News from the Juice Shop ecosystem

German OWASP Day 2025

by Björn Kimminich / @bkimminich.bsky.social

https://owasp-juice.shop

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

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

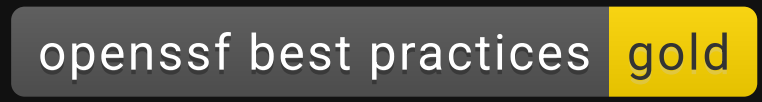
http://**ebook!**
owasp-juice.shop

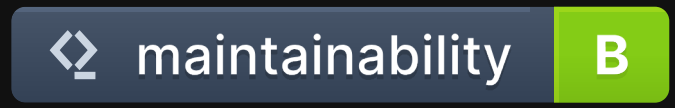
- Free and Open source: Licensed under the MIT license with no hidden costs or caveats
- Easy-to-install: Choose between node.js, Docker and Vagrant to run on Windows/Mac/Linux
- Self-contained: Additional dependencies are pre-packaged or will be resolved and downloaded automatically
- Self-healing: 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

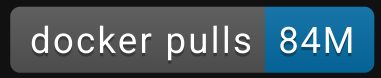
http://owasp-juice.shop | @owasp_juiceshop

Juice Shop Success Pyramid™

Some amazing facts & stats about the project



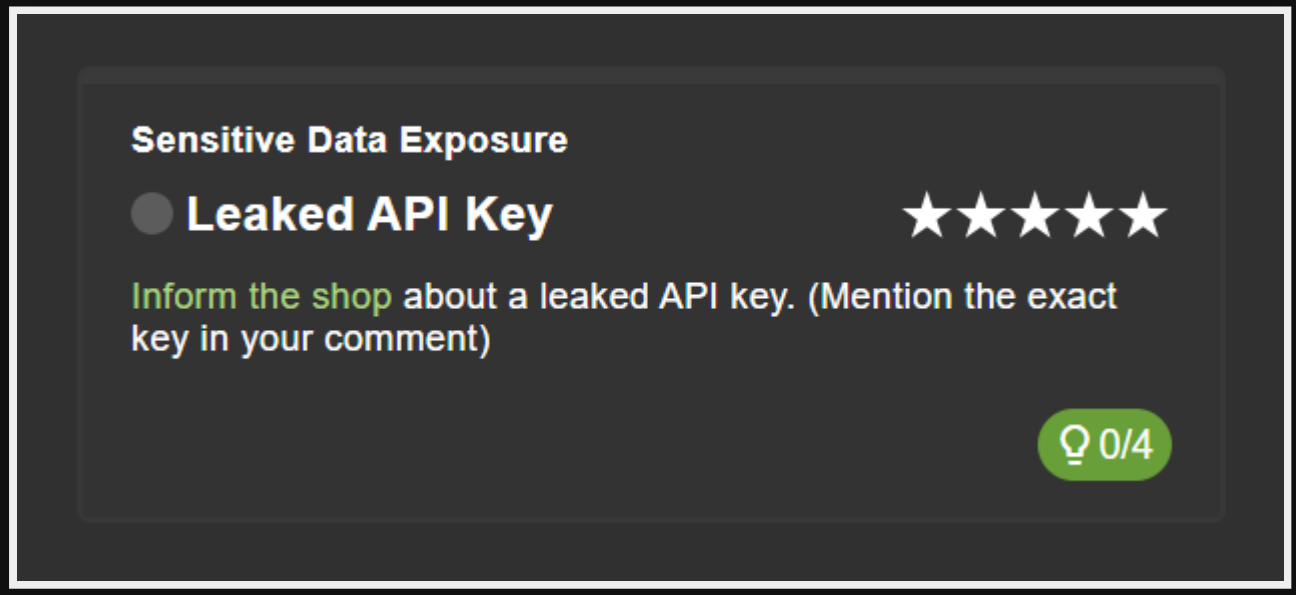




New Challenges

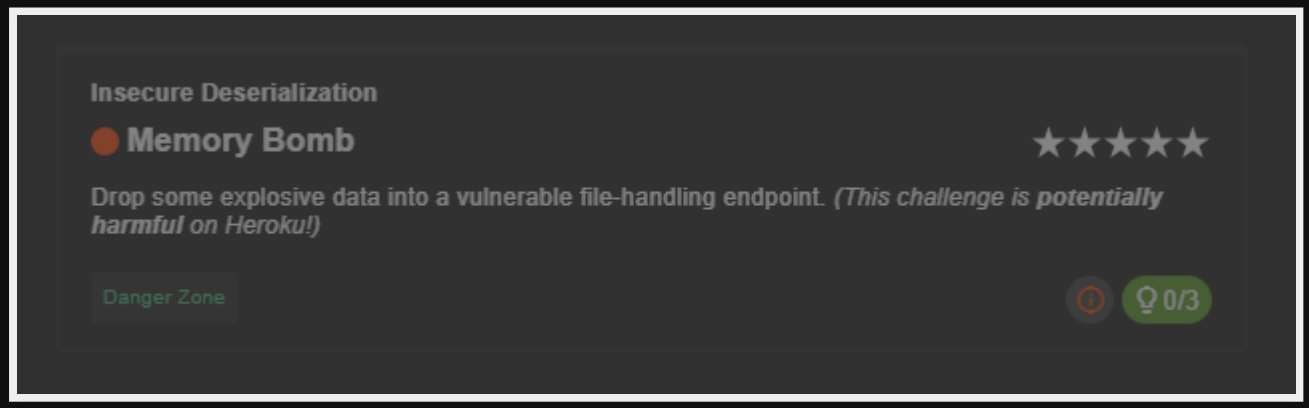
★★★★★ Leaked API Key

Juice Shop uses this behind the scenes



⭐⭐⭐⭐⭐ Memory Bomb

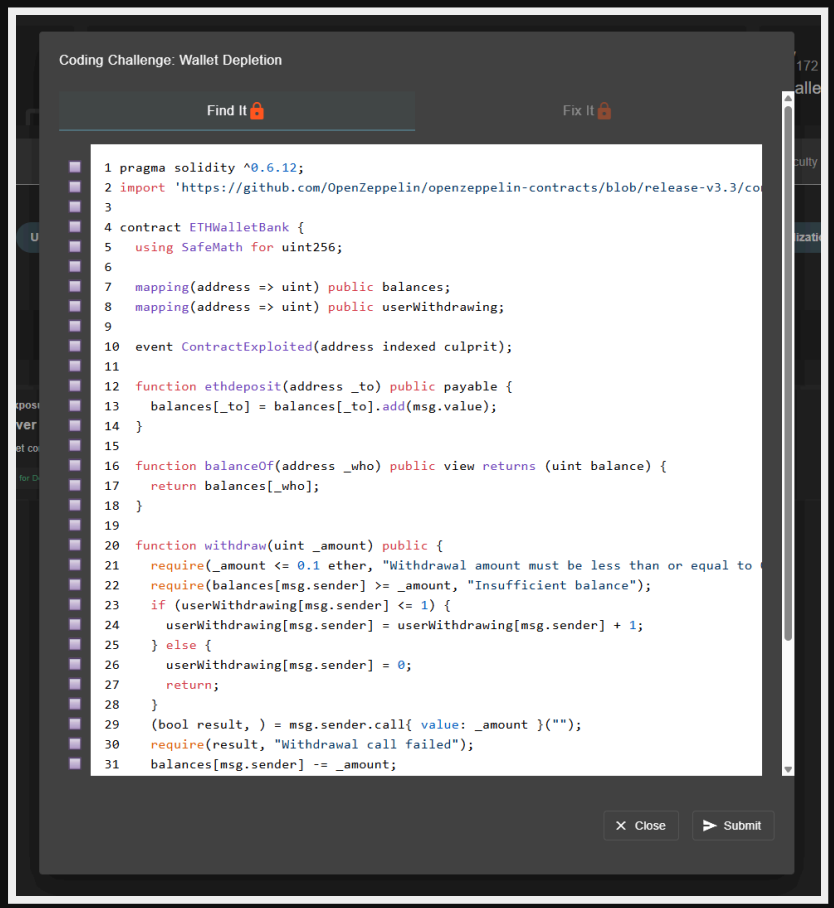
It's a bit like XXE*, only with YAML

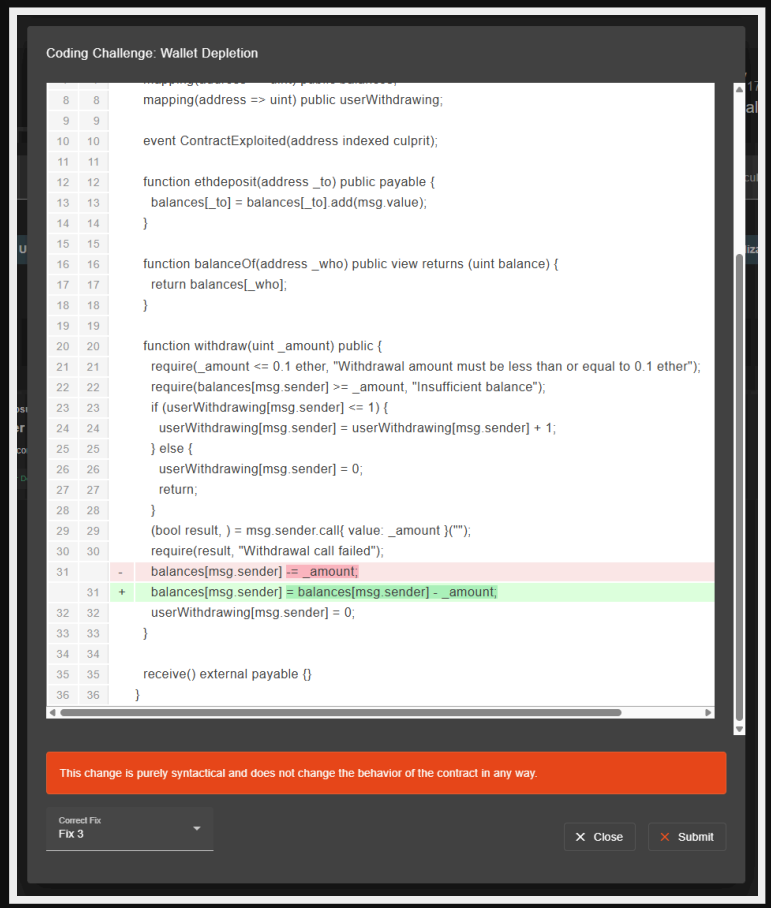


*= It's also just as dangerous as XXE, so the challenge is turned off by default on the public demo server and when running Juice Shop in Docker or on Heroku.

