13 - OSWAP-A01 [Reto] – curl como herramienta de auditoría

Vamos a usar OWASP Juice Shop para poner en práctica esta tarea.

Es una app oficial moderna para practicar el OWASP

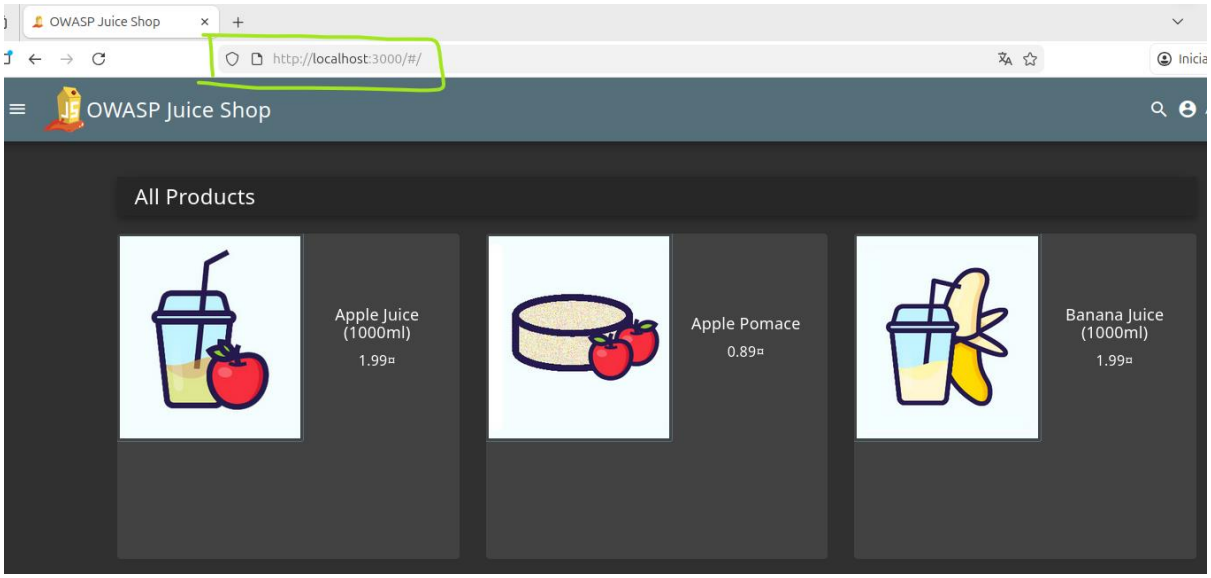
Tiene:

- login
- roles (user / admin)
- pedidos
- carrito
- APIs REST reales
- muchas vulnerabilidades A01 reales (IDOR, bypass, etc.)

Y lo más importante puedemos auditarla solo con curl.

Instalación

```
rui@rui-VMware-Virtual-Platform:~$ sudo docker run -d -p 3000:3000 bkimminich/juice-shop
[sudo] contraseña para rui:
Unable to find image 'bkimminich/juice-shop:latest' locally
latest: Pulling from bkimminich/juice-shop
fd4aa3667332: Pull complete
bfb59b82a9b6: Pull complete
017886f7e176: Pull complete
```



Vemos que tenemos curl

```
rui@rui-VMware-Virtual-Platform:~$ curl --version
curl 8.5.0 (x86_64-pc-linux-gnu) libcurl/8.5.0 OpenSSL/3.0.13 zlib/1.3 brotli/1.1.0 zstd/1.5.5 lib
idn2/2.3.7 libpsl/0.21.2 (+libidn2/2.3.7) libssh/0.10.6/openssl/zlib nghttp2/1.59.0 librtmp/2.3 Op
enLDAP/2.6.10
```

Acceso sin login

curl -i http://localhost:3000/rest/basket/1

Si devuelve datos hay Broken Access Control.

```
rui@rui-VMware-Virtual-Platform:~$ curl -i http://localhost:3000/rest/basket/1
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Date: Tue, 17 Feb 2026 11:29:45 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Transfer-Encoding: chunked

<html>
  <head>
    <meta charset='utf-8'>
    <title>UnauthorizedError: No Authorization header was found</title>
    <style>* {
  margin: 0;
  padding: 0;
  outline: 0;
```

Panel admin.

Vemos que devuelve 200 por lo que es un fallo crítico.

```
rui@rui-VMware-Virtual-Platform:~$ curl -b cookies.txt -i http://localhost:3000/administration
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Tue, 17 Feb 2026 11:26:24 GMT
ETag: W/"1252f-19c6b59f951"
Content-Type: text/html; charset=UTF-8
Content-Length: 75055
Vary: Accept-Encoding
Date: Tue, 17 Feb 2026 11:35:32 GMT
Connection: keep-alive
Keep-Alive: timeout=5
```

Vemos que no podemos ver la cesta de otros usuarios. Por lo que no hay brecha en ese caso

```
rui@rui-VMware-Virtual-Platform:~$ curl -b cookies.txt -i http://localhost:3000/rest/basket/3
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Date: Tue, 17 Feb 2026 11:39:04 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Transfer-Encoding: chunked
```

```
rui@rui-VMware-Virtual-Platform:~$ curl -b cookies.txt \
  -D headers.txt \
  -o body.txt \
  -w "STATUS=%{http_code}\n" \
  http://localhost:3000/rest/basket/2
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   972    0   972    0     0   226k      0 --:--:-- --:--:-- --:--:--  237k
STATUS=401
```