福建科立讯通信有限公司指挥调度管理平台存在未授权访问漏洞

一、 漏洞描述

福建科立讯通信有限公司创立于 2001 年，是以专业通信为核心的解决方案提供商和运营服务商。

福建科立讯通信有限公司指挥调度管理平台存在未授权访问漏洞。攻击者可利用漏洞未授权获取服务器敏感信息。

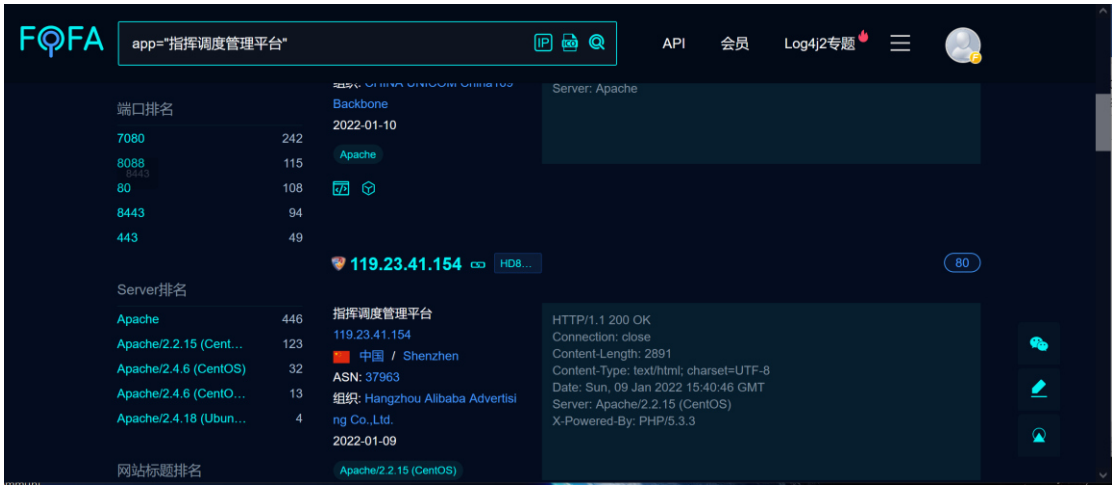
二、漏洞影响

指挥调度管理平台

三、漏洞复现

复现一

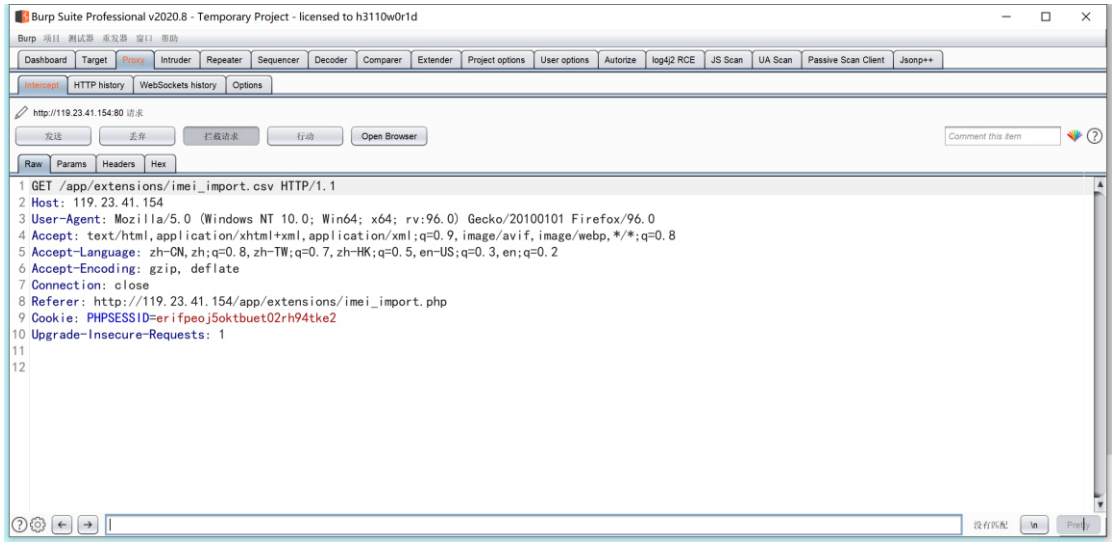
1、fafo 搜索：app="指挥调度管理平台"



