

News from the Juice Shop ecosystem



German OWASP Day 2025

by **Björn Kimminich** / [@bkimminich.bsky.social](https://bsky.app/profile/bkimminich.bsky.social)

<https://owasp-juice.shop>

Star 12,065

Fork 15,502

[Follow @owasp_juiceshop](#) 118

[bluesky Follow](#)

[Follow r/owasp_juiceshop](#) 451

Like 943

[Follow @owasp_juiceshop](#)

OWASP JUICE SHOP

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!



Customer Testimonials



DSCHADOW

The most trustworthy online shop out there.



SHEHACKSPURPLE

The best juice shop on the whole internet!



VANDERAJ

Actually the most bug-free vulnerable application in existence!



<http://owasp-juice.shop>

[@owasp_juiceshop](https://twitter.com/owasp_juiceshop)

JUICE SHOP CTF Extension



The Node package *juice-shop-ctf-cli* helps you to prepare Capture the Flag events with the OWASP Juice Shop challenges for different popular CTF frameworks. This interactive utility allows you to populate a CTF game server in a matter of minutes.

<http://ctf.owasp-juice.shop>



Main selling points

FREE

[http://ebook!
owasp-juice.shop](http://ebook!owasp-juice.shop)



- Free and Open source: Licensed under the MIT license with no hidden costs or caveats
- 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
- Self-healing: The simple SQLite and MarsDB databases are wiped and repopulated from scratch on every server startup
- Gamification: The application notifies you on solved challenges and keeps track of successfully exploited vulnerabilities on a Score Board
- Re-branding: Fully customizable in business context and look & feel to your own corporate or customer requirements
- CTF-support: Challenge notifications optionally contain a flag code for your own Capture-The-Flag events



<http://owasp-juice.shop> | [@owasp_juiceshop](https://twitter.com/owasp_juiceshop)

Juice Shop Success Pyramid™

Some amazing facts & stats about the project

contributors 130

owasp flagship project

code style standard

openssf best practices gold

coverage 85%

cy tests passed

maintainability B

GitHub ★ 12k

Forks 16k

downloads 421k

sourceforge downloads 87k

docker pulls 84M

New Challenges



Leaked API Key

Juice Shop uses this behind the scenes

Sensitive Data Exposure

Leaked API Key



Inform the shop about a leaked API key. (Mention the exact key in your comment)

0/4



Memory Bomb

It's a bit like XXE^{*}, only with YAML

The screenshot shows a challenge interface for 'Memory Bomb' under the category 'Insecure Deserialization'. The challenge is rated with five stars. The description reads: 'Drop some explosive data into a vulnerable file-handling endpoint. (This challenge is potentially harmful on Heroku!)'. At the bottom left, there is a 'Danger Zone' label. At the bottom right, there is a red circle with a white exclamation mark and a green circle with a white question mark and the text '0/3'.

*= It's also just as dangerous as XXE, so the challenge is turned off by default on the public demo server and when running Juice Shop in Docker or on Heroku.

New Category: Observability Failures

Groups all challenges related to OWASP Top 10 **A9:2025**

The image shows a screenshot of a challenge interface with four cards. Each card has a title, a description, and a progress indicator. The cards are: 1. 'Exposed Metrics' (1 star, 0/3 progress, tags: Good Practice, With Coding Challenge). 2. 'Access Log' (4 stars, 0/5 progress, tag: With Coding Challenge). 3. 'Misplaced Signature File' (5 stars, 0/3 progress, tags: Good Practice, Contraption). 4. 'Leaked Access Logs' (5 stars, 0/4 progress, tag: OSINT).

Challenge Title	Stars	Progress	Tags
Exposed Metrics	★	0/3	Good Practice, With Coding Challenge
Access Log	★★★★	0/5	With Coding Challenge
Misplaced Signature File	★★★★★	0/3	Good Practice, Contraption
Leaked Access Logs	★★★★★	0/4	OSINT

Category Mapping 2025

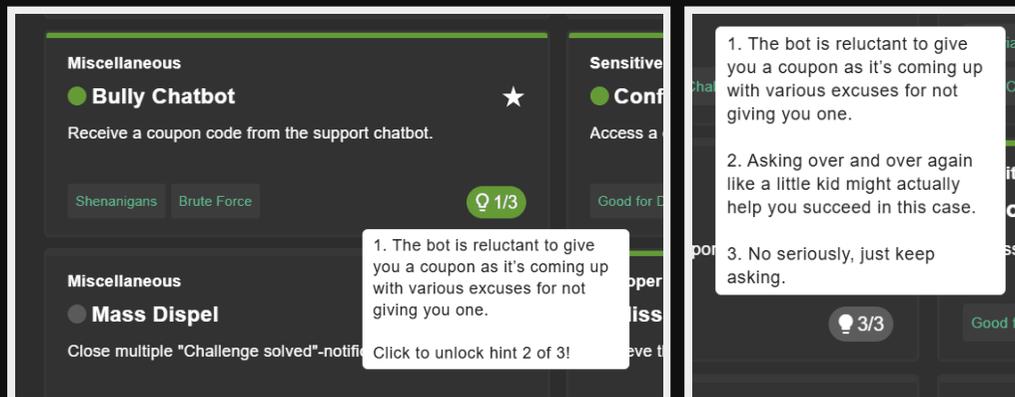
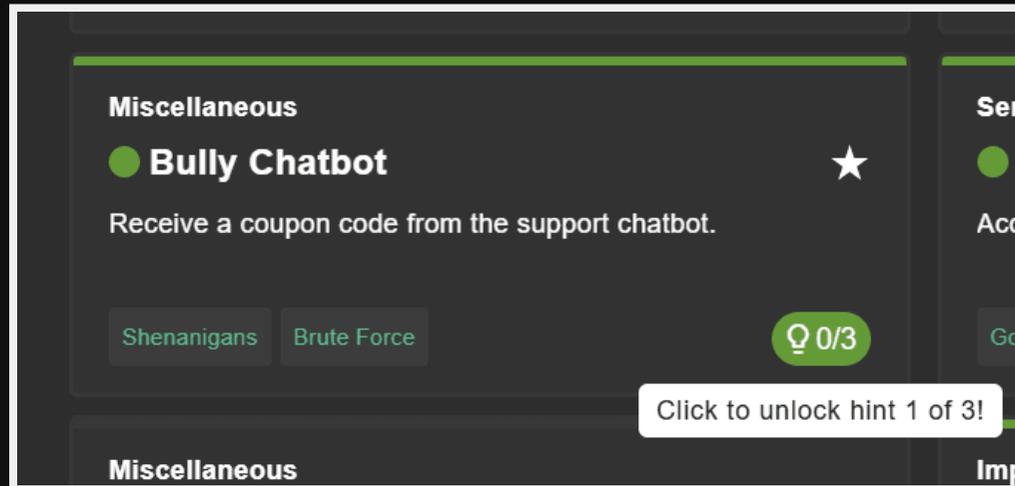
Juice Shop is 100% incompliant with the OWASP TOP 10:2025 RC

