



Once upon a time...

...developers and security experts relied on mostly server-side rendered vulnerable applications to train their web hacking skills.

In 2014, the **Juice Shop** entered the stage to change that.

OWASP Juice Shop

An Open Source Software

and security Fairytale

<https://owasp-juice.shop>

Copyright (c) 2014-2023 Björn Kimminich | @bkimminich | infosec.exchange/@bkimminich




Chapter I


The Idea

2008: Altoro Mutual




Stars 176



[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 239

The Bodgeit Store

We bodge it, so you dont have to!

Guest user

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

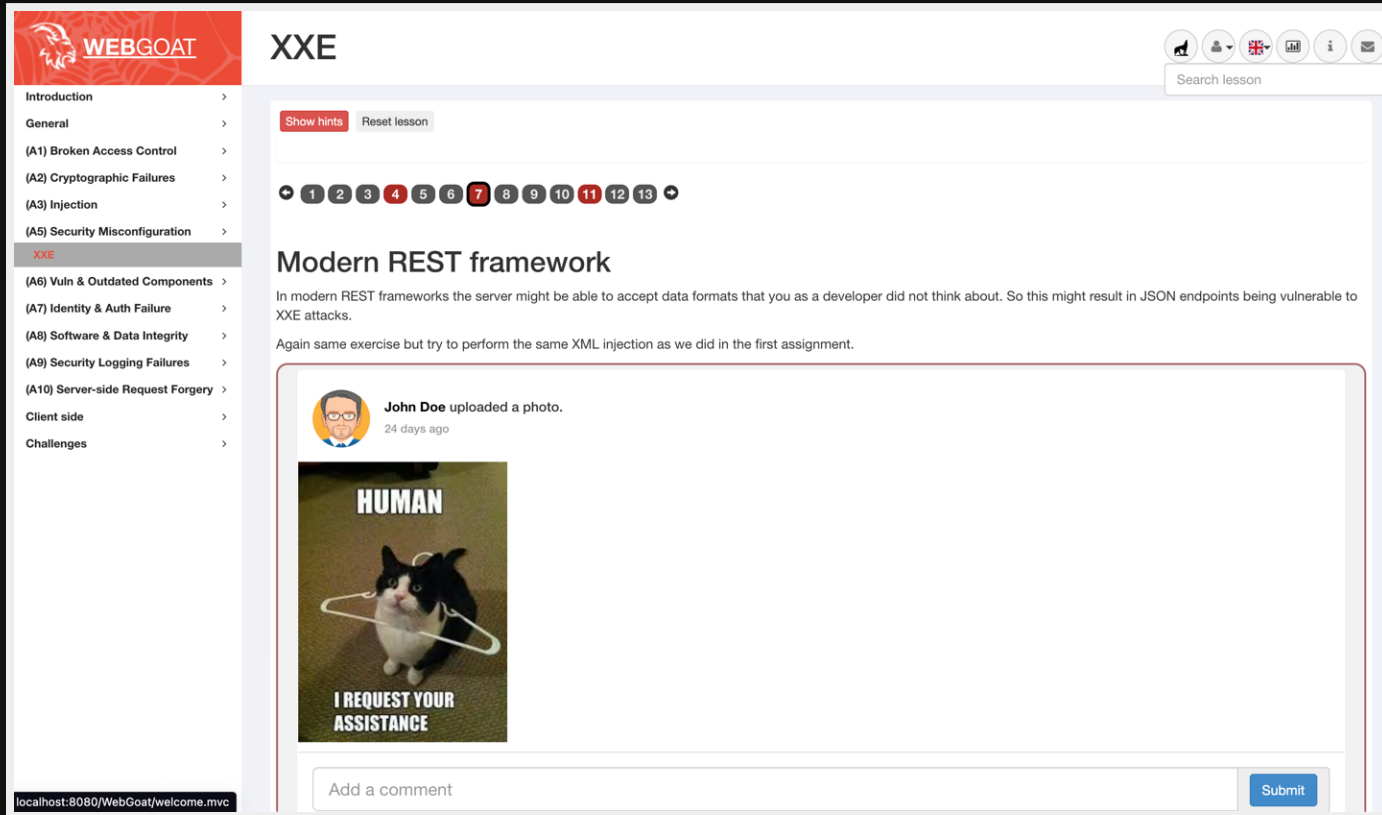
[Doodahs](#)
[Gizmos](#)
[Thingamajigs](#)
[Thingies](#)
[Whatchamacallits](#)
[Whatsits](#)
[Widgets](#)

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](#)

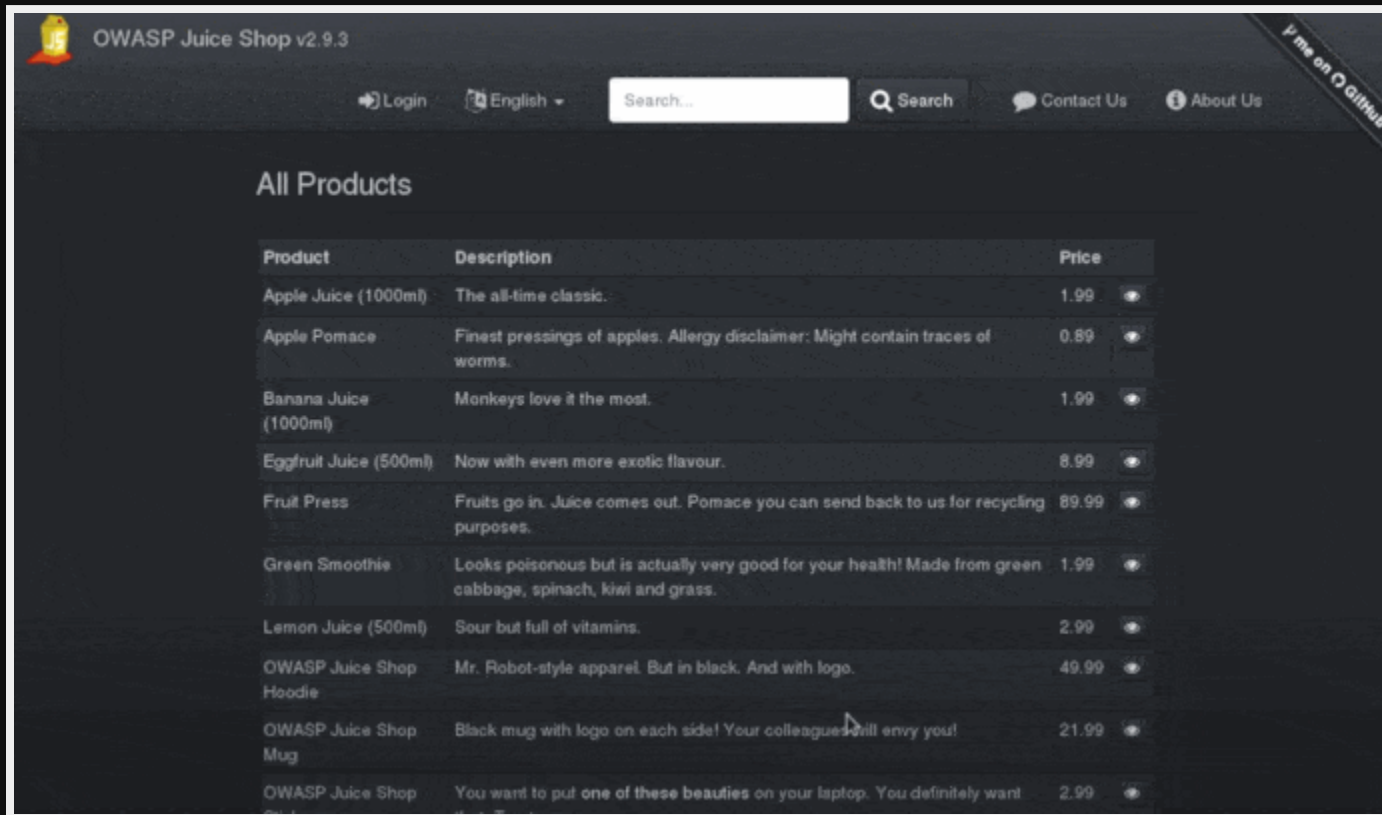
OWASP WebGoat Stars



The screenshot displays the OWASP WebGoat application interface. The top navigation bar includes the WebGoat logo and the title "XXE". A search bar is located in the top right corner. The left sidebar contains a menu with various sections, including "Introduction", "General", "(A1) Broken Access Control", "(A2) Cryptographic Failures", "(A3) Injection", "(A5) Security Misconfiguration", "XXE", "(A6) Vuln & Outdated Components", "(A7) Identity & Auth Failure", "(A8) Software & Data Integrity", "(A9) Security Logging Failures", "(A10) Server-side Request Forgery", "Client side", and "Challenges". The main content area shows a lesson titled "Modern REST framework" with a "Show hints" button and a "Reset lesson" button. A progress indicator shows 13 steps, with step 7 highlighted. The lesson text explains that modern REST frameworks can accept data formats not considered by developers, making JSON endpoints vulnerable to XXE attacks. It includes an exercise: "Again same exercise but try to perform the same XML injection as we did in the first assignment." Below the text is a social media post by "John Doe" from 24 days ago, featuring a meme of a black and white cat with a white hanger around its neck. The meme text reads "HUMAN" at the top and "I REQUEST YOUR ASSISTANCE" at the bottom. At the bottom of the page, there is a "Add a comment" input field and a "Submit" button. The URL in the bottom left corner is "localhost:8080/WebGoat/welcome.mvc".

