



# EJERCICIOS

## UNIDAD TRABAJO 3:

# DOJO WEB SECURITY – OWASP JUICE SHOP

---

PUESTA EN PRODUCCIÓN SEGURA

Esta unidad didáctica se ha desarrollado para el Curso de Especialización de Ciberseguridad en entornos de las Tecnologías de la Información. En concreto para el módulo de Puesta en Producción Segura, cuyos aspectos básicos del currículo vienen recogidos en el Real Decreto 479/2020.

**Licencia:** Creative Commons Atribución - No Comercial -Compartir Igual (CC BY-NC-SA 4.0)

**José Gaspar Sánchez García.**

<b>NOMBRE Y APELLIDOS:</b>	<a href="#">ALUMNO/A [JOSE FRANCISCO MURCIA FUENTES]</a>
<b>FECHA DE COMIENZO:</b>	<a href="#">[24/05/2025]</a>

# Normas de entrega:

## Corrección:

-  Por cada día de retraso sin justificación en la entrega, se restará 1 punto a la nota.
-  Es muy importante cuidar la presentación y limpieza de las respuestas entregadas al profesor.

## Forma de Entrega:

- A través de la plataforma Moodle GVA AULAS: <https://aulas.edu.gva.es/> **Documentos a entregar:**
- Este mismo fichero con las preguntas llenadas (usar fuente Verdana de tamaño 12 color azul en cursiva – **Estilo Respuesta**): **[Respuesta]**
- Cambia el nombre al documento, y añade tu primer apellido y tu nombre al final.
- Documento con la respuesta a las cuestiones y explicación al desarrollo de la práctica, En formato del documento **PDF**.

## Normas:

- Realizar los ejercicios sobre una máquina virtual **Kali Linux PePS-<codId>** como máquina atacante para realizar la penetración.
- Prepararemos una máquina **Dojo Linux PePS-<codId>**, que utilizaremos para instalar las distintas plataformas de entrenamiento.
- Cambiar **<codId>** por las iniciales de tu nombre y apellidos, más el año actual. Ejemplo: José Gaspar Sánchez García → **JGSG25**.
- Las respuestas deben ir entre los corchetes **[ ]**
- **Capturar pantallas completas**, donde se observe el nombre de la máquina virtual creada.
- Los enunciados de los ejercicios deben aparecer claramente con las respuestas a los ejercicios.
- En caso de que se detecte copia o plagio con los ejercicios de otros compañeros, se invalidará la nota del ejercicio.

<b>Índice:</b>	1. Introducción .....	<b>¡Error! Marcador no definido.</b>
2. Instalar plataforma de entrenamiento DOJO .....	3	
3. OWASP Juice Shop .....	6	
4. ¿Como crear un CTF con OWASP Juice Shop y Traefik?.....	15	

# 1. Introducción

En esta unidad se presentan los diferentes métodos y recursos que sirven de ayuda a los desarrolladores para determinar el nivel de seguridad requerido por aplicaciones web y móviles, para conseguir su puesta en producción de un modo seguro.

## 2. Instalar plataforma de entrenamiento DOJO

1. Accedemos a la página web de DOJO: <https://websecuritydojo.sourceforge.io/>.

The screenshot shows the SourceForge project page for 'Web Security Dojo'. The page includes the following information:

- Project Summary:** Efficient AD Report Tool
- Rating:** ★★★★☆ 3 Reviews
- Downloads:** 122 This Week
- Last Update:** 2020-03-04
- Platform:** Linux | Mac | Windows
- Features:**
  - vulnerable web applications
  - common web security testing tools
  - popular industry web application security guidelines
  - no Internet connect required to use
- Description:** Web Security Dojo is a virtual machine that provides the tools, targets, and documentation to learn and practice web application security testing. A preconfigured, stand-alone training environment ideal for classroom and conferences. No Internet required to use. Ideal for those interested in getting hands-on practice for ethical hacking, penetration testing, bug bounties, and capture the flag (CTF). A single OVA file will import into VirtualBox and VMware. There is also an Ansible script for those brave souls that want transform their stock Ubuntu into a virtual dojo. Bow to your sensei!
- Logins:** username: dojo  
password: dojo

On the right side of the page, there is an advertisement titled 'HOW SLEEP AMOUNT affects your ADHD' which includes four categories of sleep duration and their effects:

Sleep Duration	Effects
0-3 HOURS	Irritability and mood swings, Hyperactivity or total shutdown, Impulsivity spikes
4-5.5 HOURS	Foggy focus, Poor time management, Low motivation
6-7 HOURS	Improved focus, but still inattentive, Better emotional control, Still prone to zoning out or forgetfulness
7.5-9 HOURS	Noticeable longer attention and memory, Reduced ADHD severity, Greater emotional resilience

Figura 1. Web Security DOJO.

