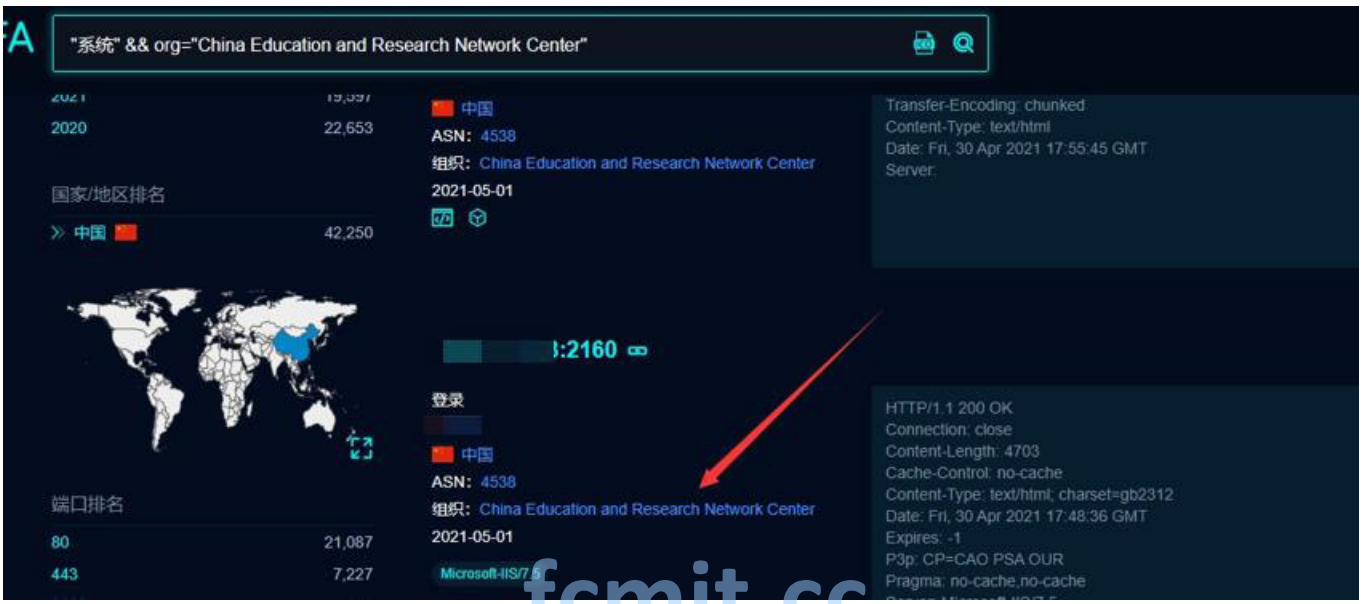
edusrc通用思路：

Ps:此文章是我在2021年四月份所写，这次就直接利用一下了！

思路：要想刷屏上分，就得找系统来挖掘，对于不会审计的我来说只有做一些黑盒测试（会审计大佬可以忽略这一点）

首先我们利用fofa找一些与edu有关的系统

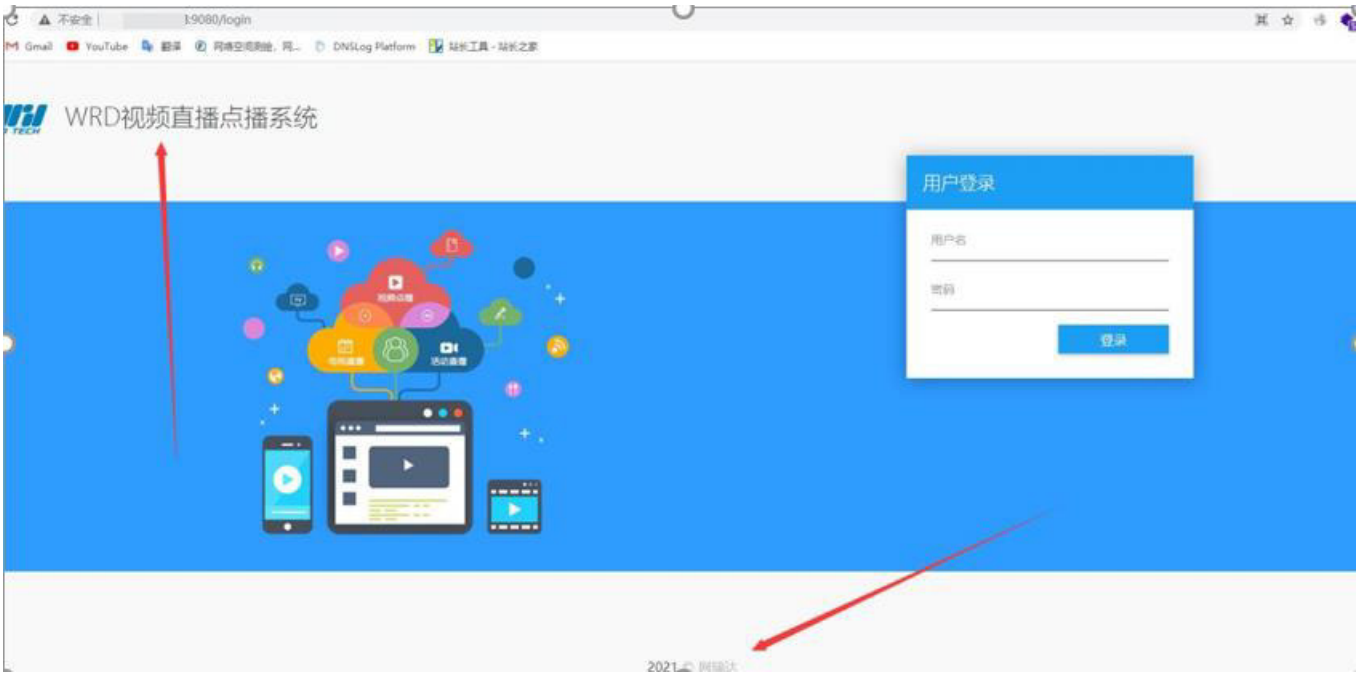