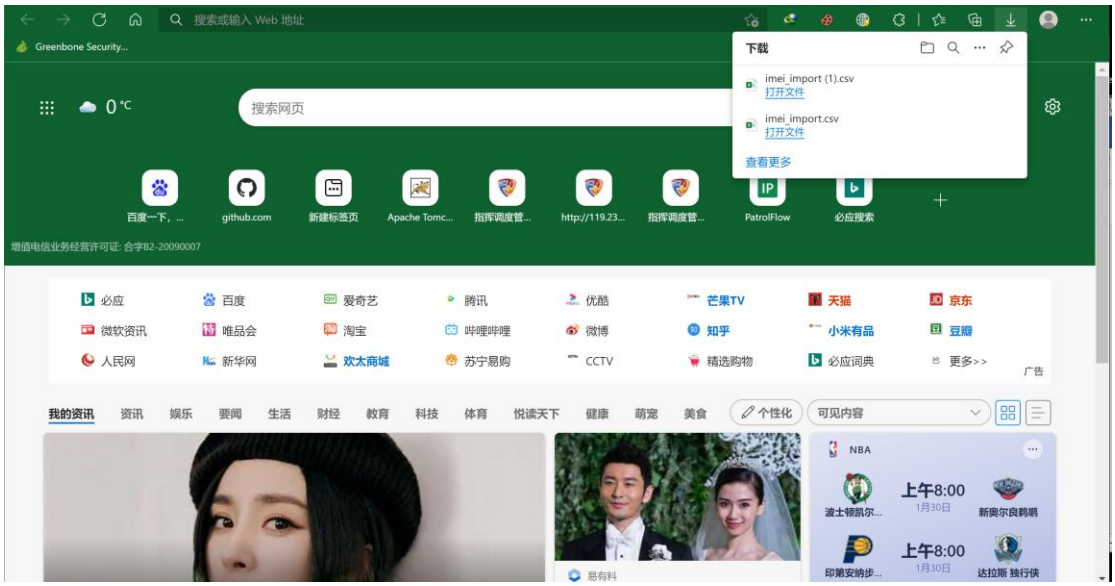
2、以 IP：http://119.23.41.154 为例

账号，密码：admin/admin

3、进入到系统后，如图，点击 IMEI 管理，再点击导入，下载 execl 模板，抓包

