

Relatório – Desafios de hack so site Juice Shop

Data: 29/06/2025

1. Desafio: Score Board (Broken Access Control)

O que eu fiz:

- Acessei o site do Juice Shop localmente no navegador usando o link: `http://localhost:3000`
- Sem fazer login, abri o menu lateral clicando no botão `≡` no canto superior esquerdo.
- Cliquei na opção “Score Board”.
- A página abriu normalmente e mostrou todos os desafios disponíveis, inclusive os que já estavam resolvidos.

O que deveria acontecer:

- Essa área só deveria ser acessível por usuários logados.

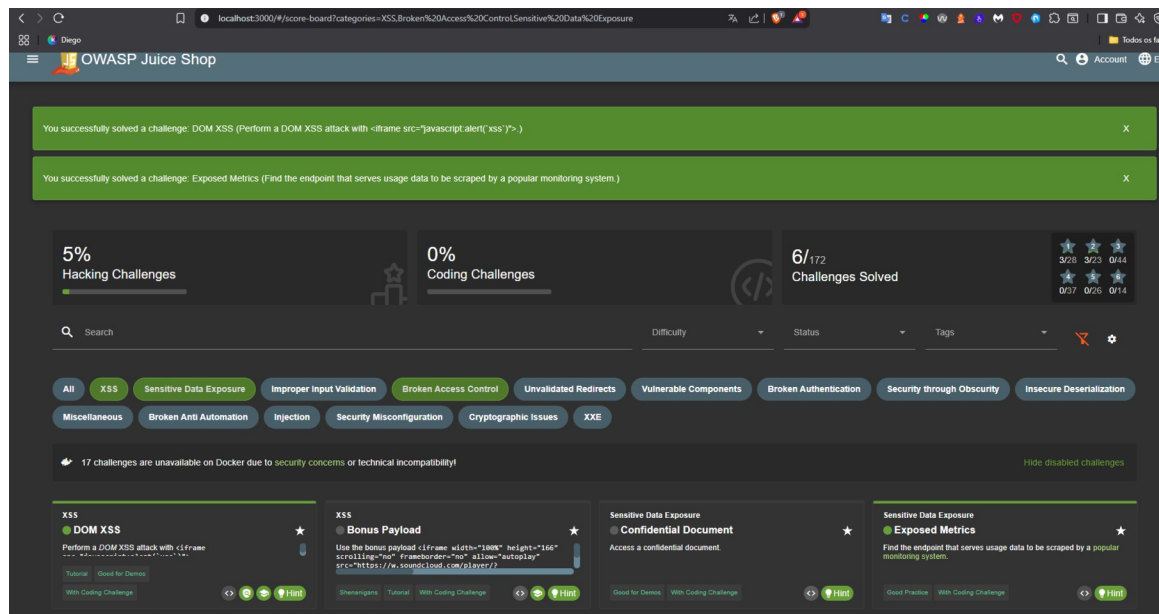
O que está errado:

- O sistema não verifica se a pessoa está autenticada (logada).
- Isso é uma falha chamada “Broken Access Control” (controle de acesso quebrado), porque deixa qualquer um ver algo que deveria ser restrito.

Impacto:

- Uma pessoa pode descobrir detalhes sobre o funcionamento do sistema sem permissão.

Evidência:



2. Desafio: Login sem senha (SQL Injection)

O que eu fiz:

- Fui até a tela de login: `http://localhost:3000/#/login`
- No campo Email, digitei: `' OR 1=1--`
- No campo Senha, coloquei: `123456`
- Depois cliquei no botão “Log in”.

O que aconteceu:

- O sistema me deixou entrar, mesmo sem fornecer um e-mail e senha válidos.

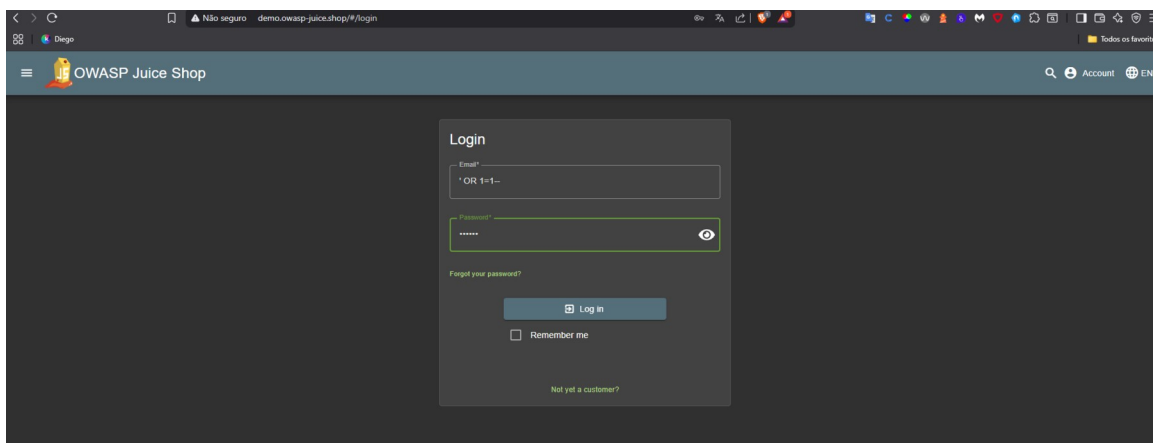
Por que isso acontece:

- Esse é um caso clássico de SQL Injection.
- O que o sistema entendeu foi: “se o campo email for verdadeiro OU 1=1 (que sempre é verdadeiro), então permita o login”.
- O `--` no final serve para comentar o resto da consulta.

