

# CURSO ONLINE DE CIBERSEGURIDAD

Especialidad Administración de  
Sistemas de Ciberseguridad

## Taller 1

Unidad 5. Seguridad en  
administración de sistemas



VICEPRESIDENCIA  
PRIMERA DEL GOBIERNO  
MINISTERIO  
DE ASUNTOS ECONÓMICOS  
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO  
DE DIGITALIZACIÓN E  
INTELIGENCIA ARTIFICIAL

 **incibe**

INSTITUTO NACIONAL DE CIBERSEGURIDAD



# Contenidos

1	<i>PENTESTING WEB</i>	4
2	INSTALACIÓN Y CONFIGURACIÓN DE JUICE SHOP	6
3	VULNERABILIDAD <i>DIRECTORY TRAVERSAL</i>	23
4	ENUNCIADO EJERCICIO PRÁCTICO 1	27
5	SOLUCIONARIO EJERCICIO PRÁCTICO 1	29

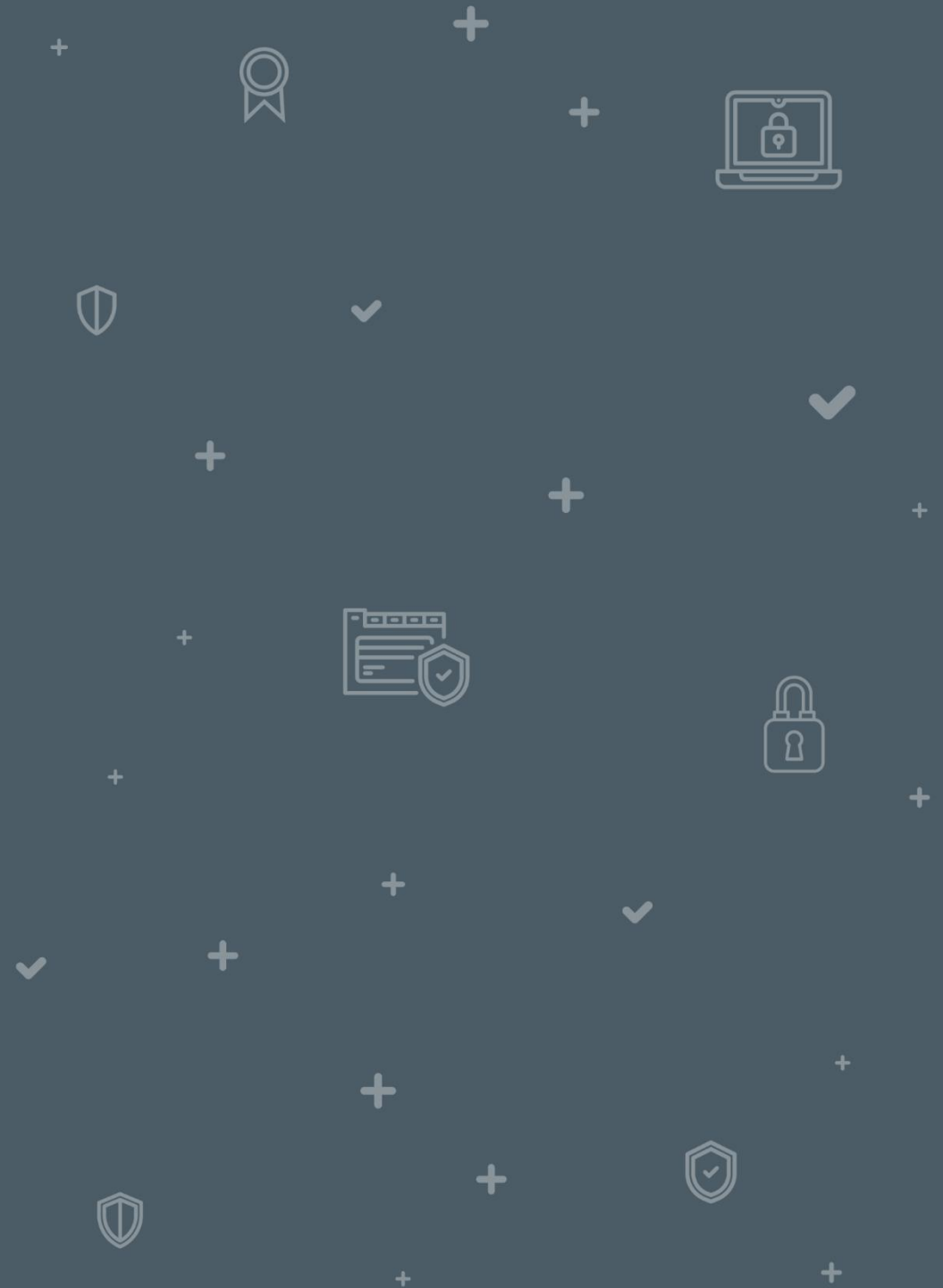
# Contenidos

<b>6</b>	<b>VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN</b>	<b>33</b>
<b>7</b>	<b>ENUNCIADO EJERCICIO PRÁCTICO 2</b>	<b>58</b>
<b>8</b>	<b>SOLUCIONARIO EJERCICIO PRÁCTICO 2</b>	<b>60</b>
<b>9</b>	<b>VULNERABILIDAD INYECCIÓN XSS</b>	<b>70</b>
<b>10</b>	<b>ENUNCIADO EJERCICIO PRÁCTICO 3</b>	<b>77</b>
<b>11</b>	<b>SOLUCIONARIO EJERCICIO PRÁCTICO 3</b>	<b>79</b>

Duración total del taller: 3 horas

# *PENTESTING WEB*

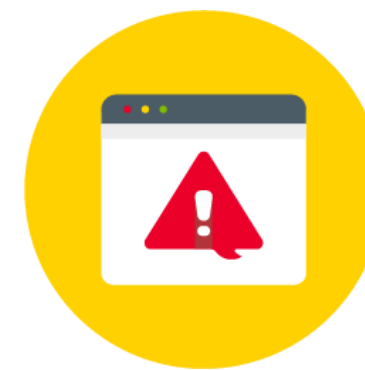
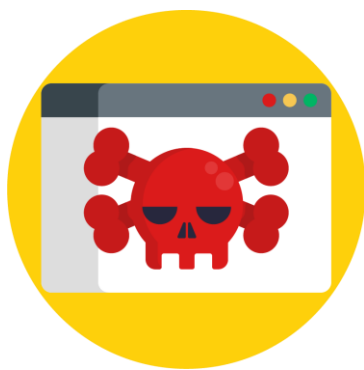
# 1



# 1 PENTESTING WEB

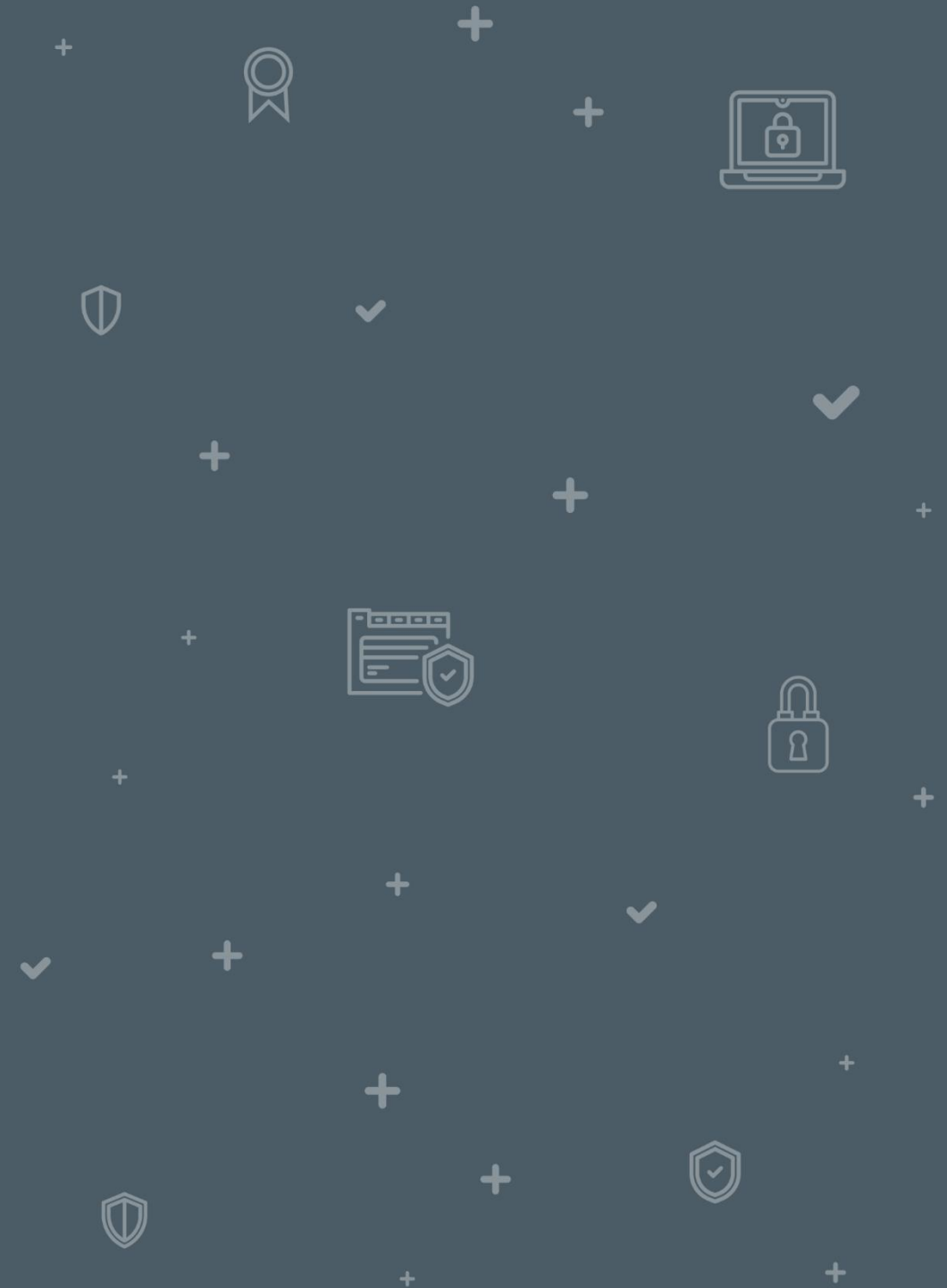
---

En esta práctica realizarás la instalación del entorno de *hacking Juice shop*, una máquina creada para practicar y realizar pruebas de ataques a páginas web.



# INSTALACIÓN Y CONFIGURACIÓN DE JUICE SHOP

## 2



## 2 INSTALACIÓN Y CONFIGURACIÓN DE JUICE SHOP

---

- Descarga el entorno de Juice Shop en la máquina Kali Linux. Lo más recomendable es hacerlo utilizando Node.js.
  - Juice Shop funciona con diferentes versiones de Node.js, por lo que instalarás la versión más reciente (Node.js vs16).
  - Para ello, primero deberás abrir la máquina virtual Kali Linux.
  - Después, deberás instalar **Node Version Manager (nvm)**, un *script bash* creado para administrar múltiples versiones de Node.js y no saturar el sistema operativo con paquetes innecesarios.
    - Abre una terminal en la máquina Kali Linux y descarga el siguiente *script* con el comando desde Kali: **curl -o- https://raw.githubusercontent.com/nvm-sh/nvm/v0.38.0/install.sh | bash.**

## 2 INSTALACIÓN Y CONFIGURACIÓN DE JUICE SHOP



Ilustración 1: Ubicación del botón de terminal Kali Linux.

```
(incibe@kali)-[~]  
$ curl -o- https://raw.githubusercontent.com/nvm-sh/nvm/v0.38.0/install.sh | bash
```

Ilustración 2: Comando `curl -o- https://raw.githubusercontent.com/nvm-sh/nvm/v0.38.0/install.sh | bash`.



## 2 INSTALACIÓN Y CONFIGURACIÓN DE JUICE SHOP

```
(incibe@kali)-[~]
$ curl -o- https://raw.githubusercontent.com/nvm-sh/nvm/v0.38.0/install.sh | bash
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             %         Dload  Upload  Total   Spent    Left   Speed
100 14926  100 14926    0     0  75383      0  --:--:-- --:--:-- --:--:-- 75383
=> Downloading nvm from git to '/home/incibe/.nvm'
=> Clonando en '/home/incibe/.nvm' ...
remote: Enumerating objects: 355, done.
remote: Counting objects: 100% (355/355), done.
remote: Compressing objects: 100% (302/302), done.
remote: Total 355 (delta 39), reused 170 (delta 28), pack-reused 0
Recibiendo objetos: 100% (355/355), 228.96 KiB | 1.29 MiB/s, listo.
Resolviendo deltas: 100% (39/39), listo.
* (HEAD desacoplado en FETCH_HEAD)
master
=> Compressing and cleaning up git repository

=> Appending nvm source string to /home/incibe/.bashrc
=> Appending bash_completion source string to /home/incibe/.bashrc
=> Close and reopen your terminal to start using nvm or run the following to use it now:

export NVM_DIR="$HOME/.nvm"
[ -s "$NVM_DIR/nvm.sh" ] && \. "$NVM_DIR/nvm.sh" # This loads nvm
[ -s "$NVM_DIR/bash_completion" ] && \. "$NVM_DIR/bash_completion" # This loads nvm bash_completion
```

Ilustración 3: Ejecución del comando `curl -o- https://raw.githubusercontent.com/nvm-sh/nvm/v0.38.0/install.sh | bash.`

## 2 INSTALACIÓN Y CONFIGURACIÓN DE JUICE SHOP

- Reinicia el terminal para aplicar los cambios realizados por el *script*. A continuación, verifica la versión instalada de NVM y después ya puedes instalar la última versión de Node.js
- Utiliza el siguiente comando para verificar la versión instalada: **nvm -v**

```
(incibe@kali)-[~]  
$ nvm -v  
0.38.0
```

Ilustración 4: Versión instalada de NVM.

## 2 INSTALACIÓN Y CONFIGURACIÓN DE JUICE SHOP

- Utiliza el siguiente comando para instalar la última versión: **nvm install --lts**

```
(incibe@kali)-[~]  
$ nvm install --lts  
Installing latest LTS version.  
Downloading and installing node v16.15.1 ...  
Downloading https://nodejs.org/dist/v16.15.1/node-v16.15.1-linux-x64.tar.xz...  
#####  
Computing checksum with sha256sum  
Checksums matched!  
Now using node v16.15.1 (npm v8.11.0)  
Creating default alias: default -> lts/* (-> v16.15.1)
```

Ilustración 5: Instalación de la última versión de Node.js

## 2 INSTALACIÓN Y CONFIGURACIÓN DE JUICE SHOP

- Utiliza el siguiente comando para verificar la última versión instalada actualizada: **node --version**

```
(incibe® kali)-[~]  
$ node --version  
v16.15.1
```

Ilustración 6: Última versión instalada de Node.js actualizada.

## 2 INSTALACIÓN Y CONFIGURACIÓN DE JUICE SHOP

- Una vez configurado lo anterior, instala el entorno Juice Shop. Para ello, accede al [enlace](#).
  - Haz clic en la carpeta *Files*, donde podrás descargar la última versión.

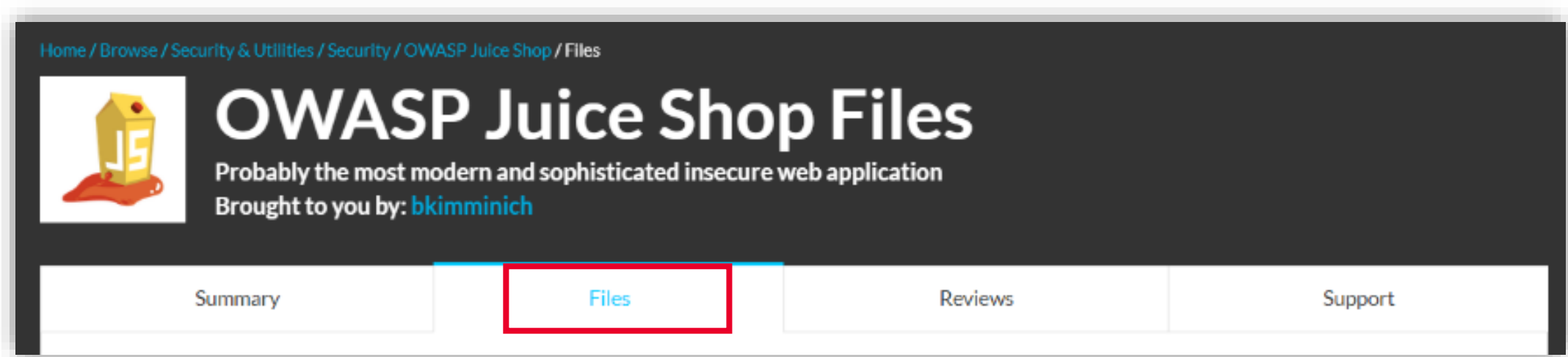
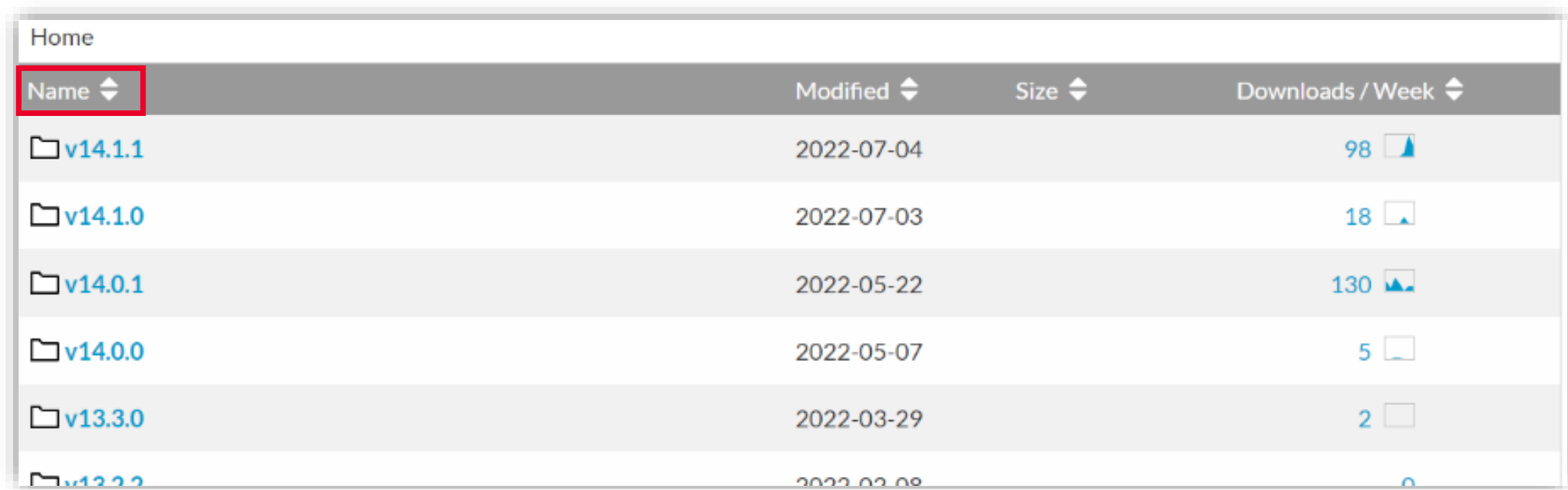


Ilustración 7: Ubicación de la carpeta *Files* en Juice shop.

## 2 INSTALACIÓN Y CONFIGURACIÓN DE JUICE SHOP

- Identifica el sistema operativo que vas a utilizar y qué versión de Node.js dispones.



The screenshot shows a web interface for searching Node.js versions. At the top, there is a 'Home' link. Below it is a table with columns: 'Name', 'Modified', 'Size', and 'Downloads / Week'. The 'Name' column is highlighted with a red box. The table lists several versions of Node.js, including v14.1.1, v14.1.0, v14.0.1, v14.0.0, v13.3.0, and v13.2.2. Each row shows the version number, the date it was modified, and the number of downloads per week, along with a small line graph icon.

Name	Modified	Size	Downloads / Week
v14.1.1	2022-07-04		98
v14.1.0	2022-07-03		18
v14.0.1	2022-05-22		130
v14.0.0	2022-05-07		5
v13.3.0	2022-03-29		2
v13.2.2	2022-03-08		0

Ilustración 8: Búsqueda de versiones de Node.js.

## 2 INSTALACIÓN Y CONFIGURACIÓN DE JUICE SHOP

- En este caso, descarga la versión para Linux con la versión 16 de Node.js anterior. Aunque la versión de Juicy Shop, según la imagen, es la 14, podrás ver la versión de Node.js dentro de cada una de las carpetas, como se muestra en la imagen siguiente. Si quieres emplearlo en un sistema operativo diferente al Kali Linux de la máquina virtual, descarga la opción adecuada.



<a href="#">juice-shop-14.1.1_node16_linux_x64.tgz</a>	2022-07-04	146.9 MB	34 	
--	------------	----------	--	---

Ilustración 9: Versión para Linux con la versión 16 de Node.js.

## 2 INSTALACIÓN Y CONFIGURACIÓN DE JUICE SHOP



Ilustración 10: Descarga de Juicy Shop 14.1.1 compatible con Node16.



## 2 INSTALACIÓN Y CONFIGURACIÓN DE JUICE SHOP

- Una vez completada la descarga, se abrirá una ventana emergente en la que deberás seleccionar la opción *Save File*. Pulsa en *OK*.

