# 简述appscan工具的三种扫描方式

**注意事项：**

1.不管用什么方式扫描，一定记得每次扫描后保存scan文件、生成pdf报告。任意一次扫描结束发现无高、中问题，请妥善保管这两个文件。

2.没有提到的设置均如图默认。

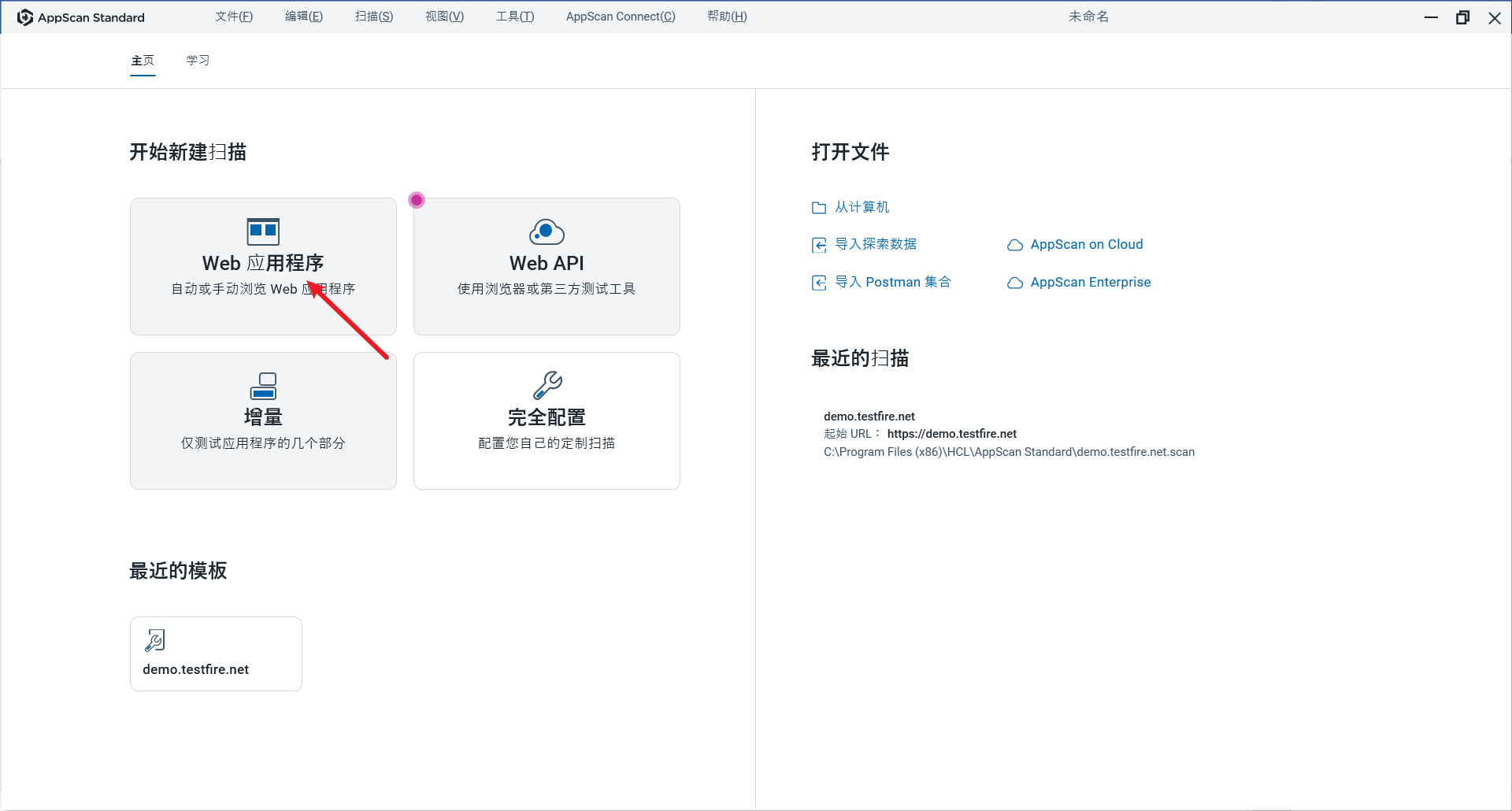
3.扫描过程中有防火墙提示，请点击允许。

## 一、登录扫描方式（常规）

适用范围：appscan内的浏览器可以正常打开登录页面且可以正常进行登录回放**（也就是第9步可用）**

步骤截图：

1.点击web应用程序



2.粘贴登录页面到指示处



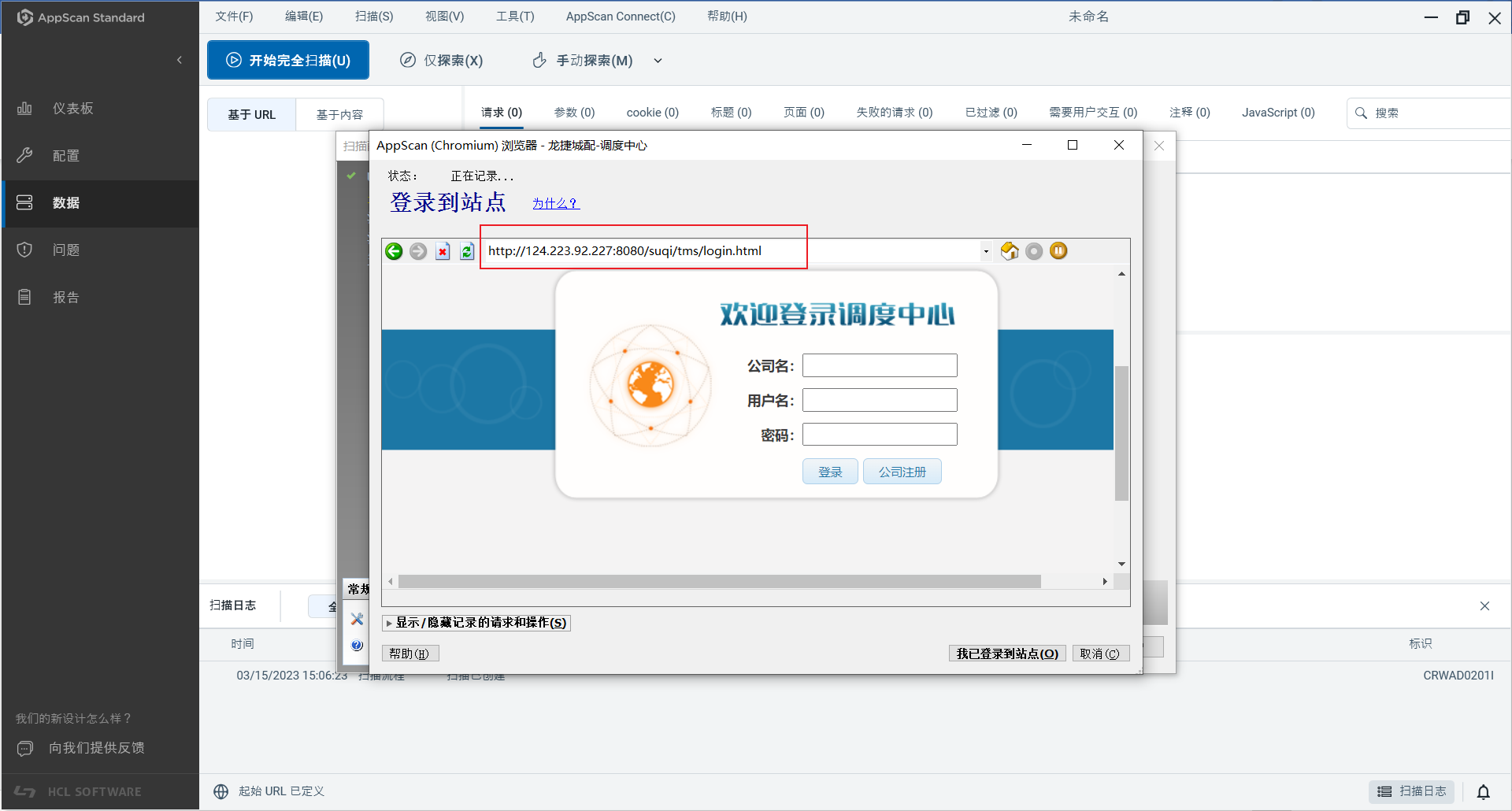
