	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

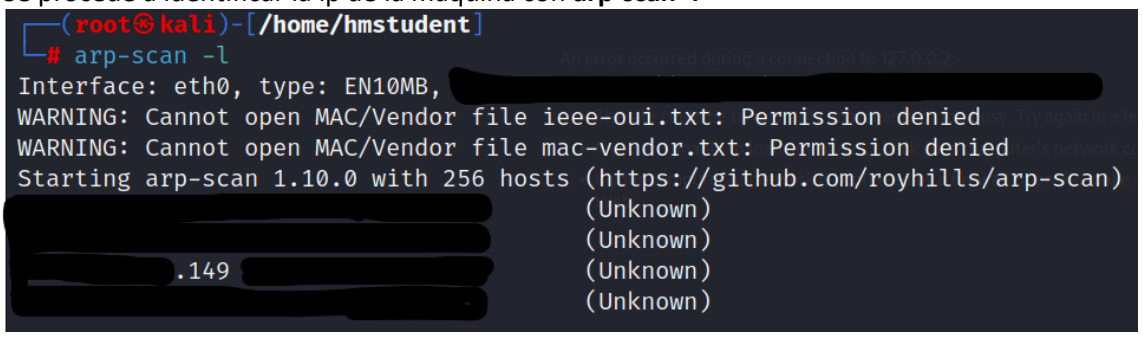
Fecha de creación:
09.01.2025

Índice

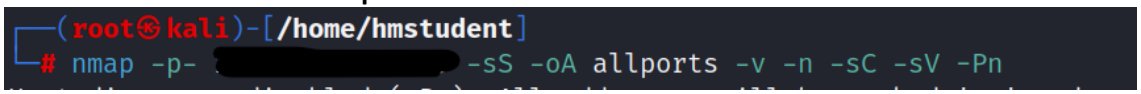
Tabla de contenido

1. Reconocimiento

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



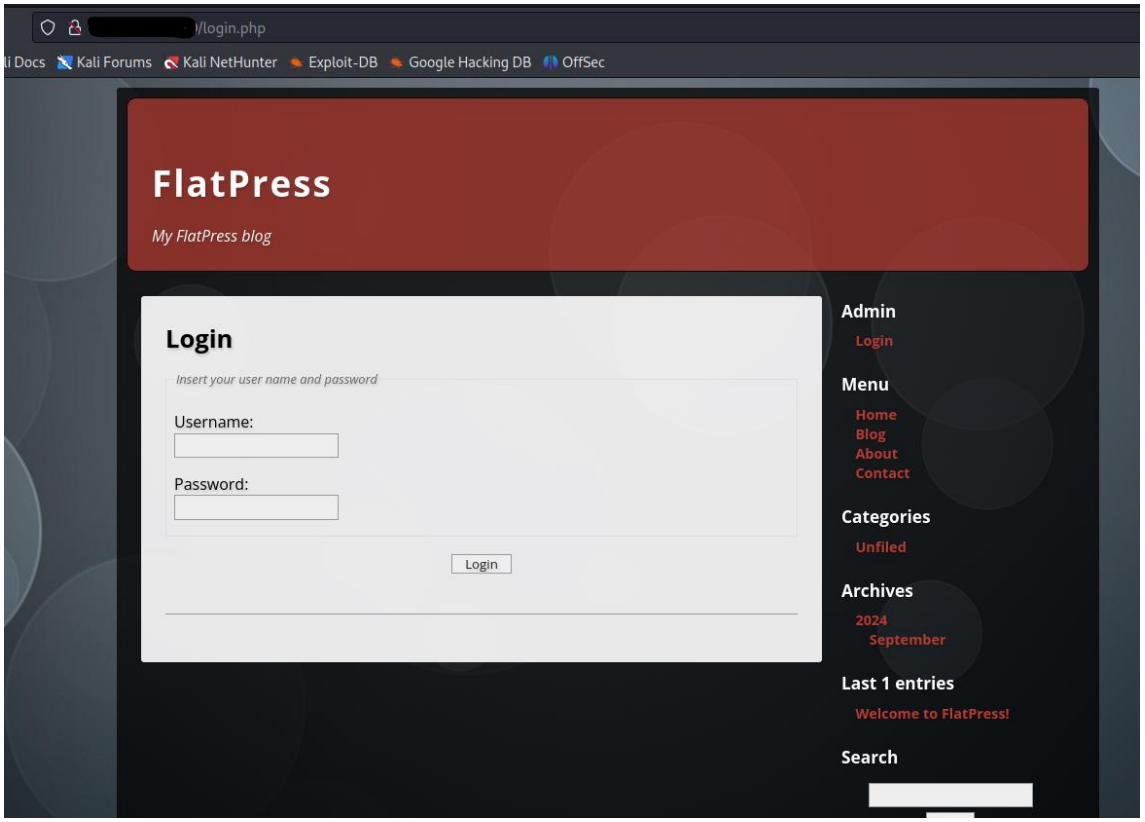
Se realiza el escaneo con **nmap**



