攻防世界 Misc高手进阶区 7分题 流量分析

原创

思源湖的鱼 于 2021-02-03 16:44:34 发布 734 收藏 5

分类专栏： ctf 文章标签： ctf 攻防世界 misc

本文链接：https://blog.csdn.net/weixin_44604541/article/details/113603748

前言

继续ctf的旅程

攻防世界Misc高手进阶区的7分题

本篇是流量分析的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

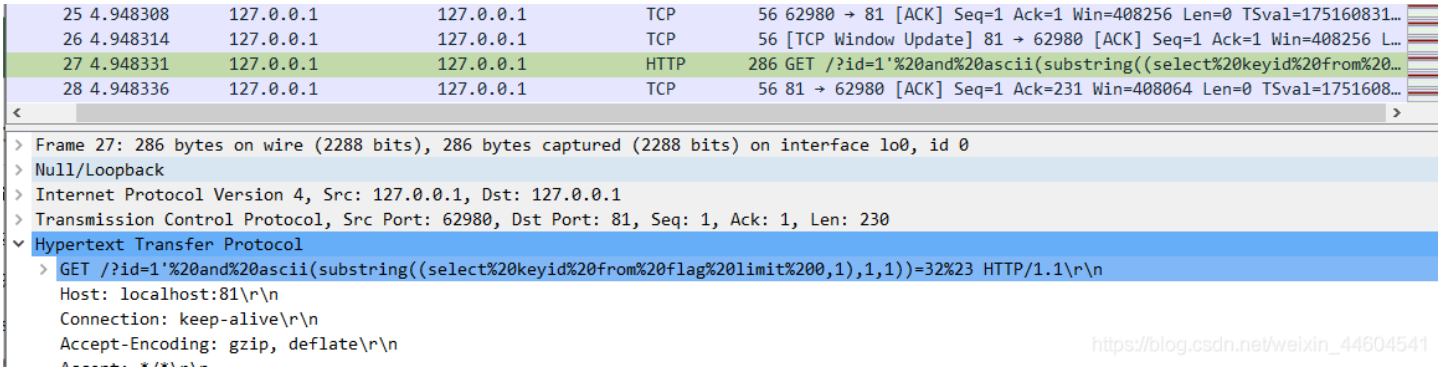
解题过程

题目描述

得到一个流量包

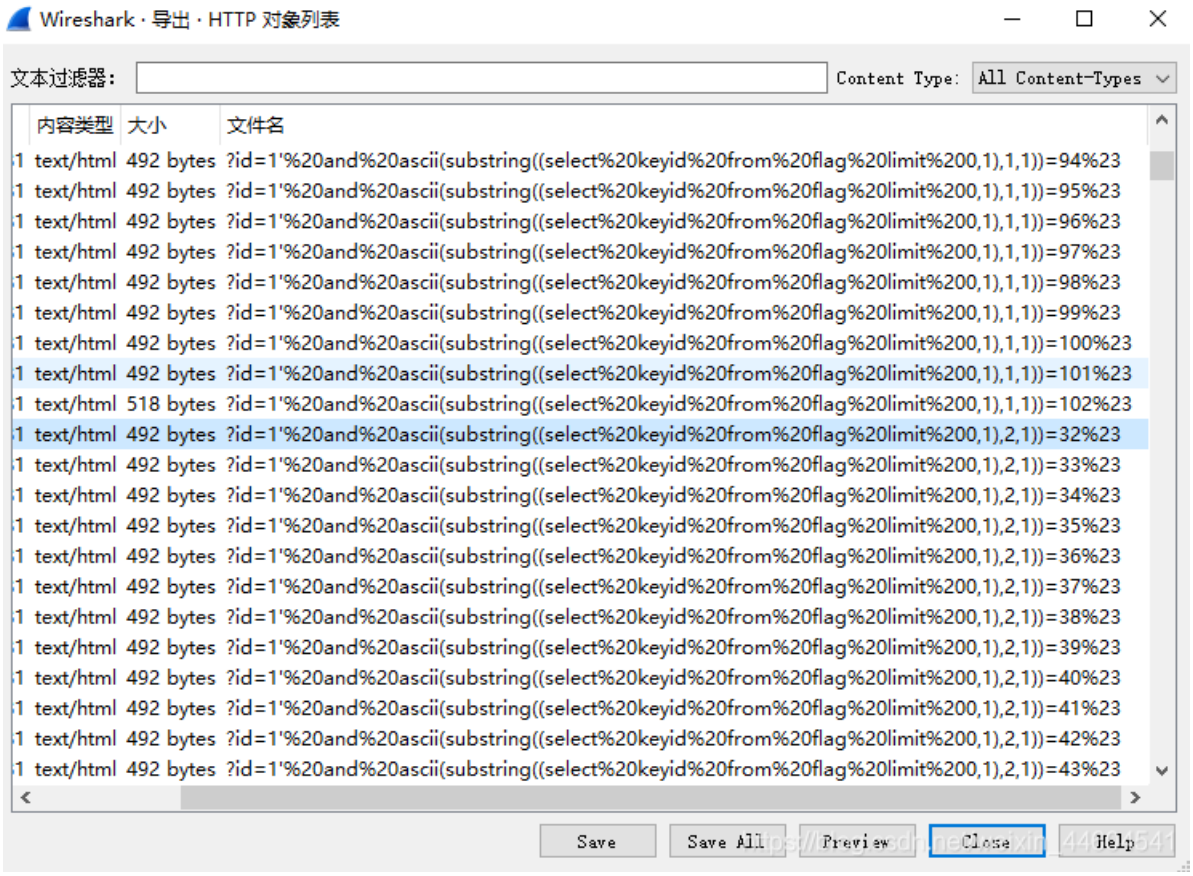
根据题目描述

应该找下get请求或post请求



找到get语句

```
id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),1,1))=32%23
```



substring函数取字符串的特定位置，从1取到38
查看每个位置对应的ascii码
当ascii码正确时，取下个位置

简单写个脚本

```python
import re

with open("1.pcapng", "rb") as f:
    contents = f.read()
    res = re.compile(r'0,1\),(\d+),1\)\)=(\d+)%23').findall(str(contents))
    dic = {}
    for a, b in res:
        if a in dic:
            if int(b) > dic[a]:
                dic[a] = int(b)
        else:
            dic[a] = int(b)
    flag = ""
    for i in range(1,39):
        flag += chr(dic[str(i)])
    print(flag)
```

```
flag{c2bbf9cecdaf656cf524d014c5bf046c}
>>>
```

得到flag

结语

简单题