Category	Mappings	Category	Mappings
Broken Access Control	A1:2025 , A6:2025 , A1:2021 , API1:2019, API5:2019, CWE-22, CWE-285, CWE-639, CWE-918, WASC-02, WASC-09, WASC-16	Broken Anti-Automation	A6:2025 , OWASP-AT-004, API4:2019, OWASP-AT-010, OAT-009, OAT-015, OAT-008, CWE-362, WASC-11, WASC-21
Broken Authentication	A7:2025 , A6:2025 , A7:2021 , API2:2019, P6:2021, CWE-287, CWE-352, WASC-01, WASC-49	Cryptographic Issues	A4:2025 , A2:2021 , CWE-326, CWE-327, CWE-328, CWE-950
Improper Input Validation	ASVS V5, API6:2019, CWE-20, WASC-20	Injection	A5:2025 , A3:2021 , API8:2019, P1:2021, CWE-74, CWE-89, WASC-19, WASC-28, WASC-31
Insecure Deserialization	A8:2025 , A8:2021 , A8:2017 , CWE-502	Miscellaneous	P5:2021
Observability Failures	A9:2025 , A9:2021 , CWE-778	Security Misconfiguration	A2:2025 , A10:2025 , A5:2021 , API7:2019, API9:2019, API10:2019, CWE-209, WASC-14, WASC-15
Sensitive Data Exposure	A3:2017 , API3:2019, OTG-CONFIG-004, P2:2021, CWE-200, CWE-530, CWE-548, WASC-13	Vulnerable Components	A3:2025 , A6:2021 , CWE-1104
XML External Entities (XXE)	A2:2025 , A5:2021 , A4:2017 , CWE-611, WASC-43	Cross Site Scripting (XSS)	A5:2025 , A3:2021 , A7:2017 , CWE-79, WASC-08

Other Features

Multiple Challenge Hints

All challenges now come with one or more unlockable hints



Auto-sync with eBook

Juice Shop and its Companion Guide use the same YAML data source

The screenshot shows the OWASP Juice Shop documentation website. The header includes the OWASP Juice Shop logo and a search bar. The breadcrumb trail indicates the current page is 'Pwning OWASP Juice Shop / Part II - Challenge hunting / Miscellaneous'. The left sidebar contains a table of contents with categories like Preface, Part I - Hacking preparations, and Part II - Challenge hunting. The main content area features a challenge titled 'Receive a coupon code from the support chatbot'. The challenge description states: 'This challenge is about nagging the support chatbot to hand out a coupon code that can subsequently be used to get a discount during the checkout process.' A list of instructions follows, with the first one highlighted in blue: 'The bot is reluctant to give you a coupon as it's coming up with various excuses for not giving you one.' Other instructions include 'Asking over and over again like a little kid might actually help you succeed in this case.' and 'No seriously, just keep asking.' Below this is another challenge titled 'Close multiple "Challenge solved"-notifications in one go'. Its description says: 'This "challenge" is nothing more than an opportunity to learn about a convenience feature that allows users to close multiple "Challenge solved"-notifications at once.' Instructions for this challenge include: 'Either check the official documentation or inspect a notification UI element directly.' and 'This challenge is most easily solvable immediately after a server restart.' A right sidebar contains a 'Contents' section with links to various pages like 'Receive a coupon code from the support chatbot', 'Close multiple "Challenge solved"-notifications in one go', 'Read our privacy policy', 'Find the carefully hidden "Score Board" page', 'The Juice Shop is susceptible to a known vulnerability in a library for which an advisory has already been issued', 'Behave like any "white hat" should before getting into the action', and 'Withdraw more ETH from the new wallet than you deposited'.

OWASP Juice Shop

Search the docs

Pwning OWASP Juice Shop / Part II - Challenge hunting / Miscellaneous

Receive a coupon code from the support chatbot

This challenge is about nagging the support chatbot to hand out a coupon code that can subsequently be used to get a discount during the checkout process.

- The bot is reluctant to give you a coupon as it's coming up with various excuses for not giving you one.
- Asking over and over again like a little kid might actually help you succeed in this case.
- No seriously, just keep asking.

Close multiple "Challenge solved"-notifications in one go

This "challenge" is nothing more than an opportunity to learn about a convenience feature that allows users to close multiple "Challenge solved"-notifications at once.

- Either check the official documentation or inspect a notification UI element directly.
- This challenge is most easily solvable immediately after a server restart.

Alternatively you can also inspect any "Challenge solved" notification in your browser to understand

Contents

- Receive a coupon code from the support chatbot
- Close multiple "Challenge solved"-notifications in one go
- Read our privacy policy
- Find the carefully hidden 'Score Board' page
- The Juice Shop is susceptible to a known vulnerability in a library for which an advisory has already been issued
- Behave like any "white hat" should before getting into the action
- Withdraw more ETH from the new wallet than you deposited

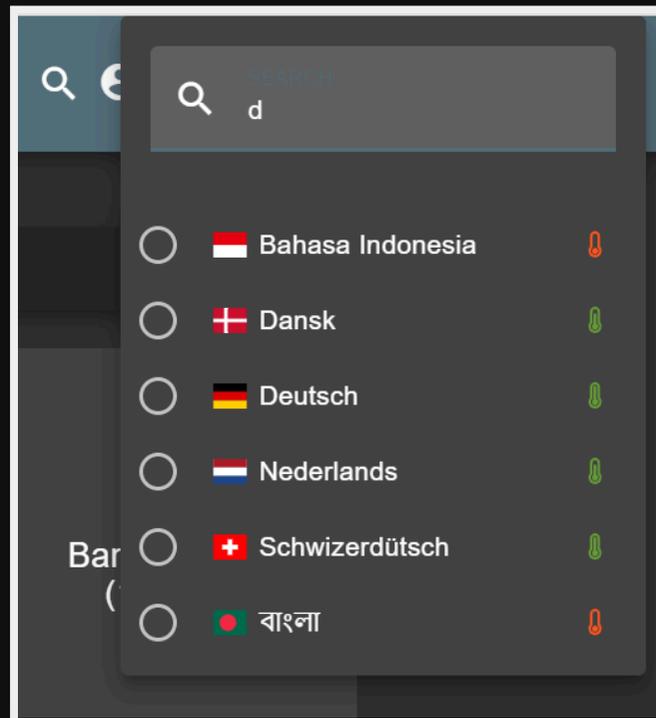
Solution Webhook also tracks hints

Number of available and used hints is part of the payload

```
{
  "solution": {
    "challenge": "localXssChallenge",
    "hintsAvailable": 2, // <-- new
    "hintsUnlocked": 0, // <-- new
    "cheatScore": 0,
    "totalCheatScore": 0.15,
    "issuedOn": "2025-09-04T18:24:33.027Z"
  },
  "ctfFlag": "b0d70dce...b85fac6785dba2349b",
  "issuer": {
    "hostName": "fv-az116-673",
    "os": "Linux (5.4.0-1031-azure)",
    "appName": "OWASP Juice Shop",
    "config": "default",
    "version": "19.0.0"
  }
}
```

