i春秋GetFlag

转载

weixin_30701575 于 2019-08-14 00:42:00 发布 256 收藏
文章标签： php python
原文链接：http://www.cnblogs.com/wosun/p/11349506.html

进去是个提示界面，提示我们这是个迷你文件管理系统，我们需要登录然后下载文件再获得flag。

然后我们查看源码，没什么信息，点login进去查看源码，没什么信息

下方出现了一个substr(md5(captcha), 0, 6)=7619f5

然后下面有个Captcha:的输入框，每次刷新captcha也会变化。貌似这个captcha会一直变化，类似于验证码一类的东西。

然后分析这个captcha，他是先对captcha进行md5加密，然后输出其前六位。这里我们需要破解这个获取正确的captcha。

这里附上一个dalao的python脚本。链接：https://www.cnblogs.com/leixiao-/p/9785148.html

```
import requests
import base64
import sys
import hashlib

def getMd5(index):
    for i in range(100000,100000000):
        x = i
        md5 = hashlib.md5(str(x).encode("utf8")).hexdigest()
        if md5[0:6] == index:
            return x;
print(getMd5("7619f5"))
```

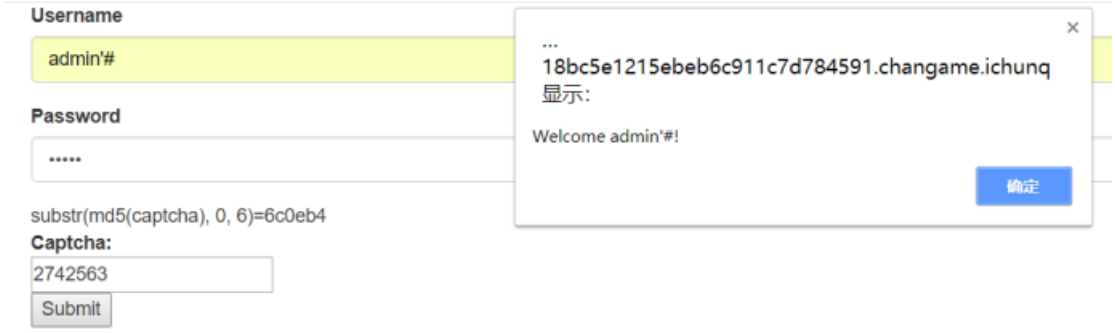
直接跑一下就得到captcha的值了（大概一分钟的样子），其中getMd5的值是你自己的substr(md5(captcha), 0, 6)=7619f5的值

然后就可以尝试登录了（这个必须要先搞定captcha，不然我们的输入没用）

这里试试admin，admin’，admin”，admin#

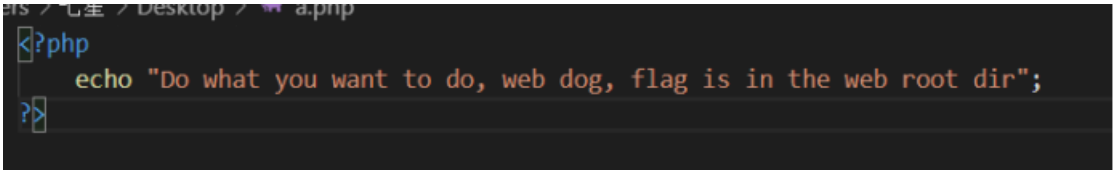
发现admin’#会爆出error

再试试admin'#就成功登录了。（密码随意）



进去后里面有三个文件，不用说，全部下载（点超链接）下来试试

一次打开，发现两个txt就是忽悠我们的，有用的是那个php文件



提示我们flag在web root dir（web根目录）

所以我们就想办法去查看根目录文件，既然这里可以下载普通的文件就应该可以通过这种方式下载根目录的文件

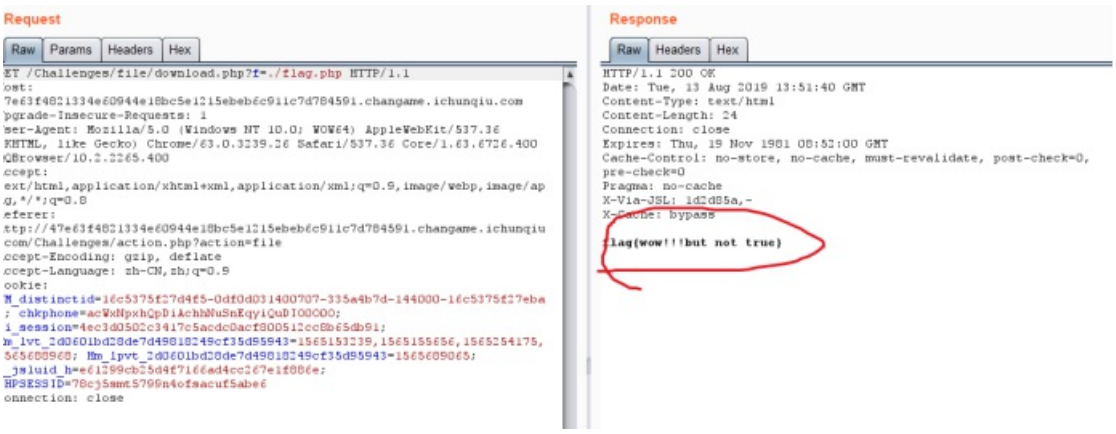
看url，里面没有什么奇怪的传入，再抓包试试，没什么特别的地方，打开抓包，点超链接试试

发现GET处是文件id查询的形式，所以这里应该就可以从这里查看到根目录文件

不多说，传入repeater中go一遍，发现response下面会直接显示文件内容

所以这里就可以直接查看文件了，试试flag.php，./flag.php

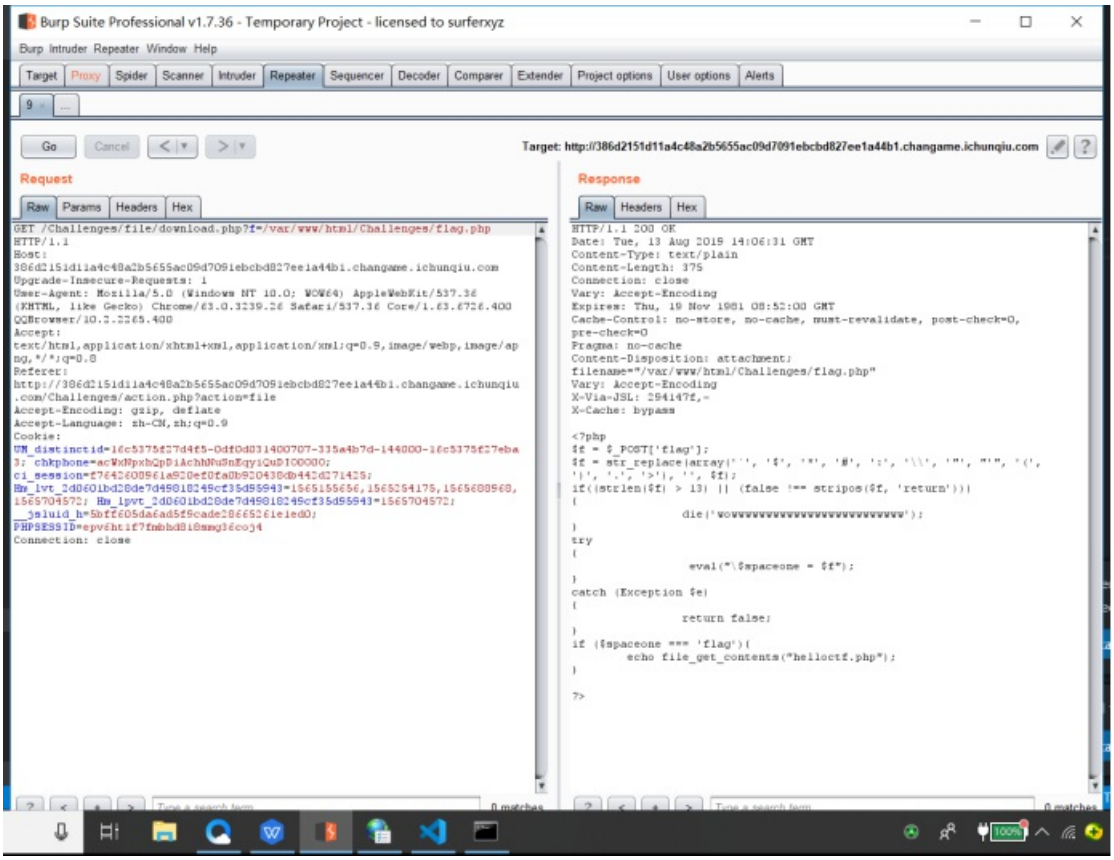
发现f=./flag.php时会给出提示

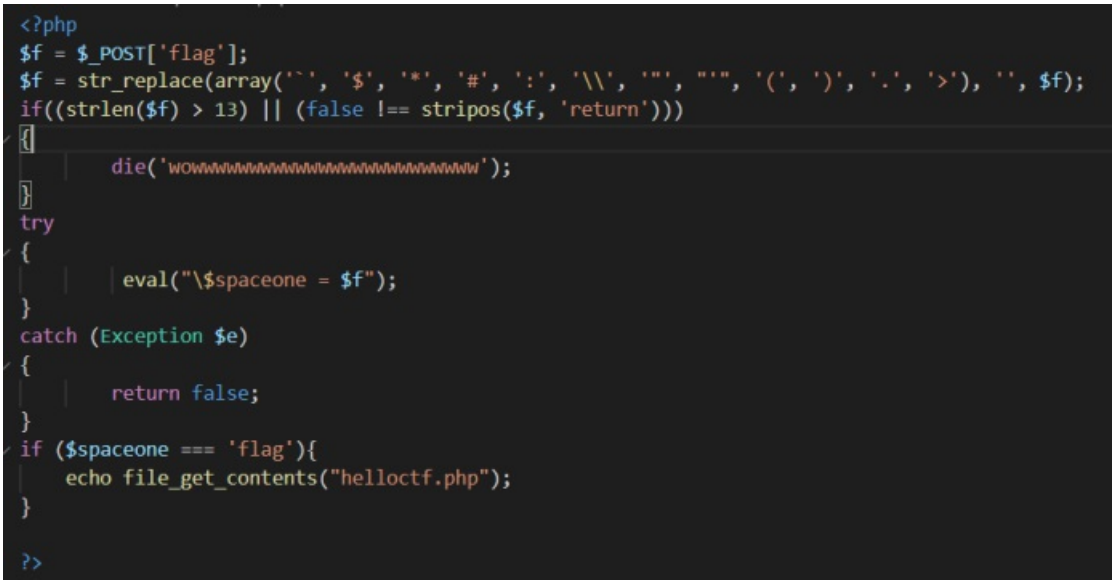


再试了试././flag.php也没有用。。。。./././flag.php也没用，看来这里不能用目录缩写来跳过，只能输入正确的根目录

而一般的根目录是/var/www/html/，所以这里试试/var/www/html/flag.php，不行

再试试/var/www/html/Challenges/flag.php就看到一大堆提示获取flag的php代码





分析代码：

1.定义一个变量f，其值是表单中传入的flag值

2.把变量f中的`，$,*,#,:,\\,'',',(,),.,>符号全部转换为' '

3.如果f的长度大于13或则f中有return就输出wowwwwwwwww并退出

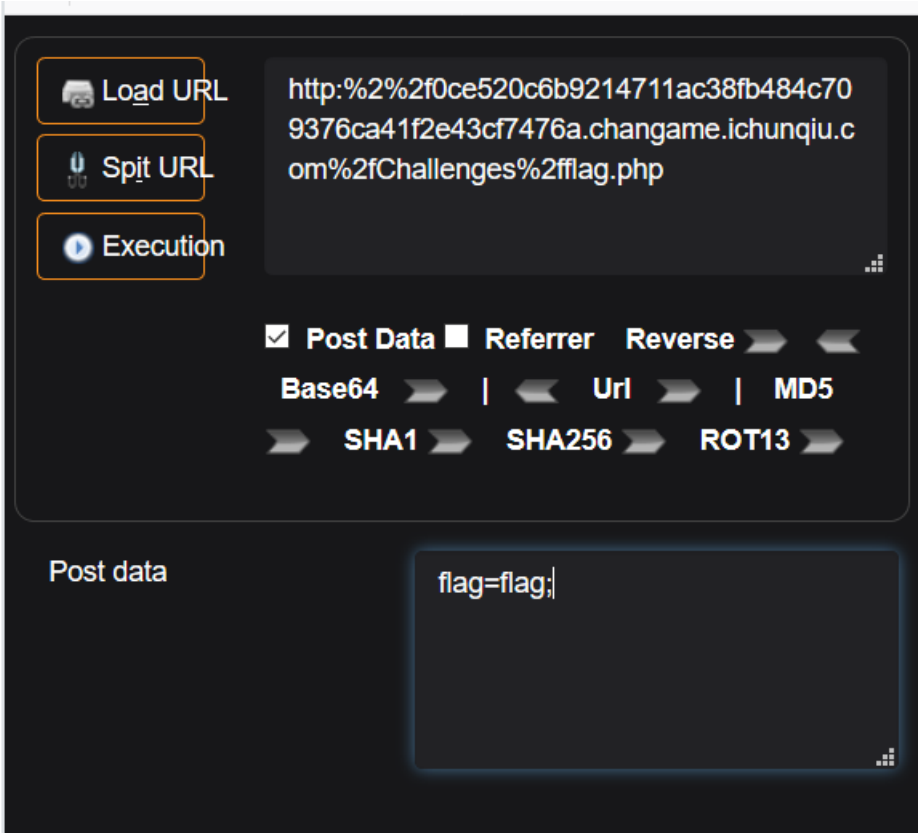
4.如果触发异常（f的字符等于spaceone的）会返回false

5.如果spaceone的值等于flag这个字符串就输出helloctf.php文件的内容

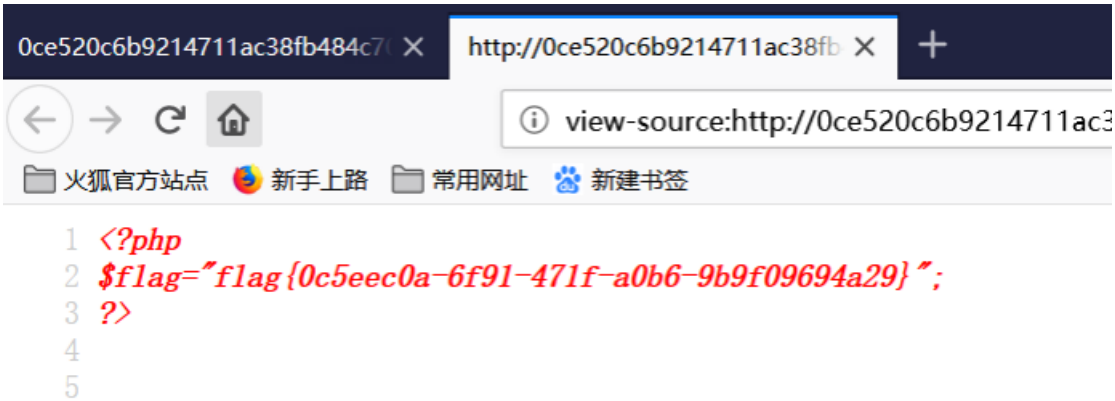
所以这里如果让spaceone等于flag就行了，且f不等于flag。

构造post：flag=flag;这里让flag等于flag;就使用;巧妙的避开了不等于spaceone

使用firefox的插件进行传值



页面会出现白色的跳转，所以这里直接查看源码得到flag（被注释了）



转载于:https://www.cnblogs.com/wosun/p/11349506.html