

## Score board:

The screenshot shows the OWASP Juice Shop Score Board interface. At the top, there are filters for 'Search', 'Difficulty', 'Status', and 'Tags'. Below these are several tabs for challenge categories: 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. A message at the top states: "17 challenges are unavailable on Docker due to security concerns or technical incompatibility!" with a link to "Hide disabled challenges". The main area displays a grid of challenges. Some visible challenges include:

- Miscellaneous: Score Board (Tutorial, Code Analysis, With Coding Challenge, Hint)
- XSS: DOM XSS (Tutorial, Good for Demos, With Coding Challenge, Hint)
- XSS: Bonus Payload (Shenanigans, Tutorial, With Coding Challenge, Hint)
- Miscellaneous: Privacy Policy (Good Practice, Tutorial, Good for Demos, Hint)
- Miscellaneous: Bully Chatbot (Shenanigans, Brute Force, Hint)
- Sensitive Data Exposure: Confidential Document (Good for Demos, With Coding Challenge, Hint)
- Security Misconfiguration: Error Handling (Prerequisite, Hint)
- Sensitive Data Exposure: Exposed Metrics (Good Practice, With Coding Challenge, Hint)

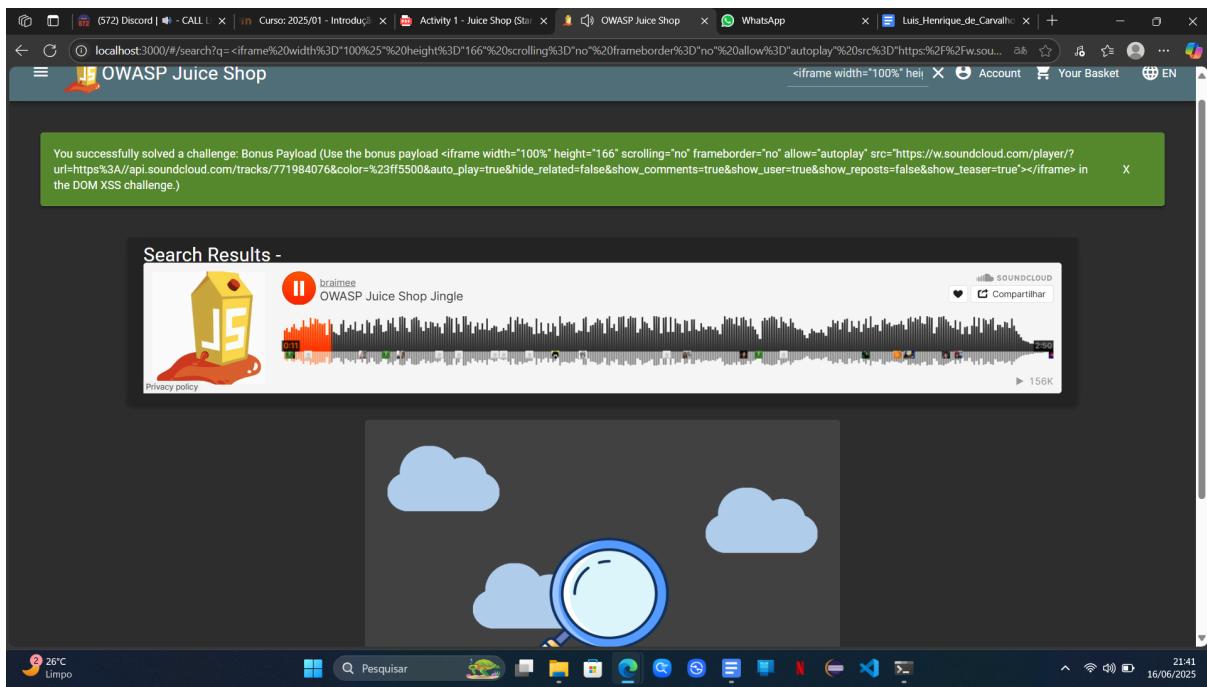
## DOM XSS

The screenshot shows the OWASP Juice Shop DOM XSS challenge page. At the top, there is a navigation bar with various tabs and links. The main content area has two green success messages:

- You successfully solved a challenge: Score Board (Find the carefully hidden 'Score Board' page.)
- You successfully solved a challenge: DOM XSS (Perform a DOM XSS attack with <iframe src="javascript:alert('xss')">.)

