



Actividad | 1 | Pérdida de Autenticación y Gestión

Auditoría Informática

Ingeniería en Desarrollo de Software



TUTOR: Jessica Hernández Romero

ALUMNO: Carlos Fco Estrada Salazar

FECHA: 24/10/2025

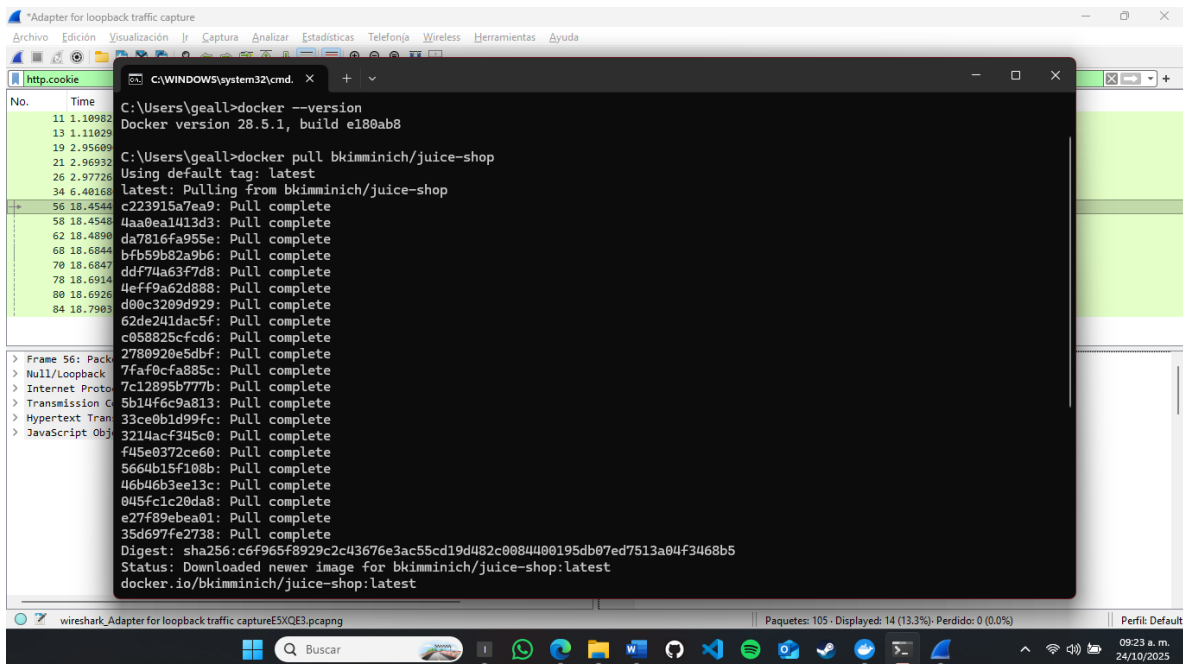
DESARROLLO

Descripción del sitio:

OWASP Juice Shop es una aplicación web intencionalmente vulnerable creada por el proyecto OWASP (Open Web Application Security Project) con fines educativos y de práctica en ciberseguridad. Su objetivo principal es ayudar a estudiantes, desarrolladores y analistas de seguridad a comprender y detectar las vulnerabilidades más comunes en aplicaciones web modernas. Está desarrollada con tecnologías como **Node.js**, **Express** y **Angular**, simulando una tienda en línea donde los usuarios pueden realizar compras ficticias. Sin embargo, la aplicación contiene múltiples fallos de seguridad basados en el **OWASP Top 10**, como inyección SQL, cross-site scripting (XSS), exposición de datos sensibles y fallas de autenticación. Juice Shop se utiliza ampliamente en cursos, laboratorios y competiciones de hacking ético (CTFs), ofreciendo una forma segura y controlada de aprender cómo funcionan los ataques reales y cómo proteger los sistemas frente a ellos.

