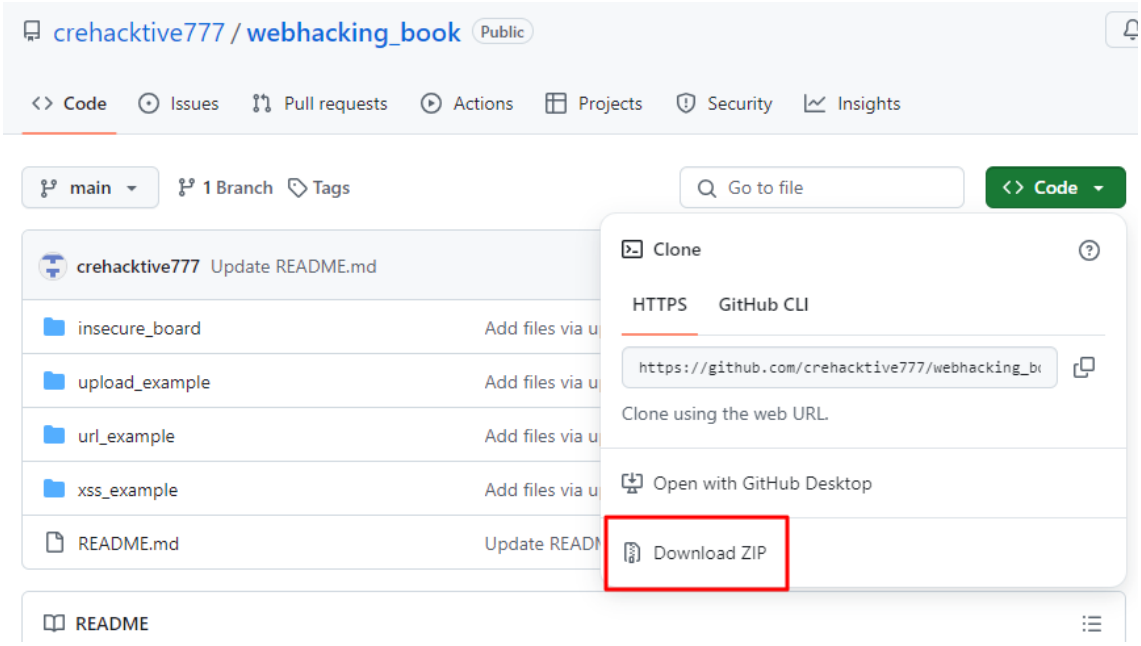
가상 환경 구축

실습을 위한 가상 환경을 구축해보자. 소스 코드는 다음 깃허브에서 내려받을 수 있다.

- 깃허브: github.com/crehacktive777/webhacking_book

깃허브 접속 후 페이지 우측 상단의 [Code]를 클릭한 다음 [Download ZIP] 버튼을 클릭해 압축 파일을 다운로드한다.

