APPScan 使用手册

变更记录			
变更日期	变更内容	修订人	版本号
2014/11/10	编订初稿	Nino Ella	V0.1
2014/11/21	增加 AppScan 测试覆盖项说明、注意事项	Nino Ella	V0.1.1
2014/12/10	更新了 9.0 版本的相关特性以及常见问题	Nino Ella	V0.2

目录

1. 引言.....3
   1.1 软件简介.....3
   1.2 编写目的.....3
   1.3 适用范围.....3
   1.4 参考资料.....3
   1.5 说明.....3
   1.6 使用流程图.....4
   1.7 AppScan 测试覆盖项说明.....4
2. 安装运行环境要求.....5
3. 安装流程.....6
   3.1 注意事项.....6
   3.2 软件安装.....6
   3.3 软件破解.....8
4. 使用说明.....8
   4.1 工作面板简介.....9
   4.2 扫描流程配置.....9
   4.3 扫描结果.....16
   4.4 生成报告.....16

1.引言

1.1 软件简介

AppScan 是 IBM 公司推出的一款自动化 Web 应用安全和渗透测试工具。它旨在模拟实际的黑客入侵技术和攻击，对 Web 应用进行爬取及审计，从而找出该应用目前存在的漏洞及风险问题。AppScan 支持在从开发到生产的整个过程中对 Web 应用进行测试，高效管理测试结果，并在整个企业范围内宣传安全知识，从而帮助企业确保大部分易受攻击的输入点免遭攻击。

1.2 编写目的

AppScan覆盖的漏洞范围较广，操作也较为简单。为了方便安全工作的展开，特编写此安装说明书及用户使用手册。

1.3 适用范围

AppScan 的检测对象为 Web 应用和 Web Service，包括：Adobe 的 Flash，JavaScript，Ajax 和简单对象访问协议（SOAP）的 Web 服务。

AppSccan 使用手册的阅读对象包括项目经理、QA、测试人员、安全评估人员等。

1.4 参考资料

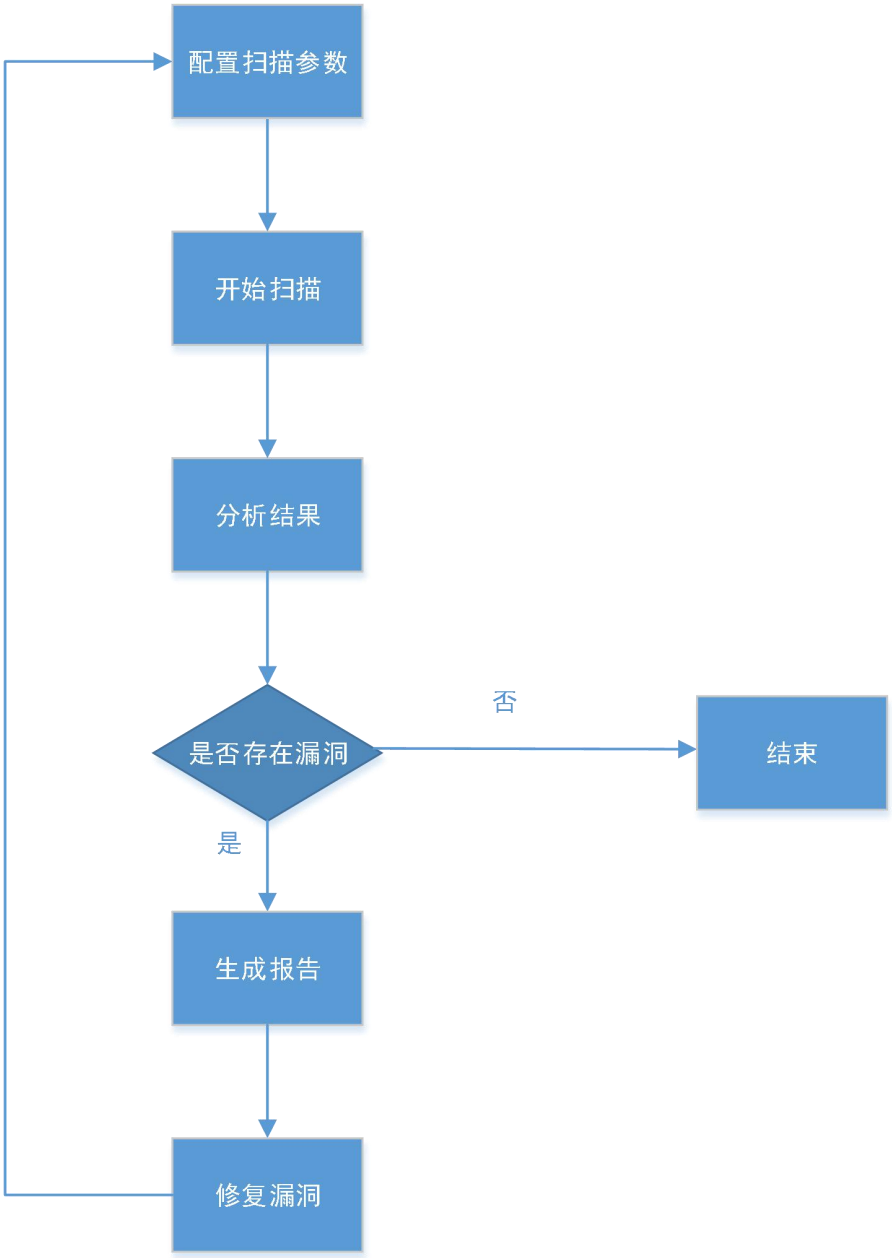
- 《AppScan Getting Started Guide》
- 《AppScan User Guide》
- http://www.ibm.com/developerworks/cn/downloads/r/appscan/