Server-side rendered and lesson-based training application

Juice Shop

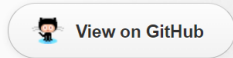
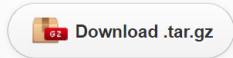
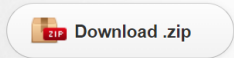


Rich Internet Application (RIA) designed for realism, manual exploration and hacking w/ or w/o pentesting tools

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

Log in

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

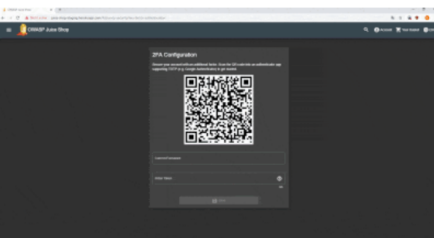
[Main](#) [Overview](#) [News](#) [Challenges](#) [Learning](#) [CTF](#) [Ecosystem](#) [Supporters](#)



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 \(GitHub\)](#)

But 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!

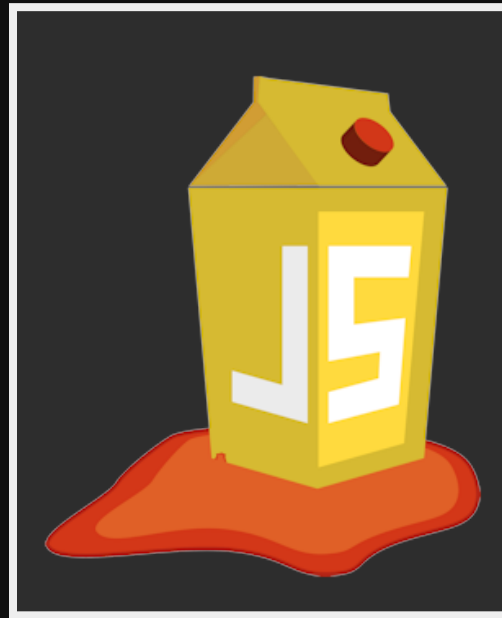
Logo Evolution

2014



Public Domain

2015



CC-BY 4.0

2017+



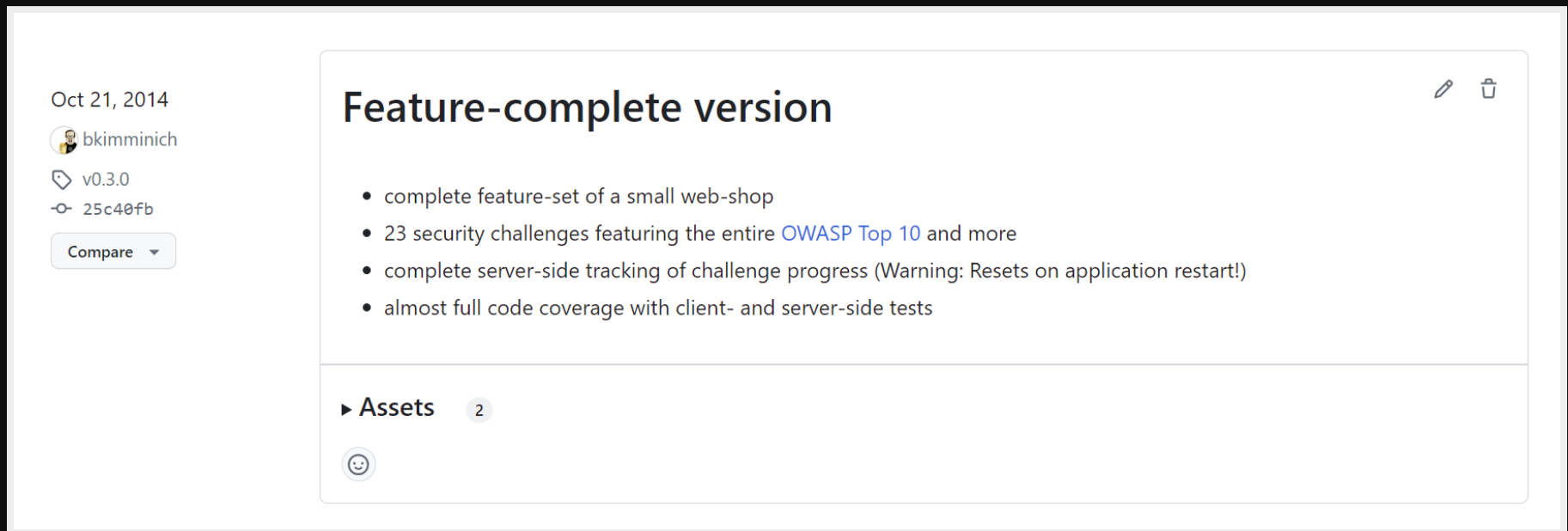
CC-BY 4.0




Chapter II


The Challenges


2014: 23 Hacking Challenges



Oct 21, 2014

 bkimminich

 v0.3.0


 25c40fb

[Compare](#)

Feature-complete version

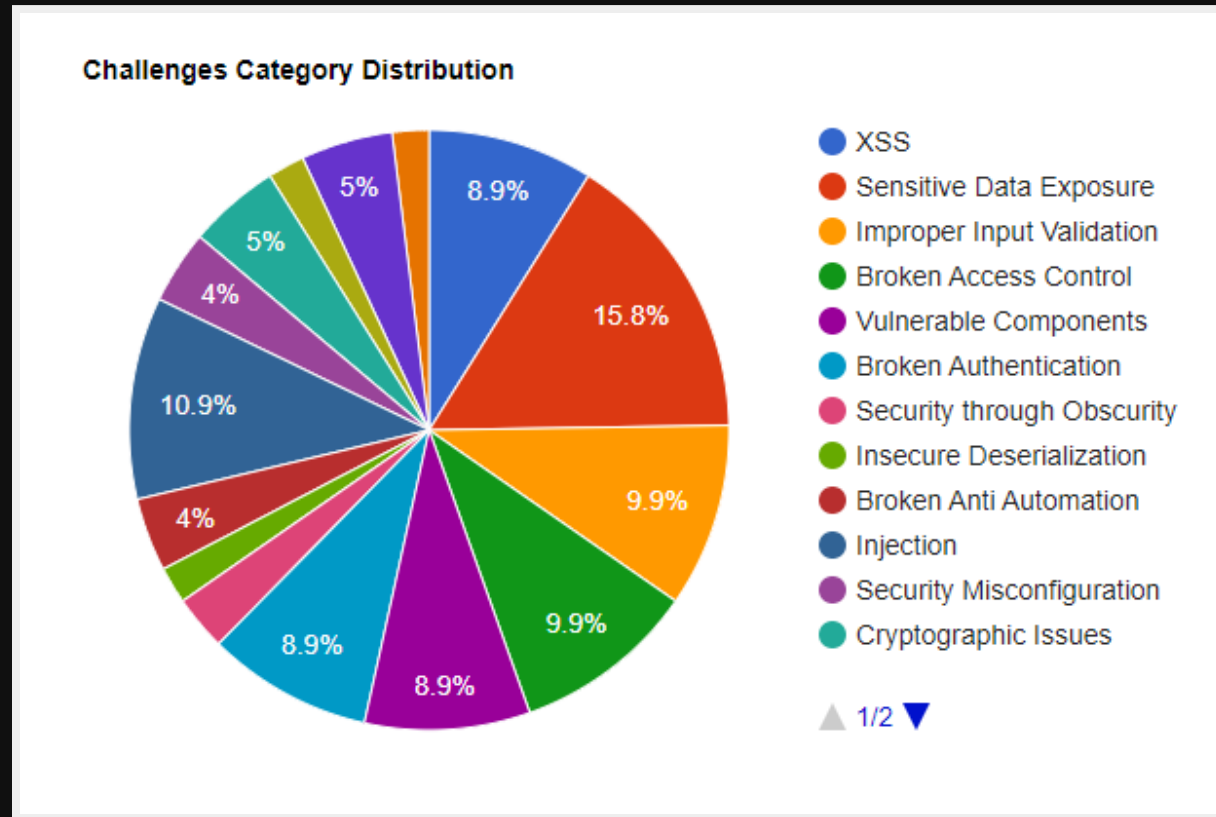
- complete feature-set of a small web-shop
- 23 security challenges featuring the entire [OWASP Top 10](#) and more
- complete server-side tracking of challenge progress (Warning: Resets on application restart!)
- almost full code coverage with client- and server-side tests