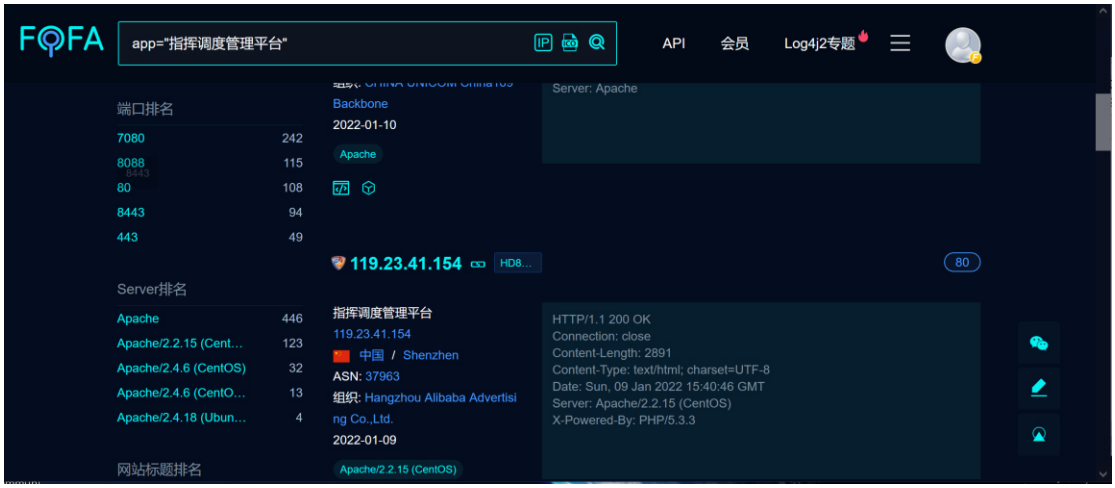


4、复制下载链接，更换浏览器进行访问，成功未授权下载文件



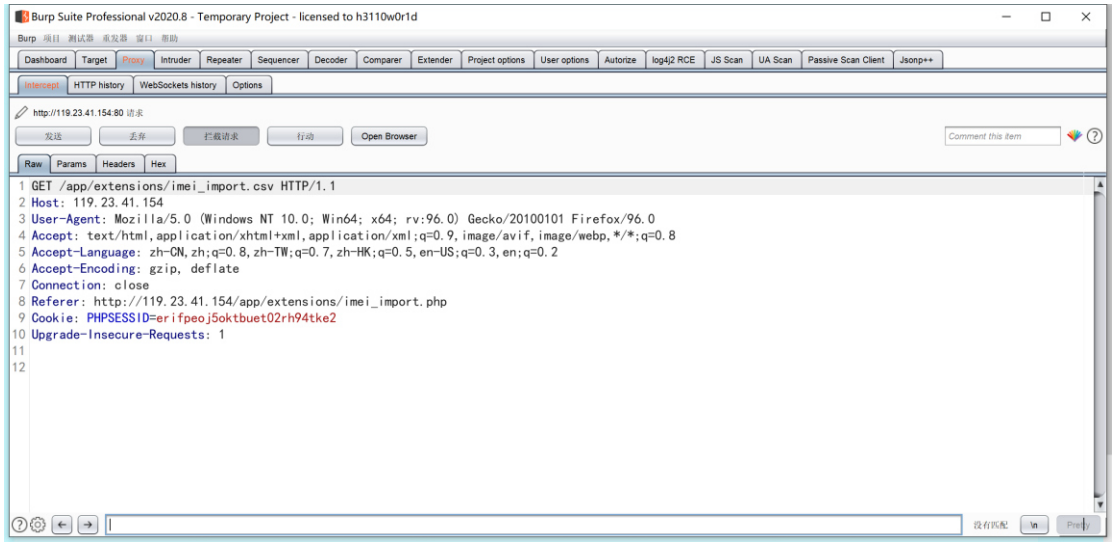
复现二

1、fafo 搜索：app="指挥调度管理平台"

