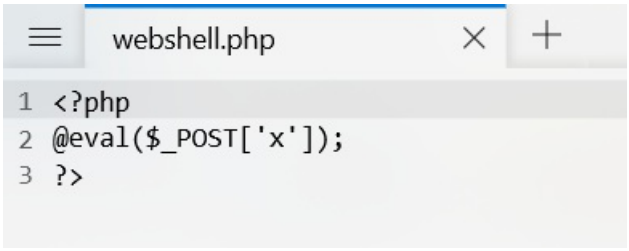
BUUCTF之Upload [ACTF2020 新生赛]

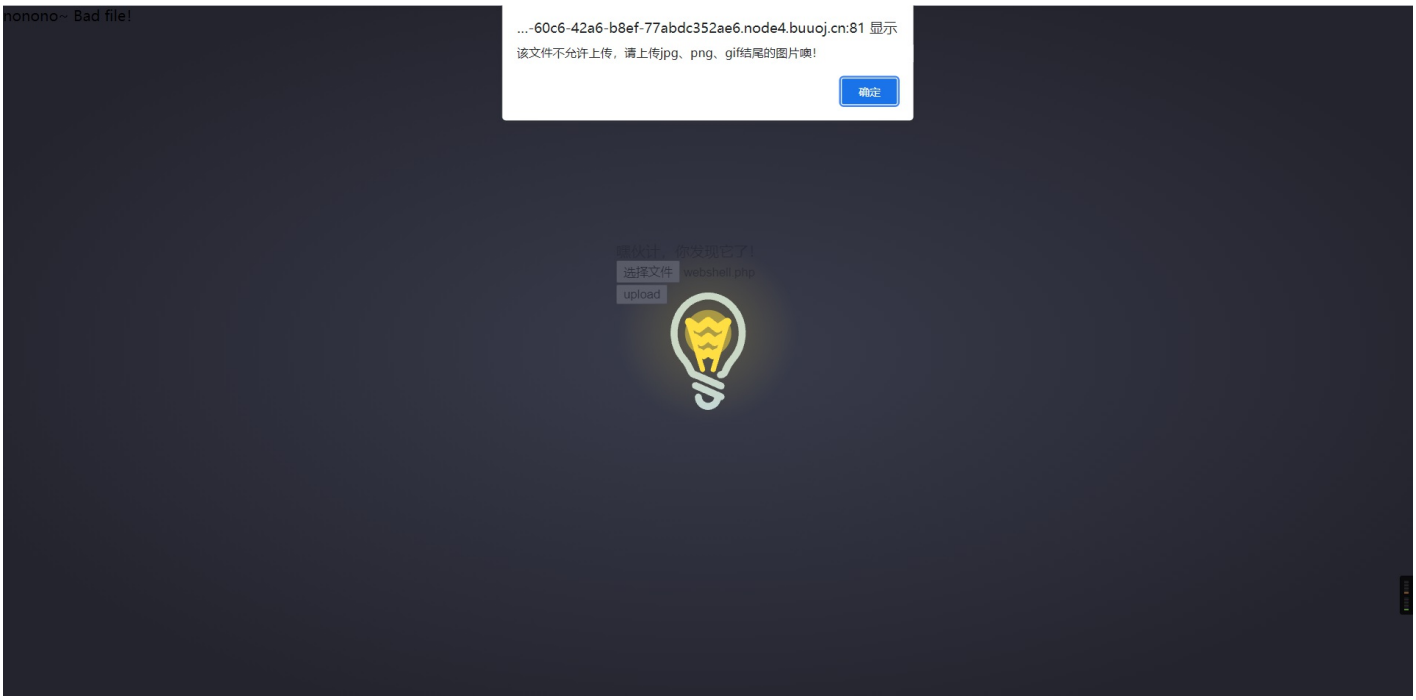
原创

金 帛 于 2022-04-19 22:15:04 发布 51 收藏