▶ **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: 102 Hacking Challenges



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

2014: 3 Difficulty Levels

Score Board		
<div style="background-color: #f4a460; width: 36%; height: 10px; margin-bottom: 5px;"></div>		
Description	Difficulty	Status
Find the carefully hidden "Score Board" page.	★	solved
Provoke an error that is not very gracefully handled.	★	solved
Log in with the administrator's user account.	★	solved
Log in with Jim's user account.	★★	unsolved
Log in with Bender's user account.	★★	unsolved
XSS Tier 1: Perform a reflected XSS attack with <code><script>alert("XSS1")</script></code> .	★	solved
XSS Tier 2: Perform a persisted XSS attack with <code><script>alert("XSS2")</script></code> bypassing a client-side security mechanism.	★★	unsolved
XSS Tier 3: Perform a persisted XSS attack with <code><script>alert("XSS3")</script></code> bypassing a server-side security mechanism.	★★★	unsolved
XSS Tier 4: Perform a persisted XSS attack with <code><script>alert("XSS4")</script></code> without using the frontend application at all.	★★	unsolved
Retrieve a list of all user credentials via SQL injection	★★	unsolved
Log in with the administrator's user credentials without previously changing them or applying SQL injection.	★	solved
Get rid of all 5-star customer feedback.	★	solved
Post some feedback in another user's name.	★★	unsolved
Wherever you go, there you are.	★★★	unsolved
Access someone else's basket.	★	unsolved
Place an order that makes you rich.	★★	unsolved
Access a confidential document.	★	unsolved
Access a forgotten backup file.	★★	solved
Access the administration section of the store.	★	solved
Change Bender's password into <code>sturmChissic</code> .	★★	unsolved
Change the link in the description of the O-Salt product to <code>http://imminish.de</code> .	★★	unsolved
Inform the shop about a vulnerable library it is using. (Mention the exact library name and version in your complaint.)	★★	solved
Find the hidden easter egg .	★★	unsolved
Apply some advanced cryptanalysis to find the real easter egg.	★★★	unsolved
Forge a coupon code that gives you a discount of at least 80%.	★★★	unsolved

2018: 6 Difficulty Levels

Score Board

3%

Difficulty

★ 1/7 ★ 2/8 ★ 3/13 ★ 4/15 ★ 5/10 ★ 6/6

★

Name	Description	Status
Admin Section	Access the administration section of the store.	unsolved
Confidential Document	Access a confidential document.	unsolved
Error Handling	Provoke an error that is not very gracefully handled.	unsolved
Redirects Tier 1	Let us redirect you to a donation site that went out of business.	unsolved
Score Board	Find the carefully hidden 'Score Board' page.	solved
XSS Tier 1	Perform a <i>reflected</i> XSS attack with <code><script>alert("XSS")</script></code>	unsolved
Zero Stars	Give a devastating zero-star feedback to the store.	unsolved

★★

Name	Description	Status
Basket Access	Access someone else's basket.	unsolved
Christmas Special	Order the Christmas special offer of 2014.	unsolved
Deprecated Interface	Use a deprecated B2B interface that was not properly shut down.	unsolved
Five-Star Feedback	Get rid of all 5-star customer feedback.	unsolved
Login Admin	Log in with the administrator's user account.	unsolved
Login MC SafeSearch	Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass.	unsolved
Password Strength	Log in with the administrator's user credentials without previously changing them or applying SQL Injection.	unsolved
Weird Crypto	Inform the shop about an algorithm or library it should definitely not use the way it does.	unsolved

★★★

Name	Description	Status
Blockchain Tier 1	Learn about the Token Sale before its official announcement.	unsolved
Forced Feedback	Post some feedback in another users name.	unsolved

2019: Categories & Filters

Score Board 5%



Show all

Show solved

- 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
- Show all

Name	Difficulty	Description	Category	Status
API-only XSS	★★★	Perform a <i>persisted</i> XSS attack with <code><iframe src="javascript:alert(`xss`)"></code> without using the frontend application at all.	XSS	solved
Classic Stored XSS	★★	Perform an XSS attack with <code><script>alert(`xss`)</script></code> on a legacy page within the application.	XSS	unsolved
Client-side XSS Protection	★★★	Perform a <i>persisted</i> XSS attack with <code><iframe src="javascript:alert(`xss`)"></code> bypassing a <i>client-side</i> security mechanism.	XSS	unsolved
DOM XSS	★	Perform a <i>DOM</i> XSS attack with <code><iframe src="javascript:alert(`xss`)"></code> .	XSS	solved
Database Schema	★★★	Exfiltrate the entire DB schema definition via SQL Injection.	Injection	unsolved
Login Admin	★★	Log in with the administrator's user account.	Injection	unsolved
Login Bender	★★★	Log in with Bender's user account.	Injection	unsolved
Login Jim	★★★	Log in with Jim's user account.	Injection	unsolved
Reflected XSS	★	Perform a <i>reflected</i> XSS attack with <code><iframe src="javascript:alert(`xss`)"></code> .	XSS	unsolved

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(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 🔓

Side by Side Line by Line

filterTable () {

```

1 1 filterTable () {
2 2   let queryParams: string = this.route.snapshot.queryParams.q
3 3   if (queryParams) {
4 4     queryParams = queryParams.trim()
5 5     this.dataSource.filter = queryParams.toLowerCase()
6 6     - this.searchValue = this.sanitizer.bypassSecurityTrustHtml(queryParam)
7 7     + this.searchValue = this.sanitizer.bypassSecurityTrustScript(queryParam)
8 8     this.gridDataSource.subscribe((result: any) => {
9 9       if (result.length === 0) {
10 10        this.emptyState = true
11 11        } else {
12 12          this.emptyState = false
13 13        }
14 14      })
15 15    } else {
16 16      this.dataSource.filter = ''
17 17      this.searchValue = undefined
18 18      this.emptyState = false
19 19    }
20 20  }

```

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 27 challenges

2023: The current Score Board

The screenshot displays the 'Score Board' interface for the year 2023. At the top, it shows a progress bar for 'Score Board' at 21% and 'Coding Score' at 0%. Below this, there are navigation buttons for difficulty levels (1-6) and filters for 'Show solved', 'Show tutorials only', and 'Show unavailable'. A category filter bar is visible, listing various security topics like 'Broken Access Control', 'Broken Anti Automation', etc. The main content is a table of challenges.