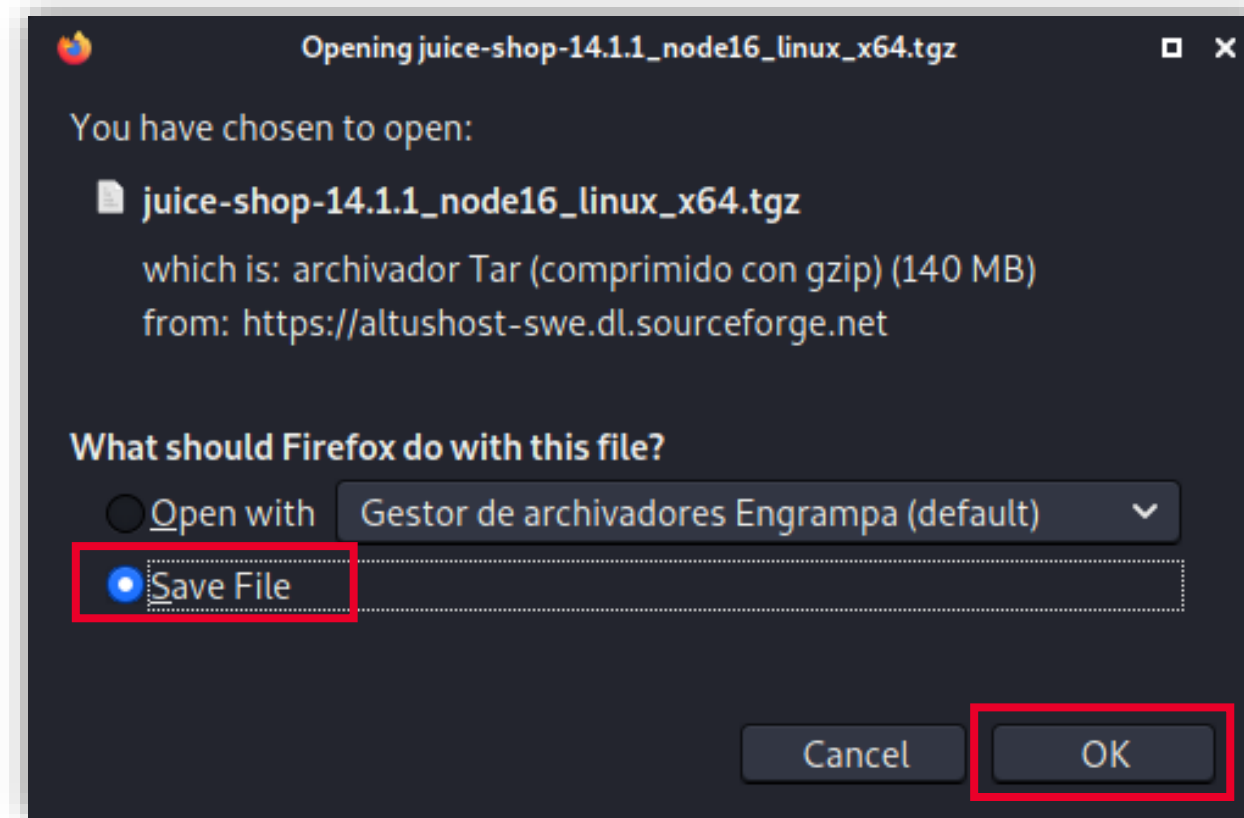
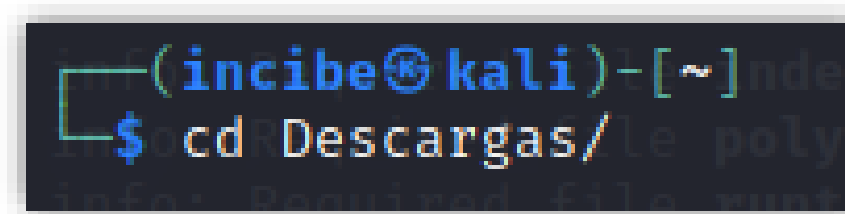


Ilustración 11: Opción de guardar seleccionada.

## 2 INSTALACIÓN Y CONFIGURACIÓN DE JUICE SHOP

- A no ser que hayas indicado otra ruta, el archivo se habrá almacenado por defecto en el directorio «**Descargas**». En nuestro caso, lo hemos dejado en «Descargas», sin embargo, lo conveniente es que muevas el archivo a otro directorio, donde estés almacenando la información de este curso. Abre una terminal en la máquina Kali Linux y accede a la carpeta donde hayas dejado el archivo, como hemos comentado, en nuestro caso «Descargas».



```
(incibe@kali)-[~]
$ cd Descargas/
```

Ilustración 12: Acceso a la carpeta «Descargas» en Kali Linux.

## 2 INSTALACIÓN Y CONFIGURACIÓN DE JUICE SHOP

- Dentro de la carpeta, descomprime el archivo antes descargado que tiene una extensión .tgz. Se descomprime utilizando el comando **tar -xzf juice-shop-14.1.1\_node16\_linux\_x64.tgz**

```
info: Port 3000 is available (OK)
(incibe@kali)-[~/Descargas]
$ tar -xzf juice-shop-14.1.1_node16_linux_x64.tgz
info: Server listening on port 3000
```

Ilustración 13: Comando tar -xzf juice-shop-14.1.1\_node16\_linux\_x64.tgz.

## 2 INSTALACIÓN Y CONFIGURACIÓN DE JUICE SHOP

- Tras completar la descarga, accede a la carpeta de Juice shop para ejecutar esta herramienta.

```
(incibe@kali)-[~/Descargas/juice-shop_14.1.1]
$ ls
build      config      CONTRIBUTING.md  data  fileServer  frontend  HALL_OF_FAME.md
CODE_OF_CONDUCT.md  config.schema.yml  ctf.key  encryptionkeys  ftp  i18n
```

```
lib      models      package.json  REFERENCES.md  SECURITY.md  SOLUTIONS.md  uploads
LICENSE  node_modules  README.md    routes         server.ts   swagger.yml   views
```

Ilustración 14: Carpeta de Juice Shop.

## 2 INSTALACIÓN Y CONFIGURACIÓN DE JUICE SHOP

- Para ejecutar el entorno, utiliza el comando **npm start**

```
(incibe@kali)~[~/Descargas/juice-shop_14.1.1]
$ npm start
> juice-shop@14.1.1 start
> node build/app

info: All dependencies in ./package.json are satisfied (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Detected Node.js version v16.15.1 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Entity models 19 of 19 are initialized (OK)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file styles.css is present (OK)
info: Required file main.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file runtime.js is present (OK)
info: Required file vendor.js is present (OK)
(node:73882) [DEP0152] DeprecationWarning: Custom PerformanceEntry accessors are deprecated. Please use the detail property.
(Use `node --trace-deprecation ...` to show where the warning was created)
info: Port 3000 is available (OK)
info: Server listening on port 3000
```

Ilustración 15: Ejecución del comando npm start.

## 2 INSTALACIÓN Y CONFIGURACIÓN DE JUICE SHOP

- A continuación, se notificará un mensaje que indica que el servidor está escuchando en el puerto 3000. Abre el navegador con la IP del *localhost* (127.0.0.1) y el puerto anteriormente mencionado (3000).

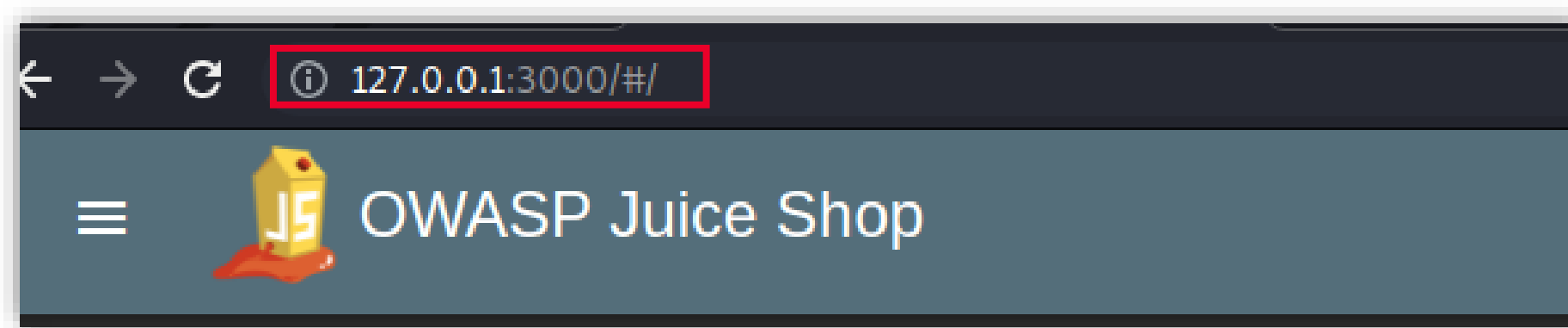
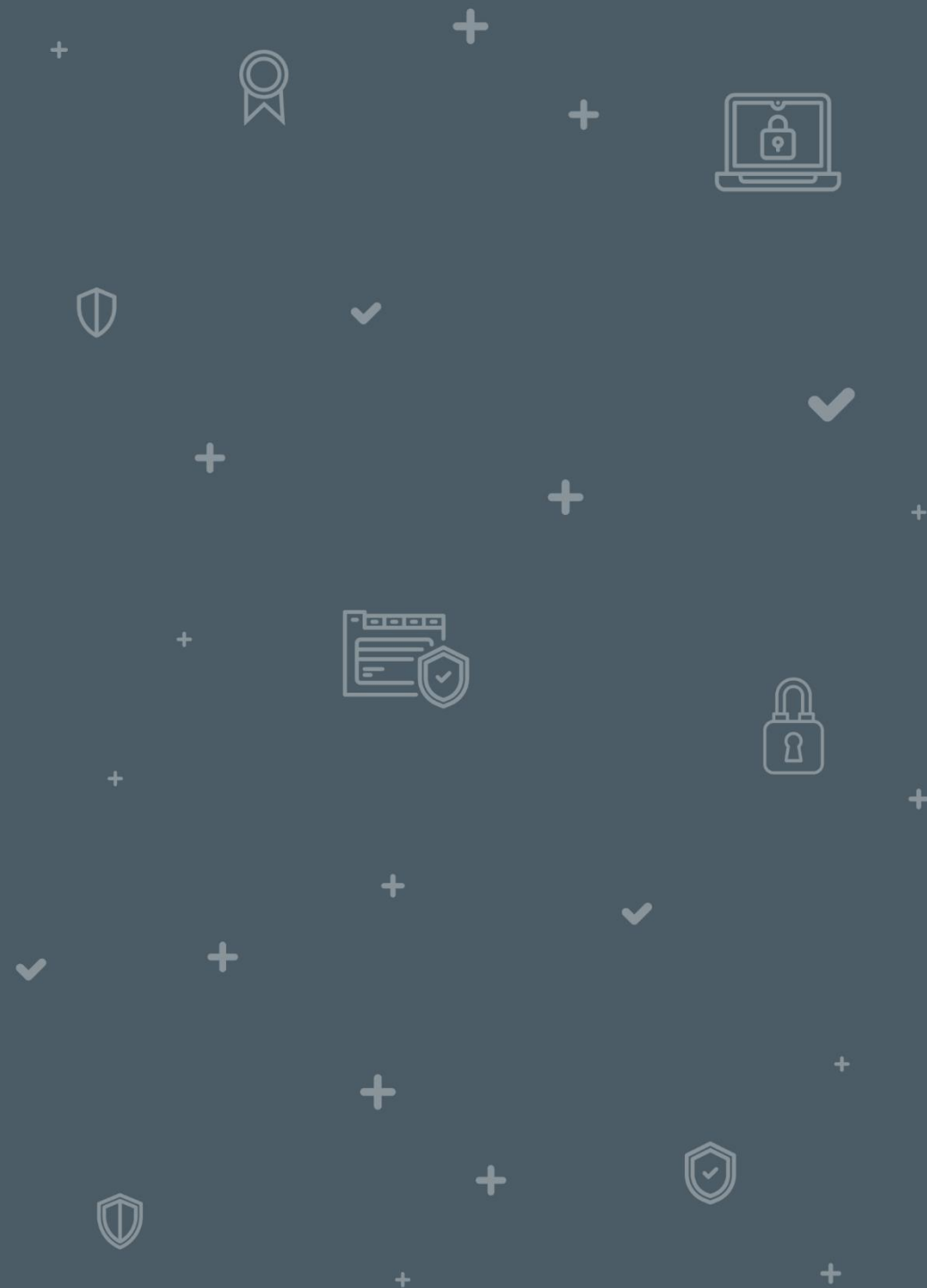


Ilustración 16: IP del *localhost* (127.0.0.1) y el puerto 3000 en la barra del navegador.

# 3

## VULNERABILIDAD *DIRECTORY* *TRAVERSAL*



## 3 VULNERABILIDAD *DIRECTORY TRAVERSAL*

---

Un *directory traversal* o *path traversal* consiste en explotar una vulnerabilidad que ocurre cuando no existe suficiente seguridad en cuanto a la validación de un usuario, permitiéndole acceder a cualquier tipo de directorio sin ningún control. La finalidad de este ataque es acceder a un archivo al que no se debería poder acceder o no debería ser accesible y se basa en la falta de seguridad en el código o mala configuración.

En este caso, lanzarás la herramienta **Dirbuster**, que funciona mediante fuerza bruta, probando todos los directorios típicos de una página web. Para ello, configurarás una terminal de la máquina Kali Linux, ejecutarás el comando **dirb** y añadirás la dirección **http** de la aplicación Juice Shop.



## 3 VULNERABILIDAD DIRECTORY TRAVERSAL

- Abre una terminal de Kali Linux y escribe el comando **dirb http://127.0.0.1:3000**

Ilustración 17: Ejecución del comando dirb junto con la dirección http de la Juice Shop.

```
(incibe@kali)-[~]
$ dirb http://127.0.0.1:3000/

DIRB v2.22
By The Dark Raver

START_TIME: Wed Jul 6 10:47:58 2022
URL_BASE: http://127.0.0.1:3000/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

— Scanning URL: http://127.0.0.1:3000/ —
+ http://127.0.0.1:3000/assets (CODE:301|SIZE:179)
+ http://127.0.0.1:3000/ftp (CODE:200|SIZE:11040)
+ http://127.0.0.1:3000/profile (CODE:500|SIZE:1299)
+ http://127.0.0.1:3000/promotion (CODE:200|SIZE:6586)
+ http://127.0.0.1:3000/redirect (CODE:500|SIZE:3764)
+ http://127.0.0.1:3000/robots.txt (CODE:200|SIZE:28)
+ http://127.0.0.1:3000/snippets (CODE:200|SIZE:683)
+ http://127.0.0.1:3000/video (CODE:200|SIZE:10075518)
+ http://127.0.0.1:3000/Video (CODE:200|SIZE:10075518)

END_TIME: Wed Jul 6 10:49:24 2022
DOWNLOADED: 4612 - FOUND: 9
```

## 3 VULNERABILIDAD DIRECTORY TRAVERSAL

- Con este resultado, observa que se encuentran varios directorios que no deberían ser accesibles, entre ellos, el directorio «**robots.txt**», un archivo que se encuentra en la raíz de un sitio web e indica a qué partes no quieren que accedan los rastreadores de los motores de búsqueda. Una buena configuración de la página web no mostraría este directorio, ya que no debería ser accesible.

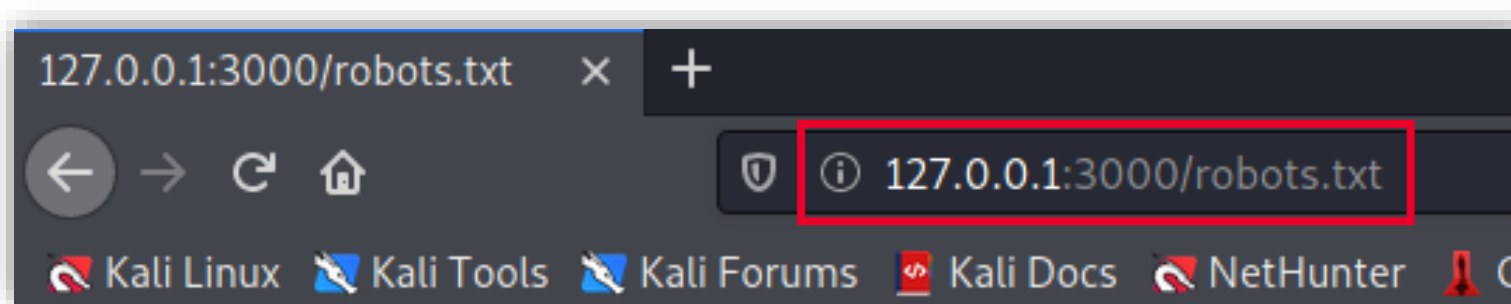
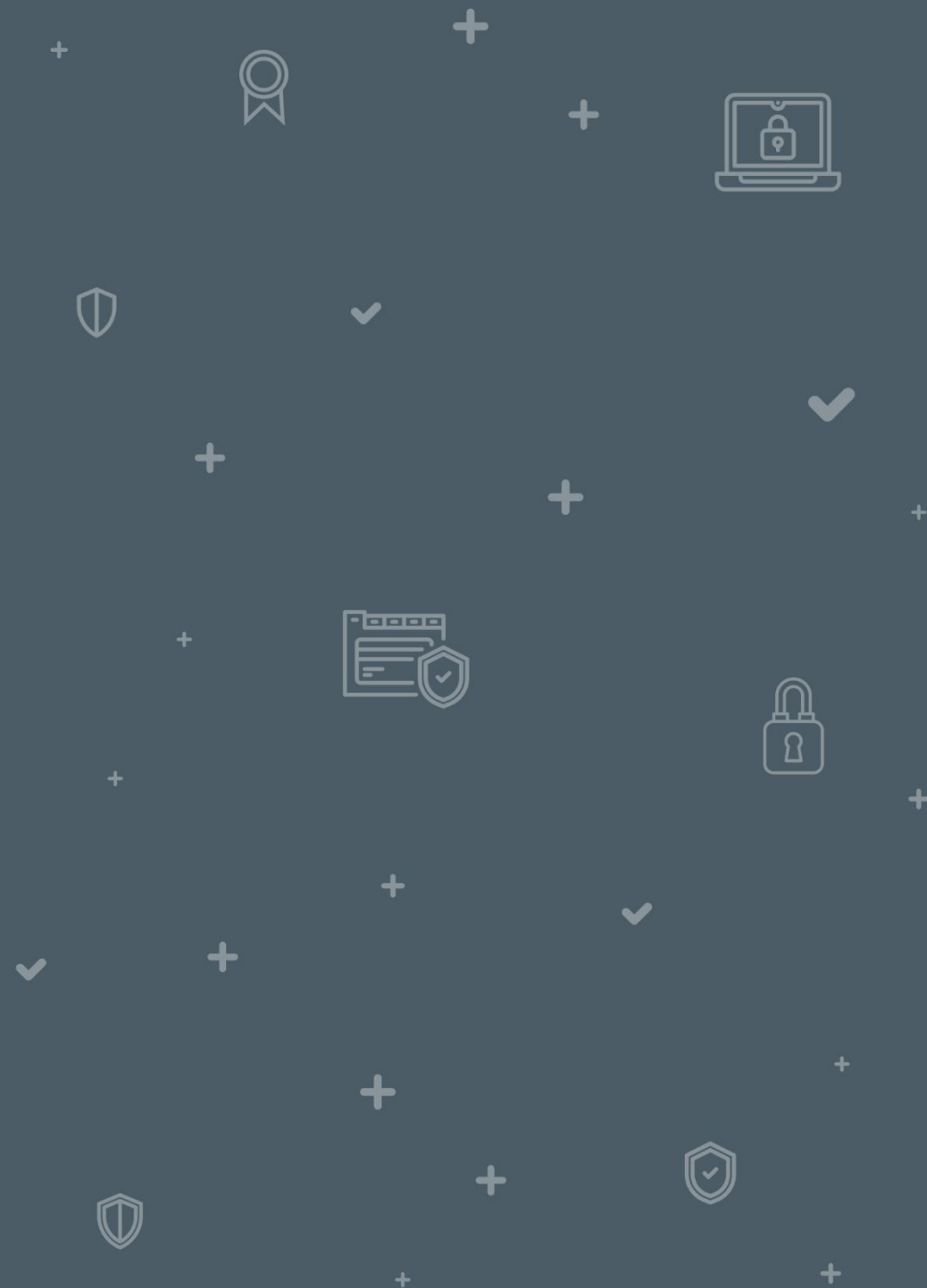


Ilustración 18: Directorio «robots.txt».

# 4

## ENUNCIADO EJERCICIO PRÁCTICO 1



## 4 ENUNCIADO EJERCICIO PRÁCTICO 1

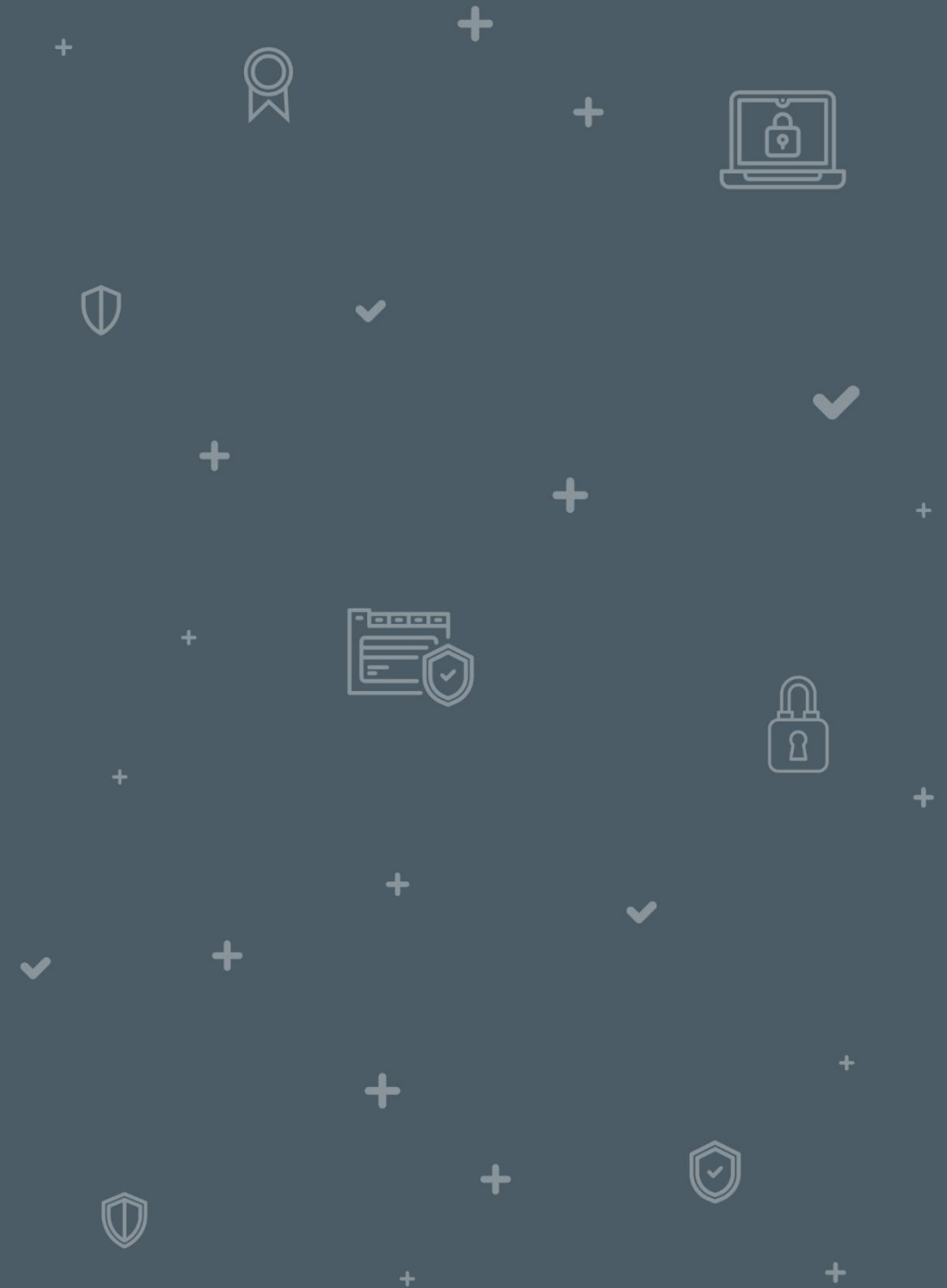
---



¿Podrías encontrar algún archivo con información sensible en alguno de estos directorios?

# 5

## SOLUCIONARIO EJERCICIO PRÁCTICO 1



## 5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- En el directorio «robots.txt» indica que está deshabilitado el directorio «**/ftp**», lo que puede tratarse de un directorio al que el creador de la web no quiere que se acceda porque puede contener información privada.