分类专栏： BUUCTF之WEB 文章标签： CTF

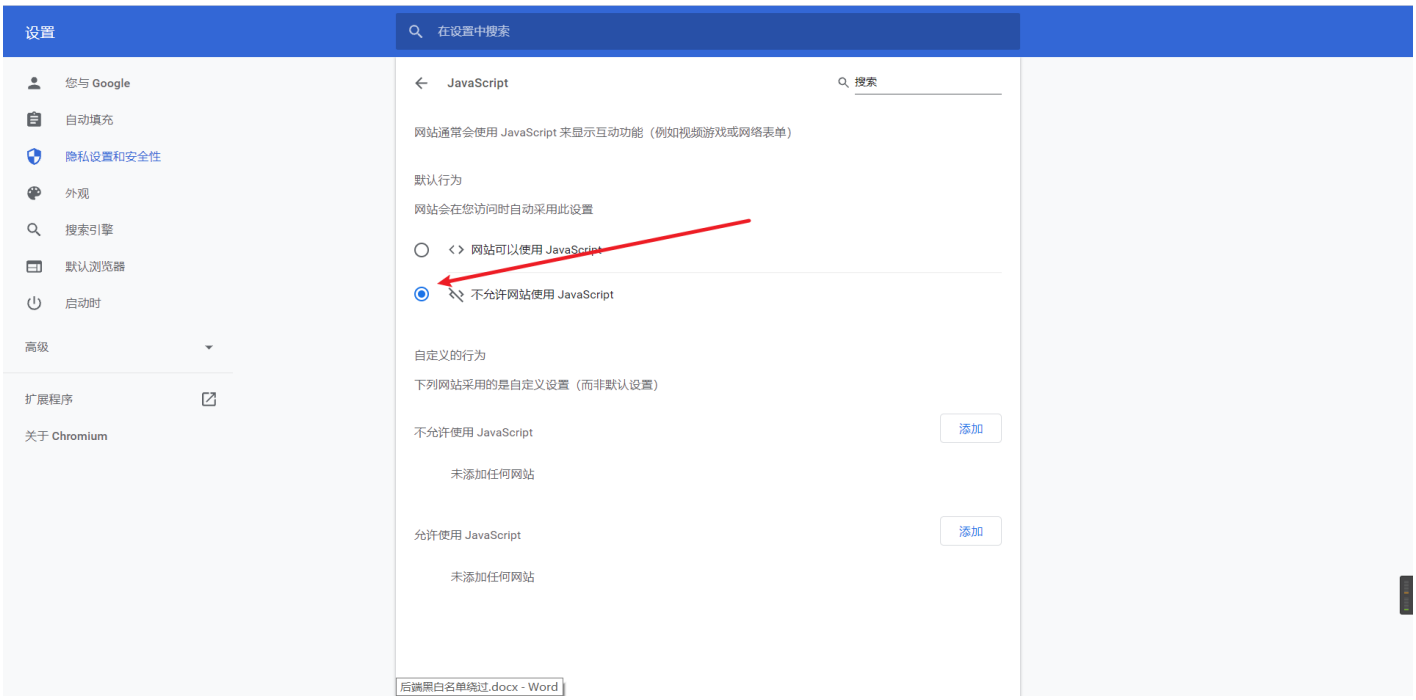
本文链接：https://blog.csdn.net/l2872253606/article/details/124284898

