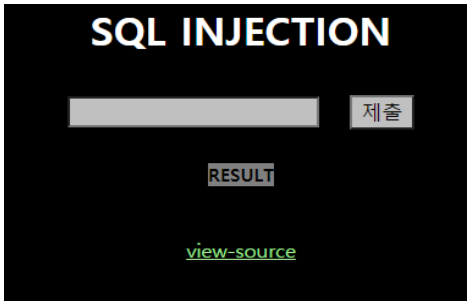
[5주차 웹해킹 과제_김수현]

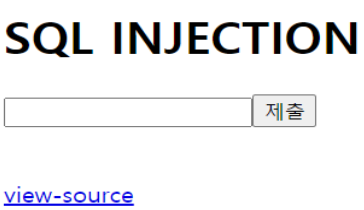
18번)




```php
<?php
  if($_GET['no']){
  $db = dbconnect();
  if(preg_match("/#|select|₩(| ||limit|=|0x/i",$_GET['no'])) exit("no hack");
  $r=mysqli_fetch_array(mysqli_query($db,"select id from chall27 where id='guest' and no={{$_GET['no']}}")) or die("query error");
  if($r['id']=="guest") echo("guest");
  if($r['id']=="admin") solve(27); // admin's no = 2
}
?>
```

18번 문제는 일단 view-source를 통해서 소스코드를 먼저 살펴보았다. 항상 웹 해킹을 할 때는 php로 시작하는 코드부분을 중심으로 봐야 한다는 것을 알았기 때문에 그 부분부터 살펴보았다. 사실 코드를 봤을 때는 무슨 말인지는 잘 모르겠지만 일단 알 수 있는 건 $result의 id의 값이 guest이고, $no에는 $_GET['no']에 알맞은 id값을 넣어줘야 한다는 것을 알았다. 또한 주석으로 admin's no = 2라고 되어있는데, 이 사실을 어떻게 활용해야 될 지 모르겠다. 그리고 마지막에 id에 admin을 입력해야 문제 18번이 풀리는 것을 알겠는데, 도저히 어떤 방식으로 접근해야 되는지 또한 모르겠다.

27번)




```php
<?php
 if($_GET['no']){
   $db = dbconnect();
   if(preg_match("/ |₩/|₩(|₩)|₩||&|select|from|0x/i",$_GET['no'])) exit("no hack");
   $result = mysqli_fetch_array(mysqli_query($db,"select id from chall18 where id='guest' and no=$_GET[no]")); // admin's no = 2

   if($result['id']=="guest") echo "hi guest";
   if($result['id']=="admin"){
     solve(18);
     echo "hi admin!";
   }
 }
?>
```

사실 27번 문제 또한 18번 문제와 비슷한 문제라고 생각이 들었다. Id의 값이 guest이고, id의 값이 admin으로 바꿔주어야 문제가 풀리는 것 같다. 위의 문제와 같이 주석에서 admin's no = 2라고 알려주어서 한번 정답창에다가 no=2를 입력해보았다. 그랬더니 no back이라는 문구가 뜨면서 오류가 났다. 다시 2 만 입력해보았는데 querry error가 떴다. 그리고 1을 입력했더니 guest라는 문구가 떴다. 뭔가 guest의 no 값이 1인 것 같은데 그 다음을 잘 모르겠다.