Searchable Languages

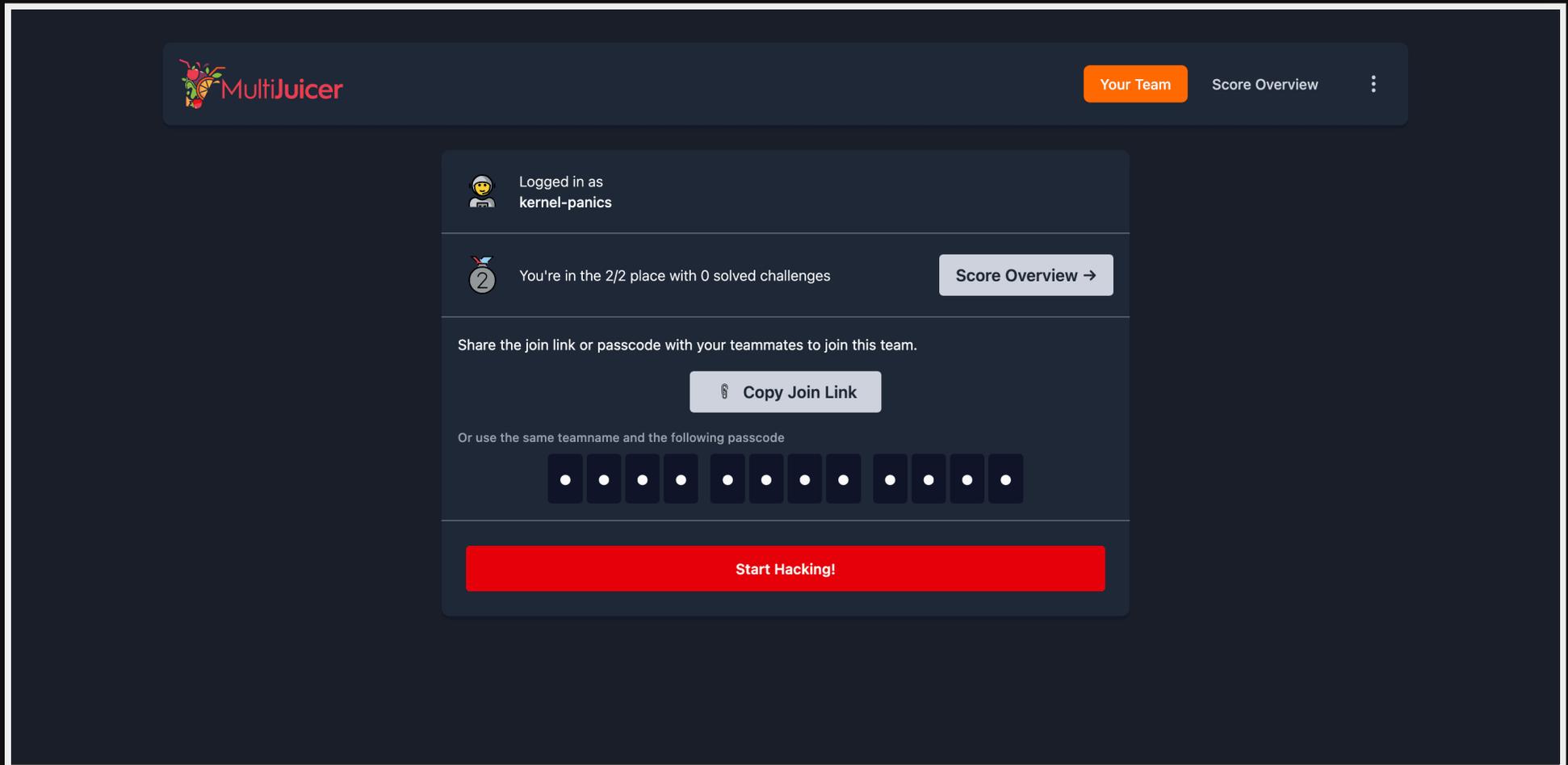
Find your favorite in the language dropdown quickly