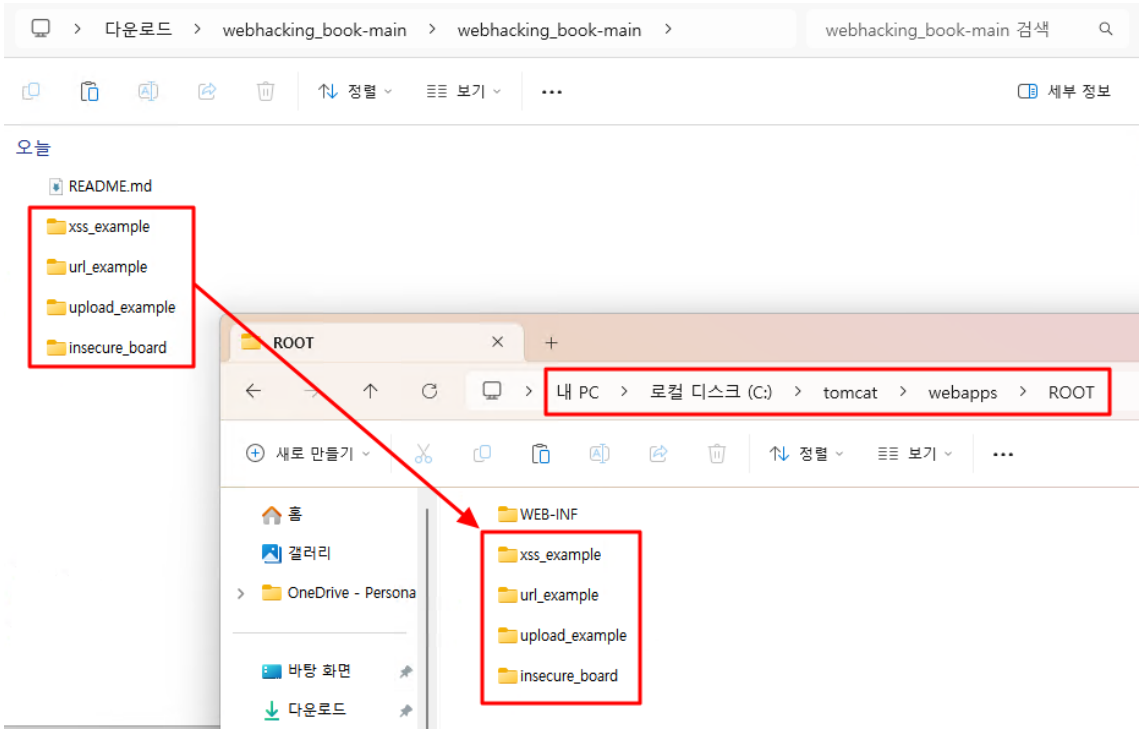


▶ 깃허브에서 압축 파일 다운로드

압축 파일을 해제하면 총 4 개의 디렉터리를 볼 수 있다. 각 디렉터리별 용도는 다음과 같다.

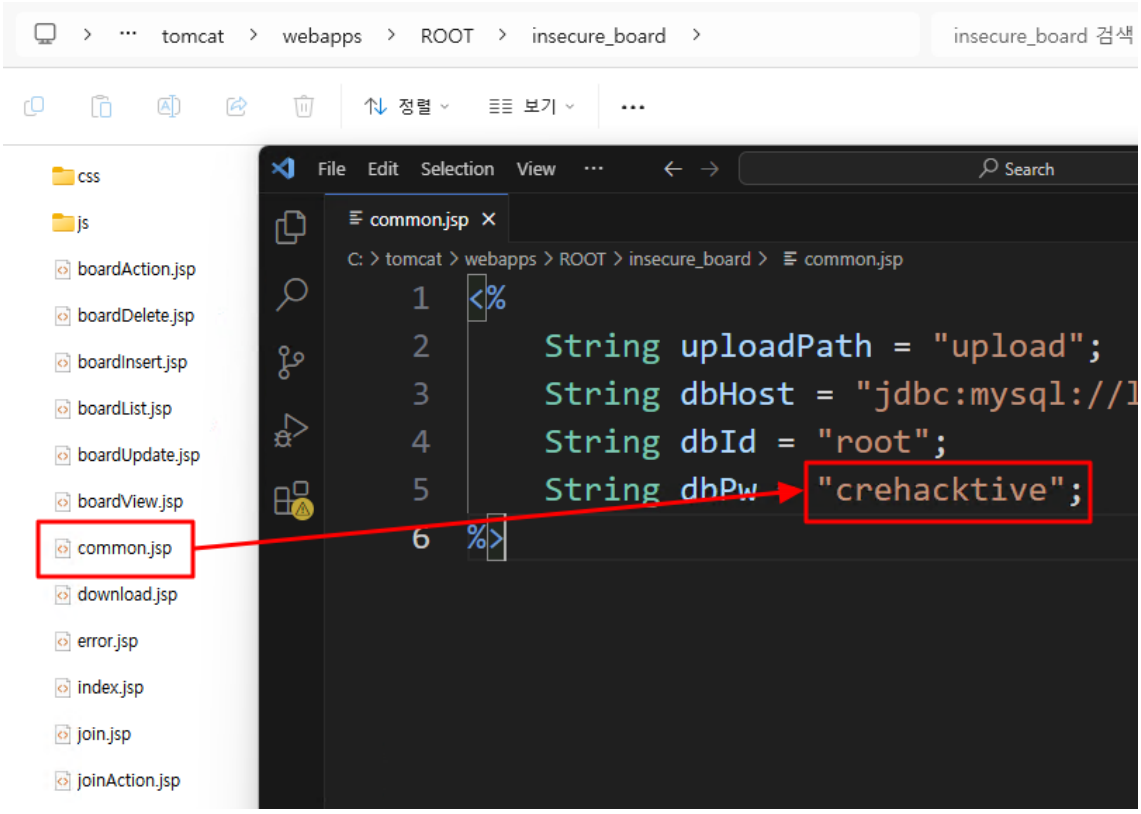
- **insecure_board:** 모든 취약점 실습
- **upload_example:** 파일 업로드 취약점 실습
- **url_example: URL** 접근 제한 미흡 취약점 실습
- **xss_example:** XSS 취약점 실습