3.点击下一步



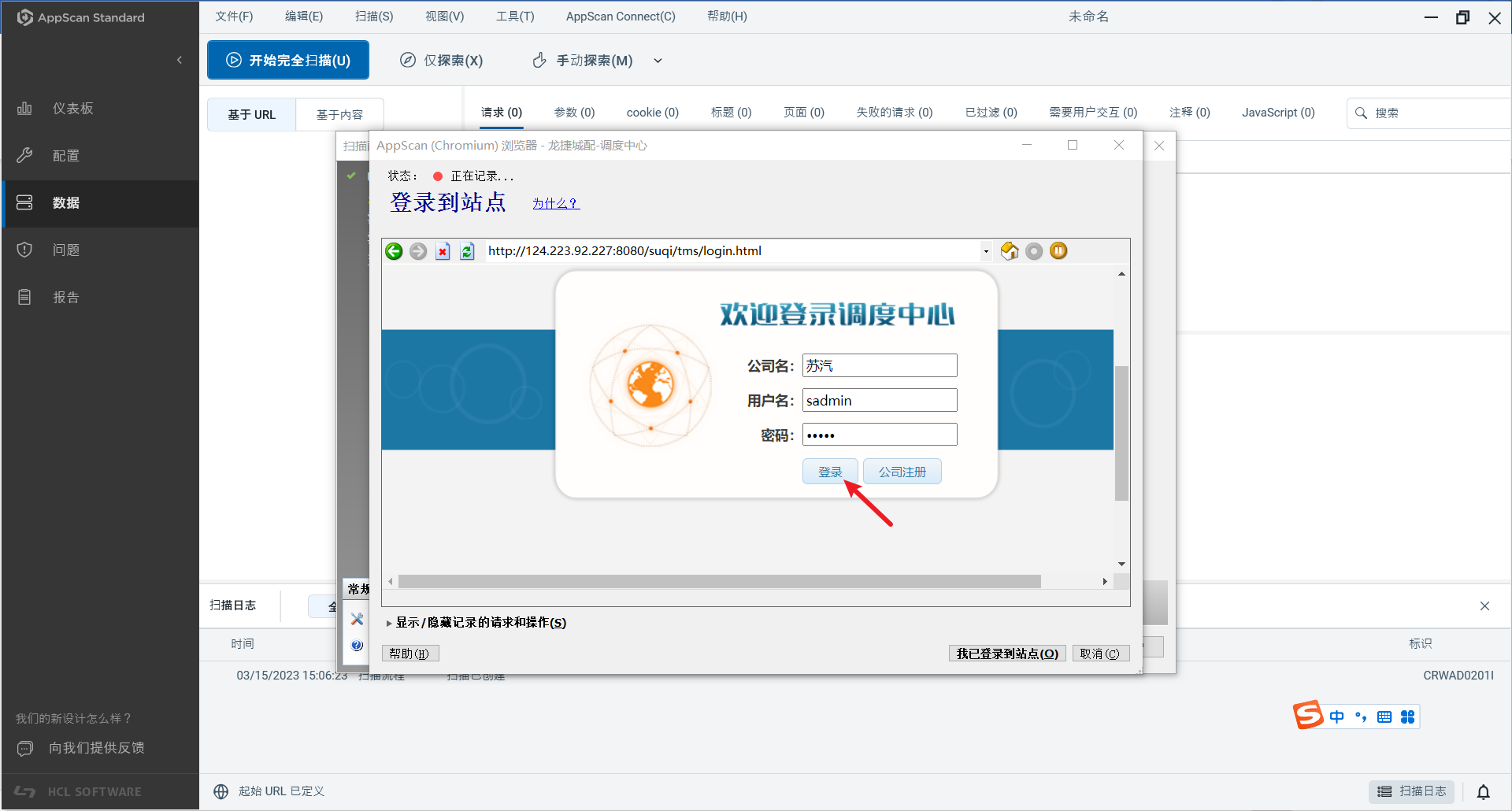
4.选择“记录”选项，点击右边“记录”按钮，选择任意一个浏览器（一般选第一个）



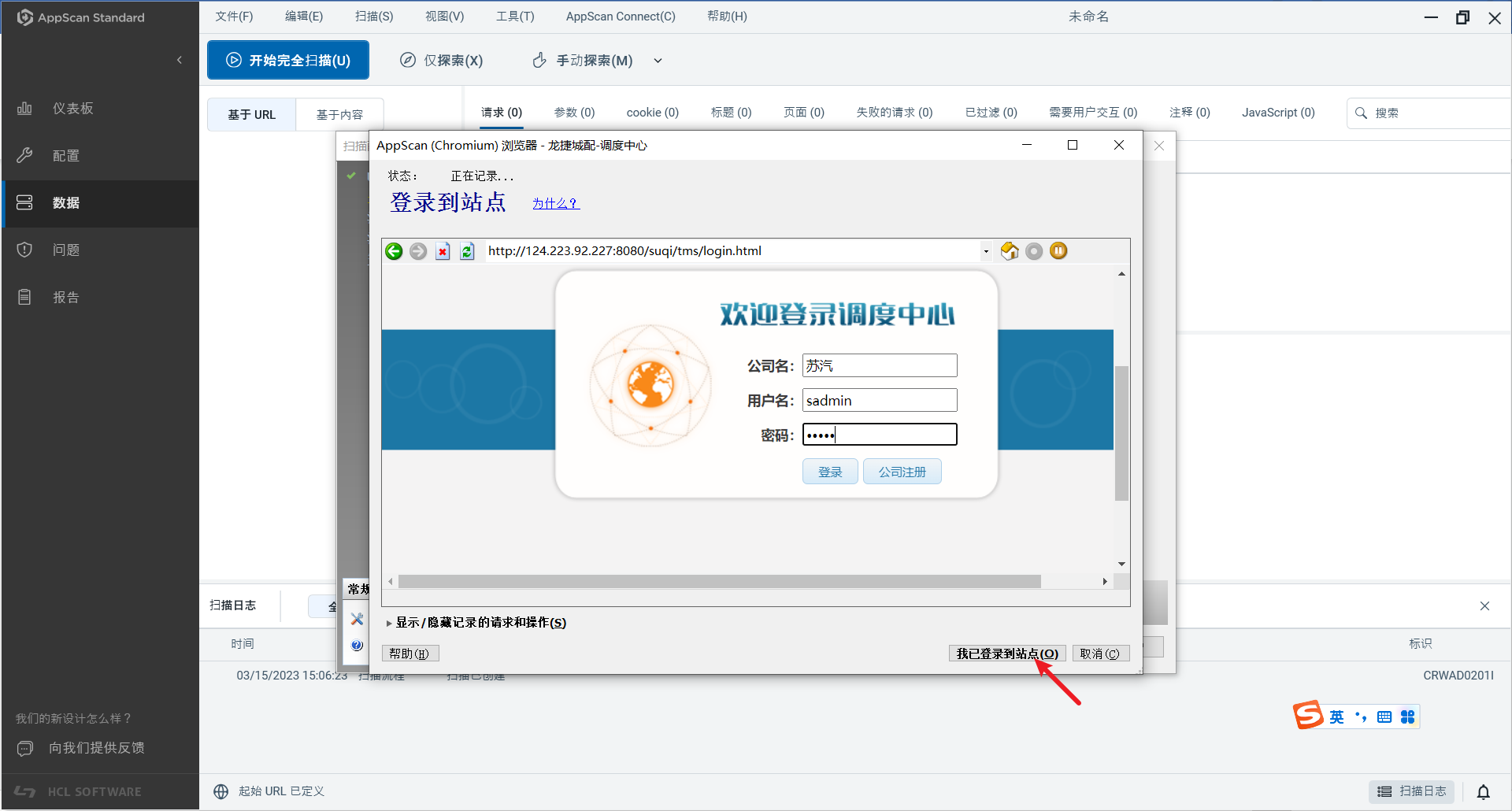
5.弹出登陆页面（如果不能弹出登陆页面，或显示该浏览器不支持，请看第三种扫描方法）



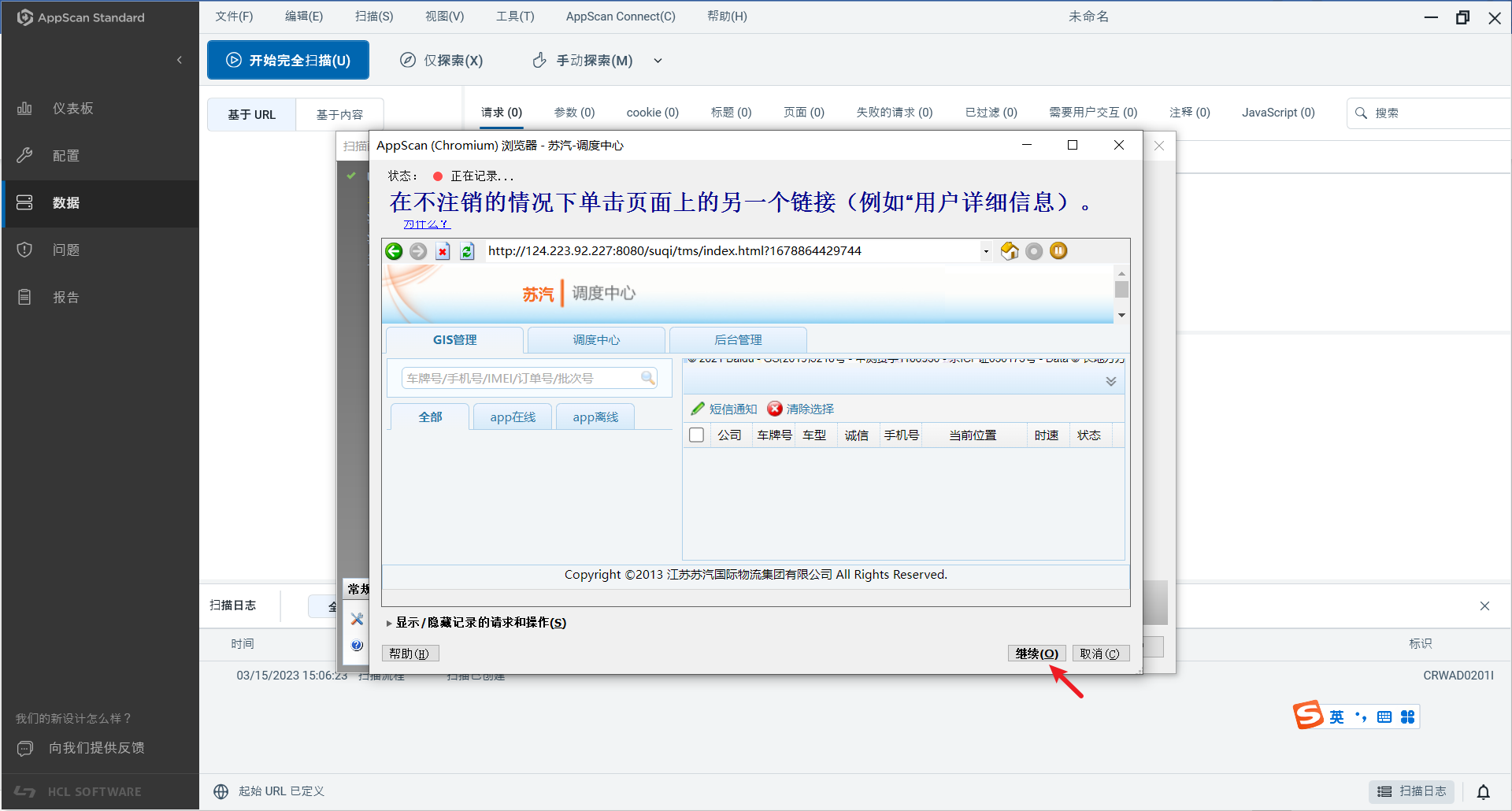
6.输入账号密码，点击登录

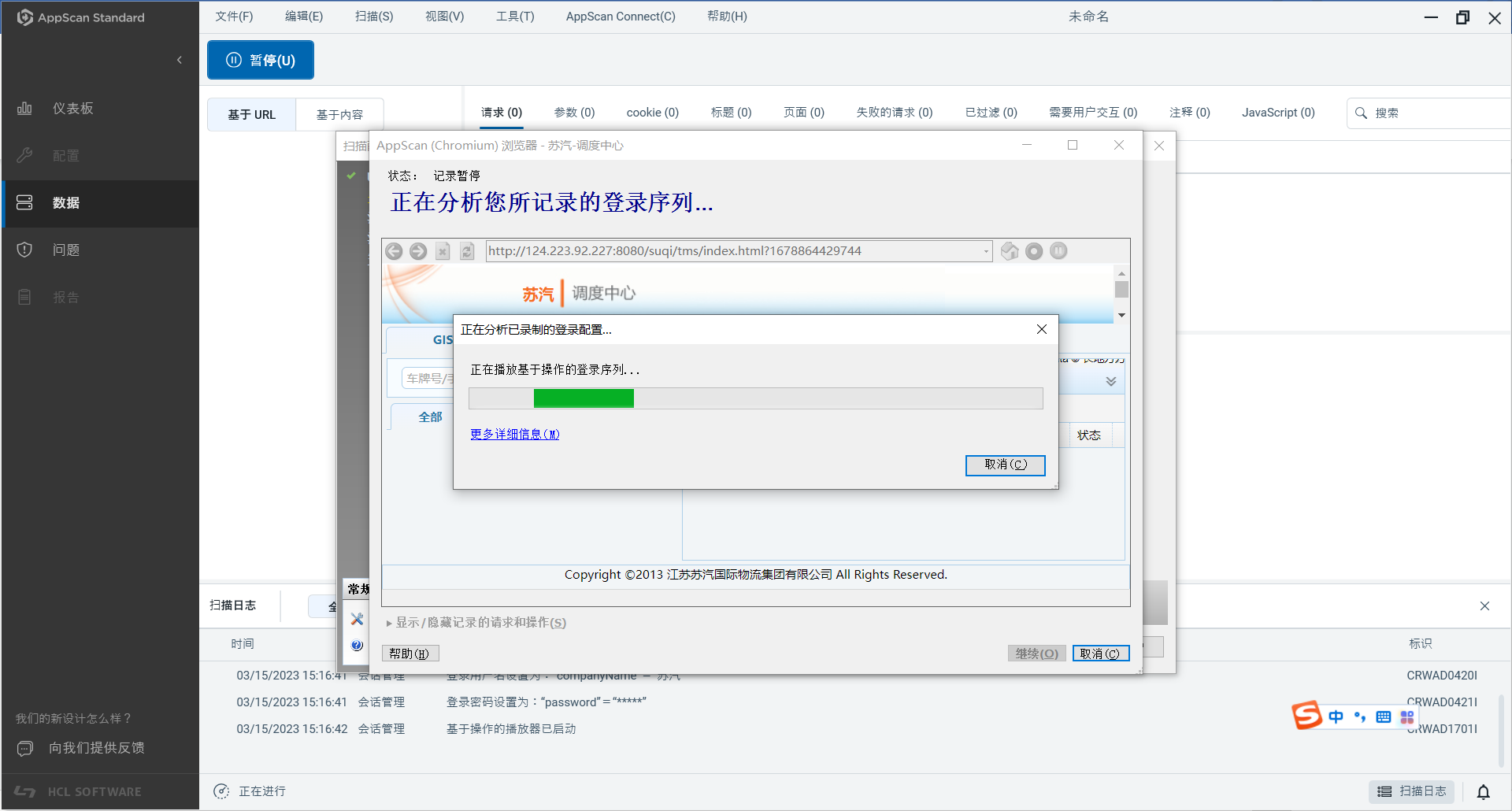


7.登录成功后，点击“我已登录到站点”