废话不多说直接上传一个简单的木马

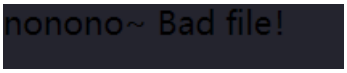




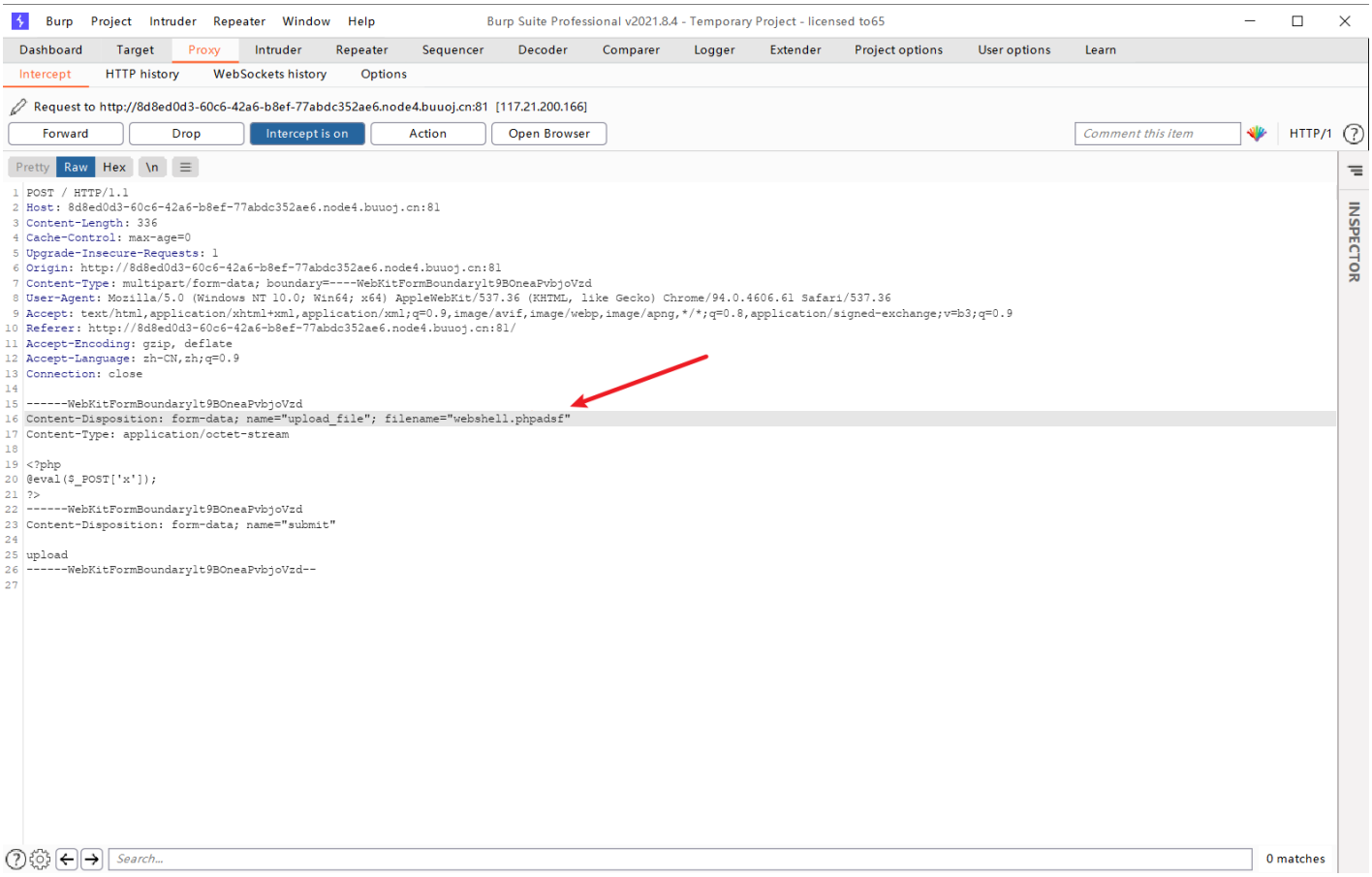
发现有前端js认证，emmm，烦，直接到设置里面暂时把js脚本禁用



刷新页面，重新上传木马



