과목명	시큐어코딩
담당교수	우사무엘 교수님
과제명	11주차 실습 보고서
학과	소프트웨어학과
학번	32151671
이름	박민혁
제출일자	2021-05-23

목차

I. Part 1 : Mac 실습 환경 구축

II. Part 2 : Window 실습 환경 구축

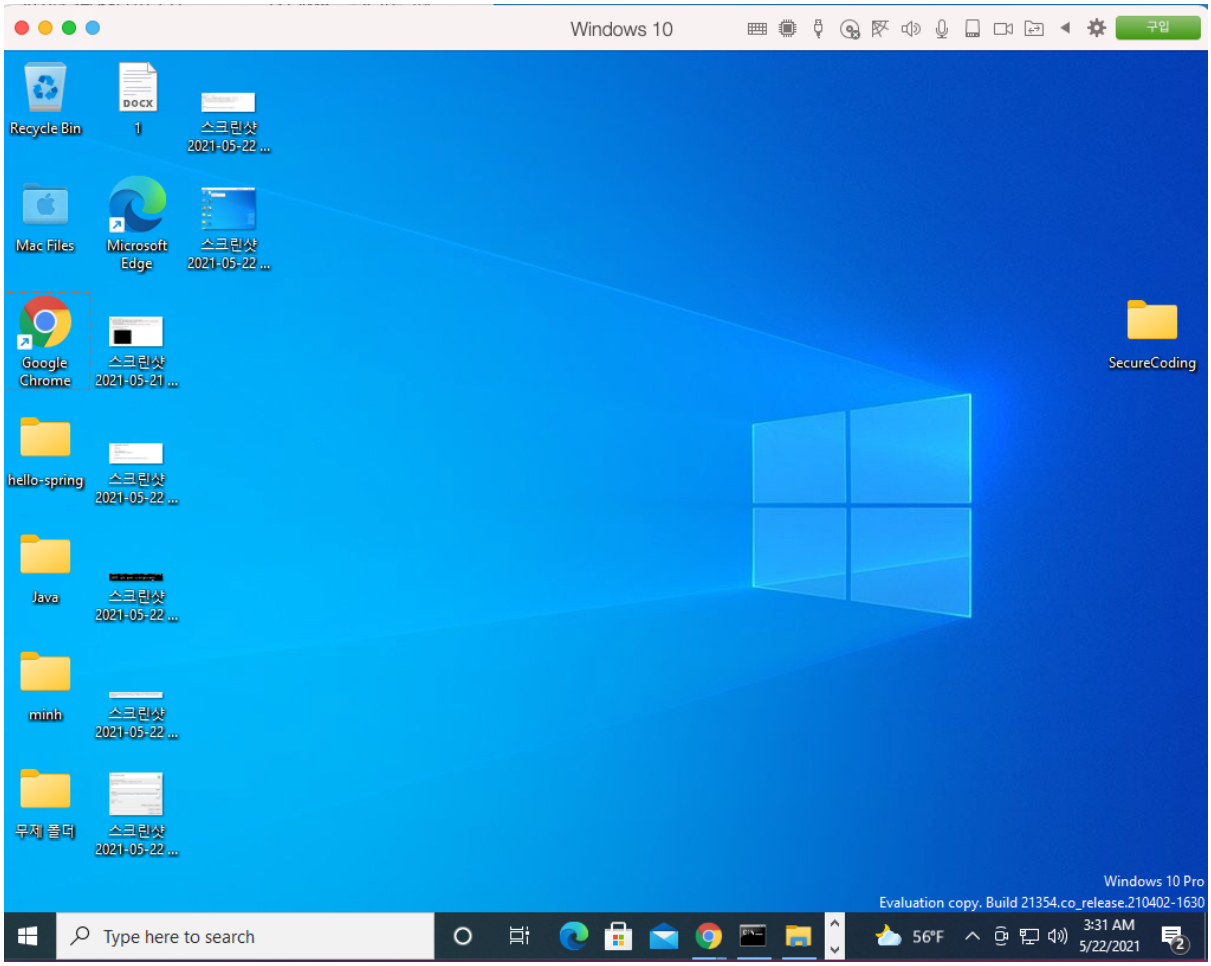
III. Part 3 : 실습 수행 결과

1. Part 1 : Mac 실습 환경 구축

(1). 서론

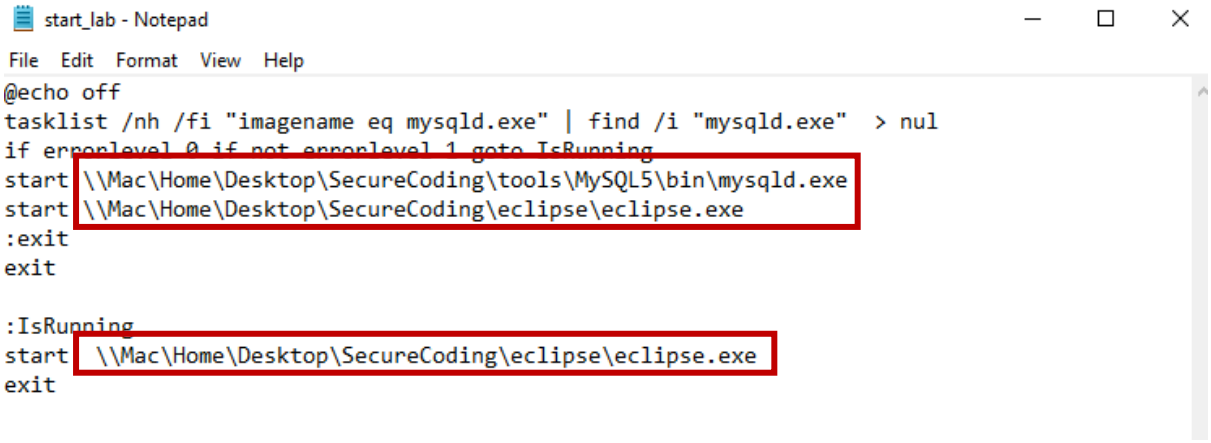
맥 환경에서 실습 환경 구축을 하다가 에러가 너무 많이 났었고 에러 났던 곳까지 보고서를 작성 후, 윈도우 노트북을 빌려 실습환경을 구축했습니다. 그래서 Part 1에서는 막혔던 부분까지의 설명과 Part 2, Part 3에서는 윈도우에서 11주차 보고서에 대한 것을 작성하였습니다.

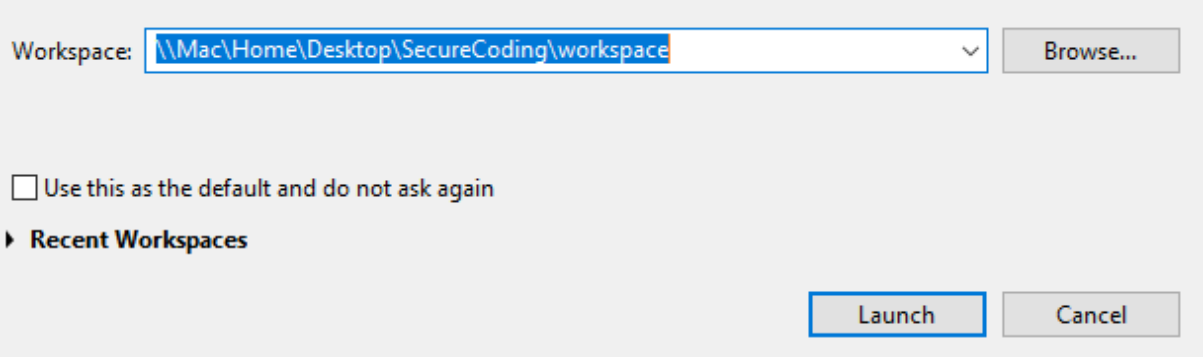
(2). 본론



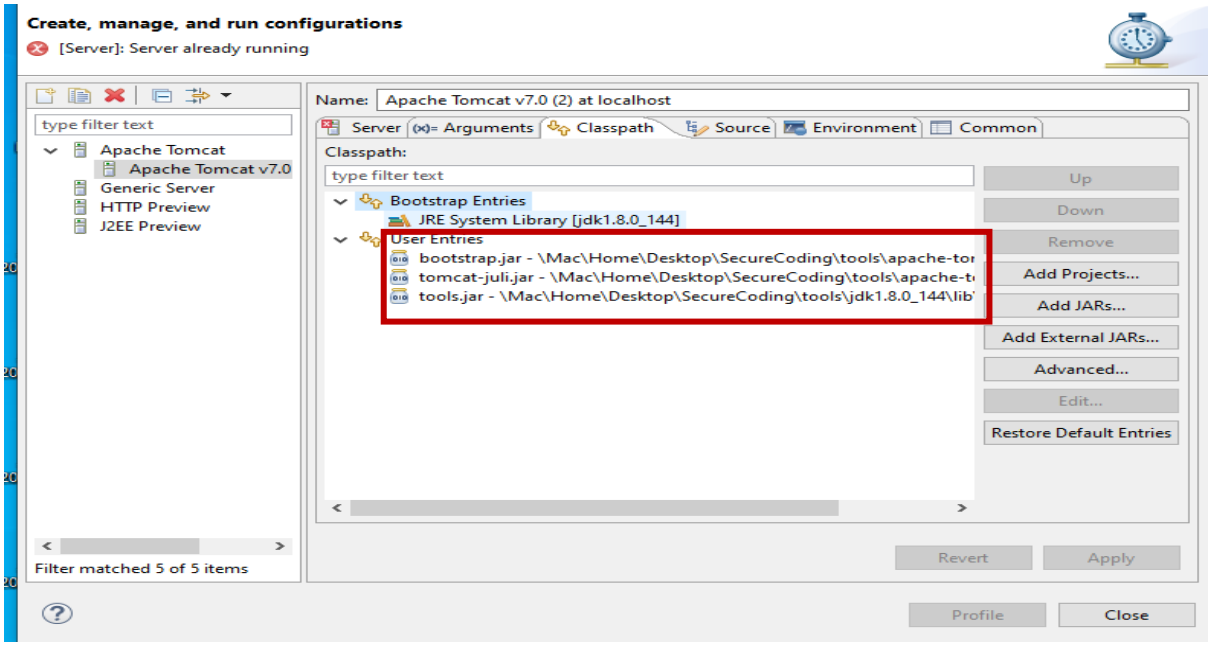
저는 가상환경으로 Parallels를 사용하고 있습니다. 전에는 우분투를 설치해 리눅스 환경을 사용하고 있었는데 이번 실습이 윈도우에서 실행이 가능한 것이라 아래 링크에 따라서 윈도우 환경을 다운 받았습니다.