Web3 Coding Challenges

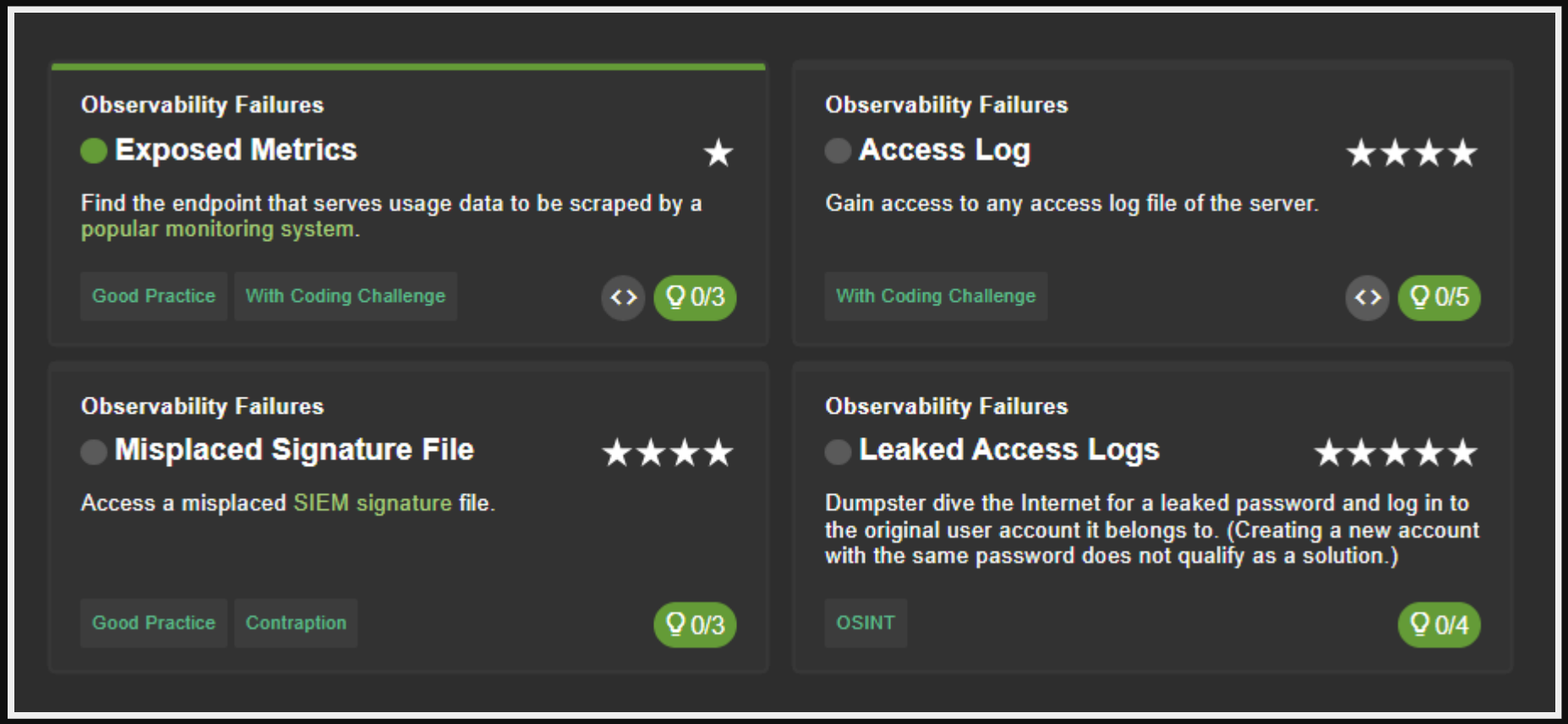
Most Web3 challenges now have an accompanying coding challenge





New Category: Observability Failures

Groups all challenges related to OWASP Top 10 A9:2025



Category Mapping 2025

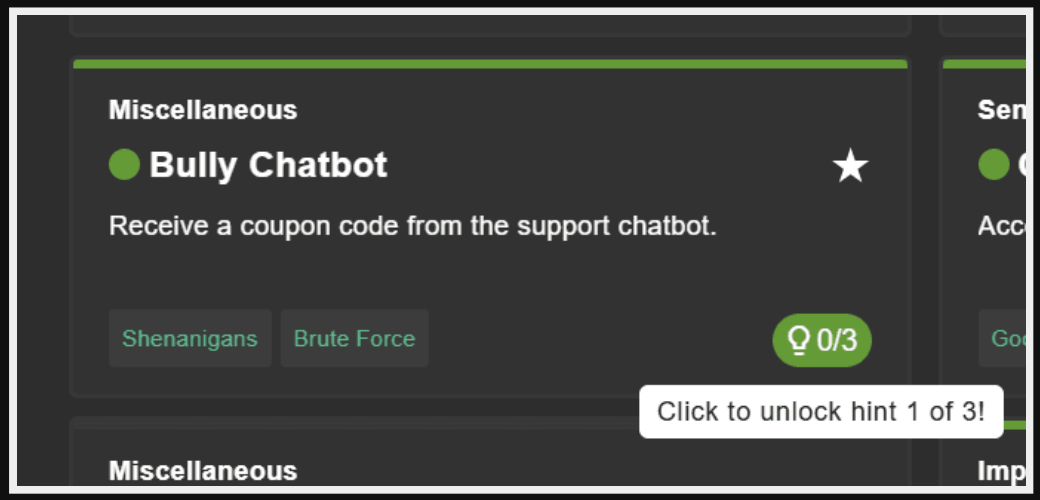
Juice Shop is 100% incompliant with the OWASP TOP 10:2025 RC

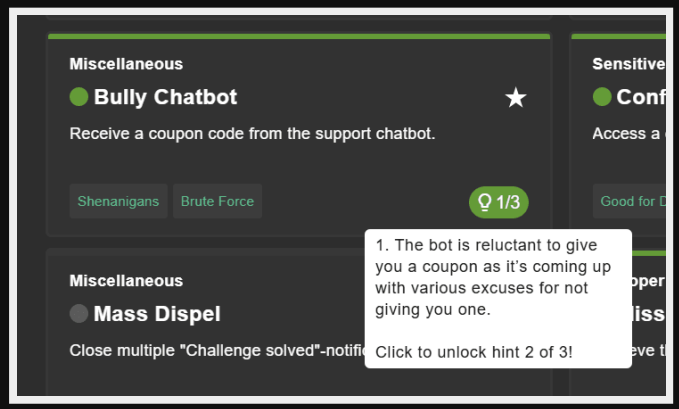
Category	Mappings	Category	Mappings
Broken Access Control	**A1:2025**, **A6:2025**, **A1:2021**, API1:2019, API5:2019, CWE-22, CWE-285, CWE-639, CWE-918, WASC-02, WASC-09, WASC-16	Broken Anti-Automation	**A6:2025**, OWASP-AT-004, API4:2019, OWASP-AT-010, OAT-009, OAT-015, OAT-008, CWE-362, WASC-11, WASC-21
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