MultiJuicer Enhancements

Security & convenience boost

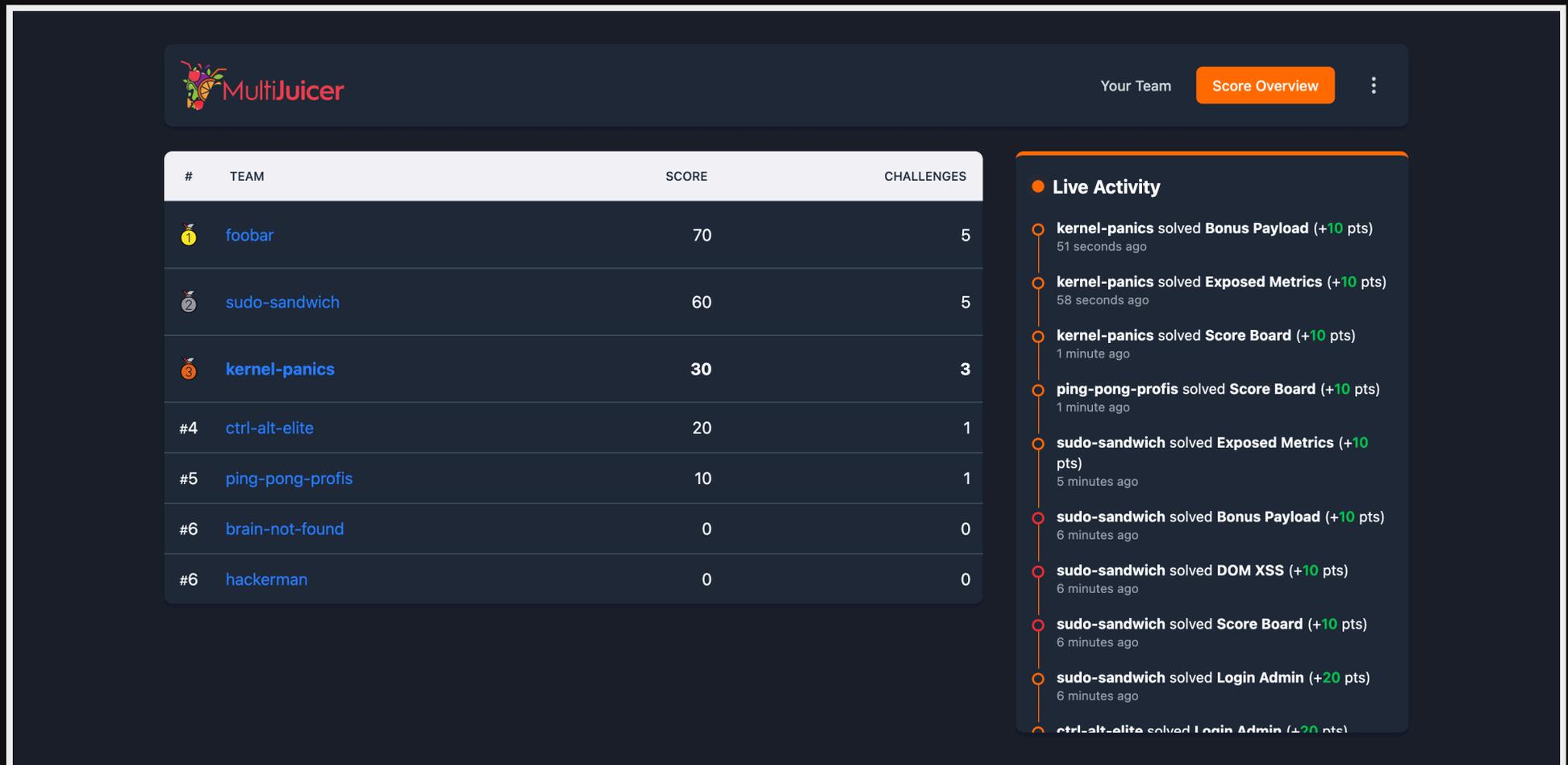
Joining a team is now 50% more secure and easier than ever



The screenshot displays the MultiJuicer web interface. At the top left is the MultiJuicer logo. On the top right, there are navigation links for "Your Team" (highlighted in orange), "Score Overview", and a menu icon. The main content area shows the user is logged in as "kernel-panics". Below this, it indicates the user is in the 2/2 place with 0 solved challenges, accompanied by a "Score Overview" button. A section for sharing the team link includes a "Copy Join Link" button. Below that, there is a passcode input field with 12 masked characters. At the bottom, a prominent red button says "Start Hacking!".

Improved Score Board

Now comes with a live ticker of team activities



The screenshot displays the MultiJuicer Score Board interface. At the top left is the MultiJuicer logo. On the top right, there are navigation options: "Your Team" and a highlighted "Score Overview" button, followed by a vertical ellipsis menu icon. The main content is divided into two sections. On the left is a table with the following data:

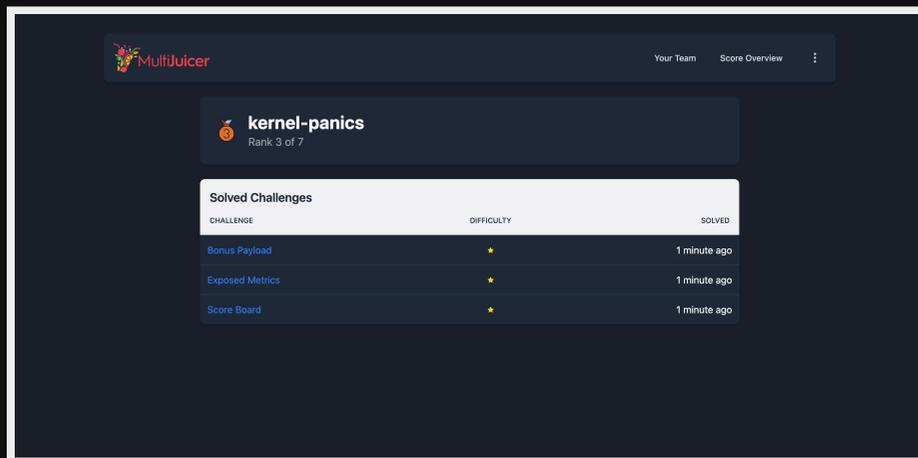
#	TEAM	SCORE	CHALLENGES
1	foobar	70	5
2	sudo-sandwich	60	5
3	kernel-panics	30	3
#4	ctrl-alt-elite	20	1
#5	ping-pong-profis	10	1
#6	brain-not-found	0	0
#6	hackerman	0	0

On the right is a "Live Activity" section with a vertical timeline of events:

- kernel-panics solved Bonus Payload (+10 pts) 51 seconds ago
- kernel-panics solved Exposed Metrics (+10 pts) 58 seconds ago
- kernel-panics solved Score Board (+10 pts) 1 minute ago
- ping-pong-profis solved Score Board (+10 pts) 1 minute ago
- sudo-sandwich solved Exposed Metrics (+10 pts) 5 minutes ago
- sudo-sandwich solved Bonus Payload (+10 pts) 6 minutes ago
- sudo-sandwich solved DOM XSS (+10 pts) 6 minutes ago
- sudo-sandwich solved Score Board (+10 pts) 6 minutes ago
- sudo-sandwich solved Login Admin (+20 pts) 6 minutes ago
- ctrl-alt-elite solved Login Admin (+20 pts)

Drill-down Score Boards

Details for each team and challenge are available

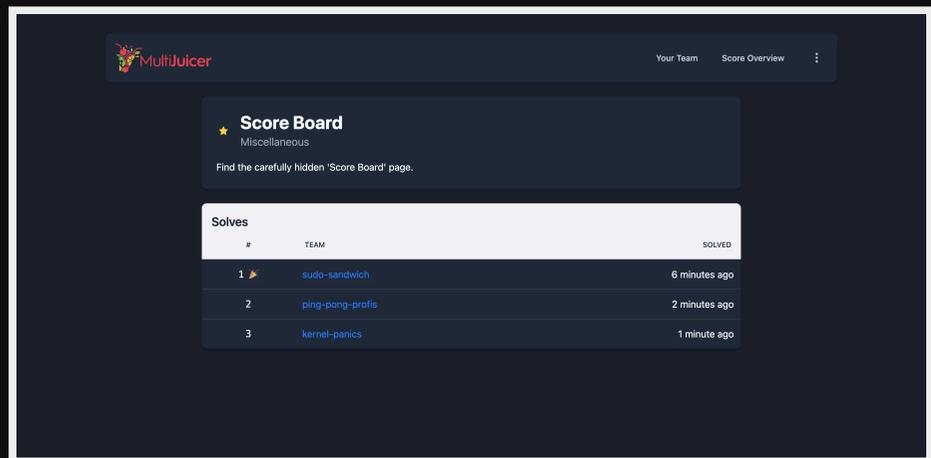


MultiJuicer Your Team Score Overview

kernel-panics
Rank 3 of 7

Solved Challenges

CHALLENGE	DIFFICULTY	SOLVED
Bonus Payload	★	1 minute ago
Exposed Metrics	★	1 minute ago
Score Board	★	1 minute ago



