

四叶草云演-CTF02# 单身二十年的手速

原创

[weixin_43973521](#) 于 2021-02-22 14:39:42 发布 248 收藏

分类专栏: [四叶草云演CTF实战](#)

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/weixin_43973521/article/details/113937948

版权



[四叶草云演CTF实战](#) 专栏收录该内容

4 篇文章 4 订阅

订阅专栏

- 网址: <https://www.yunyansec.com/#/experiment/ctf/>
- 题目: 单身二十年的手速

单身20年的手速

单身20年的手速, 提交flag值格式为: ssctf{}

难度: | 解出人数: 253 | 考点: 抓包 | 1

题目地址

<http://fcdb87e5.yunyansec.com/>

环境关闭倒计时: 00:53:42 [延时30分钟](#) [释放环境](#)

题目附件

暂无附件

https://blog.csdn.net/weixin_43973521

题解:

启动环境, 查看源码无发现, 打开burpsuite抓包

Request to http://fcdb87e5.yunyansec.com:80 [1.85.2.120]

Forward Drop Intercept is on Action

Raw Params Headers Hex

GET /search_key.php HTTP/1.1
Host: fcdb87e5.yunyansec.com
Upgrade-Insecure-Requests: 1
DNT: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 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://fcdb87e5.yunyansec.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_f6095793646f2ba4a15ac9ee2cd1af7a=1613907502,1613963338,1613974457,1613974467; Hm_lpvt_f6095793646f2ba4a15ac9ee2cd1af7a=1613974585
Connection: close

- Send to Spider
- Do an active scan
- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R**
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser
- Engagement tools
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Don't intercept requests
- Do intercept
- Convert selection

Comment

https://blog.csdn.net/weixin_43973521

点击go发送，得到flag

Request

Raw Params Headers Hex

Response

Raw Headers Hex HTML Render

HTTP/1.1 200 OK
Content-Length: 183
Content-Type: text/html
Date: Mon, 22 Feb 2021 06:38:20 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
X-Powered-By: PHP/5.5.9-1ubuntu4.17
Connection: close

```
<<!DOCTYPE html>  
<html lang="en">  
<head>  
<script>window.location="2.php"; </script>  
<title>key</title>  
</head>  
<body>  
ssctf{e32f79d81ff22f0f929f94d9424ca5eb}</body>  
</html>
```

0 matches

395 bytes | 18 millis

得到 **ssctf{e32f79d81ff22f0f929f94d9424ca5eb}**