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	👍👎
Bjoern's Favorite Pet	★★★	Reset the password of Bjoern's OWASP account via the <i>Forgot Password</i> mechanism with the original 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/ap1.soundcloud.com/tracks/771984676&color=323ff550&auto_play=true&hide_reXSS"></iframe></code> in the DOM XSS 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>slurmCl@ssic</i> without using SQL Injection or Forgot Password.	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	★★★★★	Stick <i>cute cross-domain kittens</i> all over our delivery boxes.	Security Misconfiguration	Contraption	unsolved	
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	
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	

2023: Redesign from scratch

The screenshot shows the OWASP Juice Shop score board for XSS challenges. The browser address bar shows the URL: localhost:3000/#/score-board-preview?categories=XSS. The page header includes the OWASP Juice Shop logo, a search icon, and links for Account, Your Basket, and EN. The main content area displays progress for Hacking Challenges (11%), Coding Challenges (6%), and Challenges Solved (14/156). A search bar and filters for Difficulty, Status, and Tags are present. A category filter bar shows 'XSS' selected, along with other categories like 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 challenge list includes:

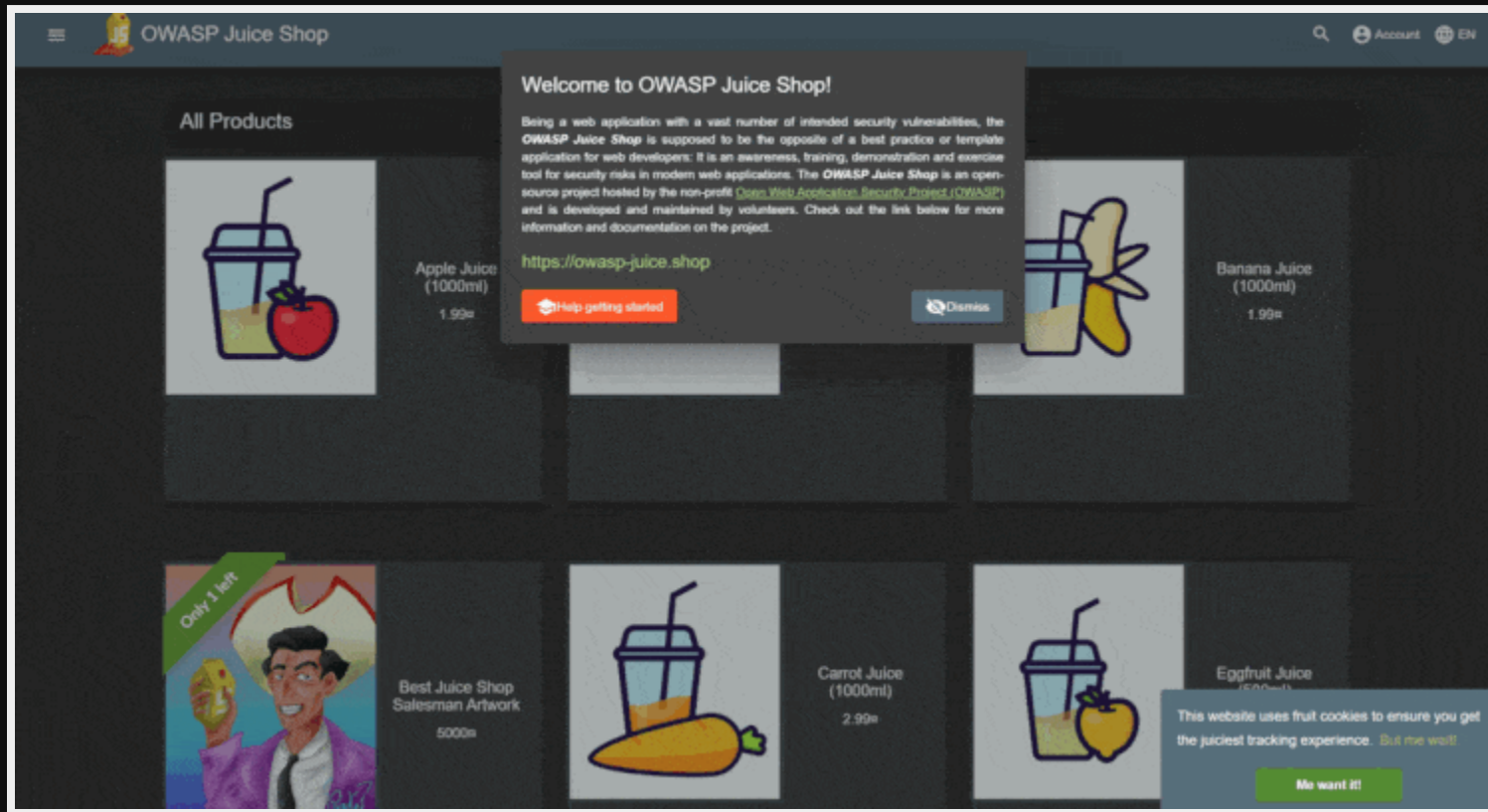
- API-only XSS** (★★★): Perform a *persisted* XSS attack with `<iframe src="javascript:alert('xss')">` without using the frontend application at all. (Danger Zone, Hint)
- Bonus Payload** (★): `hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true"></iframe>` in the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



Chapter III

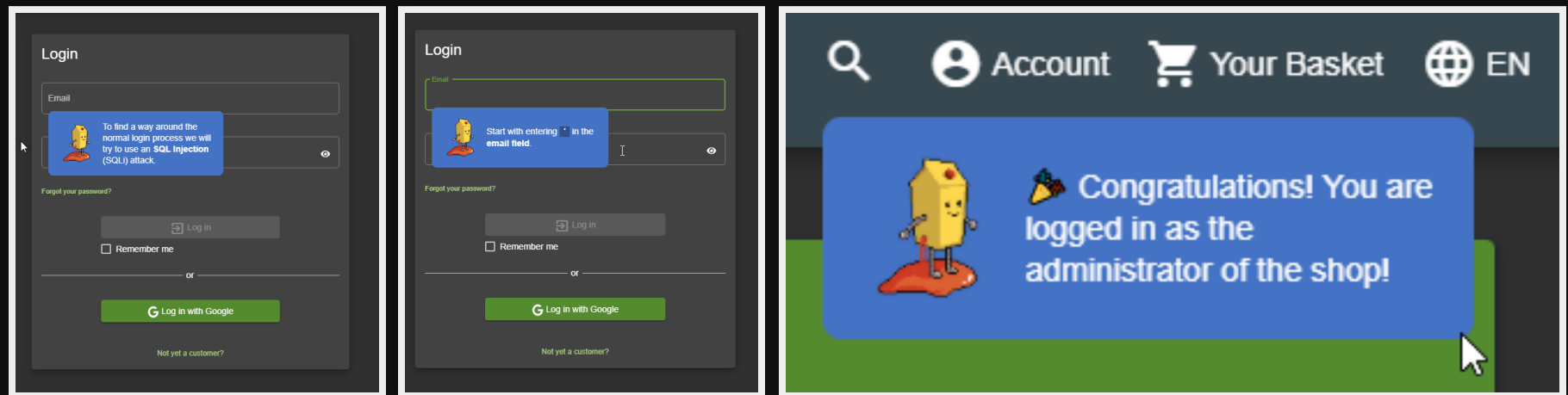
The Features

Realistic Fake Webshop



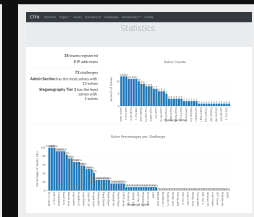
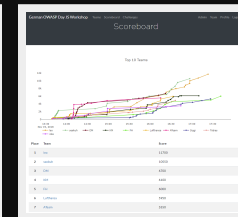
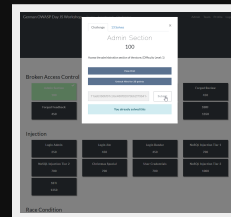
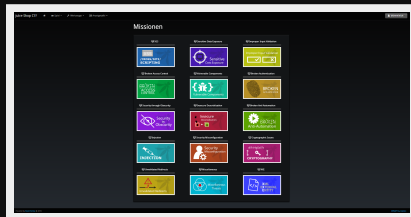
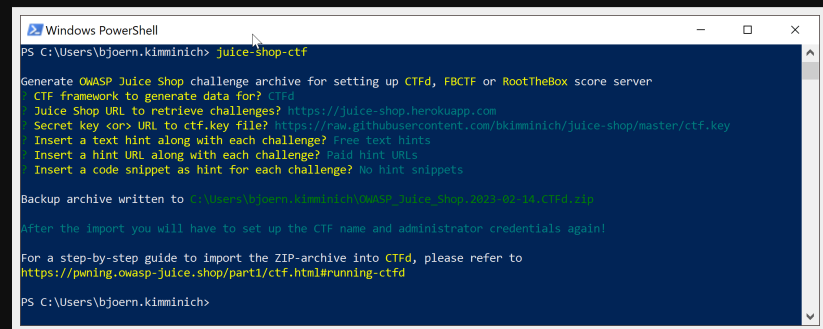
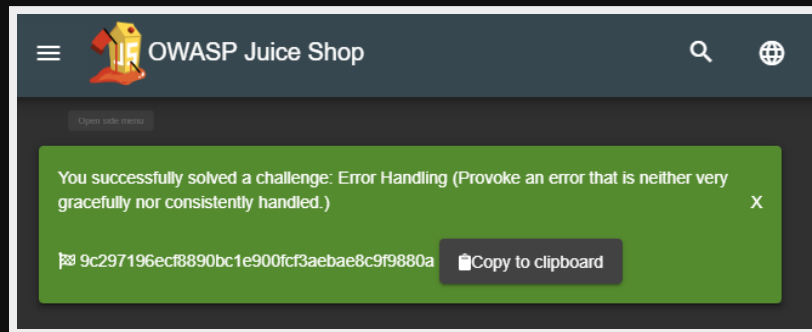
Juice Shop offers not only the full online shopping use case but also user profile management, 2FA, product reviews, customer services, chatbot assistance, user photo stories and much more