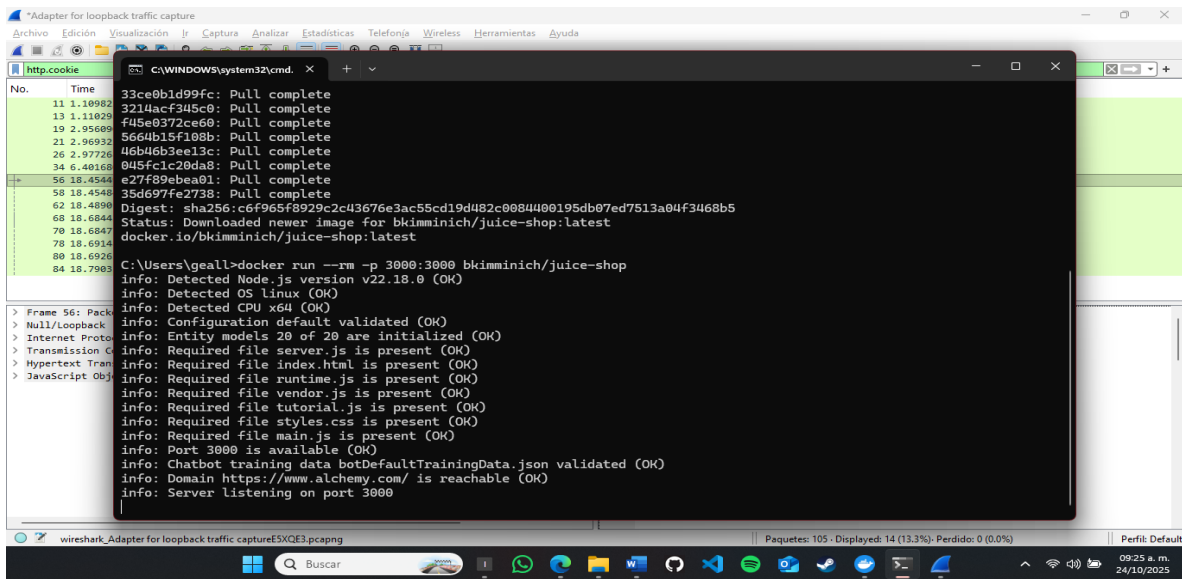
Ataque al sitio:

Para realizar esta actividad utilicé Docker para ejecutar OWASP Juice Shop en **localhost**, asegurando un entorno de práctica local. Además, monté una máquina virtual para demostrar los comandos y ejecutar la aplicación desde una dirección IP, lo que permitió simular un entorno web más realista y probar la conectividad remota.



