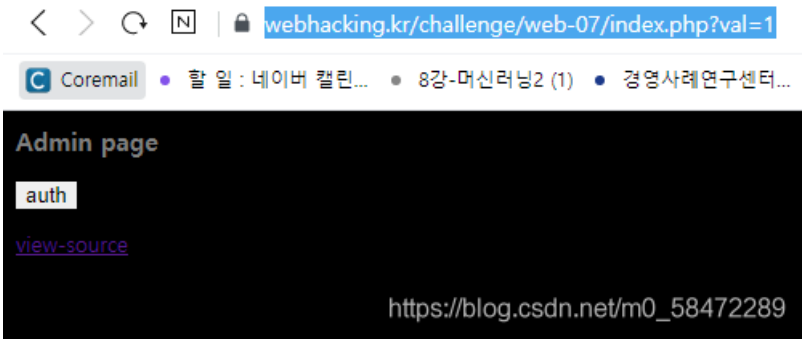
# 【Web】Webhacking.kr旧版第七题

原创

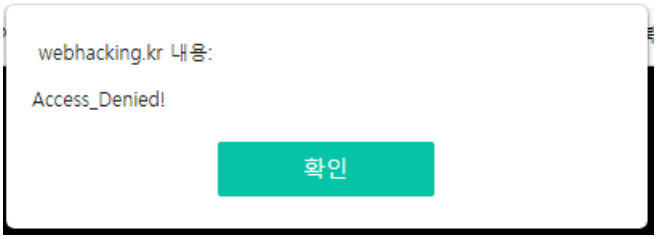
juminxiu 于 2021-06-12 00:49:29 发布 82 收藏
分类专栏： 信息安全（Information Security） 文章标签： 网络安全



积分：30




进题后只能看到一个auth的按钮。连COOKIE里也没有什么东西。但有个val变量的GET。




直接按auth的话他会告诉我Acess Denied！按view-source来看看后台的源码。

```php
<?php
  include "../../config.php";
  if($_GET['view_source']) view_source();
?><html>
<head>
<title>Challenge 7</title>
</head>
<body>
<?php
$go=$_GET['val'];
if(!$go) { echo("<meta http-equiv=refresh content=0;url=index.php?val=1>"); }
echo("<html><head><title>admin page</title></head><body bgcolor='black'><font size=2 color=gray><b>
<h3>Admin page</h3></b><p>");
if(preg_match("/2|-|₩+|from|_|=|₩₩s|₩+|₩//i",$go)) exit("Access Denied!");
$db = dbconnect();
$rand=rand(1,5);
if($rand==1){
  $result=mysqli_query($db,"select lv from chall7 where lv=($go)") or die("nice try!");
}
if($rand==2){
  $result=mysqli_query($db,"select lv from chall7 where lv=(($go))") or die("nice try!");
}
if($rand==3){
  $result=mysqli_query($db,"select lv from chall7 where lv=((($go)))") or die("nice try!");
}
if($rand==4){
  $result=mysqli_query($db,"select lv from chall7 where lv=(((($go))))") or die("nice try!");
}
if($rand==5){
  $result=mysqli_query($db,"select lv from chall7 where lv=(((((($go)))))") or die("nice try!");
}
$data=mysqli_fetch_array($result);
if(!$data[0]) { echo("query error"); exit(); }
if($data[0]==1){
  echo("<input type=button style=border:0;bgcolor='gray' value='auth' onclick=₩"alert('Access_Denied!')₩"><p>");
}
elseif($data[0]==2){
  echo("<input type=button style=border:0;bgcolor='gray' value='auth' onclick=₩"alert('Hello admin')₩"><p>");
  solve(7);
}
?>
<a href=./?view_source=1>view-source</a>
</body>
</html>
```

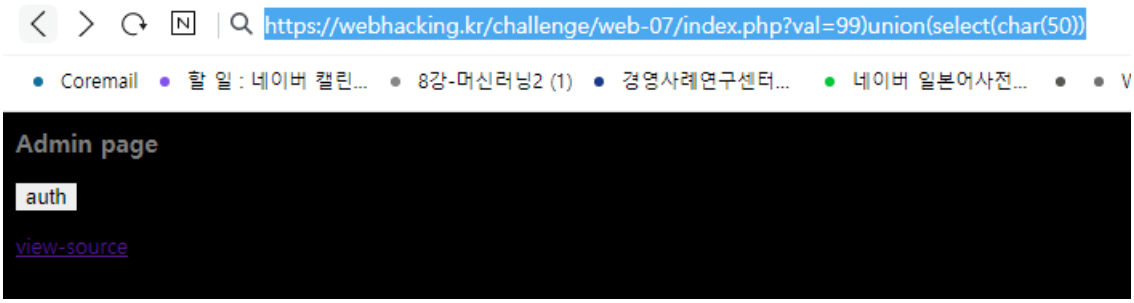


中间有一个以随机的seed驱动的跟switch-case差不多的构造。最后要求我们把“2”这个数值注入到系统。上面还有filtering，那明显就是个SQLi。

其实rand随机到2、3、4、5的话我们都可以pwn。因为为了用上union，我们前面至少需要两个左括号。因为会自动把字符串parse到数值，并且我们无法直接用2，所以我们要用ASCII来替换一下。结果我们可以得到这段代码。

```
99)union(select(char(50))
```

用GET发过去的话既可以得到答案。




成功页面