Hacking Instructor



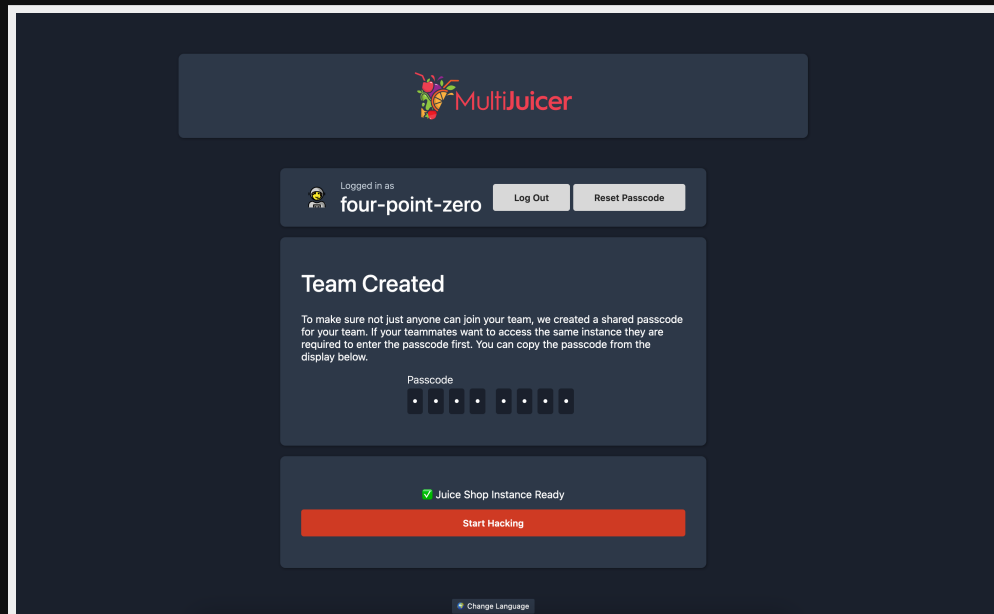
Several challenges come with an embedded interactive tutorial helping newcomers to get going

Sophisticated CTF-support

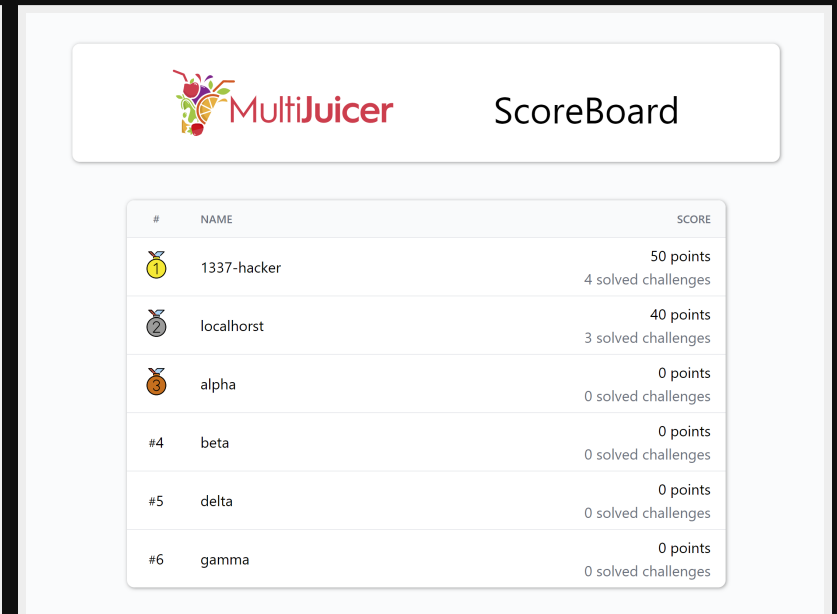


Built-in flag notifications and official **juice-shop-ctf-cli** help setting up hacking events on **CTFd**, **FBCTF** or **RootTheBox** conveniently

MultiJuicer Platform



The screenshot shows the MultiJuicer user interface. At the top, the MultiJuicer logo is displayed. Below it, the user is logged in as 'four-point-zero'. There are 'Log Out' and 'Reset Passcode' buttons. A 'Team Created' message is shown, indicating that a shared passcode has been generated for the team. The passcode is displayed as a series of dots. Below the passcode, there is a green checkmark and the text 'Juice Shop Instance Ready', followed by a red 'Start Hacking' button. At the bottom, there is a 'Change Language' link.

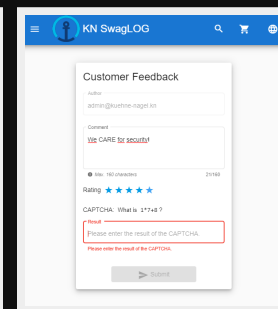
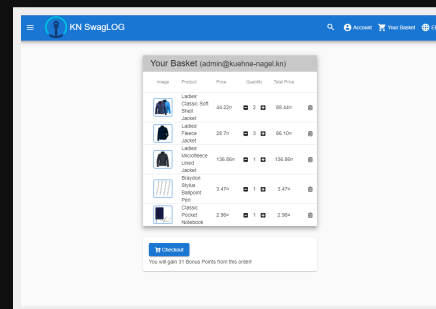
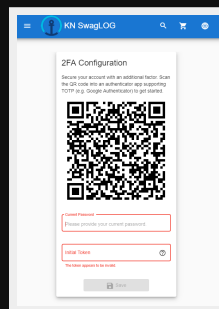
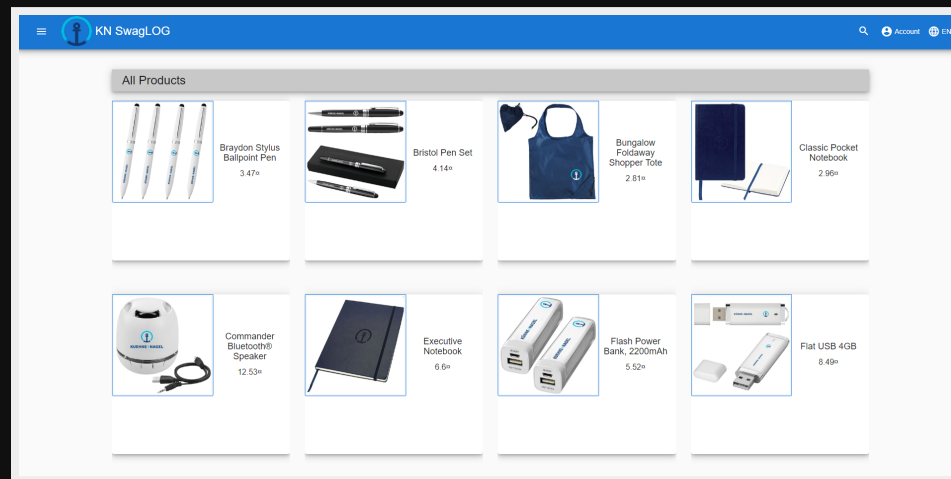


The screenshot shows the MultiJuicer ScoreBoard. At the top, the MultiJuicer logo is displayed next to the title 'ScoreBoard'. Below the title is a table with the following data:

#	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

Official platform to run isolated Juice Shop instances for training or CTF participants on a central Kubernetes cluster