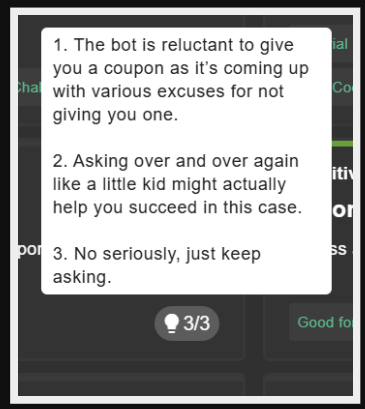
Other Features

Multiple Challenge Hints

All challenges now come with one or more unlockable hints

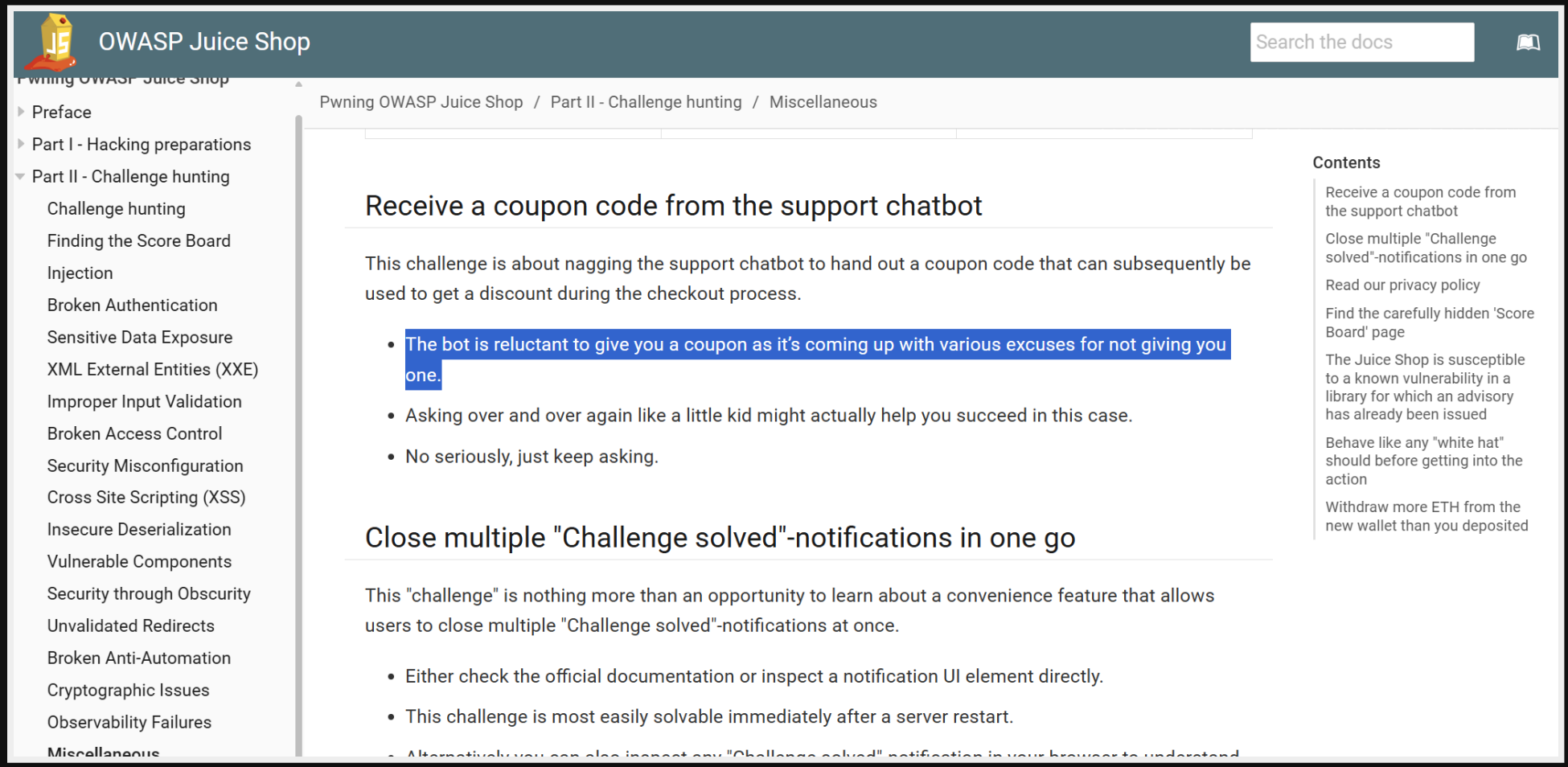






Auto-sync with eBook

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