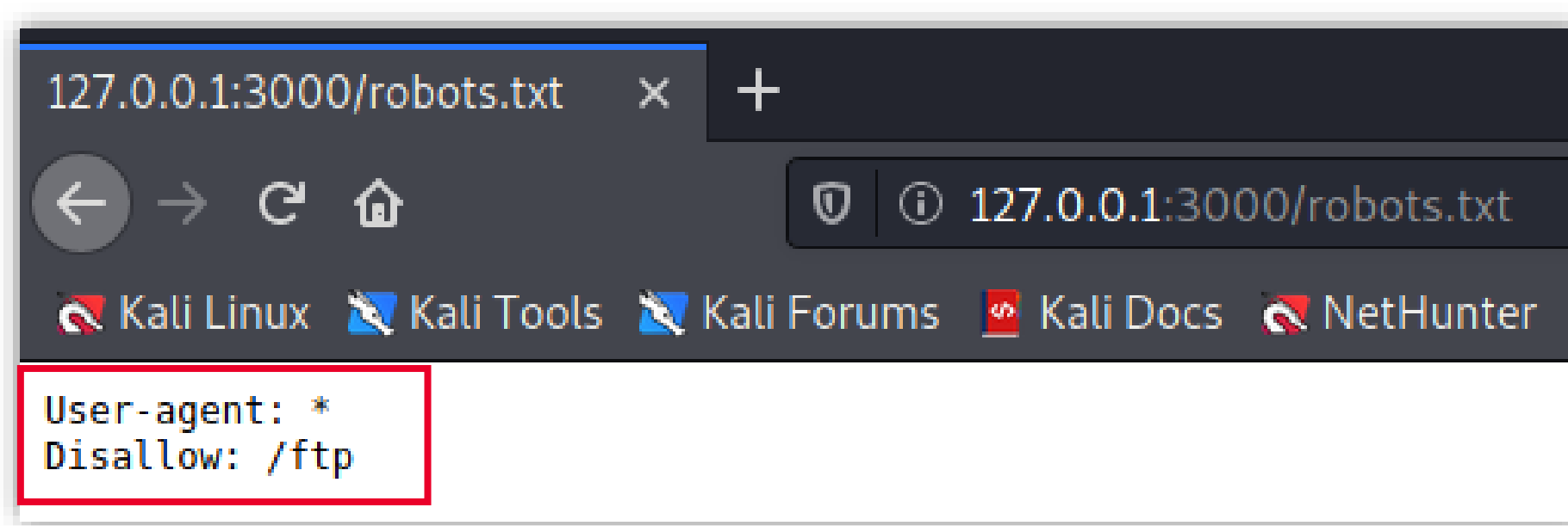


Ilustración 19: El directorio «/ftp» está deshabilitado.

## 5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

- Como sabemos, esta página tiene una mala configuración. Por tanto, al entrar en el directorio «/ftp», aparecen varios archivos con datos sensibles que no deberían ser accesibles, entre ellos, uno denominado «legal.md», que podría ser información confidencial de esta web.

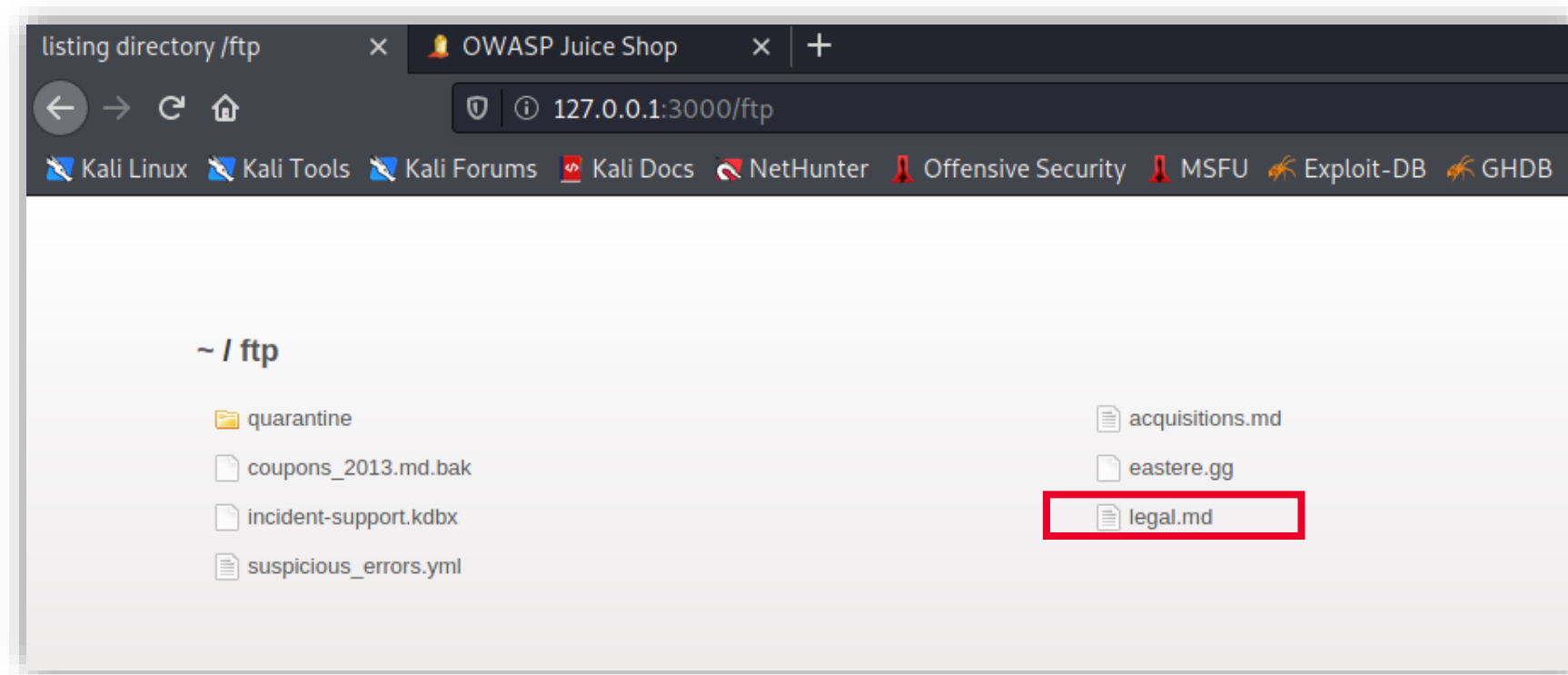


Ilustración 20: Archivos con datos sensibles.

## 5 SOLUCIONARIO EJERCICIO PRÁCTICO ACTIVIDAD 1

---

- Abre los archivos «legar.md» y «acquisitions.md».
  - Al volver al menú principal de Juice Shop, observa que se ha resuelto la prueba de acceso a un documento confidencial.



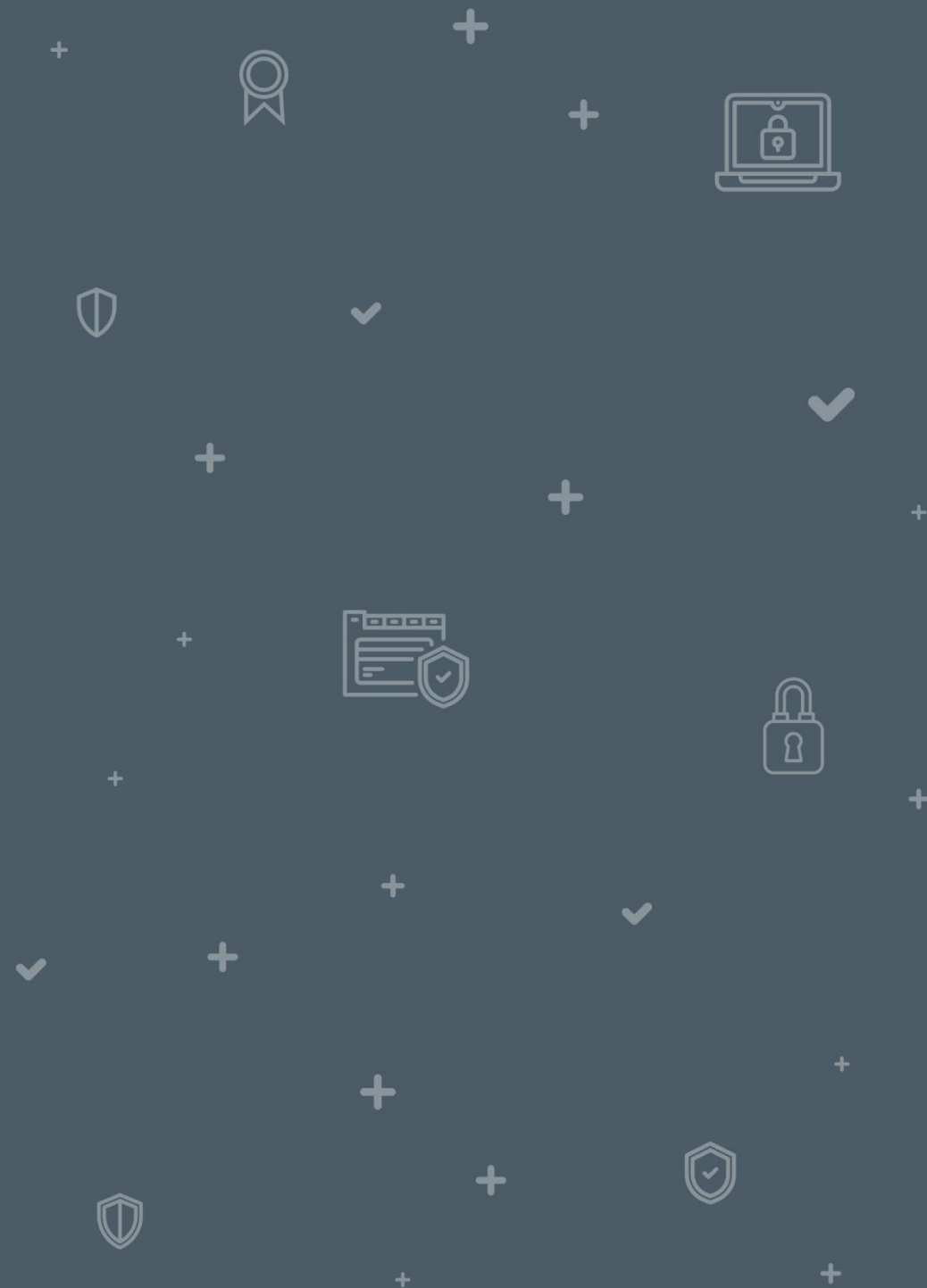
You successfully solved a challenge: Confidential Document (Access a confidential document.)

Ilustración 21: Resolución de la prueba de acceso a un documento confidencial.



# 6

## VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN



## 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

- En el menú principal de la página, observa que los productos tienen reseñas. En una de ellas, hay un usuario que puede ser de interés, ya que puede tratarse de un administrador con permisos, cuyo correo electrónico sería **admin@juice-sh.op**. En este caso, el objetivo es conseguir la contraseña de este usuario a través de un ataque por fuerza bruta.

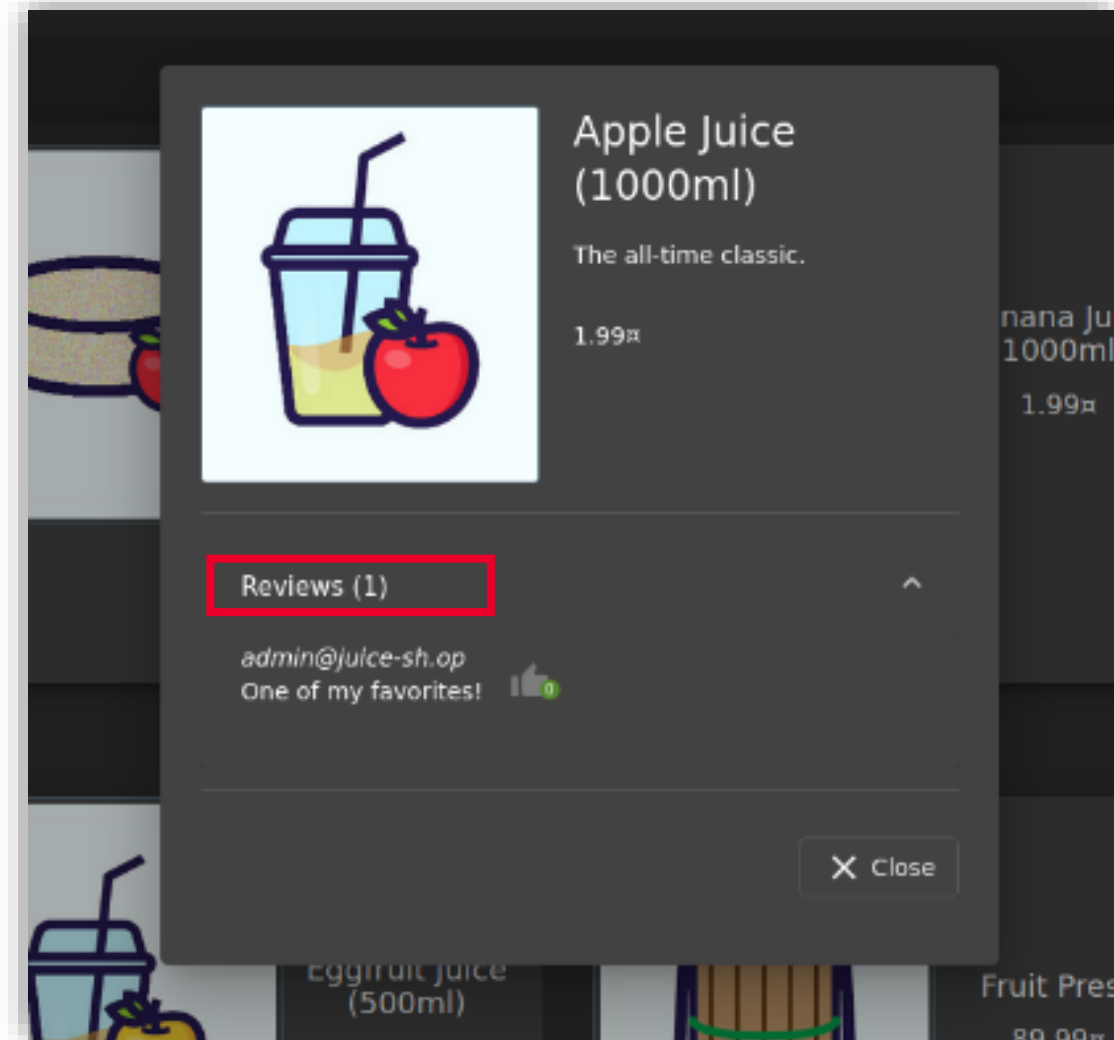


Ilustración 22: Apartado de reseñas.

## 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

---

- Intenta registrarte con este usuario.
- Para probar esta vulnerabilidad, necesitas la herramienta **BurpSuite**, un conjunto de herramientas diseñado para ayudar en las pruebas de penetración de aplicaciones web a través de HTTP y HTTPS.
  - La herramienta principal es un *proxy* diseñado para permitir el análisis y la edición del tráfico web. El *proxy* puede interceptar solicitudes y respuestas web y leerlas y editarlas en tiempo real antes de que lleguen a sus respectivos destinos.
- Para usar esta herramienta, deberás instalar y configurar el *proxy*.
  - Añade una extensión denominada **FoxyProxy**, que encontrarás en este [enlace](#) y haz clic en «Agregar a Firefox».

## 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

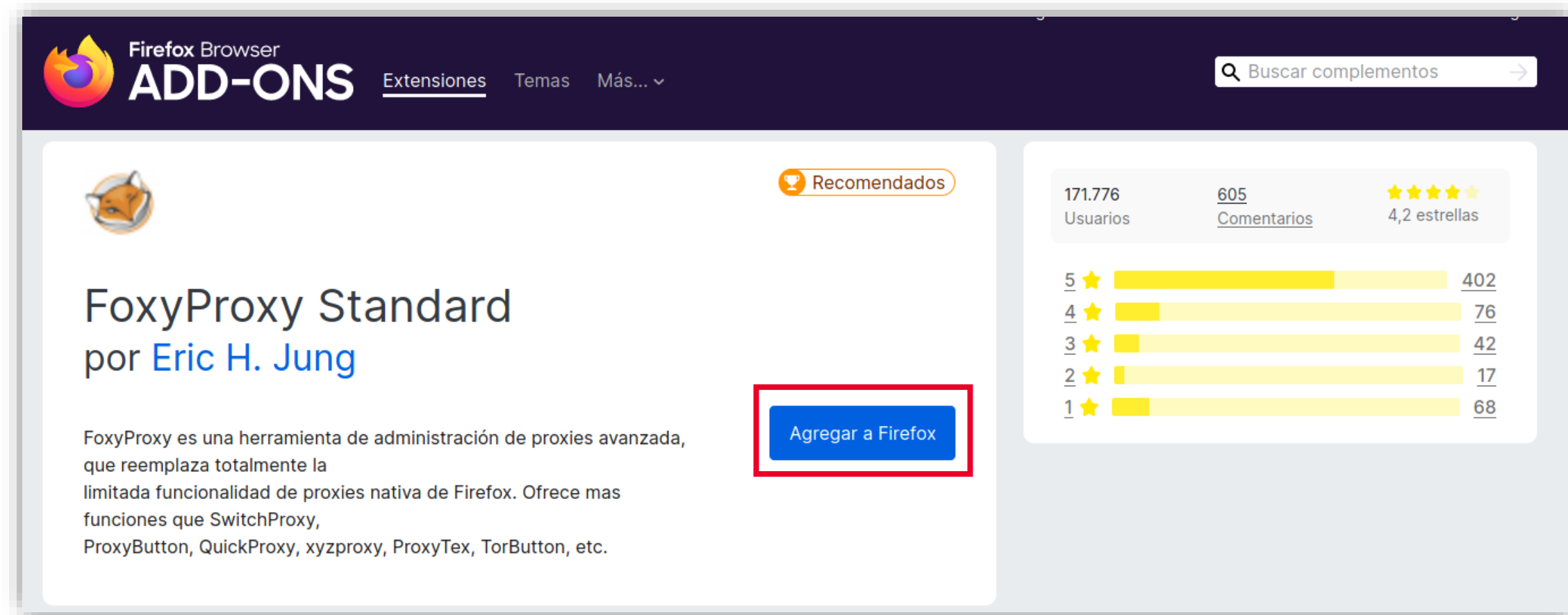


Ilustración 23: Extensión FoxyProxy y ubicación del botón «Agregar a Firefox».

## 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

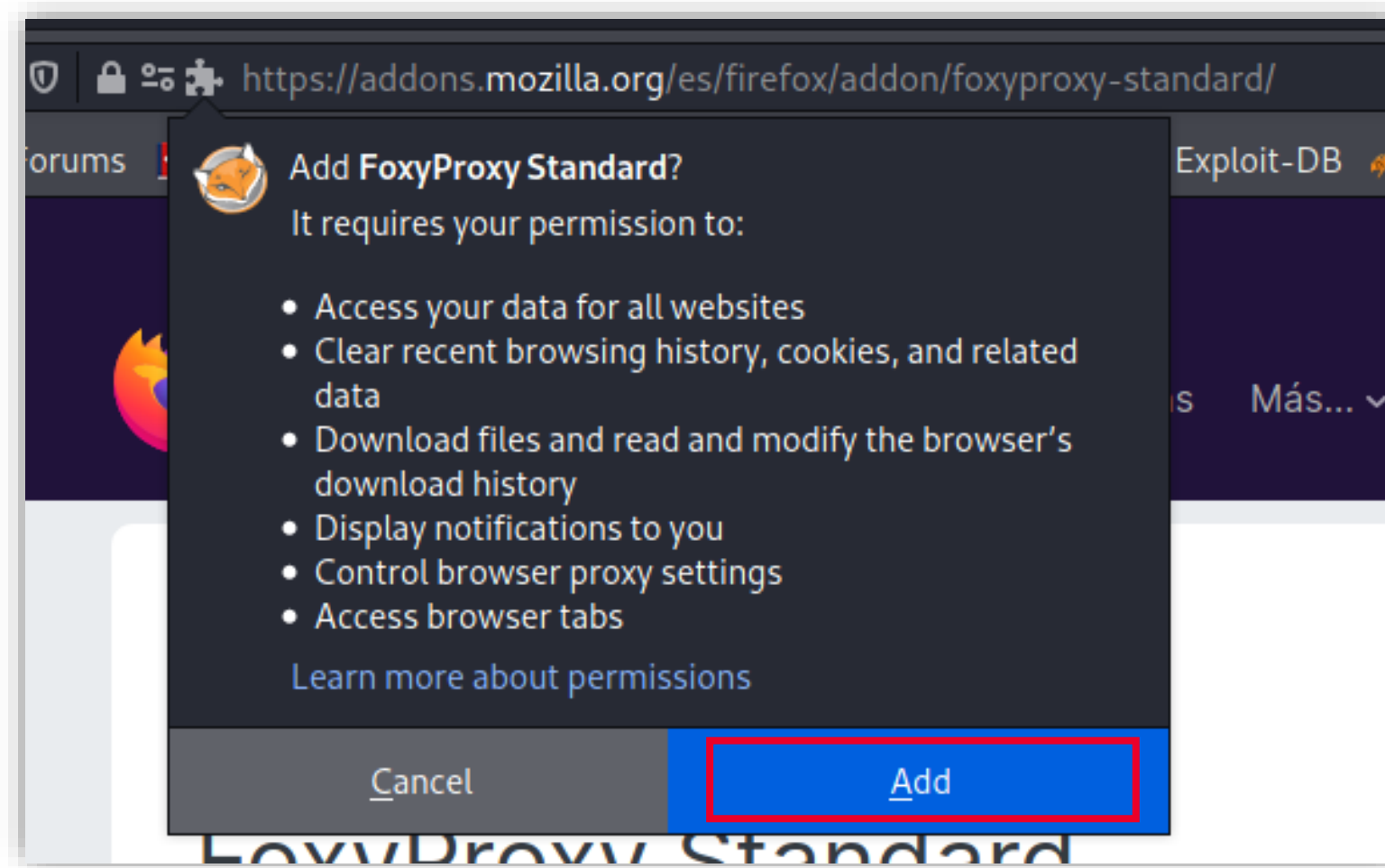


Ilustración 24: Añadir extensión FoxyProxy estándar.

## 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

- Una vez añadida, aparecerá un icono en la parte superior derecha, donde se desplegará un menú. Haz clic en «Options».