8.这个时候注意了，如果是单系统，不用管，直接点继续；如果是登录一个大系统，里面有很多子系统，需要鼠标点击各个子系统，只点击子系统名称不操作，然后点击继续





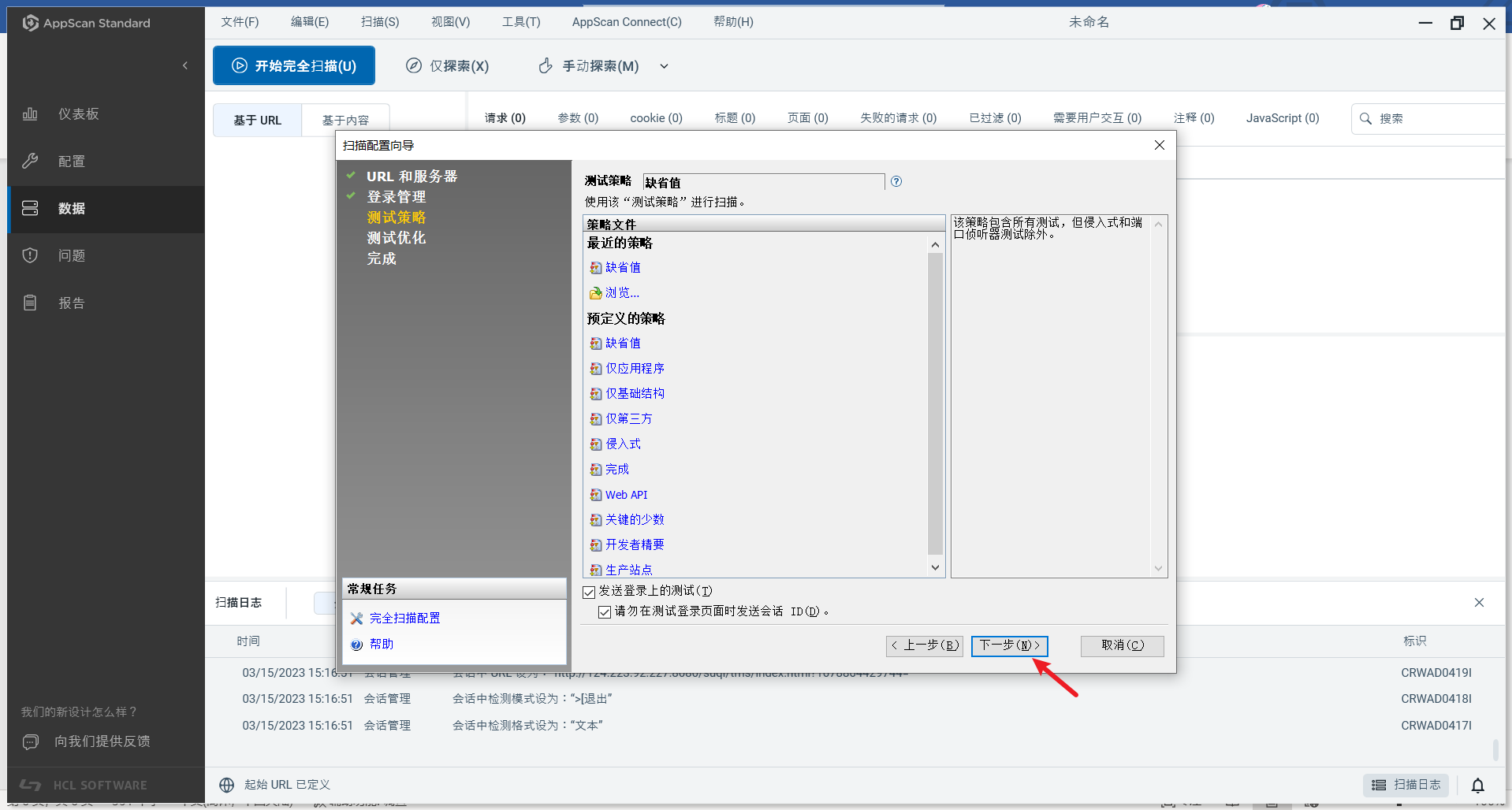
9.正常情况下，会这样显示



10.点击下一步



11.点击下一步



12.选择“无优化”