2. Descargamos una imagen de la máquina virtual en formato **.ova** (*Open Virtual Appliance*).

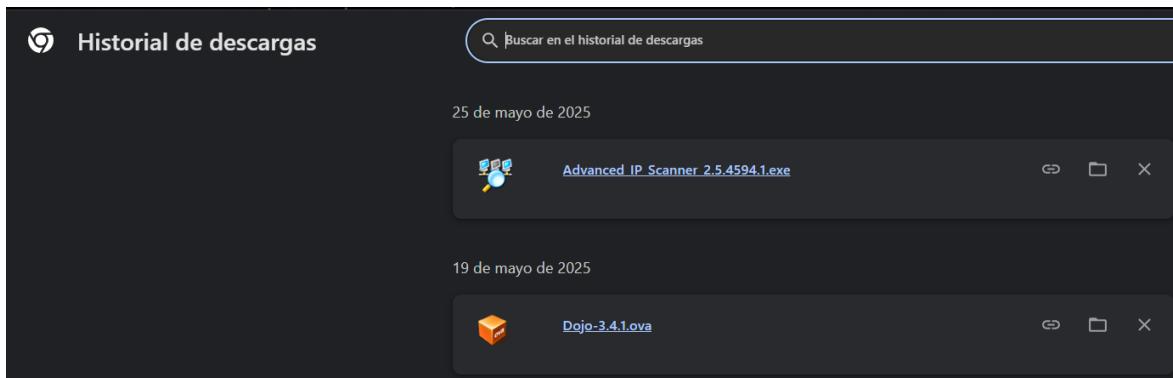


Figura 2. Fichero en formato ova: Dojo-3.4.1.ova

### 3. Crear una máquina virtual en VirtualBox.

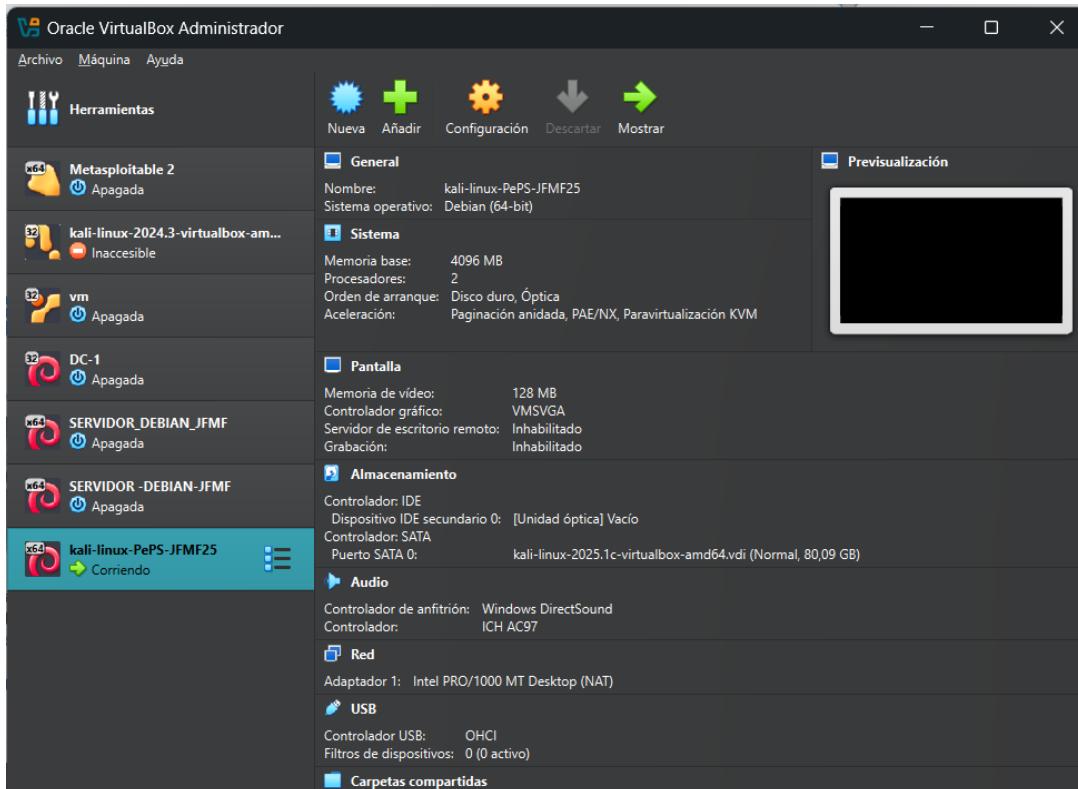


Figura 3. Máquina VirtualBox Kali.

### 4. Realizar el proceso de instalación de “Web Security DOJO”.

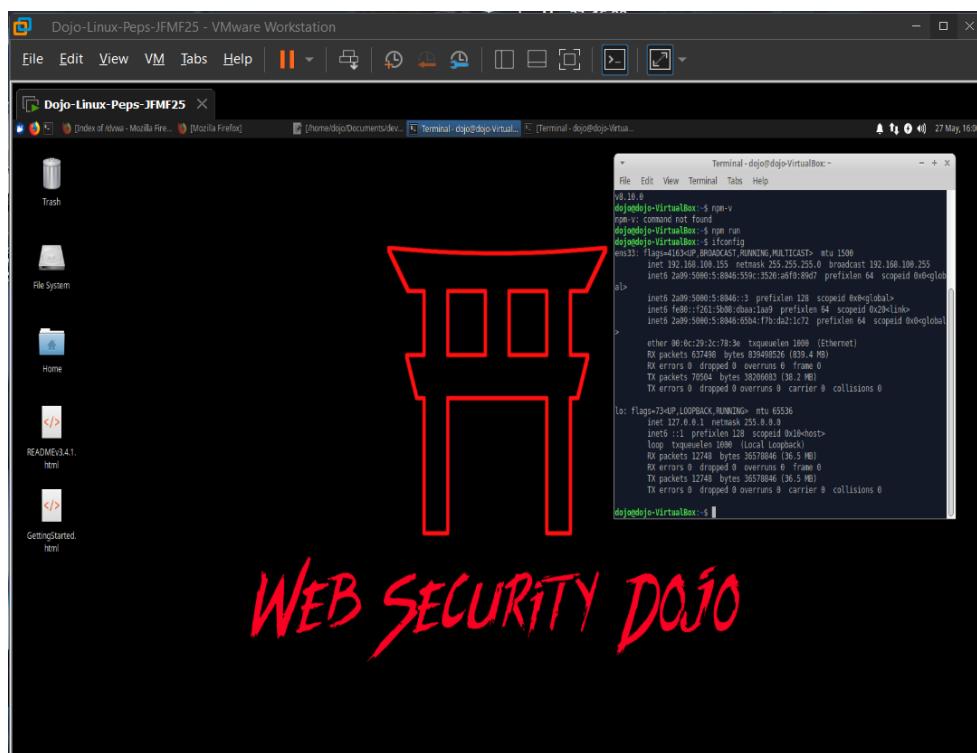


Figura 4. Escritorio y dirección IP de máquina DOJO.