Impacto:

- Qualquer pessoa pode conseguir acesso ao sistema sem credenciais válidas.
- Isso representa uma brecha de segurança grave.

---Evidência:



3. Desafio: DOM XSS com <iframe>

O que eu fiz:

- Fui até a página “Customer Feedback”: <http://localhost:3000/#/contact>
- Preenchi o nome e email com qualquer valor.
- No campo de comentário escrevi: `<iframe src="javascript:alert('XSS')">`
- Enviei o formulário.
- Depois, ao visualizar a mensagem no site, apareceu um alerta no navegador com a mensagem “XSS”.

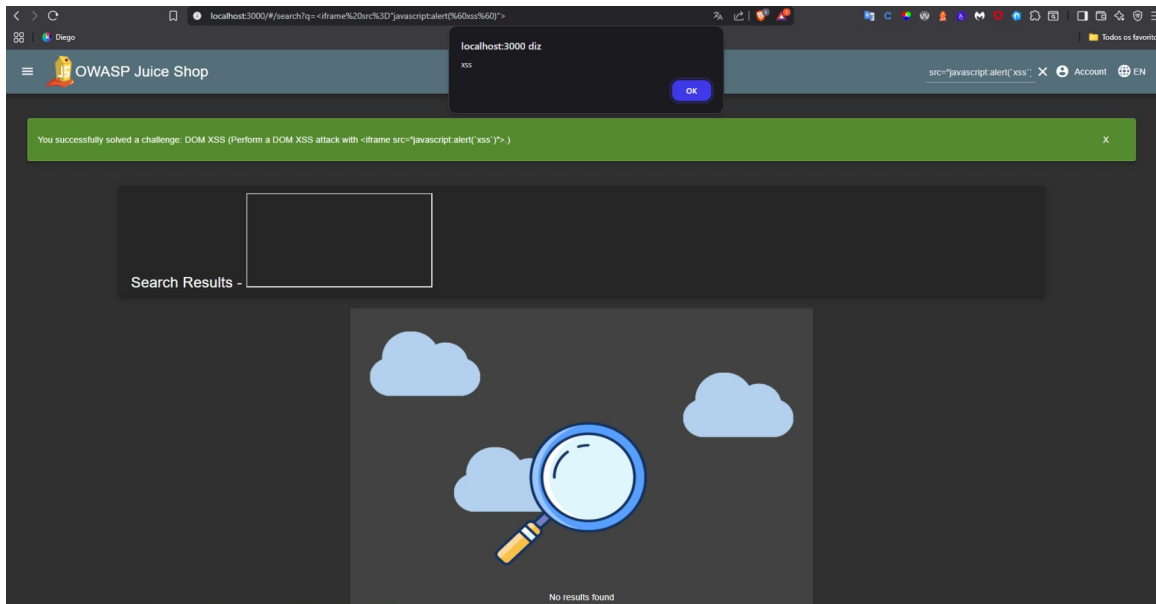
O que significa:

- O site executou um código JavaScript malicioso que eu mesmo inseri.
- Isso é uma falha chamada XSS (Cross-Site Scripting), do tipo DOM-based.

Impacto:

- Permite que atacantes executem scripts maliciosos no navegador dos usuários.

Evidencia:



4. Desafio: Exposed Metrics (/metrics)

O que eu fiz:

- Digitei diretamente no navegador o seguinte endereço: <http://localhost:3000/metrics>
- A página carregou várias informações internas da aplicação.