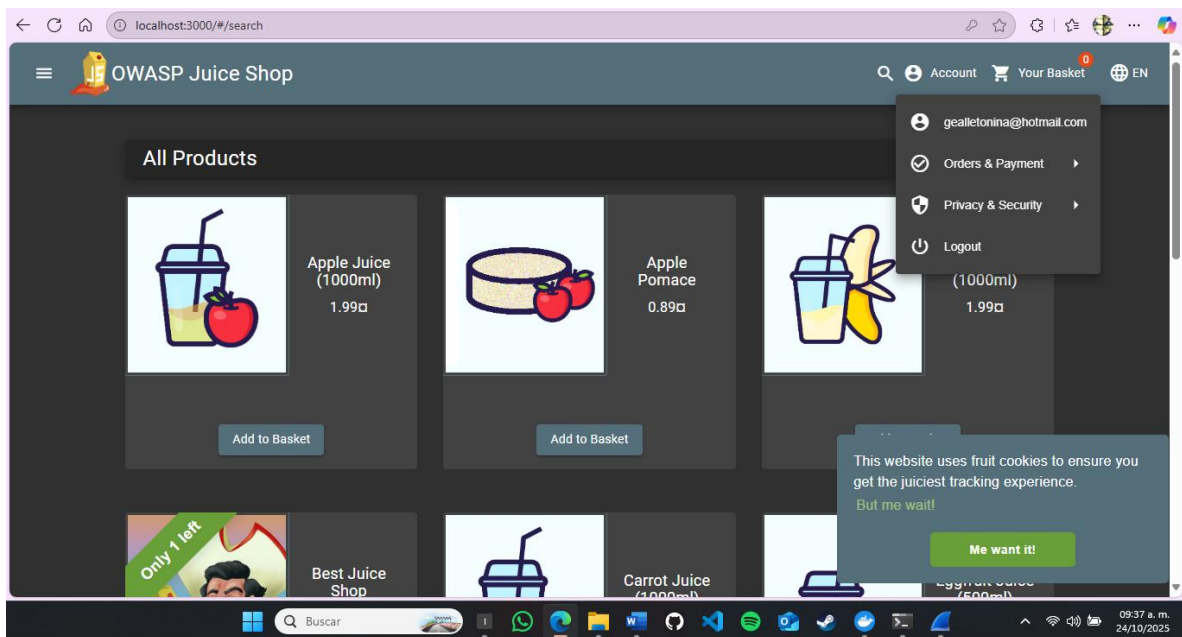
```
*Adapter for loopback traffic capture
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
http.cookie C:\WINDOWS\system32\cmd
No. Time C:\Users\geall>docker --version
11 1.10902 Docker version 28.5.1, build e180ab8
13 1.11829
19 2.95609
21 2.96932
26 2.97726
34 6.40168
56 18.45444 c223915a7ea9: Pull complete
58 18.45448 4aa0ea1413d3: Pull complete
62 18.48900 da7816fa955e: Pull complete
68 18.68444 bfb59b82a9b6: Pull complete
70 18.6847 ddf74a63f7d8: Pull complete
78 18.6914 4eff9a62d888: Pull complete
80 18.6926 d80c3209d929: Pull complete
84 18.7903 62de241dac5f: Pull complete
c058825cfd6: Pull complete
2780920e5dbf: Pull complete
7faf0cfa885c: Pull complete
7c12895b777b: Pull complete
5b14f6c9a813: Pull complete
33ce0b1d99fc: Pull complete
3214acf345c0: Pull complete
f445c0372ce60: Pull complete
5684b15f108b: Pull complete
46b46b3ee13c: Pull complete
045fc1c20da8: Pull complete
e27f89e01: Pull complete
35d697fe2738: Pull complete
Digest: sha256:c6f965f8929c2c43676e3ac55cd19d482c0884400195db07ed7513a04f3468b5
Status: Downloaded newer image for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest
```

Levantando la aplicación OWASP Juice Shop dese Docker.



Una vez terminado me asegure de que estuviera corriendo en el puerto 3000

En WireShark utilice el servidor *Npcap Loopback Adapter* para la práctica en local, después utilice el filtro de captura *tcp port 3000*, una vez iniciada la captura realizo las acciones requeridas en la aplicación OWASP Juice Shop.



Una vez realizadas las acciones de login detengo la captura en WireShark para realizar los filtros correspondientes para localizar la petición de login.

Adapter for loopback traffic capture

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

http

No.	Time	Source	Destination	Protocol	Length	Info
30	3.367357	:::1	:::1	HTTP/3...	792	HTTP/1.1 200 OK, JSON (application/json)
32	3.389774	:::1	:::1	HTTP	370	HTTP/1.1 304 Not Modified
34	6.401680	:::1	:::1	HTTP	821	GET /rest/admin/application-configuration HTTP/1.1
36	6.410477	:::1	:::1	HTTP	370	HTTP/1.1 304 Not Modified
56	18.454496	:::1	:::1	HTTP/3...	890	POST /rest/user/login HTTP/1.1, JSON (application/json)
58	18.454841	:::1	:::1	HTTP	799	GET /rest/user/whoami HTTP/1.1
60	18.486572	:::1	:::1	HTTP/3...	458	HTTP/1.1 200 OK, JSON (application/json)
62	18.489057	:::1	:::1	HTTP	798	GET /rest/user/whoami HTTP/1.1
64	18.521553	:::1	:::1	HTTP	367	HTTP/1.1 304 Not Modified
66	18.550477	:::1	:::1	HTTP/3...	1265	HTTP/1.1 200 OK, JSON (application/json)
68	18.684427	:::1	:::1	HTTP	2310	GET /rest/basket/6 HTTP/1.1
70	18.684779	:::1	:::1	HTTP	2312	GET /rest/user/whoami HTTP/1.1
78	18.691482	:::1	:::1	HTTP	2313	GET /api/Quantities/ HTTP/1.1
80	18.692628	:::1	:::1	HTTP	2322	GET /rest/products/search?q= HTTP/1.1
82	18.788174	:::1	:::1	HTTP/3...	578	HTTP/1.1 200 OK, JSON (application/json)