Below the messages is a search bar with the placeholder "Search Results -". The background features a cartoon illustration of clouds and a magnifying glass.

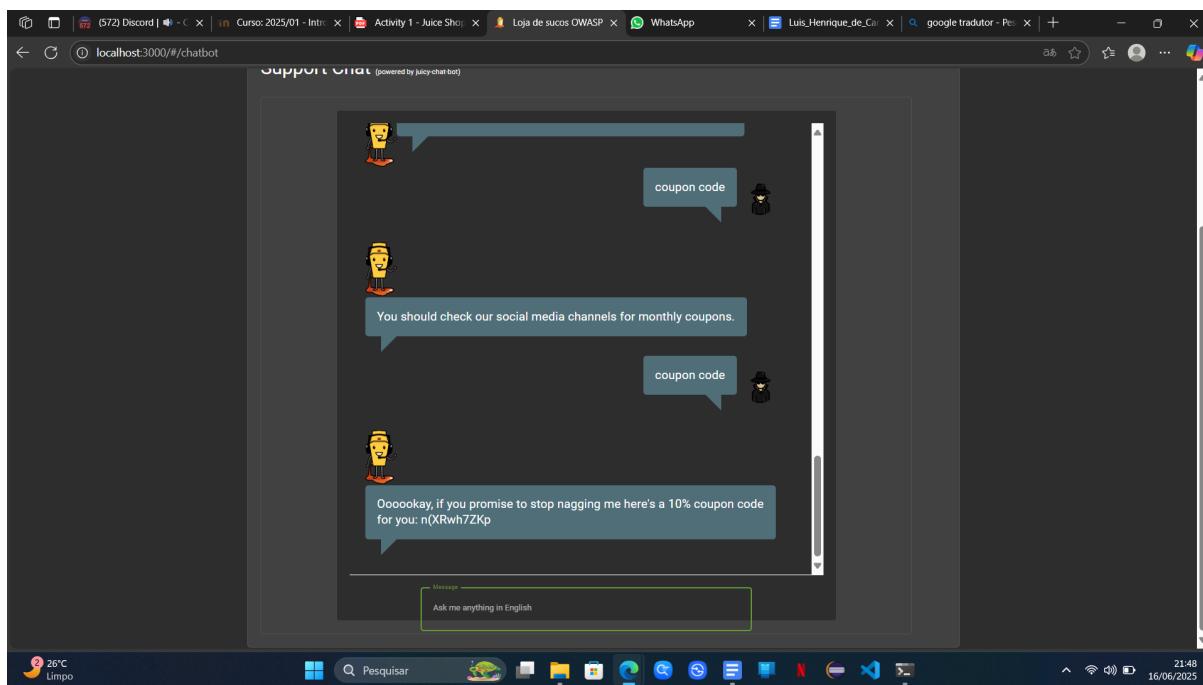
## Bonus Payload



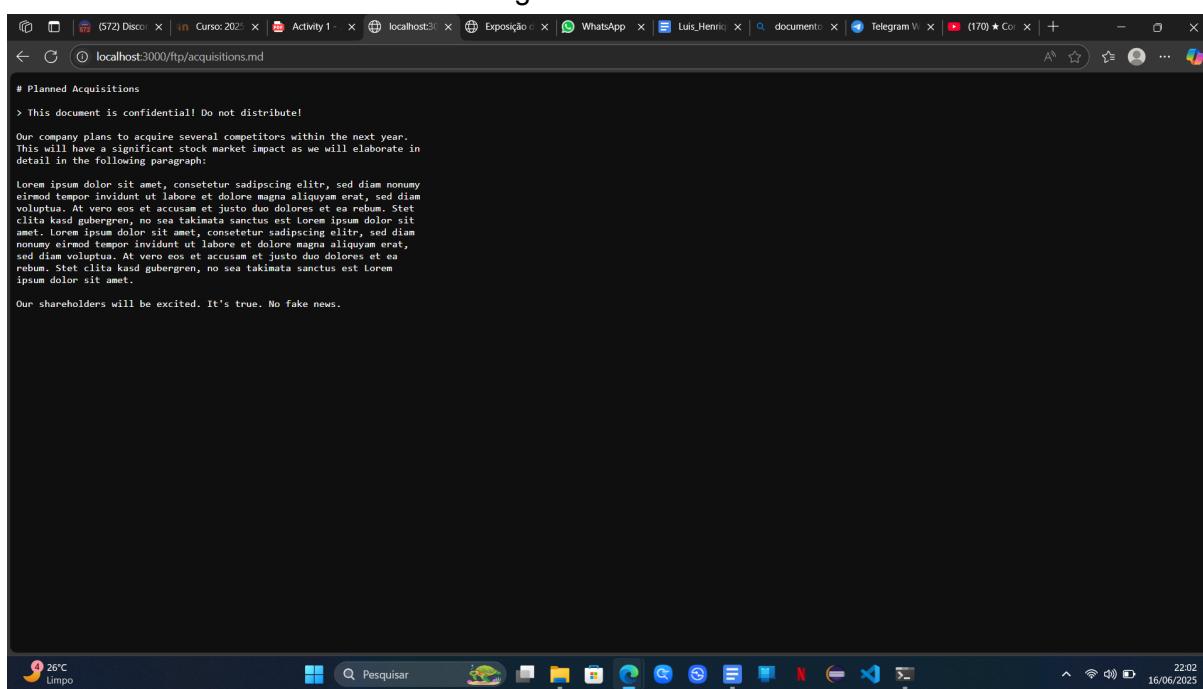
## Privacy Policy

A screenshot of a Windows desktop showing a web browser window for the OWASP Juice Shop. The page displays the 'Privacy Policy' challenge solved. It includes a green success message at the top. Below it is the actual privacy policy text, which states the effective date is March 15, 2019, and describes the collection, use, and disclosure of personal data. The taskbar at the bottom shows various open applications like Discord, WhatsApp, and Microsoft Office.

## Chatbot



## Confidential Document e Error Handling



You successfully solved a challenge: Error Handling (Provoked an error that is neither very gracefully nor consistently handled.)

You successfully solved a challenge: Confidential Document (Access a confidential document.)

## About Us

### Corporate History & Policy

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consetetur adipiscing elitr, sed diam nonumy nibh euismod tincidunt ut laoreet dolore magna aliquyam erat, sed diam voluptua. Check out our boring terms of use if you are interested in such lame stuff. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr. At accusam aliquyam diam diam dolore dolores duo eirmod eos erat, et nonumy sed tempor et invidunt justo labore Stet clita ea et gubergren, kasd magna rebum.

### Customer Feedback

```
# HELP file_uploads_count Total number of successful file uploads grouped by file type.
# TYPE file_uploads_count counter

# HELP file_upload_errors Total number of failed file uploads grouped by file type.
# TYPE file_upload_errors counter

# HELP juiceshop_startup_duration_seconds Duration juiceshop required to perform a certain task during startup
# TYPE juiceshop_startup_duration_seconds gauge
juiceshop_startup_duration_seconds{task="validateConfig",app="juiceshop"} 0.02539541