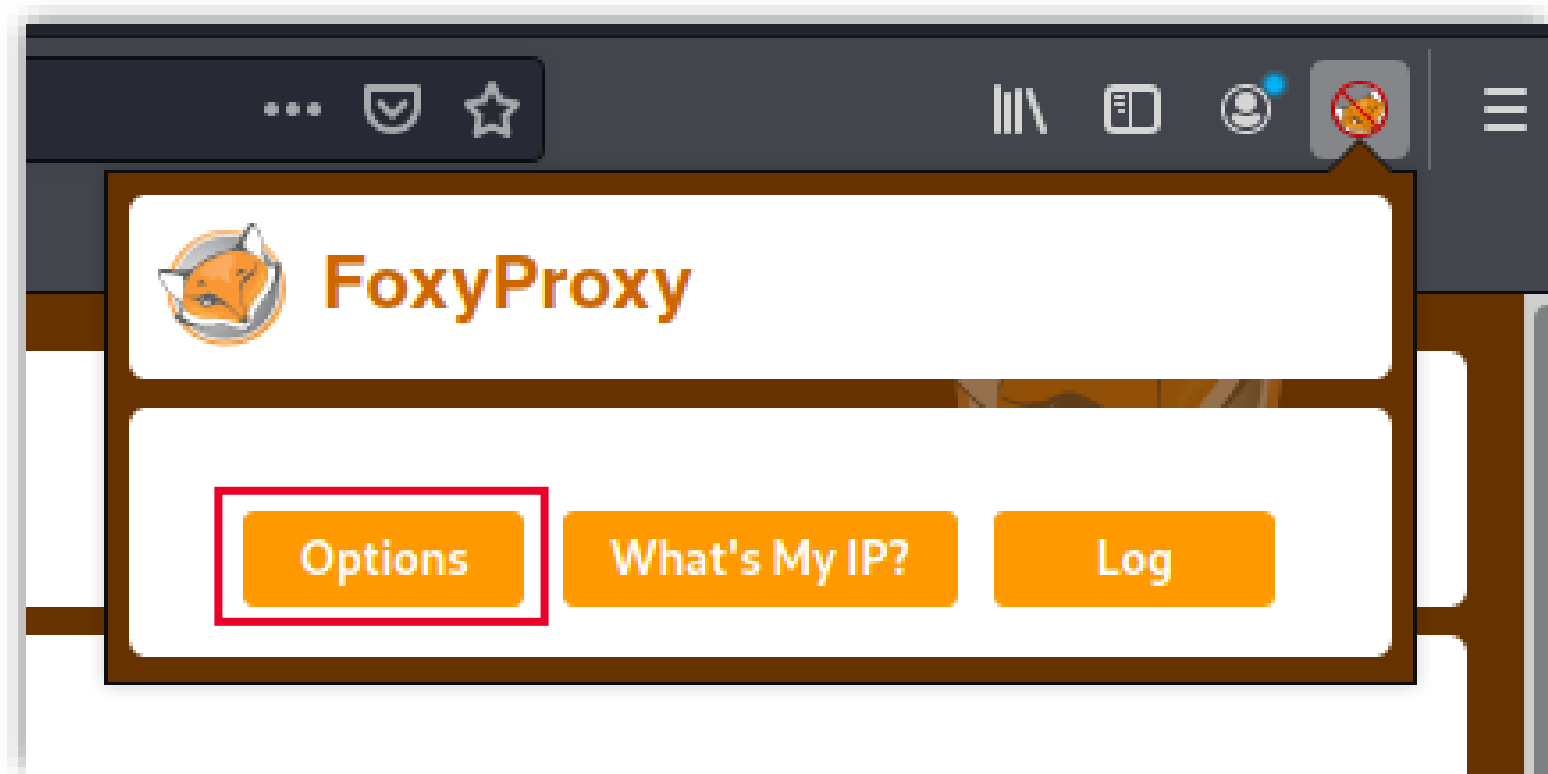


Ilustración 25: Menú y botón de «Options».

## 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

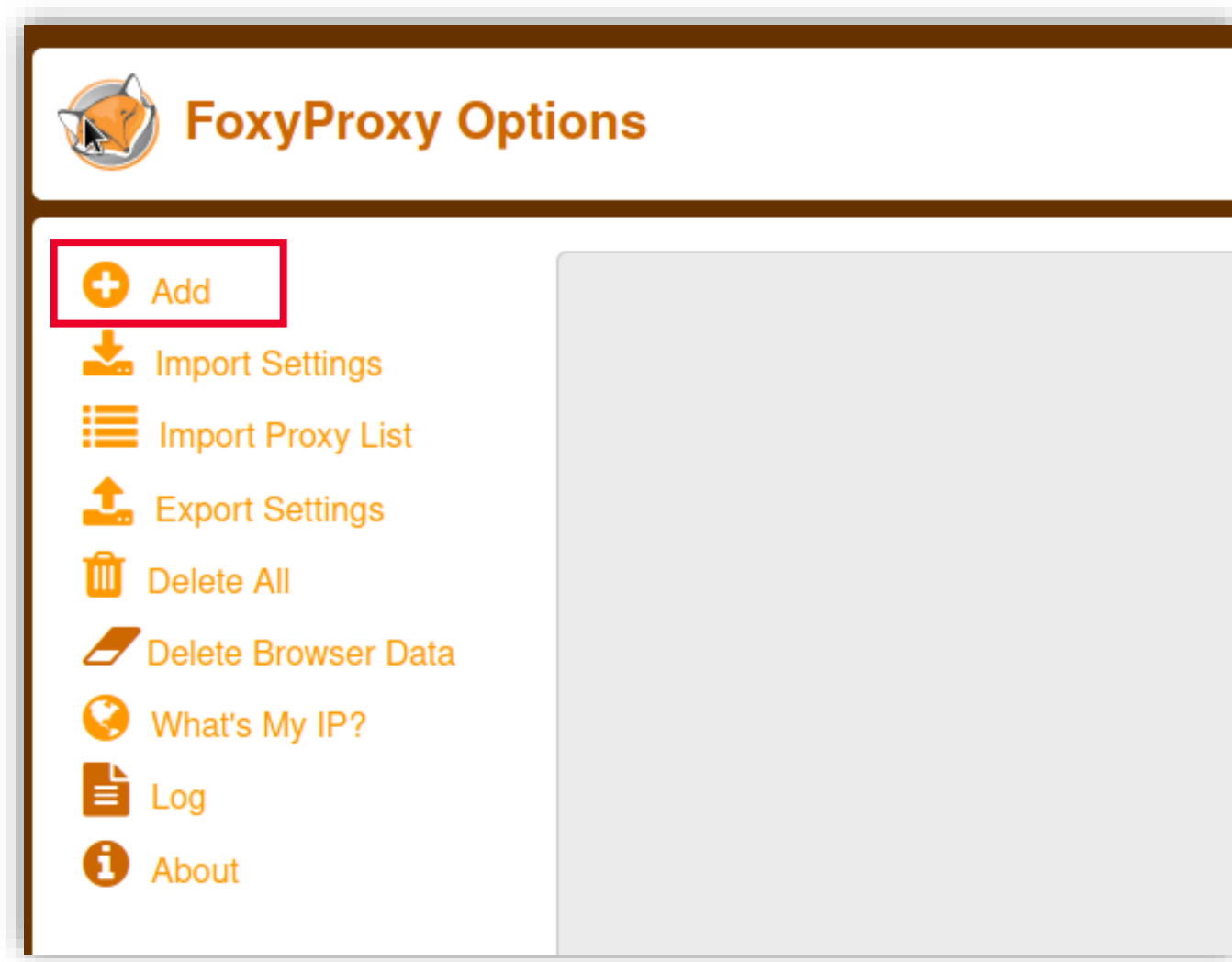
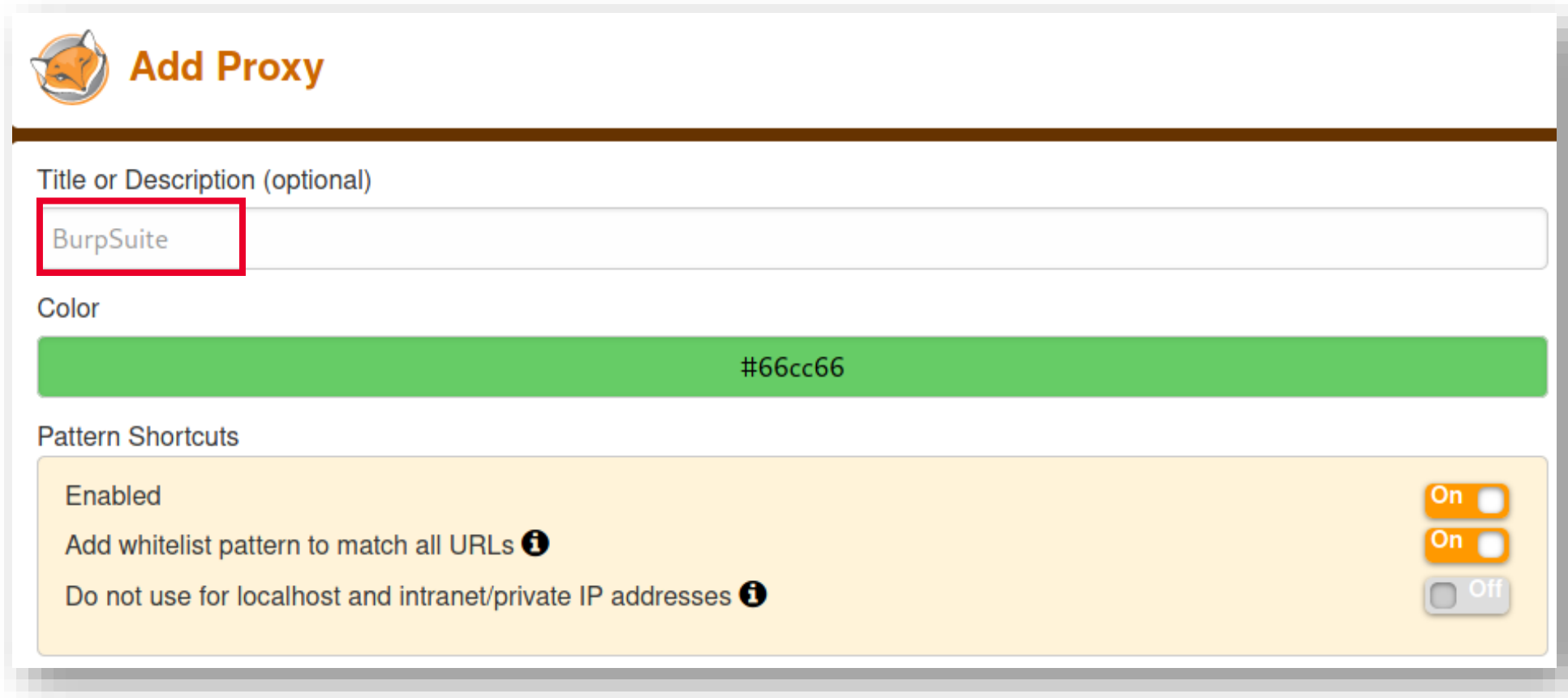



Ilustración 26: Opción «Añadir».

## 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

- Añade la siguiente configuración y haz clic en «Save».



 **Add Proxy**

Title or Description (optional)


BurpSuite

Color

#66cc66

Pattern Shortcuts

Enabled ☒ On

Add whitelist pattern to match all URLs  ☒ On


Do not use for localhost and intranet/private IP addresses  ☐ Off

Ilustración 27: Campos de configuración.



## 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

Proxy Type

HTTP

Proxy IP address or DNS name ★

127.0.0.1

Port ★

8080

Username (optional)

username

Password (optional) 👁

\*\*\*\*\*

Cancel Save & Add Another Save & Edit Patterns Save

Ilustración 28: Campos de configuración y clic en «Save».

## 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

- Una vez instalado y configurado el *proxy*, abre la herramienta BurpSuite dentro de la máquina Kali Linux, la cual viene instalada por defecto.
- Ejecuta el comando **burpsuite**. Se abrirá una ventana emergente que indica un aviso de que existe una nueva versión disponible, que no actualizarás por ahora. Haz clic en «Close» para continuar con la versión actual.

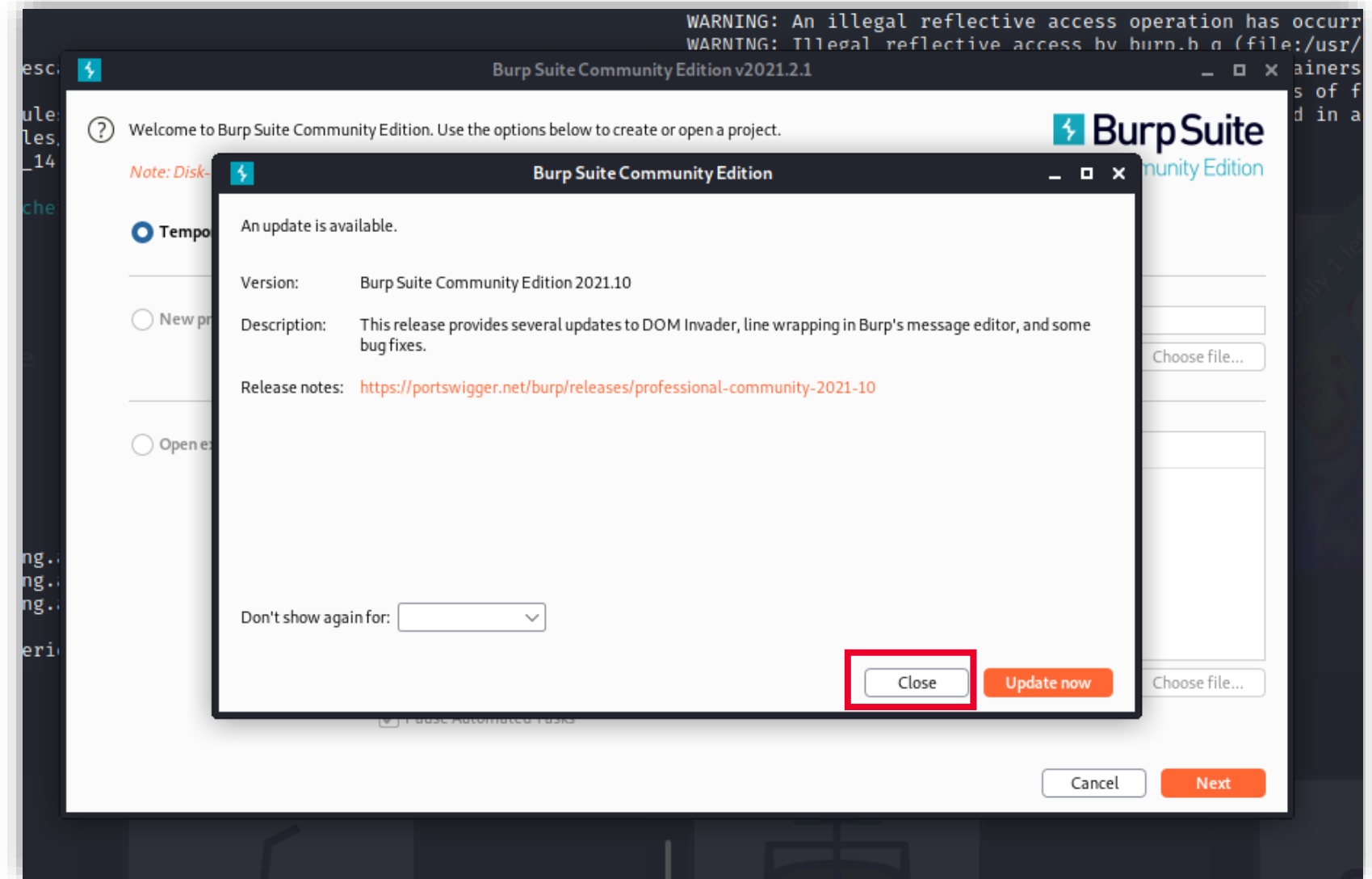


Ilustración 29: Botón de cierre en la ventana de actualización.

## 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

- Una vez abierto BurpSuite, inicia el ataque. Para ello, accede antes a la página de *Login* de nuestra Juice Shop.

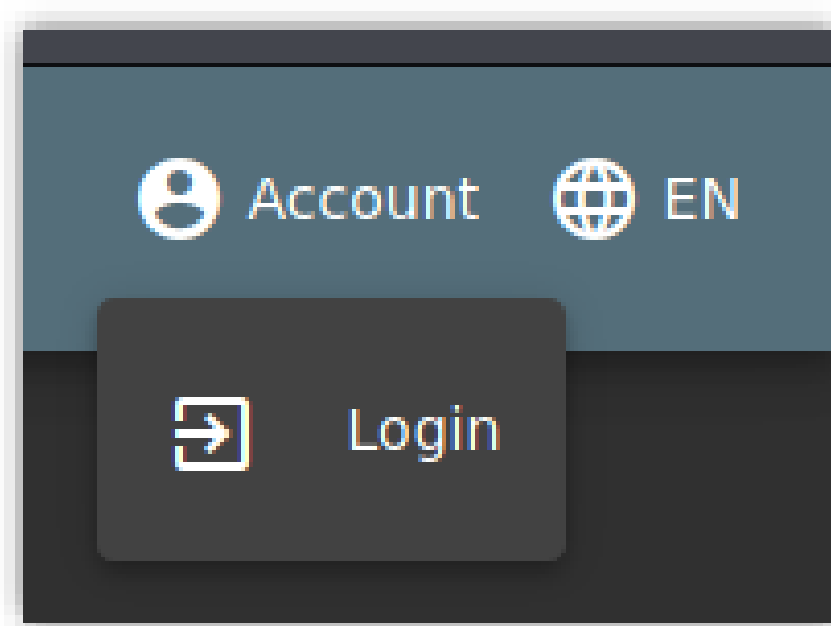


Ilustración 30: Página de *Login* de Juice Shop.

## 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

- Activa el *proxy* antes instalado pulsando en el icono que está en la esquina superior derecha del navegador y seleccionando la opción BurpSuite antes configurada.

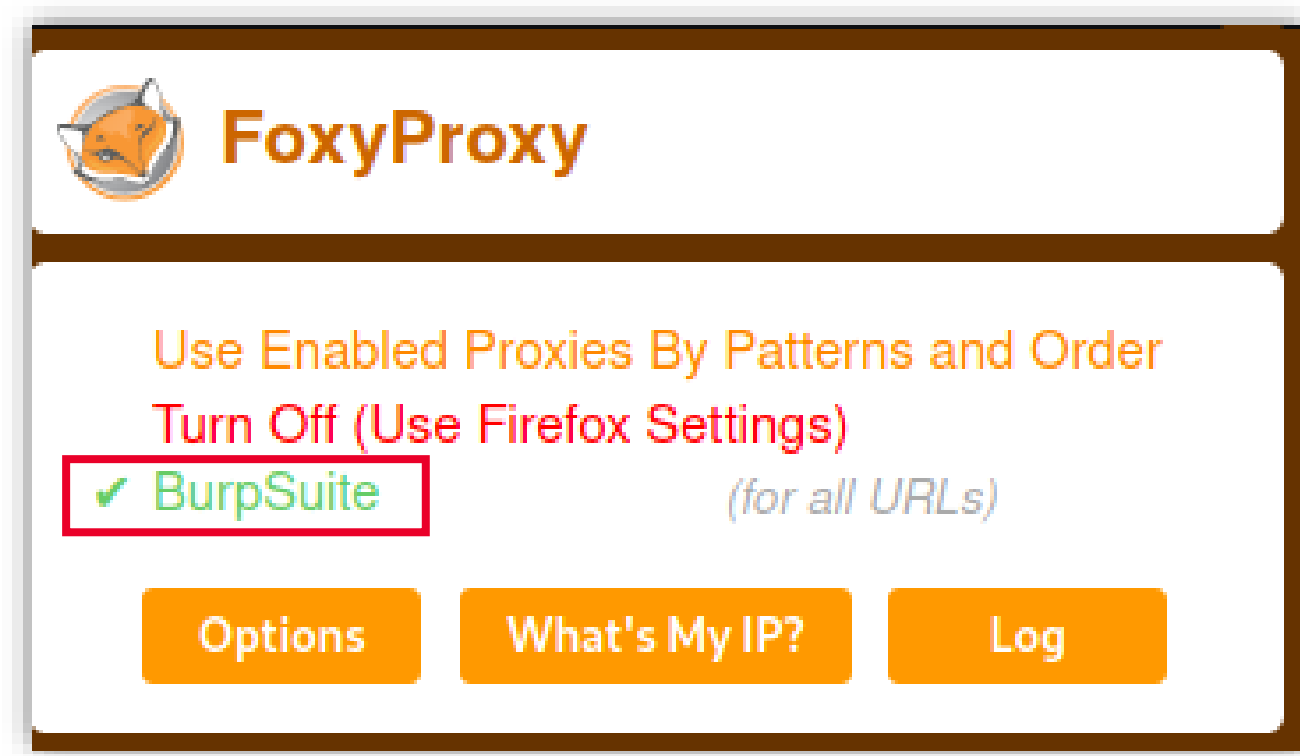
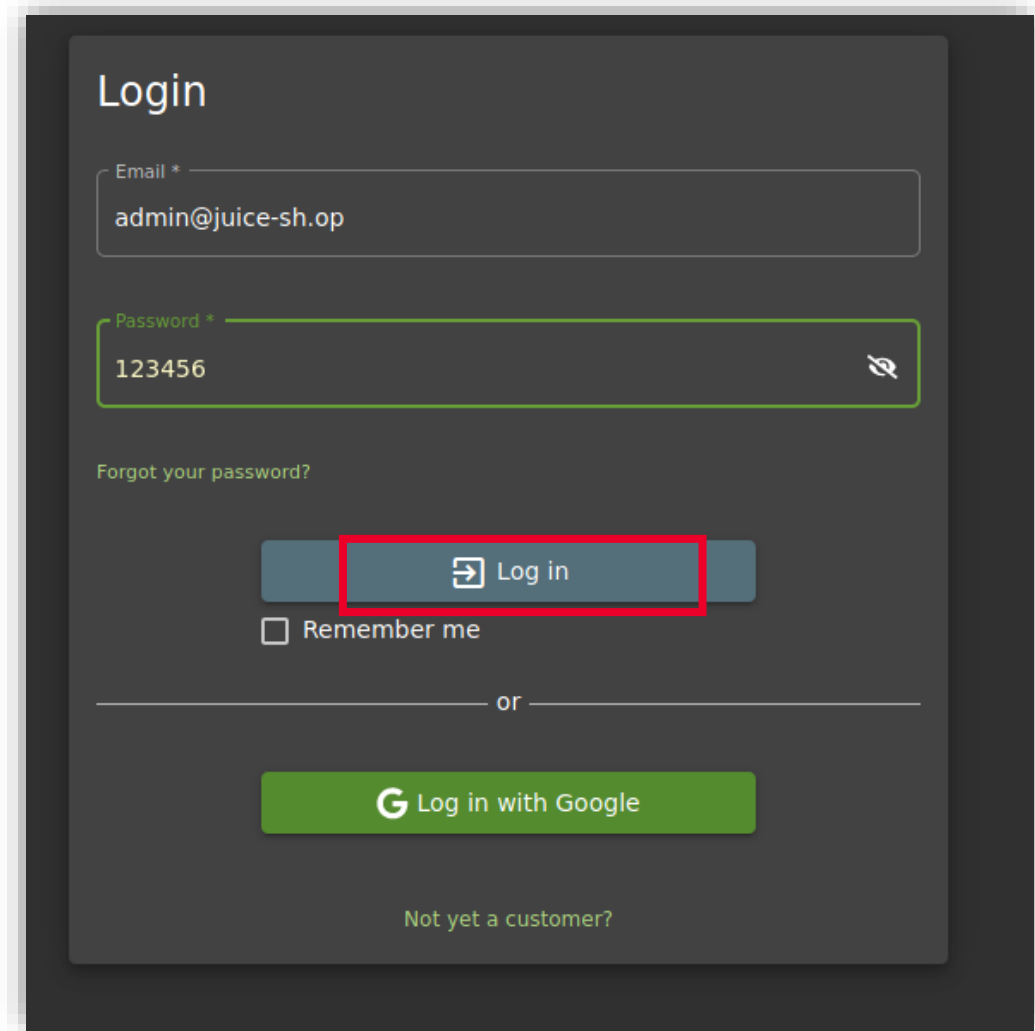


Ilustración 31: Opción BurpSuite antes configurada.