Theming & Re-branding



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

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
```

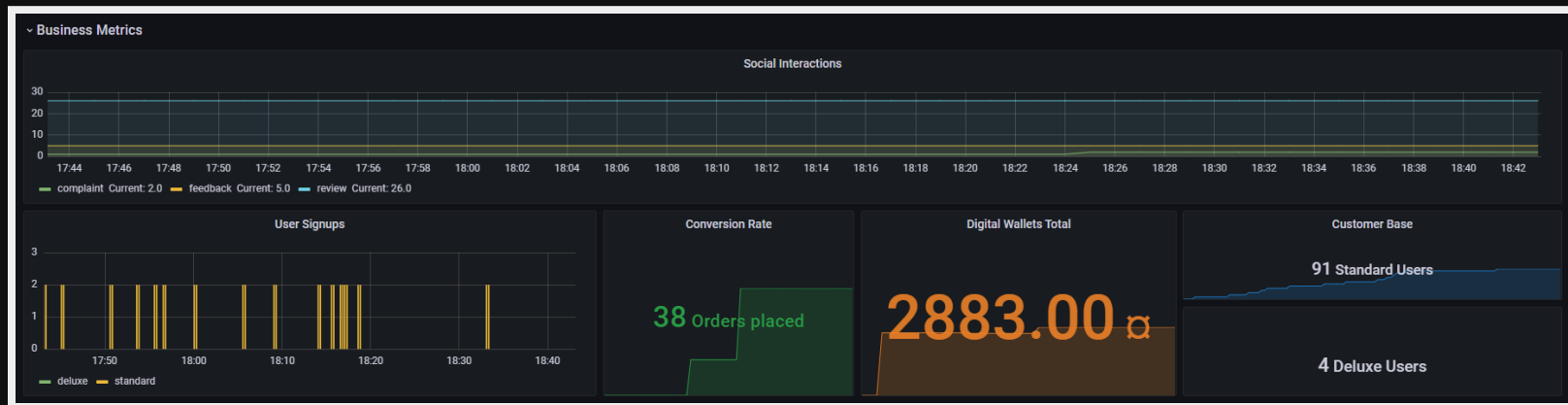
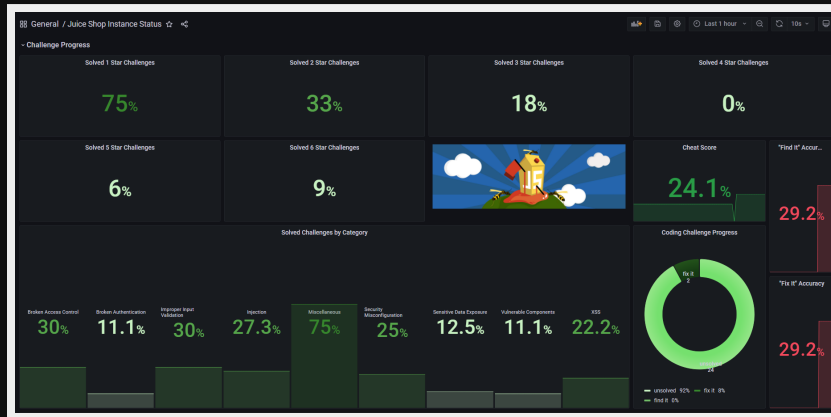
Solved challenges are rated based on cheating probability

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

Grafana Dashboard



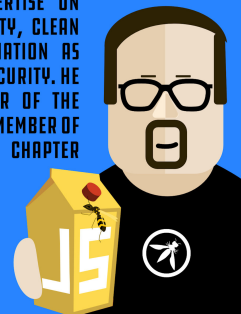
JSON template allows to import a dashboard into Grafana consuming and displaying all metrics gathered via Prometheus

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

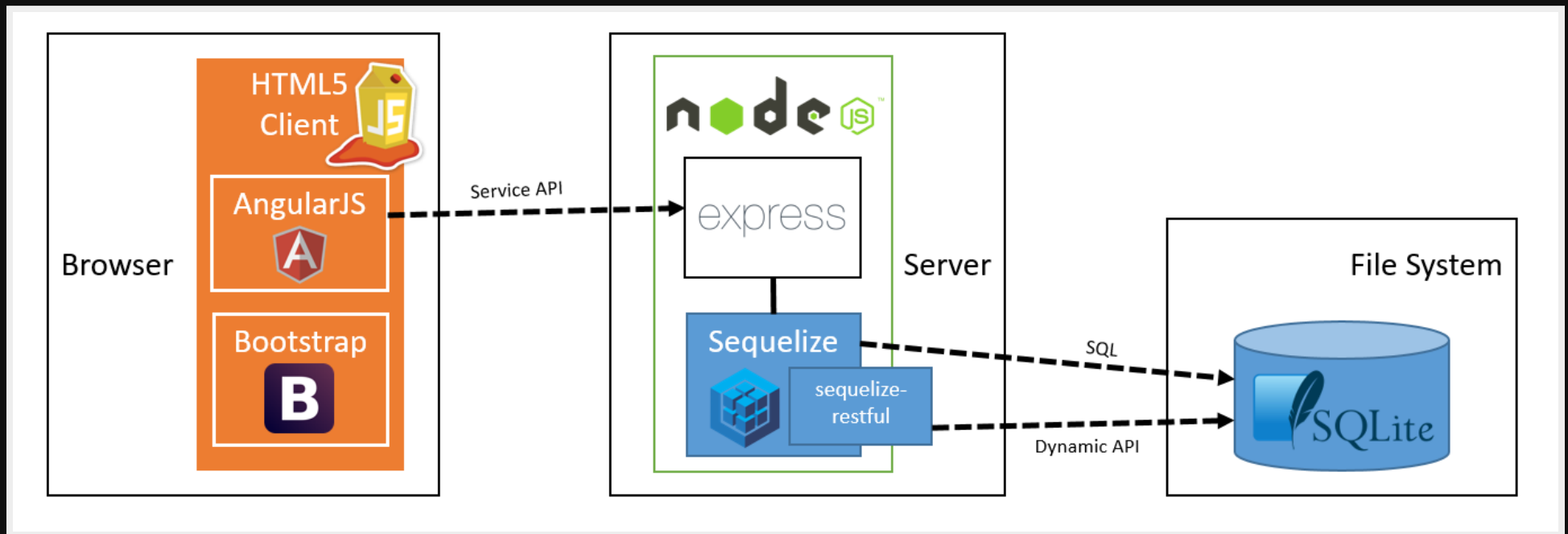
The **free** official companion guide is available **on Leanpub** and can also be **read online**



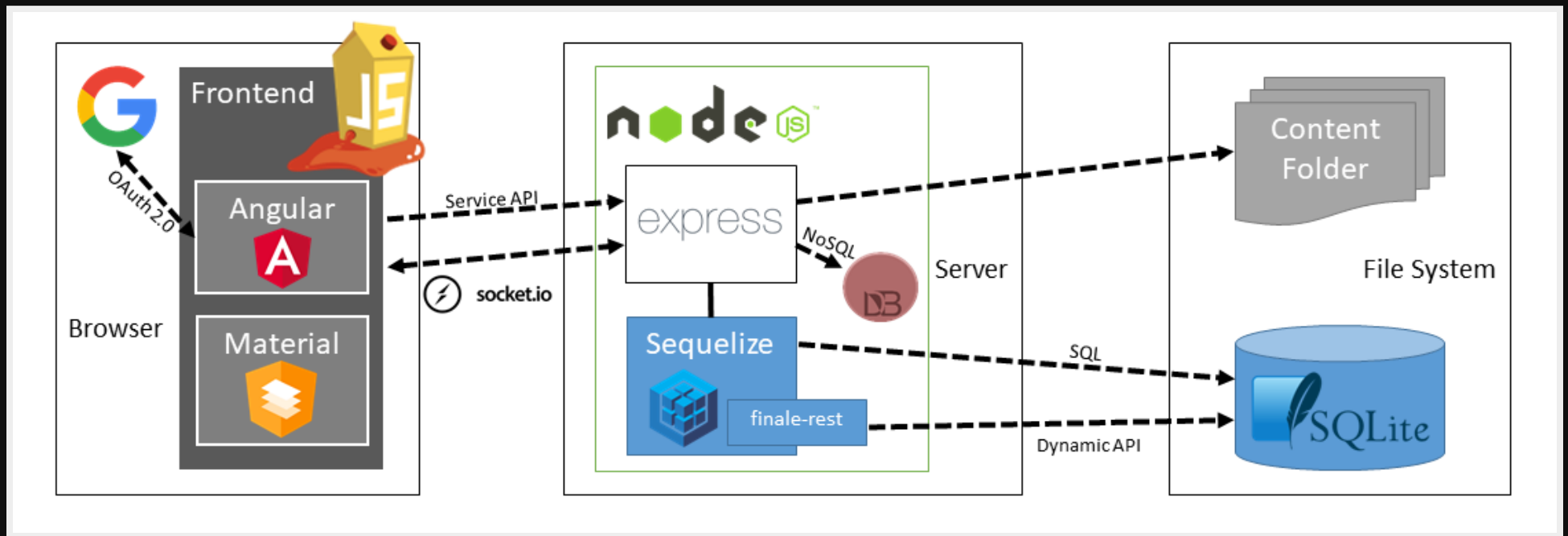
Chapter IV

The Technology

2014: "Bleeding-edge" Web-Architecture



2023: "Still-modern" Web-Architecture



Simple Installation



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



Chapter V

The Community

Core Team

Björn
Kimminich

Jannik
Hollenbach

Shubham
Palriwala

Timo
Pagel



Björn Kimminich's GitHub Stats

☆ Total Stars Earned: 559
🕒 Total Commits (2023): 721
👤 Total PRs: 730
🔍 Total Issues: 533
📅 Contributed to (last year): 25

A+

Jannik Hollenbach's GitHub Stats

☆ Total Stars Earned: 46
🕒 Total Commits (2023): 303
👤 Total PRs: 491
🔍 Total Issues: 145
📅 Contributed to (last year): 13

A-

Shubham Palriwala's GitHub Stats

☆ Total Stars Earned: 53
🕒 Total Commits (2023): 283
👤 Total PRs: 245
🔍 Total Issues: 140
📅 Contributed to (last year): 19

A-

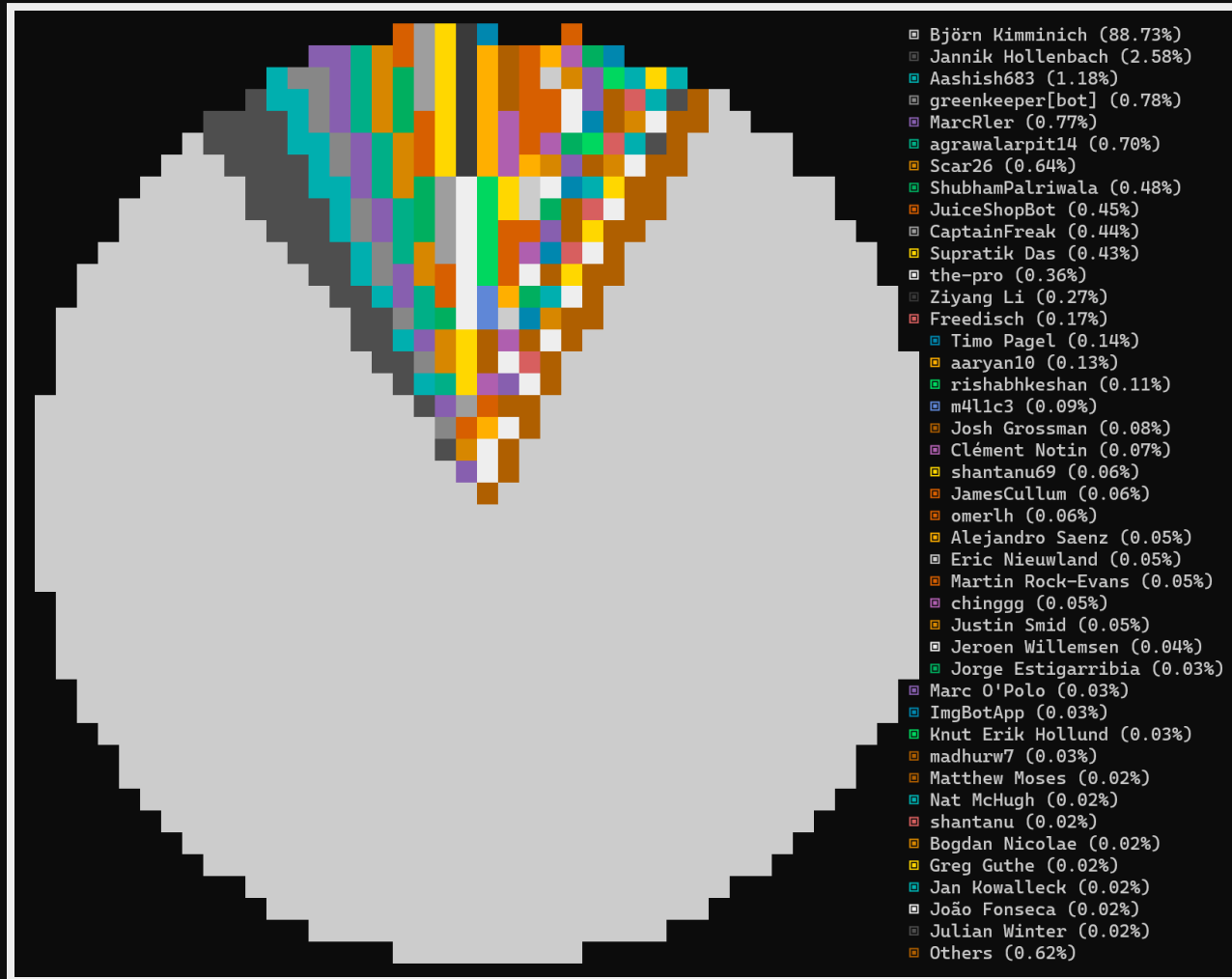
Timo Pagel's GitHub Stats

☆ Total Stars Earned: 503
🕒 Total Commits (2023): 352
👤 Total PRs: 315
🔍 Total Issues: 140
📅 Contributed to (last year): 12





















A+

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

Contributions are welcome!



Visit our [backlog on GitHub](#) & [translations on Crowdin](#). Issues labelled with [good first issue](#) and/or [help wanted](#) are the best starting point for new contributors

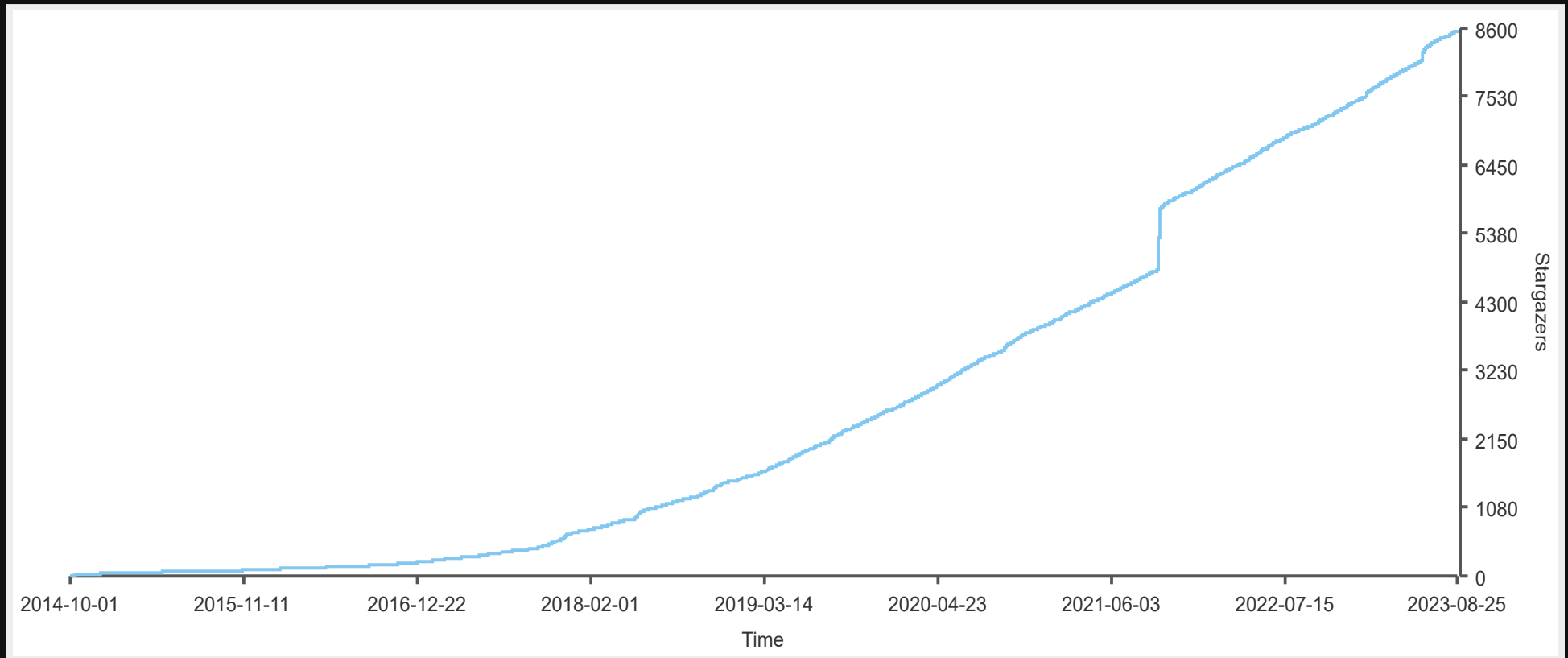
Vennligst hjelp med å få den norske oversettelsen over dagens nivå på 15%!

Contribution Rewards



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

GitHub Stars over time



Quiz: What might have caused the upward spike in 2021?

!ykb n rj7 duHjiθ no "tgnibnθrj" saw qohz θiut

Juice Shop Success Pyramid™

contributors 95

owasp flagship project

code style standard

openssf best practices gold

test coverage 87%