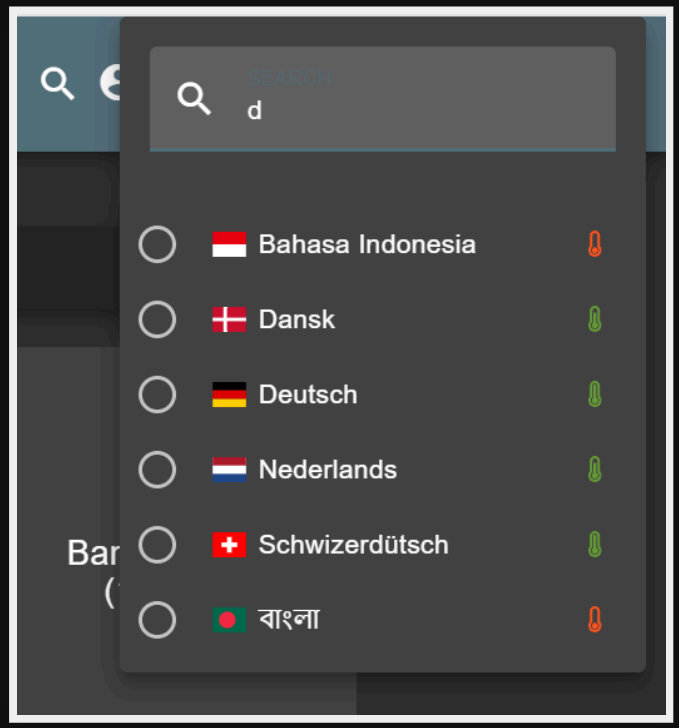
Solution Webhook also tracks hints

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

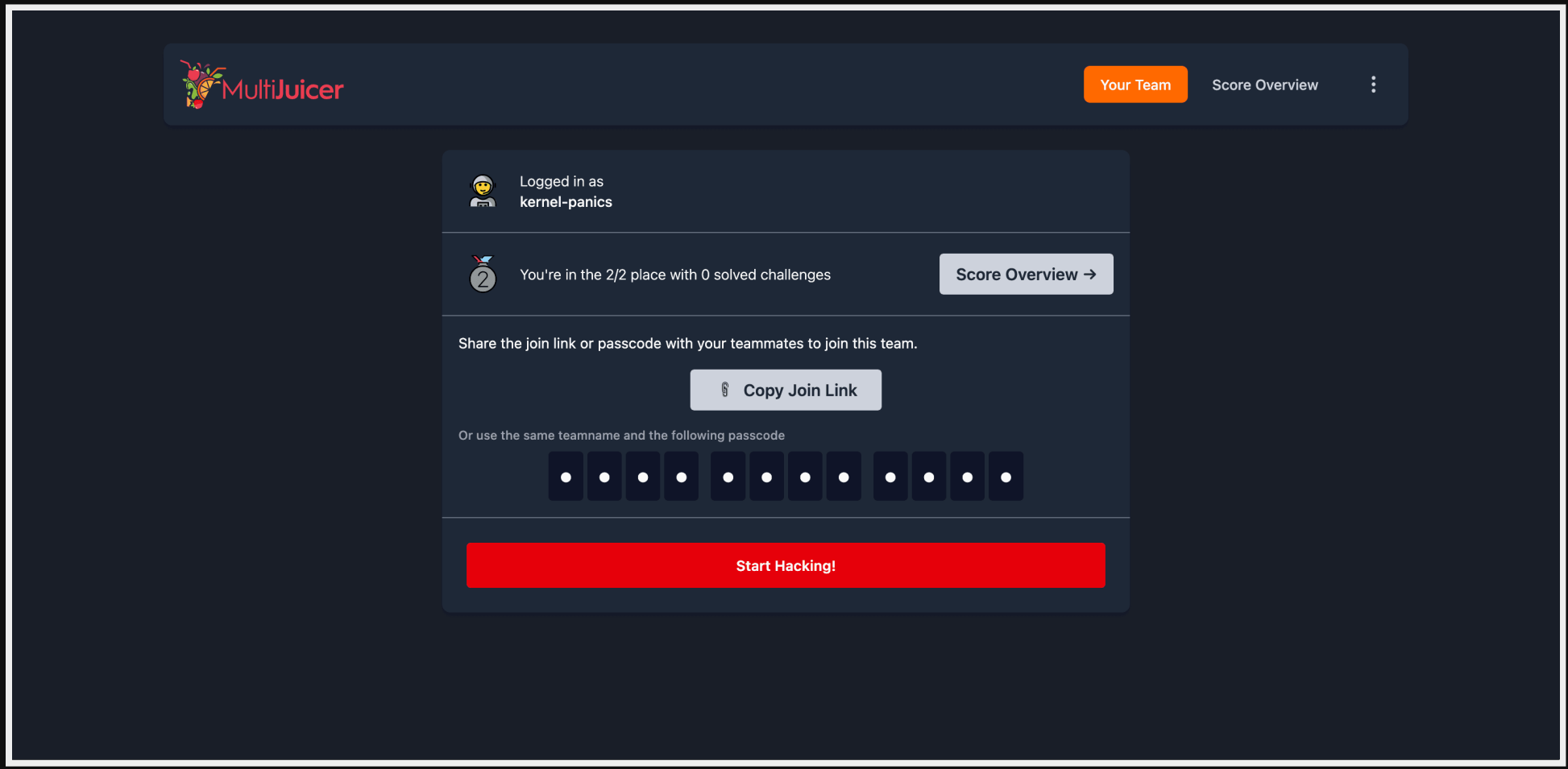
Find your favorite in the language dropdown quickly



