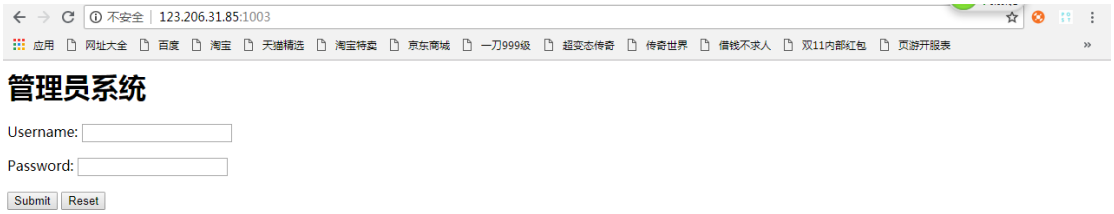
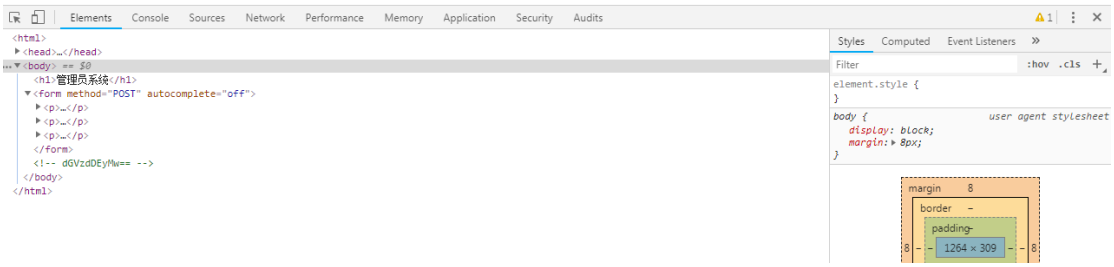
bugku 管理员系统

