下载备份文件，找到关键信息。

有：连接数据库的账号和密码，admin表的一条admin md5密码。管理员的session信息。

首先尝试phpmyadmin数据库写文件和利用日志写shell。

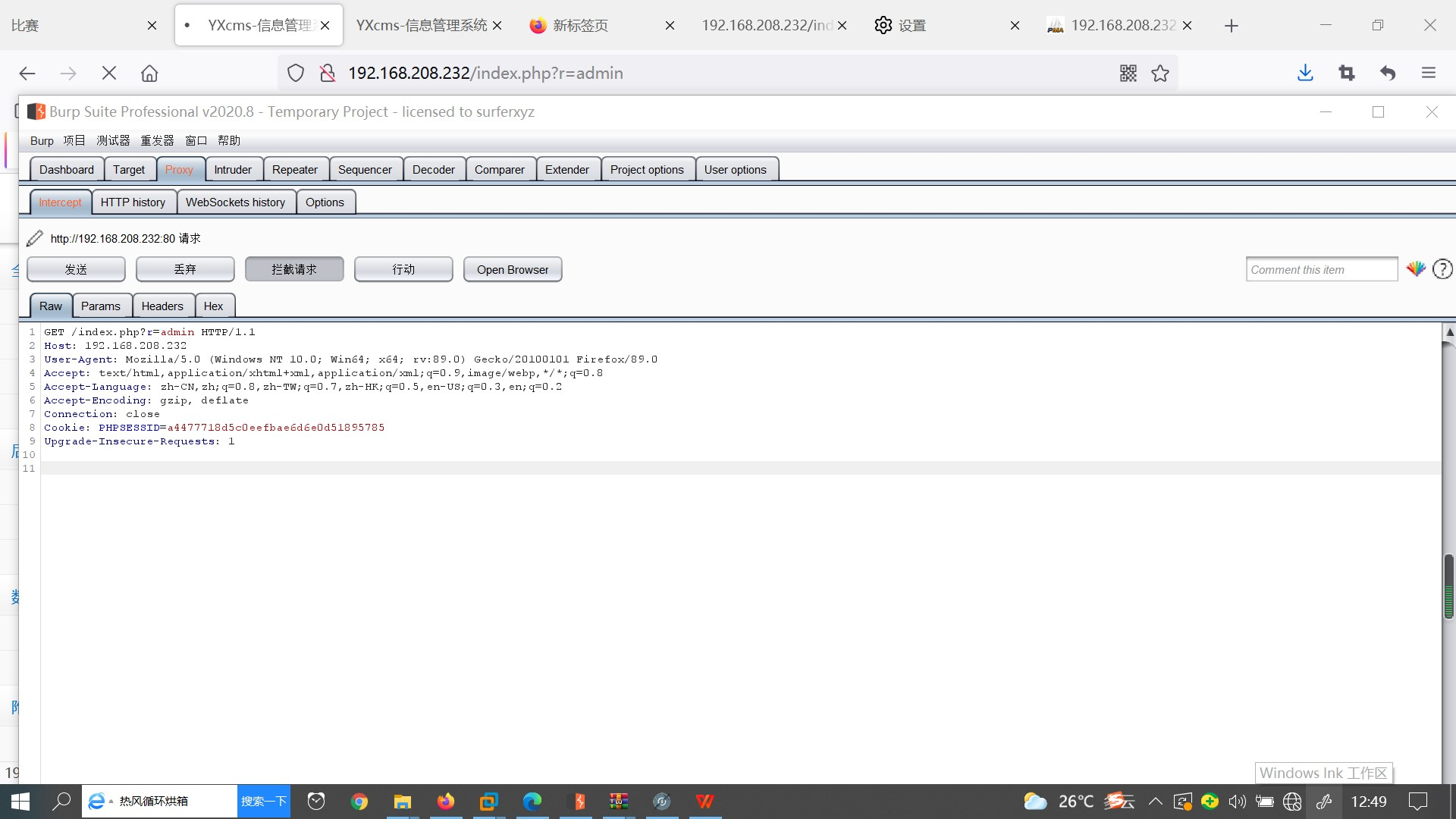