다운로드받은 4 개의 디렉터리를 [톰캣설치경로]/webapps/ROOT 로 이동한다.



▶ 디렉터리 이동

insecure_board 디렉터리 내 common.jsp 파일을 열어 dbPw 변수에 MySQL 패스워드를 입력한다.



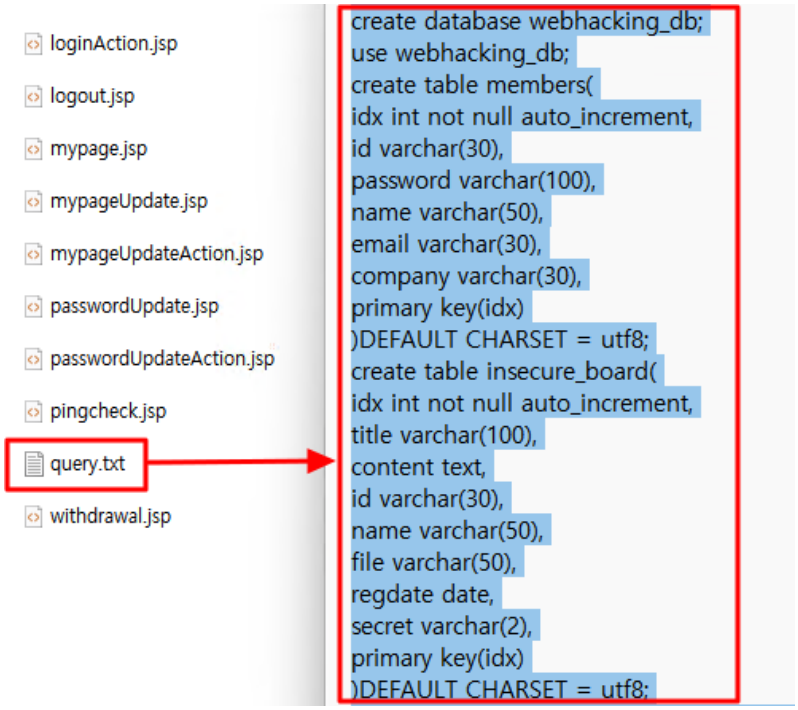
▶ common.jsp 에서 데이터베이스 패스워드 입력

MySQL 을 실행하고 창이 열리면 패스워드를 입력한다.

```
Enter password: ***********
Welcome to the MySQL monitor.  Commands end with ; or ₩g.
Your MySQL connection id is 399
Server version: 8.0.29 MySQL Community Server - GPL

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '₩h' for help. Type '₩c' to clear the current input statement.
```

```
mysql>
```

insecure_board 디렉터리 내 query.txt 파일을 열고 전체 내용을 복사한다.



