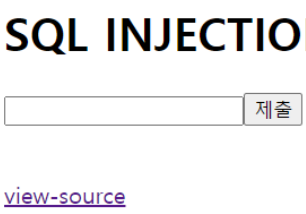
[Webhacking.kr] old-27



챌린지를 눌러보면 이렇게만 나온다. View-source를 누르면 소스 코드가 나온다.

```
<?php
  include "../../config.php";
  if($_GET['view_source']) view_source();
?><html>
<head>
<title>Challenge 27</title>
</head>
<body>
<h1>SQL INJECTION</h1>
<form method=get action=index.php>
<input type=text name=no><input type=submit>
</form>
<?php
  if($_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
}
?>
<br><a href=?view_source=1>view-source</a>
</body>
</html>
```

이중에서 SQL 인젝션과 관련이 있어보이는 부분만 자세히 살펴보았다.

```
<?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
}
?>
```

- **if($_GET['no']):** 클라이언트가 no 파라미터를 제공하면 다음 로직을 실행한다.
- **$db = dbconnect();:** 데이터베이스에 연결한다.
- **preg_match(...):** 정규 표현식을 사용해 클라이언트가 제공한 no 값에서 특정 문자열 패턴이 있는지 확인한다. 이 문자열에는 #, select, (, 공백, limit, =, 0x 이 포함되는데, 이 문자열들이 발견되면 exit("no hack")을 실행해, 즉시 스크립트를 중단하고 "no hack" 메시지를 출력한다. 즉 위에 나열된 문자들을 쿼리문에 쓰지 않고 문제를 해결해야 한다.

- **SQL 쿼리: mysqli_query($db, "select id from chall27 where id='guest' and no=({$_GET['no']})")**

  사용자가 입력한 no 값을 기반으로 chall27 테이블에서 id='guest'인 레코드를 조회하는 SQL 쿼리를 실행한다.

- **if($r['id']=="guest") echo("guest");:** 결과로 guest의 ID를 찾으면 "guest" 메시지를 출력한다.

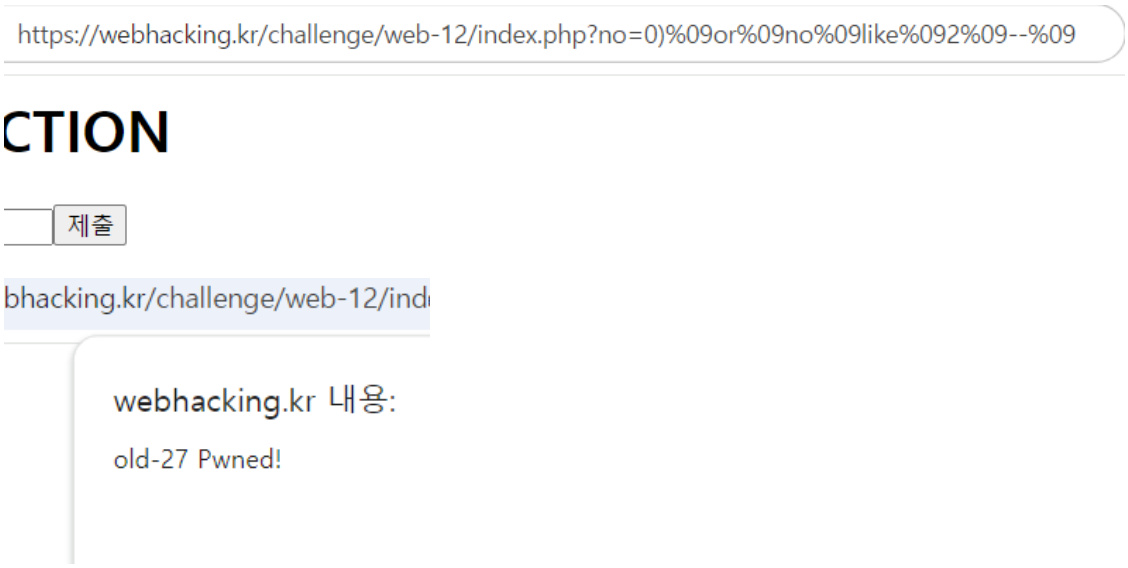
- **if($r['id']=="admin") solve(27);:** admin ID를 찾으면 solve(27) 함수를 호출하여 문제를 해결한다. 이 문제에서 admin의 no는 2라고 주석에 적혀 있다.

즉 우리는 no에 기존에 적힌 값을 무시하고 admin의 no인 2를 넣어주어야 한다.

이런 문제들은 주석처리 등을 이용해 풀어왔지만 이 문제에서는 preg_match 부분 때문에 =, #을 사용하지 못하므로 like, -- 등을 대신 사용해야 한다.

따라서 no의 값을 2로 조작하기 위해 no=0) or no like 2-- 과 같은 쿼리문을 넣어주어야 한다. 이 조건문의 경우 기존 쿼리의 조건이 false(즉, 0)로 무효화되지만, 뒤에 붙는 OR 조건이 참이 될 경우 쿼리가 실행될 수 있게 한다. 이후 뒤의 die 부분을 주석으로 처리한다. 즉 no 필드에 2가 포함된 행을 반환하게 한다.

쿼리문을 url의 get 형식으로 보내므로 기존의 공백 대신 url 필터링 문자를 넣어야 한다. 결과적으로는 no=0)%09or%09no%09like%092%09--%09과 같은 형태가 된다. (주석 처리도 --뒤에 공백을 넣어주어야 한다고 한다) 이렇게 입력하면 쿼리문이 "select id from chall27 where id='guest' and no=(0)%09or%09no%09like%092%09--%09~~")) or die("query error");~~와 같은 형태가 된다고 할 수 있다.



url뒤에 index.php?를 입력한 후 쿼리문을 입력해주면 이렇게 문제를 해결 할 수 있다.