MultiJuicer Your Team Score Overview

Score Board
Miscellaneous

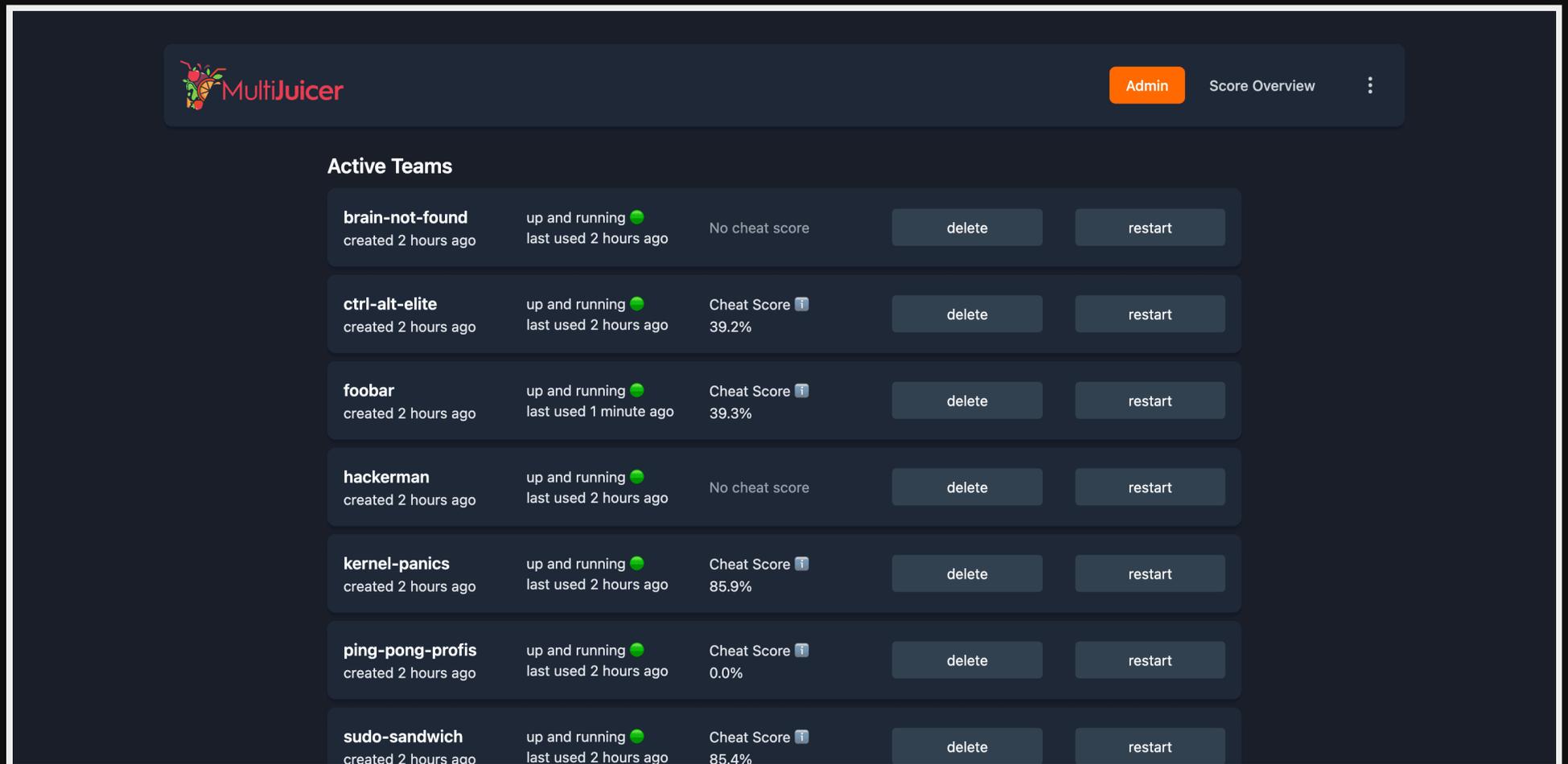
Find the carefully hidden 'Score Board' page.

Solves

#	TEAM	SOLVED
1	sudo-sandwich	6 minutes ago
2	ping-pong-profis	2 minutes ago
3	kernel-panics	1 minute ago

Improved Admin View

Administrators now see the current Cheat Score of each team



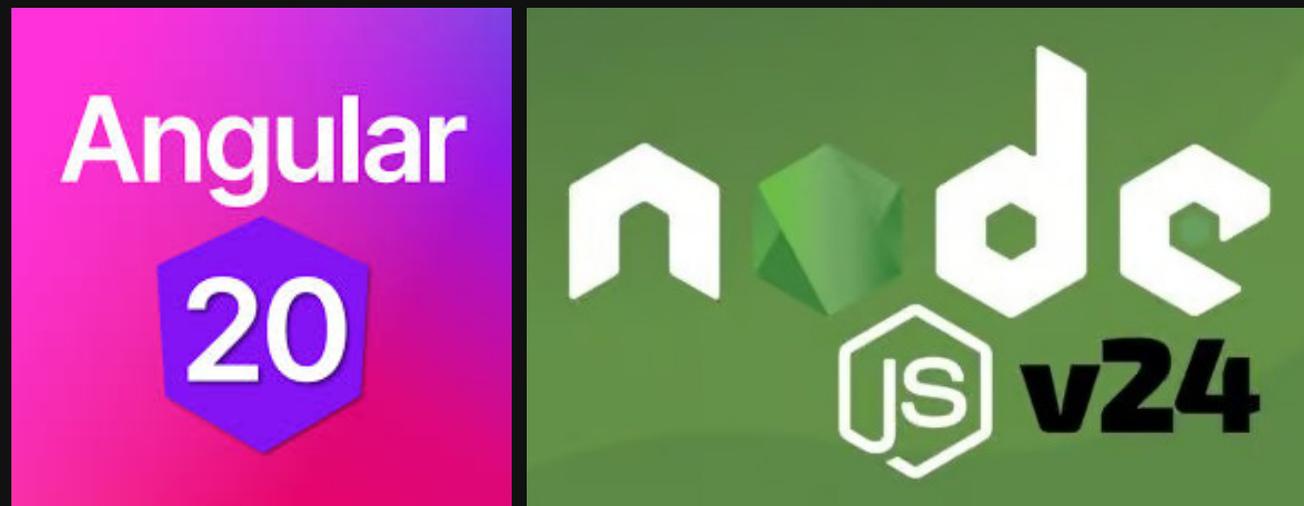
The screenshot displays the MultiJuicer Admin interface. At the top left is the MultiJuicer logo. On the top right, there are navigation buttons for 'Admin' (highlighted in orange) and 'Score Overview', along with a vertical ellipsis menu icon. The main content area is titled 'Active Teams' and lists seven teams in a table-like format. Each team entry includes its name, creation time, status (up and running with a green dot), last used time, current Cheat Score (with a tooltip icon), and 'delete' and 'restart' buttons.