▶ query.txt

MySQL 로 돌아와 복사한 내용을 붙여 넣는다.

```
mysql> create database webhacking_db;
Query OK, 1 row affected (0.01 sec)

mysql> use webhacking_db;
Database changed
mysql> create table members(
    -> idx int not null auto_increment,
    -> id varchar(30),
    -> password varchar(100),
    -> name varchar(50),
```

```
    -> email varchar(30),
    -> company varchar(30),
    -> primary key(idx)
    -> )DEFAULT CHARSET = utf8;
Query OK, 0 rows affected, 1 warning (0.04 sec)

mysql> create table insecure_board(
    -> idx int not null auto_increment,
    -> title varchar(100),
    -> content text,
    -> id varchar(30),
    -> name varchar(50),
    -> file varchar(50),
    -> regdate date,
    -> secret varchar(2),
    -> primary key(idx)
    -> )DEFAULT CHARSET = utf8;
Query OK, 0 rows affected, 1 warning (0.03 sec)

mysql> create table customer_info(idx int, id varchar(15), password varchar(30), jumin
varchar(15));
Query OK, 0 rows affected (0.03 sec)

mysql> insert into customer_info values(1, 'admin', '@dmin!q@w#e', '810203-1023113');
Query OK, 1 row affected (0.01 sec)

mysql> insert into customer_info values(2, 'gugucon', '99c0n', '861121-1244251');
Query OK, 1 row affected (0.01 sec)

mysql> insert into customer_info values(3, 'sonata_zzang', 'sosohan123', '890912-
1601812');
Query OK, 1 row affected (0.01 sec)

mysql> insert into customer_info values(4, 'halls', 'halls920912', '921001-1881222');
Query OK, 1 row affected (0.01 sec)

mysql> insert into customer_info values(5, 'tkworld', '1q2w3e4r', '870405-1285264');
```

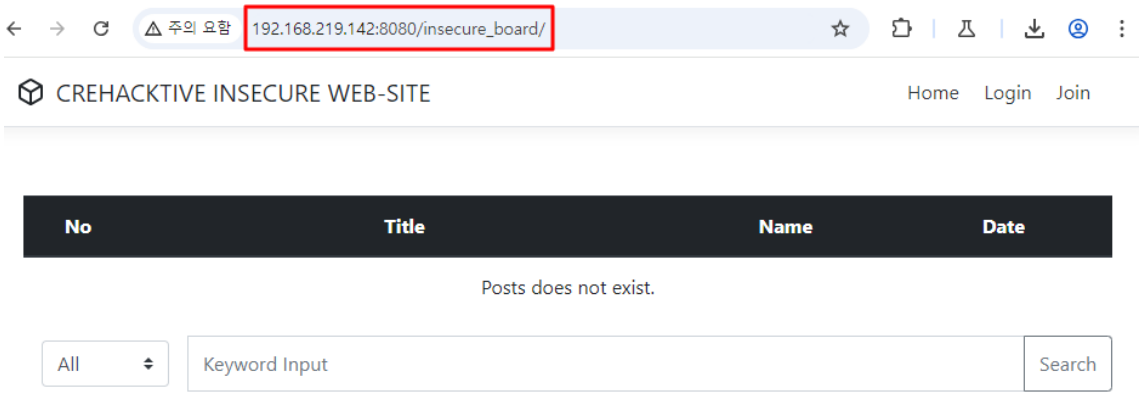
```
Query OK, 1 row affected (0.01 sec)

mysql>
```

데이터베이스를 선택하고 테이블을 조회했을 때 다음과 같이 출력되면 쿼리가 정상적으로 실행된 것이다.

```
mysql> use webhacking_db
Database changed
mysql> show tables;
+-------------------------+
| Tables_in_webhacking_db |
+-------------------------+
| customer_info           |
| insecure_board          |
| members                 |
+-------------------------+
3 rows in set (0.00 sec)
```