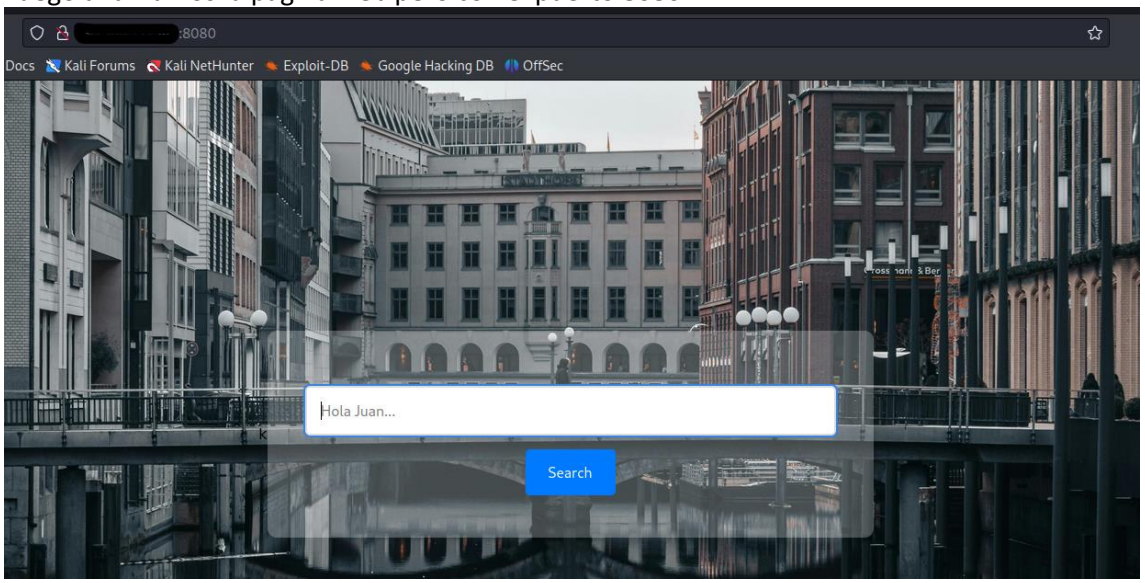
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
| 256 c85f17628c260a7bb2c6073331648430 (ECDSA)
|_ 256 e39258d850ac005a4902d7e93318478c (ED25519)
80/tcp open http Apache httpd 2.4.62 ((Debian))
|_http-generator: FlatPress fp-1.2.1
|_http-favicon: 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