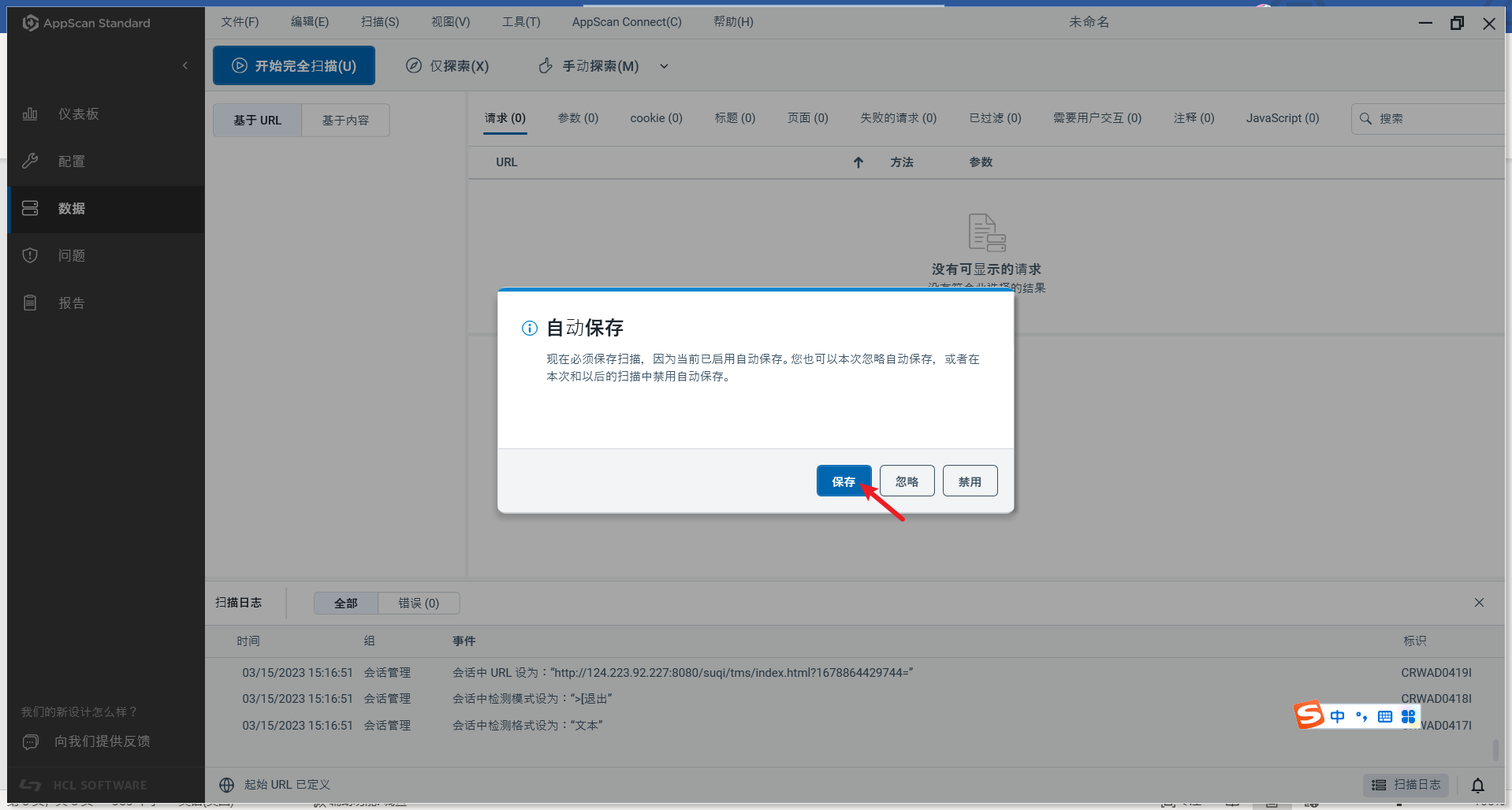
13.点击下一步



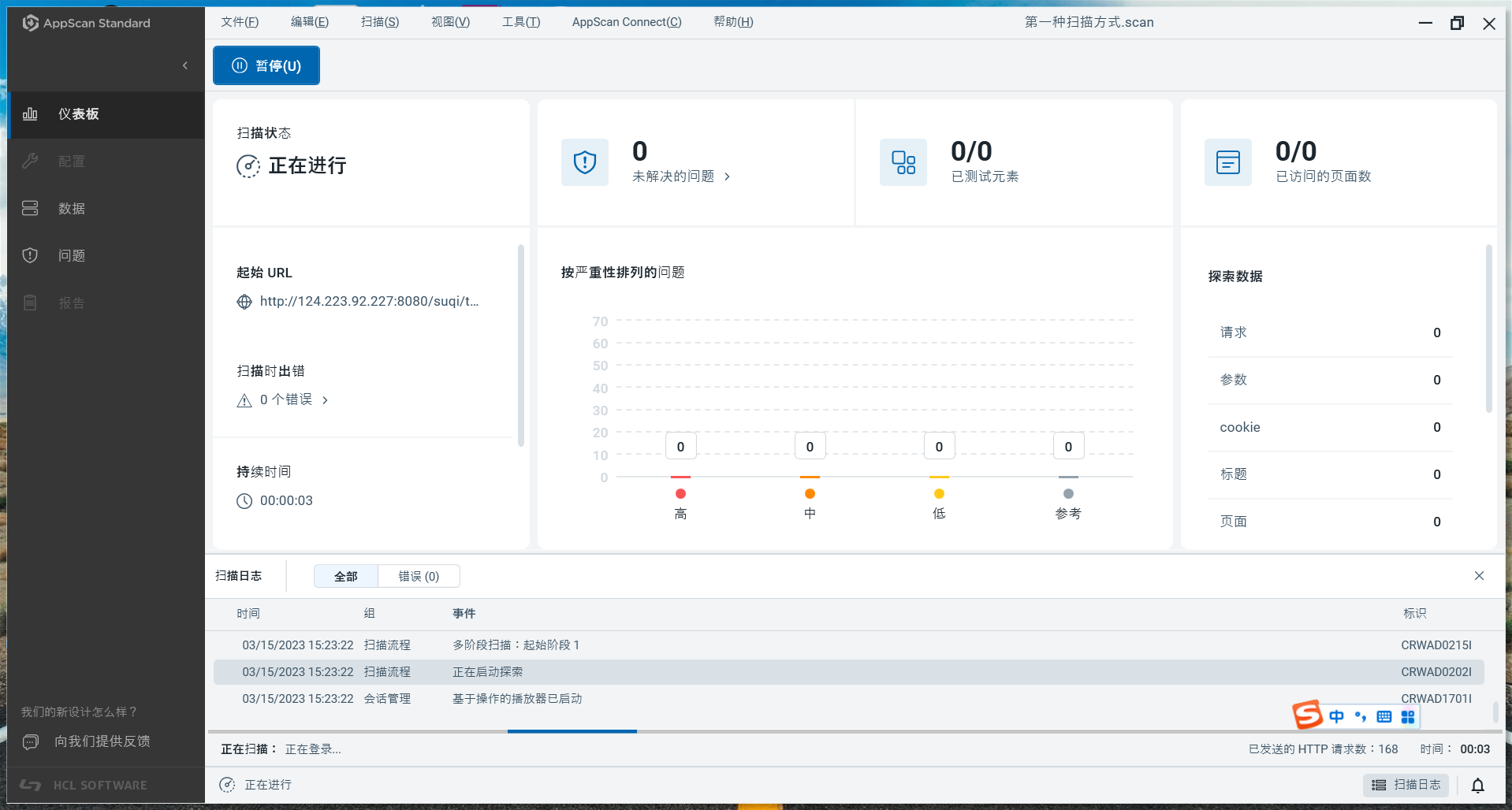
14.选择启动扫描，点击完成



15.提示保存，保险起见，一定要保存（如果忘记，最后也能保存）

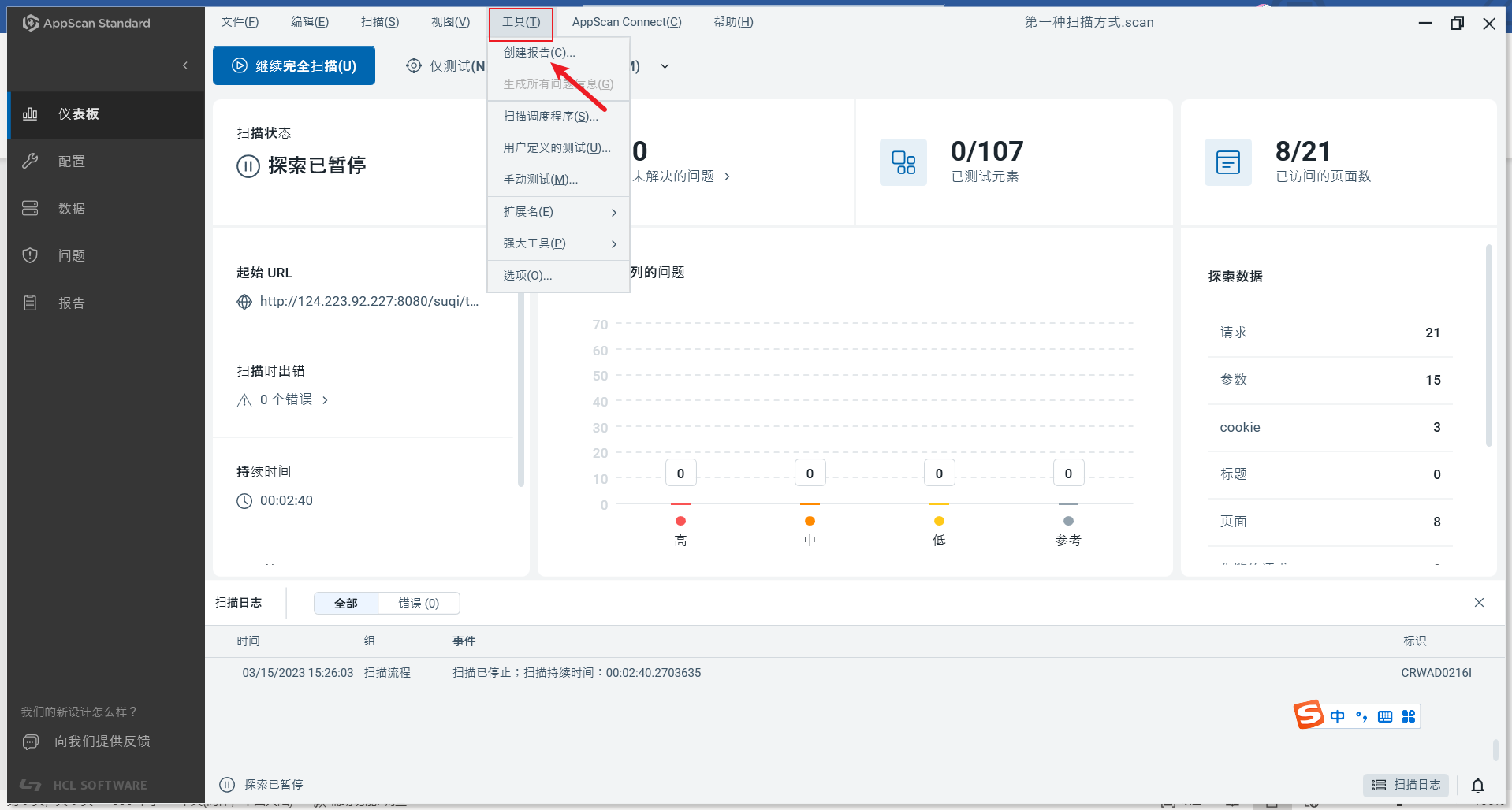


16.保存scan文件到自定义目录，保存后会自动执行扫描

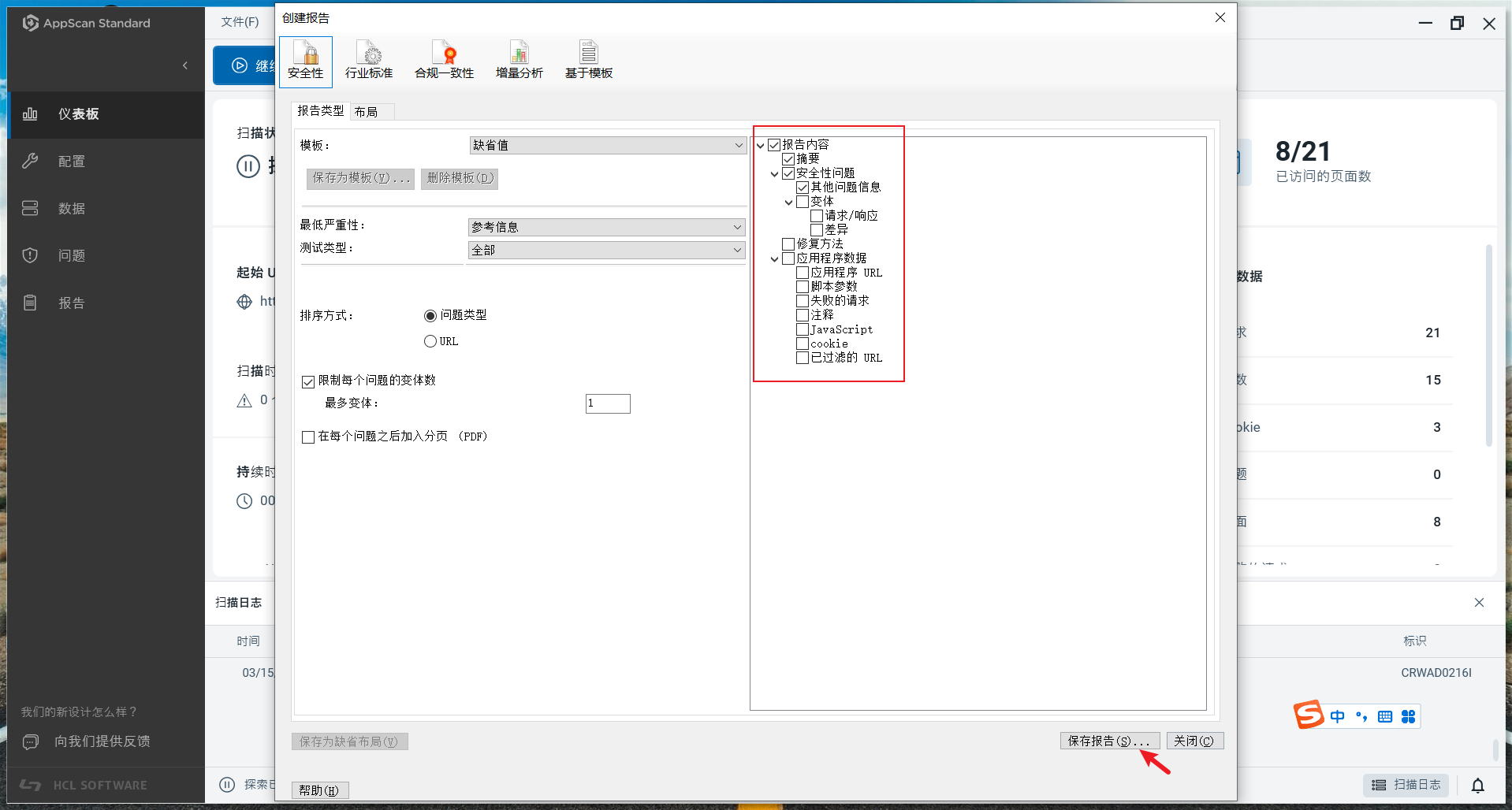


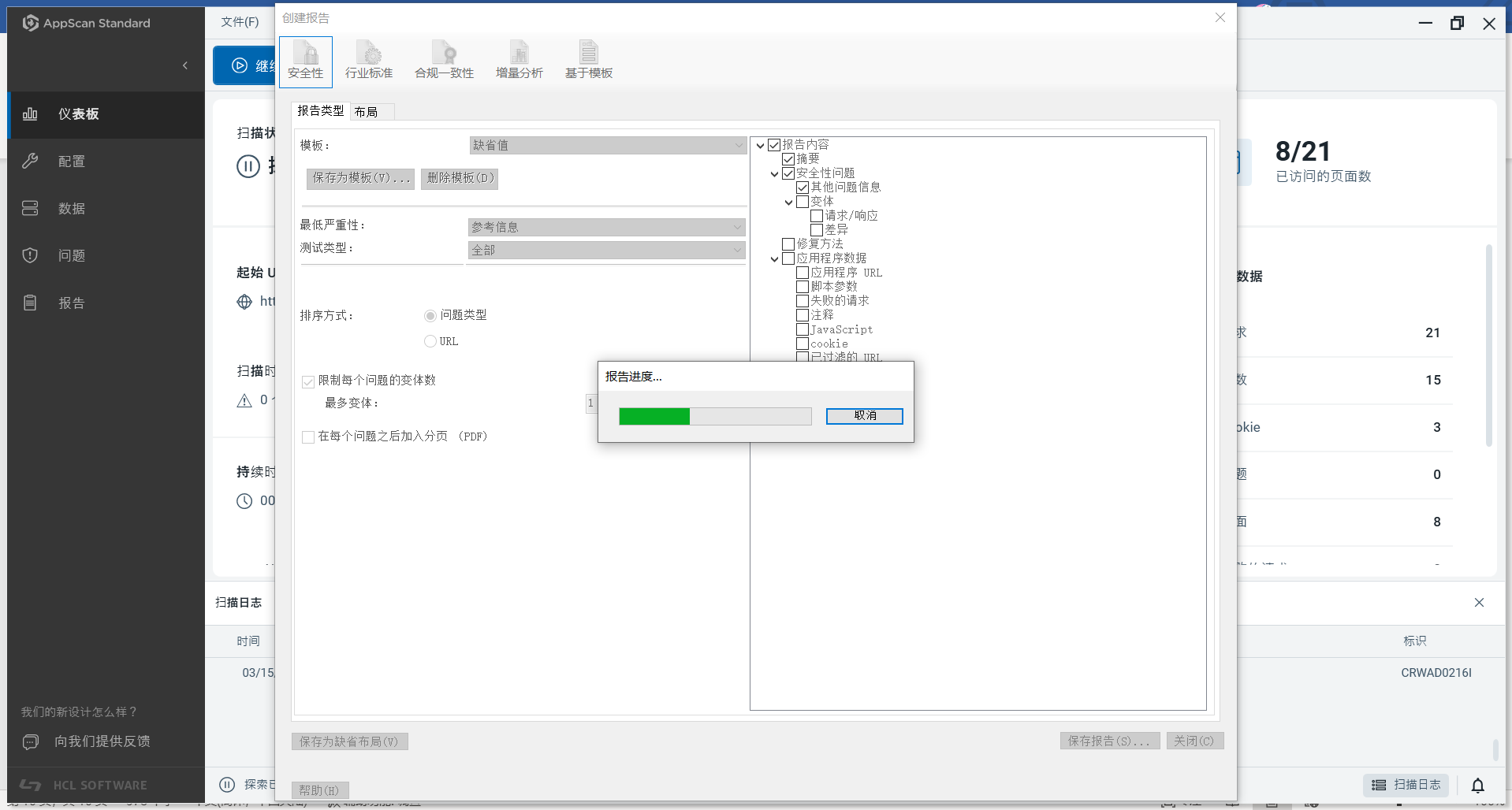
17.等待扫描完成（扫描的节奏是先探索URL，然后再扫描，有时候会分阶段，系统较大时，会比较慢，请耐心等待，过程中如果中断，可点击继续）