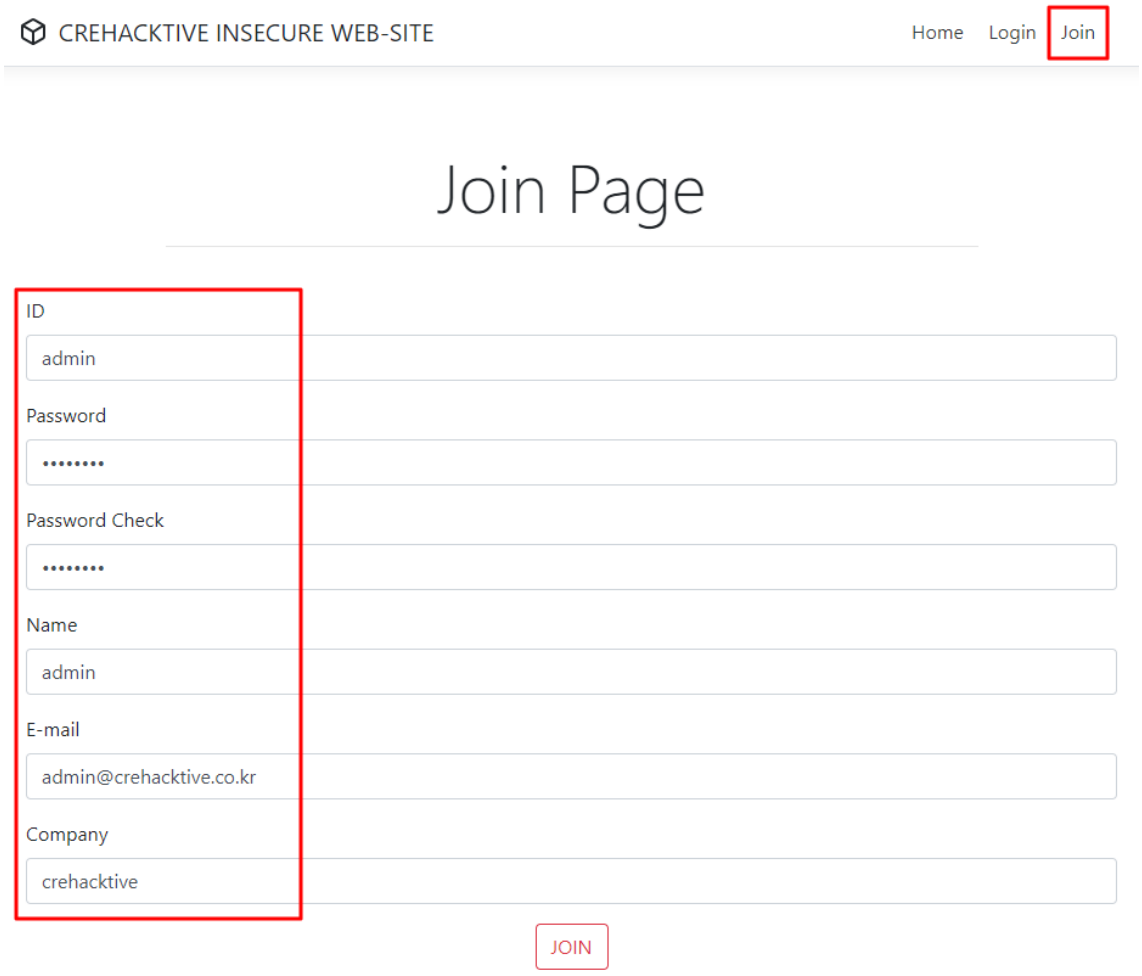
웹 브라우저에서 `127.0.0.1:8080/insecure_board` 혹은 CMD 창에서 `ipconfig` 명령어를 실행 후 출력되는 본인의 IP 입력를 입력해 취야한 게시판에 접속한다(예시 이미지는 가상 환경 구축 서버와 진단 PC 가 다른 호스트이기 때문에 실습마다 `127.0.0.1` 주소가 아닌 사설 IP 로 접속한다.).

TIP 만약 500 내부 서버 오류가 발생하면 common.jsp 에서 데이터베이스 계정 정보가 올바르게 입력되었는지 다시 확인한다.



