




# 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](#)

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\\_44604541/article/details/113603748](https://blog.csdn.net/weixin_44604541/article/details/113603748)

版权

## CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

### 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

**题目描述: sql注入**

得到一个流量包

根据题目描述

应该找下get请求或post请求

25	4.948308	127.0.0.1	127.0.0.1	TCP	56	62980 → 81 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=175160831...
26	4.948314	127.0.0.1	127.0.0.1	TCP	56	[TCP Window Update] 81 → 62980 [ACK] Seq=1 Ack=1 Win=408256 L...
27	4.948331	127.0.0.1	127.0.0.1	HTTP	286	GET /?id=1'%20and%20ascii(substring((select%20keyid%20from%20...)
28	4.948336	127.0.0.1	127.0.0.1	TCP	56	81 → 62980 [ACK] Seq=1 Ack=231 Win=408064 Len=0 TSval=1751608...

```

> Frame 27: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface lo0, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 62980, Dst Port: 81, Seq: 1, Ack: 1, Len: 230
< Hypertext Transfer Protocol
  > GET /?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),1,1))=32%23 HTTP/1.1\r\n
    Host: localhost:81\r\n
    Connection: keep-alive\r\n
    Accept-Encoding: gzip, deflate\r\n
    ----- * (*):--

```

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

找到get语句

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

Wireshark · 导出 · HTTP 对象列表

文本过滤器:  Content Type: All Content-Types

内容类型	大小	文件名
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),1,1))=94%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),1,1))=95%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),1,1))=96%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),1,1))=97%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),1,1))=98%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),1,1))=99%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),1,1))=100%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),1,1))=101%23
1 text/html	518 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),1,1))=102%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),2,1))=32%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),2,1))=33%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),2,1))=34%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),2,1))=35%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),2,1))=36%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),2,1))=37%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),2,1))=38%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),2,1))=39%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),2,1))=40%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),2,1))=41%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),2,1))=42%23
1 text/html	492 bytes	?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),2,1))=43%23

Buttons: Save, Save All, Preview, Close, Help

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

```
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