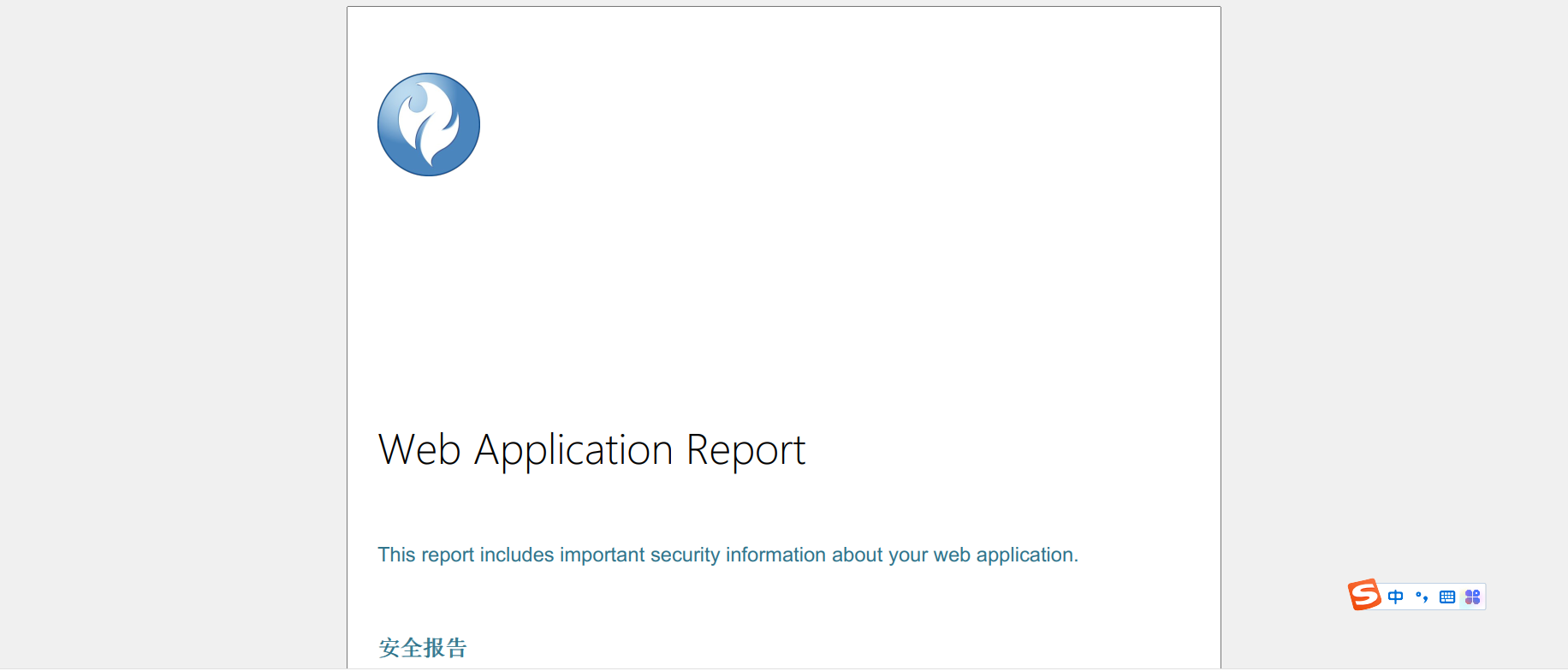
18.扫描过程我就不展示了，扫描结束会有一个扫描已结束的弹窗，然后开始导出报告，路径：工具-创建报告