语法：“系统” &&org=“China Education and Research Network Center”



其中可以在前面加一些：阅卷系统、评分系统、直播系统、录播系统。（我们需要找的是弱口令能进去的系统）

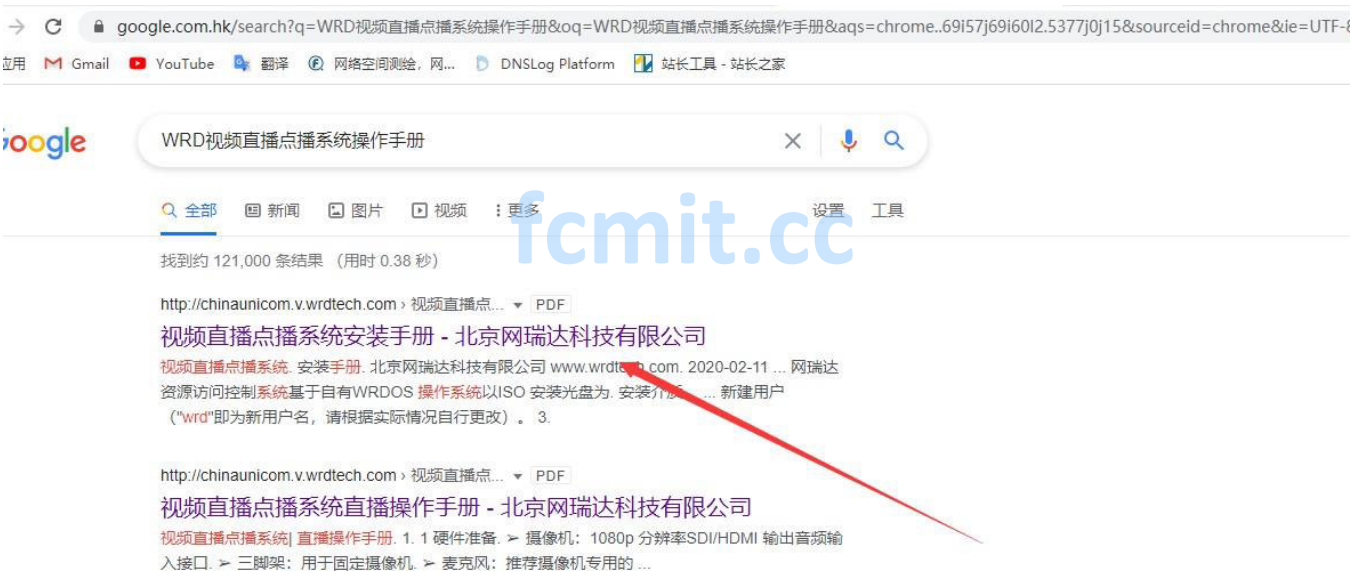
此次渗透我使用的是：“点播系统” &&org=“China Education and Research Network Center”

