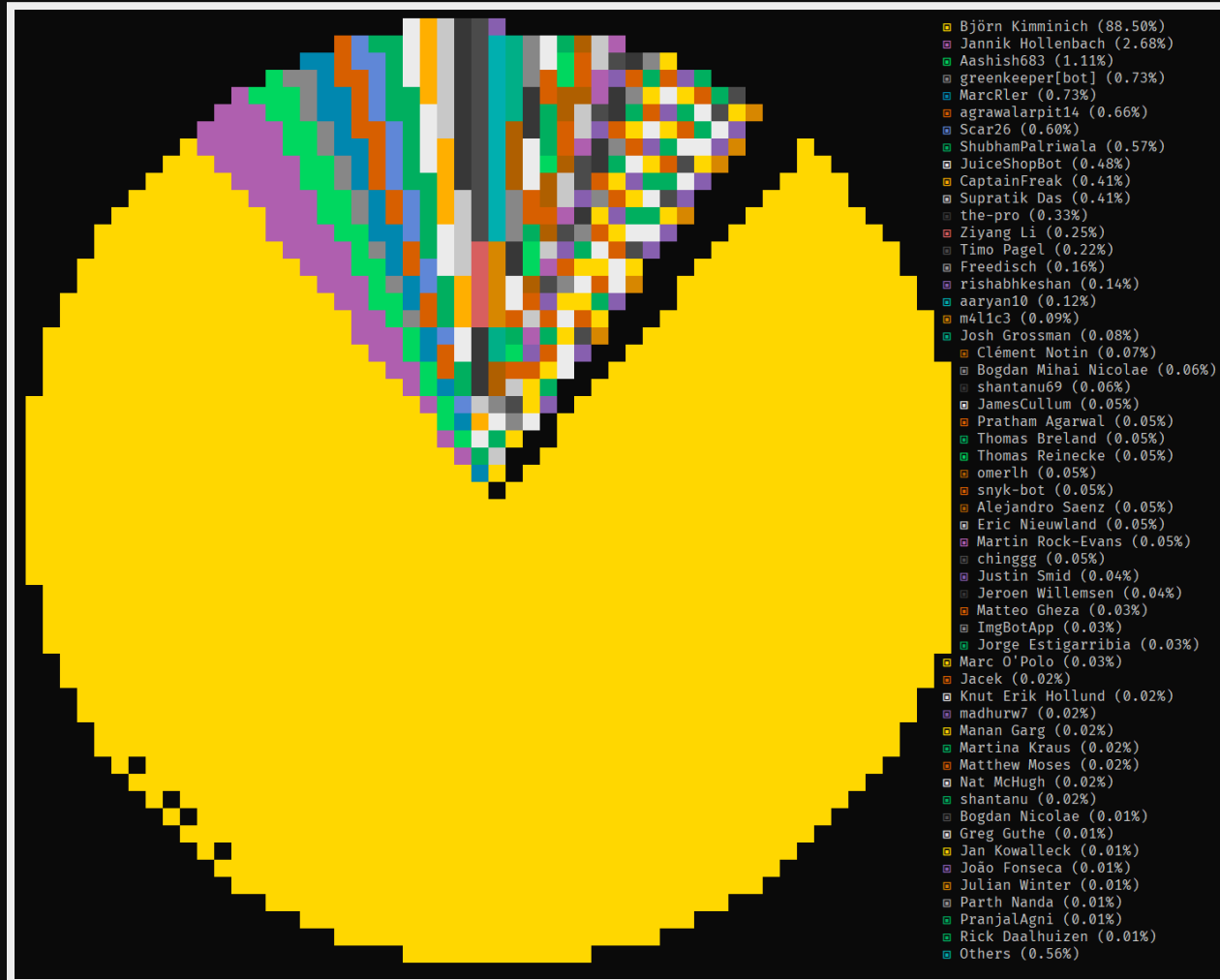


Shubham
Palriwala























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

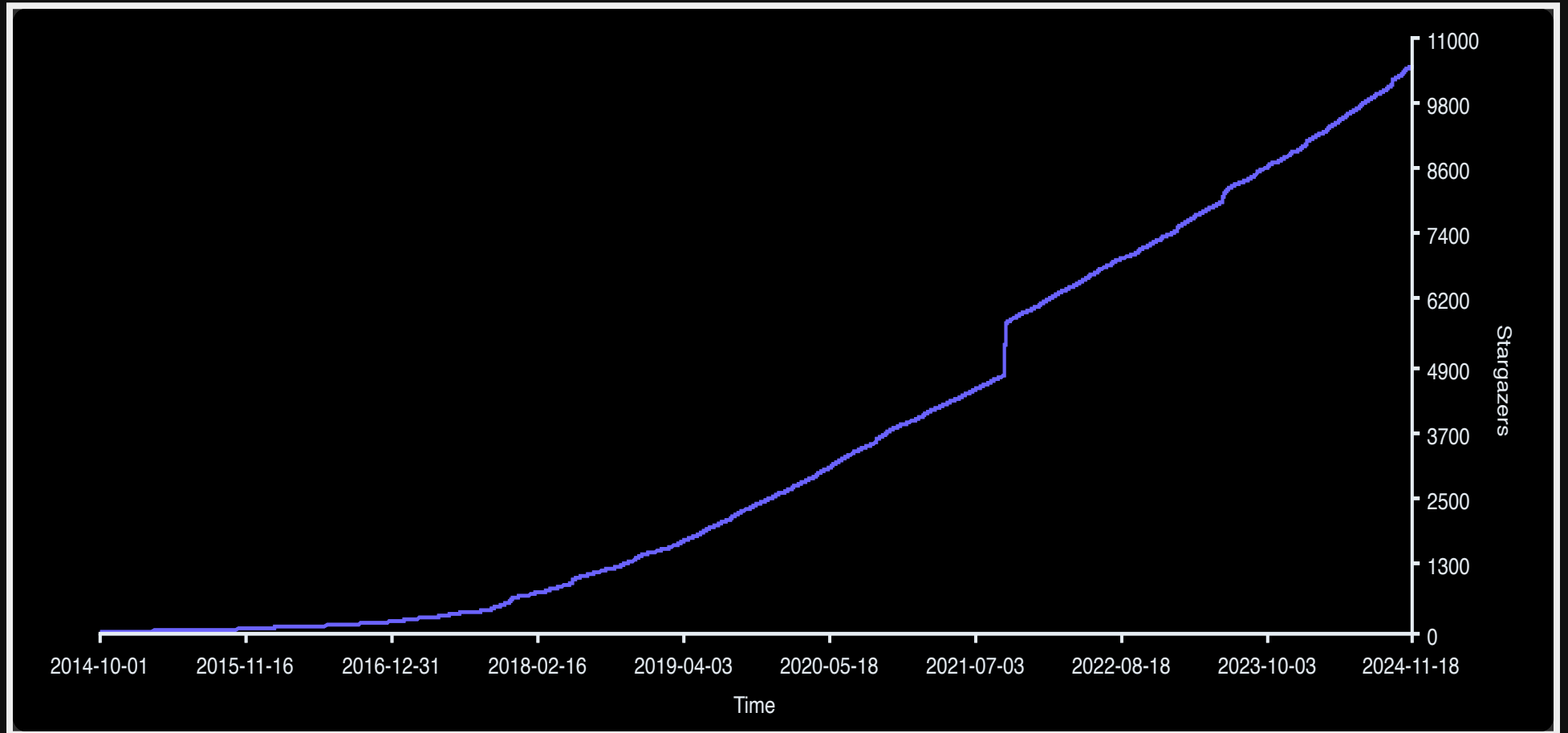
Top 40+ Code Contributors



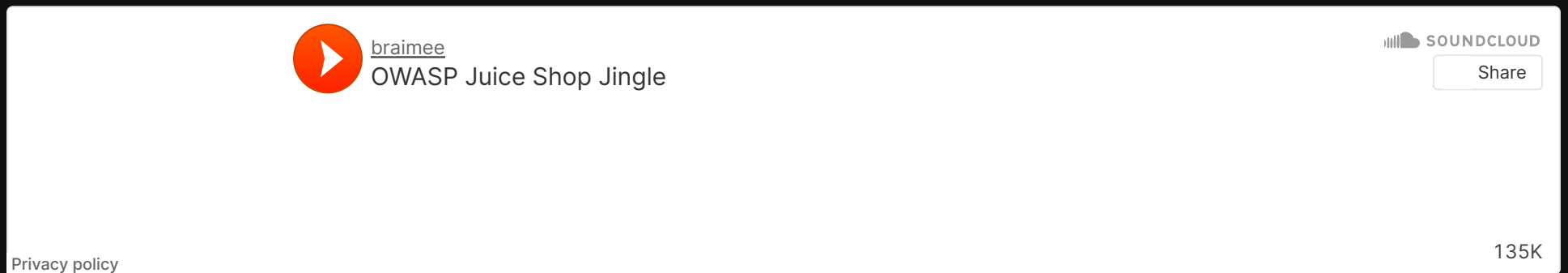
Top 20+ I18N Contributors

Name	Languages	Translated ↓
 Björn Kimminich (bkimminich)	Dutch; German...	42 610
 tongsonghua (yolylight)	Chinese Simpli...	9689
 Derek Chan (ChanDerek)	Chinese Traditi...	5411
 REMOVED_USER	Romanian	5009
 Yannick (yannickboy15)	Dutch	3872
 NCAA	Danish	3855
 Enrique Rossel (erossel)	Spanish	3416
 Simon Basset (simbas)	French	2933
 MortenHC	Danish	2597
 janesmae	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



The image shows a SoundCloud player interface. On the left, there is a red play button icon, the username 'braimee', and the track title 'OWASP Juice Shop Jingle'. On the right, there is the SoundCloud logo and a 'Share' button. At the bottom right of the player, the number '135K' is displayed. At the bottom left, there is a 'Privacy policy' link.

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)

A celebratory scene featuring a golden crown with the number '15' on it, sitting on a red and gold pedestal. The background is dark blue with stars, confetti, and balloons. The text 'The Future' is overlaid in white.

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...?

ANNIVERSARY



Thank you for listening!
<https://owasp-juice.shop>

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

@jannik@infosec.exchange