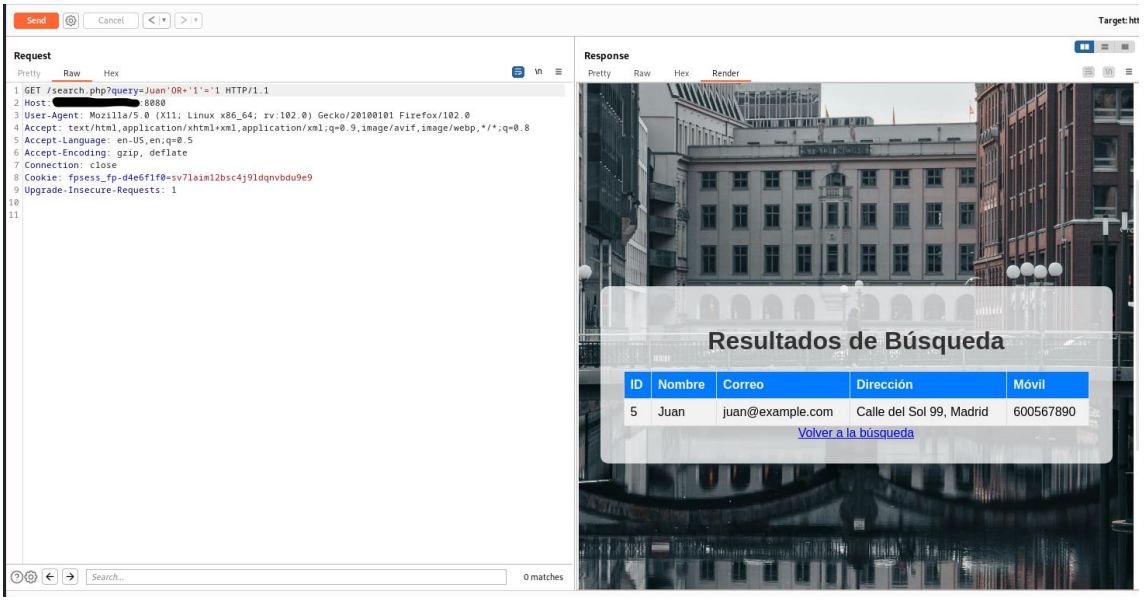


Luego analizamos la pagina web pero con el puerto 8080

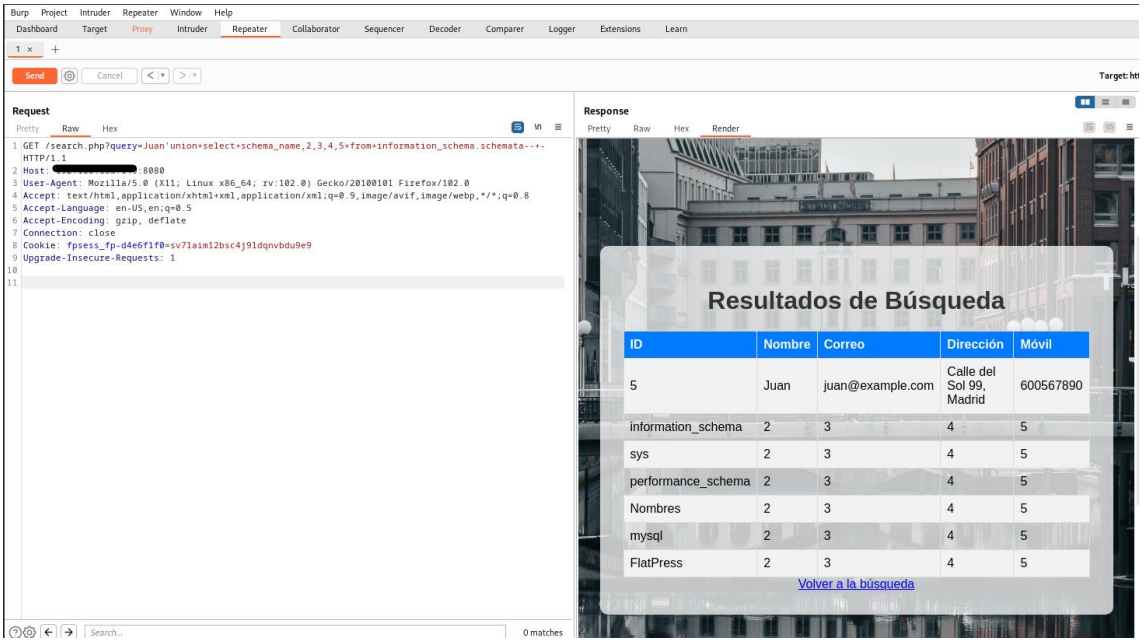


Vemos que tiene un cuadro de Search así que con Burp Suite procedemos a capturar la petición y enviar una inyección sql para ver si es vulnerable