## 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

- Una vez activado, intenta acceder con el usuario mencionado antes (admin@juice-sh.op) poniendo cualquier contraseña aleatoria.



Login

Email \*

admin@juice-sh.op

Password \*

123456

Forgot your password?

Log in

☐ Remember me

or

Log in with Google

Not yet a customer?

Ilustración 32: *Login* con el usuario admin@juice-sh.op y una contraseña aleatoria.

## 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

- Cuando pulses la opción «Log in», se abrirá la ventana emergente de BurpSuite con la petición de *log in* que acabas de lanzar.

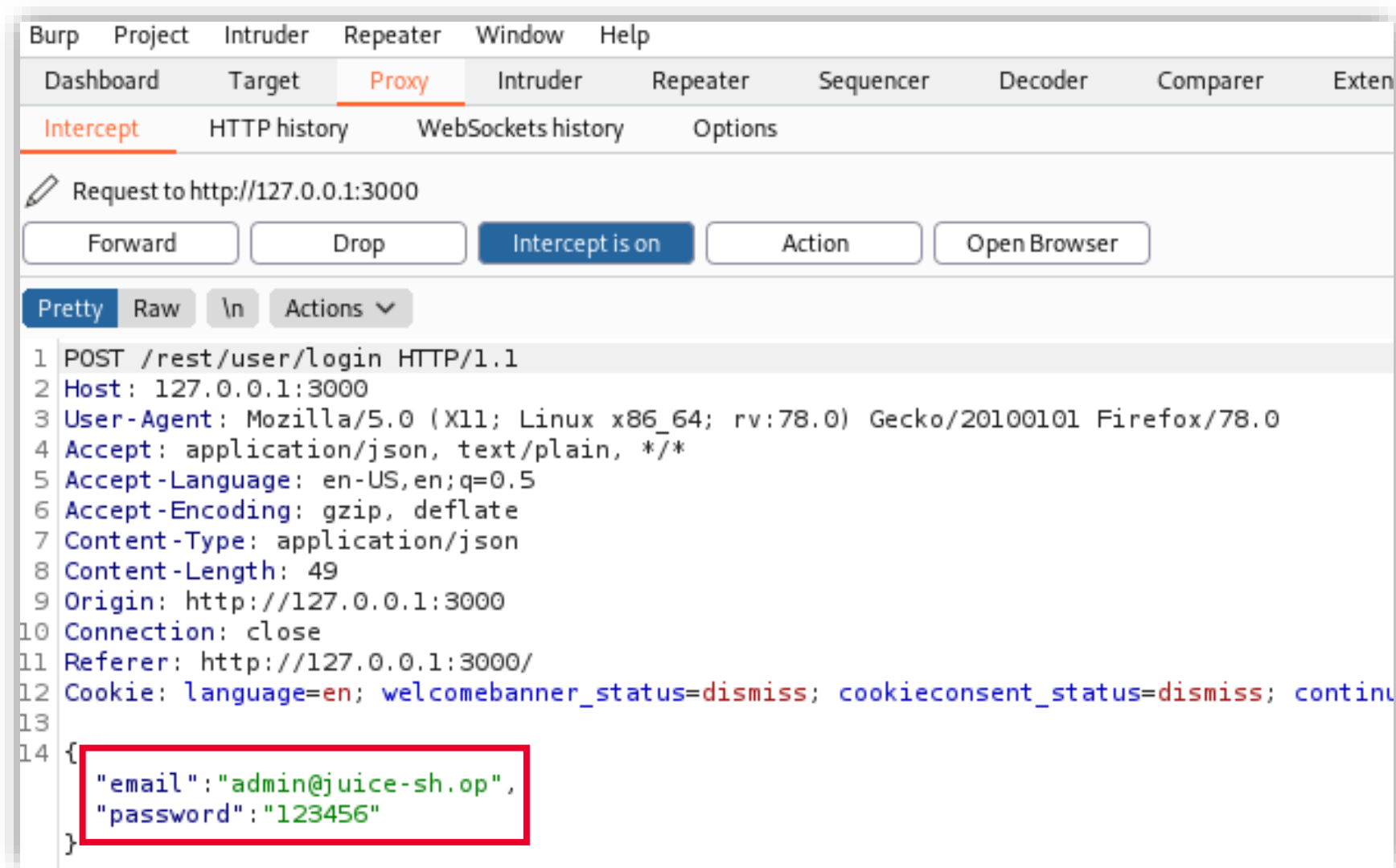


Ilustración 33: Ventana emergente de BurpSuite con la petición de *log in*.

# 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

- La petición ha sido interceptada por BurpSuite y en esta aparecen datos sensibles, como el usuario y contraseña que has probado anteriormente, lo que se debe a una mala configuración de la página.
- Una vez interceptada esta petición, haz clic derecho sobre esta petición y selecciona la opción «*Send to Intruder*».

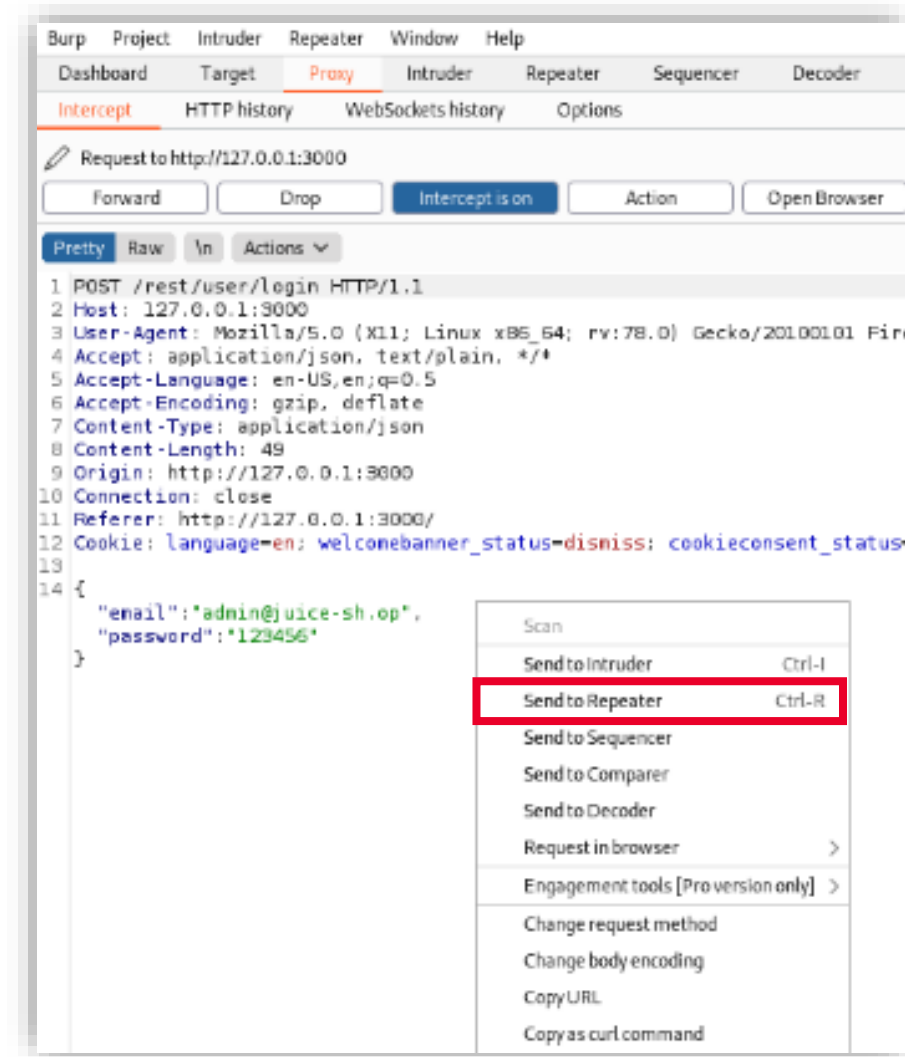


Ilustración 34: Opción «*Send to Intruder*».

# 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

- Dentro del menú «*Intruder*», selecciona el submenú «*Positions*».

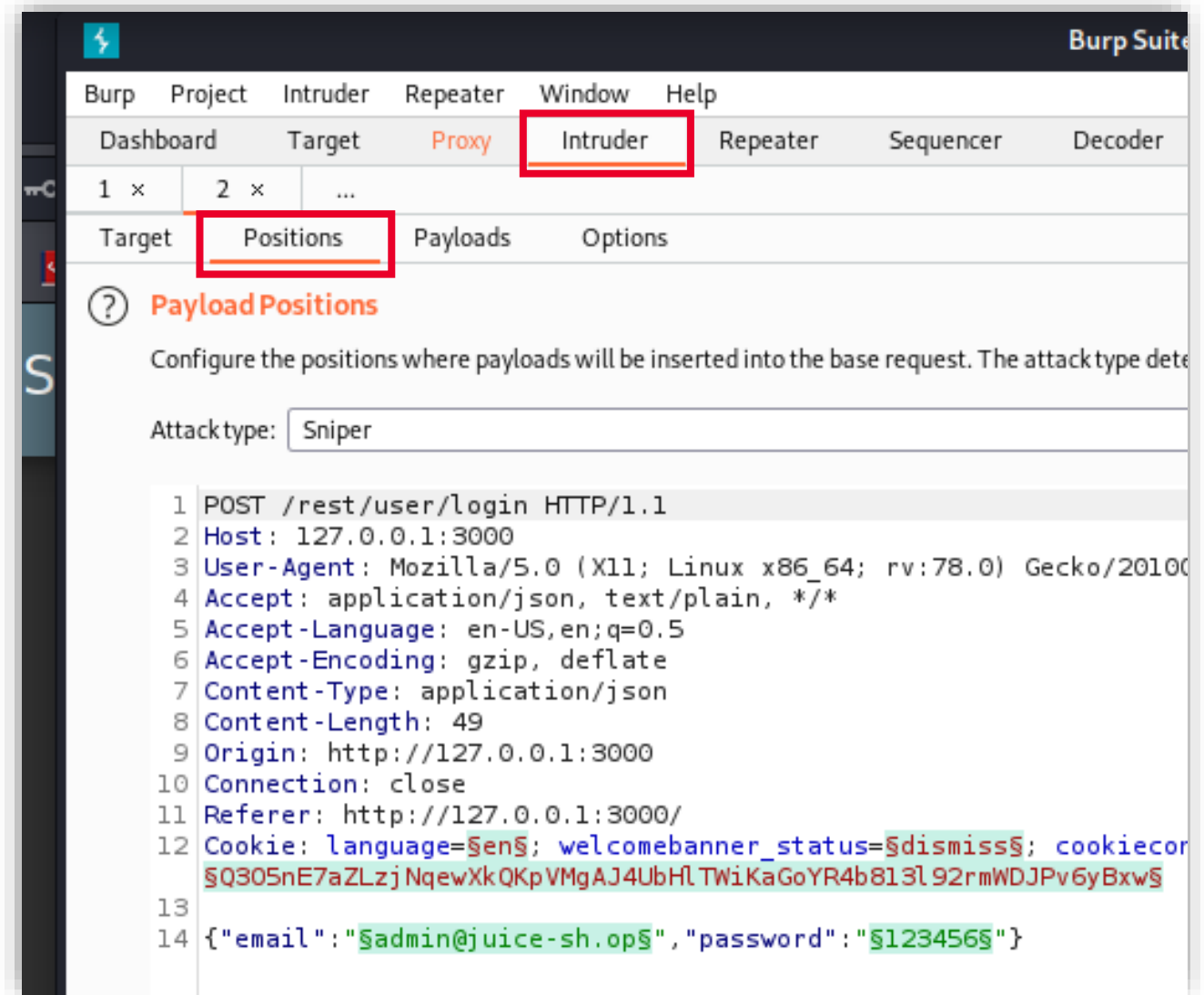


Ilustración 35: Menú «*Intruder*» y submenú «*Positions*».



## 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

- Para llevar a cabo este ataque de fuerza bruta, necesitamos un diccionario de contraseñas. A continuación, crearás tu propio diccionario, aunque existen varios ya creados que también podrías utilizar.
  - Para ello, accede a la terminal Kali y crea un documento denominado **passwords.txt** por medio del comando **nano**.

```
(incibe@kali)-[~]uptime.js is present
$ nano passwords.txtndor.js is present (
(node:73882) [DEP0152] DeprecationWarning:
```

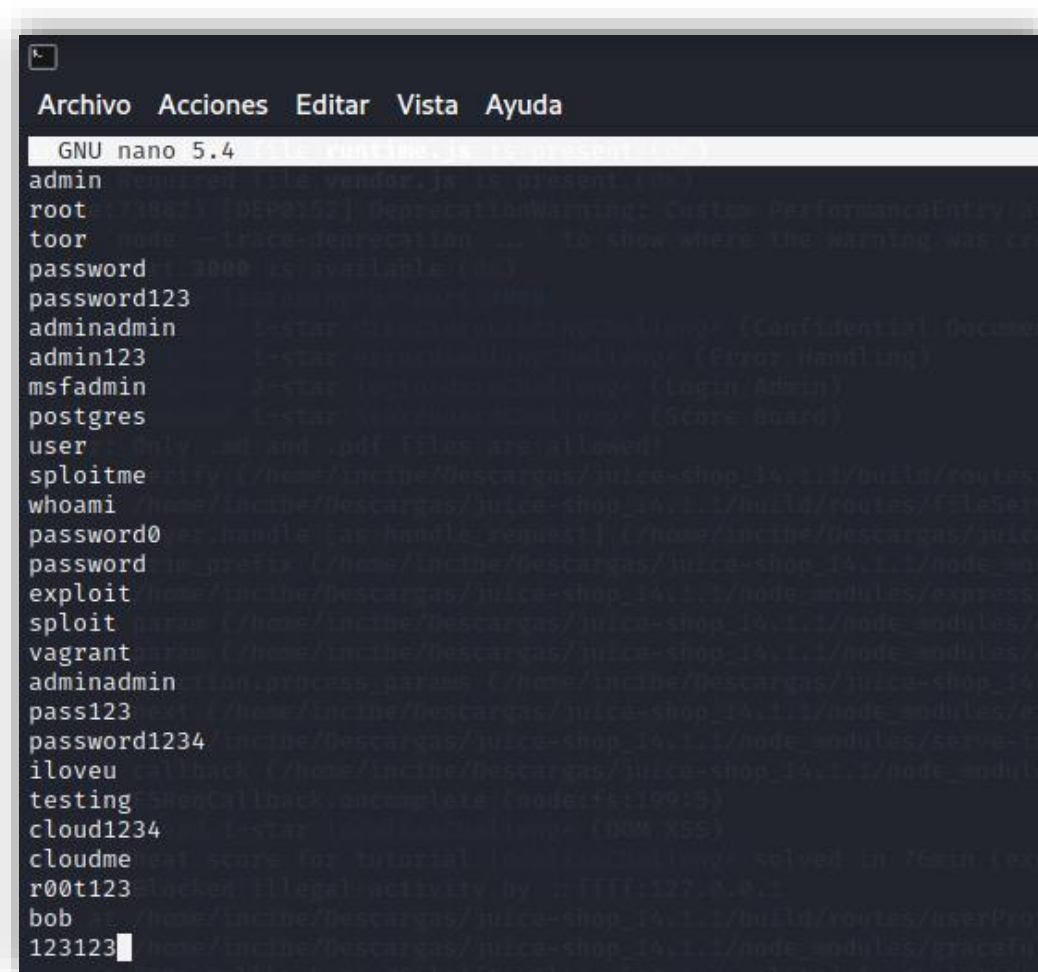
Ilustración 36: Ejecución del comando *nano* para crear el documento passwords.txt.

# 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

- Aparecerá un documento donde copiarás las contraseñas más típicas y dónde podrás incluir las que tú quieras. Por ejemplo, puedes copiar las siguientes:

- |                      |                       |                    |
|----------------------|-----------------------|--------------------|
| ■ <i>admin</i>       | ■ <i>user</i>         | ■ <i>cloud1234</i> |
| ■ <i>root</i>        | ■ <i>sploitme</i>     | ■ <i>r00t123</i>   |
| ■ <i>toor</i>        | ■ <i>whoami</i>       | ■ <i>bob</i>       |
| ■ <i>password</i>    | ■ <i>password0</i>    | ■ <i>123123</i>    |
| ■ <i>password123</i> | ■ <i>vagrant</i>      |                    |
| ■ <i>adminadmin</i>  | ■ <i>pass123</i>      |                    |
| ■ <i>admin123</i>    | ■ <i>password1234</i> |                    |
| ■ <i>msfadmin</i>    | ■ <i>ilovei</i>       |                    |
| ■ <i>postgres</i>    | ■ <i>testing</i>      |                    |

Ilustración 37: Listado de contraseñas típicas.

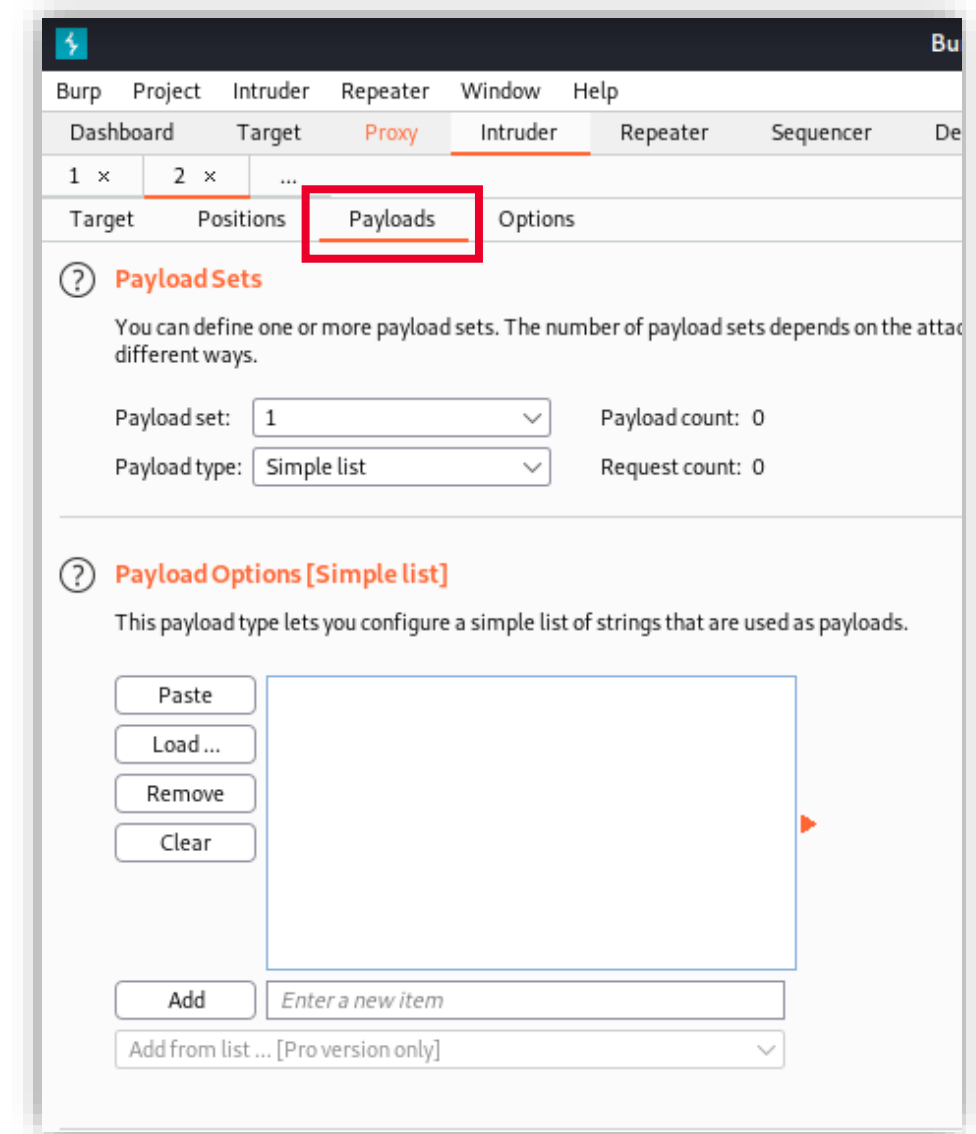


```
GNU nano 5.4 file runtime.txt is present (1/1)
admin
root
toor
password
adminadmin
admin123
msfadmin
postgres
user
sploitme
whoami
password0
password
exploit
sploit
vagrant
adminadmin
pass123
password1234
iloveu
testing
cloud1234
cloudme
r00t123
bob
123123
```

# 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

- Para guardar este documento deberás pulsar «Control + O» y después «Control + X» para salir de este documento.
- Una vez guardado, este diccionario lo podrás utilizar en BurpSuite para intentar conseguir la contraseña de este usuario.
  - Para ello, accede a la herramienta BurpSuite y haz clic el submenú «Payloads».

Ilustración 38:  
Submenú *Payloads*.



## 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

---

- En este menú es donde vas a utilizar tu diccionario creado anteriormente.
  - En «*Payload Options*», haz clic en la opción «*Load*».
- En la ventana emergente, podrás encontrar el diccionario que has creado anteriormente. Selecciónalo y pulsa «Abrir» para cargarlo.

# 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

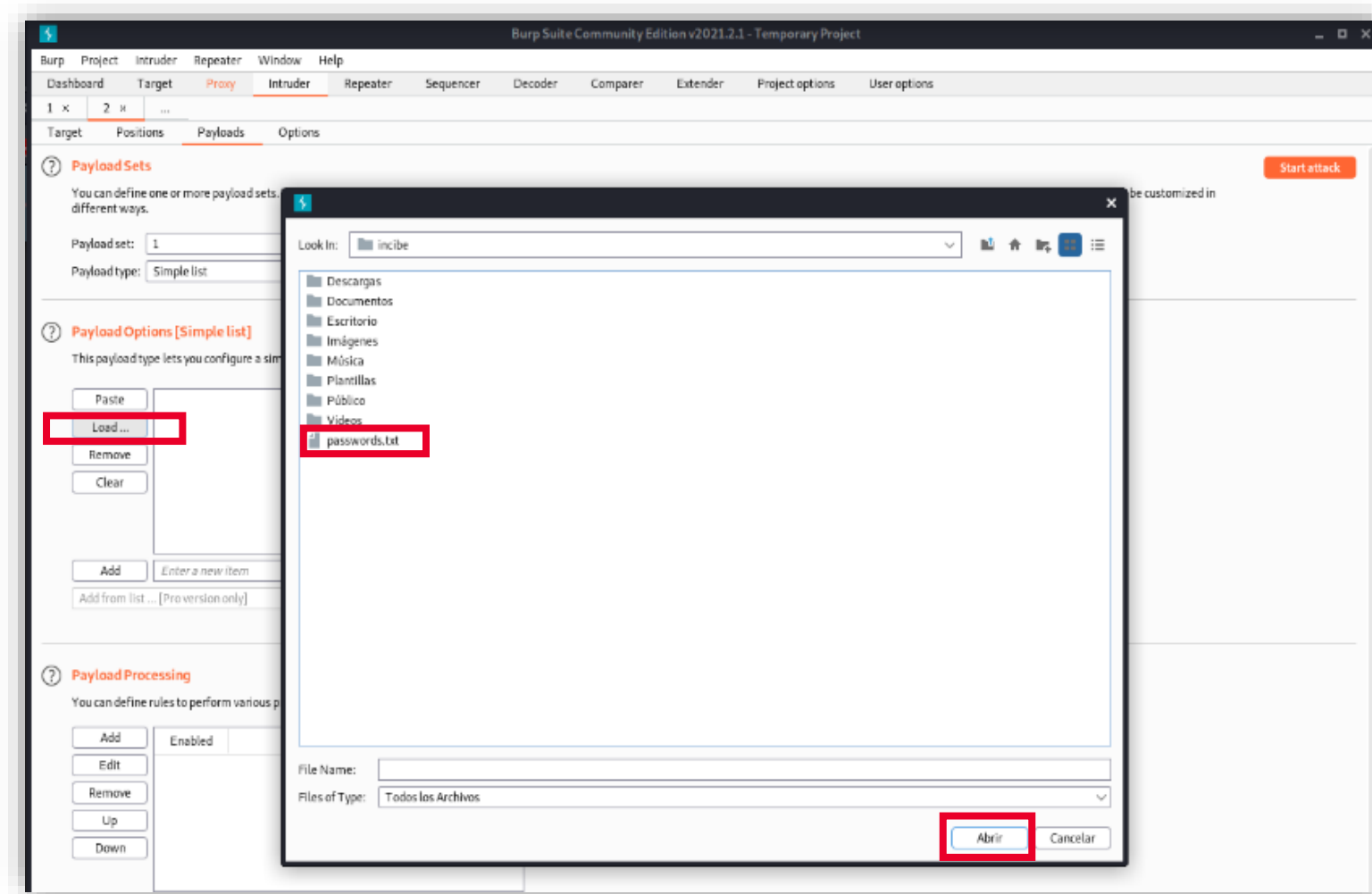


Ilustración 39: Ubicación del diccionario creado.