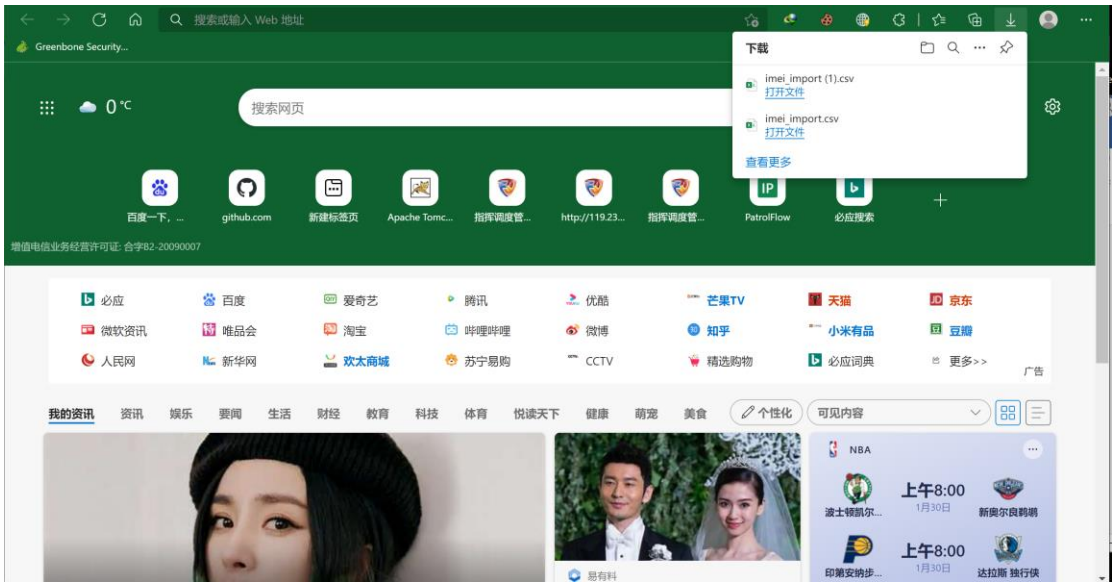


2、以 IP：http://117.35.109.162:7080/为例

3、进入到系统后，如图，点击 IMEI 管理，再点击导入，下载 execl 模板，抓包

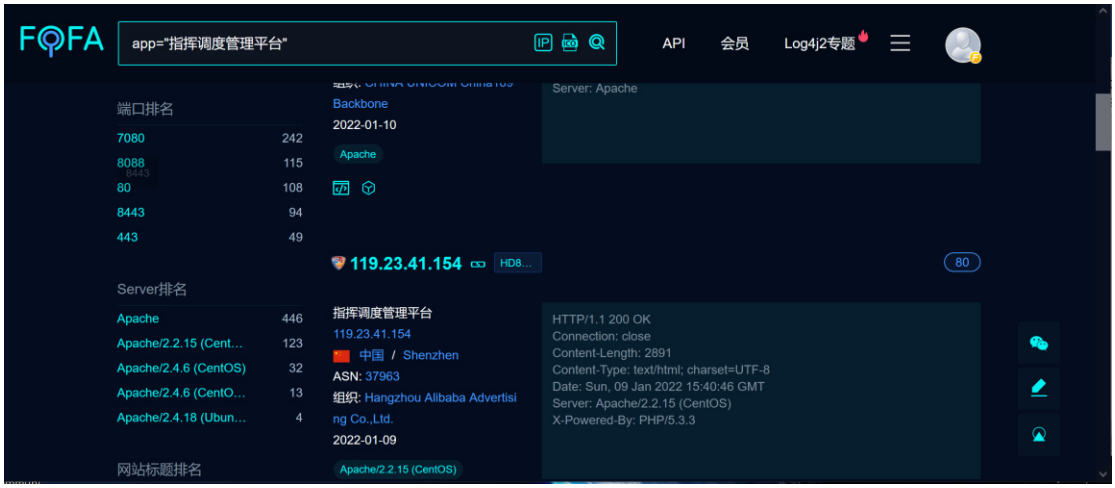


4、复制下载链接，更换浏览器进行访问，成功未授权下载文件



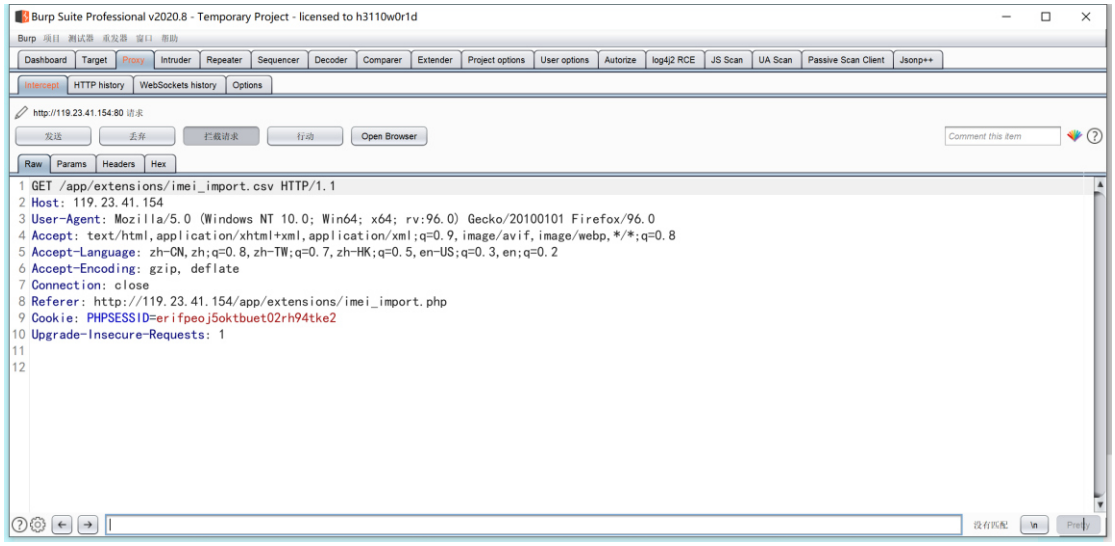
复现三

1、fafo 搜索：app="指挥调度管理平台"

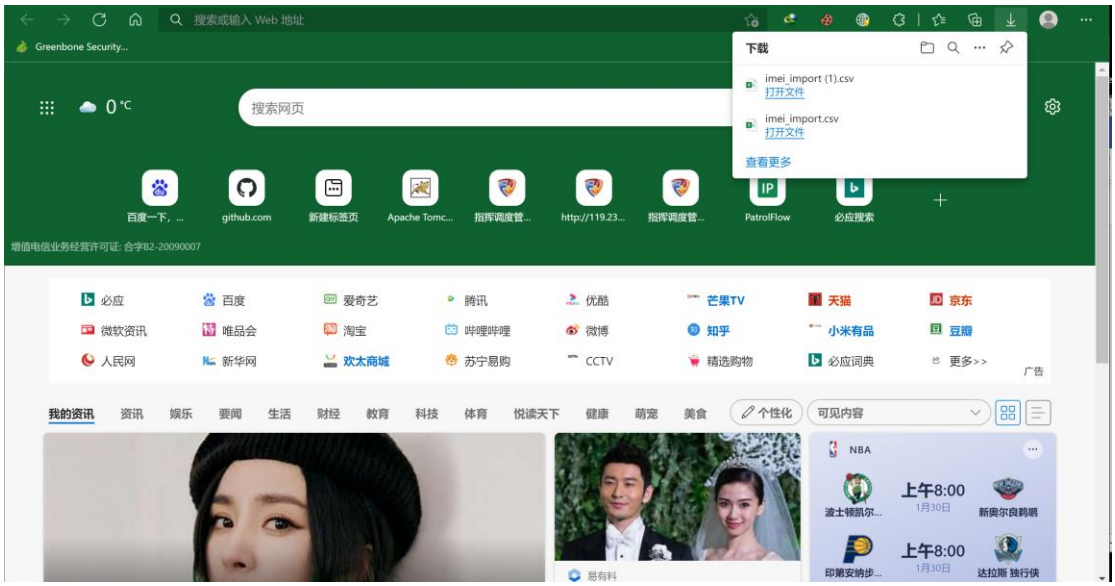


2、以 IP：http://111.21.226.162:7080/为例

3、进入到系统后，如图，点击 IMEI 管理，再点击导入，下载 execl 模板，抓包



4、复制下载链接，更换浏览器进行访问，成功未授权下载文件



其余 URL

http://124.71.107.89:8088/
http://222.173.80.222:7080/
http://123.160.244.201:8443/
http://120.194.221.68:8443/
http://220.182.61.60:8088/
http://218.56.180.159:8443/
http://58.213.91.232:8088/

四、修复建议

a) 在后台进行有效的身份验证及访问控制。此类漏洞通常会整站存在，所以在修复时需要进行全局修复。

b) 针对请求增设 token 设置，校验每次请求的真实有效性