i春秋——“百度杯”CTF比赛 十月场——GetFlag（md5碰撞、文件包含、网站绝对路径）...

转载

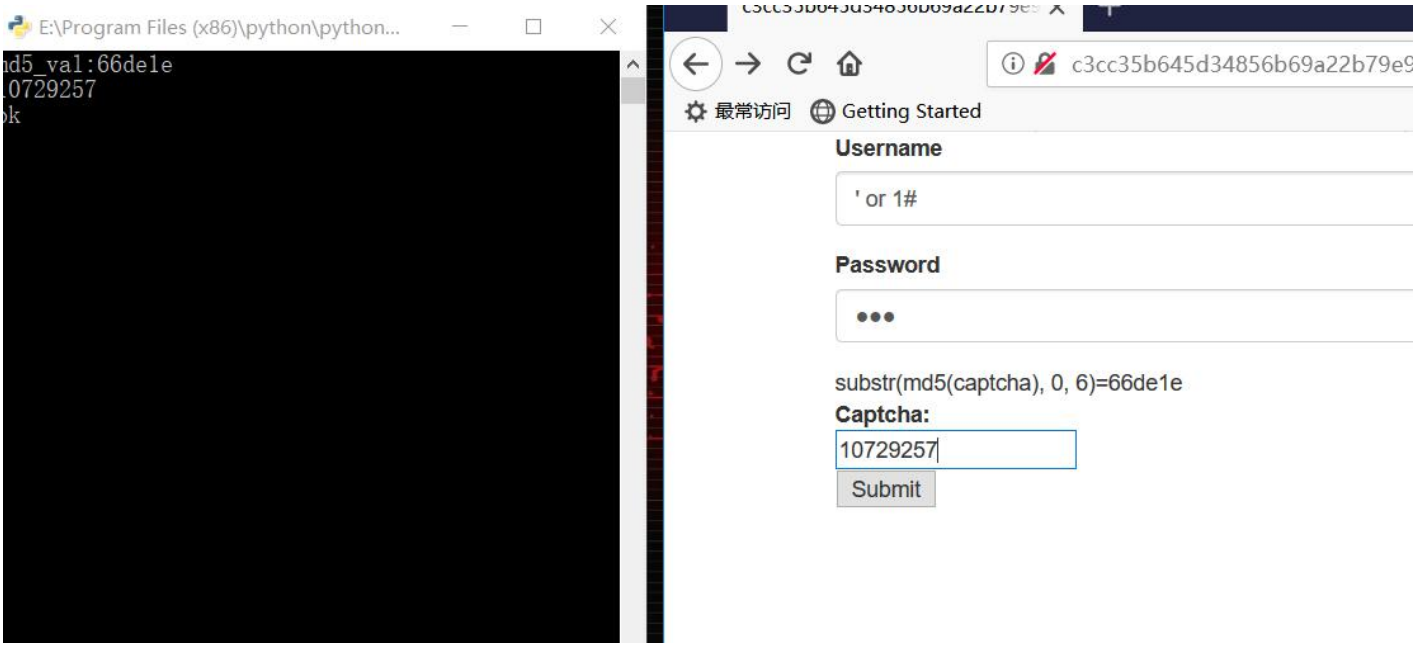
weixin_30475039 于 2018-10-14 09:39:00 发布 152 收藏
文章标签： php
原文链接：http://www.cnblogs.com/leixiao-/p/9785148.html