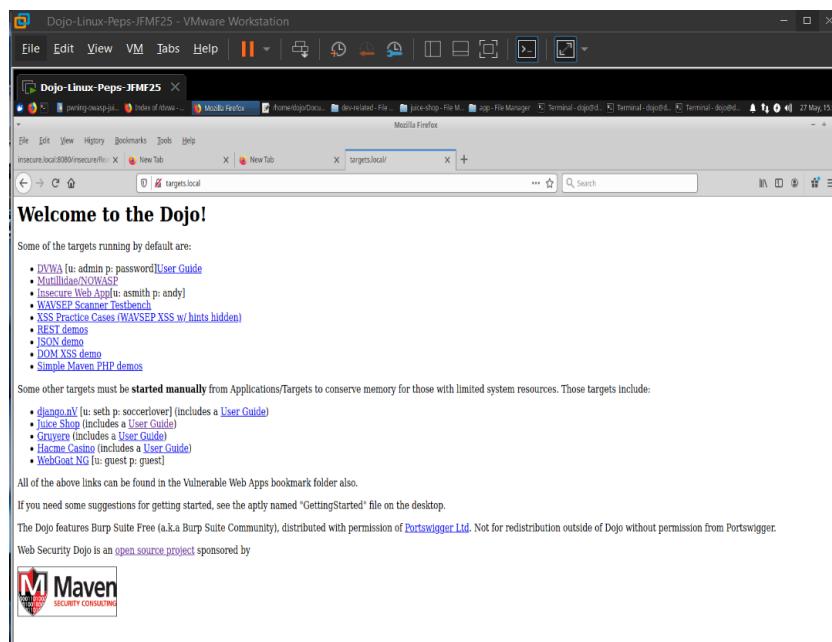
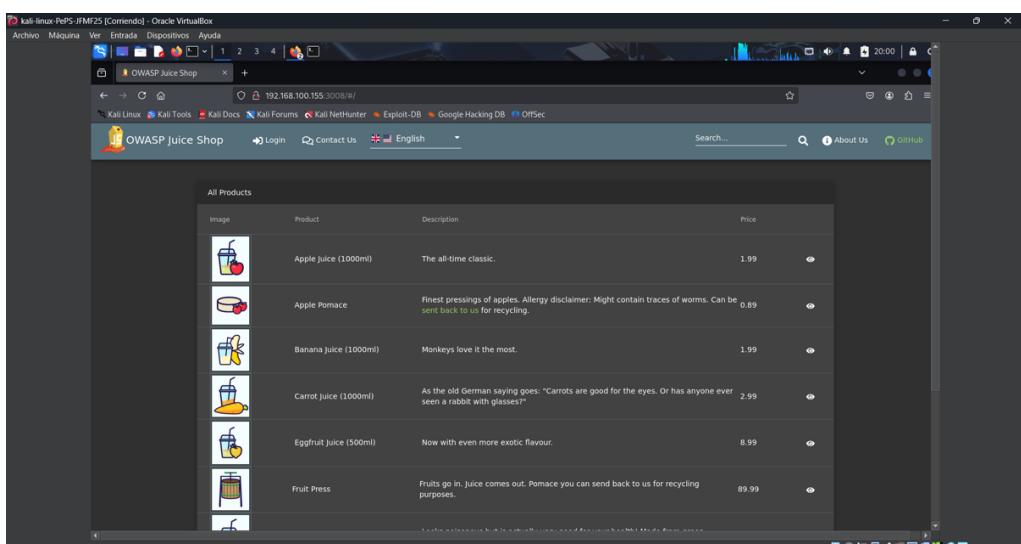


Figura 5. Welcome to the Dojo

5. Una vez realizado el proceso de instalación, comprobar la instalación desde otra máquina accediendo a las diferentes aplicaciones web vulnerables que se incluyen en la plataforma.  
*[Arrancamos el servidor para poder acceder desde nuestra maquina Kali remota.]*

```
Terminal - dojo@dojo-VirtualBox:~/targets/juice-shop/app
File Edit View Terminal Tabs Help
dojo@dojo-VirtualBox:~/targets/juice-shop/app$ npm start
> juice-shop@0.3.0 start /home/dojo/targets/juice-shop/app
> node app
Detected Node.js version v8.10.0 (OK)
Configuration default validated (OK)
Server listening on port 3008
```

The terminal output shows the command 'npm start' being run in the 'juice-shop' directory. It confirms the Node.js version (v8.10.0) and configuration (default). The final line, 'Server listening on port 3008', is highlighted with a red box.



## 3. OWASP Juice Shop

Juice Shop está escrito en Node.js, Express y Angular. Fue la primera aplicación escrita completamente en JavaScript que figura en el directorio de proyectos de OWASP. La aplicación contiene una gran cantidad de desafíos de diversa dificultad en los que se supone que el usuario debe explotar las vulnerabilidades subyacentes.

6. Encontrar este tablero de puntuación es en realidad uno de los desafíos (fáciles).

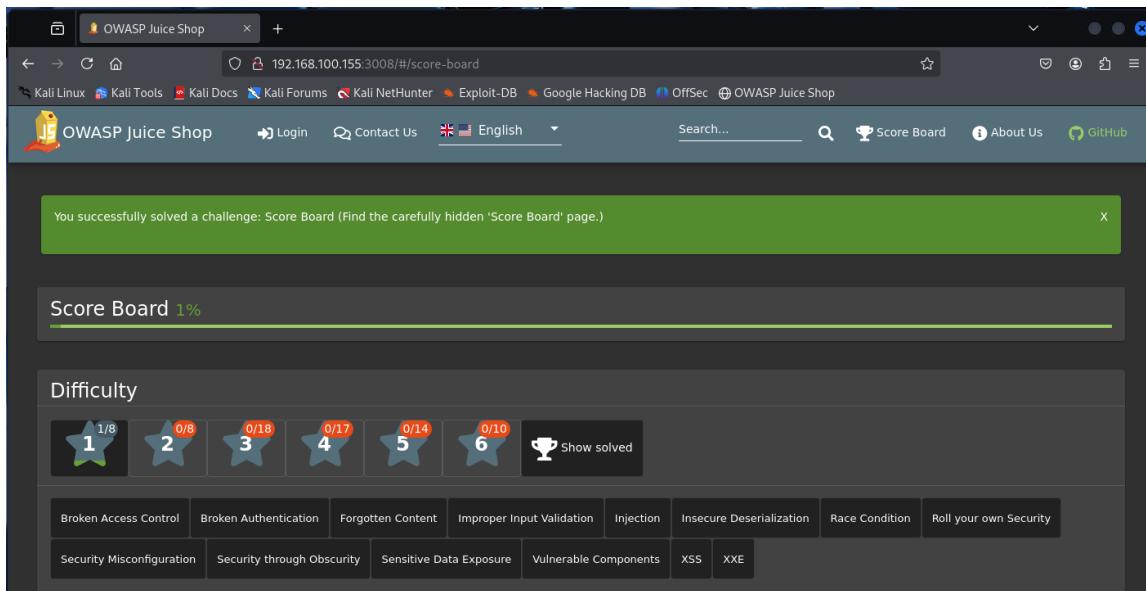


Figura 6. Juice-Shop: score-board.