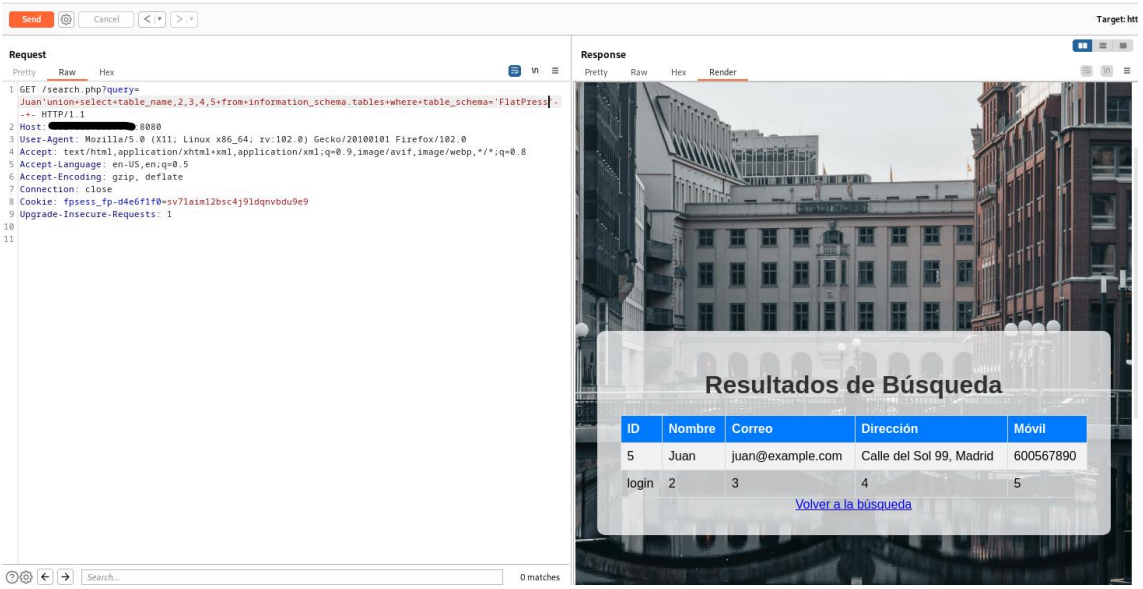
Comprobamos que si es vulnerable a una inyección sql



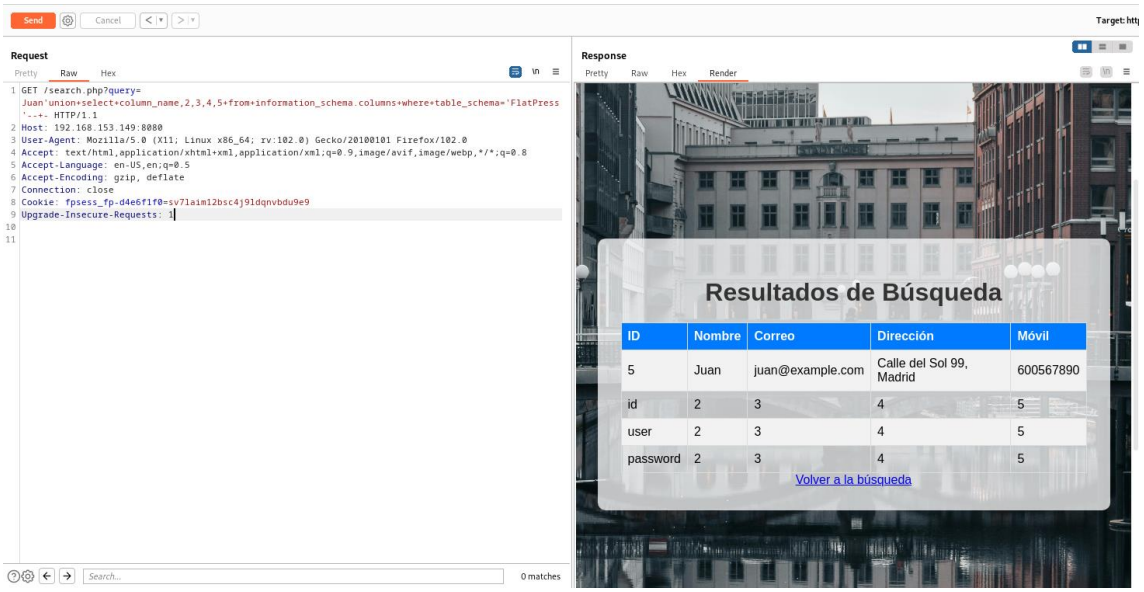
Necesitamos saber el número de columnas que tenemos y las bases de datos que hay