当确定系统后，我们就开始寻找目标站点，能通过弱口令进入的系统是最好的（admin\admin admin\123456)



通过上述的弱口令测试并没有进入后台，此时肯定会有爆破密码的想法，但是爆破成功的可能性太小了，于是我思考是否能通过找到操作手册发现默认密码，观察页面有关键字： 网瑞达和WRD视频直播点播系统

于是使用谷歌查找：WRD视频直播点播系统操作手册



点进去看看能否找到默认密码,运气还是好，碰巧发现了默认密码：默认管理端用户名『admin』 密码为『Wrd123!@#』。

5.1 系统管理

安完成 OS 基本设置后，视频直播点播系统的管理端默认使用 HTTP 协议访问，进入管理端口也可以设置管理端使用 HTTPS 协议访问。

管理端发布的链接为『/admin』可用 Chrome、Firefox、Safari 等现代浏览器访问 URL：http://<ip>/admin 。

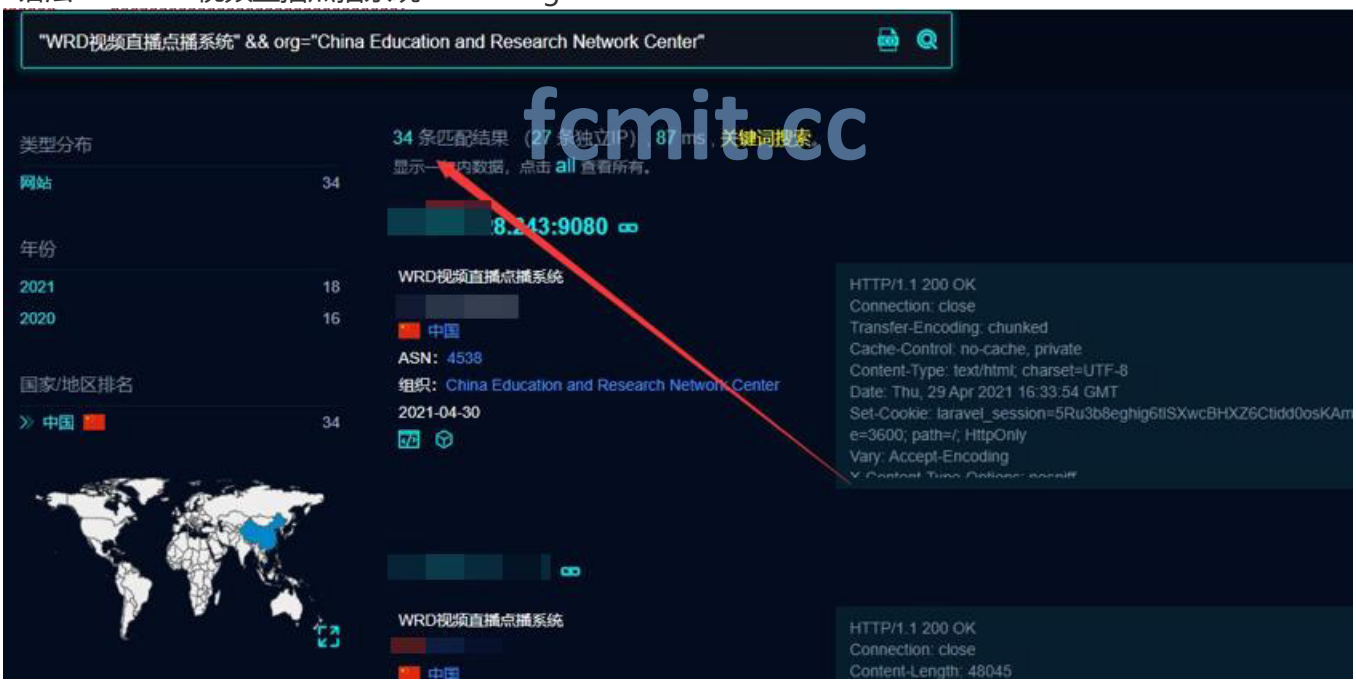
默认管理端用户名『admin』 密码为『Wrd123!@#』。

特别地，强烈建议用户修改默认账户密码，以提高系统安全性。

密码修改入口为：管理端『系统设置』/『用户管理』菜单。

发现WRD视频直播点播系统默认密码后，继续使用fofa构造语句查找能进入的系统（如果大多数都是默认密码，此处就是一个弱口令通杀）

语法： “WRD视频直播点播系统” && org=“China Education and Research Network Center”



运气还是有点倒霉的，这么多站点只有一个通过默认密码进入了系统： http://223.99.203.174:8081/login （已修复），

测试完后，心里很复杂，这么多站点，就一个弱口令，看见有相关公司，于是在fofa一次公司名称，看看有没有别的站点：

语法： “网瑞达” && org=“China Education and Research Network Center”

发现这个公司的系统产品挺多的然后继续进行默认密码测试，在1063个站点下，大约测试出了10多个站点，全部已经提交平台并且修复：

2021-04-27	东北大学秦皇岛分校	高危	通过
2021-04-27	南京特殊教育师范学院	高危	已修复
2021-04-27	青岛远洋船员职业学院	高危	通过
2021-04-27	兰州城市学院	高危	通过
2021-04-27	南京特殊教育师范学院	高危	已修复
2021-04-27	云南财经大学	高危	通过
2021-04-27	云南财经大学	高危	通过
2021-04-27	南京艺术学院	高危	通过
2021-04-27	东北大学秦皇岛分校	高危	通过
2021-04-27	兰州城市学院	中危	通过
2021-04-26	昌邑市第一中学	中危	通过

