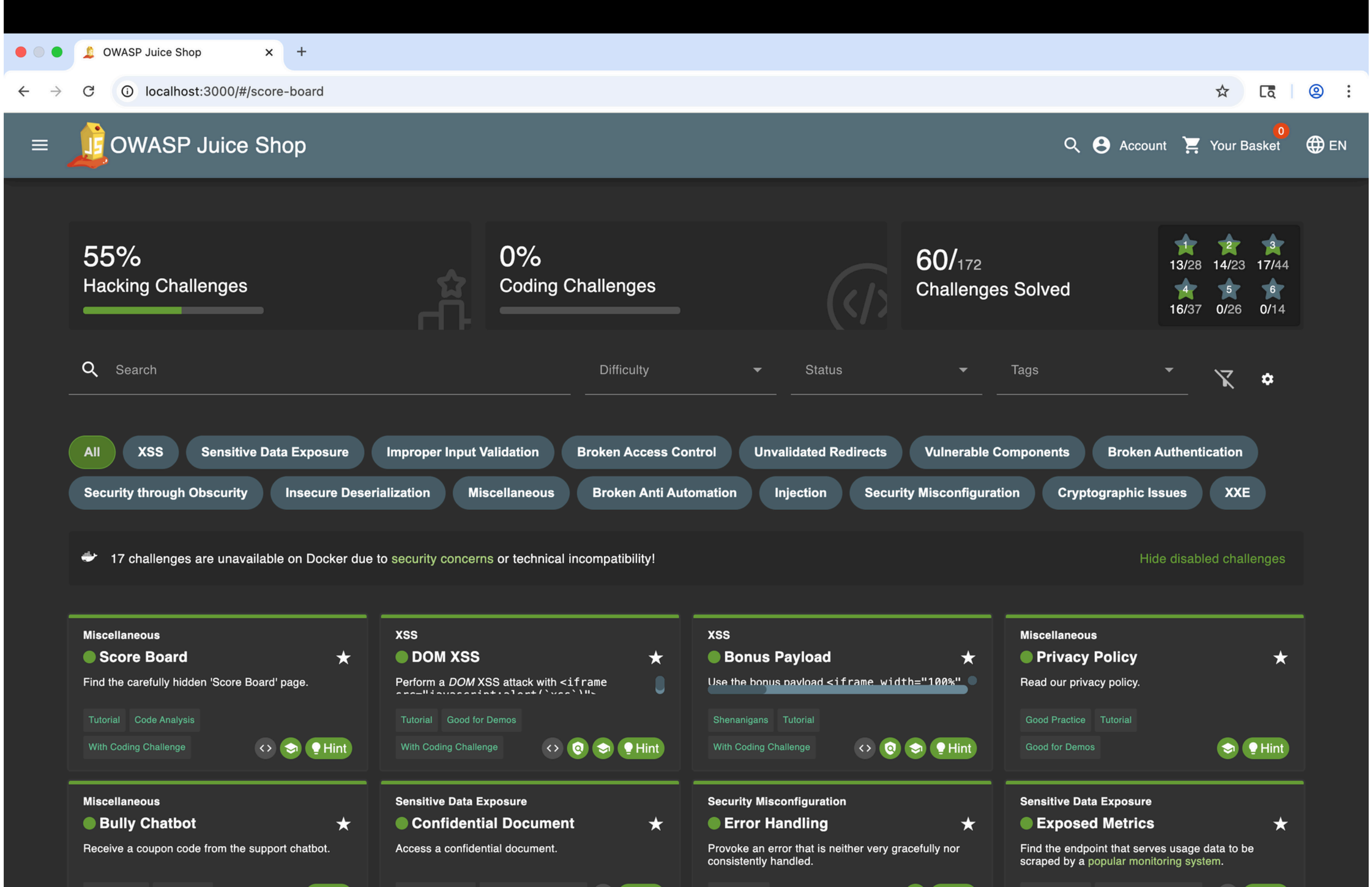
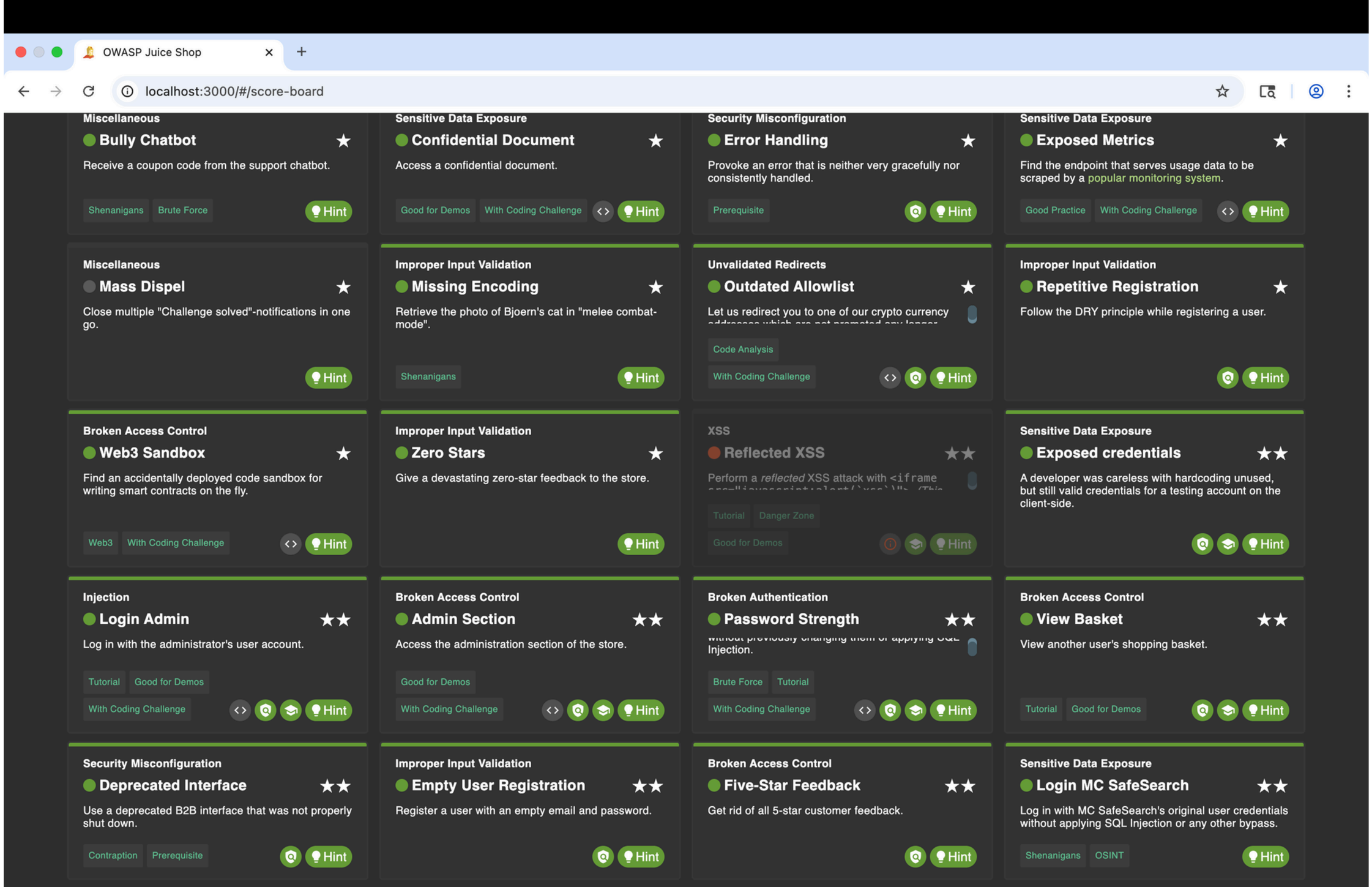
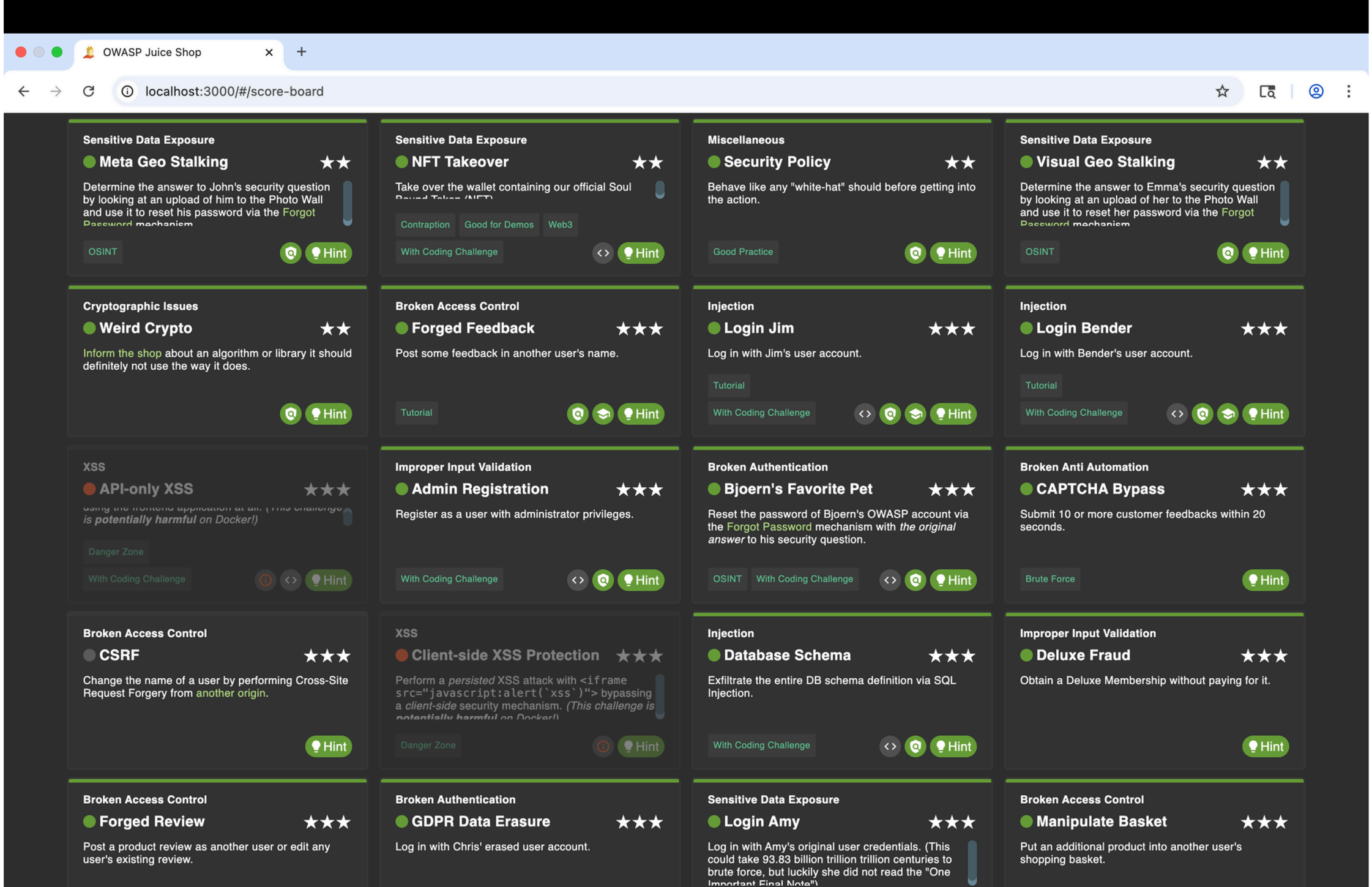
