buuctf [ACTF2020 新生赛]Upload 1

原创

Naptmn 于 2021-02-24 00:14:24 发布 740 收藏

分类专栏： buuctf CTF

本文链接：https://blog.csdn.net/qq_45569969/article/details/114006000


buuctf 同时被 2 个专栏收录

3 篇文章 0 订阅

订阅专栏


CTF

20 篇文章 1 订阅

订阅专栏

直接上传一个php的一句话发现无法上传

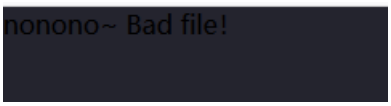
f12找到前端验证

这里有两个方法

1、直接删除这个元素

2、先上传jpg格式的一句话，bp抓包改为php

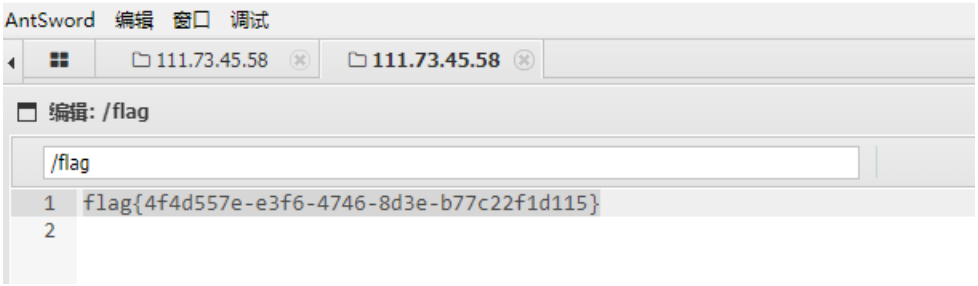
发现上传后后端仍然有检查



于是我们上传phtml格式的一句话木马（这里同样需要绕开前端验证）

> phtml可以理解为是另外一个php的文件后缀名

上传成功后蚁剑连接即可


AntSword 编辑 窗口 调试
111.73.45.58
111.73.45.58
编辑: /flag
/flag
1 flag{4f4d557e-e3f6-4746-8d3e-b77c22f1d115}
2