1.5 说明

- 目前使用的是 Appscan 9.0.0.0 的破解版，破解工具可能带有木马后门。
- AppScan 在扫描过程中可能带有攻击性，具有一定的风险。
- 该使用手册目前仅涉及对 Web 应用的测试，Web Service 有待后续补充。
- 建议先去掉 Web 应用的验证码或密码提示问题功能，然后再使用 AppScan 进行扫描。
- 使用 AppScan 对被测系统的性能影响比较大，而且可能导致一些垃圾数据，建议只在测试环境执行。
- 由于自动化工具在很多情况下只是提示一种漏洞存在的可能，因此需要对所有的结果进行人工的分析判断，可以使用辅助工具或者是手动验证。

1.6 使用流程图

软件使用流程图如下图所示：



1.7 AppScan 测试覆盖项说明

自动化测试工具 AppScan 涉及如下测试项：

- 参数操作
  - 跨站脚本
  - SQL注入
  - 代码执行
  - 文件包含

- 脚本源代码检查
- CRLF注入
- Cross Frame Scripting (XFS)
- PHP代码注入
- XPath注入
- 全路径泄漏
- LDAP注入
- Cookie 操作

■ 文件检查

- 检查备份的文件及目录
- URI中的跨站脚本
- 检查脚本错误

■ 目录检查

- 查找常见的文件
- 发现敏感的文件和目录
- 发现存在弱权限控制的目录
- 路径和SESSIONID中的跨站脚本

■ 文本搜索

- 目录列表
- 源代码泄漏
- 注释信息搜索
- 常见文件检查
- Email地址收集
- 本地路径泄漏
- 错误信息

■ Google Hacking

2.安装运行环境要求

环境	配置	配置标准
硬 件要求	处理器	Core 2 Duo 2 GHz (或同等处理器)
	内存	3GB RAM
	硬盘容量	30GB
软 件要求	操作系统 (32/64 位)	● Windows 8 ● Windows 7 ● Windows XP Professional with SP3、SP2 ● Windows Server 2008：Standard 和 Enterprise with SP1、SP2 ● Windows Vista： Business， Ultimate 和 Enterprise with SP1、SP2

	浏览器	Microsoft Internet Explorer V6 或更高版本
	其他	Microsoft.NET Framework V4.5 (可选)需要 Adobe Flash Player for Internet Explorer 10.1.102.64，以用于 Flash 执行 (可选)用于定制报告模板的 Microsoft Word2007、2010 和 2013