MultiJuicer Enhancements

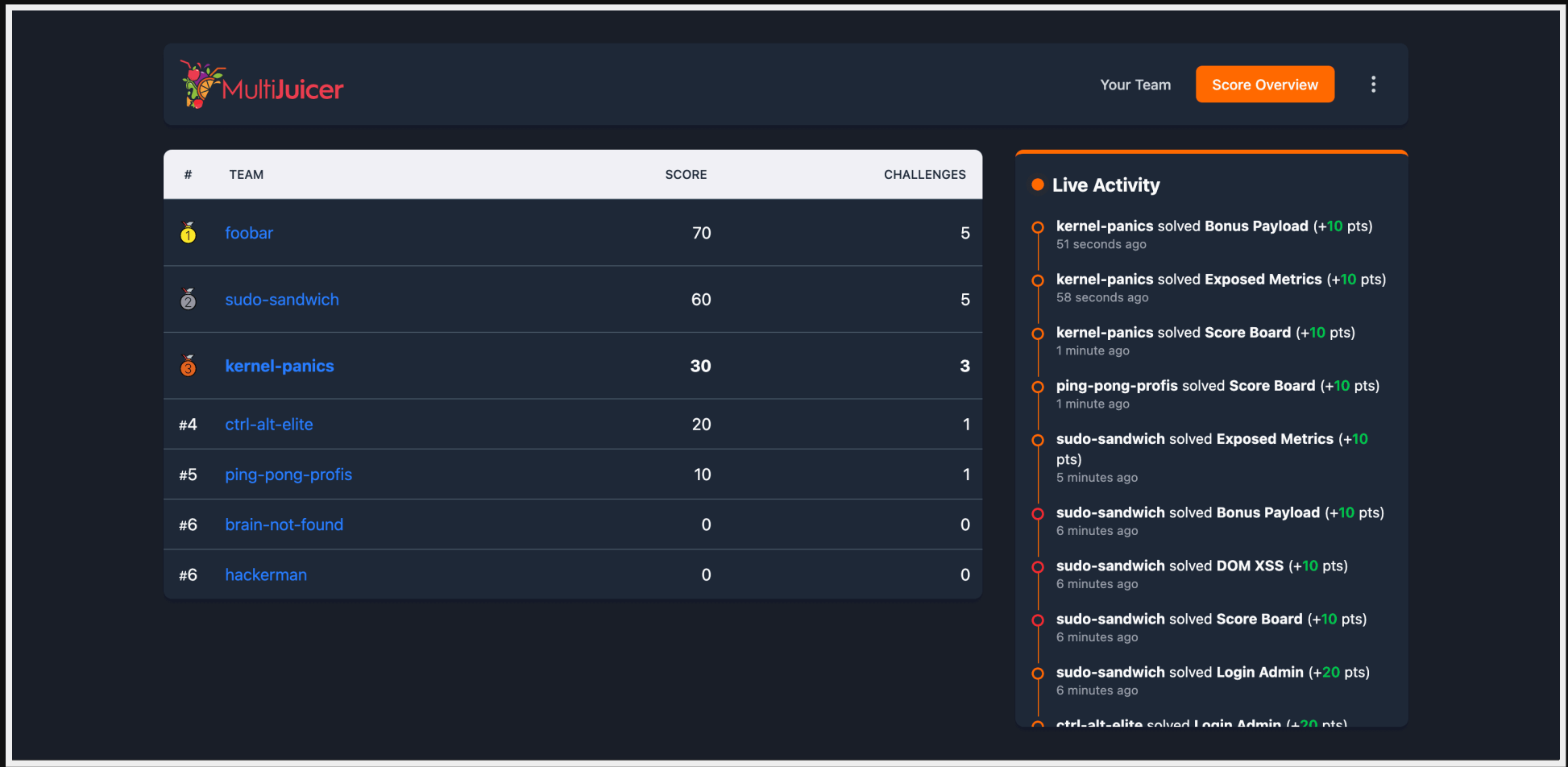
Security & convenience boost

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



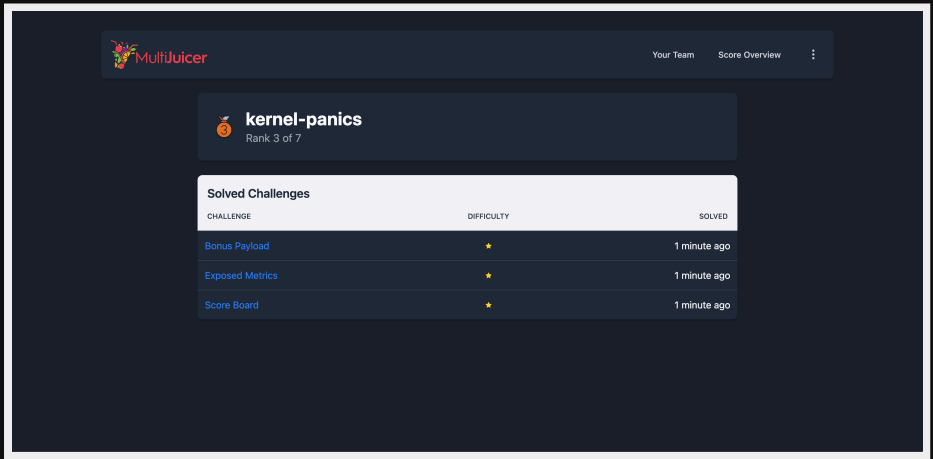
Improved Score Board

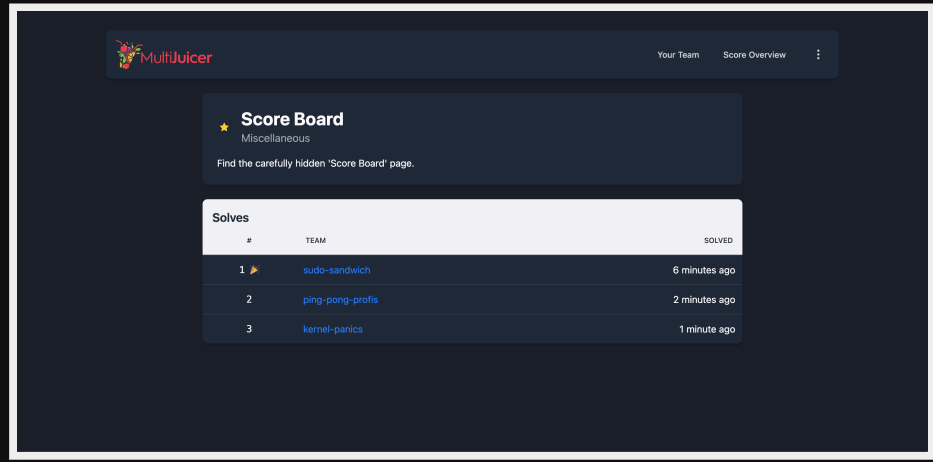
Now comes with a live ticker of team activities