maintainability A

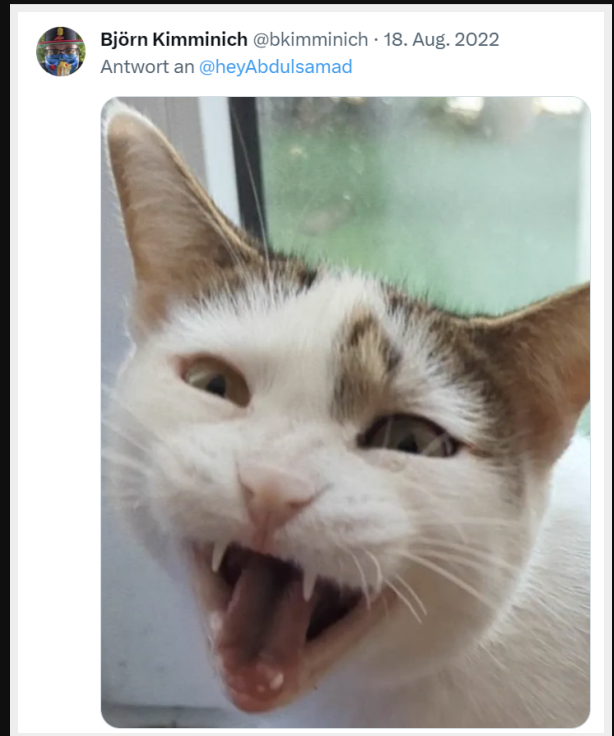
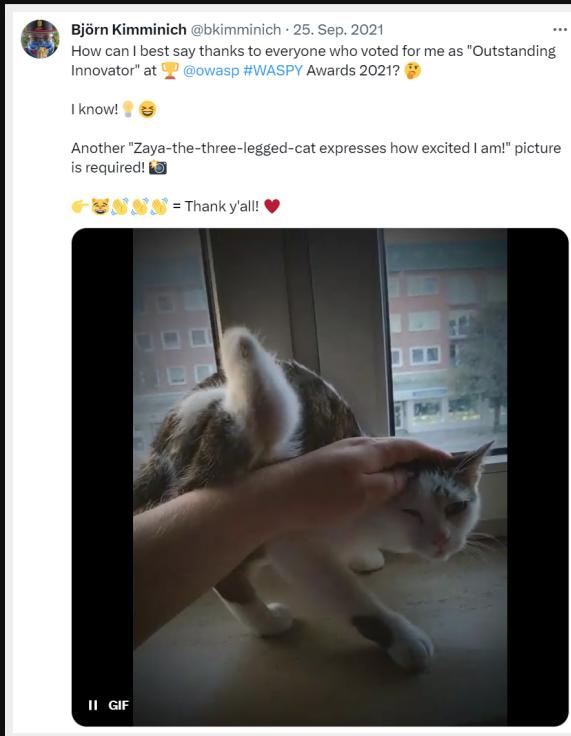
GitHub ★ 8.6k

downloads 223k

docker pulls 80M

sourceforge downloads 52k

2018: Official Project Pet



One of the many "social stalking" challenges in Juice Shop is about finding out the name of Björn's family cat.

2020: Official Jingle



[braimee](#)

OWASP Juice Shop Jingle

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 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)

And they all participated in GSoC happily ever after...

GSoC 2023: Web3 Challenges

The screenshot displays the OWASP Juice Shop interface. At the top, the header includes a hamburger menu, the OWASP Juice Shop logo, and navigation links for search, account, and language (EN). The main content area is divided into two columns. The left column features the 'BEE Haven' challenge, which includes an illustration of a bee and a yellow truck labeled 'BEEES'. Below the illustration, a welcome message reads: 'Welcome to Bee Haven, the hive of BEE tokens! Immerse yourself in the buzz as our generous Bee Owner shares the joy of bees with you. Embrace their bountiful generosity, but remember, taking too many bees at once may disrupt their harmonious abode.' A status bar shows 'Faucet Balance: 0 | Your BEE Balance: 0' and a green 'Connect your MetaMask' button. Below this is an input field for 'Enter no. of BEEs:' and a blue 'Claim BEEs' button. The right column features 'The Enchanted Honey Pot' challenge, with an illustration of a glowing pot and a bee. The text below reads: 'Deep within the magical realm, the Enchanted Honey Pot awaits its rightful owner. To unlock its wonders, you must trade the essence of the buzzing kingdom - BEE tokens. Gather these mystical tokens from the generous Bee Haven.' An orange 'Mint the Pot - 1000 BEE' button is positioned at the bottom of this section. A notification banner at the bottom of the interface states: 'Please install a Web3 Wallet like Metamask to proceed. X'

Rishabh Keshan has designed and implemented several amazing challenges around typical Web3 security flaws.

GSoC 2023: Antora eBook

The screenshot shows a web page for "Pwning OWASP Juice Shop" rendered in Antora format. The page has a dark header with a search bar and navigation links. The main content area is titled "Challenge tracking" and "The Score Board". It contains two paragraphs of text and a screenshot of the application's score board interface. The score board shows a list of challenges with their difficulty levels, descriptions, and completion status. The right sidebar contains a "Contents" menu with links to various sections of the book.