juiceshop_startup_duration_seconds{task="cleanUpOldFIFO",app="juiceshop"},0.0455386176
juiceshop_startup_duration_seconds{task="listDataSources",app="juiceshop"},0.196710886
juiceshop_startup_duration_seconds{task="datacreator",app="juiceshop"},1.743427531
juiceshop_startup_duration_seconds{task="customizeApplication",app="juiceshop"},0.008485702
juiceshop_startup_duration_seconds{task="customizeEasterEgg",app="juiceshop"},0.004308329
juiceshop_startup_duration_seconds{task="ready",app="juiceshop"},1.8

# HELP process_cpu_user_seconds_total Total user CPU time spent in seconds.
# TYPE process_cpu_user_seconds_total counter
process_cpu_user_seconds_total{app="juiceshop"} 38.058271

# HELP process_cpu_system_seconds_total Total system CPU time spent in seconds.
# TYPE process_cpu_system_seconds_total counter
process_cpu_system_seconds_total{app="juiceshop"} 11.765416

# HELP process_cpu_seconds_total Total user and system CPU time spent in seconds.
# TYPE process_cpu_seconds_total counter
process_cpu_seconds_total{app="juiceshop"},49.823687

# HELP process_start_time_seconds Start time of the process since unix epoch in seconds.
# TYPE process_start_time_seconds gauge
process_start_time_seconds{app="juiceshop"},1750119846

# HELP process_resident_memory_bytes Resident memory size in bytes.
# TYPE process_resident_memory_bytes gauge
process_resident_memory_bytes{app="juiceshop"},1835333568

# HELP process_virtual_memory_bytes Virtual memory size in bytes.
# TYPE process_virtual_memory_bytes gauge
process_virtual_memory_bytes{app="juiceshop"},1421316096

# HELP process_heap_bytes Process heap size in bytes.
# TYPE process_heap_bytes gauge
process_heap_bytes{app="juiceshop"},232042496

# HELP process_open_fds Number of open file descriptors.
# TYPE process_open_fds gauge
process_open_fds{app="juiceshop"},24
```