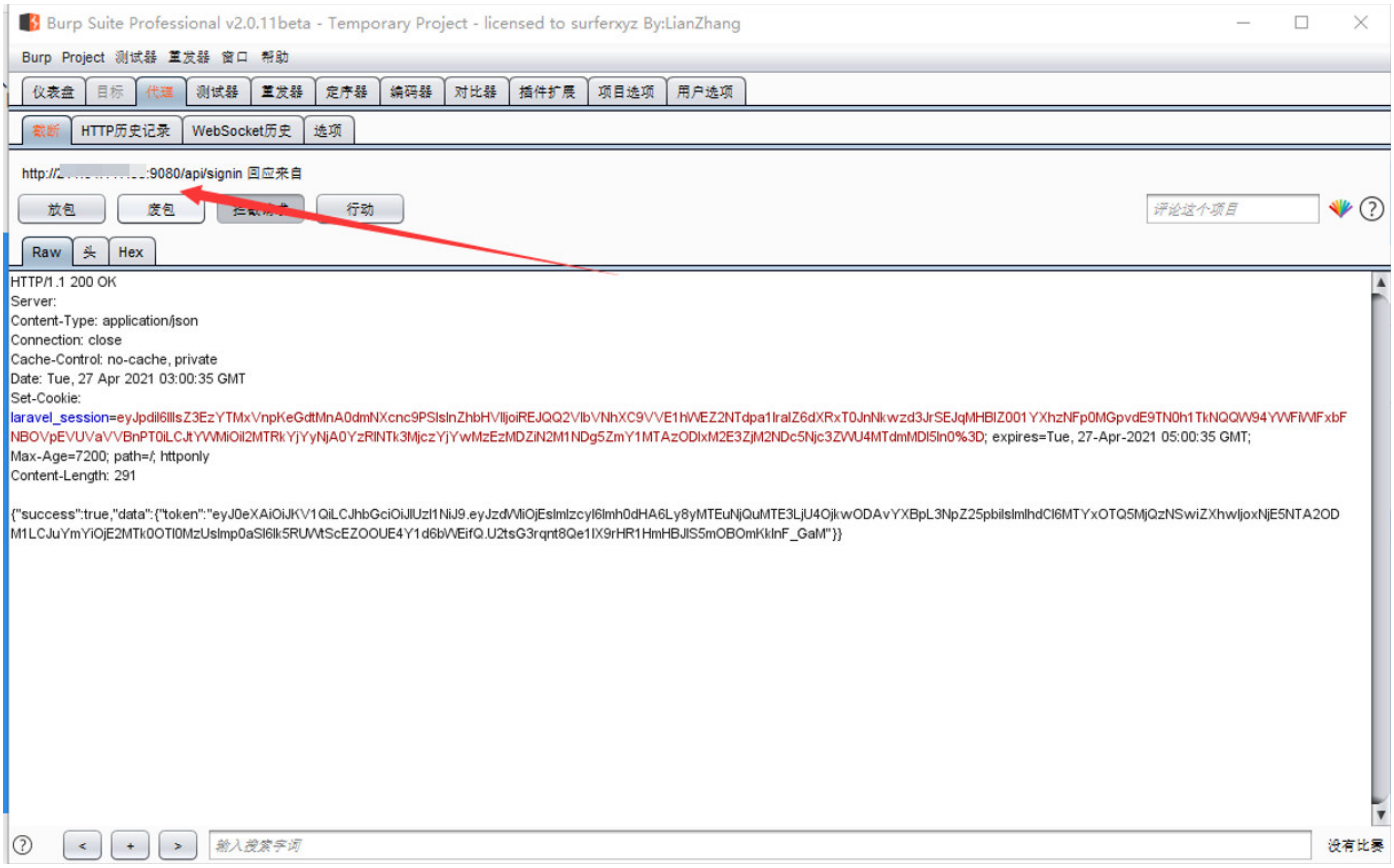
看着这么多站点，却只有一点点能通过默认密码进入，心里非常的失落，于是有了能不能越权登录的想法：首先在登录框抓登录的返回包看见false,顺手修改为true,放包：