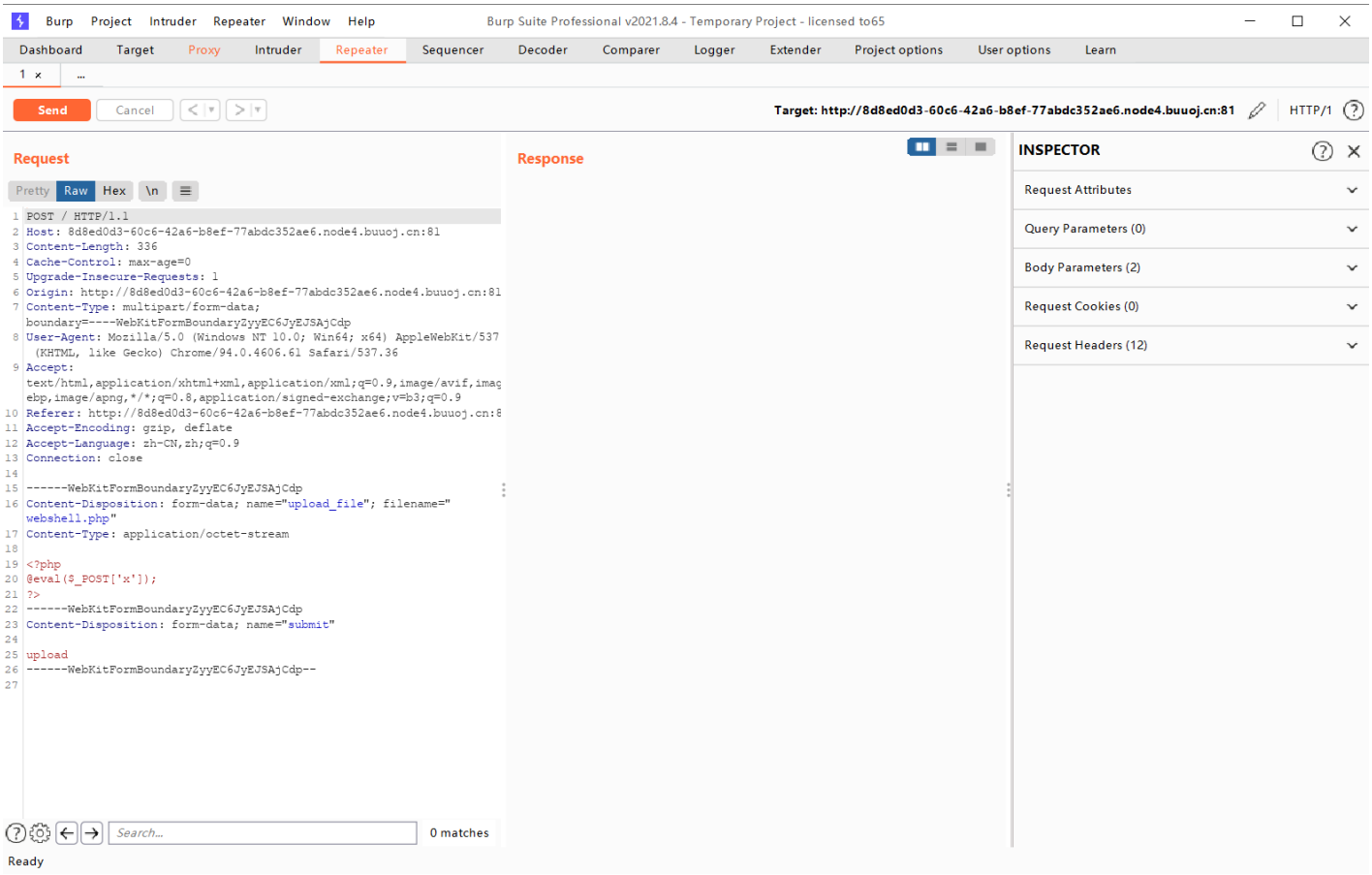
虽然没有被前端拦截，但是回显了这个，木马被检测出来了，先试试看是过滤了什么，burpsuite抓包，后缀名随便起



然后点击发送

```
Upload Success! Look here~ ./uplo4d/d51ad3b215cb1e3ac4d30fc405320de7.phpadsf
```

