webhacking.kr 39번문제

Xero

박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

2016-04-01

Email: wnsgurzxc@naver.com

Facebook: https://www.facebook.com/wnsgurzxc

제출 칸과 버튼만 보인다.

제출

소스를 보면 index.phps를 가리킨다.

Index.phps로 들어가면 소스는 다음과 같다.

```
$pw="????";
if($_POST[id])
{
$_POST[id]=str_replace("\\","",$_POST[id]);
$_POST[id]=str_replace("'","''",$_POST[id]);
$_POST[id]=substr($_POST[id],0,15);
$q=mysql_fetch_array(mysql_query("select 'good' from zmail_member where id='$_POST[id]"));
if($q[0]=="good") @solve();
}
?>
```

₩를 없애고, '를 "로 만든다.

그리고 15자리만 가져온다.

쿼리문을 보면 id='\$ POST[id] 부분에 뒤쪽 닫는 싱글 쿼터가 없다.

'를 "로 바꾸고 15자리에서 끊는 걸 이용해서 다음과 같이 값을 보냈다.

1 '

위와 같이 보내면 "가 되고 15자리에서 끊기므로 쿼터가 생겨서 쿼리문이 제대로 작동할 것이다.

정상작동하고 클리어되었다.

You have cleared the 39 problems.

Score + 100