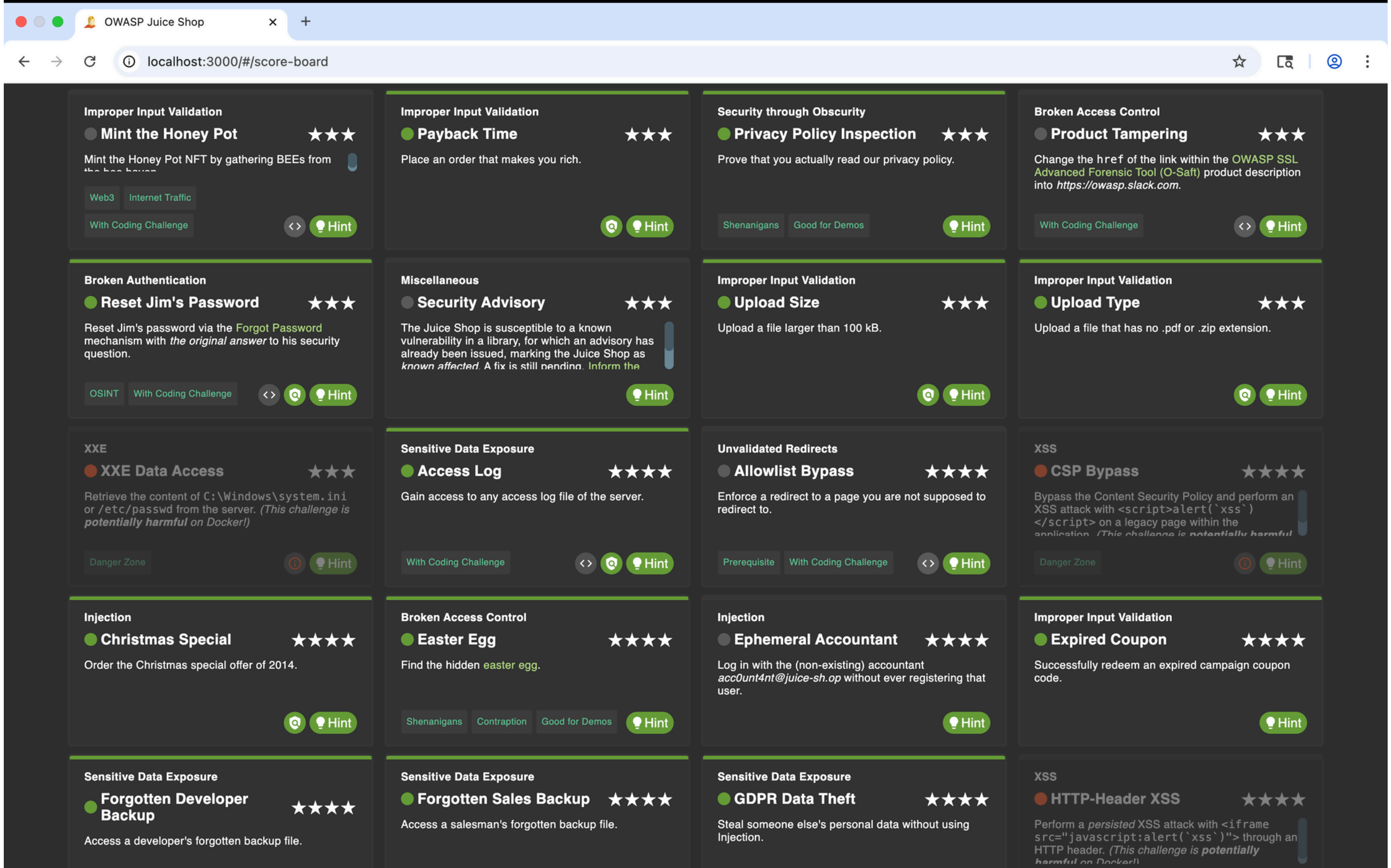
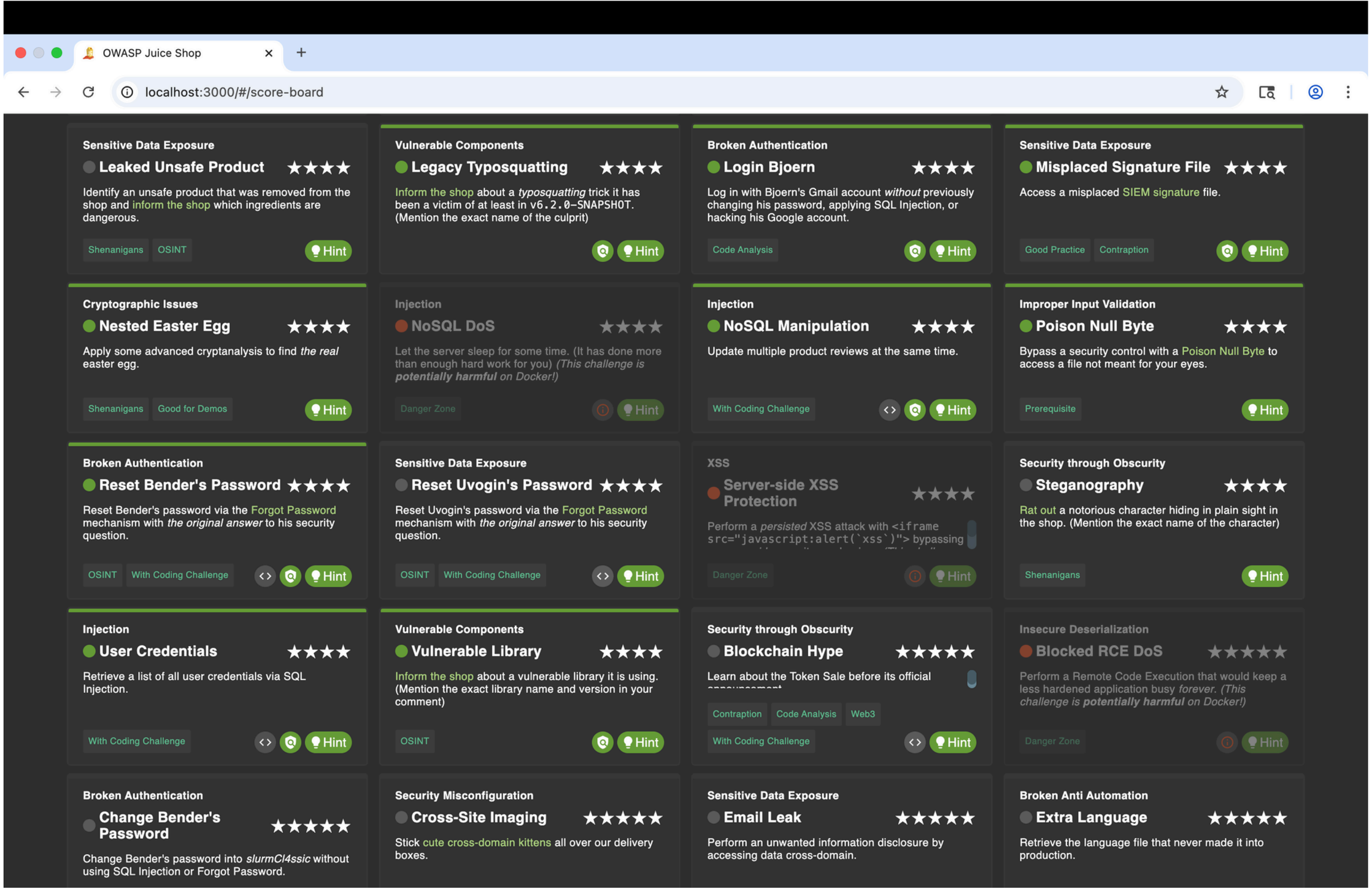

OWASP Juice Shop
localhost:3000/#/score-board
OWASP Juice Shop
Account
Your Basket
0
EN
55%
Hacking Challenges
0%
Coding Challenges
60/172
Challenges Solved
1 13/28
2 14/23
3 17/44
4 16/37
5 0/26
6 0/14
Search
Difficulty
Status
Tags
All
XSS
Sensitive Data Exposure
Improper Input Validation
Broken Access 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
Find the carefully hidden 'Score Board' page.