## 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

- Una vez cargado, haz clic en la opción «*Start attack*» y empezará a realizar el ataque de fuerza bruta.

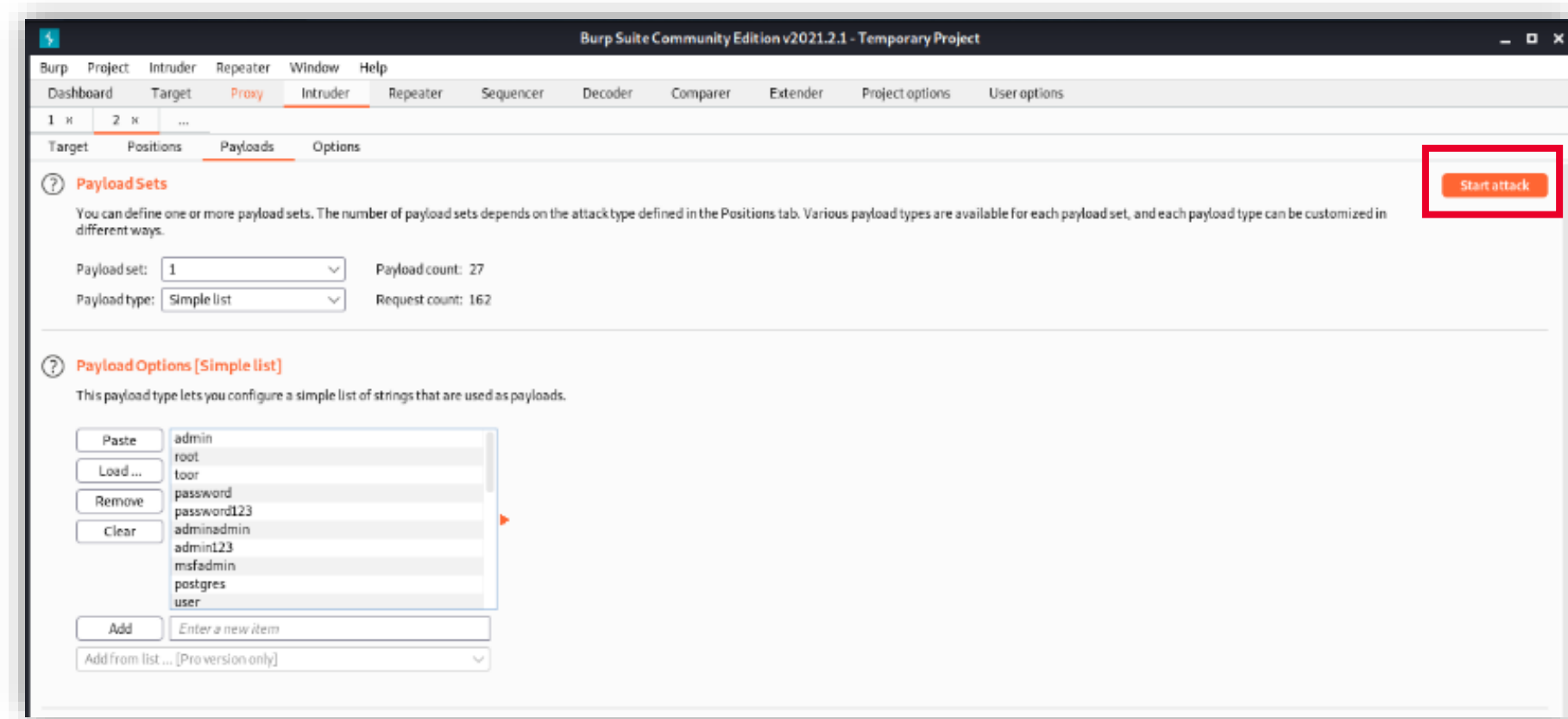


Ilustración 40: Botón «*Start attack*» .

# 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

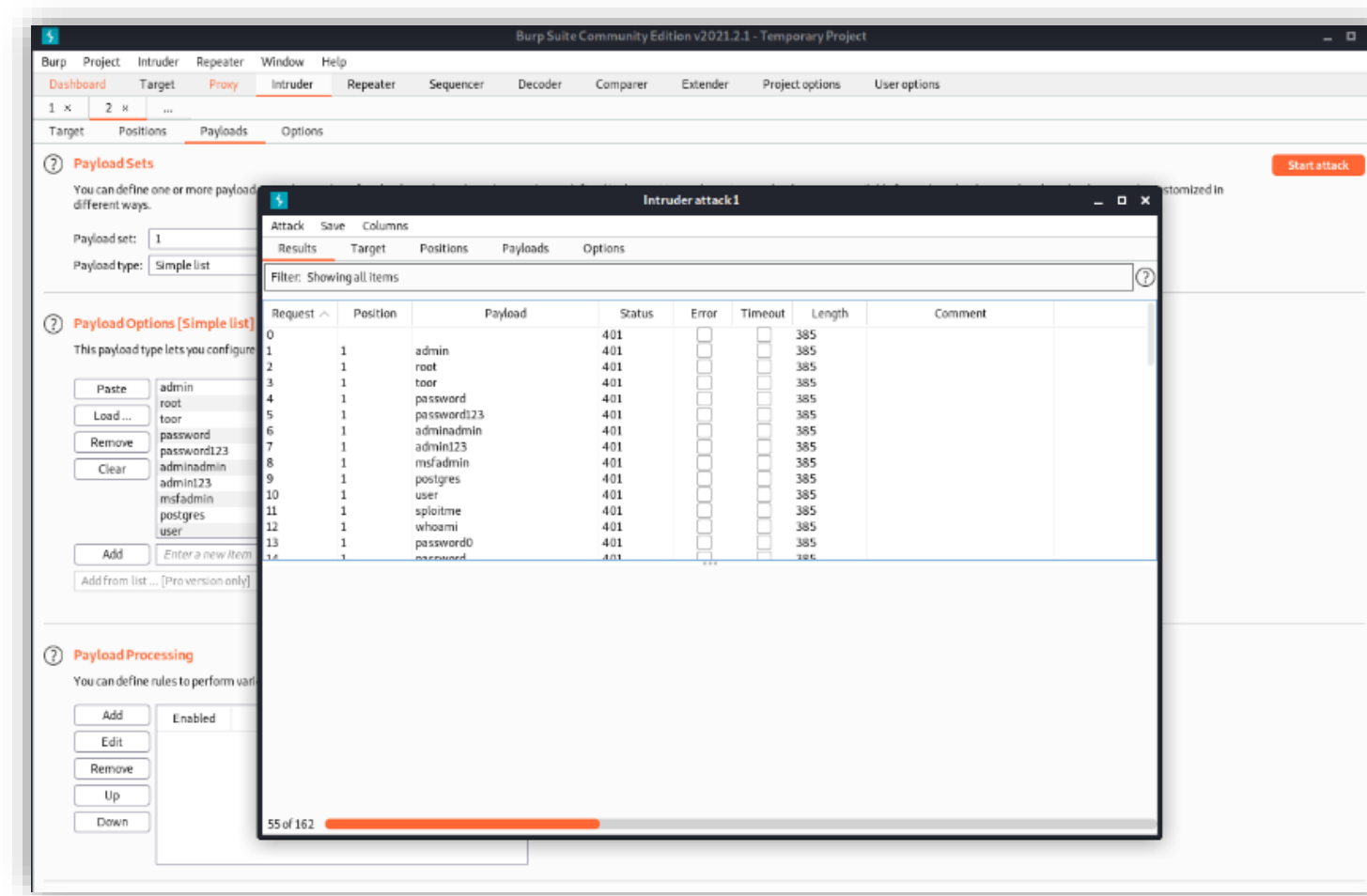


Ilustración 41: Inicio del ataque.

## 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

- Cuando haya terminado el ataque, verás que ha encontrado la contraseña del usuario, ya que reporta como *Status* un código 200, que quiere decir que la solicitud ha tenido éxito.

142	6	admin123	200	<input type="checkbox"/>	<input type="checkbox"/>	1180
...						

Ilustración 42: *Status* con código 200.



## 6 VULNERABILIDAD FALLO DE AUTENTICACIÓN E IDENTIFICACIÓN

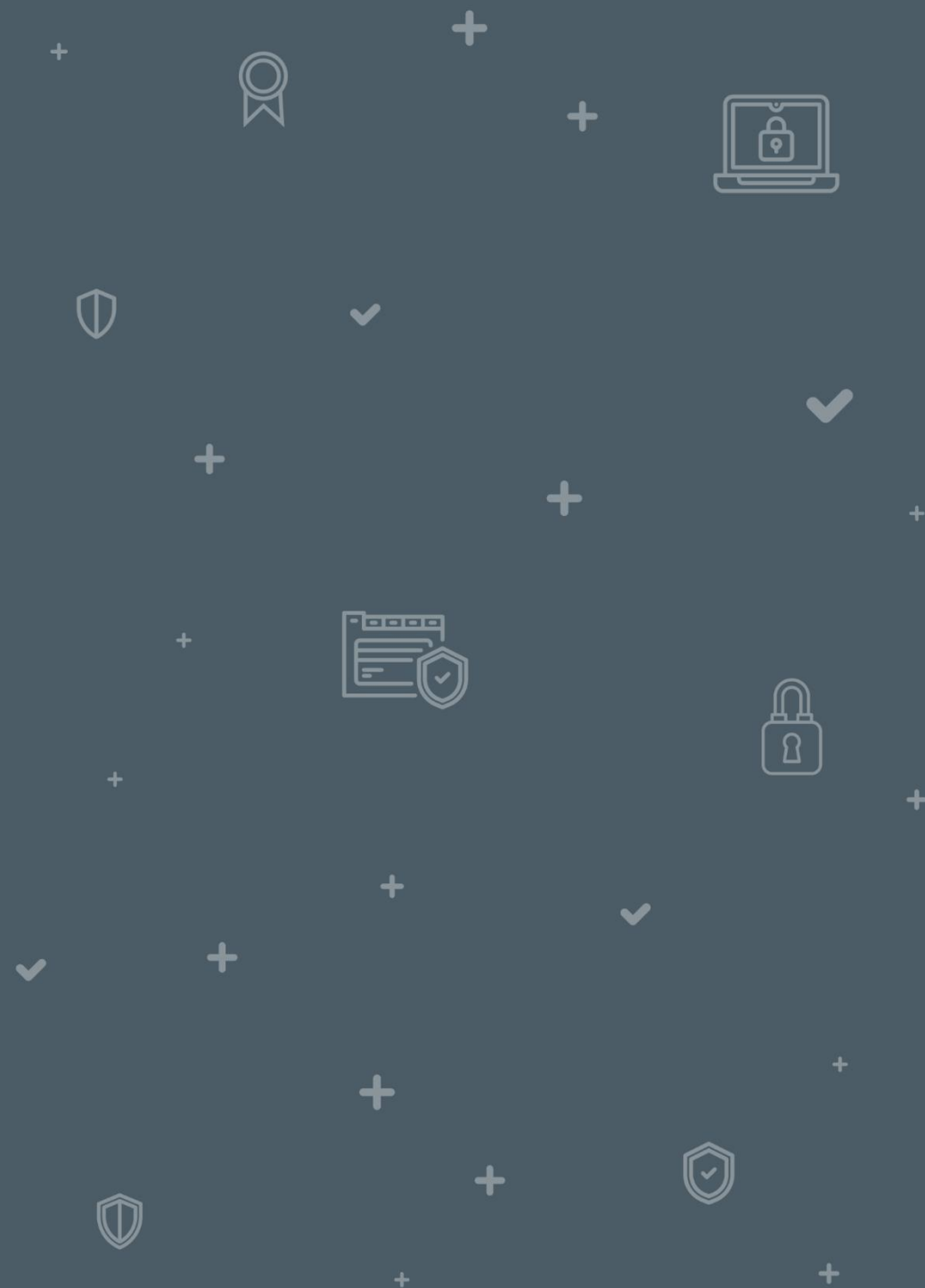
- Ahora sabes que la contraseña de este usuario es admin123, con lo que ya puedes acceder suplantándole, con el agravante de que este usuario tiene permisos de administrador.

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

Ilustración 43: Ataque realizado con éxito.

# 7

## ENUNCIADO EJERCICIO PRÁCTICO 2



## ENUNCIADO EJERCICIO PRÁCTICO 2

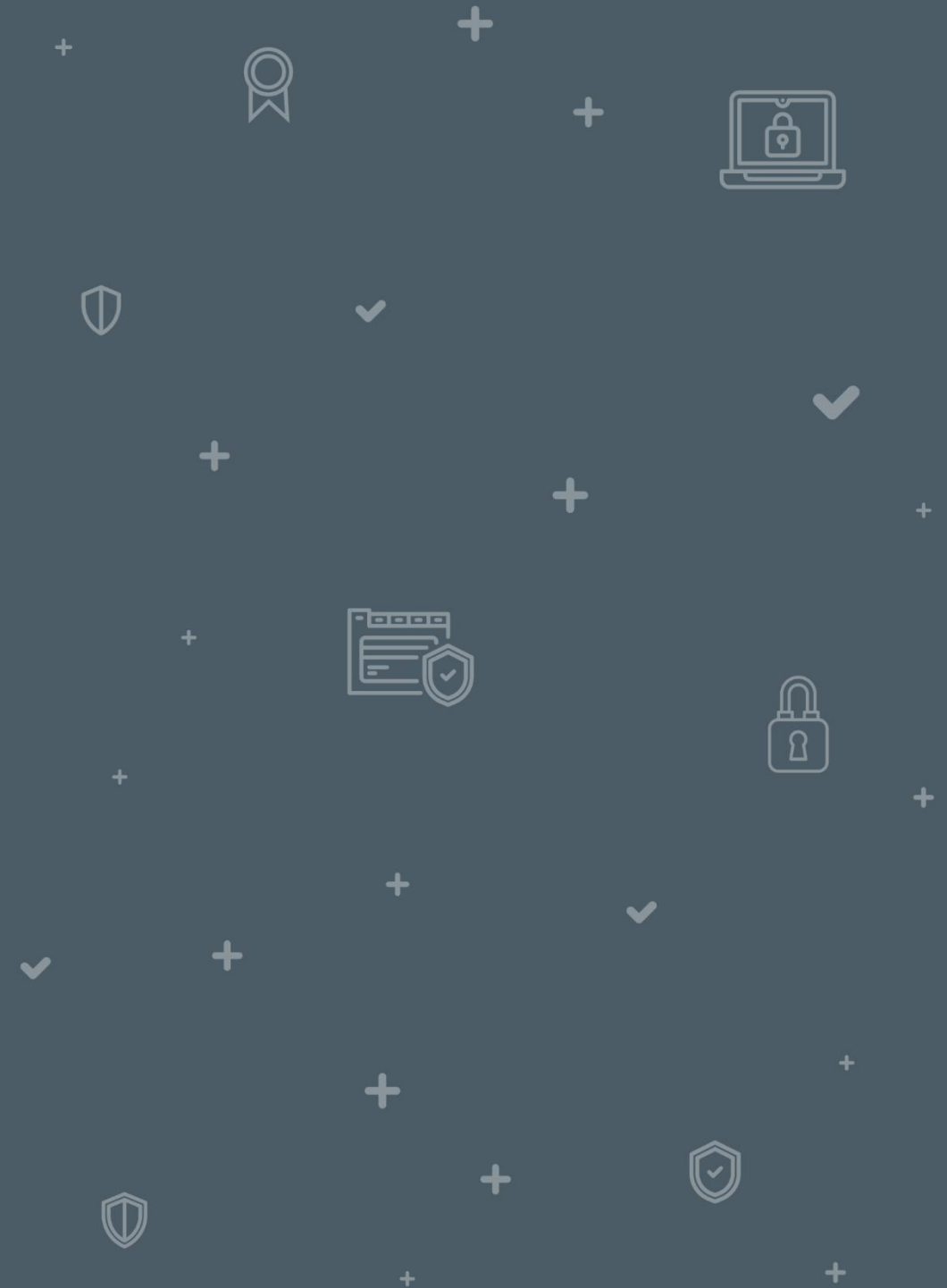
---



¿Existe otra manera de registrarte sin disponer de los datos anteriores?

# 8

## SOLUCIONARIO EJERCICIO PRÁCTICO 2

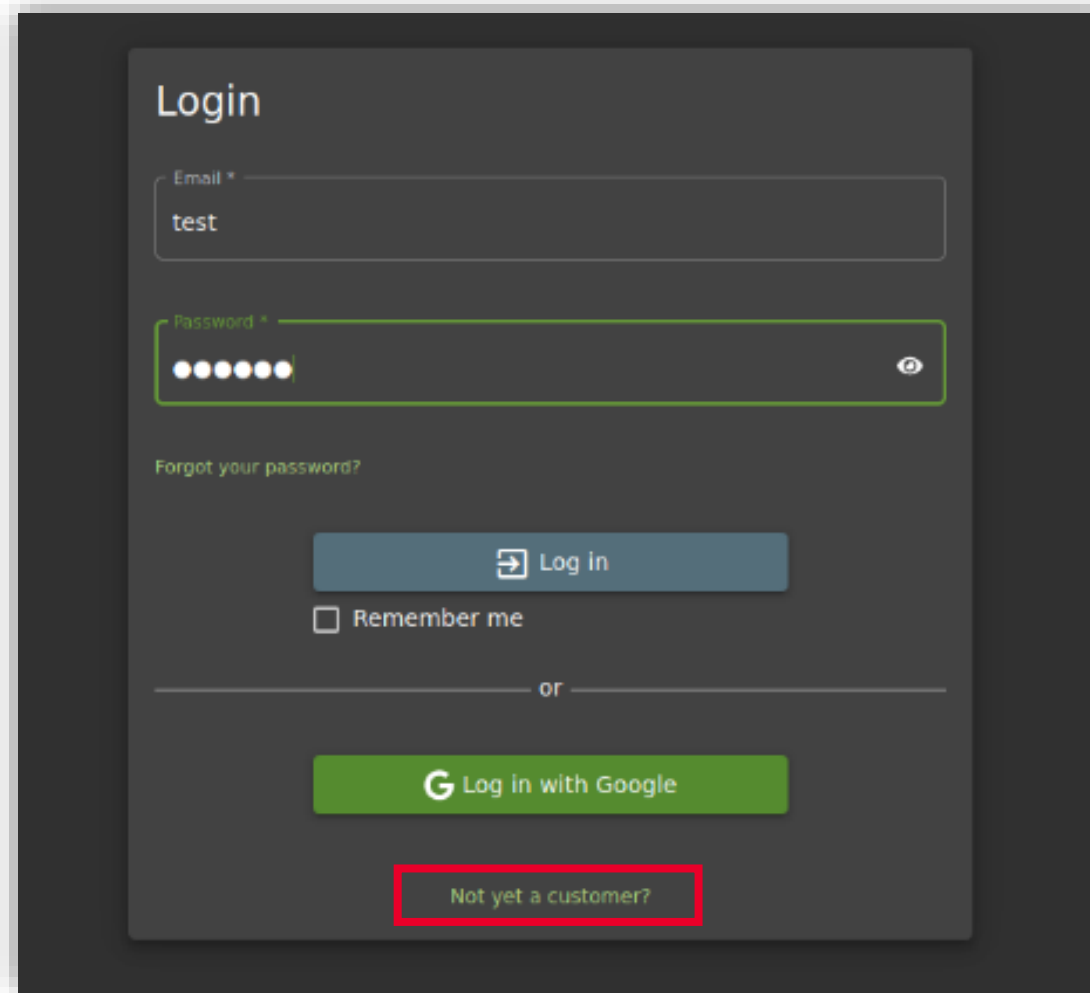


## 8 SOLUCIONARIO EJERCICIO PRÁCTICO 2

---

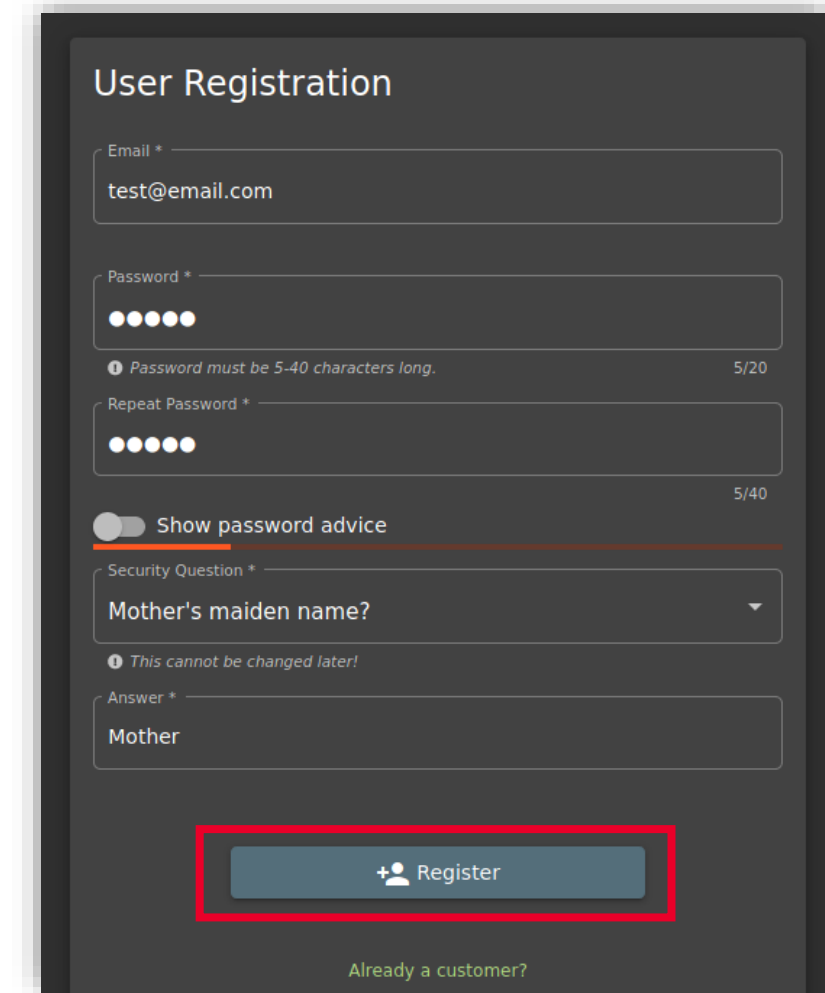
- Existen varias maneras de acceder como administrador, te explicaremos otra.
- Accede a la página de *Log In*. Una vez allí, activa el *proxy* y abre BurpSuite. De esta forma, las peticiones no llegan de forma directa a la página web, sino que pasan primero por el *proxy*, y en caso de que se quiera enviar alguna información al navegador, se deberá realizar desde el *proxy*. Esto permite la posibilidad de modificar y alterar las peticiones desde el *proxy* antes de que se envíen.
  - En la página de *Log In* esta vez haz clic a *Not yet a costumer* y pondrás cualquier usuario y contraseña, con una pregunta de seguridad aleatoria y cualquier respuesta. Pulsa en *Register*.