## Mass Dispel

localhost:3000/#/score-board?difficulties=1

# OWASP Juice Shop

You successfully solved a challenge: Mass Dispel (Close multiple "Challenge solved"-notifications in one go.)

**14%**  
Hacking Challenges

**0%**  
Coding Challenges

**15/172**  
Challenges Solved

1	2	3
13/28	2/23	0/44
4	5	6
0/37	0/26	0/14

Search
Difficulty: 1
Status
Tags
Filter
Settings

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
XXE

17 challenges are unavailable on Docker due to security concerns or technical incompatibility! Hide disabled challenges

Miscellaneous

- Score Board

XSS

- DOM XSS

XSS

- Bonus Payload

Miscellaneous

- Privacy Policy

6 25°C Limpio

9:25 17/06/2025

## Missing Encoding

localhost:3000/#/photo-wall

# OWASP Juice Shop

You successfully solved a challenge: Missing Encoding (Retrieve the photo of Björn's cat in "melee combat-mode")

## Photo Wall

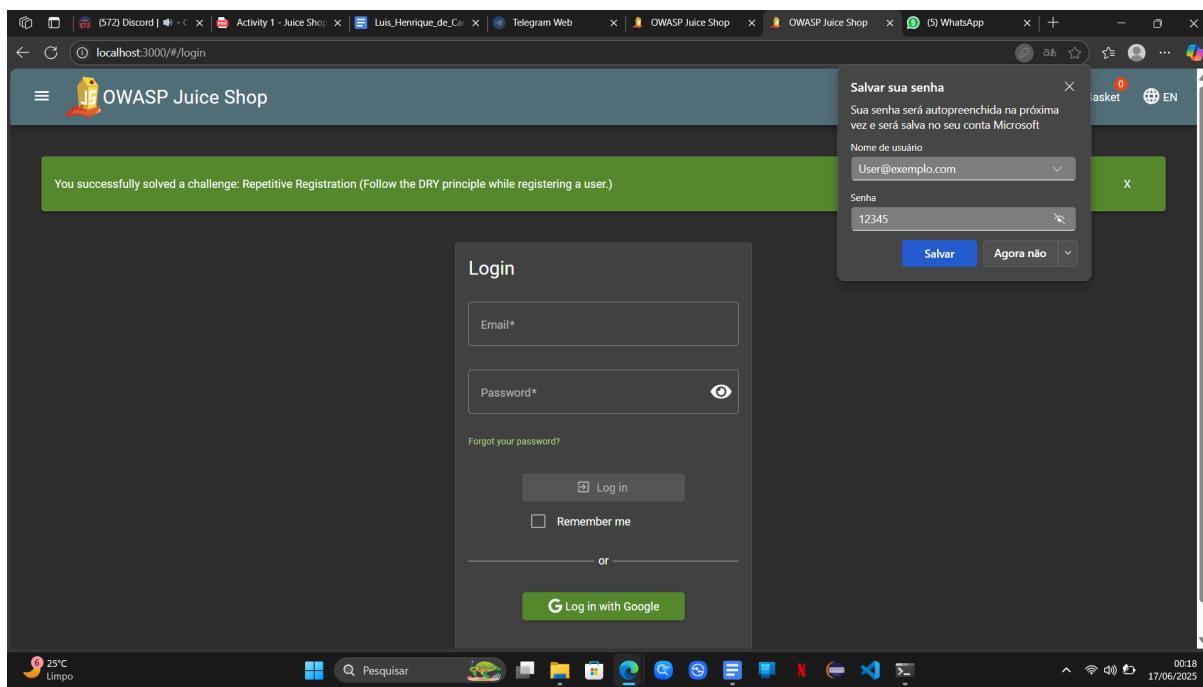
The screenshot shows a browser window displaying the OWASP Juice Shop application. The user has solved a challenge titled 'Missing Encoding'. On the right side of the screen, the developer tools' Elements tab is open, showing the HTML structure of a photo card. The card contains a image element with a src attribute pointing to a file named 'lego-157280069477.jpg'. The developer tools also show the CSS styles applied to the card, including classes like 'mat-card' and 'mat-card-elevation-2'. The browser's status bar at the bottom indicates it's 22:55 on June 16, 2025.