19.导出报告（红框位置，可选可不选，不影响结果，我习惯都选上，方便开发分析），点击保存报告即可







## 二、无登录扫描方式（好用）

适用范围：

1）appscan内的浏览器可以正常打开登录页面但不能进行登录回放**（也就是第9步不可用，不能成功配置登录），不能显示下面这张图：**



**2）本地使用了vpn进行访问目标地址**

**步骤截图：**

这个时候就要用到第二种扫描方式。

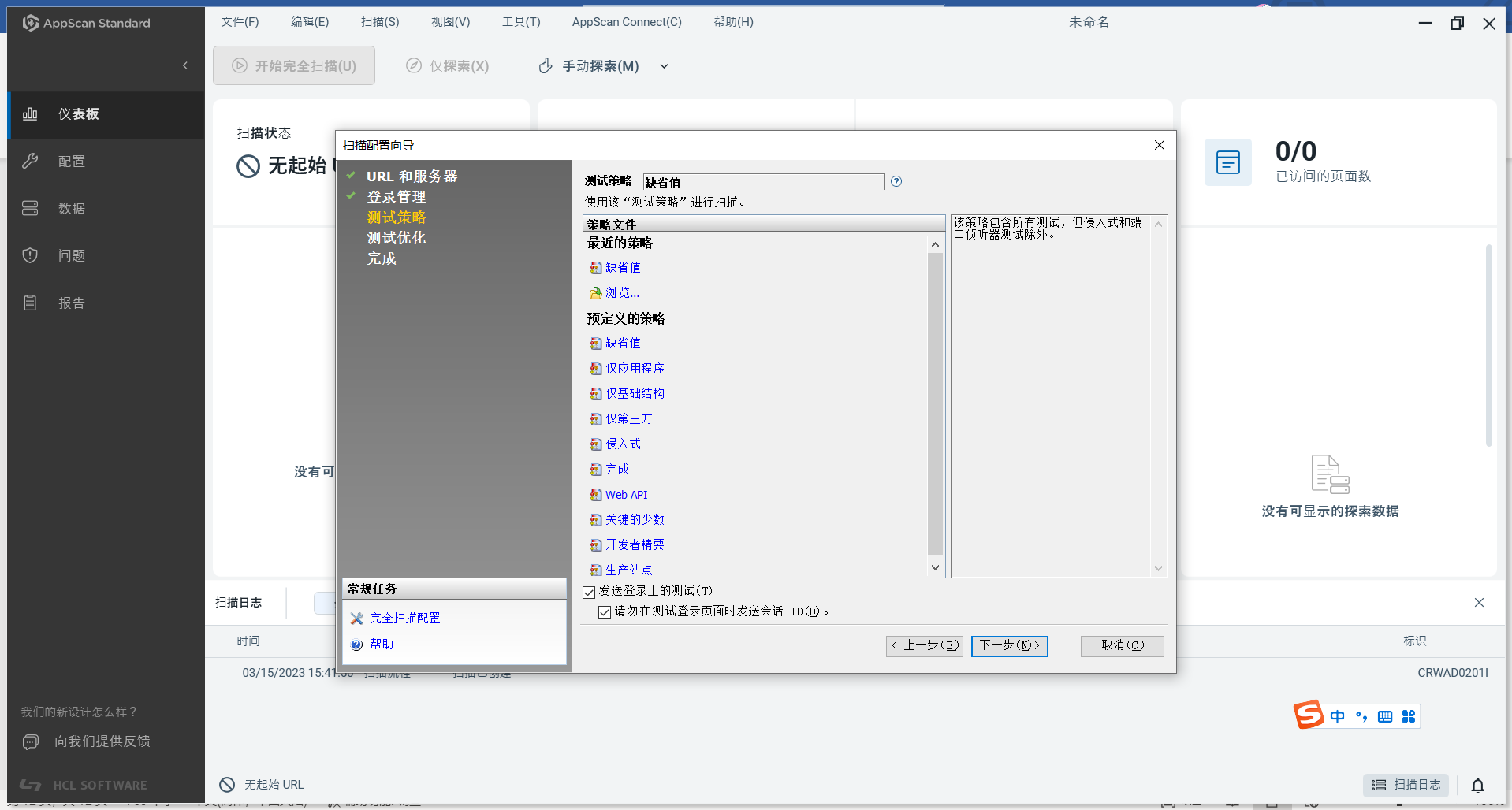
利用第一种扫描方式的步骤，从第4步开始不一致



4.第一种方式选择的是记录，第二种方式要选择无（第四个选项），点击下一步



5.点击下一步



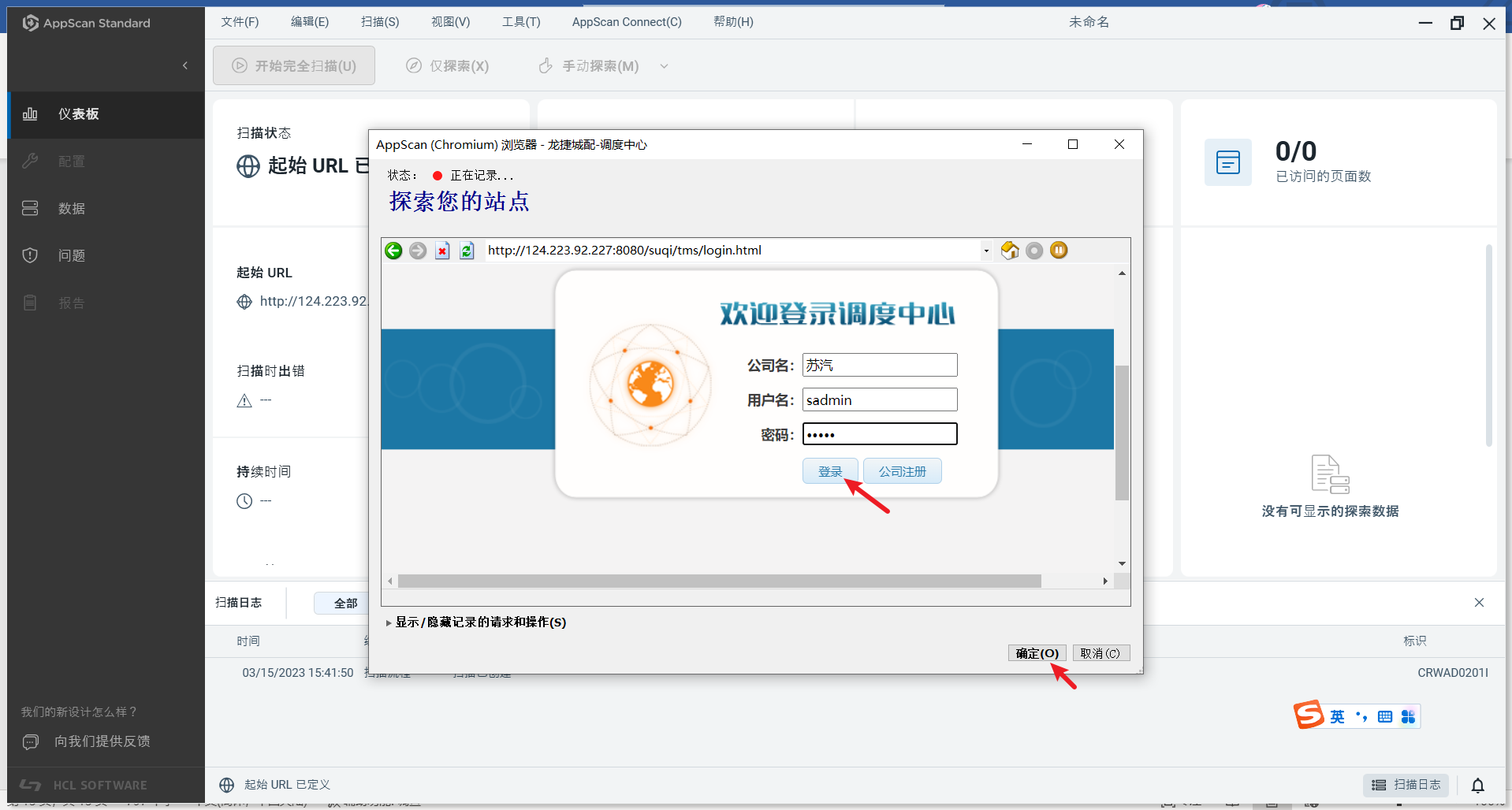
6.选择无优化，点击下一步



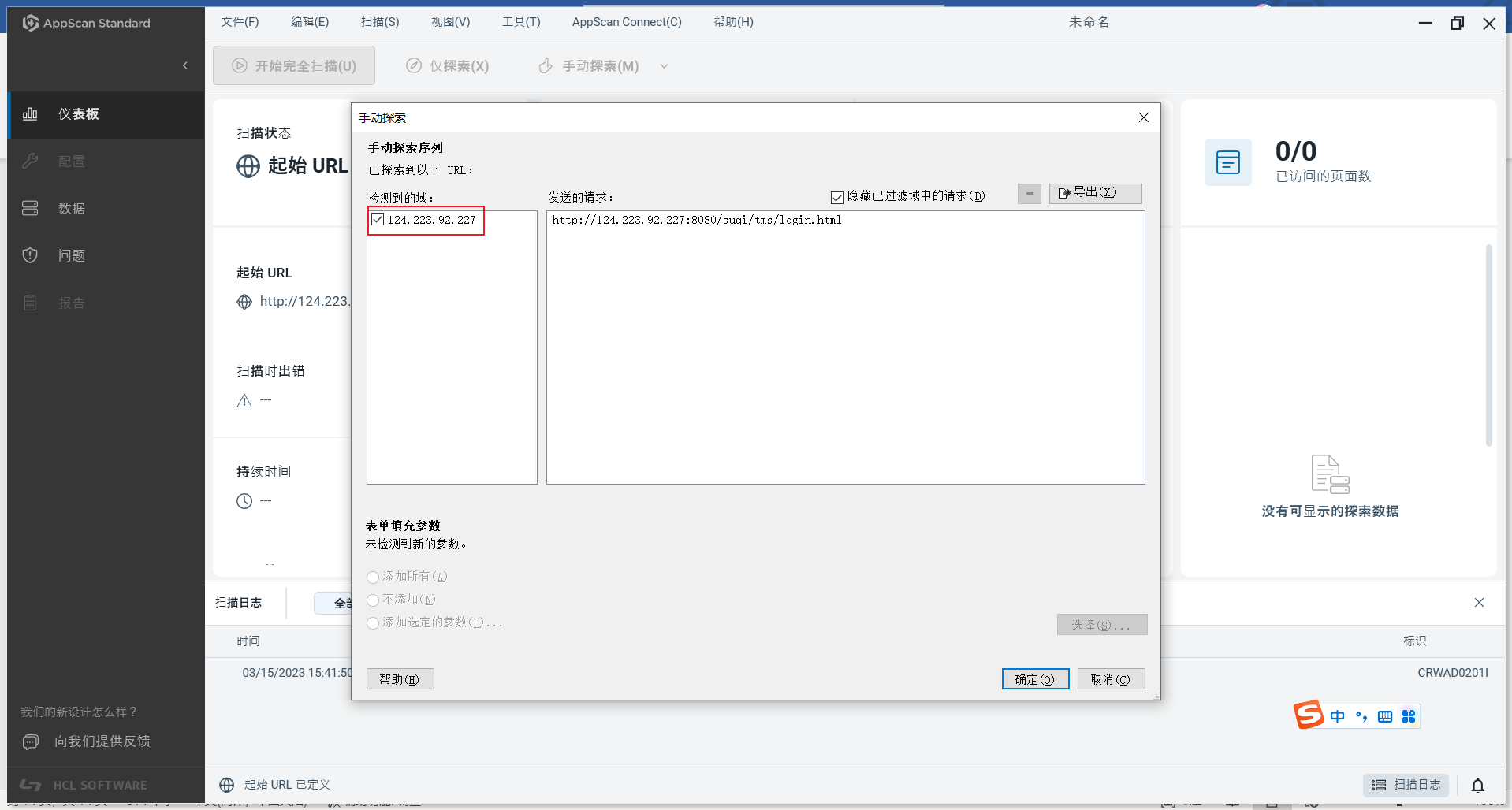
7.选择“手动探索”，点击完成



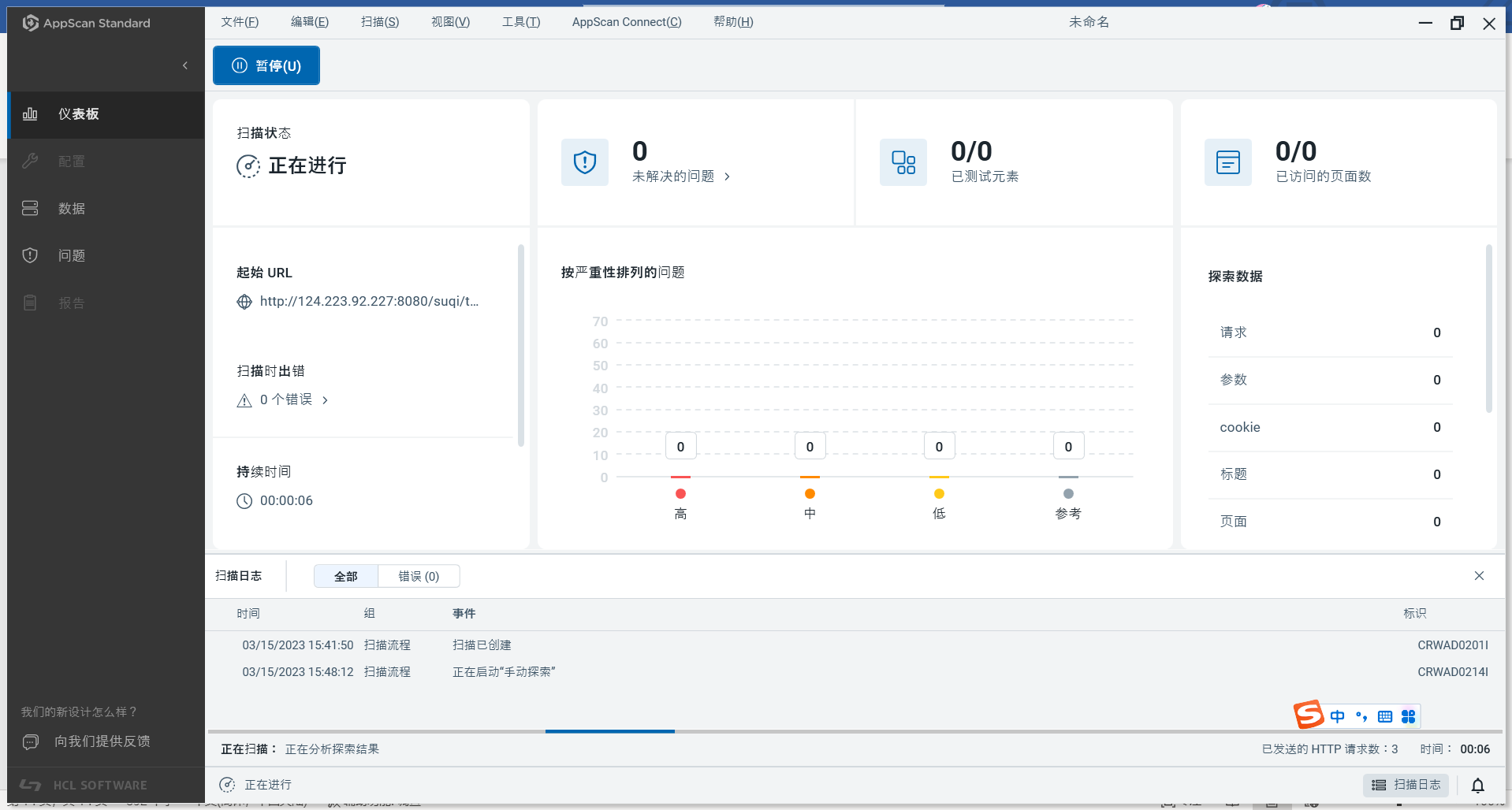
8.输入账号密码，点击登录，再点击确定



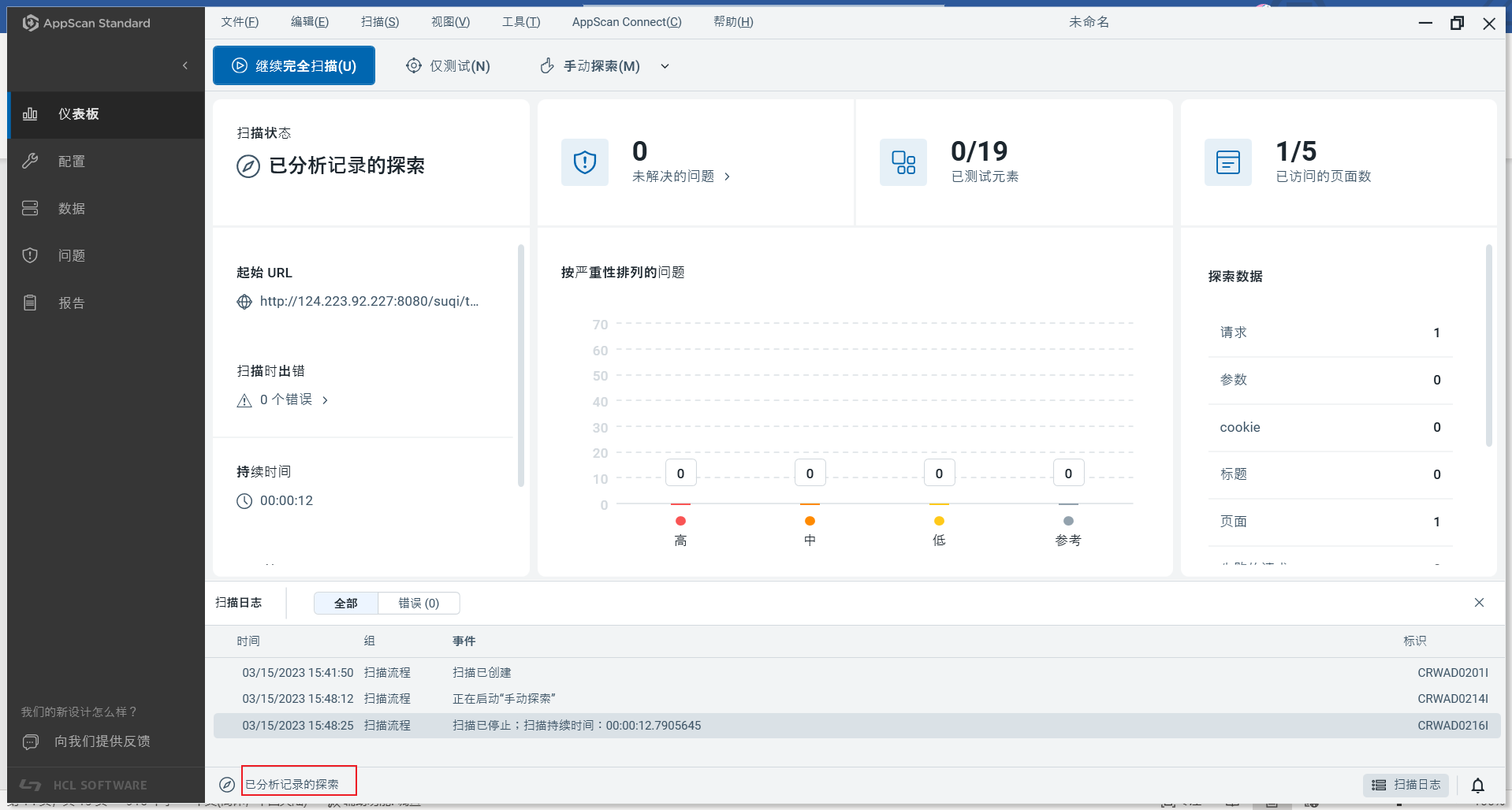
9.会出现目标IP（默认勾选），如果出现其他的，不要点，只点目标IP即可，右侧空白处可能会出现多条URL，不要管，只保证选择目标IP即可，点击确定（如果左右两边或任意一边为空，可以多尝试几次，抓住每一次可行的机会）