Pwning OWASP Juice Shop

Search the docs

Pwning OWASP Juice Shop / Part I - Hacking preparations / Challenge tracking

Challenge tracking

The Score Board

In order to motivate you to hunt for vulnerabilities, it makes sense to give you at least an idea what challenges are available in the application. Also, you should know when you actually solved a challenge successfully, so you can move on to another task. Both these cases are covered by the application's score board.

On the score board you can view a list of all available challenges with a brief description. Some descriptions are *very explicit* hacking instructions. Others are just *vague hints* that leave it up to you to find out what needs to be done.

Name	Difficulty	Description	Category	Tag	Notes	Feedback
Admin Section	☆☆	Access the administration section of the shop.	Broken Access Control	Goal for DevSec	Green	Feedback
Blockchain Page	☆☆☆☆	Learn about the Bitcoin blockchain by official announcement.	Security Through Obscurity	Goal for DevSec	Green	Feedback
Hidden Payload	☆	Use the hidden payload (CVE-2019-1328) to get the "Goal for DevSec" flag.	OSINT	Goal for DevSec	Green	Feedback
Daily Challenge	☆	Receive a custom code from the support staff.	Miscellaneous	Goal for DevSec	Green	Feedback
Change Vendor's Password	☆☆☆☆	Change vendor's password into admin/cred without using SQL Injection or Forgot Password.	Broken Authentication	Goal for DevSec	Green	Feedback
Confidential Document	☆	Access a confidential document.	Sensitive Data Exposure	Goal for DevSec	Green	Feedback
Cross Site Scripting	☆☆☆☆	Inject a custom payload into the admin board.	Security Misconfigurations	Goal for DevSec	Green	Feedback

Desktop anzeigen

Parth Nanda has tirelessly migrated the entire "Pwning OWASP Juice Shop" guide from Markdown/GitBook to AsciiDoc/Antora.



Epilogue

Project Roadmap

Move **Pwning OWASP Juice Shop** eBook away from legacy gitbook (GSoC 2023 Project w/ Parth Nanda)

Add Web3 specific hacking and coding challenges (GSoC 2023 Project w/ Rishabh Keshan)

Renovate the Score Board for best possible user experience (**Preview branch**)

Enhance precision of cheat detection with new data sources and algorithms

Bring **overall test coverage** back over 90%+

Sell NFT collection ⇒ ₪:€ \$UÇ€\$\$



The End...?

To be continued...!