Tutorial
Code Analysis
With Coding Challenge
Hint
XSS
DOM XSS
Perform a DOM XSS attack with
Tutorial
Good for Demos
With Coding Challenge
Hint
XSS
Bonus Payload
Use the bonus payload
Shenanigans
Tutorial
With Coding Challenge
Hint
Miscellaneous
Privacy Policy
Read our privacy policy.
Good Practice
Tutorial
Good for Demos
Hint
Miscellaneous
Bully Chatbot
Receive a coupon code from the support chatbot.
Sensitive Data Exposure
Confidential Document
Access a confidential document.
Security Misconfiguration
Error Handling
Provoke an error that is neither very gracefully nor consistently handled.
Sensitive Data Exposure
Exposed Metrics
Find the endpoint that serves usage data to be scraped by a popular monitoring system.


OWASP Juice Shop
localhost:3000/#/score-board
Miscellaneous
Bully Chatbot
Receive a coupon code from the support chatbot.
Shenanigans
Brute Force
Hint
Sensitive Data Exposure
Confidential Document
Access a confidential document.
Good for Demos
With Coding Challenge
Hint
Security Misconfiguration
Error Handling
Provoke an error that is neither very gracefully nor consistently handled.
Prerequisite
Hint
Sensitive Data Exposure
Exposed Metrics
Find the endpoint that serves usage data to be scraped by a popular monitoring system.
Good Practice
With Coding Challenge
Hint
Miscellaneous
Mass Dispel
Close multiple "Challenge solved"-notifications in one go.
Hint
Improper Input Validation
Missing Encoding
Retrieve the photo of Bjoern's cat in "melee combat-mode".
Shenanigans
Hint
Unvalidated Redirects
Outdated Allowlist
Let us redirect you to one of our crypto currency
Code Analysis
With Coding Challenge
Hint
Improper Input Validation
Repetitive Registration
Follow the DRY principle while registering a user.
Hint
Broken Access Control
Web3 Sandbox
Find an accidentally deployed code sandbox for writing smart contracts on the fly.
Web3
With Coding Challenge
Hint
Improper Input Validation
Zero Stars
Give a devastating zero-star feedback to the store.
Hint
XSS
Reflected XSS
Perform a reflected XSS attack with <iframe
Tutorial
Danger Zone
Good for Demos
Hint
Sensitive Data Exposure
Exposed credentials
A developer was careless with hardcoding unused, but still valid credentials for a testing account on the client-side.
Hint
Injection
Login Admin
Log in with the administrator's user account.
Tutorial
Good for Demos
With Coding Challenge
Hint
Broken Access Control
Admin Section
Access the administration section of the store.
Good for Demos
With Coding Challenge
Hint
Broken Authentication
Password Strength
Injection.
Brute Force
Tutorial
With Coding Challenge
Hint
Broken Access Control
View Basket
View another user's shopping basket.
Tutorial
Good for Demos
Hint
Security Misconfiguration
Deprecated Interface
Use a deprecated B2B interface that was not properly shut down.
Contraption
Prerequisite
Hint
Improper Input Validation
Empty User Registration
Register a user with an empty email and password.
Hint
Broken Access Control
Five-Star Feedback
Get rid of all 5-star customer feedback.
Hint
Sensitive Data Exposure
Login MC SafeSearch
Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass.
Shenanigans
OSINT
Hint


OWASP Juice Shop
localhost:3000/#/score-board
Sensitive Data Exposure
Meta Geo Stalking
Determine the answer to John's security question by looking at an upload of him to the Photo Wall and use it to reset his password via the Forgot Password mechanism
OSINT
Hint
Sensitive Data Exposure
NFT Takeover
Take over the wallet containing our official Soul
Contraption
Good for Demos
Web3
With Coding Challenge
Hint
Miscellaneous
Security Policy
Behave like any "white-hat" should before getting into the action.
Good Practice
Hint
Sensitive Data Exposure
Visual Geo Stalking
Determine the answer to Emma's security question by looking at an upload of her to the Photo Wall and use it to reset her password via the Forgot Password mechanism
OSINT
Hint
Cryptographic Issues
Weird Crypto
Inform the shop about an algorithm or library it should definitely not use the way it does.
Hint
Broken Access Control
Forged Feedback
Post some feedback in another user's name.
Tutorial
Hint
Injection
Login Jim
Log in with Jim's user account.
Tutorial
With Coding Challenge
Hint
Injection
Login Bender
Log in with Bender's user account.
Tutorial
With Coding Challenge
Hint
XSS
API-only XSS
is potentially harmful on Docker!)
Danger Zone
With Coding Challenge
Hint
Improper Input Validation
Admin Registration
Register as a user with administrator privileges.
With Coding Challenge
Hint
Broken Authentication
Bjoern's Favorite Pet
Reset the password of Bjoern's OWASP account via the Forgot Password mechanism with the original answer to his security question.
OSINT
With Coding Challenge
Hint
Broken Anti Automation
CAPTCHA Bypass
Submit 10 or more customer feedbacks within 20 seconds.
Brute Force
Hint
Broken Access Control
CSRF
Change the name of a user by performing Cross-Site Request Forgery from another origin.
Hint
XSS
Client-side XSS Protection
Perform a persisted XSS attack with <iframe src="javascript:alert(`xss`)"> bypassing a client-side security mechanism. (This challenge is
Danger Zone
Hint
Injection
Database Schema
Exfiltrate the entire DB schema definition via SQL Injection.
With Coding Challenge
Hint
Improper Input Validation
Deluxe Fraud
Obtain a Deluxe Membership without paying for it.
Hint
Broken Access Control
Forged Review
Post a product review as another user or edit any user's existing review.
Broken Authentication
GDPR Data Erasure
Log in with Chris' erased user account.
Sensitive Data Exposure
Login Amy
Log in with Amy's original user credentials. (This could take 93.83 billion trillion trillion centuries to brute force, but luckily she did not read the "One
Broken Access Control
Manipulate Basket
Put an additional product into another user's shopping basket.


OWASP Juice Shop
localhost:3000/#/score-board
Improper Input Validation
Mint the Honey Pot
Mint the Honey Pot NFT by gathering BEEs from
Web3
Internet Traffic
With Coding Challenge
Hint
Improper Input Validation
Payback Time
Place an order that makes you rich.
Hint
Security through Obscurity
Privacy Policy Inspection
Prove that you actually read our privacy policy.
Shenanigans
Good for Demos
Hint
Broken Access Control
Product Tampering
Change the href of the link within the OWASP SSL Advanced Forensic Tool (O-Saft) product description into https://owasp.slack.com.
With Coding Challenge
Hint
Broken Authentication
Reset Jim's Password
Reset Jim's password via the Forgot Password mechanism with the original answer to his security question.
OSINT
With Coding Challenge
Hint
Miscellaneous
Security Advisory
The Juice Shop is susceptible to a known vulnerability in a library, for which an advisory has already been issued, marking the Juice Shop as known affected. A fix is still pending. Inform the
Hint
Improper Input Validation
Upload Size
Upload a file larger than 100 kB.
Hint
Improper Input Validation
Upload Type
Upload a file that has no .pdf or .zip extension.
Hint
XXE
XXE Data Access
Retrieve the content of C:\Windows\system.ini or /etc/passwd from the server. (This challenge is potentially harmful on Docker!)
Danger Zone
Hint
Sensitive Data Exposure
Access Log
Gain access to any access log file of the server.
With Coding Challenge
Hint
Unvalidated Redirects
Allowlist Bypass
Enforce a redirect to a page you are not supposed to redirect to.
Prerequisite
With Coding Challenge
Hint
XSS
CSP Bypass
Bypass the Content Security Policy and perform an XSS attack with <script>alert(`xss`)</script> on a legacy page within the
Danger Zone
Hint
Injection
Christmas Special
Order the Christmas special offer of 2014.
Hint
Broken Access Control
Easter Egg
Find the hidden easter egg.
Shenanigans
Contraption
Good for Demos
Hint
Injection
Ephemeral Accountant
Log in with the (non-existing) accountant acc0unt4nt@juice-sh.op without ever registering that user.
Hint
Improper Input Validation
Expired Coupon
Successfully redeem an expired campaign coupon code.
Hint
Sensitive Data Exposure
Forgotten Developer Backup
Access a developer's forgotten backup file.
Sensitive Data Exposure
Forgotten Sales Backup
Access a salesman's forgotten backup file.
Sensitive Data Exposure
GDPR Data Theft
Steal someone else's personal data without using Injection.
XSS
HTTP-Header XSS
Perform a persisted XSS attack with <iframe src="javascript:alert(`xss`)"> through an HTTP header. (This challenge is potentially


OWASP Juice Shop
localhost:3000/#/score-board
Sensitive Data Exposure
Leaked Unsafe Product
Identify an unsafe product that was removed from the shop and inform the shop which ingredients are dangerous.
Shenanigans
OSINT
Hint
Vulnerable Components
Legacy Typosquatting
Inform the shop about a typosquatting trick it has been a victim of at least in v6.2.0-SNAPSHOT. (Mention the exact name of the culprit)
Hint
Broken Authentication
Login Bjoern
Log in with Bjoern's Gmail account without previously changing his password, applying SQL Injection, or hacking his Google account.
Code Analysis
Hint
Sensitive Data Exposure
Misplaced Signature File
Access a misplaced SIEM signature file.
Good Practice
Contraption
Hint
Cryptographic Issues
Nested Easter Egg
Apply some advanced cryptanalysis to find the real easter egg.
Shenanigans
Good for Demos
Hint
Injection
NoSQL DoS
Let the server sleep for some time. (It has done more than enough hard work for you) (This challenge is potentially harmful on Docker!)
Danger Zone
Hint
Injection
NoSQL Manipulation
Update multiple product reviews at the same time.
With Coding Challenge
Hint
Improper Input Validation
Poison Null Byte
Bypass a security control with a Poison Null Byte to access a file not meant for your eyes.
Prerequisite
Hint
Broken Authentication
Reset Bender's Password
Reset Bender's password via the Forgot Password mechanism with the original answer to his security question.
OSINT
With Coding Challenge
Hint
Sensitive Data Exposure
Reset Uvogin's Password
Reset Uvogin's password via the Forgot Password mechanism with the original answer to his security question.
OSINT
With Coding Challenge
Hint
XSS
Server-side XSS Protection
Perform a persisted XSS attack with <iframe src="javascript:alert(`xss`)"> bypassing
Danger Zone
Hint
Security through Obscurity
Steganography
Rat out a notorious character hiding in plain sight in the shop. (Mention the exact name of the character)
Shenanigans
Hint
Injection
User Credentials
Retrieve a list of all user credentials via SQL Injection.
With Coding Challenge
Hint
Vulnerable Components
Vulnerable Library
Inform the shop about a vulnerable library it is using. (Mention the exact library name and version in your comment)
OSINT
Hint
Security through Obscurity
Blockchain Hype
Learn about the Token Sale before its official
Contraption
Code Analysis
Web3
With Coding Challenge
Hint
Insecure Deserialization
Blocked RCE DoS
Perform a Remote Code Execution that would keep a less hardened application busy forever. (This challenge is potentially harmful on Docker!)
Danger Zone
Hint
Broken Authentication
Change Bender's Password
Change Bender's password into slurmCl4ssic without using SQL Injection or Forgot Password.
Security Misconfiguration
Cross-Site Imaging
Stick cute cross-domain kittens all over our delivery boxes.
Sensitive Data Exposure
Email Leak
Perform an unwanted information disclosure by accessing data cross-domain.
Broken Anti Automation
Extra Language
Retrieve the language file that never made it into production.