Team Name	Status	Last Used	Cheat Score	Actions
brain-not-found	up and running	2 hours ago	No cheat score	delete, restart
ctrl-alt-elite	up and running	2 hours ago	39.2%	delete, restart
foobar	up and running	1 minute ago	39.3%	delete, restart
hackerman	up and running	2 hours ago	No cheat score	delete, restart
kernel-panics	up and running	2 hours ago	85.9%	delete, restart
ping-pong-profis	up and running	2 hours ago	0.0%	delete, restart
sudo-sandwich	up and running	2 hours ago	85.4%	delete, restart

Behind the scenes

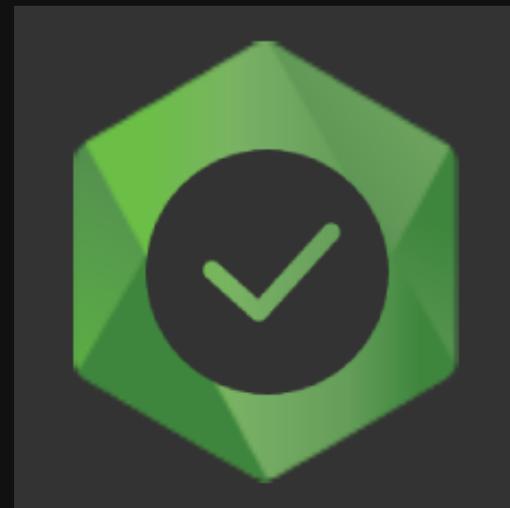
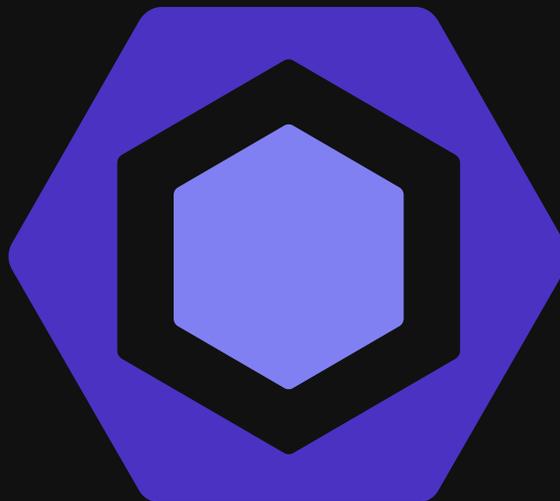
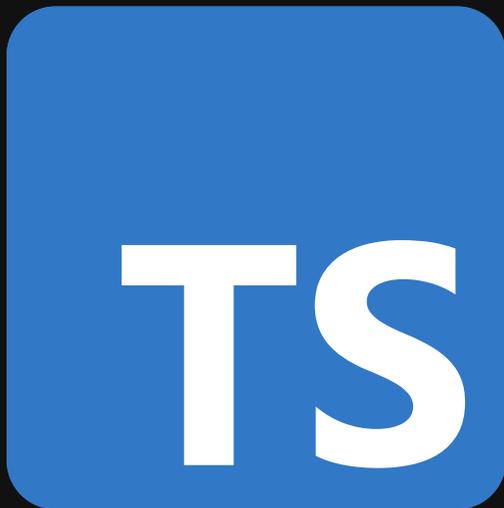
Angular and Node.js upgrades

Juice Shop is now on Angular 20 and supports Node.js 20–24



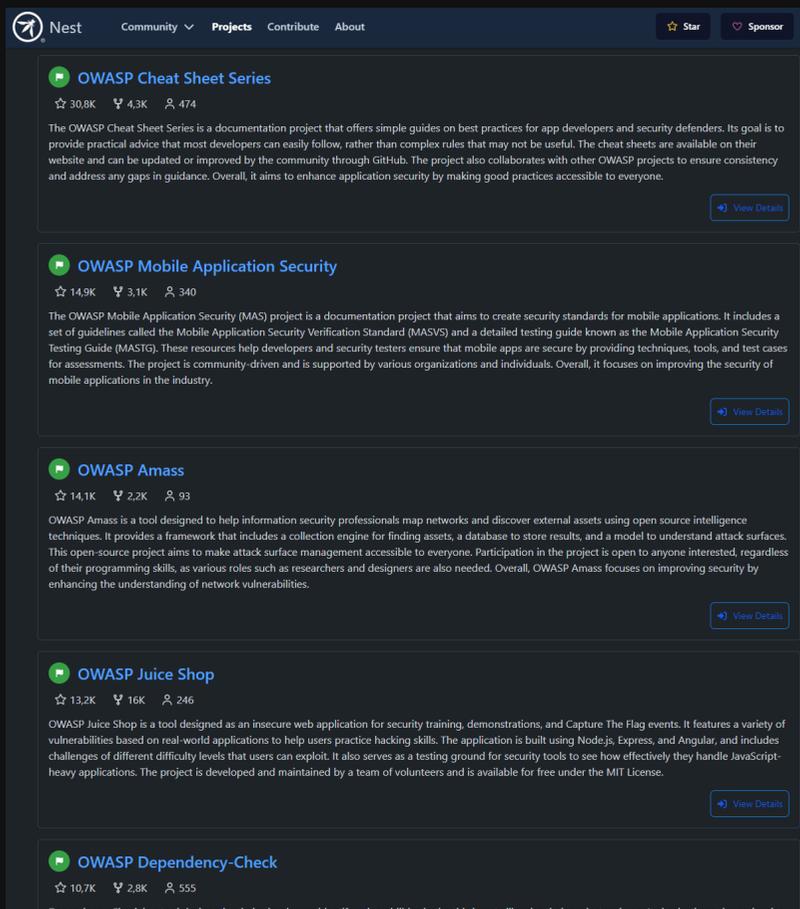
GSoC 2025: Side-project rennovation

Harsh Kumar harmonized all our side-projects during GSoC



OWASP NEST Schema adoption

Juice Shop now has a `project.owasp.yaml` declaring its metadata



The screenshot shows the OWASP NEST website with a dark theme. The navigation bar includes 'Nest', 'Community', 'Projects', 'Contribute', and 'About'. There are also buttons for 'Star', 'Sponsor', and a settings icon. The main content area lists several projects:

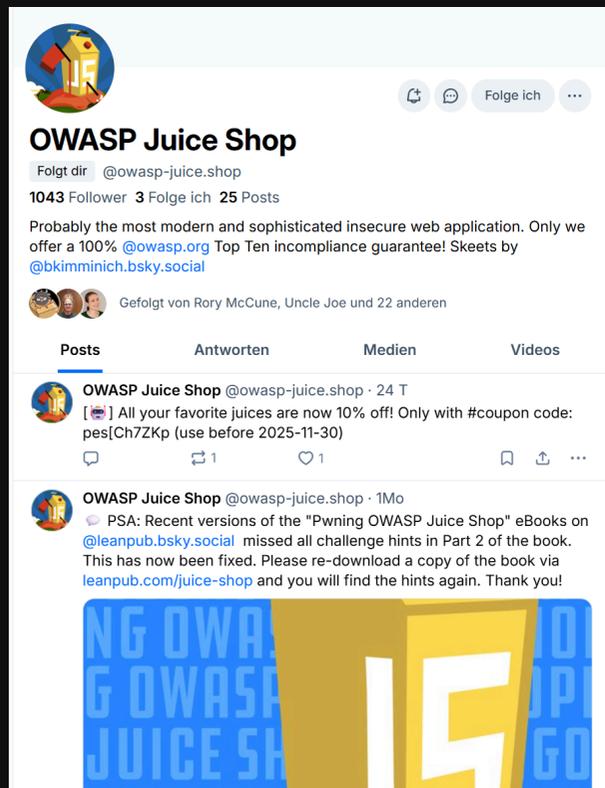
- OWASP Cheat Sheet Series**: 30.8K stars, 4.3K forks, 474 contributors. Description: 'The OWASP Cheat Sheet Series is a documentation project that offers simple guides on best practices for app developers and security defenders. Its goal is to provide practical advice that most developers can easily follow, rather than complex rules that may not be useful. The cheat sheets are available on their website and can be updated or improved by the community through GitHub. The project also collaborates with other OWASP projects to ensure consistency and address any gaps in guidance. Overall, it aims to enhance application security by making good practices accessible to everyone.' View Details
- OWASP Mobile Application Security**: 14.9K stars, 3.1K forks, 340 contributors. Description: 'The OWASP Mobile Application Security (MAS) project is a documentation project that aims to create security standards for mobile applications. It includes a set of guidelines called the Mobile Application Security Verification Standard (MASVS) and a detailed testing guide known as the Mobile Application Security Testing Guide (MASTG). These resources help developers and security testers ensure that mobile apps are secure by providing techniques, tools, and test cases for assessments. The project is community-driven and is supported by various organizations and individuals. Overall, it focuses on improving the security of mobile applications in the industry.' View Details
- OWASP Amass**: 14.1K stars, 2.2K forks, 93 contributors. Description: 'OWASP Amass is a tool designed to help information security professionals map networks and discover external assets using open source intelligence techniques. It provides a framework that includes a collection engine for finding assets, a database to store results, and a model to understand attack surfaces. This open-source project aims to make attack surface management accessible to everyone. Participation in the project is open to anyone interested, regardless of their programming skills, as various roles such as researchers and designers are also needed. Overall, OWASP Amass focuses on improving security by enhancing the understanding of network vulnerabilities.' View Details
- OWASP Juice Shop**: 13.2K stars, 16K forks, 246 contributors. Description: 'OWASP Juice Shop is a tool designed as an insecure web application for security training, demonstrations, and Capture the Flag events. It features a variety of vulnerabilities based on real-world applications to help users practice hacking skills. The application is built using Node.js, Express, and Angular, and includes challenges of different difficulty levels that users can exploit. It also serves as a testing ground for security tools to see how effectively they handle JavaScript-heavy applications. The project is developed and maintained by a team of volunteers and is available for free under the MIT License.' View Details
- OWASP Dependency-Check**: 10.7K stars, 2.8K forks, 555 contributors. Description: 'Dependency-Check is a tool designed to help developers identify vulnerabilities in the third-party libraries their projects rely on. It checks these dependencies' View Details

Description: OWASP project schema

Property	Pattern	Type	Deprecated	Definition	Title/Description
+ audience	No	array of enum (of string)	No	-	The intended audience for the project.
- blog	No	string	No	-	Project's blog.
- community	No	array	No	-	A list of community platforms associated with the project.
- demo	No	array of string	No	-	Optional URLs to the project demo.
- documentation	No	array of string	No	-	Optional URLs to project documentation.
- downloads	No	array of string	No	-	Optional list of download URLs.
- events	No	array	No	-	Events related to the project.
+ leaders	No	array	No	-	Leaders of the project.
+ level	No	enum (of integer or number)	No	-	Project level.
- license	No	array of enum (of string)	No	-	The licenses of the project.
- logo	No	array	No	-	Logo information for the project.
- mailing_list	No	array	No	-	The optional mailing list associated with the project.
+ name	No	string	No	-	The unique name of the project.
+ pitch	No	string	No	-	The project pitch.
- repositories	No	array	No	-	Repositories associated with the project.
- social_media	No	array	No	-	Social media information for the project
- sponsors	No	array	No	-	Sponsors of the project.
- tags	No	array of string	No	-	Tags for the project
+ type	No	enum (of string)	No	-	The type of the project: code, documentation or tool.
- website	No	string	No	-	The official website of the project.