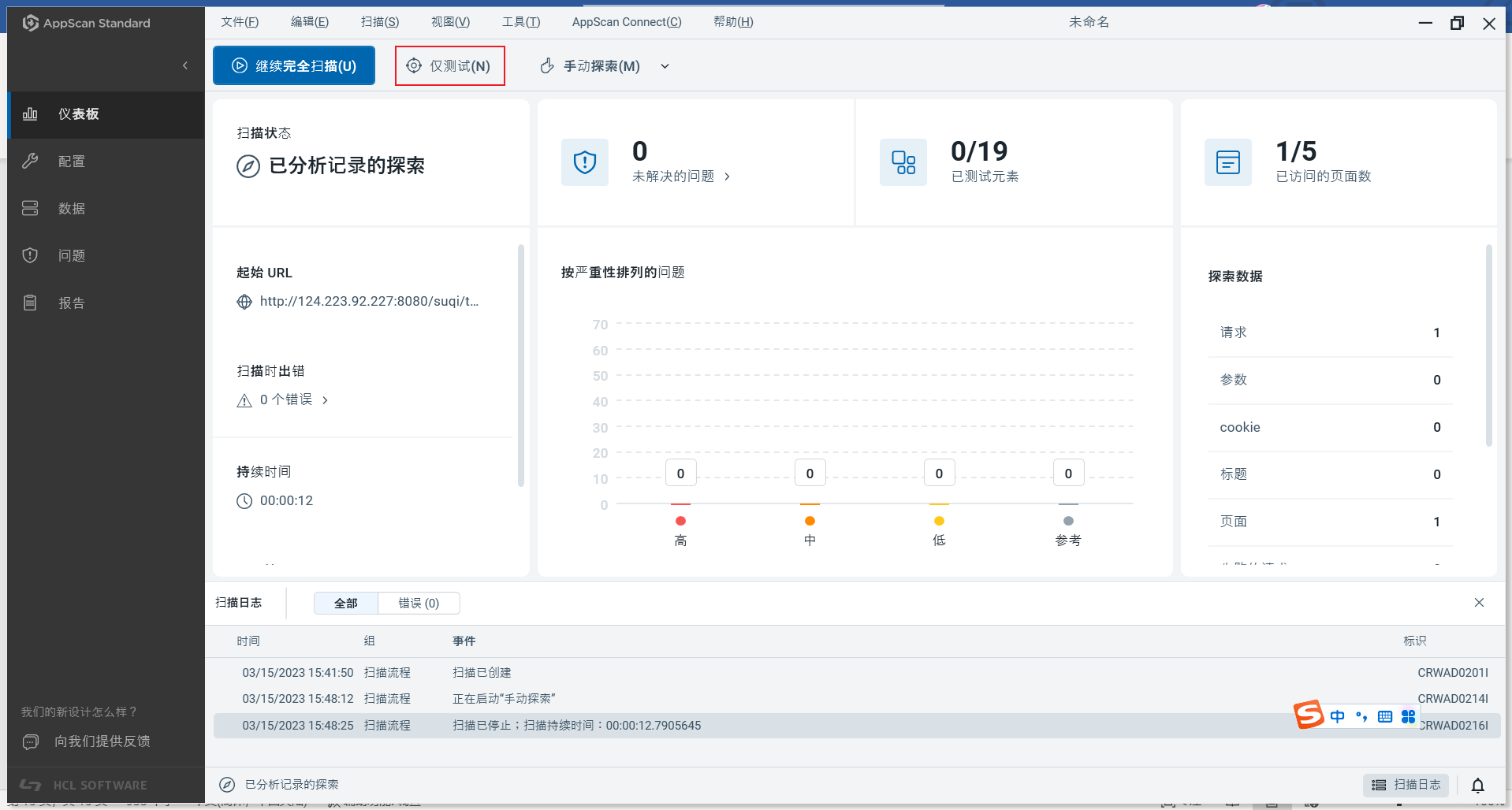
10.进行探索



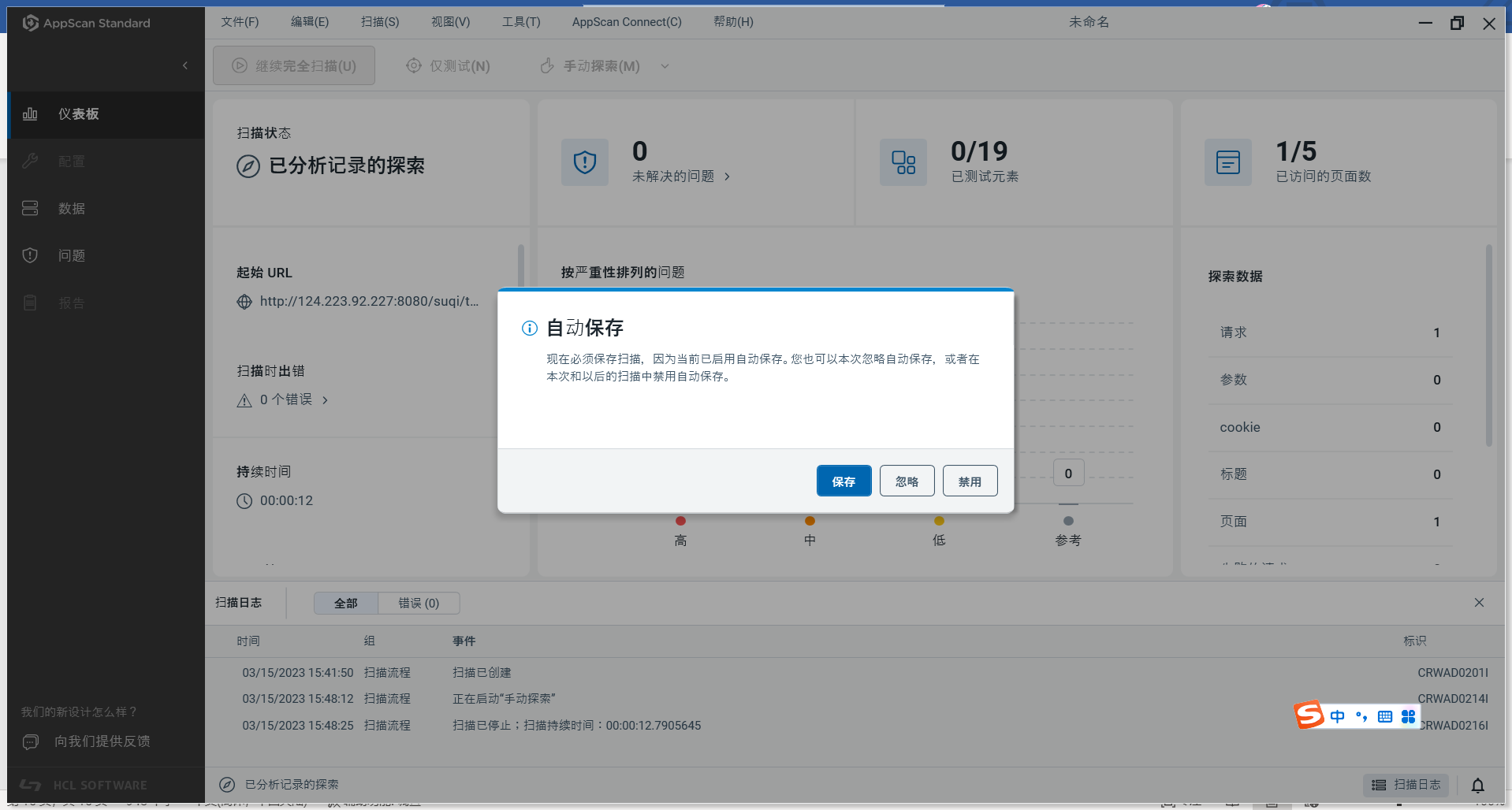
11.探索完成，会有下方的提示



12.点击“仅测试”（其他不要点）



13.保存scan文件后进行“仅测试”扫描（扫描过程中出现通信中断，不用理会，只要最后能提示扫描结束即可）



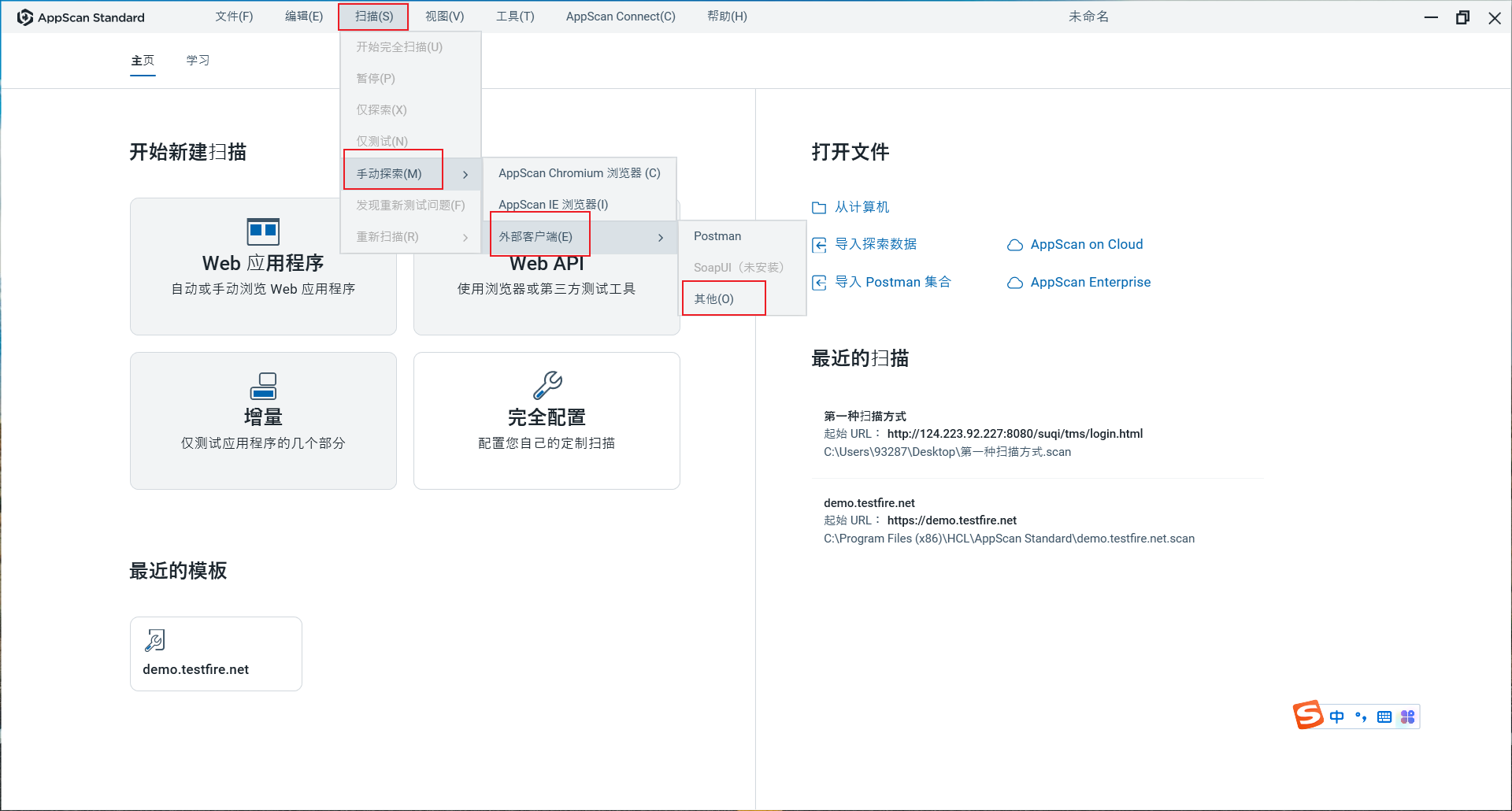
14.后续步骤同方式一

## 三、代理扫描方式

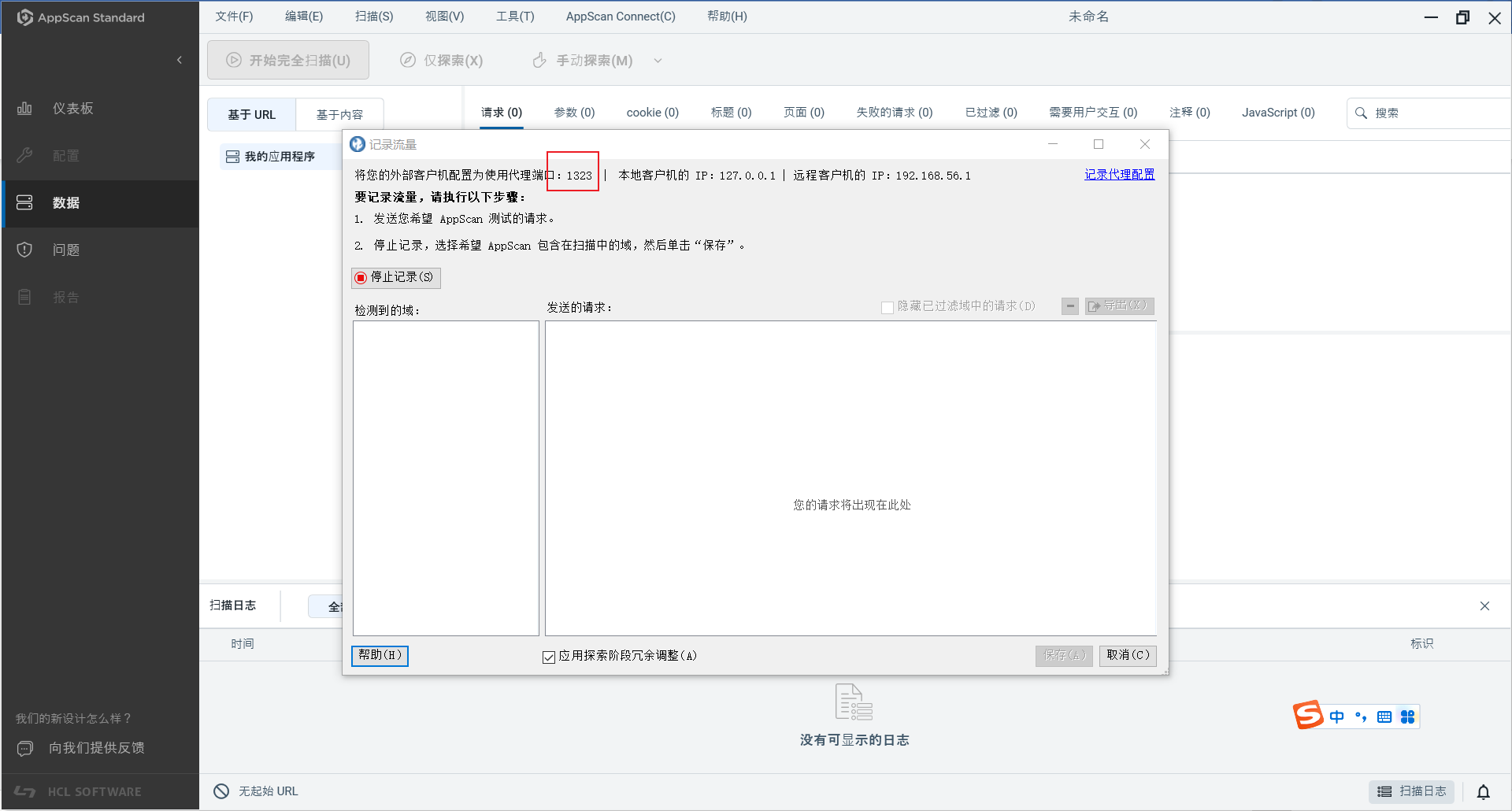
适用范围：appscan内浏览器打不开网页的时候（其实这种方式比较通用，不管能不能登录，都可以用，终极处理方式）

步骤截图：（重新列步骤）

1.依次选择扫描-手动探索-外部客户端-其他

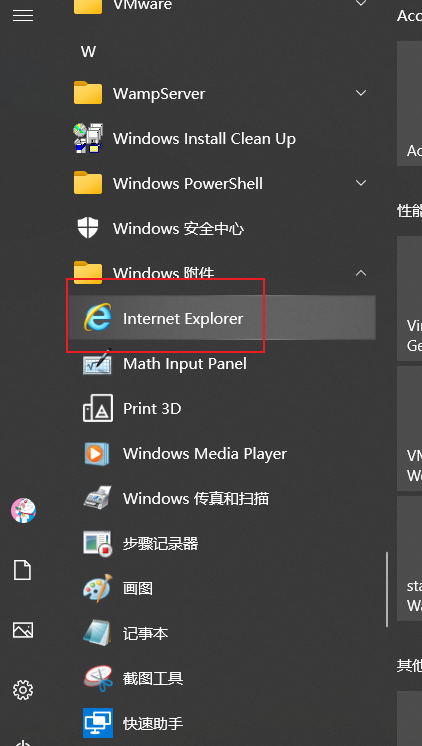


2.弹窗，牢记这个1323端口



3.上面的页面不要动

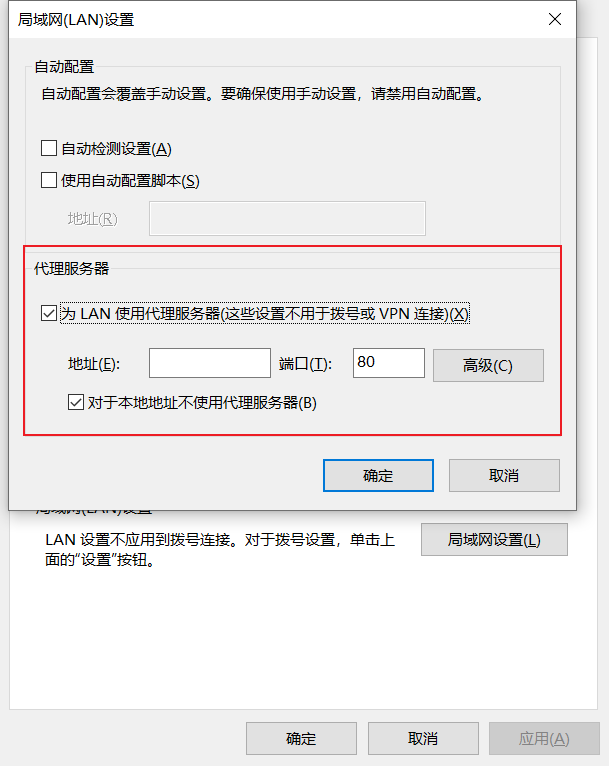
4.找到电脑上的IE浏览器，一般在windows附件下面