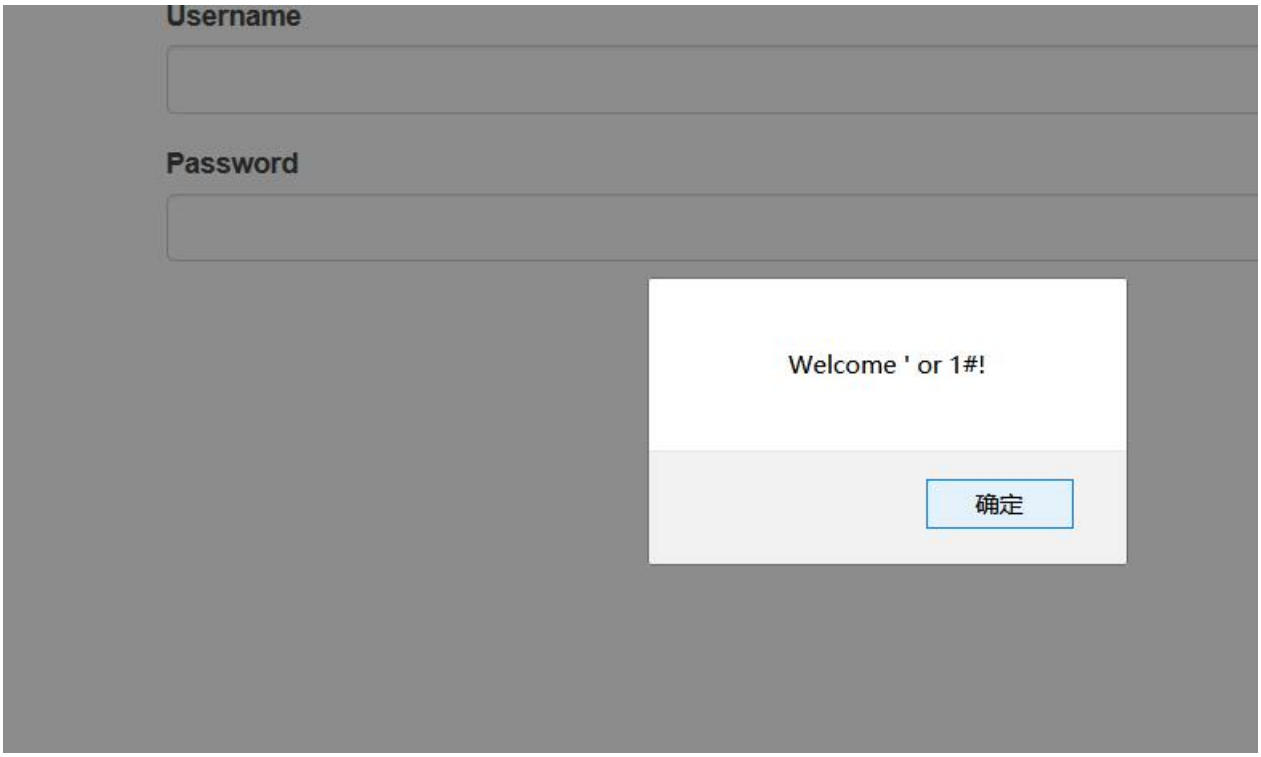
需要提交的captcha满足等式，肯定就是MD5碰撞了

附上脚本

```
import hashlib


def func(md5_val):
    for x in range(1,100000000):
        md5_value=hashlib.md5(str(x)).hexdigest()
        if md5_value[:6]==md5_val:
            return str(x)


print func(raw_input('md5_val:'))


raw_input('ok')
```

尝试后发现登录处存在sql注入，于是用 ' or 1# 登录

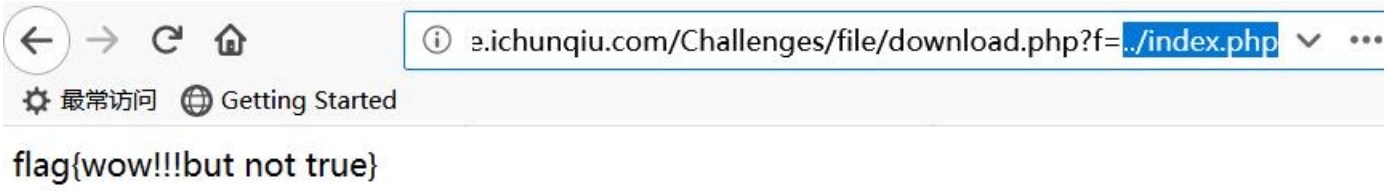




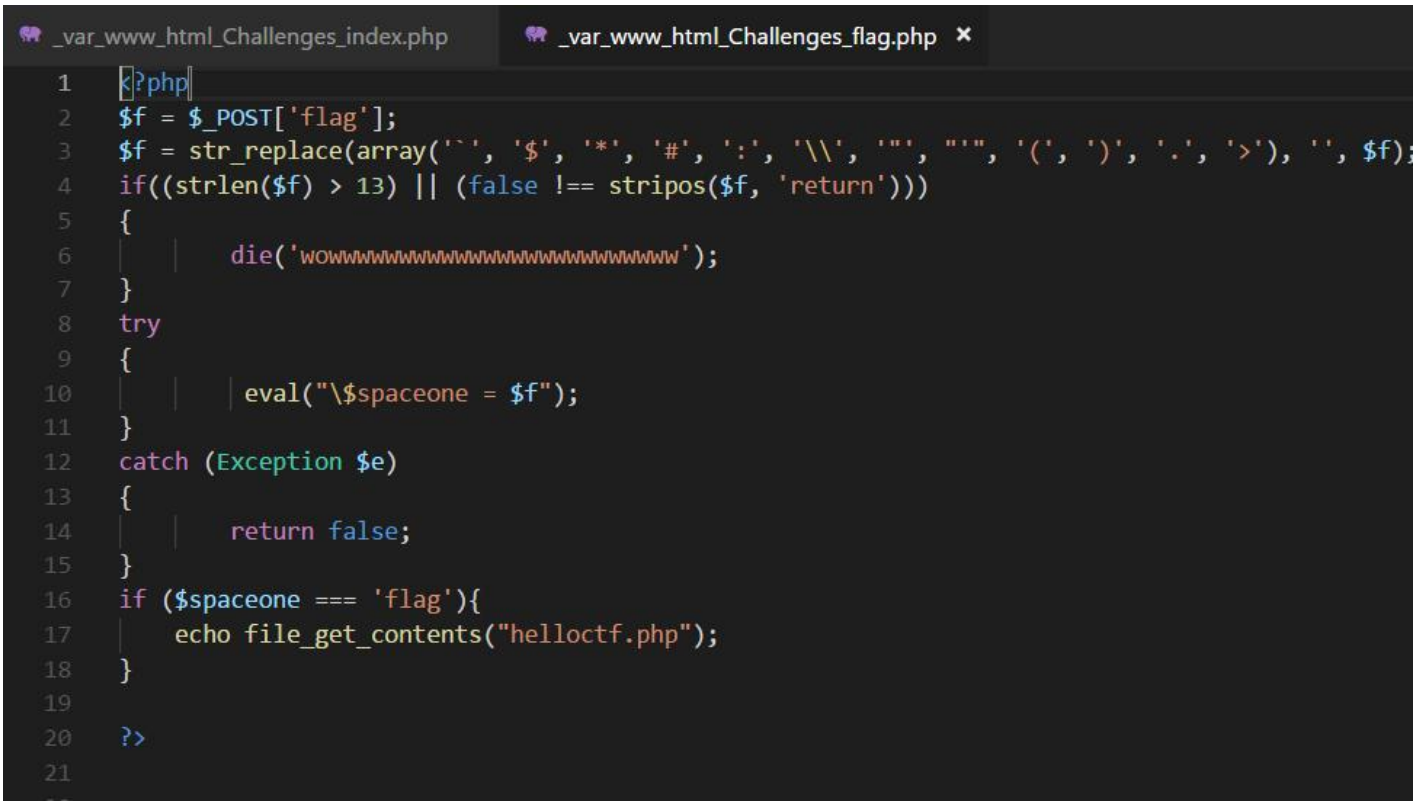
1. hello.txt
2. s.txt
3. a.php

看了下下载的几个文件发现都没有什么用，不过这个下载链接让我想到了文件包含/Challenges/file/download.php?f=

尝试读取index.php,构造../inedx.php,但是发现只要文件名包含 任意字符+斜杠 都会提示 flag{wow!!!but not true}，看来是屏蔽了目录穿越，多次尝试绕过无果，后来看了眼其他wp，这里并没有屏蔽斜杠，所以还可以用绝对路径，通过返回的header " X-Powered-By: PHP/5.5.9-1ubuntu4.19 " 得知服务器系统是ubuntu，一般网站的路径即为 /var/www/html 。

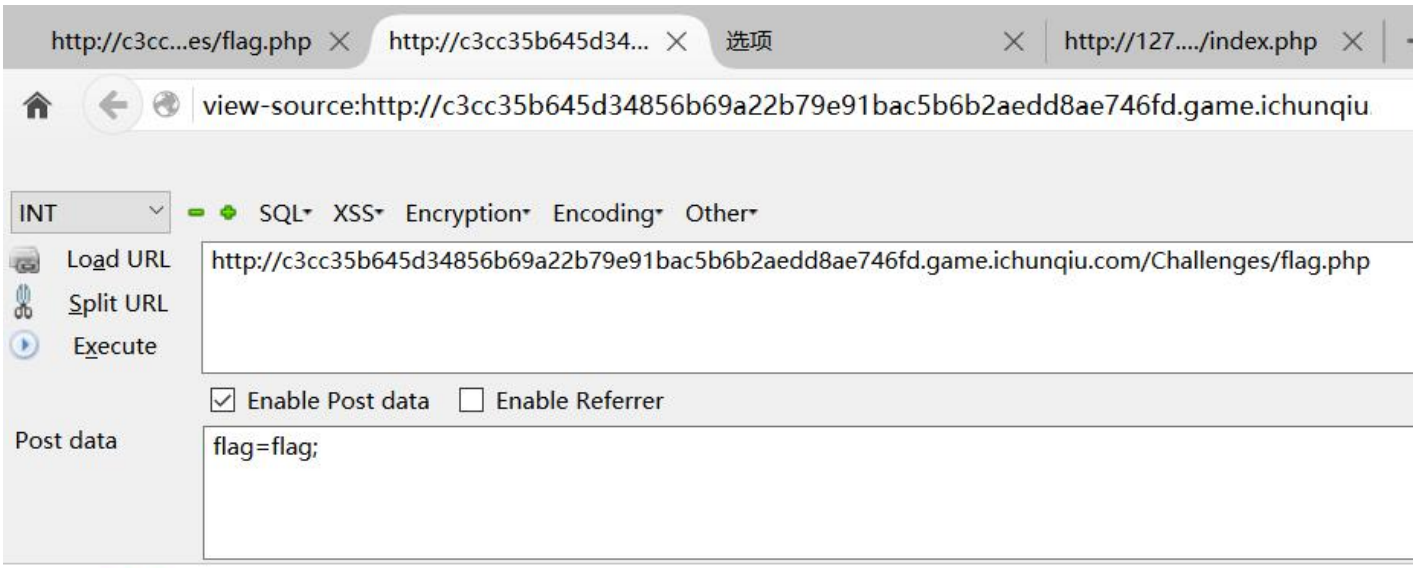


所以构造/Challenges/file/download.php?f=/var/www/html/Challenges/flag.php



看到这个 " echo file_get_contents("helloctf.php"); " 想直接包含改文件，但是发现提示error，所以继续审代码

第一眼觉得很麻烦，不过细看一下觉得这个实在没难度，构造 flag=flag; ，注意有分号的，因为eval()执行的是一句完整的php代码，当然要以分号结尾。然后eval() 那句执行的就是 $spaceone = flag; ，然后没反应？ 查看源码就可以看见了




```
<?php
$flag="flag{c77ea1ec-6ff3-4196-b924-608726da8c73}";
?>
```

转载于:https://www.cnblogs.com/leixiao-/p/9785148.html