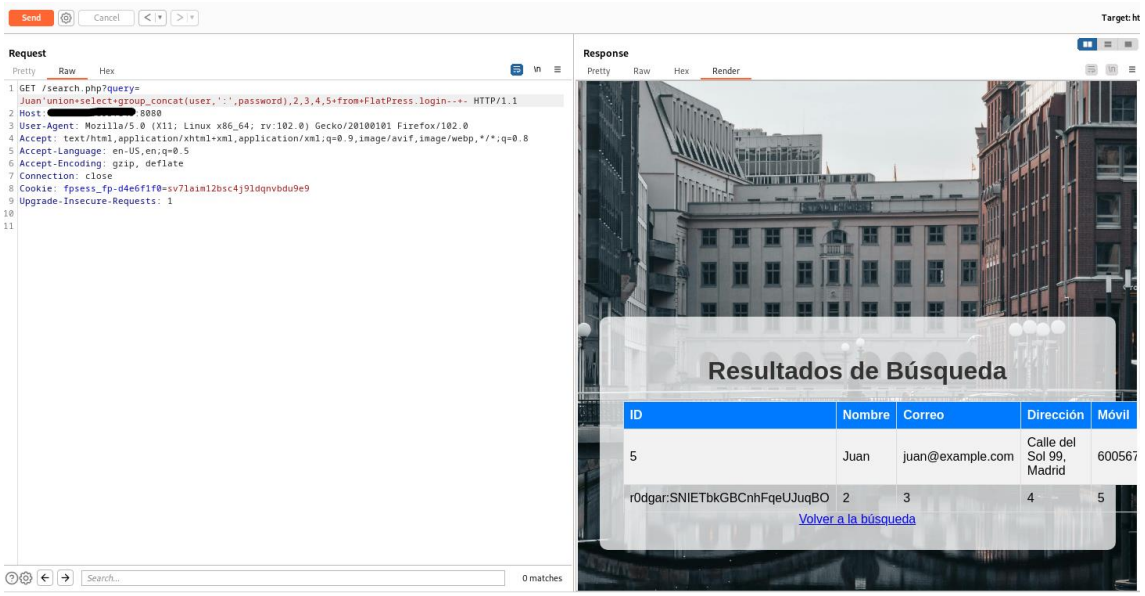
Revisamos las bases de datos y la que nos servirá seria la **FlatPress**, donde procedemos a enumerar las tablas que tiene