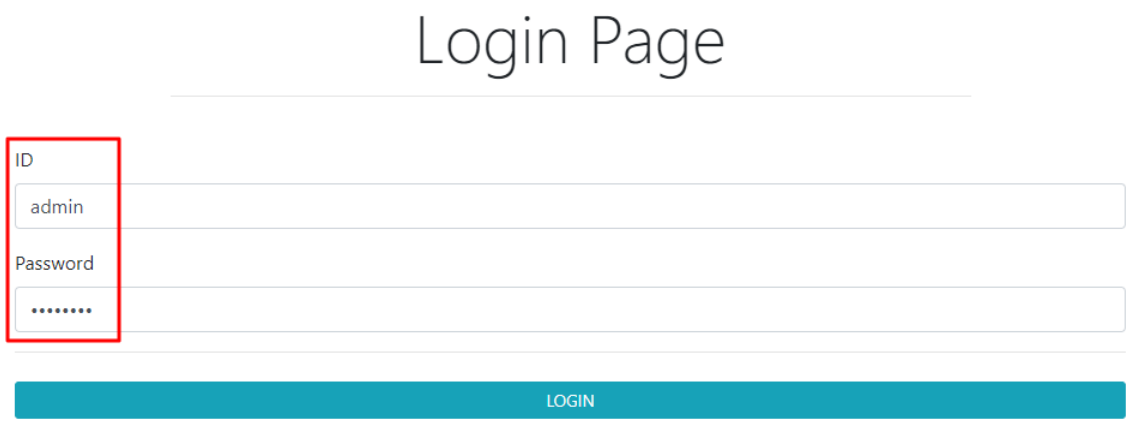
▶ 취약한 게시판 접속

실습을 위해 admin 계정을 생성해보자. 접속한 페이지 우측 상단의 [Join] 버튼을 클릭해 회원 가입 페이지로 이동한 다음 아이디가 admin 인 계정을 생성한다. 아이디는 반드시 admin 으로 생성해야 책에서 다루는 모든 실습을 매끄럽게 진행할 수 있다.



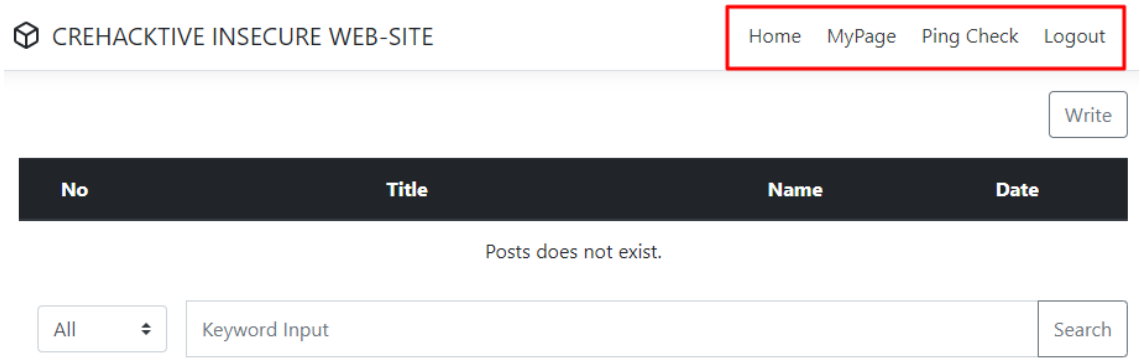
▶ admin 계정 생성

이제 생성한 계정으로 로그인을 시도한다.



▶ 로그인 시도

다음과 같은 메뉴가 출력되면 admin 계정으로 로그인에 성공한 것이다. 만약 아이디가 admin 이 아니라면 [Ping Check] 메뉴는 출력되지 않는다.



▶ admin 계정으로 로그인

MySQL 에서 `members` 테이블을 조회하면 회원 가입을 하면서 입력한 정보가 그대로 입력된 것을 알 수 있다.

```
mysql> select * from members;
+-----+-------+----------+-------+----------------------+-------------+
| idx | id    | password | name  | email                | company     |
```

```
+-----+-------+----------+-------+-----------------------+-------------+
|   1 | admin | admin123 | admin | admin@crehacktive.co.kr | crehacktive |
+-----+-------+----------+-------+-----------------------+-------------+
1 row in set (0.00 sec)
```