## 8 SOLUCIONARIO EJERCICIO PRÁCTICO 2



The image shows a login page with a dark background. At the top, the word "Login" is displayed. Below it, there are two input fields: "Email \*" containing the text "test" and "Password \*" containing six dots. A green border highlights the password field. Below the password field is a link that says "Forgot your password?". There is a blue "Log in" button with a right-pointing arrow icon. Below the button is a checkbox labeled "Remember me". A horizontal line with the word "or" in the center separates the login section from the registration section. Below the line is a green button with the Google "G" logo and the text "Log in with Google". At the bottom, there is a red-bordered box containing the text "Not yet a customer?".

Ilustración 44: Página de Log In y ubicación de Not yet a customer?



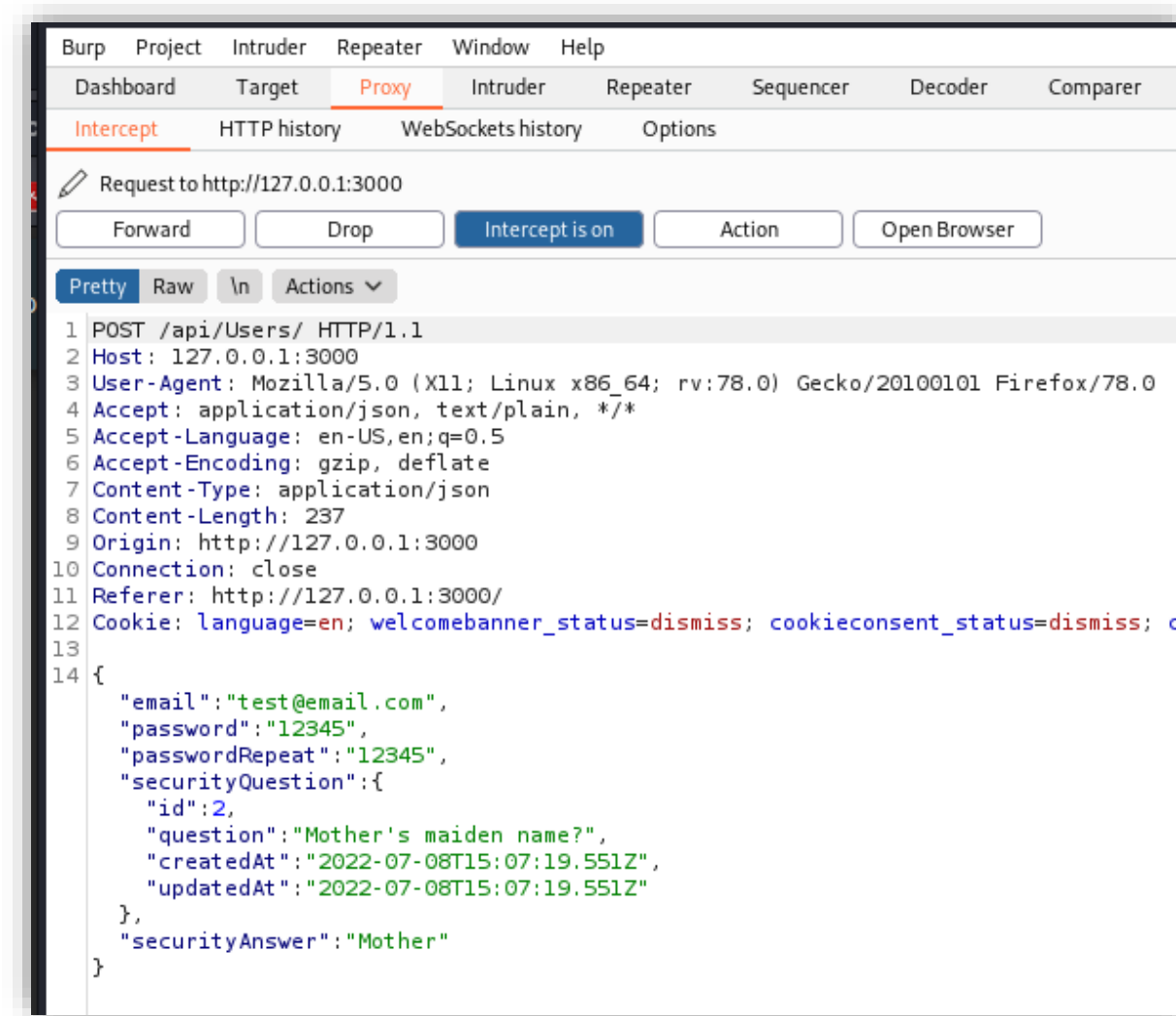
The image shows a user registration page with a dark background. At the top, the text "User Registration" is displayed. Below it are several input fields: "Email \*" containing "test@email.com", "Password \*" containing six dots with a note "Password must be 5-40 characters long." and a character count "5/20", and "Repeat Password \*" containing six dots with a character count "5/40". There is a toggle switch labeled "Show password advice". Below this is a "Security Question \*" dropdown menu with the selected option "Mother's maiden name?" and a note "This cannot be changed later!". Below the dropdown is an "Answer \*" field containing the text "Mother". At the bottom, there is a red-bordered box containing a blue button with a plus icon and the text "Register". Below the button is the text "Already a customer?".

Ilustración 45: Campos de registro de nuevo usuario.

## 8 SOLUCIONARIO EJERCICIO PRÁCTICO 2

- Cuando BurpSuite haya interceptado la petición verás que, como antes, muestra los datos que has utilizado.

Ilustración 46: Datos referentes a la petición de registro de nuevo usuario.



```
1 POST /api/Users/ HTTP/1.1
2 Host: 127.0.0.1:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Content-Length: 237
9 Origin: http://127.0.0.1:3000
10 Connection: close
11 Referer: http://127.0.0.1:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; cc
13
14 {
  "email": "test@email.com",
  "password": "12345",
  "passwordRepeat": "12345",
  "securityQuestion": {
    "id": 2,
    "question": "Mother's maiden name?",
    "createdAt": "2022-07-08T15:07:19.551Z",
    "updatedAt": "2022-07-08T15:07:19.551Z"
  },
  "securityAnswer": "Mother"
}
```

## 8 SOLUCIONARIO EJERCICIO PRÁCTICO 2

- Ahora enviarás esta petición dentro de BurpSuite en el menú *Repeater*. Para ello, haz doble clic sobre la petición y selecciona *Send to Repeater*.

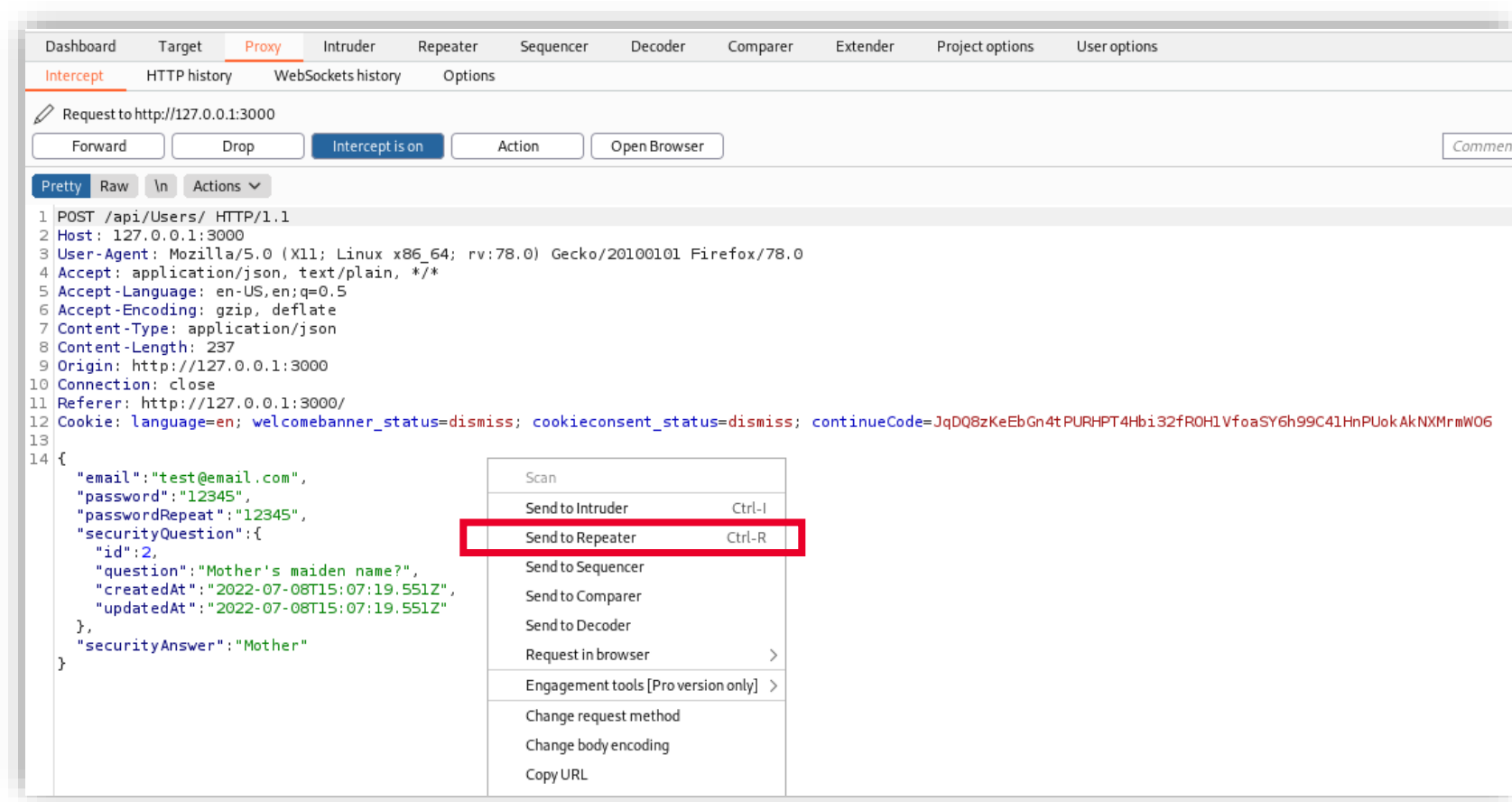


Ilustración 47: Opción *Sent to Repeater*.



## 8 SOLUCIONARIO EJERCICIO PRÁCTICO 2

---

- Una vez enviada la petición, vuelve al menú y modifica esta petición.
  - El primer campo que vas a cambiar es el de correo electrónico, en que el pondrás *admin*.
  - Añade también una coma al final de *securityAnswer*.
  - Pulsa *Enter* para añadir otra línea.
  - Escribe *username:admin*.
  - Añade otra coma y pulsa *Enter* para añadir otra línea.
  - Escribe *role:admin*.
- Ahora ya has creado un usuario administrador con todos los permisos de este.

## 8 SOLUCIONARIO EJERCICIO PRÁCTICO 2

Request

Pretty Raw \n Actions ▾

```
1 POST /api/Users/ HTTP/1.1
2 Host: 127.0.0.1:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Content-Length: 237
9 Origin: http://127.0.0.1:3000
10 Connection: close
11 Referer: http://127.0.0.1:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent
13
14 {
15   "email": "admin",
16   "password": "12345",
17   "passwordRepeat": "12345",
18   "securityQuestion": {
19     "id": 2,
20     "question": "Mother's maiden name?",
21     "createdAt": "2022-07-08T15:07:19.551Z",
22     "updatedAt": "2022-07-08T15:07:19.551Z"
23   },
24   "securityAnswer": "Mother",
25   "username": "admin",
26   "role": "admin"
27 }
```

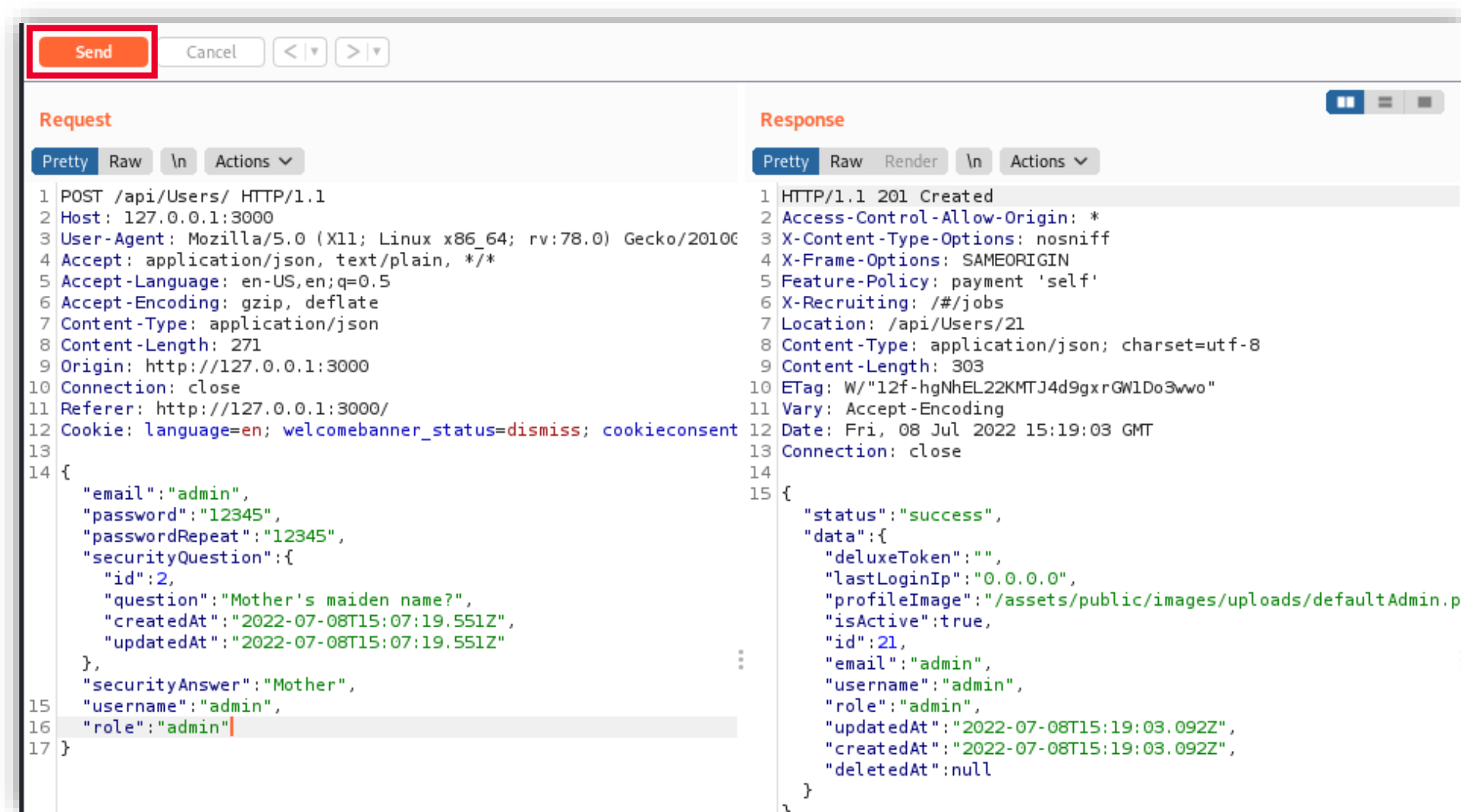
Ilustración 48: Campos a cumplimentar.

## 8 SOLUCIONARIO EJERCICIO PRÁCTICO 2

---

- Como podemos ver en la imagen de la diapositiva anterior, en el campo email nos aparece únicamente la palabra «*admin*» y no sigue el formato típico de «texto@dominio», porque el servidor no realiza este tipo de comprobaciones. En una programación segura sí se comprueba que la información facilitada sigue un formato concreto además de una longitud fija; sin embargo, como esta aplicación está desarrollada para ser vulnerable y realizar pruebas, no se realizan estas comprobaciones y por tanto, no es preciso que el email siga el formato estándar de los correos electrónicos.
- Una vez añadido todos estos campos, haz clic en *Send* y aparecerá una respuesta positiva.

## 8 SOLUCIONARIO EJERCICIO PRÁCTICO 2



## 8 SOLUCIONARIO EJERCICIO PRÁCTICO 2

---

- Al volver a la página de inicio de Juice Shop, observarás que has conseguido otro logro.

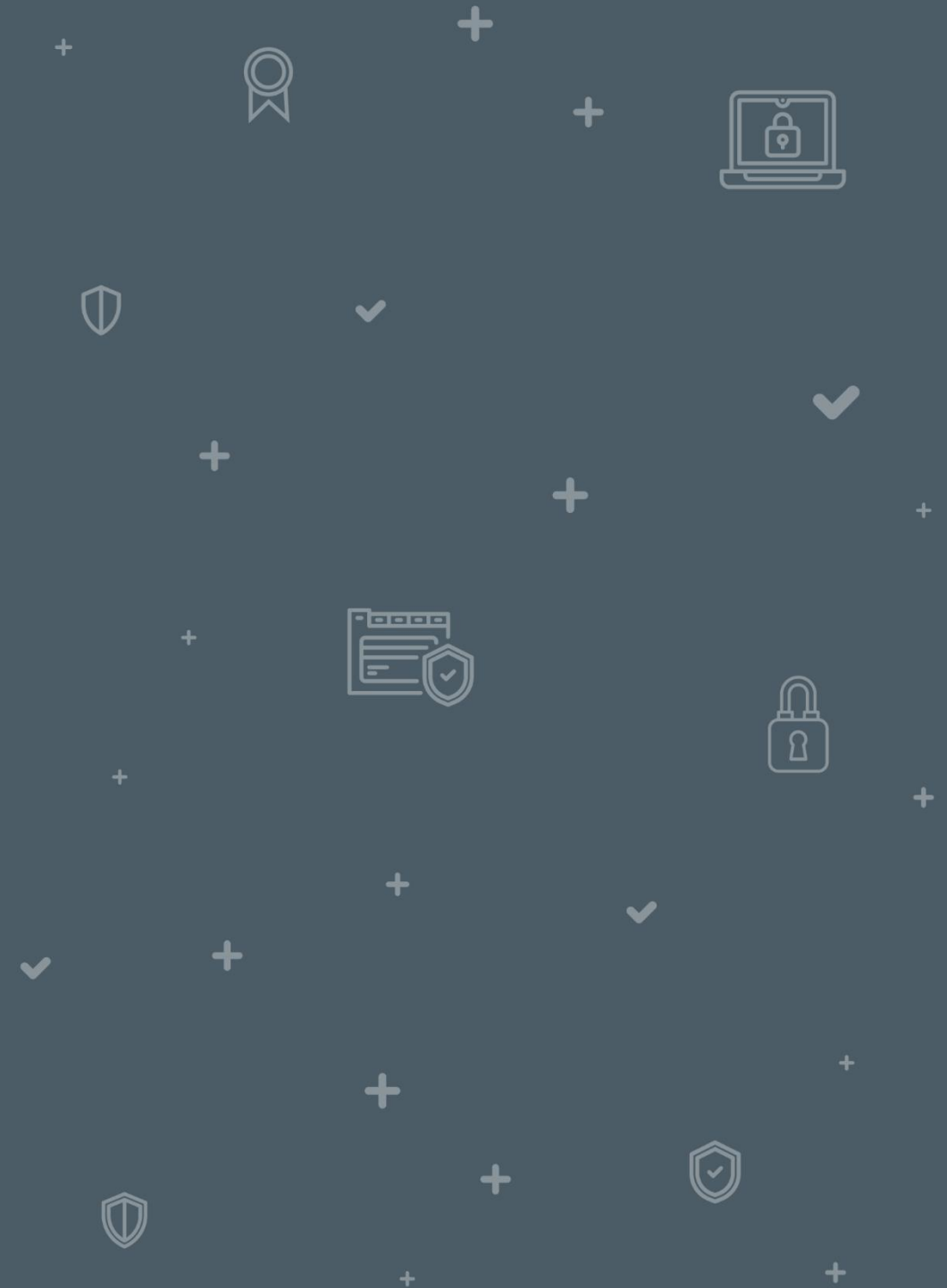
You successfully solved a challenge: Admin Registration (Register as a user with administrator privileges.)

Ilustración 50: Acción realizada con éxito.

- Ya puedes iniciar sesión con el usuario que has creado anteriormente.

# 9

## VULNERABILIDAD INYECCIÓN XSS



## 9 VULNERABILIDAD INYECCIÓN XSS

---

Las inyecciones más comunes son las inyecciones SQL y NoSQL, la inyección de comandos, inyección LDAP y Cross-Site Scripting (XSS). Este tipo de ataques pueden ocurrir cuando:

- Los datos suministrados por el usuario no son validados, filtrados o saneados por la aplicación.
- Las consultas dinámicas o las llamadas no parametrizadas sin escape de contexto se utilizan directamente en la base de datos. Una consulta dinámica es una consulta que se genera de forma dinámica –en ese momento- cuando se quiere ejecutar, en contraposición de las consultas estáticas, que ya están elaboradas de antemano y no es posible modificarlas. Las consultas o llamadas no parametrizadas hacen referencia al uso de cadenas de texto concatenadas, es decir, unidas, donde se une el valor de la variable como cadena.
- Los datos se utilizan dentro de los parámetros de búsqueda del mapeo objeto-relacional (ORM) para extraer registros adicionales y sensibles. El mapeo objeto-relacional consiste en una técnica de programación que permite convertir datos del sistema utilizados por los lenguajes de programación orientado a objetos al que se utiliza por las bases de datos relacionales.

## 9 VULNERABILIDAD INYECCIÓN XSS

---

Para realizar estas inyecciones debes tener en cuenta cómo está creada la página web, es decir, que tipo de lenguaje de programación utiliza y que tipo de base de datos usa.

En este caso, utiliza un lenguaje de programación JavaScript y tiene una base de datos SQL, por lo que basarás las inyecciones en estos datos.