3.安装流程

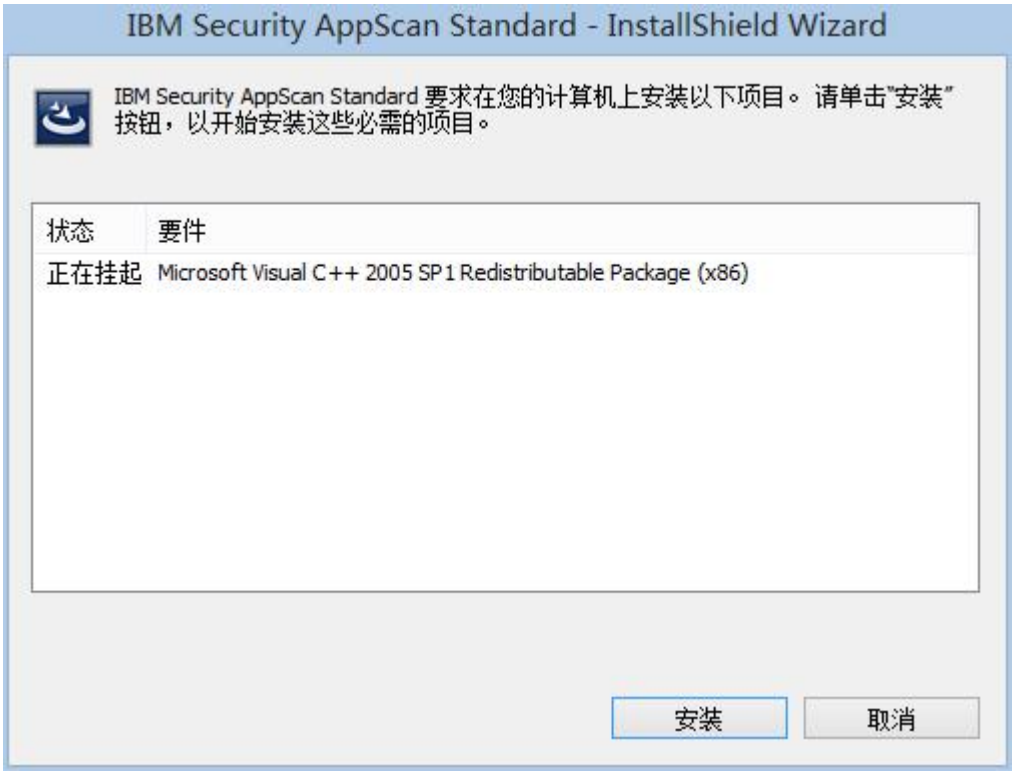
3.1 注意事项

1. 请关闭已打开的任何 Microsoft Office 应用程序。
2. 启动 Rational AppScan 安装并遵循在线指示信息。“安装向导”会指导您快速简单地完成安装。
3. 安装完成后将询问您是否要安装/下载 GSC（通用服务客户机），如果要探索 Web Service 以配置 Web Service 扫描，那么 GSC 是必要的，如果仅扫描 Web 应用程序，就不是必要的。

3.2 软件安装

在安装 Appscan9.0 版本之前，需要安装 Microsoft.NET 4.0 版本。

1. 双击 APPS_STD_EDI_9.0_WIN_ML_EVA.exe.，选择“中文（简体）”安装语言后进入安装向导，点击“下一步”，提示安装 Visual C++2005 。



2. 点击“安装”，进入软件许可协议，选中“我接受许可证协议中的全部条款”选项。
3. 点击“下一步”，进入安装目录设置，设置安装路径。
4. 点击“下一步”，开始安装程序。