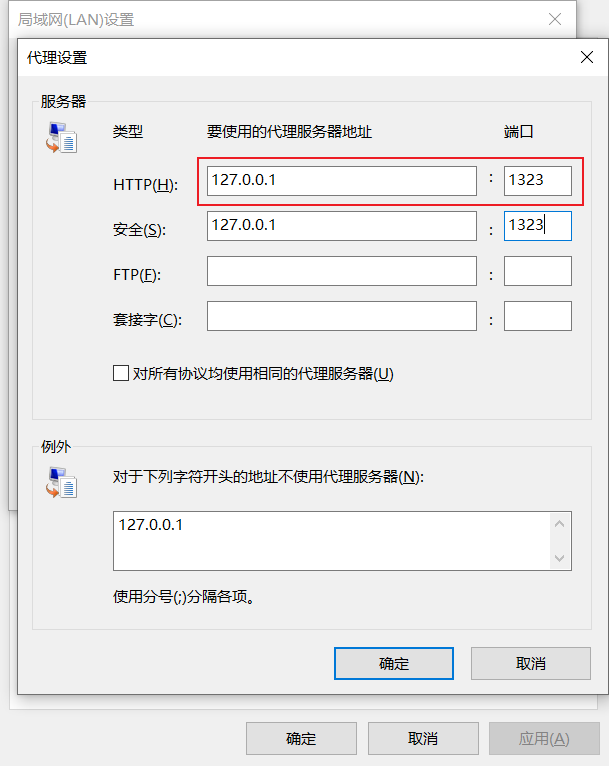
5.打开IE浏览器，点击右上角设置-internet选项，选择“连接”



6.选择局域网设置，勾选“代理服务器”



7.点击高级，如图设置代理IP和端口（端口就是刚才appscan客户端的端口1323，这个端口是动态的，但只要不管刚才端口截图就不会变），点击确定



8.点击确定（应该要点三个确定）

9.回到目标地址页面，进行简单操作（登录或非登录状态下操作均可，简单操作就是任意点击几个页面即可）（可能会有短暂卡顿，请耐心等待）



10.回到appscan页面，这里会出现和方式二一样的格式（我这里没有出现，是当前网络环境配置问题，公安和视频的网络环境均支持此方式），还是在左侧选择目标IP选项即可

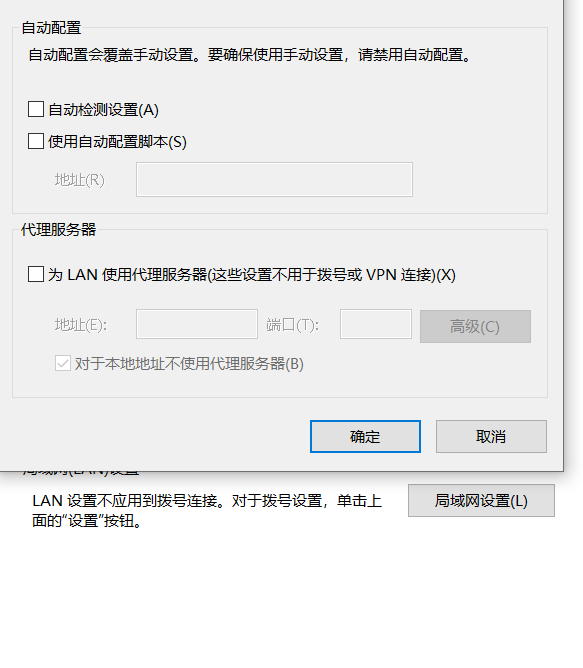


11.最后点击保存

12.然后自动进行探索，再点击“仅测试”，最后生成报告，如果没有保存scan文件，请记得一定要保存scan文件。

注意事项：

完成第三种扫描方式后，记得关闭局域网代理设置，并确定保存，不然可能会影响正常联网操作。



以上为appscan工具三种扫描方式，感谢您的阅读。