https://w4umain.com/240

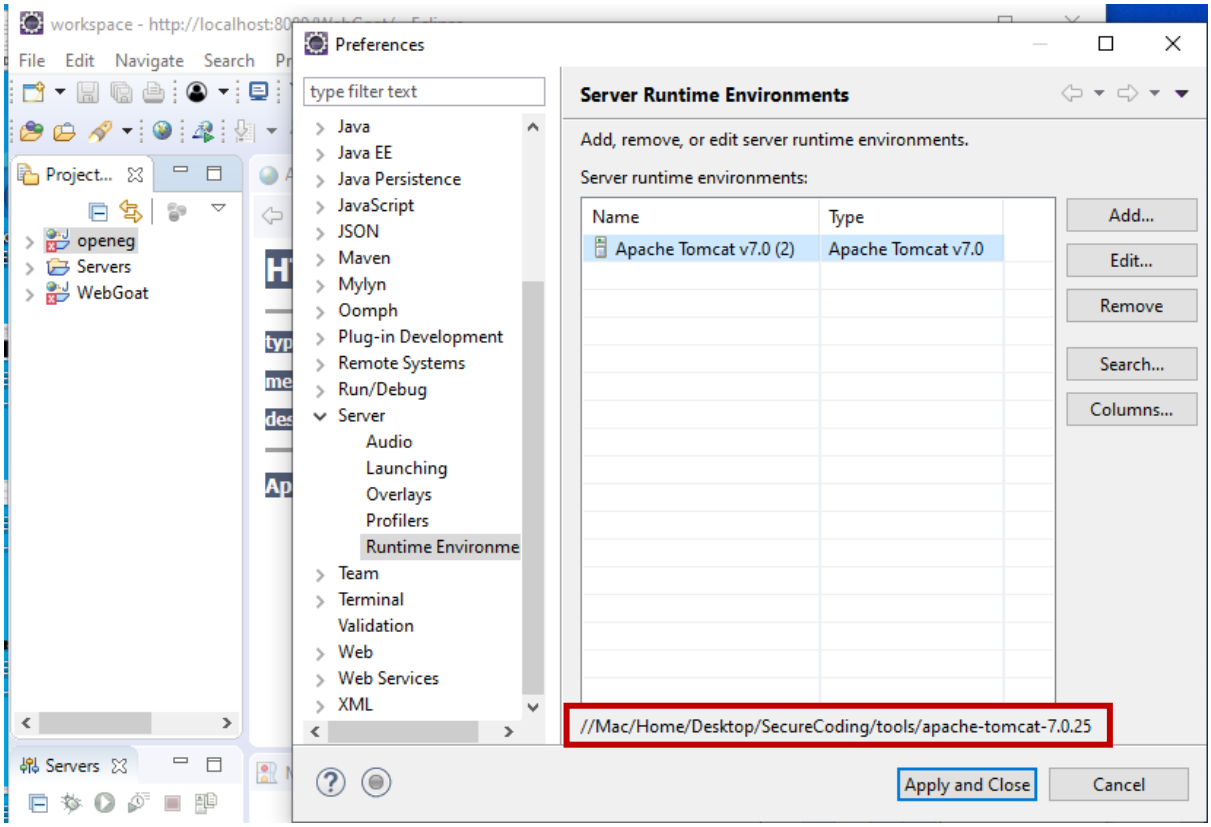




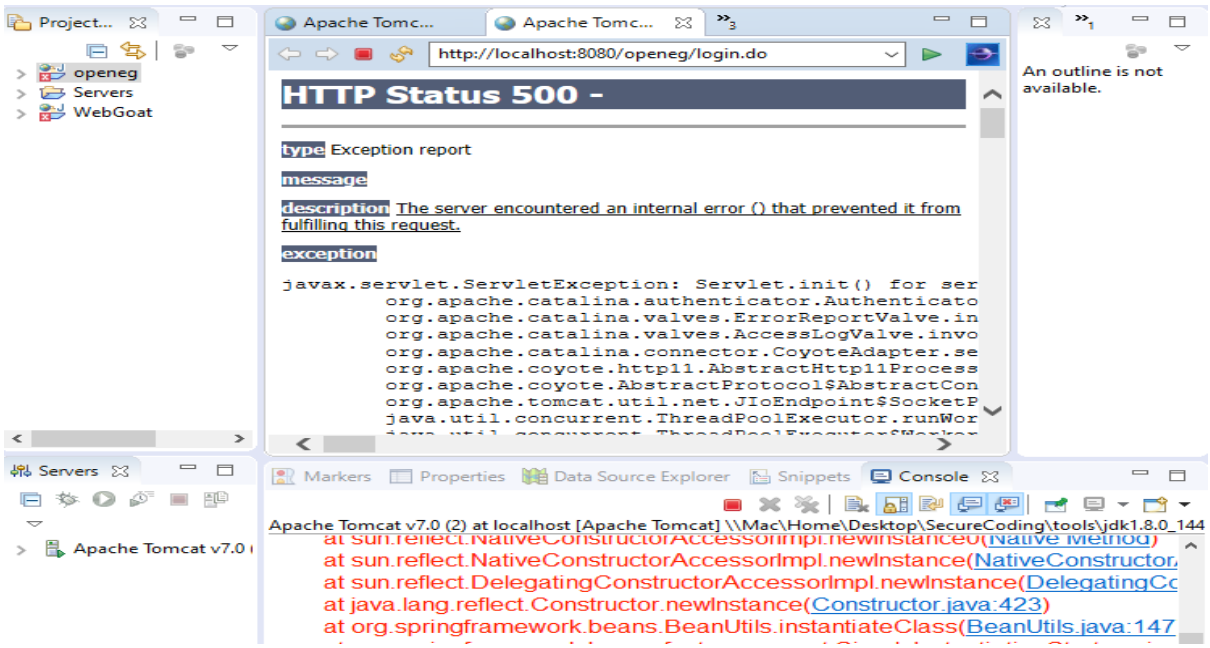
위에 사진과 같이 start_lab 경로 설정을 제 환경에 맞춰서 실행했습니다. 그 결과 이클립스까지는 잘 켜졌습니다. 또한 이클립스 워크스페이스 설정 시 기본 경로로 들어가면 안돼서 제 맥 환경에 맞게 설정하여 들어갔습니다.



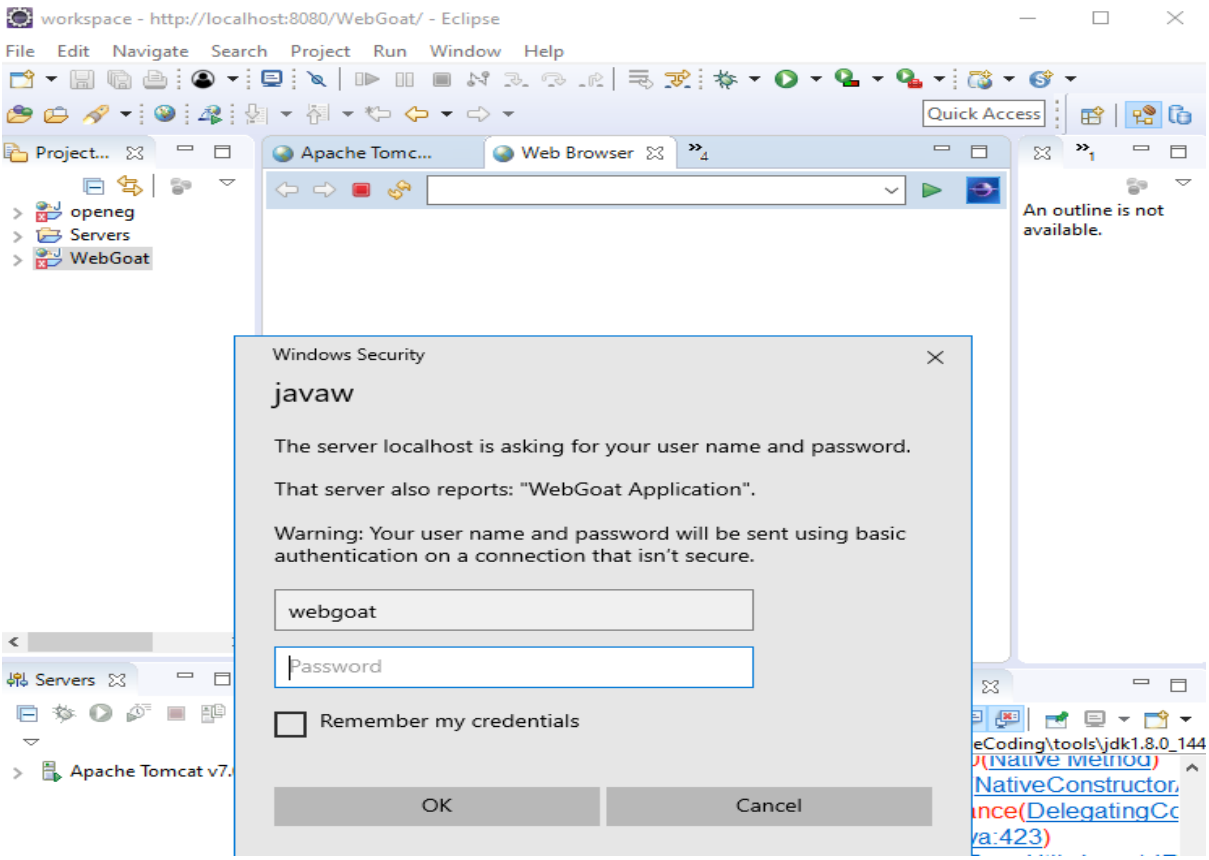
그리고 openeg를 실행시켰는데 bootstrap에 대한 경로설정 에러가 뜨길래 openeg 프로필 설정에 들어가 경로 설정을 다시 해주었습니다.



그 다음으로 Apache Tomcat을 실행하는데 디렉토리를 찾을 수 없다고 하여 설정법을 검색하여 windows -> preference -> server -> runtime environments 창에서 Apache Tomcat 경로 설정을 해주었습니다.



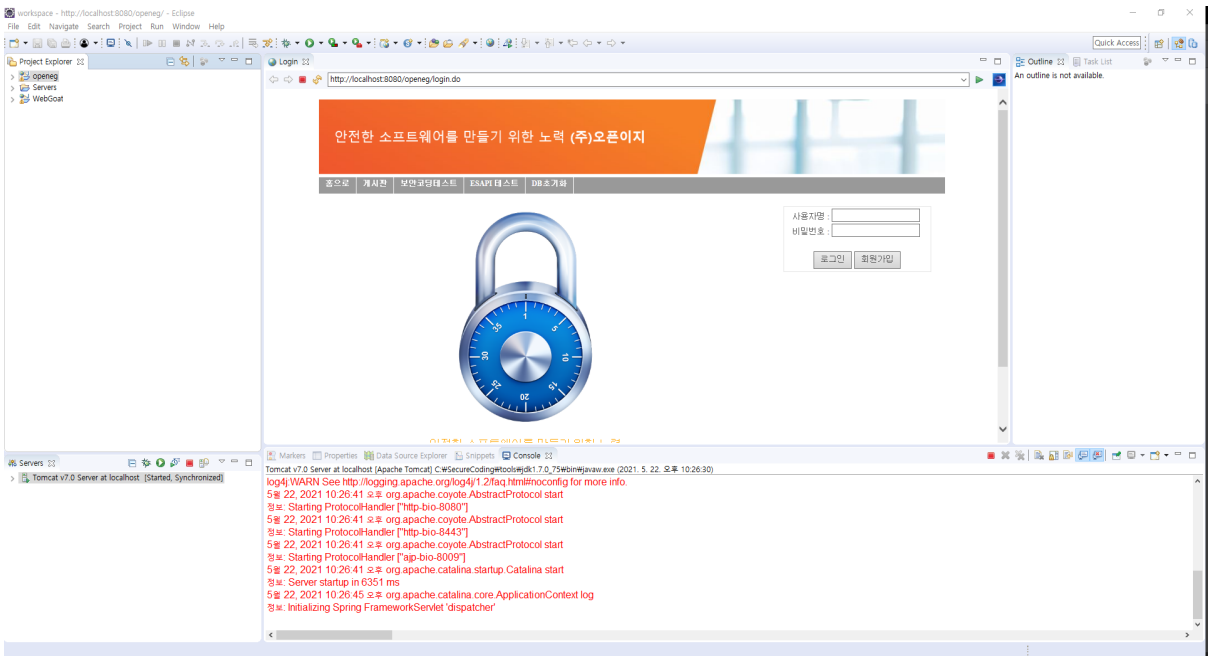
해당 설정이 끝난 후 openeg를 실행시켰는데 500번대 에러가 발생하였습니다. 그리고 description에 나와있는 에러를 검색하여 해결하려고 했지만, 해결하지 못해서 이 상태에서 멈췄습니다.



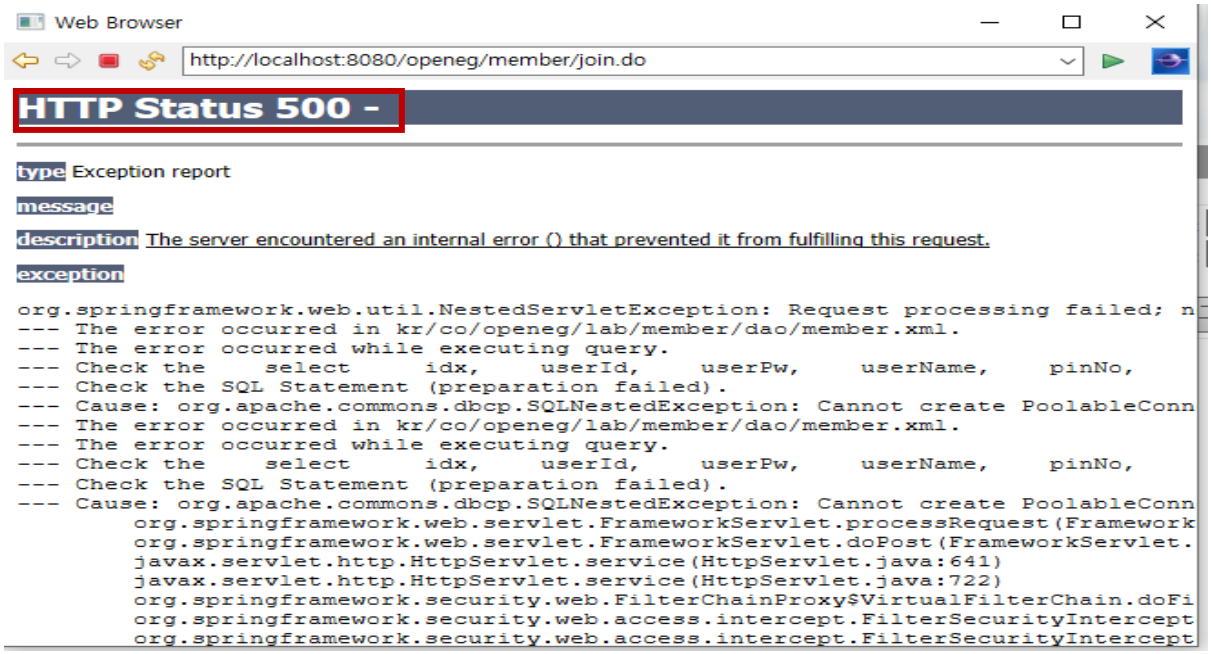
그리고 WebGoat도 실행 시켜 ppt에 나와있는 guest/guest 해당 아이디와 비번이 연결이 안돼서, 찾아 보았는데 webgoat/webgoat으로 시도해보라는 글이 있었습니다. 하지만 해당 아이디와 비밀번호도 연결이 되지 않았는데 3번 시도를 하니까 400번대 에러가 떴습니다. 500번대와 400번대 에러는 데이터베이스나, 요청이 잘못 된 것으로 알고있습니다. 그래서 3306 포트를 제가 맥 환경에서 사용해서 에러가 뜨나 확인했으나 그런 문제는 아니었고, MySQL을 명령어를 통해 다시 설치 했지만 계속적으로 에러가 발생했습니다.

2. Part 2 : Window 실습 환경 구축

(1). 웹 애플리케이션 실행



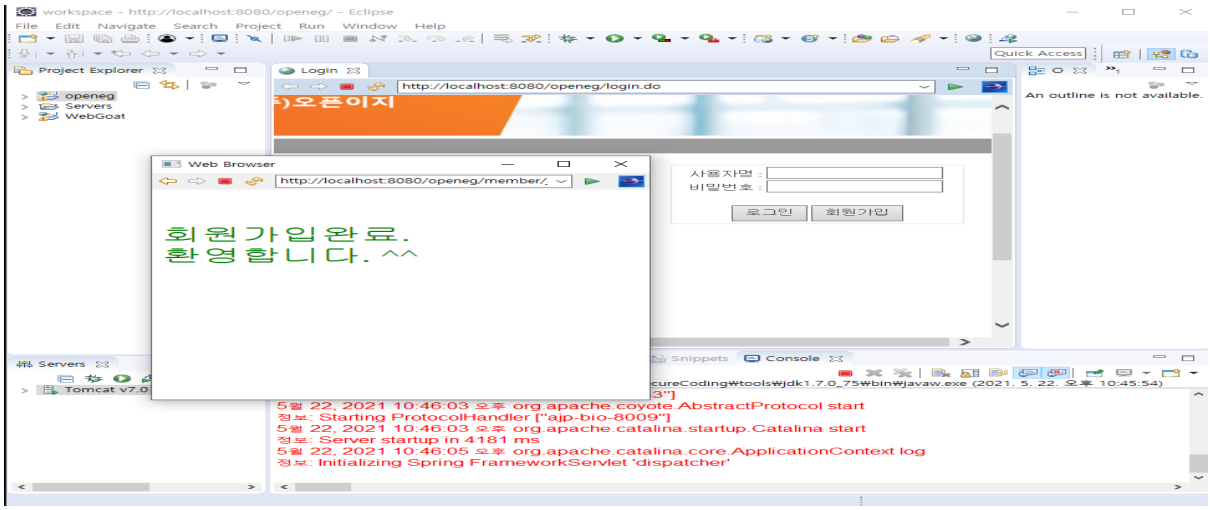
Step1, Step2를 모두 마치고 Openeg를 실행시켰다. 위에 화면은 Eclipse를 통해 실행시킨 화면이다.



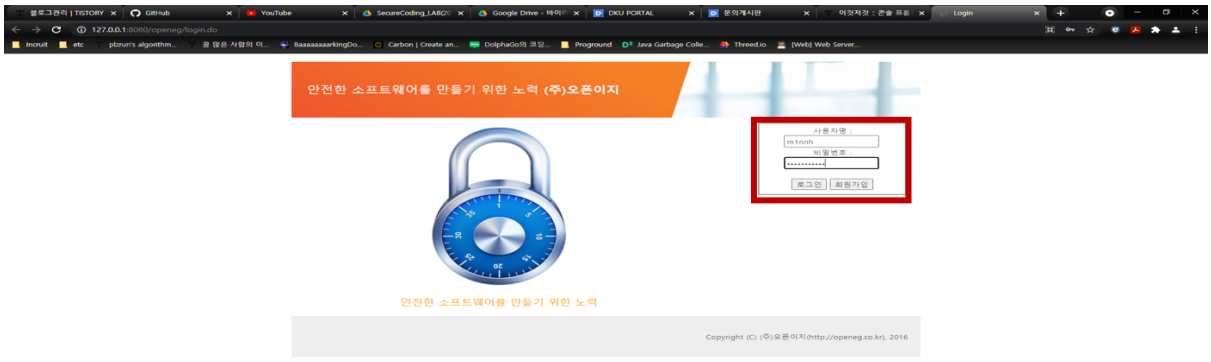
하지만 500번대 에러가 발생하였고, 500번대 에러는 데이터베이스 오류이다. 그래서 현재 내 노트북에 경로에 저장 되어있는 MySQL이 아닌 다른 MySQL이 실행되고 있는 중인 것 같았다.

```
C:₩SecureCoding₩tools₩MySQL5₩bin>.₩mysqld.exe --remove
Service successfully removed.

C:₩SecureCoding₩tools₩MySQL5₩bin>.₩mysqld.exe --install
Service successfully installed.

C:₩SecureCoding₩tools₩MySQL5₩bin>net start mysql
MySQL 서비스를 시작합니다..
MySQL 서비스가 잘 시작되었습니다.
```

그래서 관리자모드로 cmd 창을 열어 기존에 실행 하고 있었던 mysqld.exe 파일을 제거 시켜주었다. 제거 시킨 후 mysqld.exe 파일이 있는 경로로 들어가 설치를 해주고 해당 포트번호를 실행시켰다.

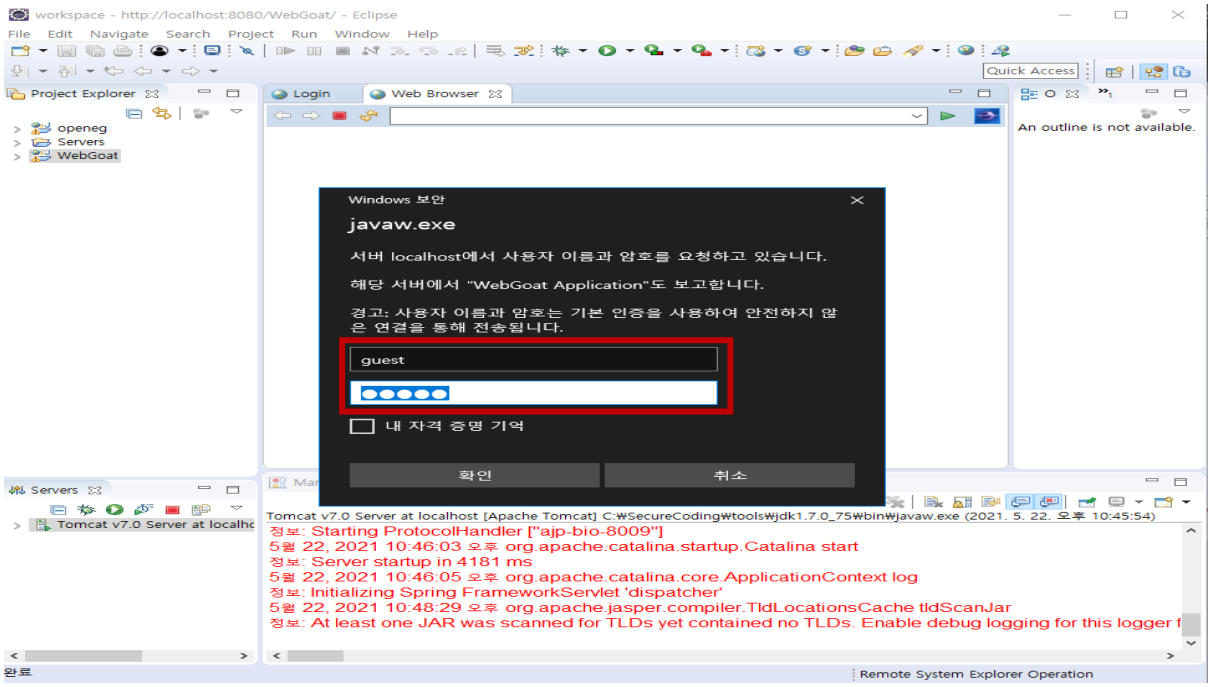


그리고 나서 해당 페이지에서 회원가입을 완료하였다.

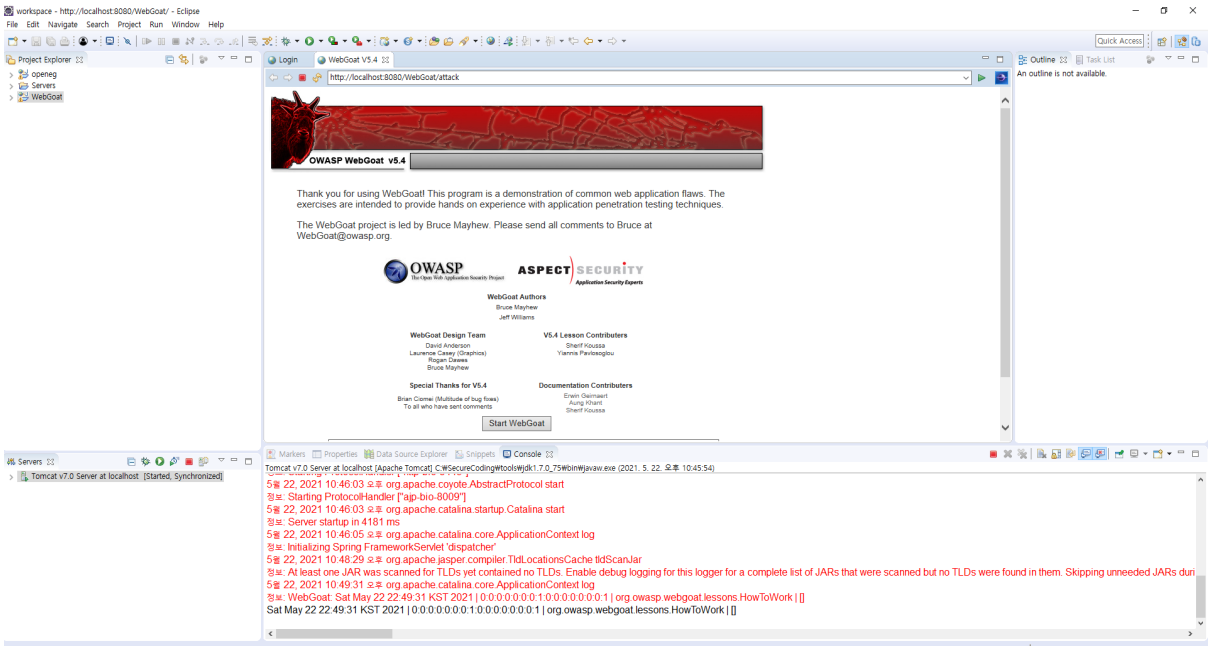


회원 가입 후 웹 브라우저를 통해 접속을 시도하였다.

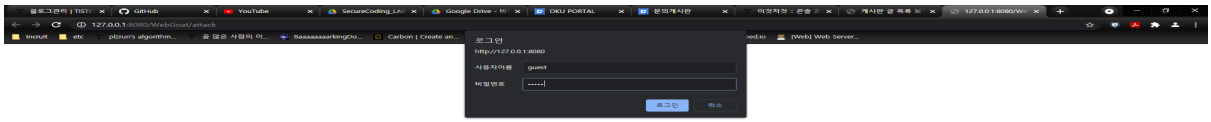
웹 브라우저를 통해서도 접속을 성공하였다.

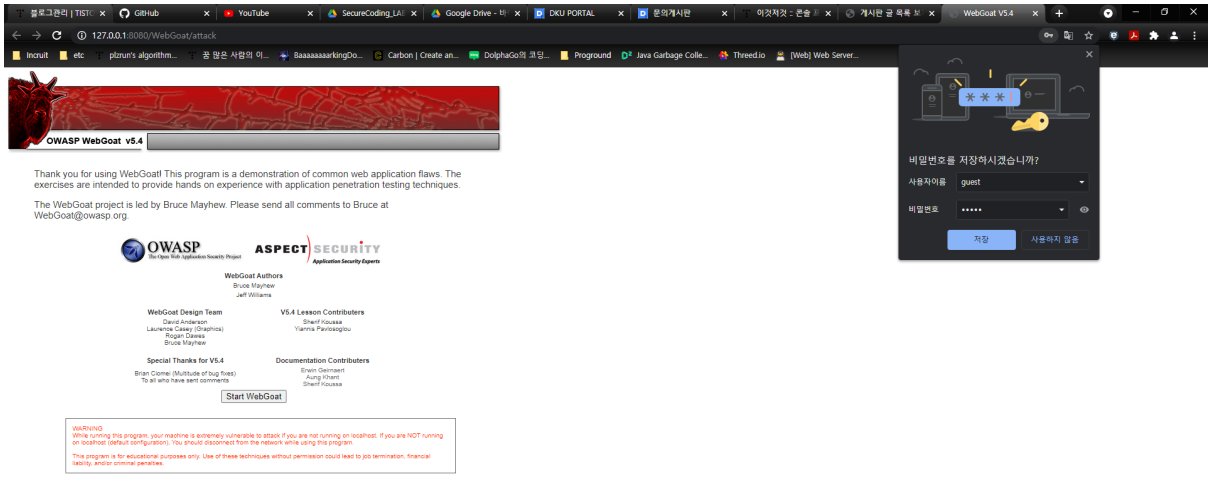


다음은 WebGoat 실행이다. 사진과 같이 eclips에서 guest/guest를 입력하였다.



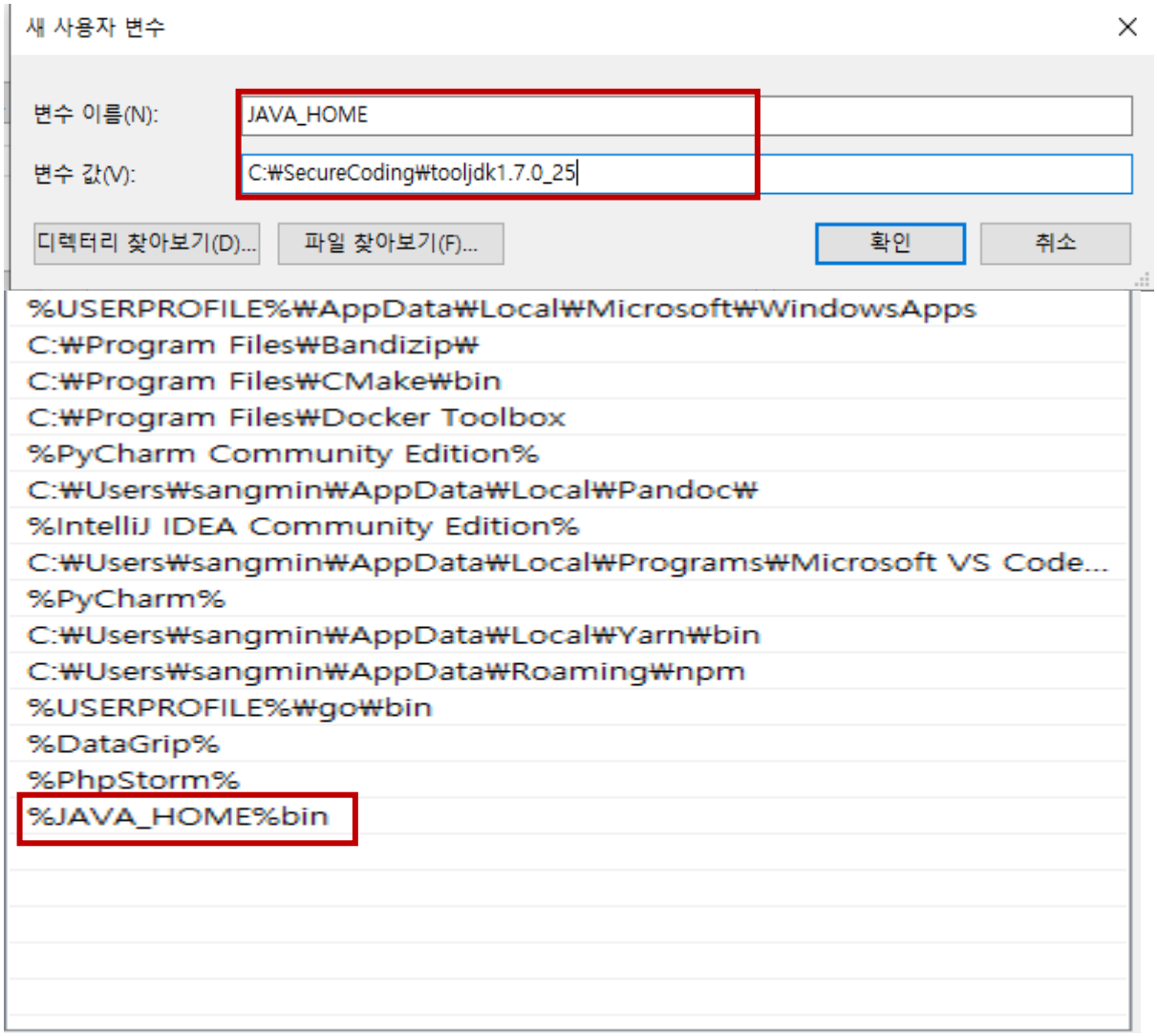
성공한 화면을 볼 수 있었다.



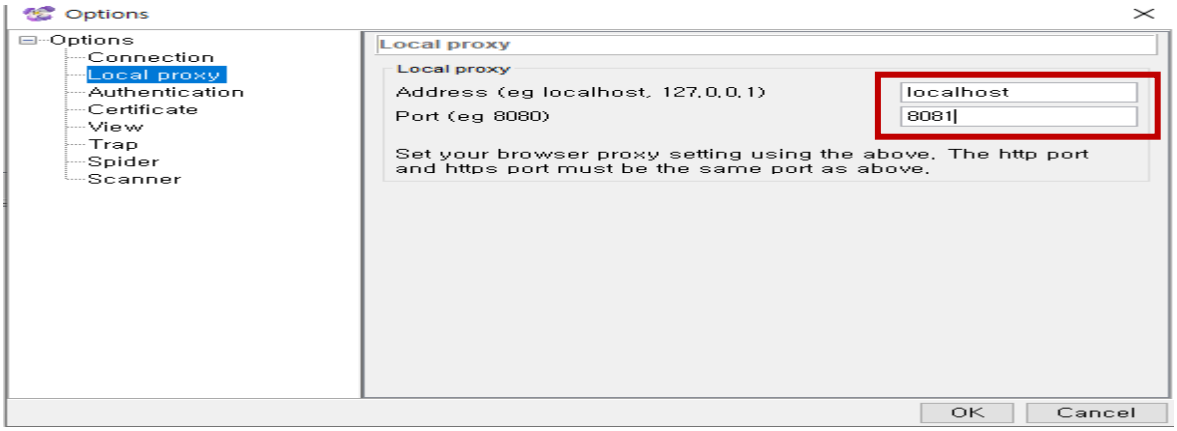


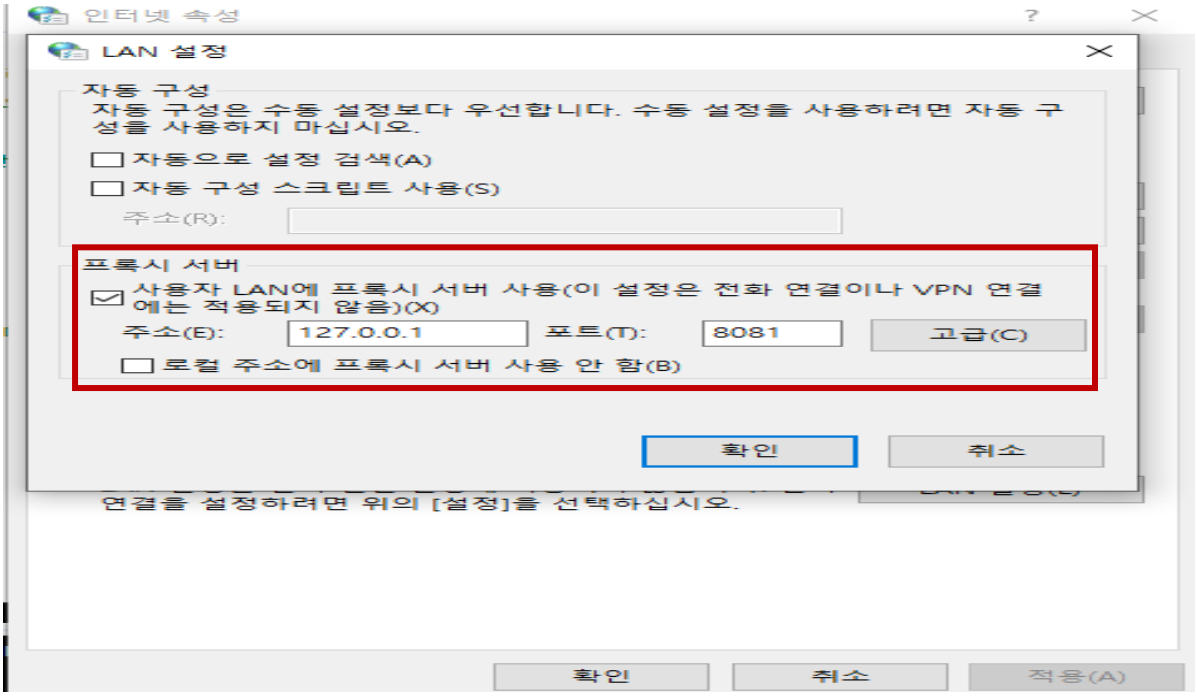
다음은 웹 브라우저를 통한 WebGoat 실행이다. 역시 사진과 같이 성공한 화면을 볼 수 있었다.

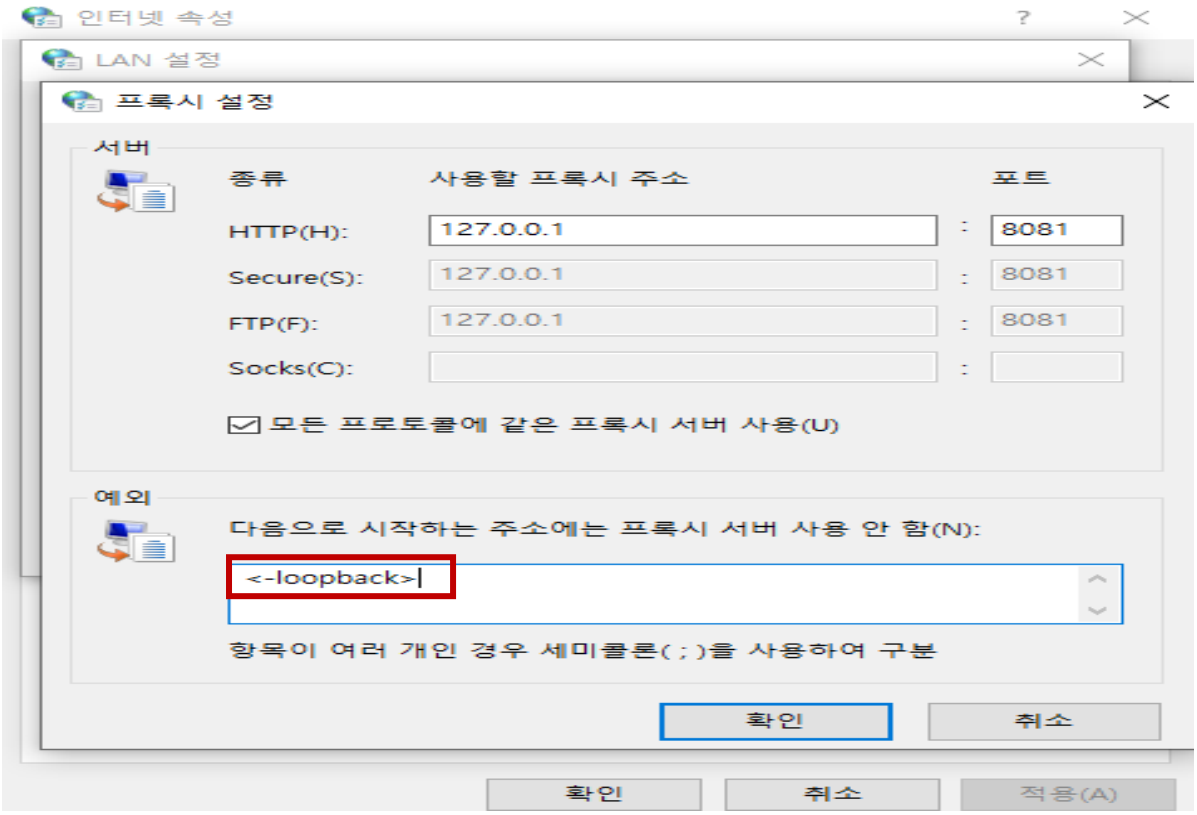
(2). 프록시 툴 설치



Paros를 설치해주고, 환경변수를 다음과 같이 JAVA_HOME 을 만들어 jdk1.7.0_25가 해당하는 경로를 설정 해주었고, 기존에 존재하는 Path 환경 변수에 %JAVA_HOME%₩bin을 추가해주었다.







환경변수 설정 후 Paros에서 프록시 설정을 해주었다.

첫 번째 사진은 Paros -> Tool -> Options -> Local proxy 설정에서 Port 번호를 8081로 설정 해주었다.

두 번째 사진은 제어판 -> 인터넷 옵션 -> 연결 -> LAN 설정 -> 프록시 서버로 들어가 주소와 포트번호를 설정 해주었다.

세 번째 사진은 고급으로 들어가 <-loopback>을 설정 해주었다.

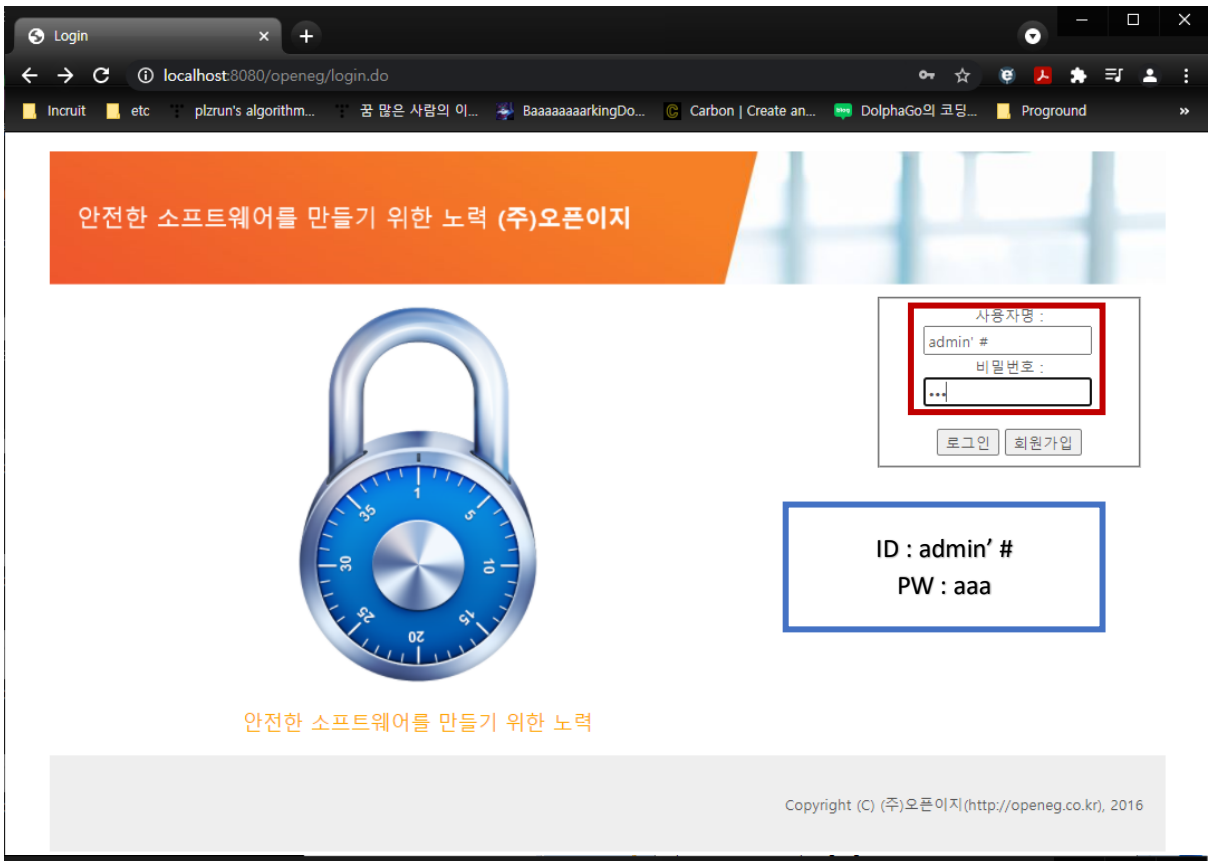
다음은 프록시 툴 동작 확인이다. Openeg를 웹을 통해 접속하고 test/password로 로그인을 시도한 후 프록시 툴을 이용한 데이터 후킹을 살펴봤다.

3. Part 3 : 실습 수행 결과

(1). 비정상적인 입력 값으로 인증 우회 가능성 확인

HTTP Status 500 Error 발생 'too many results' 구문 확인을 하여 정상적인 상황보다 많은 정보를 요청하여 서버가 표시할 수 없다는 의미이다. 우리는 이것을 이용하여 SQL 삽입 공격에 취약한 웹 애플리케이션이라는 것을 확인할 수 있다.

(2). 비정상적인 입력 값으로 인증 우회 확인



이렇게 공격 코드를 삽입하고 관리자 모드로 실행이 가능하다.

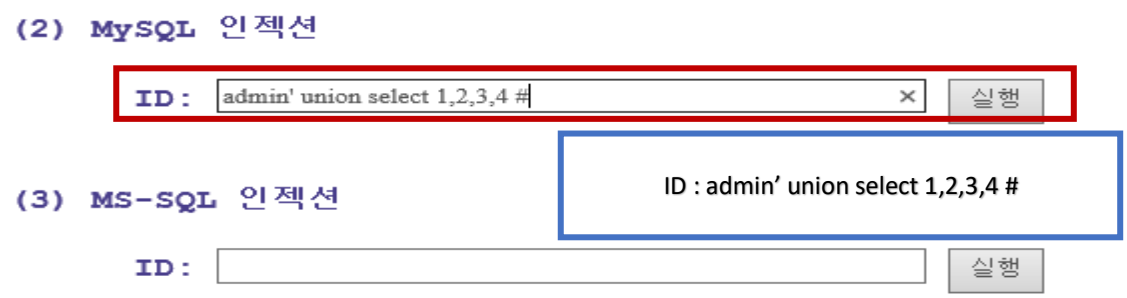
Select * from member where id = 'admin' #' and password='aaa'

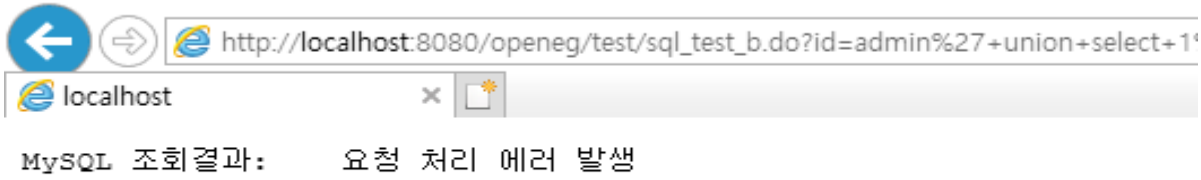
이후의 문자열을 주석으로 처리해 아무 패스워드에 상관 없이 로그인이 가능할 수 있었다.

(3). 정상적인 접근

정상적으로 접근한 것은 IDX, ID, PASSWORD, 이름이 출력 되는 것을 확인 할 수 있다.

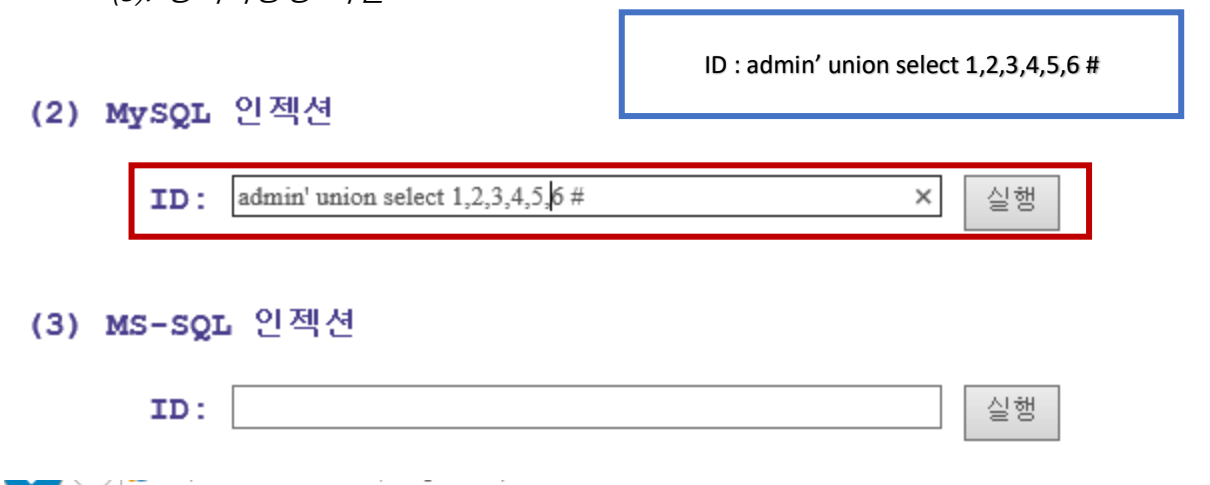
(4). 정상적인 요청 처리

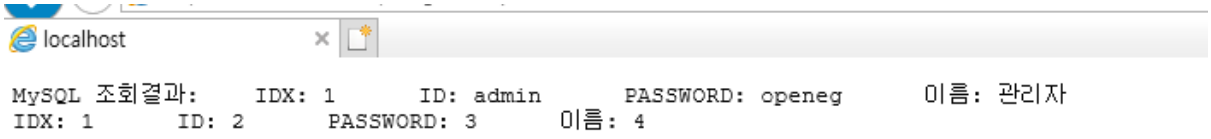




DB에서 사용하고 있는 컬럼의 개수를 확인하는 과정이다.

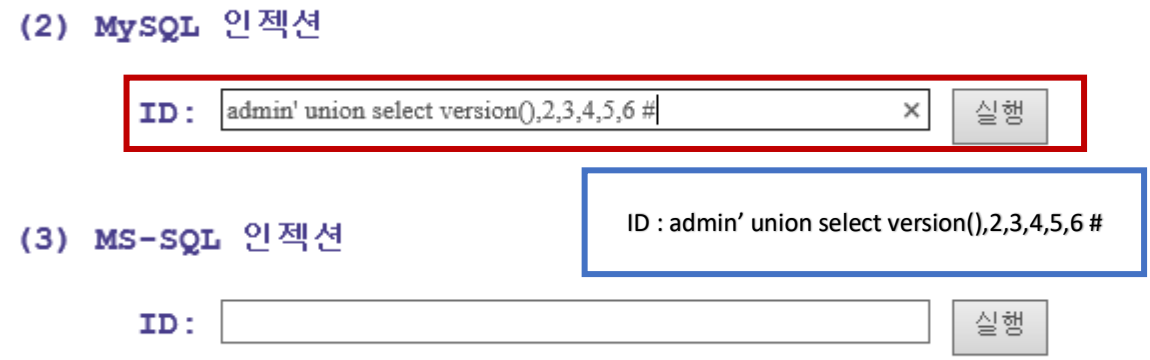
(5). 공격가능성 확인

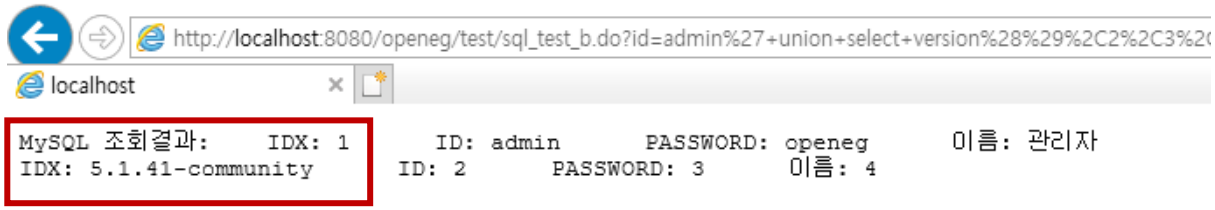




컬럼의 개수가 6일 때 결과를 확인할 수 있다. 따라서 DB의 컬럼 개수는 6개이고 이 컬럼의 개수를 6개로 맞춰주고, 1~4번 컬럼에 악성 쿼리문을 삽입하면 정보 유출이 가능하게 된다.

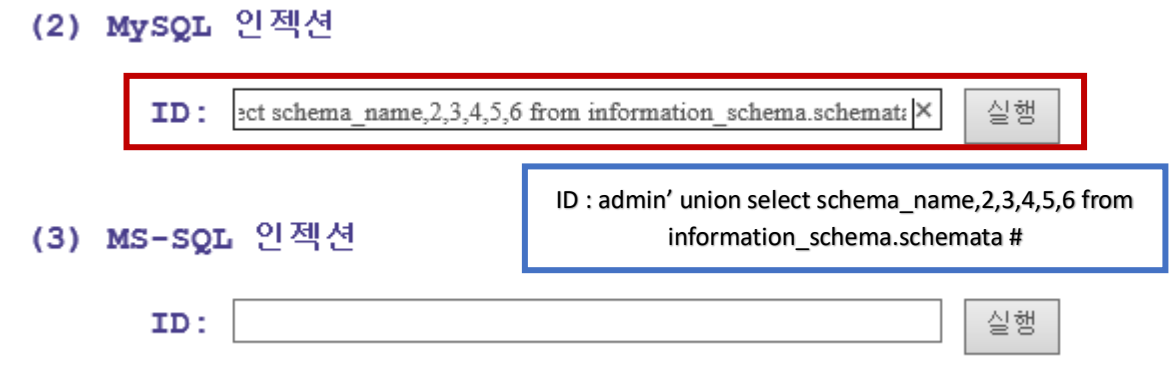
(6). DBMS 버전 확인

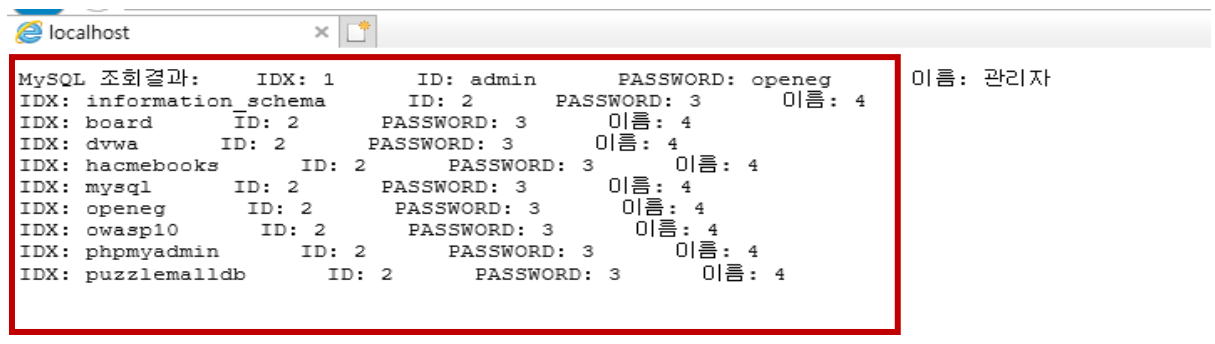




Union select와 버전 키워드를 사용함으로써 해당 DBMS의 버전 정보를 얻어올 수 있다.

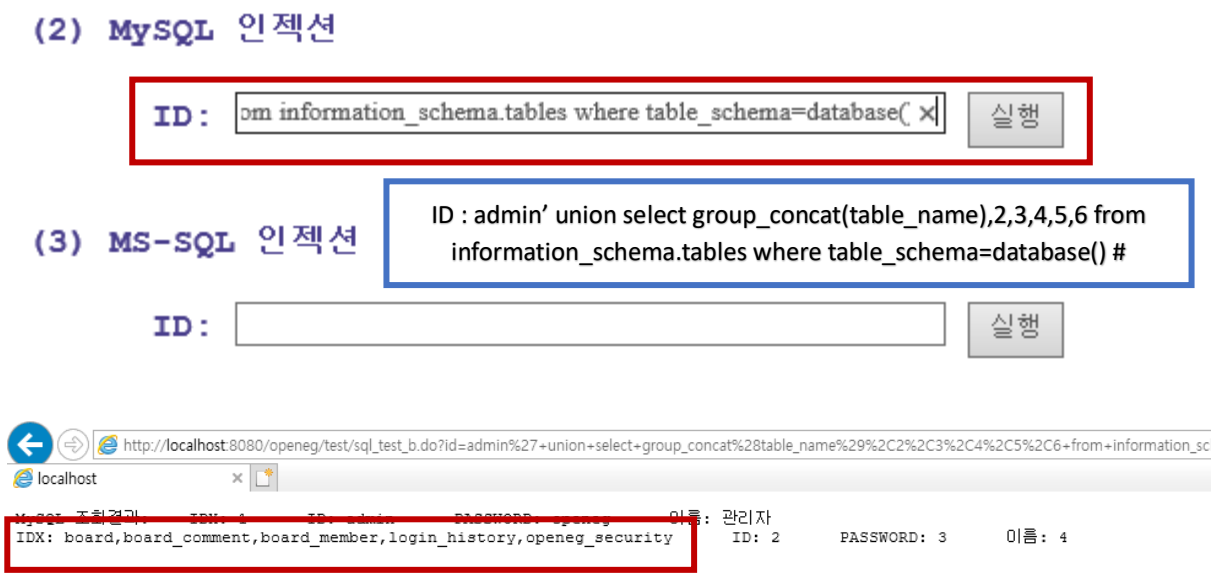
(7). 공격대상 DB목록 확인





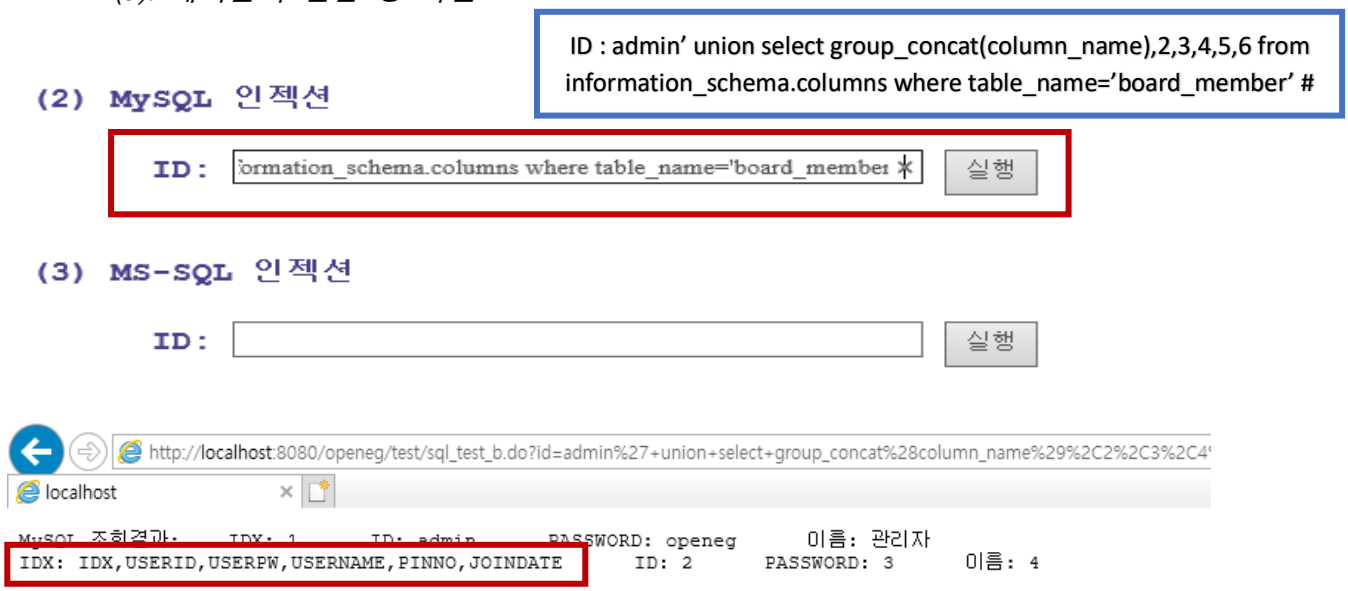
해당 공격 구문을 이용하여 데이터베이스 목록을 확인할 수 있다.

(8). 특정 DB선정 후, 테이블 목록 확인



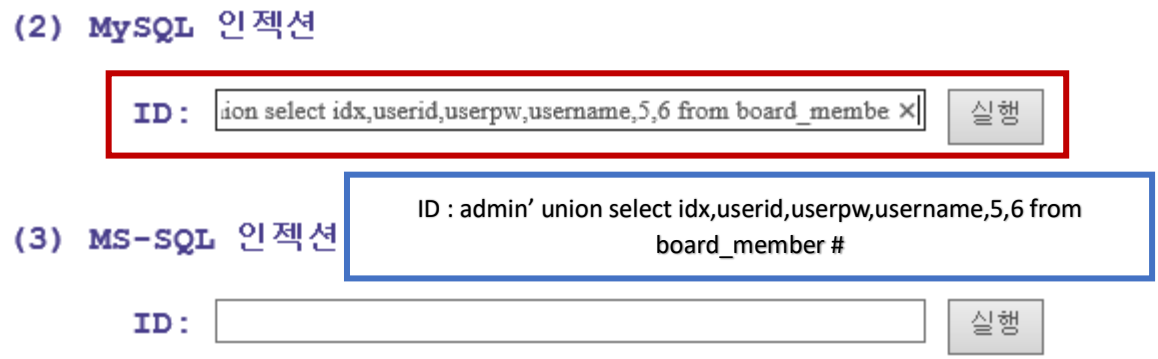
이번 공격을 통해 Information_schema DB에서 현재 사용하고 있는 데이터베이스 테이블 목록을 확인할. 수 있다.

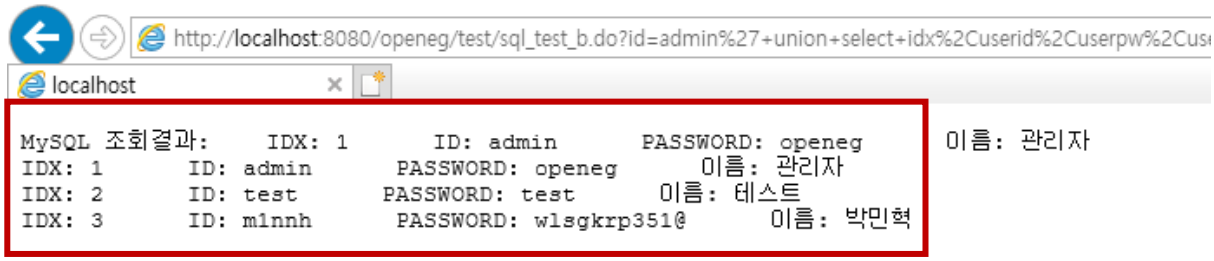
(9). 테이블의 컬럼 명 확인



이번 공격을 통해 board_member table의 컬럼명을 확인할 수 있다.

(10). 컬럼 데이터 추출





순차적인 공격을 통해 컬럼 데이터를 추출할 수 있다.

(11) 실습 환경