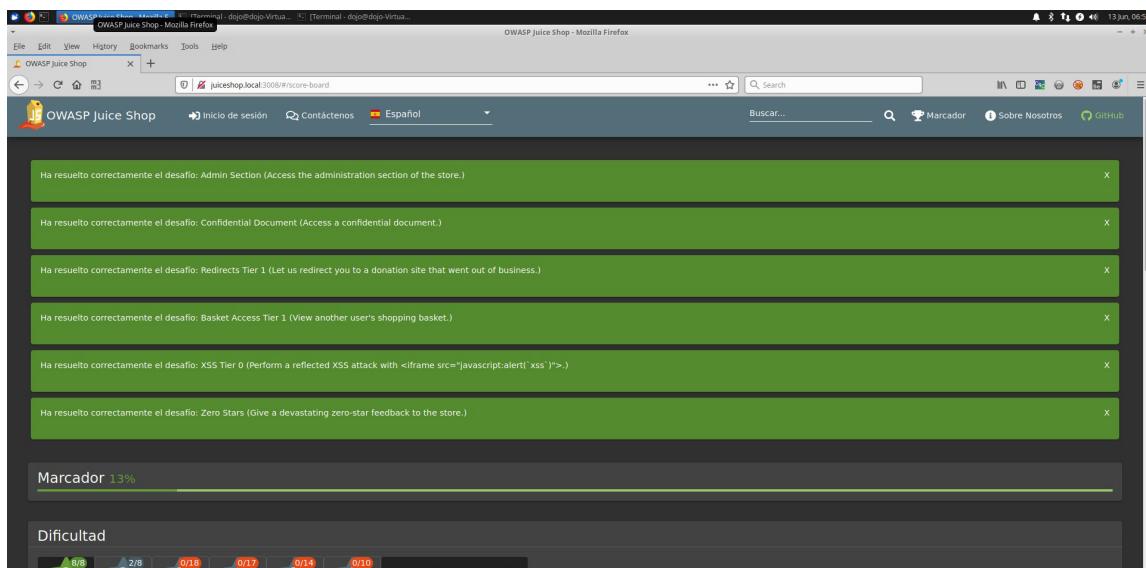


Figura 7. Juice-Shop: score-board.

7. Documenta el proceso de resolución de los diferentes desafíos que podemos encontrar en el sitio web Juice Shop. Los desafíos planteados tienen diferentes niveles de dificultad, cuantos más niveles completos mayor será tu puntuación.

#### [Descripción general de OWASP Juice Shop

*OWASP Juice Shop es una aplicación web deliberadamente insegura, diseñada para enseñar y evaluar habilidades de seguridad en aplicaciones web. Abarca vulnerabilidades del Top Ten de OWASP, lo que la convierte en un recurso valioso para capacitación en seguridad, demostraciones de concienciación y eventos de Capturar la Bandera (CTF). A continuación, se presenta un resumen de las 10 vulnerabilidades principales de OWASP, tal como se presentan en la plataforma OWASP Juice Shop:*

#### **1. Control de acceso defectuoso**

*Desafíos: Sección de administración, CSRF, Huevo de Pascua, Comentarios de cinco estrellas, Comentarios falsificados, Reseña falsificada, Manipular la cesta, Manipulación de productos.*

*Descripción: Estos desafíos implican vulnerabilidades en las que la aplicación no restringe adecuadamente el acceso a usuarios no autorizados, lo que les permite realizar acciones que no deberían poder realizar.*

#### **2. Diseño inseguro**

*Desafíos: Evitar CAPTCHA, Idioma adicional, Múltiples "Me gusta", Restablecer la contraseña del usuario Morty.*

*Descripción: Estos desafíos se centran en vulnerabilidades que permiten ataques automatizados, como eludir CAPTCHAs o realizar múltiples acciones que deberían estar limitadas.*

#### **3. Autenticación defectuosa**

*Desafíos: Mascota favorita de Bjoern, Cambiar la contraseña de Bender, Borrado de datos según el RGPD, Iniciar sesión con Bjoern, Fortaleza de la contraseña, Restablecer la contraseña de Bender, Restablecer la contraseña de Bjoern, Restablecer la contraseña de Jim, Autenticación de dos factores*

*Descripción: Estos desafíos implican vulnerabilidades en los mecanismos de autenticación, como políticas de contraseñas débiles o una autenticación de dos factores defectuosa.*

#### **4. Problemas criptográficos**

*Desafíos: Cupón falsificado, Desafío imaginario, Huevo de Pascua anidado, Muro de pago premium, Criptografía extraña*

*Descripción: Estos desafíos implican problemas con las funciones criptográficas de la aplicación, como un cifrado débil o el uso indebido de algoritmos criptográficos.*

## 5. Validación de entrada incorrecta

*Desafíos: Registro de administrador, Fraude Deluxe, Registro de usuario vacío, Cupón caducado, Mint the Honey Pot, Codificación faltante, Tiempo de recuperación, Byte nulo envenenado, Registro repetitivo, Tamaño de carga, Tipo de carga, Cero estrellas*

*Descripción: Estos desafíos implican vulnerabilidades donde la aplicación no valida correctamente la entrada, lo que provoca problemas como inyección SQL o desbordamientos de búfer.*

## 6. Inyección

*Desafíos: Especial de Navidad, Esquema de base de datos, Contador efímero, Inicio de sesión de administrador, Inicio de sesión duplicado, Inicio de sesión de Jim, DoS NoSQL, Exfiltración NoSQL, Manipulación NoSQL, SSTi, Credenciales de usuario*

*Descripción: Estos desafíos implican vulnerabilidades donde se envían datos no confiables a un intérprete como parte de un comando o consulta, lo que provoca ataques de inyección como inyección SQL o inyección de comandos.*

## 7. Deserialización insegura

*Desafíos: RCE DoS bloqueado, Bomba de memoria, RCE DoS exitoso*

*Descripción: Estos desafíos implican vulnerabilidades donde la aplicación deserializa datos no confiables, lo que provoca ejecución remota de código o ataques de denegación de servicio.*

## 8. Configuración incorrecta de la seguridad

*Desafíos: Imágenes entre sitios, Interfaz obsoleta, Manejo de errores, Equipo de soporte de inicio de sesión*

*Descripción: Estos desafíos implican vulnerabilidades donde la aplicación está mal configurada, lo que genera problemas como la exposición de información confidencial o el acceso no autorizado.*

## 9. Seguridad y protección de la información.

*Desafíos: Inspección de la política de privacidad, Esteganografía*

*Descripción: Estos desafíos implican vulnerabilidades donde la aplicación se basa en funciones ocultas u ofuscación en lugar de medidas de seguridad adecuadas.*

## 10. Exposición de datos sensibles

*Desafíos: Registro de acceso, Documento confidencial, Fuga de correo electrónico, Métricas expuestas, Credenciales expuestas, Copia de seguridad del desarrollador olvidada, Copia de seguridad del departamento de ventas olvidada, Robo de datos del RGPD, Registros de acceso filtrados entre otros.*

**Descripción:** Estos desafíos implican vulnerabilidades donde la aplicación expone datos sensibles, como registros de acceso, credenciales o información personal.

## 11. Redirecciones y reenvíos no validados

**Descripción:** Estos desafíos implican vulnerabilidades donde la aplicación redirige o reenvía a los usuarios a URL no confiables sin la validación adecuada.

## 12. Componentes vulnerables

**Desafíos:** Escritura arbitraria de archivos, JWT firmado falsificado, Typosquatting en frontend, Eliminación de chatbots, Typosquatting heredado, Lectura local de archivos, Ataque a la cadena de suministro, JWT sin firmar, Biblioteca vulnerable.

**Descripción:** Estos desafíos implican vulnerabilidades donde la aplicación utiliza componentes con vulnerabilidades conocidas, lo que genera posibles riesgos de seguridad.

## 13. XSS (Cross-Site Scripting)

**Desafíos:** XSS solo de API, Carga útil adicional, Omisión de CSP, Protección XSS del lado del cliente, XSS de DOM, XSS de encabezado HTTP, XSS reflejado, Protección XSS del lado del servidor, XSS de vídeo

**Descripción:** Estos desafíos implican vulnerabilidades donde la aplicación permite que datos no confiables se ejecuten como scripts en el navegador del usuario, lo que provoca ataques XSS.

## 14. XXE (Entidad externa XML)

**Desafíos:** Acceso a datos XXE, DoS XXE]

- Desafíos triviales.

Nombre	Descripción	Estado
Admin Section	Access the administration section of the store.	resuelto
Confidential Document	Access a confidential document.	resuelto
Error Handling	Provocar un error que no es manejado de manera muy grácil.	resuelto
Redirects Tier 1	Redirigirnos a un sitio de donación que ya no existe.	resuelto
Score Board	Encontrar la página 'Score Board' oculta.	resuelto
XSS Tier 0	Realizar un ataque XSS reflejado con <iframe src="javascript:alert('xss')">.	resuelto
XSS Tier 1	Realizar un ataque XSS de DOM con <iframe src="javascript:alert('xss')">.	resuelto
Zero Stars	Dar una retroalimentación de cinco estrellas negativas al comercio.	resuelto

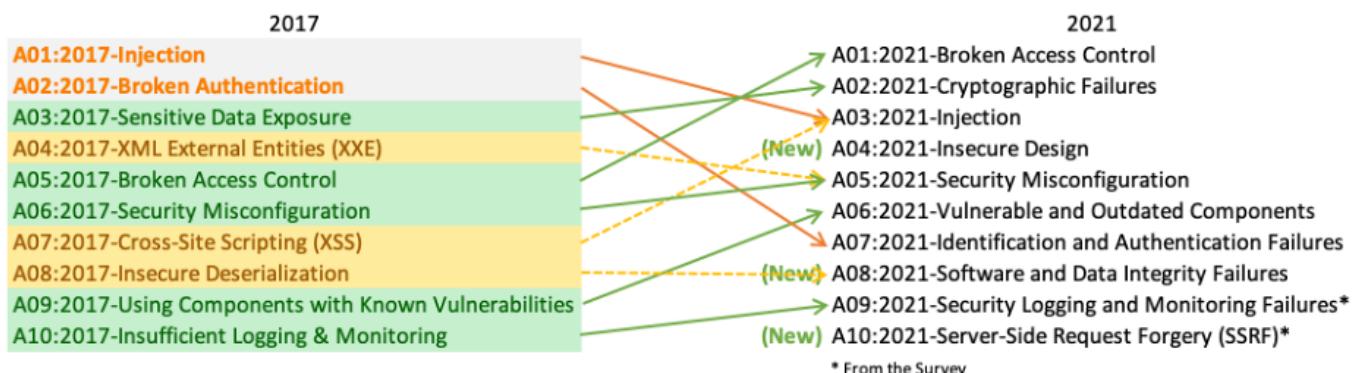
- Desafíos fáciles.

Nombre	Descripción	Estado
Basket Access Tier 1	View another user's shopping basket.	resuelto
Deprecated Interface	Use a deprecated B2B interface that was not properly shut down.	resuelto
Five-Star Feedback	Get rid of all 5-star customer feedback.	resuelto
Login Admin	Log in with the administrator's user account.	resuelto
Login MC SafeSearch	Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass.	resuelto
Password Strength	Log in with the administrator's user credentials without previously changing them or applying SQL Injection.	resuelto
Security Policy	Behave like any "white-hat" should.	resuelto
Weird Crypto	Inform the shop about an algorithm or library it should definitely not use the way it does.	resuelto

- Desafíos medios.

Nombre	Descripción	Estado
Admin Registration	Get registered as admin user.	resuelto
Basket Access Tier 2	Put an additional product into another user's shopping basket.	no resuelto
CAPTCHA Bypass Tier 1	Submit 10 or more customer feedbacks within 10 seconds.	resuelto
Forged Feedback	Post some feedback in another user's name.	resuelto
Forged Review	Post a product review as another user or edit any user's existing review.	resuelto
Forgotten Sales Backup	Access a salesman's forgotten backup file.	no resuelto
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 Important Final Note")	resuelto
Login Bender	Log in with Bender's user account.	resuelto
Login Jim	Log in with Jim's user account.	resuelto
Playback Time	Place an order that makes you rich.	no resuelto
Product Tampering	Change the href of the link within the OWASP SSL Advanced Forensic Tool (O-SaFT) product description into <a href="http://kimminich.de">http://kimminich.de</a> .	no resuelto
Reset Björn's Password Tier 1	Reset the password of Björn's OWASP account via the Forgot Password mechanism with the original answer to his security question.	resuelto

8. Además de resolver los diferentes desafíos explica en qué consisten las vulnerabilidades de OWASP Top Ten a la que están asociados. Indicando que posición ocupa la vulnerabilidad en el Top 10.