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

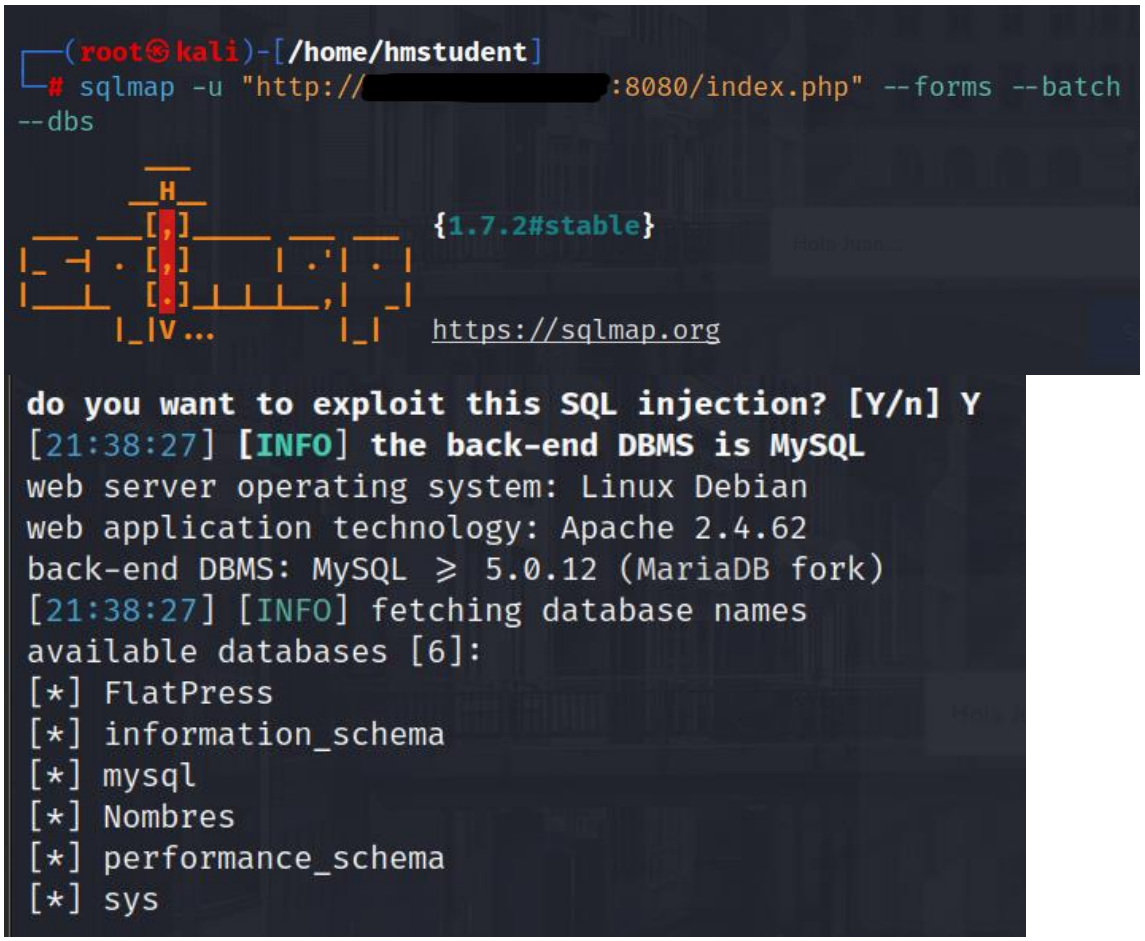


Podemos ver que existen las columnas de **user** y **password** procedemos a ver la información de las credenciales