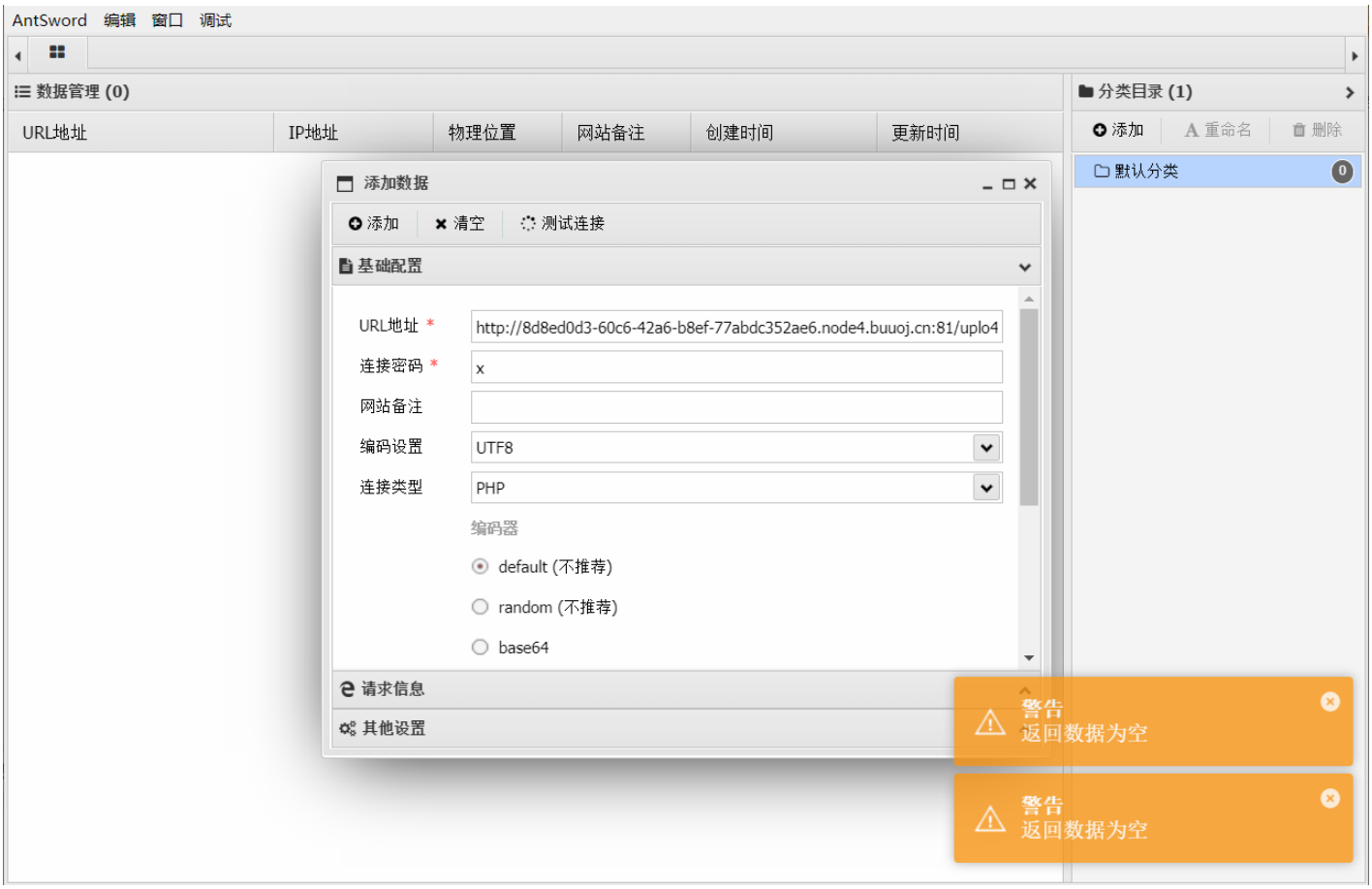
我靠，居然上传成功了，还回显了文件所在的地址，那就简单了，只要绕过文件名就行了，接着我们再次抓包，将包的内容发送到攻击器里面