## Outdated allowlist

The screenshot shows the OWASP Juice Shop application running on localhost:3000. The dashboard displays progress for Hacking Challenges (10%) and Coding Challenges (0%). It also shows 11/172 challenges solved, with a breakdown of difficulty levels (9/28, 2/23, 0/44) and status (0/37, 0/26, 0/14). Below the dashboard are search, difficulty, status, and tags filters. On the right, a browser developer tools window is open, showing the main.js file with code related to wallet management and QR code generation.

The screenshot shows the Blockchain.com explorer interface for the Bitcoin address 1AbKf-8DRZm. The address is highlighted in orange. The balance is shown as 0.00005997 BTC or \$6,41. The "Summary" section provides details about the address's activity, including total received (0.01314466 BTC), total sent (0.01308449 BTC), and total volume (0.02622895 BTC). Below this, the "Transactions" section lists two recent transactions: one from ID 7e51-0df0 to bc1q-rax3, and another from ID c801-3916 to 1AbK-DRZm.

## Repetitive Registration



## Web3 Sandbox

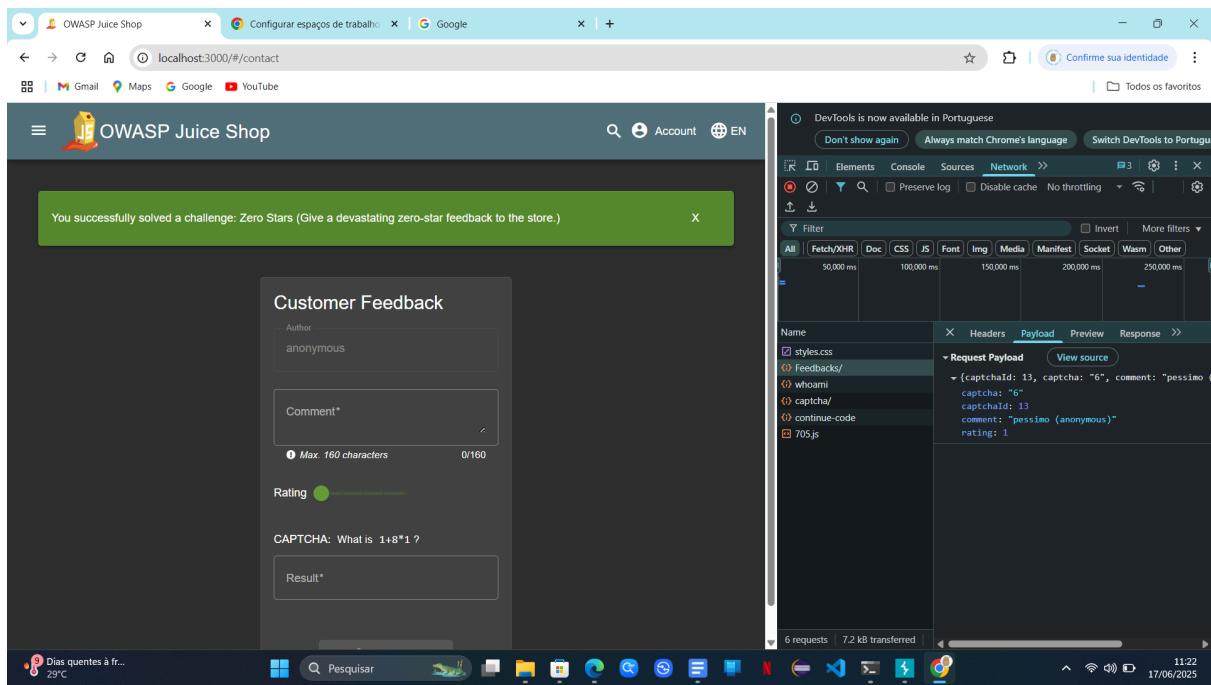
The screenshot shows a browser window for the Web3 Sandbox application. On the left, there is a "Contract Editor" pane displaying Solidity code for a HelloWorld contract:

```
1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.14;
3
4 contract HelloWorld {
5     function get()public pure returns (string memory){
6         return 'Hello Contracts';
7     }
8 }
```