5. 安装完成后提示是否下载安装 Web Service 相关组件（GSC），根据需要进行

选择。若不涉及 Web Service 的扫描，则选择 “否”。

6. 进入安装完成页面，取消立即运行 IBM Rational AppScan 选项，点击“完成”。

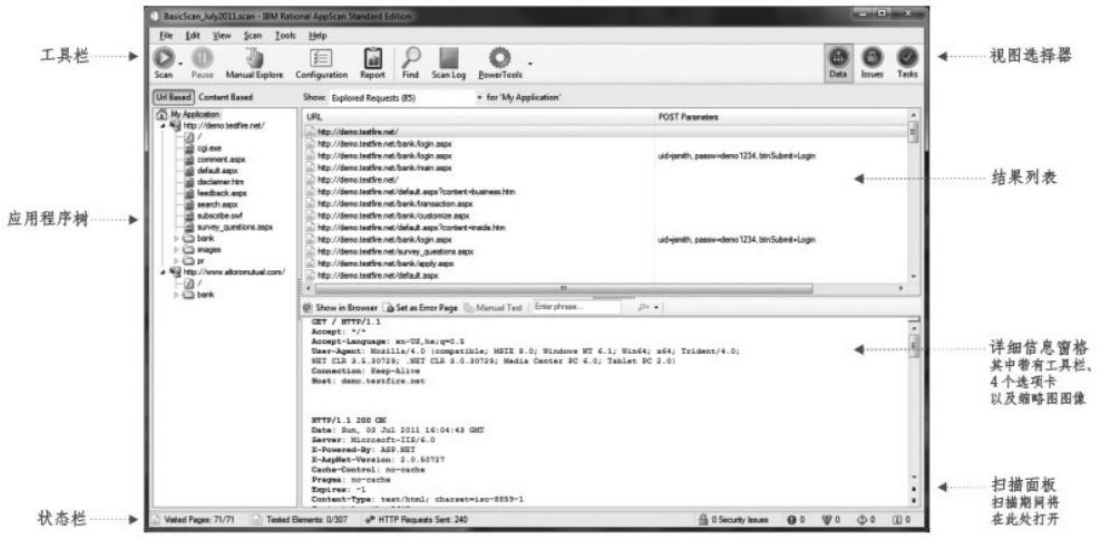
3.3 软件破解

找到 Appscan 的安装目录，使用破解的 LicenseProvider.dll 替换原安装目录下的 LicenseProvider.dll 文件。

4.使用说明

4.1 工作面板简介

AppScan 的工作面板包含菜单栏、工具栏、视图选择器和三个数据窗格：应用程序树、结果列表和“详细信息”窗格。详细信息如下：



界面	内容介绍
视图选择器	选择在主窗格中显示的数据类型，包括“应用程序数据”视图（快捷键 F4）、“安全问题”视图（快捷键 F2）、“修复任务”视图（快捷键 F3）。
结果列表	会随着扫描进度填充应用程序树。扫描完成时，该树显示在应用程序中所找到的所有文件夹、URL 和文件。
详细信息窗格	显示三个选项卡（“咨询”、“修订建议”和完整的“请求/响应”）中的结果列表内选定节点的相关详细信息。

4.2 扫描流程配置

1.打开 AppScan，进入主界面。点击工具栏中的新建或菜单栏中的文件->新建来建立新的扫描。

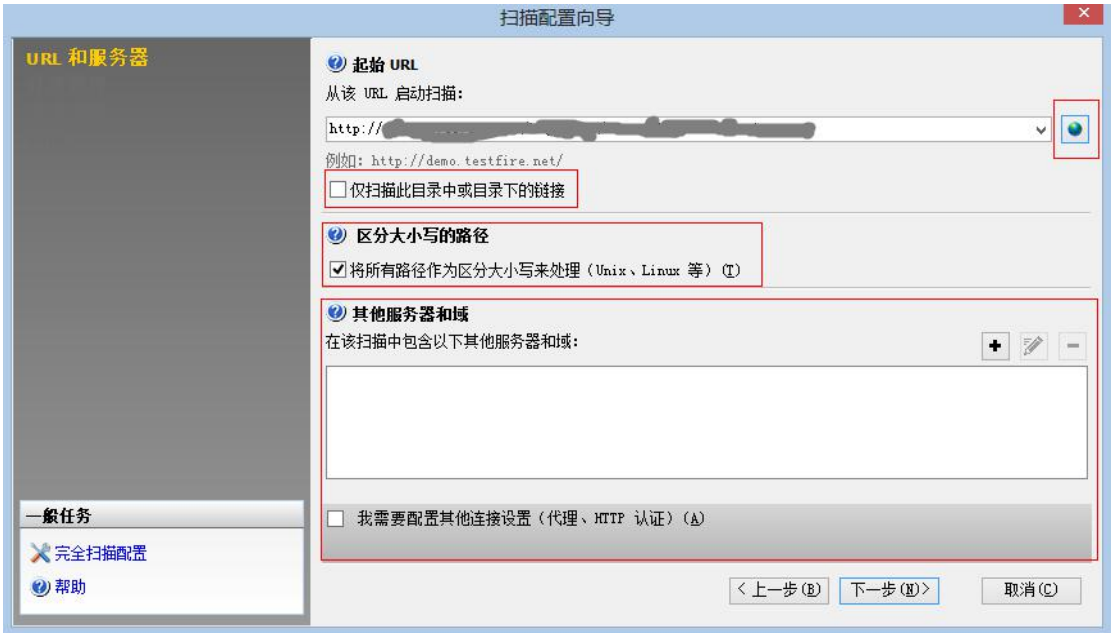
2.选择相应的模版，然后点击下一步。这里推荐选择“常规扫描”模版，或根据需要选择相应的模版。