Ahora vas a probar una inyección XSS, que permite a los atacantes colocar secuencias de comandos maliciosas en páginas web aprovechándose de malas prácticas en el código de la página web y así conseguir información confidencial o escalar privilegios.



## 9 VULNERABILIDAD INYECCIÓN XSS

- Para poder realizar esta inyección, trata de encontrar zonas de una página web donde un valor que introduzcas aparezca reflejado, es decir, que dé una respuesta. En este caso, utilizarás el campo de búsqueda.

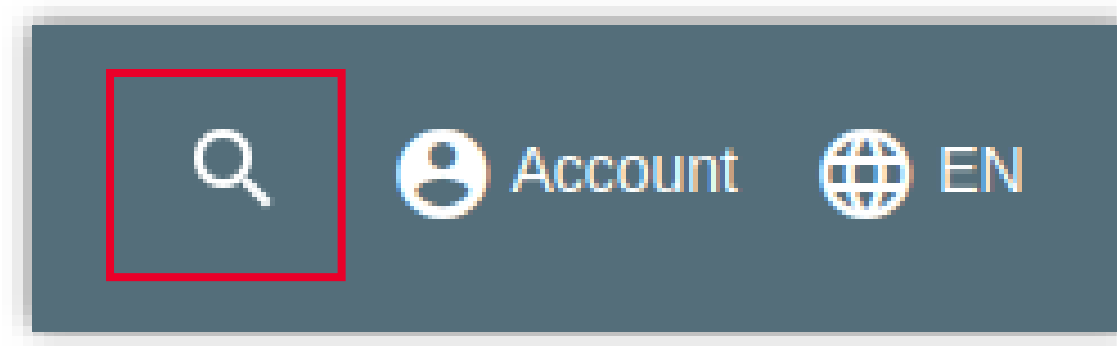


Ilustración 51: Campo de búsqueda.

## 9 VULNERABILIDAD INYECCIÓN XSS

- En este campo escribimos el siguiente texto: `<iframe src="javascript:alert(`xss`)">`

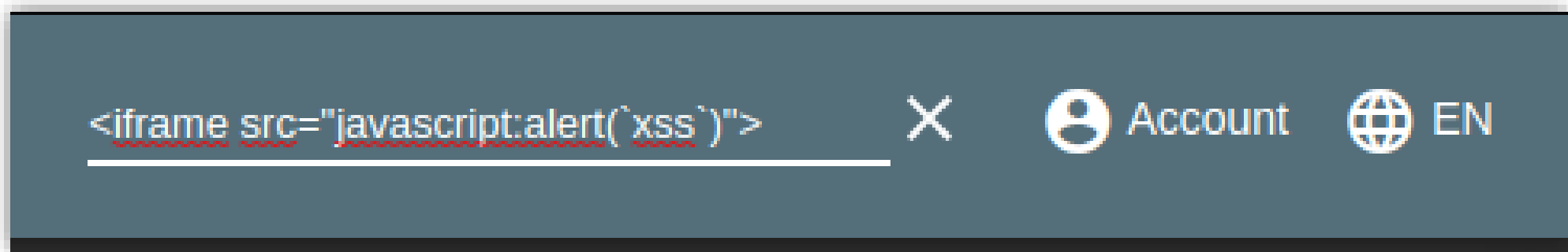


Ilustración 52: Inyección: `<iframe src="javascript:alert(`xss`)">`

## 9 VULNERABILIDAD INYECCIÓN XSS

---

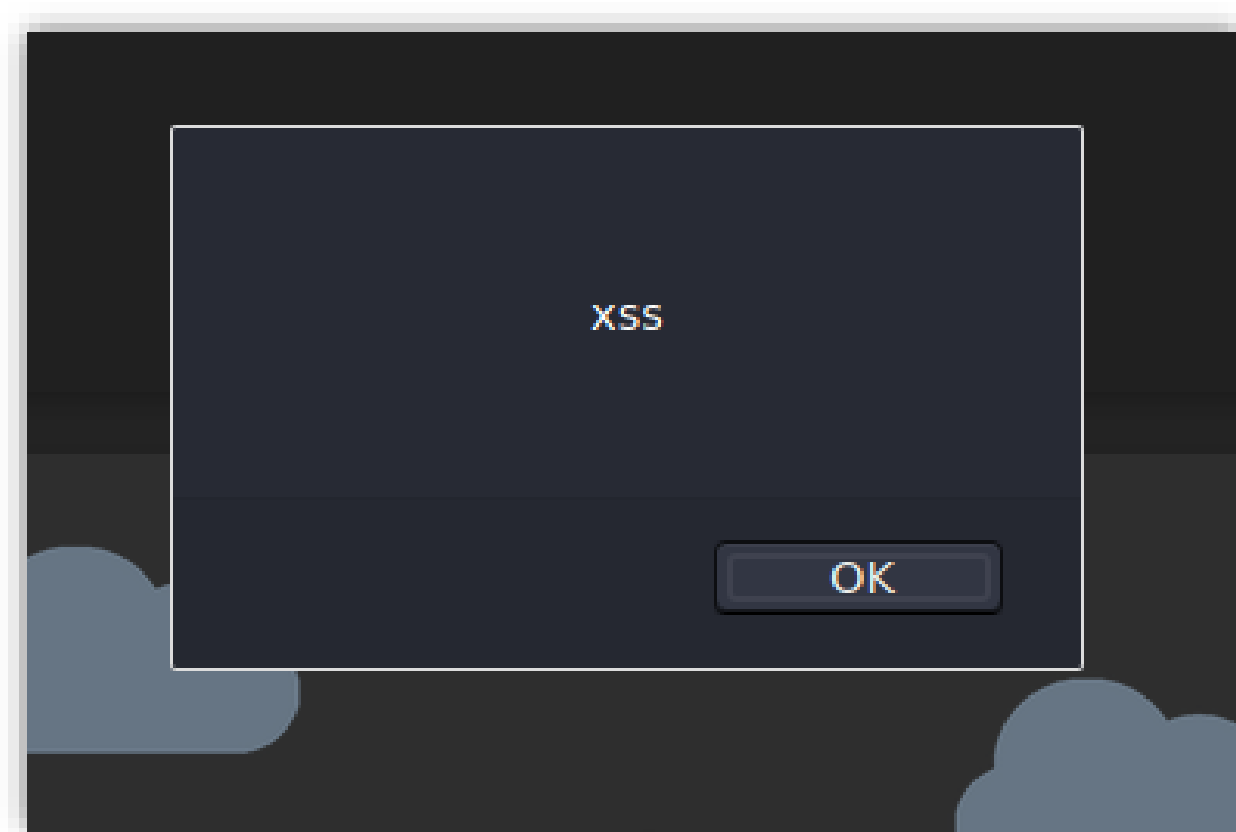


Ilustración 53: Inyección XSS.

## 9 VULNERABILIDAD INYECCIÓN XSS

- Este código provocaría que se ejecute la función **alert()** de JavaScript que hace que el navegador muestre un *pop-up* o ventana emergente con el texto indicado dentro del paréntesis de *alert*, en nuestro caso «XSS».

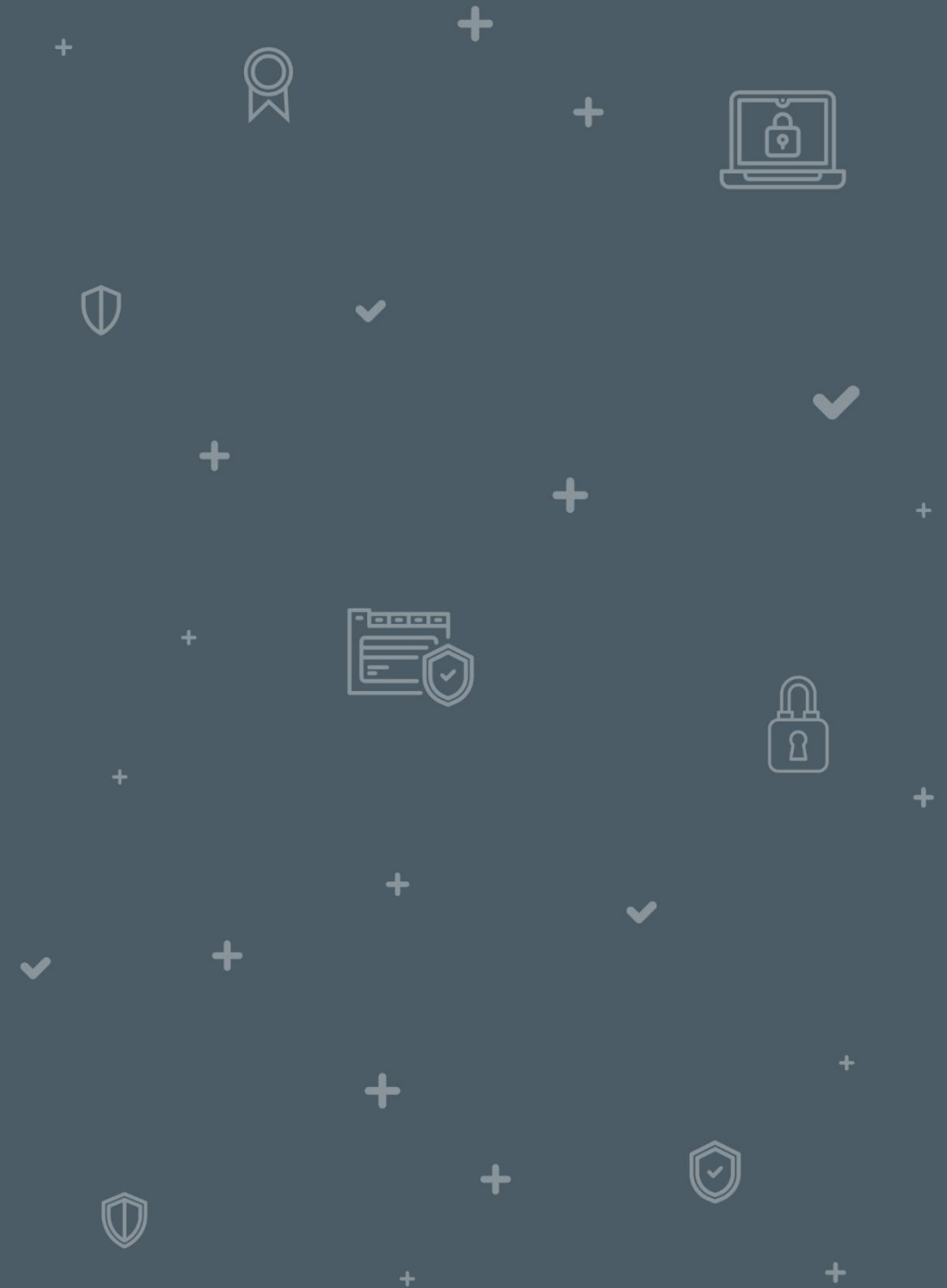
A screenshot of a challenge completion message. The message is displayed in a green rectangular box with a dark border. The text inside the box is: "You successfully solved a challenge: DOM XSS (Perform a DOM XSS attack with <iframe src='javascript:alert(`xss`)>'.)"

You successfully solved a challenge: DOM XSS (Perform a DOM XSS attack with <iframe src="javascript:alert(`xss`)>'.)

Ilustración 54: Ataque realizado con éxito.

# 10

## ENUNCIADO EJERCICIO PRÁCTICO 3



## ENUNCIADO EJERCICIO PRÁCTICO 3

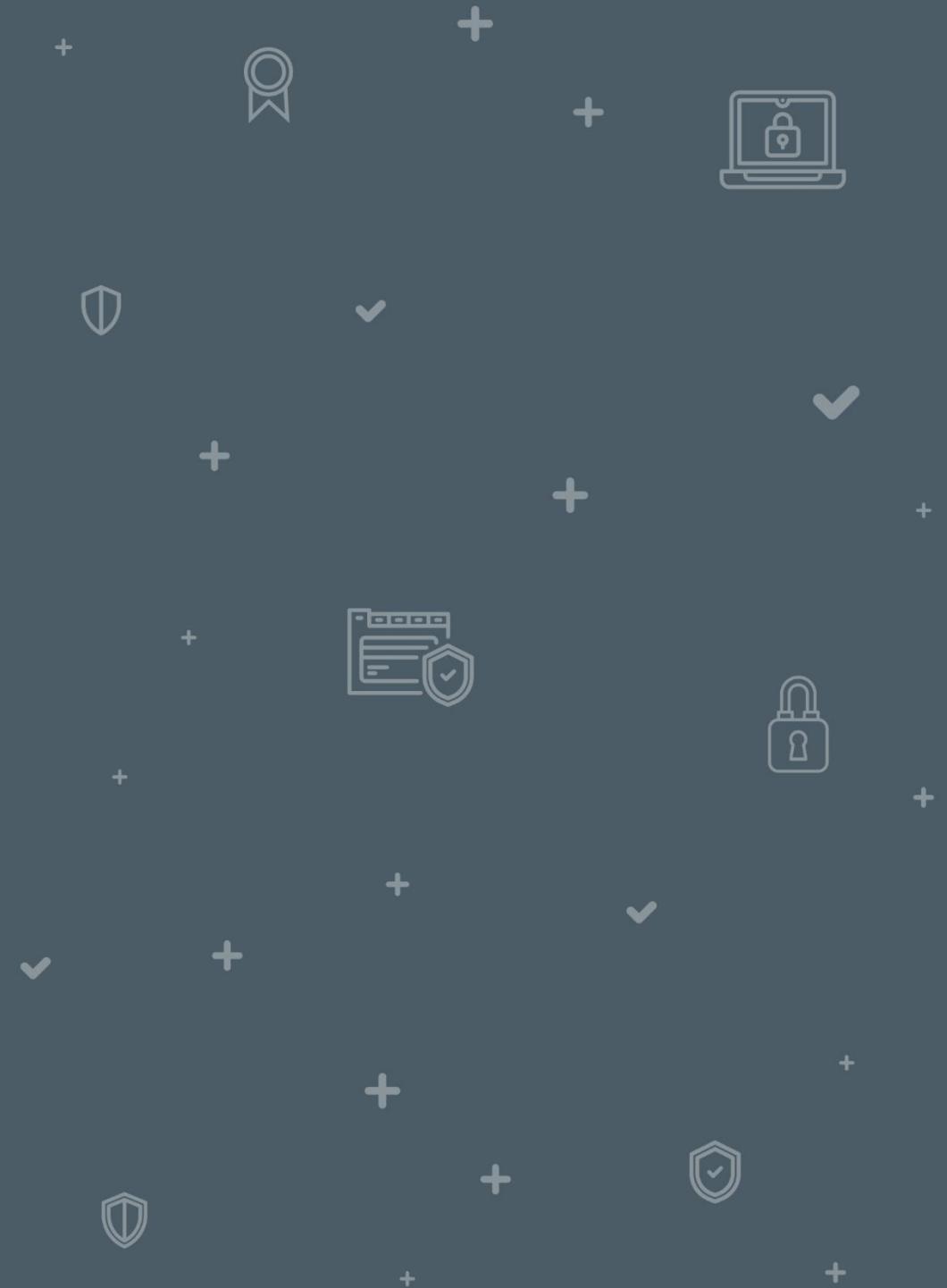
---



Descubre dónde se debería utilizar la siguiente inyección SQL: ' OR TRUE;.

# 11

## SOLUCIONARIO EJERCICIO PRÁCTICO 3





## SOLUCIONARIO EJERCICIO PRÁCTICO 3

---

- SQL (*Structured Query Language*) es un lenguaje utilizado en programación que sirve para administrar y recuperar información que está recogida en un sistema de gestión de bases de datos. La inyección SQL se aprovecha de una mala configuración de las consultas a la base de datos, ya que produce una mala validación del texto de entrada. A continuación, se muestra un ejemplo de lo que sería una consulta de la base de datos SQL.

**SELECT id**

**FROM tabla\_usuarios**

**WHERE usuario='\$usuario' AND pass='\$pass';**







## SOLUCIONARIO EJERCICIO PRÁCTICO 3

---

- Si se permite hacer una consulta concatenada, entonces se puede inyectar código SQL adicional y permitir, por ejemplo, acceder al sistema con un usuario del que no se sabe la contraseña. Probaremos con el usuario *admin*.

**SELECT id**

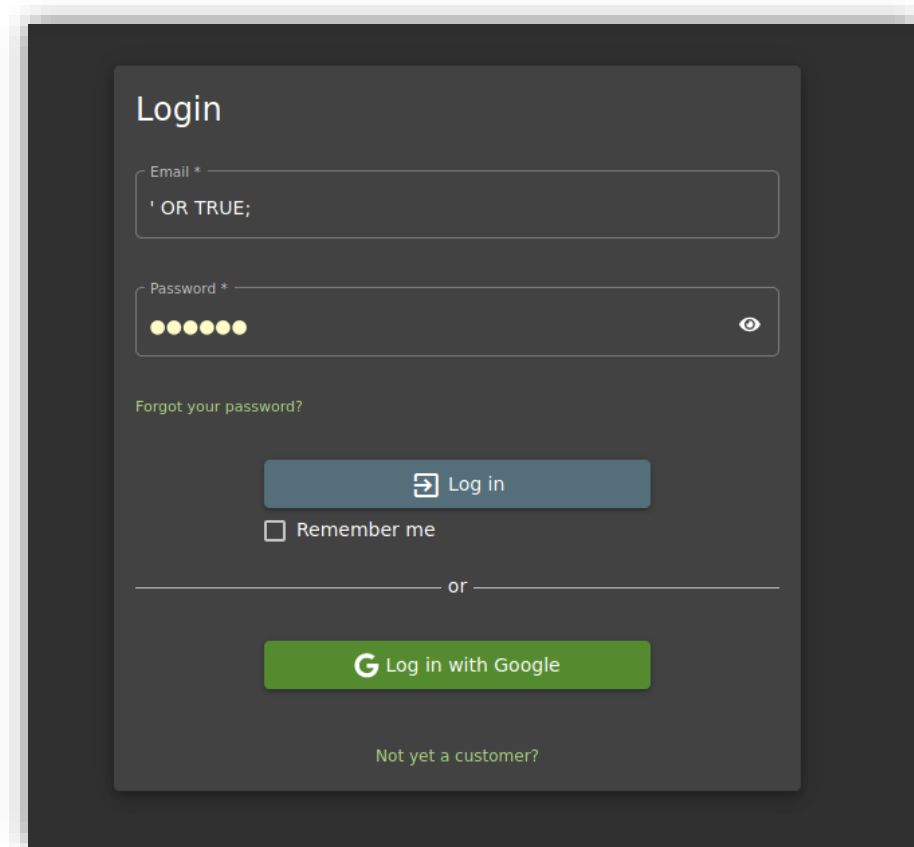
**FROM tabla\_usuarios**

**WHERE usuario='admin' AND pass="or '1'='1';** (*Que es lo mismo que 'OR TRUE;*)



# 11 SOLUCIONARIO EJERCICIO PRÁCTICO 3

- Introduce esta inyección en el *Log in*.



The image shows a login form titled "Login" on a dark background. It contains two input fields: "Email \*" and "Password \*". The "Email \*" field contains the text "' OR TRUE;". The "Password \*" field is masked with dots and has a toggle icon. Below the password field is a link "Forgot your password?". There is a "Log in" button with a right-pointing arrow icon, a "Remember me" checkbox, and a "Log in with Google" button with the Google logo. At the bottom, there is a link "Not yet a customer?".

Ilustración 55: Página de inicio de *Log in*.

# SOLUCIONARIO EJERCICIO PRÁCTICO 3

---

- El sistema, en este caso, procesaría la consulta de la siguiente forma:

```
SELECT id
FROM tabla_usuarios
WHERE usuario="OR TRUE;
```

- Esto haría que, al ser la condición verdadera siempre, es decir, que exista un usuario, se logre acceder al primer registro, que generalmente suele ser *admin*.
- Al hacer clic en *Log in*, observa que estás accediendo como el usuario *admin@juice-sh.op* con todos los privilegios de administrador, ya que es el primer usuario de la base de datos.

# 11 SOLUCIONARIO EJERCICIO PRÁCTICO 3

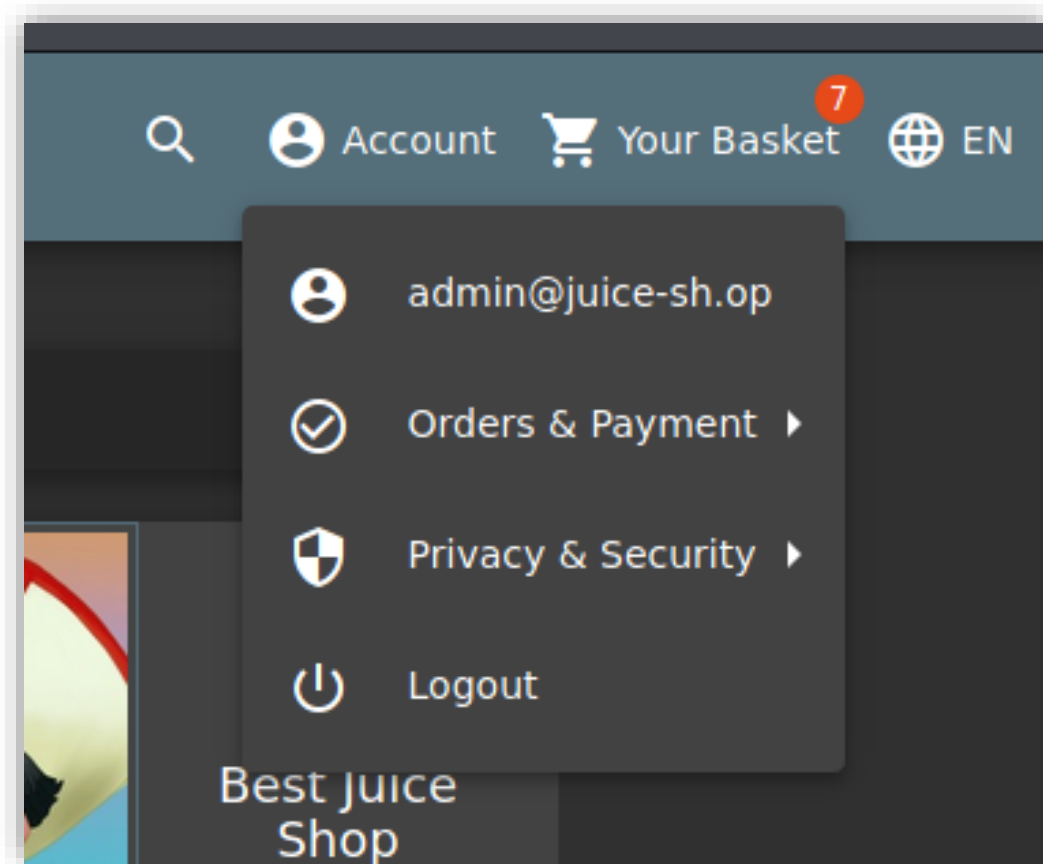


Ilustración 56: Permisos de administrador del usuario.

# ¡GRACIAS!



GOBIERNO  
DE ESPAÑA

VICEPRESIDENCIA  
PRIMERA DEL GOBIERNO  
  
MINISTERIO  
DE ASUNTOS ECONÓMICOS  
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO  
DE DIGITALIZACIÓN E  
INTELIGENCIA ARTIFICIAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD