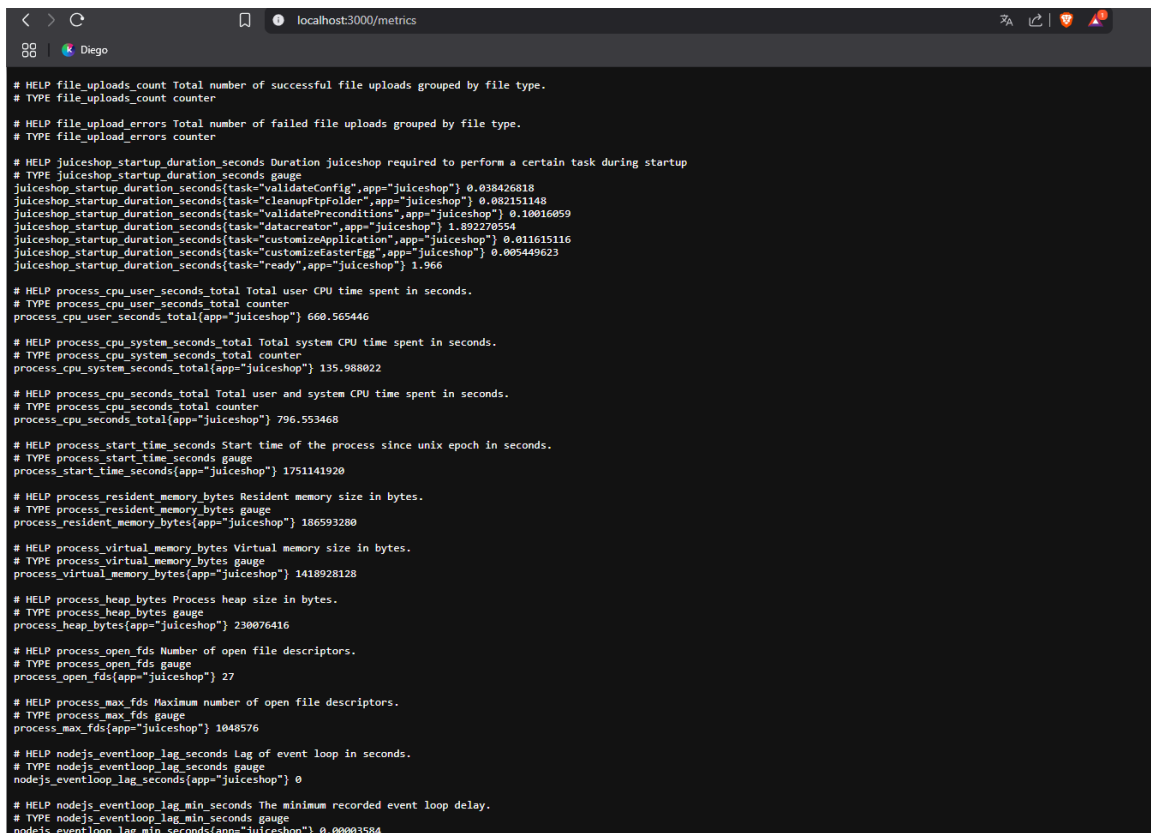
O que está errado:

- Essa rota deveria ser protegida e acessível apenas a administradores.

Impacto:

- Um invasor pode usar essas informações para entender melhor o sistema e encontrar novas falhas.

Evidencia:



```
# 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"} 0.038426818
juiceshop_startup_duration_seconds{task="cleanupFtpFolder",app="juiceshop"} 0.082151148
juiceshop_startup_duration_seconds{task="validatePreconditions",app="juiceshop"} 0.10016059
juiceshop_startup_duration_seconds{task="datacreator",app="juiceshop"} 1.892270554
juiceshop_startup_duration_seconds{task="customizeApplication",app="juiceshop"} 0.011615116
juiceshop_startup_duration_seconds{task="customizeEasterEgg",app="juiceshop"} 0.005449623
juiceshop_startup_duration_seconds{task="ready",app="juiceshop"} 1.966

# 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"} 660.565446

# 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"} 135.988022

# 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"} 796.553468

# 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"} 1751141920

# HELP process_resident_memory_bytes Resident memory size in bytes.
# TYPE process_resident_memory_bytes gauge
process_resident_memory_bytes{app="juiceshop"} 186593280

# HELP process_virtual_memory_bytes Virtual memory size in bytes.
# TYPE process_virtual_memory_bytes gauge
process_virtual_memory_bytes{app="juiceshop"} 1418928128

# HELP process_heap_bytes Process heap size in bytes.
# TYPE process_heap_bytes gauge
process_heap_bytes{app="juiceshop"} 230076416

# HELP process_open_fds Number of open file descriptors.
# TYPE process_open_fds gauge
process_open_fds{app="juiceshop"} 27

# HELP process_max_fds Maximum number of open file descriptors.
# TYPE process_max_fds gauge
process_max_fds{app="juiceshop"} 1048576

# HELP nodejs_eventloop_lag_seconds Lag of event loop in seconds.
# TYPE nodejs_eventloop_lag_seconds gauge
nodejs_eventloop_lag_seconds{app="juiceshop"} 0

# HELP nodejs_eventloop_lag_min_seconds The minimum recorded event loop delay.
# TYPE nodejs_eventloop_lag_min_seconds gauge
nodejs_eventloop_lag_min_seconds{app="juiceshop"} 0.00003584
```

5. Desafio: View Basket (Ver carrinho de outro usuário)

O que eu fiz:

- Acesse o site e, sem estar logado, cliquei em um produto e adicionei ao carrinho.
- Mesmo como usuário anônimo, o sistema criou um carrinho para mim.
- Abri o console do navegador (F12 > aba Network) e vi uma requisição como:
GET http://localhost:3000/rest/basket/3
- Troquei o número da URL, por exemplo: http://localhost:3000/rest/basket/1
- E consegui acessar o carrinho de outro usuário!

O problema:

- O sistema não verifica se aquele carrinho realmente pertence ao usuário atual.

Impacto:

- Exposição de dados pessoais e possibilidade de interferência em compras alheias.