On the right, there is a "Web3 Code Sandbox" pane with the following sections:

- Connect your MetaMask** button
- Web3 Code Sandbox** section with a bulleted list:
  - Easily compile/deploy and invoke smart contracts from below
  - You can pass ETH to the contract both while invoking/deploying by entering the GWEI Value post compilation
- Select compiler version** dropdown set to "0.8.21"
- Compile Contract** button
- Contract to deploy** section with a dropdown menu set to "Compiled Contracts" and a "GWEI value for sending ETH" input field containing "0".
- Deploy selected Contract** button

Zero stars



```
luish@BOOK-G8FM15I00Q: $ curl 'http://localhost:3000/api/Feedbacks/' \
-H 'Accept: application/json, text/plain, */*' \
-H 'Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7,es;q=0.6' \
-H 'Connection: keep-alive' \
-H 'Content-Type: application/json' \
-b 'language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss' \
-H 'Origin: http://localhost:3000' \
-H 'Referer: http://localhost:3000/' \
-H 'Sec-Fetch-Dest: empty' \
-H 'Sec-Fetch-Mode: cors' \
-H 'Sec-Fetch-Site: same-origin' \
-H 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36' \
-H 'sec-ch-ua: "Google Chrome";v="137", "Chromium";v="137", "Not/A)Brand";v="24"' \
-H 'sec-ch-ua-mobile: ?0' \
-H 'sec-ch-ua-platform: "Windows"' \
--data-raw '{"captchaId":13,"captcha":"6","comment":"pessimo (anonymous)","rating":0}' \
{"status": "success", "data": {"id": 17, "comment": "pessimo (anonymous)", "rating": 0, "updatedAt": "2025-06-17T14:22:12.990Z", "createdAt": "2025-06-17T14:22:12.990Z", "UserId": null}} luish@BOOK-G8FM15I00Q: $
```

Final:

OWASP Juice Shop   Configurar espaços de trabalho | Google

localhost:3000/#/score-board?difficulties=1

Gmail Maps Google YouTube

Todos os favoritos

The screenshot shows a grid of challenges from the OWASP Juice Shop. Each challenge card includes a title, a brief description, a difficulty rating (star), and several interaction buttons (Tutorial, Good for Demos, With Coding Challenge, Hint).

- Miscellaneous**
  - Score Board** ★  
Find the carefully hidden 'Score Board' page.  
Tutorial, Code Analysis, With Coding Challenge, Hint
  - Bully Chatbot** ★  
Receive a coupon code from the support chatbot.  
Shenanigans, Brute Force, Hint
  - Mass Dispel** ★  
Close multiple "Challenge solved"-notifications in one go.  
Hint
  - Web3 Sandbox** ★  
Find an accidentally deployed code sandbox for writing smart contracts on the fly.  
Web3, With Coding Challenge, Hint
- XSS**
  - DOM XSS** ★  
Perform a DOM XSS attack with <iframe>  
Tutorial, Good for Demos, With Coding Challenge, Hint
  - Bonus Payload** ★  
Use the bonus payload <iframe width="100%">  
Shenanigans, Tutorial, With Coding Challenge, Hint
- Sensitive Data Exposure**
  - Confidential Document** ★  
Access a confidential document.  
Good for Demos, With Coding Challenge, Hint
  - Exposed Metrics** ★  
Find the endpoint that serves usage data to be scraped by a popular monitoring system.  
Good Practice, With Coding Challenge, Hint
- Security Misconfiguration**
  - Error Handling** ★  
Provoke an error that is neither very gracefully nor consistently handled.  
Prerequisite, Hint
  - Outdated Allowlist** ★  
Let us redirect you to one of our crypto currency  
Shenanigans, With Coding Challenge, Hint
  - Repetitive Registration** ★  
Follow the DRY principle while registering a user.  
Code Analysis, With Coding Challenge, Hint
- Improper Input Validation**
  - Missing Encoding** ★  
Retrieve the photo of Björn's cat in "melee combat-mode".  
Shenanigans, Hint
  - Zero Stars** ★  
Give a devastating zero-star feedback to the store.  
Hint

Principais Notícias  
G7 pede 'desesc...' 11:25  
Pesquisar 17/06/2025