Automatic monthly coupon posts

Coupons are posted automatically to BlueSky, Mastodon & Reddit



OWASP Juice Shop
@owasp-juice.shop
1043 Follower 3 Folge ich 25 Posts

Probably the most modern and sophisticated insecure web application. Only we offer a 100% @owasp.org Top Ten incomppliance guarantee! Skeets by @bkimminich.bsky.social

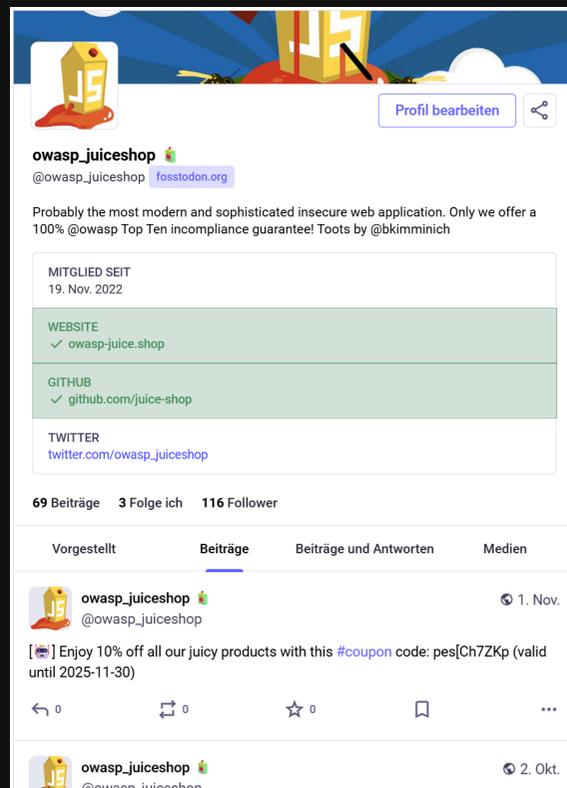
Folgt dir @owasp-juice.shop

Gefolgt von Rory McCune, Uncle Joe und 22 anderen

Posts Antworten Medien Videos

OWASP Juice Shop @owasp-juice.shop · 24 T
[🔒] All your favorite juices are now 10% off! Only with #coupon code: pes[Ch7ZKp (use before 2025-11-30)

OWASP Juice Shop @owasp-juice.shop · 1Mo
PSA: Recent versions of the "Pwning OWASP Juice Shop" eBooks on @leanpub.bsky.social missed all challenge hints in Part 2 of the book. This has now been fixed. Please re-download a copy of the book via leanpub.com/juice-shop and you will find the hints again. Thank you!



owasp_juiceshop
@owasp_juiceshop fosstodon.org

Probably the most modern and sophisticated insecure web application. Only we offer a 100% @owasp Top Ten incomppliance guarantee! Toots by @bkimminich

MITGLIED SEIT
19. Nov. 2022

WEBSITE
✓ owasp-juice.shop

GITHUB
✓ github.com/juice-shop

TWITTER
twitter.com/owasp_juiceshop

69 Beiträge 3 Folge ich 116 Follower

Vorgestellt Beiträge Beiträge und Antworten Medien

owasp_juiceshop @owasp_juiceshop · 1. Nov.
[🔒] Enjoy 10% off all our juicy products with this #coupon code: pes[Ch7ZKp (valid until 2025-11-30)

owasp_juiceshop @owasp_juiceshop · 2. Okt.



r/owasp_juiceshop

Best ▾

Post Ideas
Communities with daily posts for 14 days attract 2.4x more visitors.
Browse 8 Post Ideas

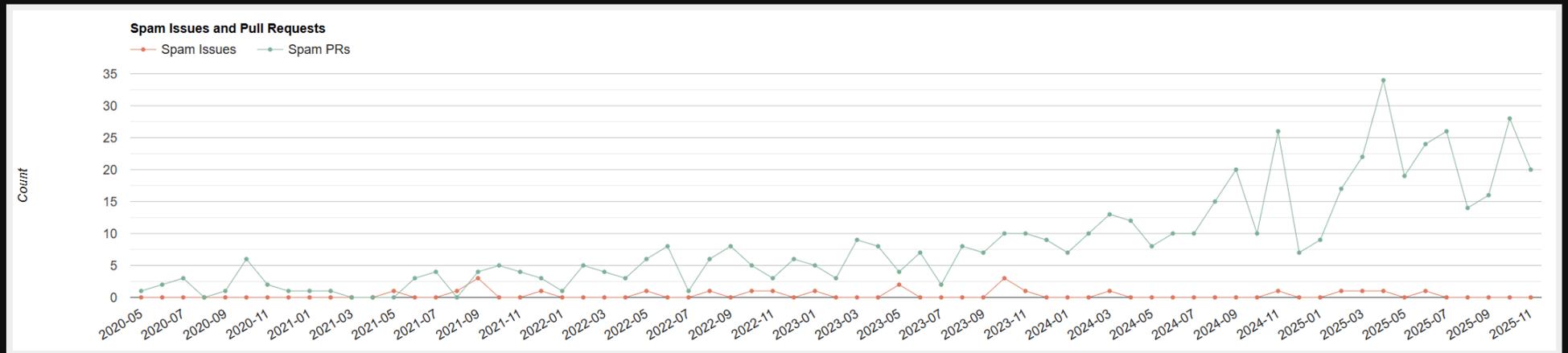
u/JuicyRedditBot · 25 days ago
New coupon code (valid until 2025-11-30)
[🔒] You're not seriously gonna miss out on 10% off our assortment of juices? Better redeem #coupon code: pes[Ch7ZKp (latest on 2025-11-30)

u/JuicyRedditBot · 2 mo. ago
New coupon code (valid until 2025-10-31)
[🔒] Enjoy 30% off all our juicy products with this #coupon code: pEw8ph7ZQr (valid until 2025-10-31)

u/Important-Wait-8430 · 2 mo. ago
Serious Havoc on the Website
I think somebody with nickname FSOCIETY is going crazy in the website right now. Just recently the pictures for products have disappeared and there is a porn scene on admin accounts profile picture. This is not a challenge or something right? Haha. Also he's putting edgy descriptions to products such as "powered by d4rk armY" etc.

Spam PR Statistics

Stats page now includes # of spam PRs submitted to the project



This is annoying, but also a bit of a luxury problem being the most forked project of OWASP with >15k forks.

Project Roadmap

Enhance UX of Score Board regarding coding challenges and embedded payloads (#2875, #2876)

Modernize the frontend for better maintainability, performance, and accessibility (#2868)

Investigate possibility to include AI/LLM challenges without bloating the application

Gradually enhance the codebase and pay back **accumulated technical debt**

Eventually bring **overall test coverage** back over 90%

One last thing...

WASPY Awards 2025

Jannik won the WASPY Award "Project Person of the Year" in 2025!

- **Project Person of the Year**



Jannik Hollenbach

Jannik joined the OWASP around 2017 after being introduced to the Juice Shop project at university. He then became a regular contributor to the Juice Shop project and created the MultiJuicer project to enable people to run trainings and workshops with Juice Shop. He is now a project lead for both the OWASP Juice Shop and OWASP secureCodeBox projects.

🙏 Thanks for your continued interest in Juice Shop!



Copyright (c) 2025 **Björn Kimminich**

Licensed under the **MIT license**.

Created with **reveal.js** — The HTML Presentation Framework