3.选择扫描类型，可选择扫描 Web 应用或者 Web Service，点击下一步。

4.输入扫描的起始 URL（一般为登录页或首页），可点击 URL 栏旁的圆点对输入网址进行确认。

这里需要注意的问题有：

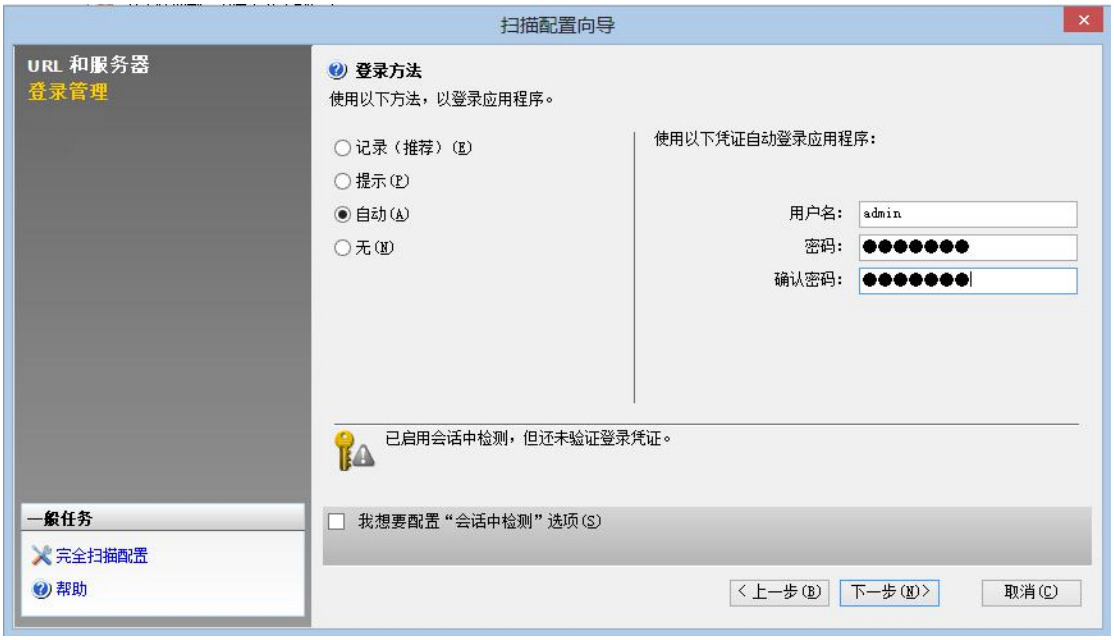
- 勾选仅扫描此目录或目录下的链接时，AppScan 只对该目录及该目录下的链接进行操作。
- 根据具体扫描的应用选择是否勾选区分大小写。
- 当需要扫描不属于起始 URL 域的链接时，可以将它们添加进来。