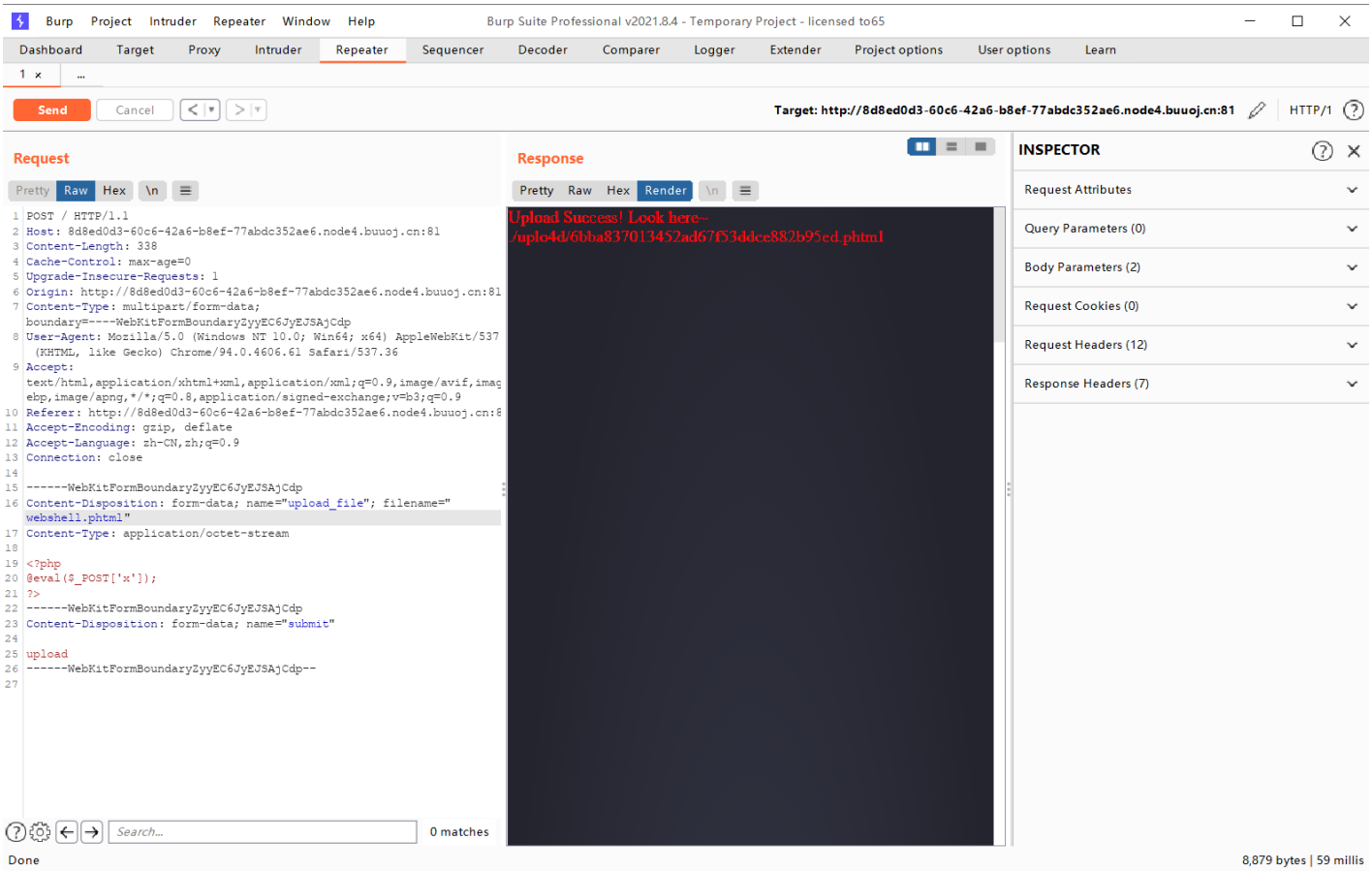
然后百度文件后缀绕过法典

> 文件上传之后缀名绕过_注定风是不羁旅人的博客-CSDN博客_文件上传后缀名绕过

一个个尝试，发现大小写能绕过，但是蚁剑连不上



继续换方法，全都试了还是不行，有点无语，但是除了php后缀外还有其他后缀，如php3、php5、phtml等，他们都能被解析成PHP执行，将后缀名换成phtml后发现上传成功



接着用蚁剑连接，找到flag文件就行了