[A07:2021 Fallos de identificación y autentificación, ataques de fuerza bruta al servidor dirbuster es ejemplo de software para este propósito.]

```

kali@kali: ~
File Actions Edit View Help
---[kali@kali: ~]---$ dirb http://192.168.100.155:3008/
DIRB v2.22
By The Dark Raver

START_TIME: Sun May 25 20:30:19 2025
URL_BASE: http://192.168.100.155:3008/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612
Scanning URL: http://192.168.100.155:3008/
+ http://192.168.100.155:3008/assets (CODE:301|SIZE:179)
+ http://192.168.100.155:3008/favicon.ico (CODE:200|SIZE:5430)
+ http://192.168.100.155:3008/ftp (CODE:200|SIZE:10606)
+ http://192.168.100.155:3008/profile (CODE:500|SIZE:1151)
+ http://192.168.100.155:3008/redirect (CODE:500|SIZE:289)
+ http://192.168.100.155:3008/robots.txt (CODE:200|SIZE:28)

END_TIME: Sun May 25 20:35:26 2025
DOWNLOADED: 4612 - FOUND: 6
---[kali@kali: ~]---$ dirb http://192.168.100.155:3008/

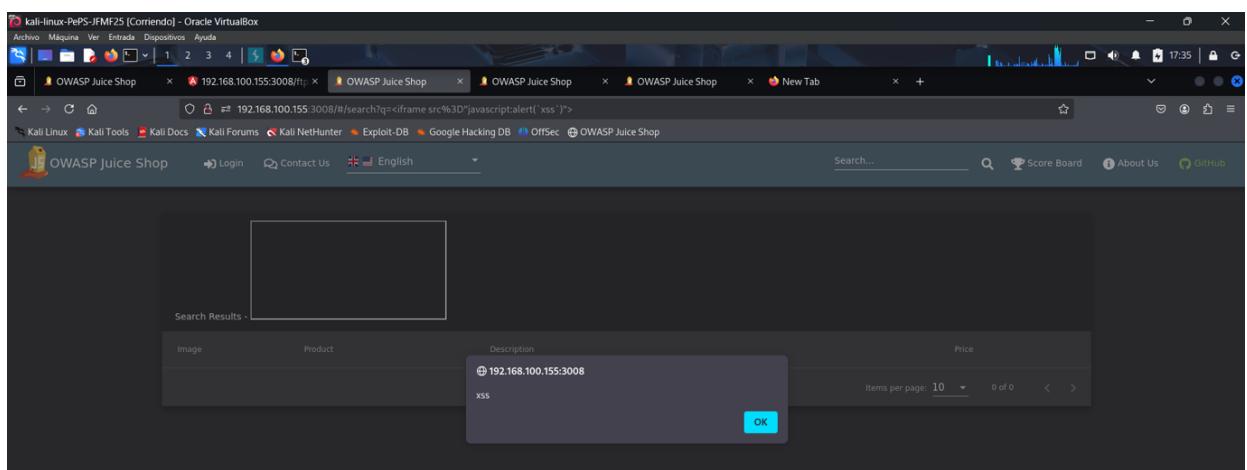
```

## 9. Muestra cómo realizar una SQL Injection en Juice Shop.

[A03:2021 – Inyección de código javascript ejecutable desde la url Una aplicación es vulnerable a los ataques cuando:

- Los datos suministrados por el usuario no son validados, filtrados o desinfectados por la aplicación.
- Las consultas dinámicas o las llamadas no parametrizadas sin escape sensible al contexto se utilizan directamente en el intérprete.
- Los datos hostiles se utilizan dentro de los parámetros de búsqueda de mapeo relacional de objetos (ORM) para extraer registros confidenciales adicionales.
- Los datos hostiles se utilizan o concatenan directamente. El SQL o comando contiene la estructura y los datos maliciosos en consultas dinámicas, comandos o procedimientos almacenados.

] ]



## 10. Autentícate con una cuenta de usuario de Administrador.

[A07:2021 - *Elevación del privilegio. Actuar como usuario sin iniciar sesión o actuar como administrador cuando se inicia sesión como usuario interceptando los parámetros y modificando los valores del rol de usuario como administrador burp suite es el software utilizado para interceptar las peticiones al servidor.*]

```

POST /api/Users HTTP/1.1
Host: 192.168.100.155:3008
Content-Length: 146
Accept-Language: en-US,en;q=0.9
Accept: application/json,*/*;q=0.8
User-Agent: Mozilla/5.0(X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Origin: http://192.168.100.155:3008
Referer: http://192.168.100.155:3008/
Content-Type: application/json
Cookie: 1eab9d4f8e-004d9444
Content-Type: application/json; charset=utf-8
Content-Length: 92
ETag: W/5c-0kvgu40yf1wFvxt4tft8ycK0
Date: Mon, 21 Mar 2022 21:13:51 GMT
Connection: keep-alive
{
    "email": "newuser@user.com",
    "isAdmin": "true",
    "password": "123456"
}

```

Response:

```

HTTP/1.1 400 Bad Request
X-Powered-By: Express
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Type: application/json; charset=utf-8
Content-Length: 92
ETag: W/5c-0kvgu40yf1wFvxt4tft8ycK0
Date: Mon, 21 Mar 2022 21:13:51 GMT
Connection: keep-alive
{
    "message": "Validation error",
    "errors": [
        {
            "field": "email",
            "message": "email must be unique"
        }
    ]
}

```

OWASP Juice Shop - 192.168.100.155:3008/#/score-board

You successfully solved a challenge: Password Strength (Log in with the administrator's user credentials without previously changing them or applying SQL Injection.)