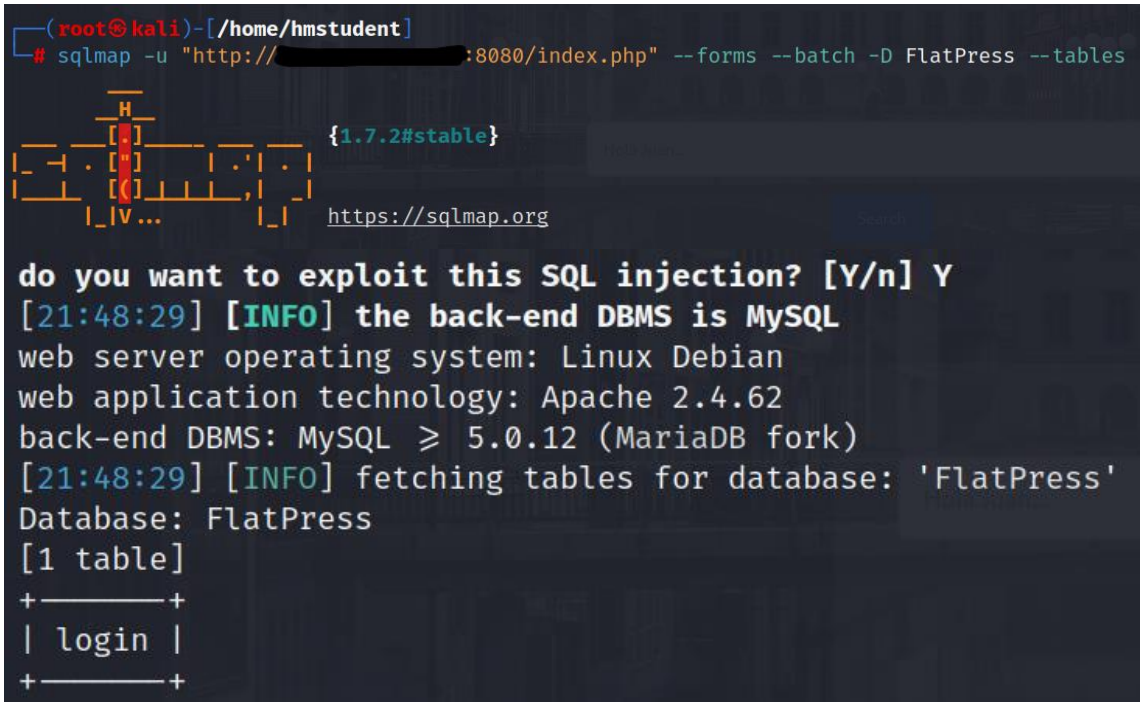


User: r0dgar
Password: SNIETbkGBCnhFqeUJuqBO

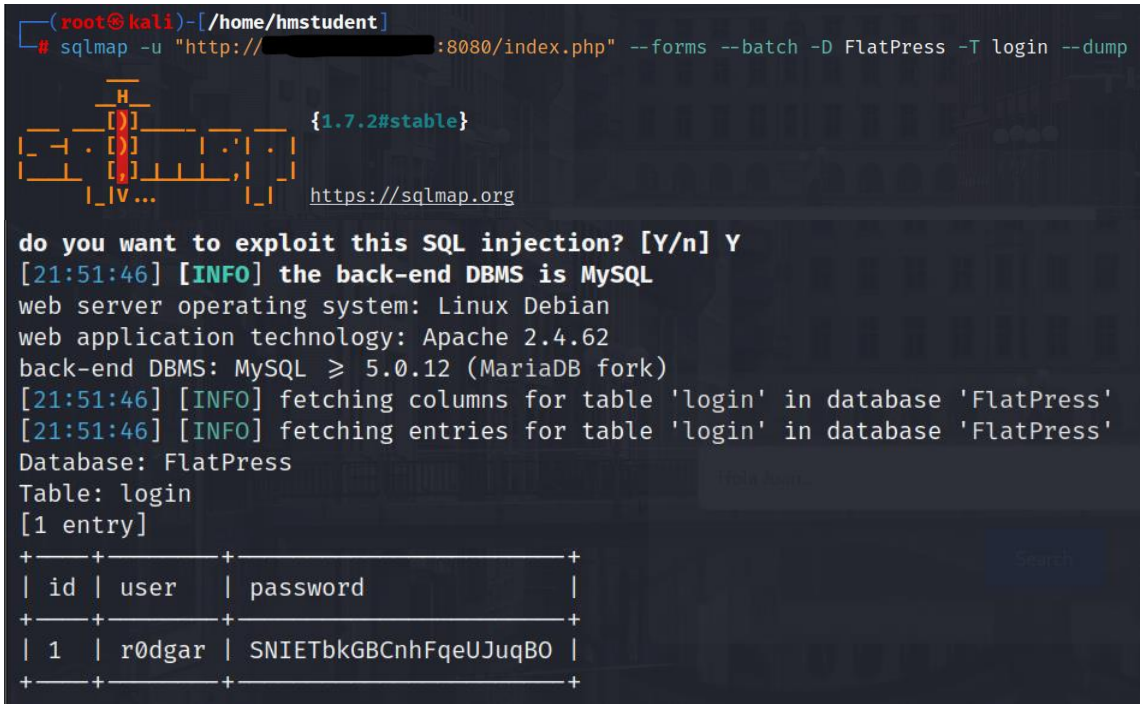
Procedemos a usar SqlMap y mostrar lo que hicimos anteriormente, pero de forma automática, listamos las bases de datos



Desplegamos las tablas de la base de datos FlatPress



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



3. Explotación

Proceso manual/ automatizado.

Automatizado

Manual

4. Escalación de privilegios si/no

N/A

5. Banderas

6. Herramientas usadas

	…
	…
	…

7. Conclusiones y Recomendaciones

CONCLUSIONES:

RECOMENDACIONES: