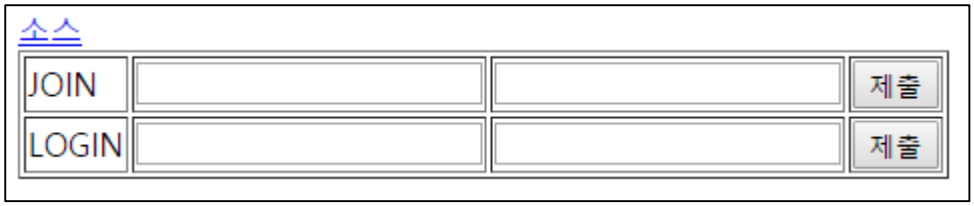
webhacking.kr 59번문제

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

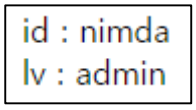
다음과 같은 창이 보인다.



소스를 눌러서 index.phps로 가면 다음과 같은 소스가 있다.

```
<?
if($_POST[lid] && $_POST[lphone])
{
$q=@mysql_fetch_array(mysql_query("select id,lv from c59 where id='$_POST[lid]' and
phone='$_POST[lphone]'"));
if($q[id])
{
echo("id : $q[id]<br>lv : $q[lv]<br><br>");
if($q[lv]=="admin")
{
@mysql_query("delete from c59");
@clear();
}
echo("<br><a href=index.php>back</a>");
exit();
}
}
if($_POST[id] && $_POST[phone])
{
if(strlen($_POST[phone])>=20) exit("Access Denied");
if(eregi("admin",$_POST[id])) exit("Access Denied");
if(eregi("admin|0x|#|hex|char|ascii|ord|from|select|union",$_POST[phone])) exit("Access
Denied");
@mysql_query("insert into c59 values('$_POST[id]',$_POST[phone],'guest')");
}
?>
```

join부분의 phone부분에 SQL Injection을 하면 될 것 같다.
reverse를 이용해서 1,reverse(id)),(1,1 라는 쿼리를 만들었다.
그러면 nimda라는 id가 admin lv을 갖게 될 것이다.
id에 nimda를 넣고 phone에 1,reverse(id)),(1,1을 넣고 Join하고 nimda / 1로 로그인하면 다음과 같이 로그인이 된다.



클리어