You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)

Score Board 12%

Difficulty

1/8	2/8	0/18	0/17	0/14	6/10	Show solved
-----	-----	------	------	------	------	-------------

Score Board Progress: 12%

Challenges Solved:

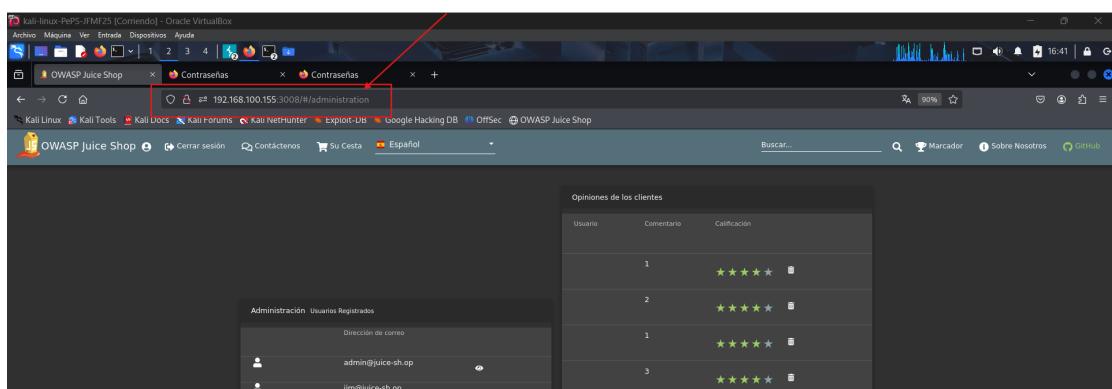
- Broken Access Control: 1/8
- Broken Authentication: 2/8
- Forgotten Content: 0/18
- Improper Input Validation: 0/17
- Injection: 0/14
- Insecure Deserialization: 6/10
- Race Condition: 0/10
- Roll your own Security: 0/10
- Security Misconfiguration: 0/10
- Security through Obscurity: 0/10
- Sensitive Data Exposure: 0/10
- Vulnerable Components: 0/10
- XSS: 0/10
- XXE: 0/10

11. Accede a la sección de administración.

[A01:2021 - Control de acceso roto: Eludir los controles de control de acceso modificando url.]

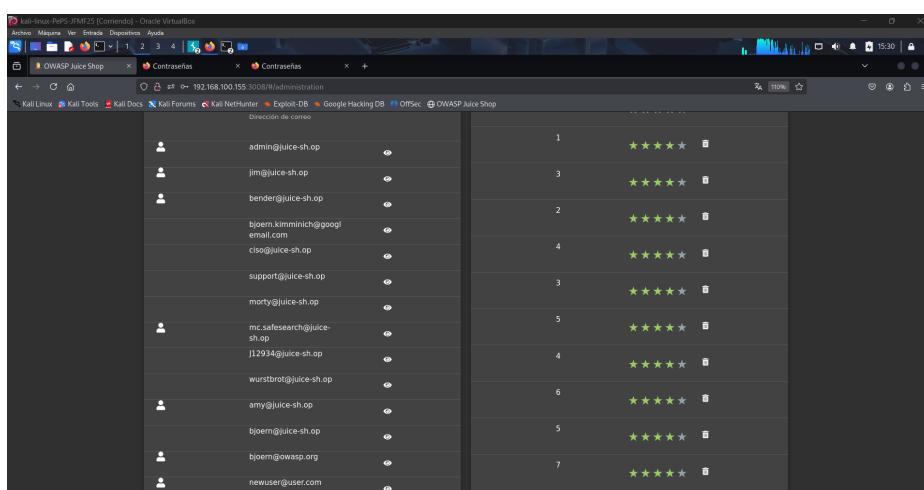
A10:2021 - Falsificación de solicitudes del lado del servidor (SSRF) Los defectos de SSRF ocurren cada vez que una aplicación web está recibiendo un recurso remoto sin validar la URL proporcionada por el usuario. Permite a un atacante forzar la aplicación para enviar una solicitud elaborada a un destino inesperado, incluso cuando está protegida por un cortafuegos, VPN u otro tipo de lista de control de acceso a la red (ACL).

]



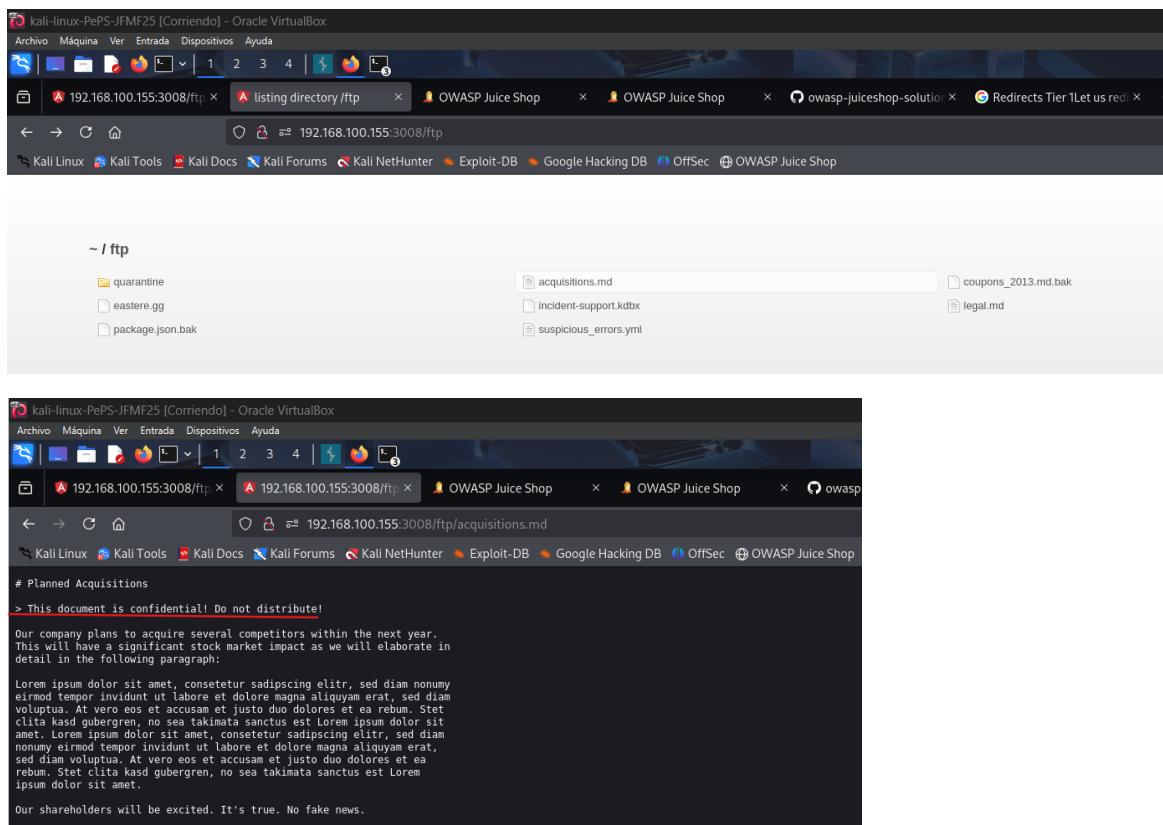
12. Obtenga un listado de los correos electrónicos de los usuarios que están registrados en la plataforma.

