

攻防世界-web-Cat(XCTF 4th-WHCTF-2017)

原创

大千SS 于 2019-07-08 00:05:05 发布 9145 收藏 9

分类专栏: [攻防世界](#) 文章标签: [攻防世界](#)

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/zz_Caleb/article/details/95041031

版权



[攻防世界 专栏收录该内容](#)

28 篇文章 1 订阅

订阅专栏

打开网页, 有一个云端测试功能, 提示我们输入域名, 输入几个进行测试

1) [baidu.com](#) 没有反馈

但是输入百度的ip: 220.181.38.148, 反馈如下

```
PING 220.181.38.148 (220.181.38.148) 56(84) bytes of data.
--- 220.181.38.148 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

2) 127.0.0.1 反馈如下

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.048 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.048/0.048/0.048/0.000 ms
```

输入的ip被执行了ping命令并返回, 是一个命令执行的功能。

尝试使用管道进行命令执行, 输入127.0.0.1 | ls, 然而得到的回显是Invalid URL, 127.0.0.1 | phpinfo的执行结果也是Invalid URL, 看来命令执行时行不通了。

网站用的是php写的, 但是这个Cloud端就不一定是php的了。

在URL的传参处?url=这里, 我们传递个%79发现传递之后变成了?url=w, 看来是可以传递url编码, 系统会接受并进行解析, 于是我们传递%80会出现报错, url编码使用的是16进制, 80也就是128, ASCII码是从0-127, 所以这个时候会报错。url编码表可以参考http://www.w3school.com.cn/tags/html_ref_urlencode.html

报错信息中可以看到:

```
<title>UnicodeEncodeError at /api/ping</title>
```

使用的是python站点

使用的是Django框架

Django框架的目录框架可以参考:

在比赛的时候有个提示:

是关于php curl的，然而最为菜鸡我当然还是不会的，看大佬们的操作是找到了一个解题点：

CURLOPT_POSTFIELDS

全部数据使用HTTP协议中的 "POST" 操作来发送。要发送文件，在文件名前面加上@前缀并使用完整路径。文件类型可在文件名后以 ';type=mimetype' 的格式指定。这个参数可以是 urlencoded 后的字符串，类似 'para1=val1¶2=val2&...'，也可以使用一个以字段名为键值，字段数据为值的数组。如果value是一个数组，Content-Type头将会被设置成multipart/form-data。从 PHP 5.2.0 开始，使用 @ 前缀传递文件时，value 必须是个数组。从 PHP 5.5.0 开始，@ 前缀已被废弃，文件可通过 [CURLFile](#) 发送。设置 CURLOPT_SAFE_UPLOAD 为 TRUE 可禁用 @ 前缀发送文件，以增加安全性。

https://blog.csdn.net/zz_Calab

然而我去官方文档中也找到了这个预定义的变量，并没有这些介绍。。。

所以根据Django的目录，我们使用@进行文件传递，对文件进行读取之后还会把内容传给url参数，如果像上面一样有超出解析范围的编码的时候就会得到错误信息。

我们的目标首先是数据库文件，看从错误信息中能不能拿到flag，可以从配置文件settings.py的报错中看看有没有database的相关信息

```
?url=@/opt/api/api/settings.py
```

报错内容搜索database可以得到：

```
: os.path.join(BASE_DIR, '\\&#39;database.sqlite3\\&#39;),
```

```
?url=@/opt/api/database.sqlite3
```

报错信息中搜索ctf，拿到WHCTF{yooooo_Such_A_G00D_@}