5.配置登录方法，这里推荐使用记录或自动两种登录方法。

➢ 自动登录（通过记录表单自动登录）

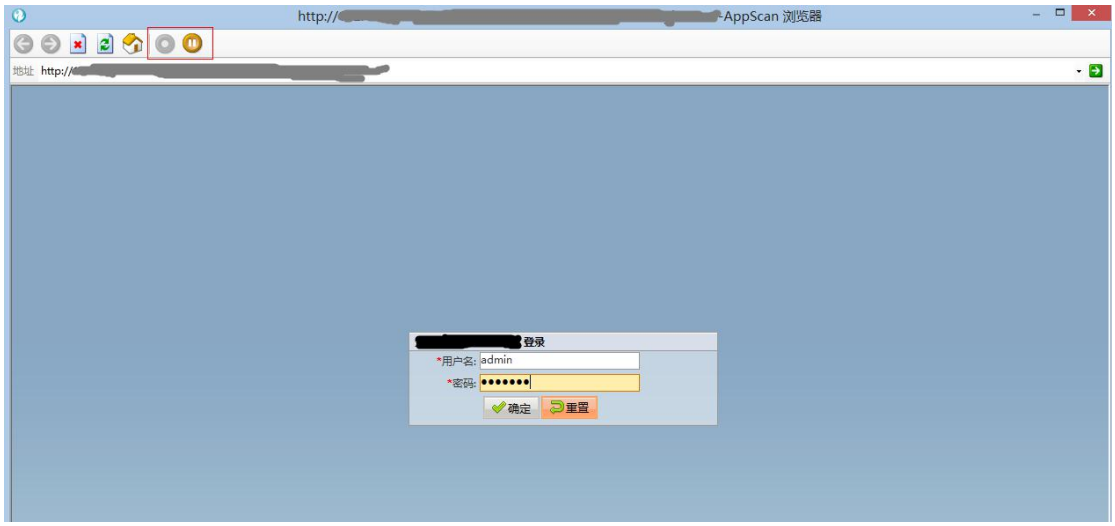
输入用户名和密码，然后点击下一步。



➢ 记录登录（通过录制登录操作完成扫描过程中的登录）

1) 点击记录新建一个新的登录记录，或者选择导入以导入一个已经录好的登录过程。这里我们介绍录制新的纪录的方法。

2) 在弹出的浏览器中输入登录的用户名以及密码，执行登录操作。左上角的暂停图标不为灰色时标明此时正在录制。

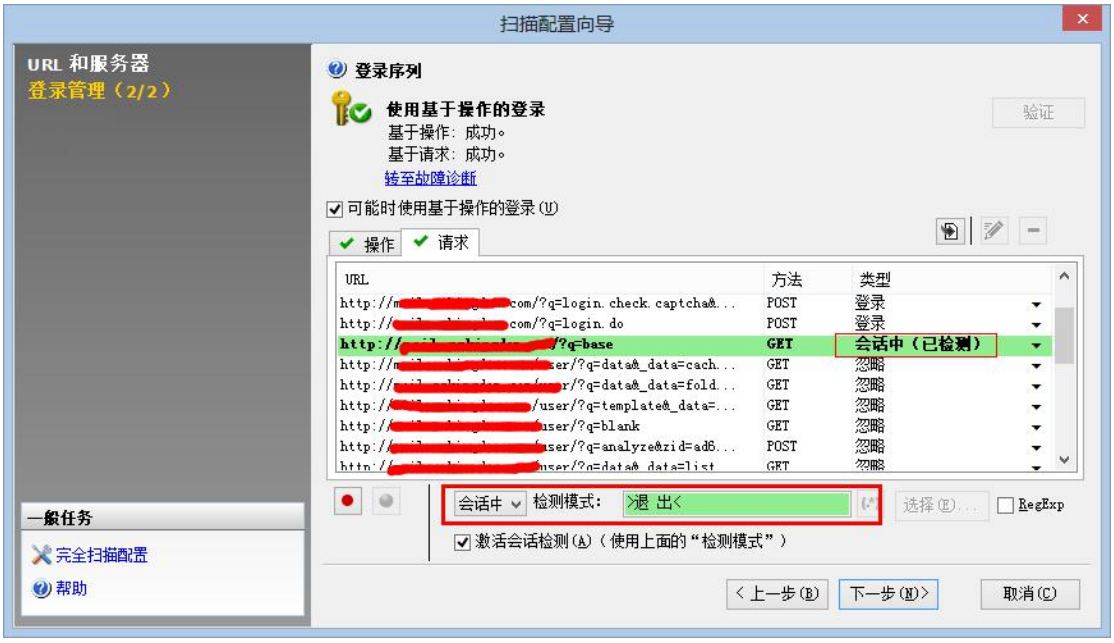


3) 成功登录后关闭浏览器，录制完毕。钥匙旁边出现绿色对勾时说明登录操作成功。勾选‘我想要配置“会话中检测”选项’，点击下一步。

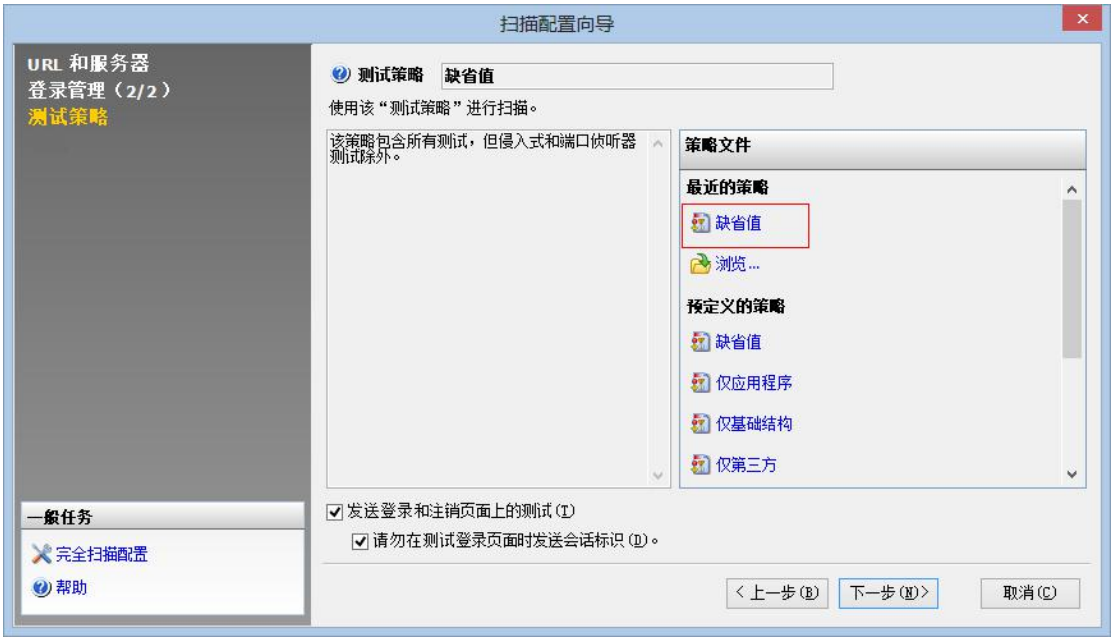
4) 配置登录序列。这里需要检查的地方有：

- 登录序列中含有类型为“会话中”的 URL。
- 类型为“会话中”的 URL 确实是处于登录状态。
- 在‘将该模式作为“会话中”状态的证明使用’一栏中，包含已经登录的标记，如登出、注销、退出、logout 等。