[A02:2021 - Fallos criptográficos. Lo primero es determinar las necesidades de protección de los datos en tránsito y en reposo. Por ejemplo, las contraseñas, los números de tarjetas de crédito, los registros de salud, la información personal y los secretos comerciales requieren protección adicional, principalmente si esos datos están sujetos a las leyes de privacidad, por ejemplo, el Reglamento General de Protección de Datos de la UE (RGPD).]



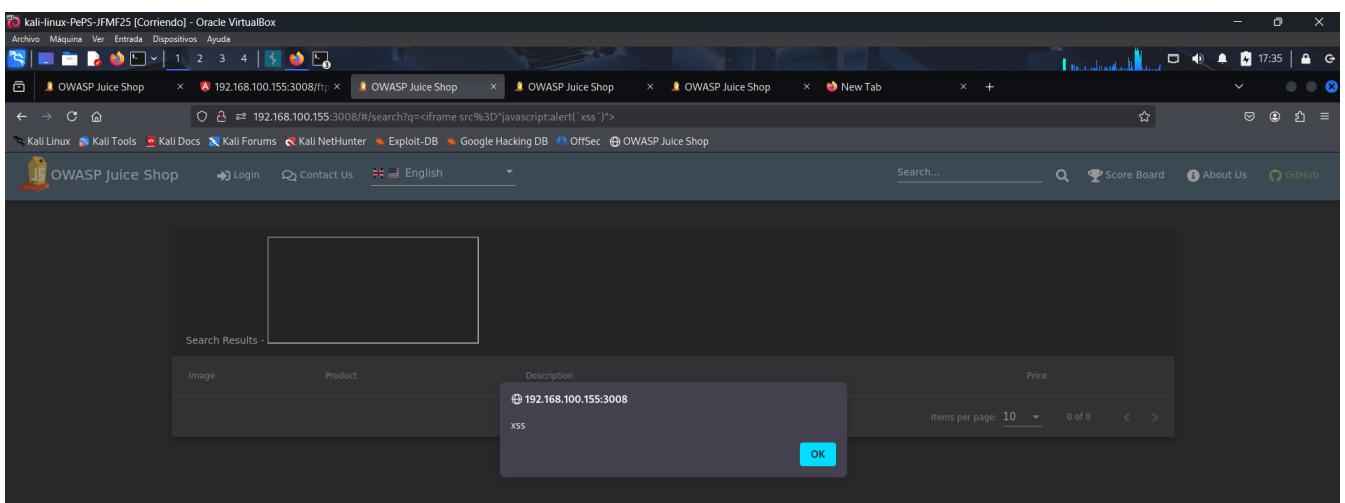
### 13. Acceda a un documento confidencial.

[A08:2021 - Las fallas de integridad del software y los datos se relacionan con el código y la infraestructura que no protegen contra las violaciones de integridad.]



### 14. Realiza un ataque DOM Cross Site-Scripting

- [A03:2021 - Las consultas dinámicas o las llamadas no parametrizadas sin escape sensible al contexto se utilizan directamente en el intérprete.  
]



15. Busca la canción del rapero **Mc Safe Search** dónde expone información confidencial.

*[A08:2021 - Las fallas de integridad del software y los datos se relacionan con el código y la infraestructura que no protegen contra las violaciones de integridad.]*

The screenshot shows a web browser window with the URL <https://genius.com/Collegehumor-protect-ya-passwordz-lyrics>. The page displays the lyrics for the song "Protect Ya Passwordz" by CollegeHumor. The lyrics mention maintaining cybersecurity and using passwords to protect money from hackers. The browser's address bar shows the URL and the search term "Protect Ya Passwordz". The page has a dark theme with orange and black colors.

The screenshot shows a web browser window with the URL <http://192.168.100.155:3008/#/search>. The page displays a success message: "You successfully solved a challenge: XSS Tier 0 (Perform a reflected XSS attack with <iframe src='javascript:alert('xss')'>.)" and another message: "You successfully solved a challenge: Login MC SafeSearch (Log in with MC SafeSearch's original user credentials without applying SQL injection or any other bypass.)". The browser's address bar shows the URL and the search term "OWASP Juice Shop". The page has a light blue header and a dark blue footer.

## 4. ¿Cómo crear un CTF con OWASP Juice Shop y Traefik?

16. **Ampliación:** Realiza el proceso de instalación de OWASP Juice Shop para poder usar esta web como plataforma de entrenamiento en modo competición *Capture The Flag*.

# **Resultados de Aprendizaje y Criterios de Evaluación**

<b>Contenidos:</b>	
<ul style="list-style-type: none"> <li>• Listas públicas de vulnerabilidades de aplicaciones web. OWASP Top Ten.</li> <li>• Vulnerabilidades web.</li> <li>• Seguridad de portales y aplicativos web. Soluciones WAF (Web Application Firewall).</li> <li>• Entrada basada en formularios. Inyección. Validación de la entrada.</li> <li>• Estándares de autenticación y autorización.</li> <li>• Robo de sesión.</li> <li>• Almacenamiento seguro de contraseñas.</li> <li>• Desarrollo seguro de aplicaciones web.</li> <li>• Contramedidas. HSTS, CSP, CAPTCHAs, entre otros.</li> </ul>	
<b>Resultados de aprendizaje</b>	<b>Criterios de evaluación</b>
<b>RA 3. Detecta y corrige vulnerabilidades de aplicaciones web analizando su código fuente y configurando servidores web.</b>	<p>a) Se han validado las entradas de los usuarios.</p> <p>b) Se han detectado riesgos de inyección tanto en el servidor como en el cliente.</p> <p>c) Se ha gestionado correctamente la sesión del usuario durante el uso de la aplicación.</p> <p>d) Se ha hecho uso de roles para el control de acceso.</p> <p>e) Se han utilizado algoritmos criptográficos seguros para almacenar las contraseñas de usuario.</p> <p>f) Se han configurado servidores web para reducir el riesgo de sufrir ataques conocidos.</p> <p>g) Se han incorporado medidas para evitar los ataques a contraseñas, envío masivo de mensajes o registros de usuarios a través de programas automáticos (bots).</p>