> Frame 56: Packet, 890 bytes on wire (7120 bits), 890 bytes captured (7120 bits) on interface
> Null/Loopback
> Internet Protocol Version 6, Src: ::1, Dst: ::1
> Transmission Control Protocol, Src Port: 53640, Dst Port: 3000, Seq: 1, Ack: 1, Len: 826
> Hypertext Transfer Protocol
> JavaScript Object Notation: application/json

Bytes 840-865: String value (json.value.string)

Paquetes: 105 - Displayed: 28 (26.7%) - Perdido: 0 (0.0%) Perfil: Default

09:43 a.m. 24/10/2025

Utilizando *http*

Adapter for loopback traffic capture

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

http.request.method == "POST"

No.	Time	Source	Destination	Protocol	Length	Info
56	18.454496	:::1	:::1	HTTP/3...	890	POST /rest/user/login HTTP/1.1, JSON (application/json)

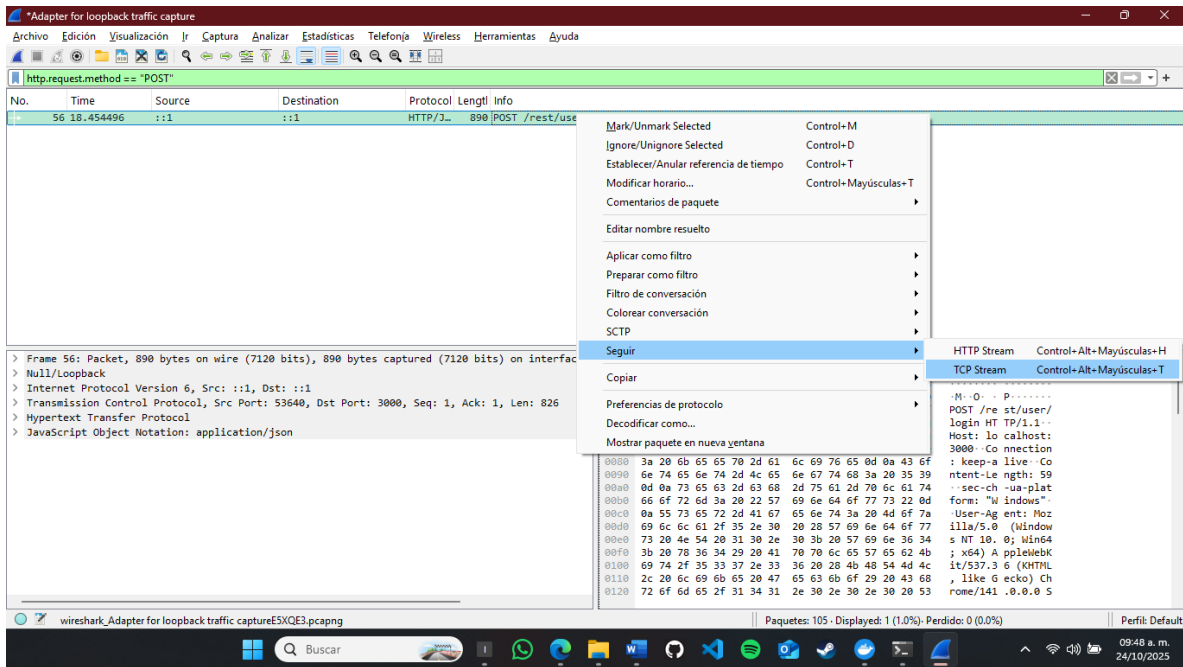
> Frame 56: Packet, 890 bytes on wire (7120 bits), 890 bytes captured (7120 bits) on interface
> Null/Loopback
> Internet Protocol Version 6, Src: ::1, Dst: ::1
> Transmission Control Protocol, Src Port: 53640, Dst Port: 3000, Seq: 1, Ack: 1, Len: 826
> Hypertext Transfer Protocol
> JavaScript Object Notation: application/json

Bytes 840-865: String value (json.value.string)

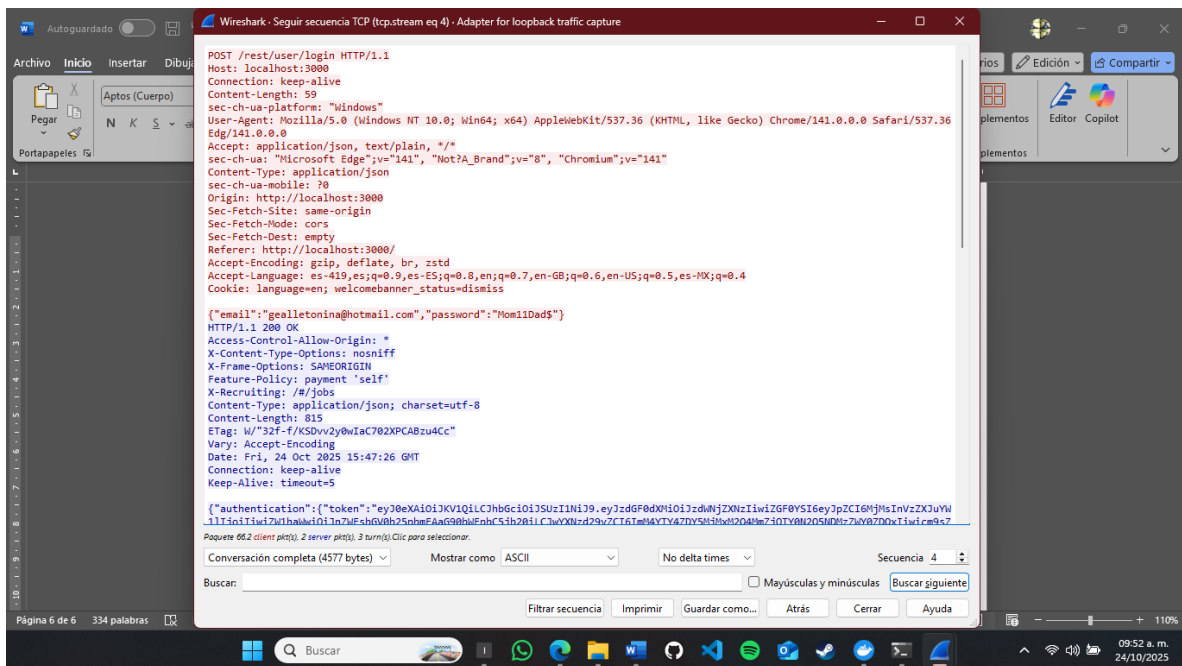
Paquetes: 105 - Displayed: 1 (1.0%) - Perdido: 0 (0.0%) Perfil: Default

09:44 a.m. 24/10/2025

Utilizando *http.request.method == "POST"*



Para ver las credenciales seleccione la linea que corresponde al POST del formulario de login/registro, y seleccione el TCP Stream para abrir la convesación completa.



Una vez en la conversación identifico las credenciales de login/registro.

CONCLUSIÓN

En esta actividad se logró comprender de manera práctica la importancia de la **seguridad en la gestión de sesiones y autenticación** dentro de aplicaciones web. Al desplegar OWASP Juice Shop en un entorno controlado y accesible desde una máquina virtual, se pudo simular un escenario de explotación seguro, donde se observó cómo la falta de cifrado en las comunicaciones (HTTP) permite capturar credenciales de usuarios mediante herramientas como **Wireshark**. Se aprendió a identificar solicitudes POST de login y registro, analizar los encabezados de cookies y evaluar si las sesiones contaban con medidas de seguridad como HttpOnly y Secure.

Asimismo, la práctica permitió experimentar cómo la exposición de cookies de sesión y credenciales en texto claro representa un riesgo de seguridad crítico, evidenciando la necesidad de implementar **HTTPS/TLS**, expiración y rotación de cookies, así como políticas de control de acceso robustas. La integración de la máquina virtual con Docker facilitó la creación de un entorno aislado, reproducible y seguro, lo que demuestra cómo se puede practicar auditoría informática sin comprometer sistemas reales.

Esta actividad reforzó la comprensión teórica con aplicaciones prácticas, destacando la relevancia de auditar periódicamente los sistemas web, identificar vulnerabilidades en autenticación y sesiones, y aplicar buenas prácticas de seguridad para proteger la información sensible de los usuarios y garantizar la integridad de los sistemas.