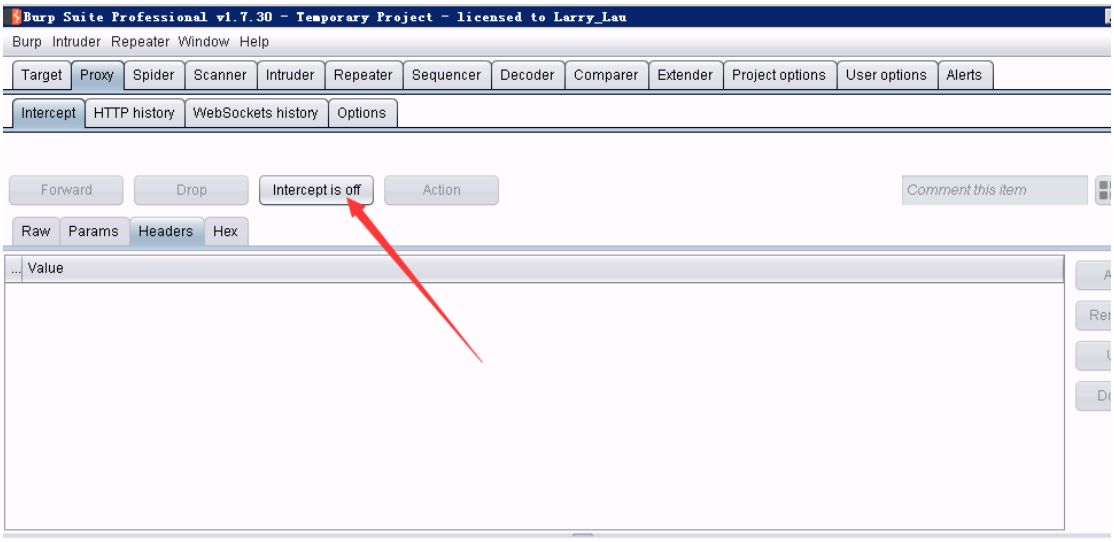




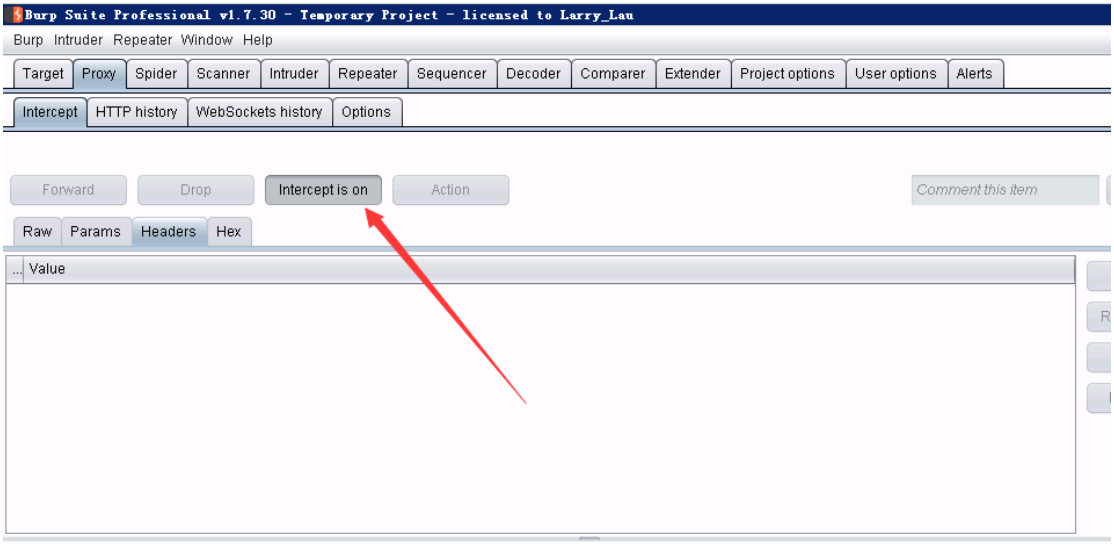
日常首先检查源码，发现一段 Base64 加密的密文，解码后的值为 test123

test123 是不是就是登陆密码呢？尝试登陆，未果.....

这里注意：



抓包工具为关闭状态(上图)

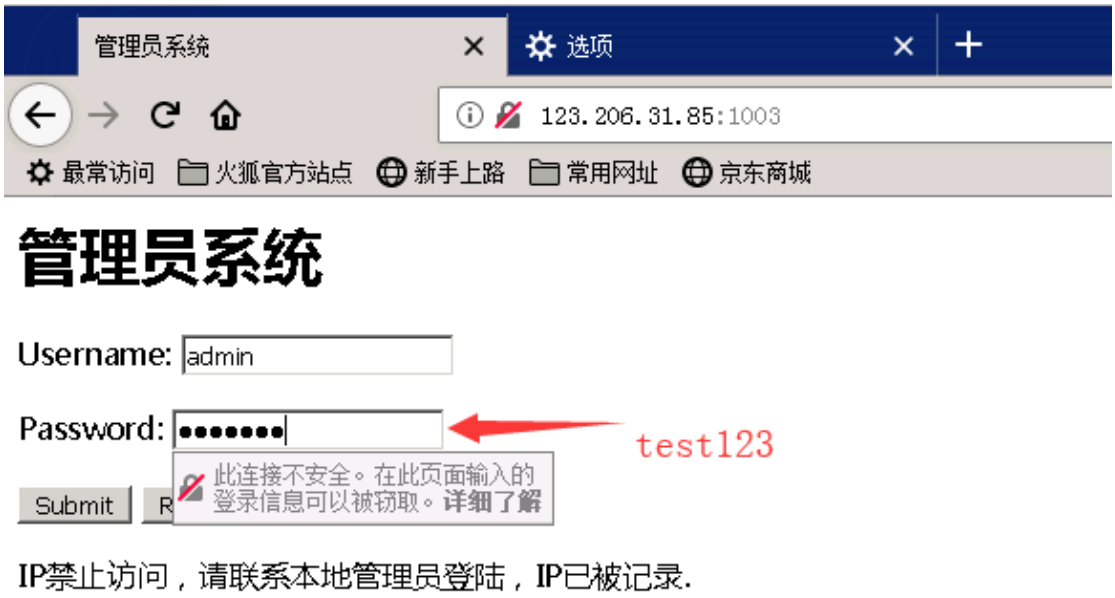


抓包工具为开启状态(上图)

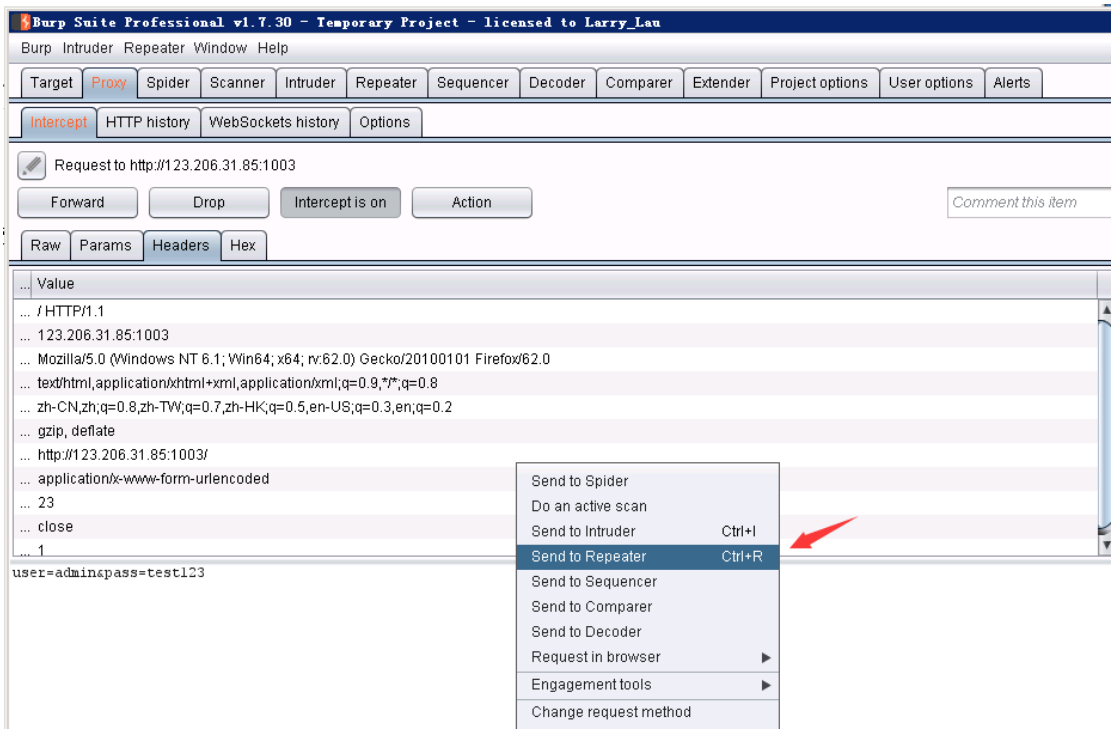
得到新思路：伪装成本地访问：

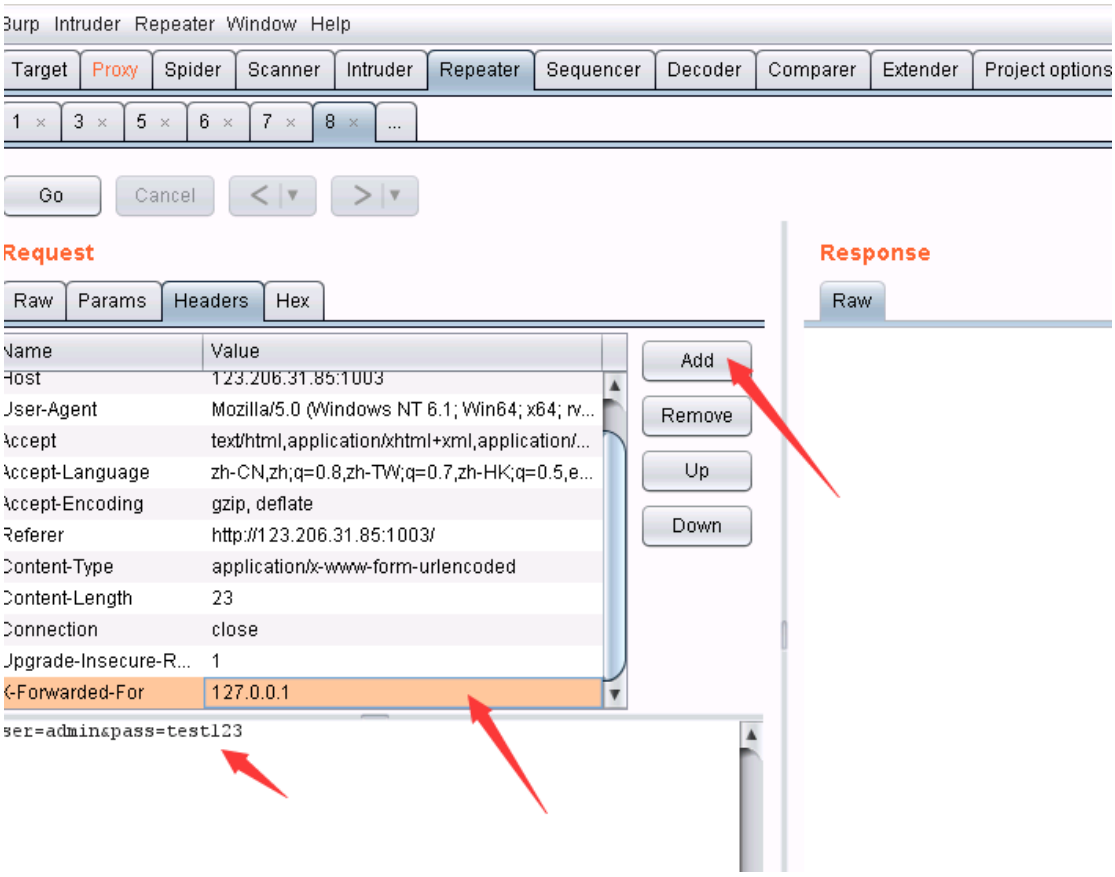
抓包

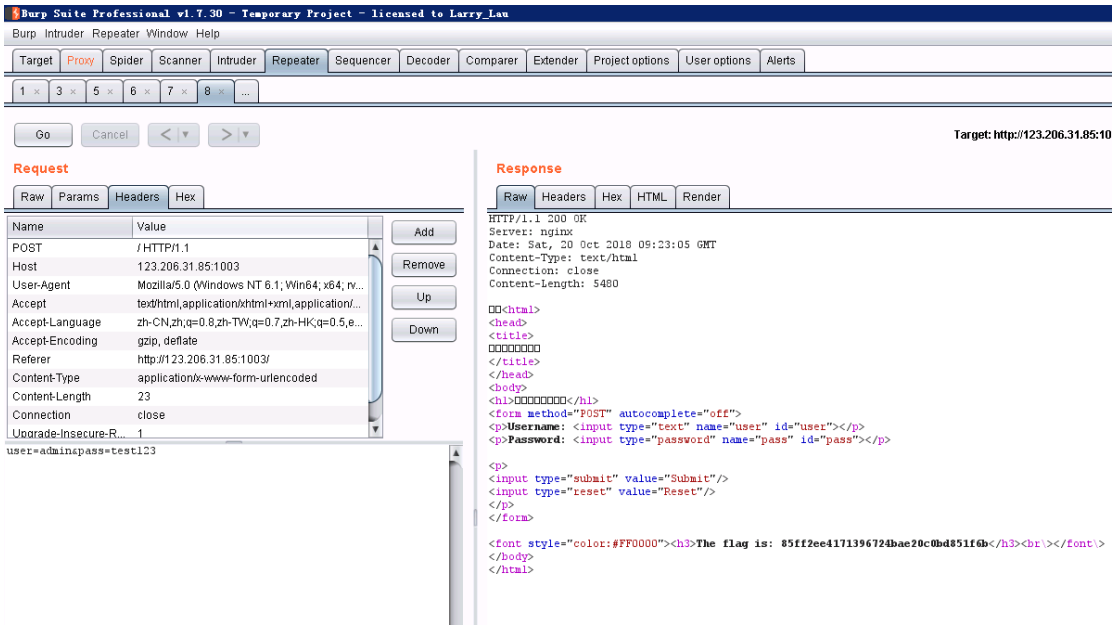
改包：Headers 中增添一对键值对： X-Forwarded-For：127.0.0.1


管理员系统
选项
123.206.31.85:1003
最常访问
火狐官方站点
新手上路
常用网址
京东商城
管理员系统
Username: admin
Password:
test123
此连接不安全。在此页面输入的登录信息可以被窃取。详细了解
Submit
IP禁止访问，请联系本地管理员登陆，IP已被记录.

抓包


Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to http://123.206.31.85:1003
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
Value
/ HTTP/1.1
123.206.31.85:1003
Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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
gzip, deflate
http://123.206.31.85:1003/
application/x-www-form-urlencoded
23
close
1
user=admin&pass=test123
Send to Spider
Do an active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools
Change request method





test123 实际是密码，账号是 admin