Drill-down Score Boards

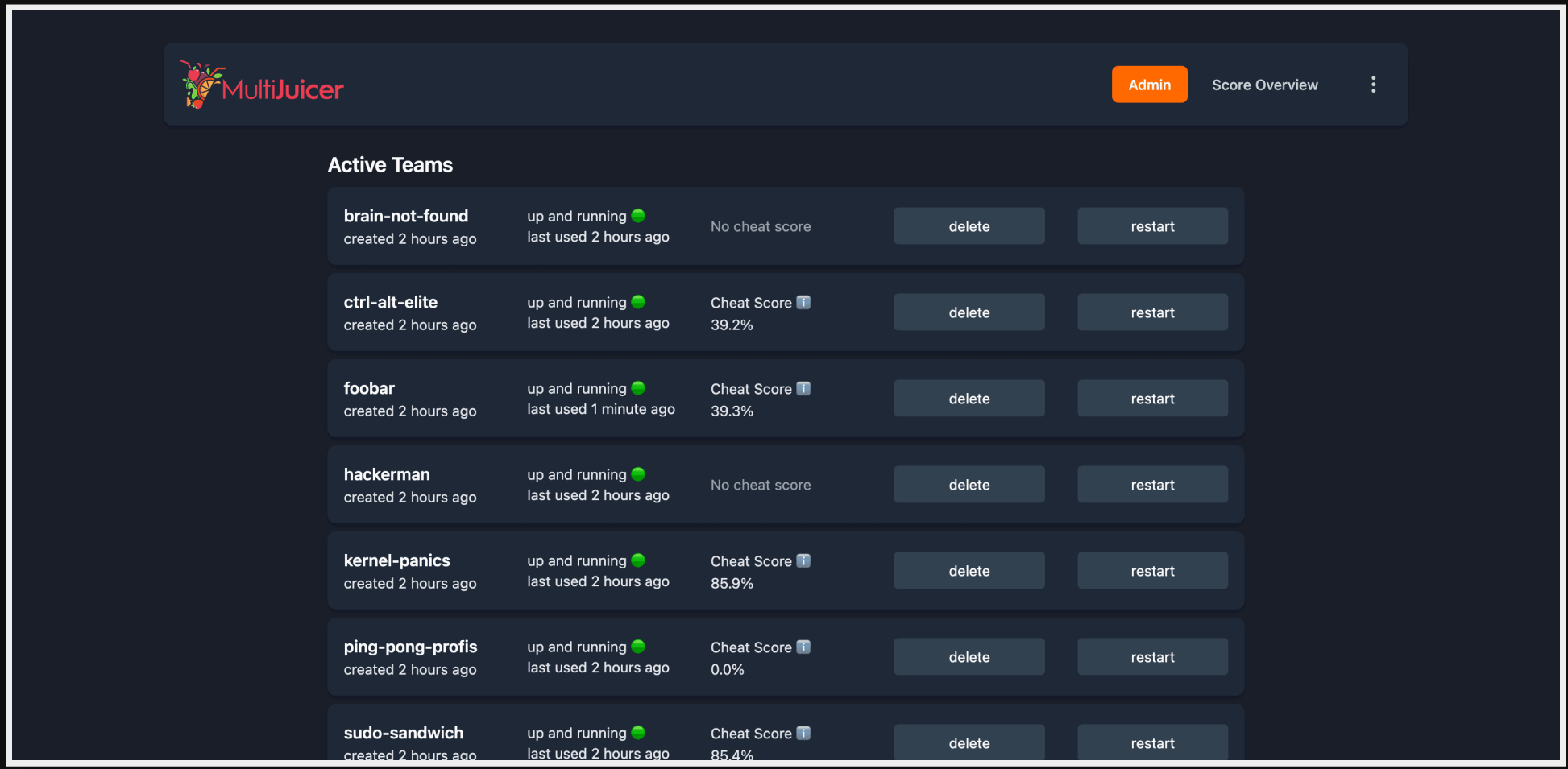
Details for each team and challenge are available





Improved Admin View

Administrators now see the current Cheat Score of each team



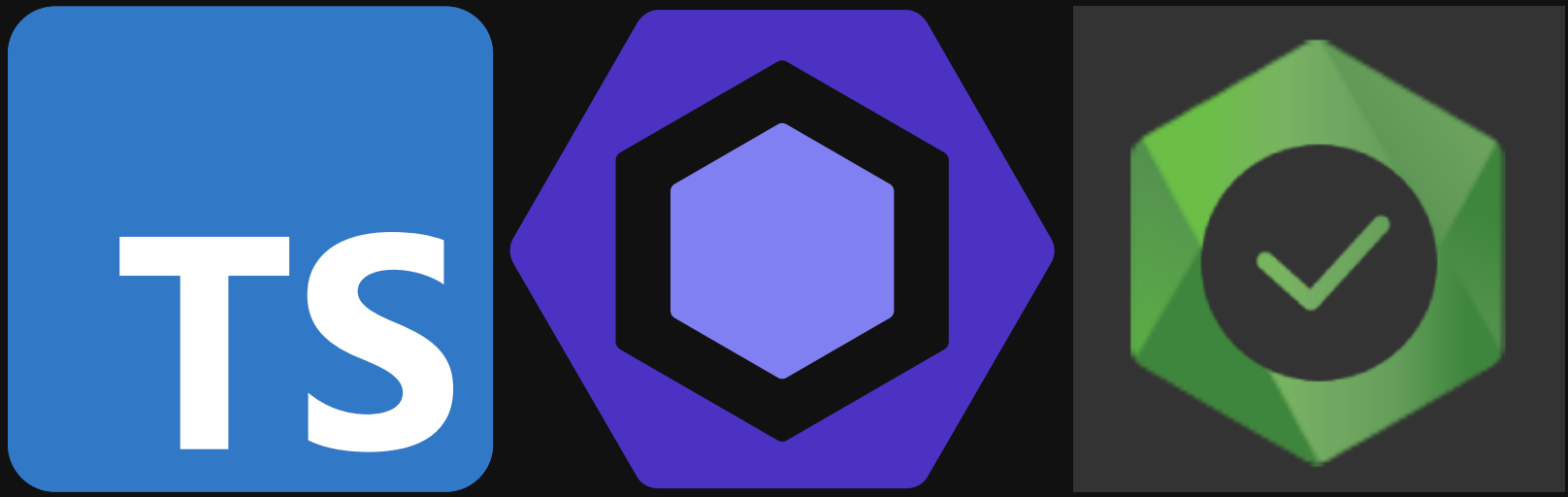
Behind the scenes

Angular and Node.js upgrades

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

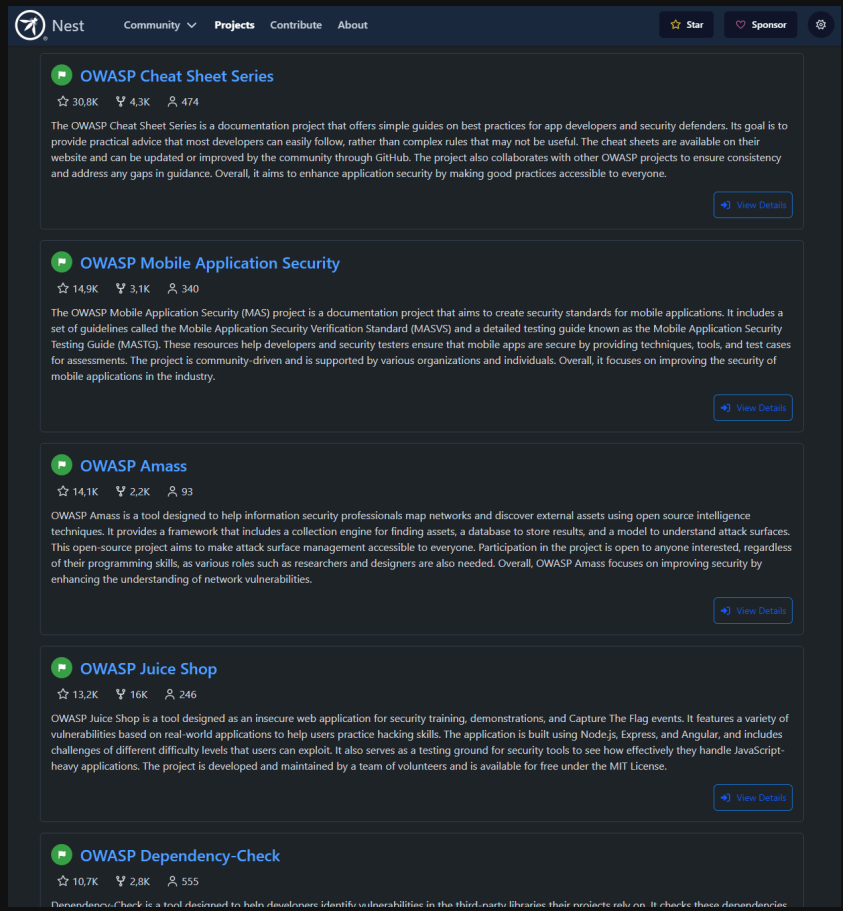
GSoC 2025: Side-project rennovation

Harsh Kumar harmonized all our side-projects during GSoC



OWASP NEST Schema adoption

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

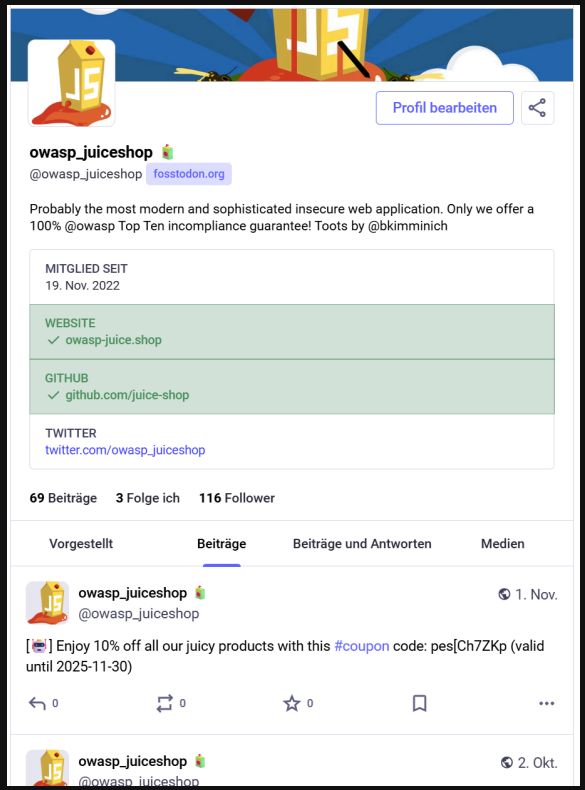


Description: OWASP project schema

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.

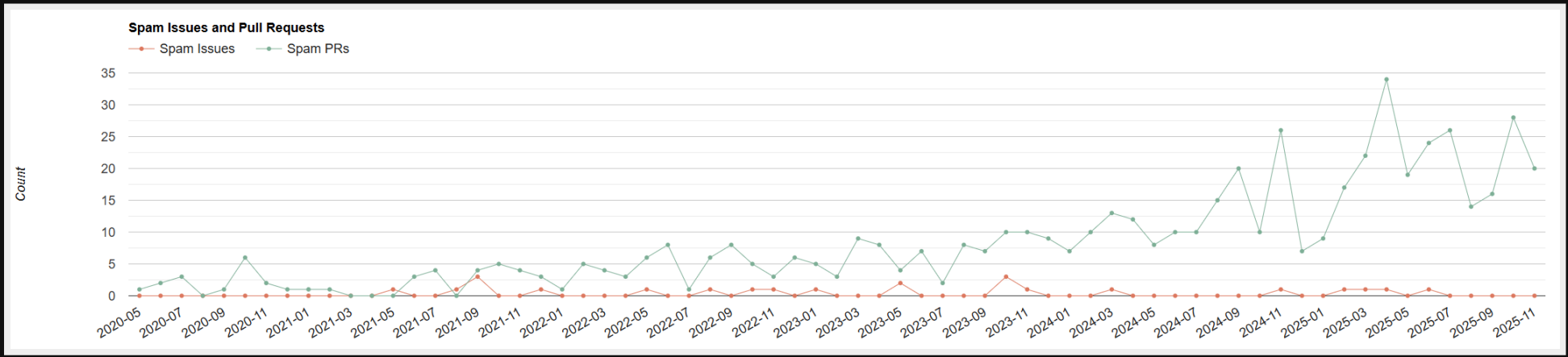
Automatic monthly coupon posts

Coupons are posted automatically to BlueSky, Mastodon & Reddit



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!

Created with reveal.js — The HTML Presentation Framework