发现这样修改数据包，在放包时无任何反应，于是我思考，能不能用默认密码进入的站点的返回包放入不能登录的站点测试：

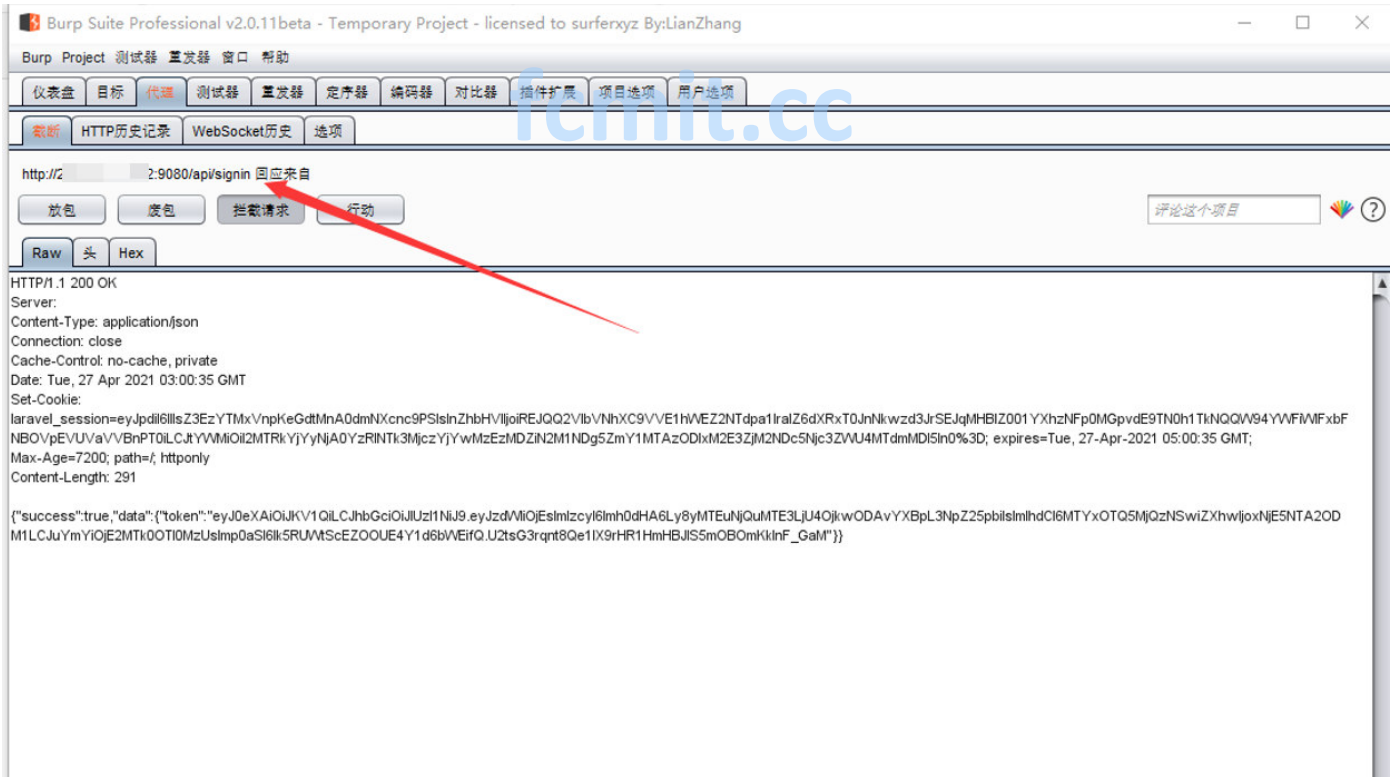
（通过测试，寻找到辅助站点：http://ip:9080/signin获取到返回登录数据包： HTTP/1.1

200 OK
Server:
Content-Type: application/json
Connection: close
Cache-Control: no-cache, private
Date: Tue, 27 Apr 2021 03:00:35 GMT
Set-Cookie:
laravel_session=eyJpdiI6IllsZ3EzYTMxVnpKeGdtMnA0dmNXcnc9PSIsInZhbHVlIjoiREJQQ2VIbVNhXC9VVE1hWEZ2NTdpa1lralZ6dXRxT0JnNkwzd3JrSEJqMHBlZ001YXhzNFp0MGpvdE9TN0h1TkNQQW94YWFiWlFxbFNBOVpEVUVaVVBnPT0iLCJtYWMiOiI2MTRkYjYyNjA0YzRlNTk3MjczYjYwMzEzMDZiN2M1NDg5ZmY1MTAzODIxM2E3ZjM2NDc5Njc3ZWU4MTdmMDI5In0%3D; expires=Tue, 27-Apr-2021 05:00:35 GMT; Max-Age=7200; path=/; httponly
Content-Length: 291