发现全局日志没开，开启这个功能需要更高权限。

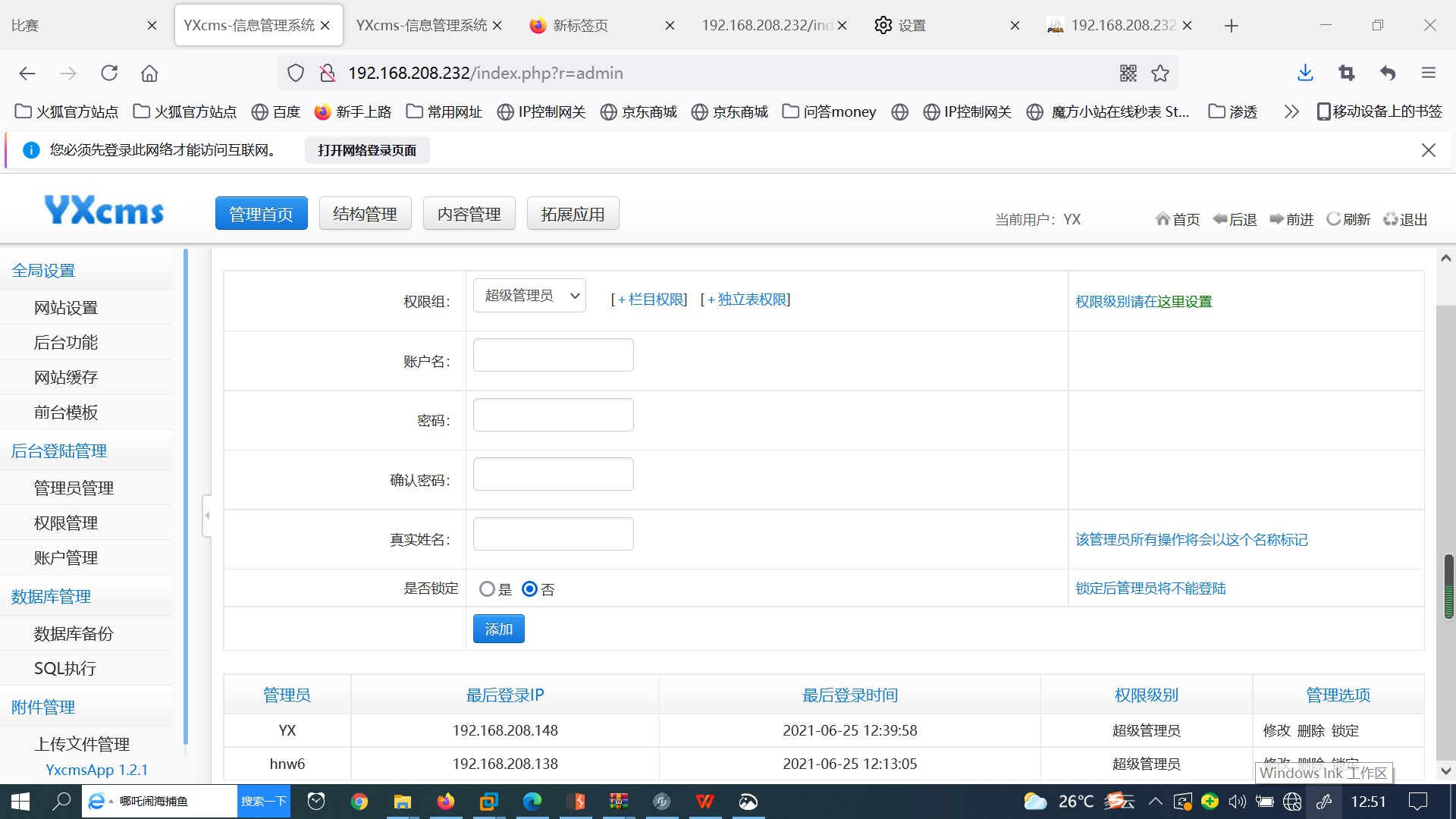
然后再尝试写文件，失败。

修改admin表，添加账户，修改密码。不知道为什么老是登不上去。

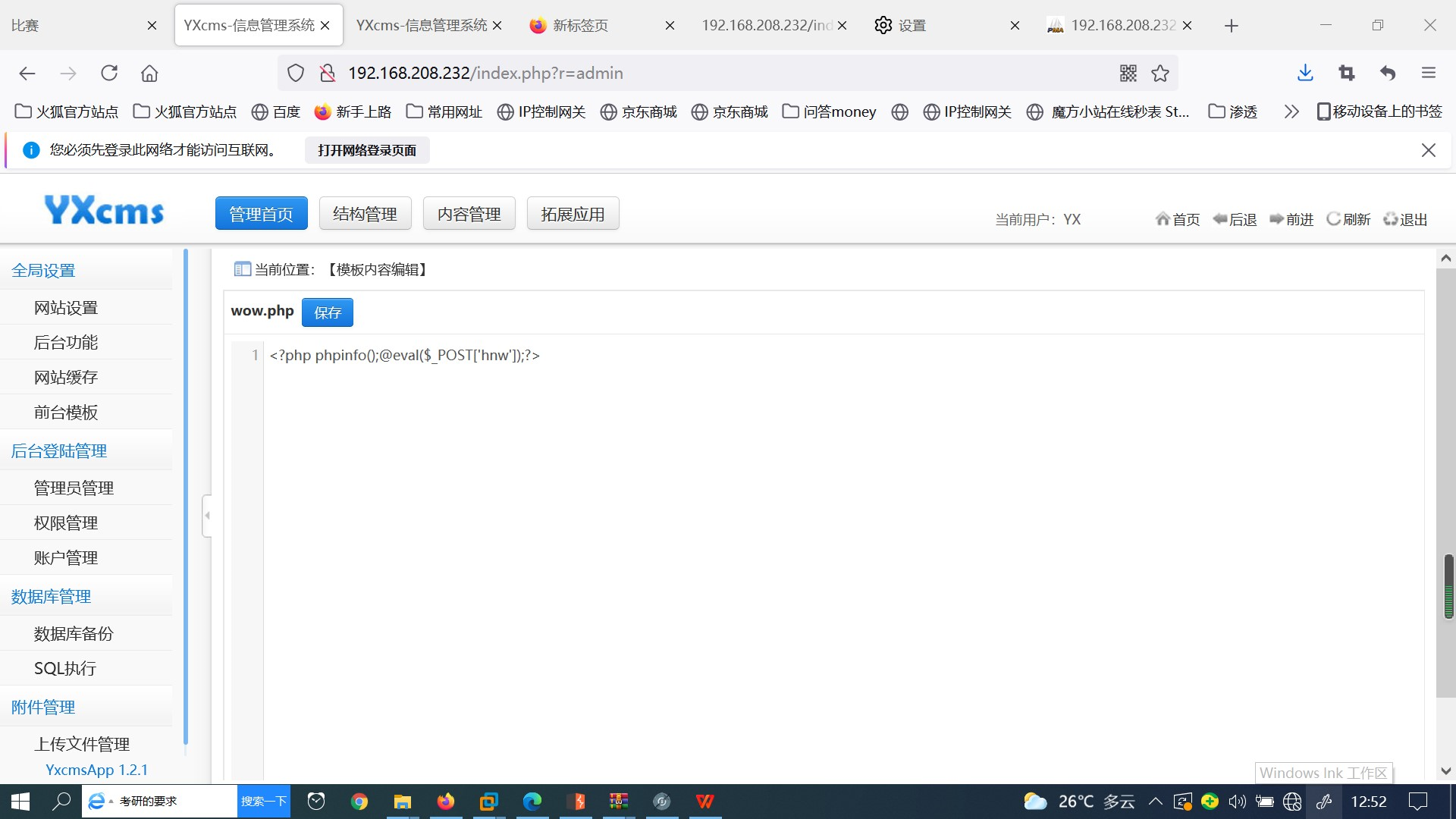
中间还利用任意文件删除漏洞，又重置了一遍yxcms，但还是没登上去。

最后burp抓包，修改session成功登入，给自己添加了一个管理员账户hnw6。





用这个账户登入，就不用burp一直修改了。然后再用已知的前台模板漏洞，写了一个shell。



蚁剑连接shell。读取flag文件。