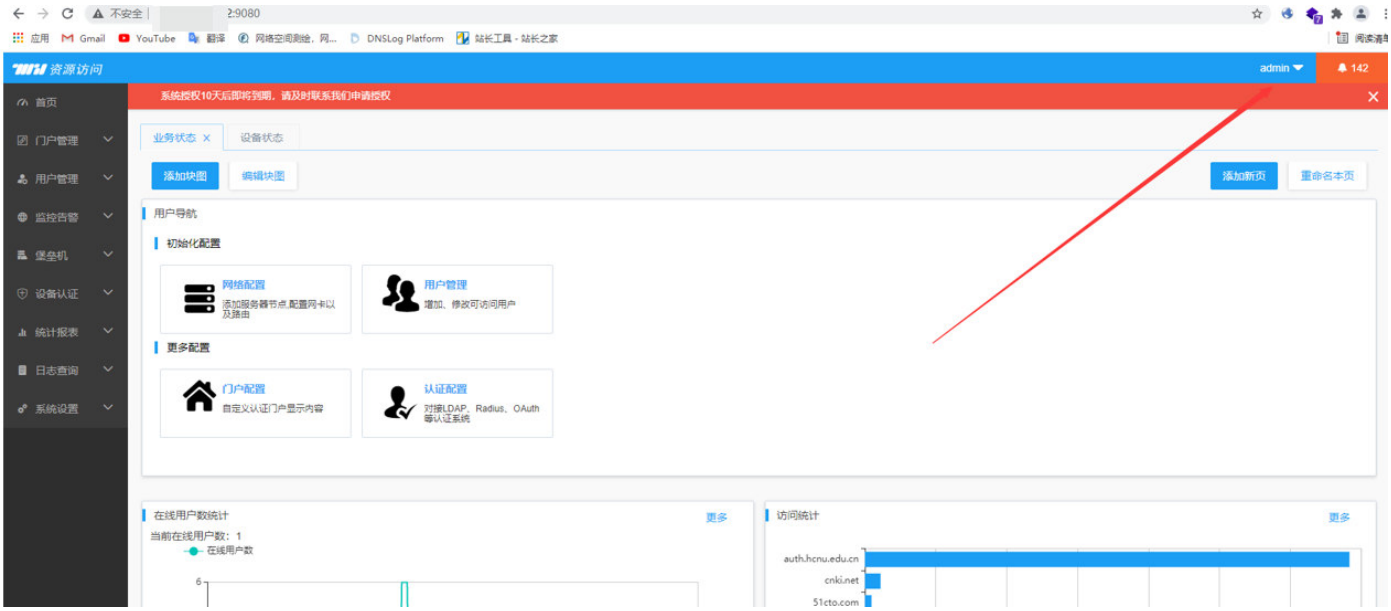
{ “success” :true, “data” :{ “token” :
“eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOjEsImlzcyI6Imh0dHA6Ly8yMTEuNjQuMTE3LjU4OjkwODAvYXBpL3NpZ25pbiIsImlhdCI6MTYxOTQ5MjQzNSwiZXhwIjoxNjE5NTA2ODM1LCJuYmYiOjE2MTk0OTI0MzUsImp0aSI6Ik5RUWtScEZOOUE4Y1d6bWEifQ.U2tsG3rqnt8Qe1lX9rHR1HmHBJlS5mOBOmKkInF_GaM” }}



去访问目标站点：http://ip:9080/signin，然后在登录处输入账号admin 密码任意 ， 抓返回， 将包换为刚获取的成功登录包然后放包：



点击放包，没想到全部的数据包放完后，就成功的进入到后台了



随后我任意选择了几个不同的学校进行了测试，都可以通过此方法进入后台，通过收集，一共有400所高校被日。