检查无误后点击下一步。

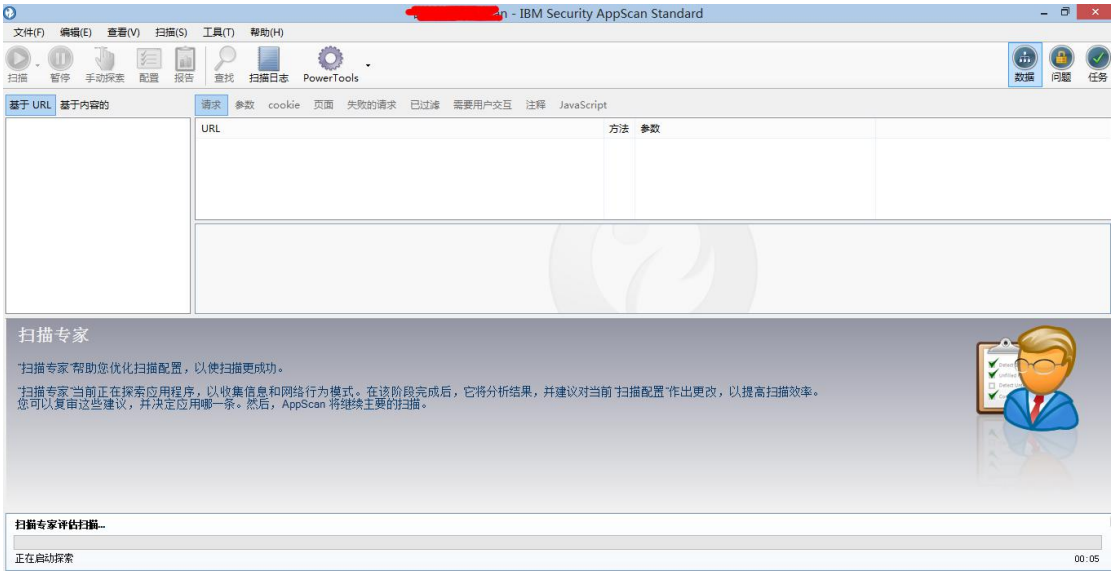


6.选择测试策略，这里推荐选择缺省策略，选择完毕后点击下一步。

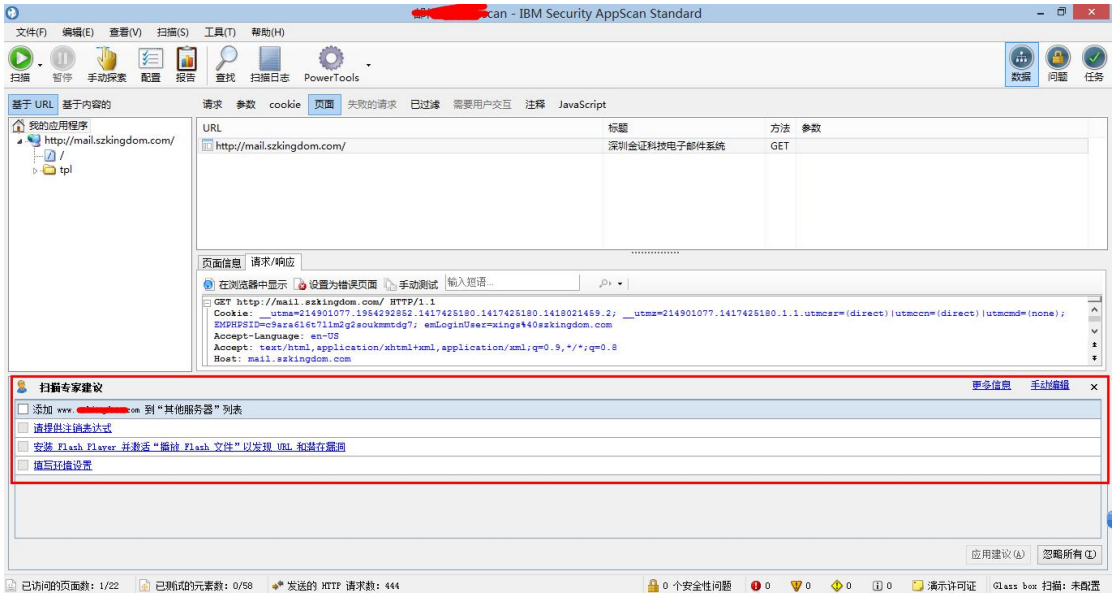


7.配置全部完成后，点击完成即可开始扫描。

8.扫描开始前，扫描专家会对已有的配置进行核查，找出配置中可以改进的方面。

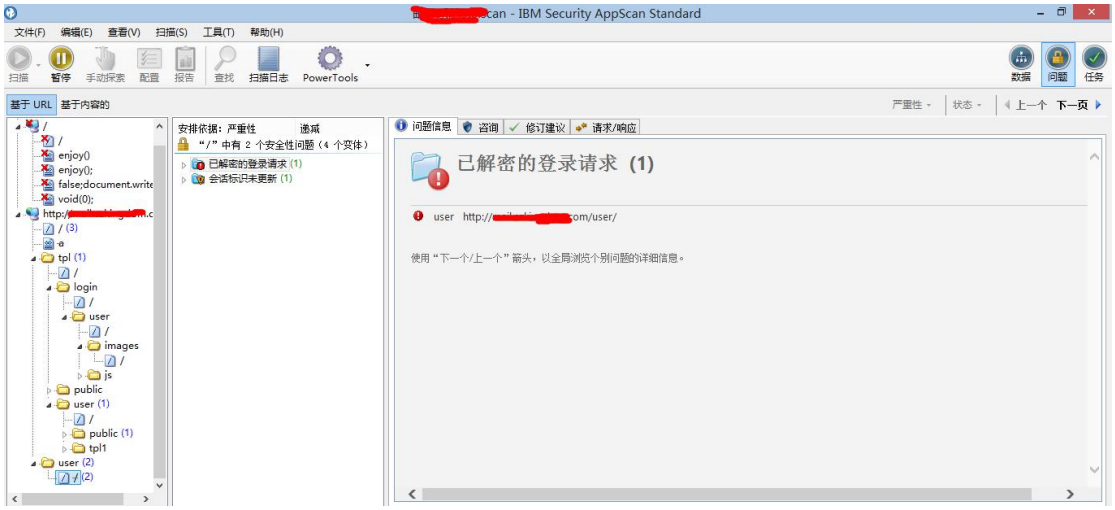


9.填写扫描专家提供的建议（可选），即可开始扫描。



4.3 扫描结果

下面是扫描完成时的状态，扫描过程中可以对有问题的链接进行查看。

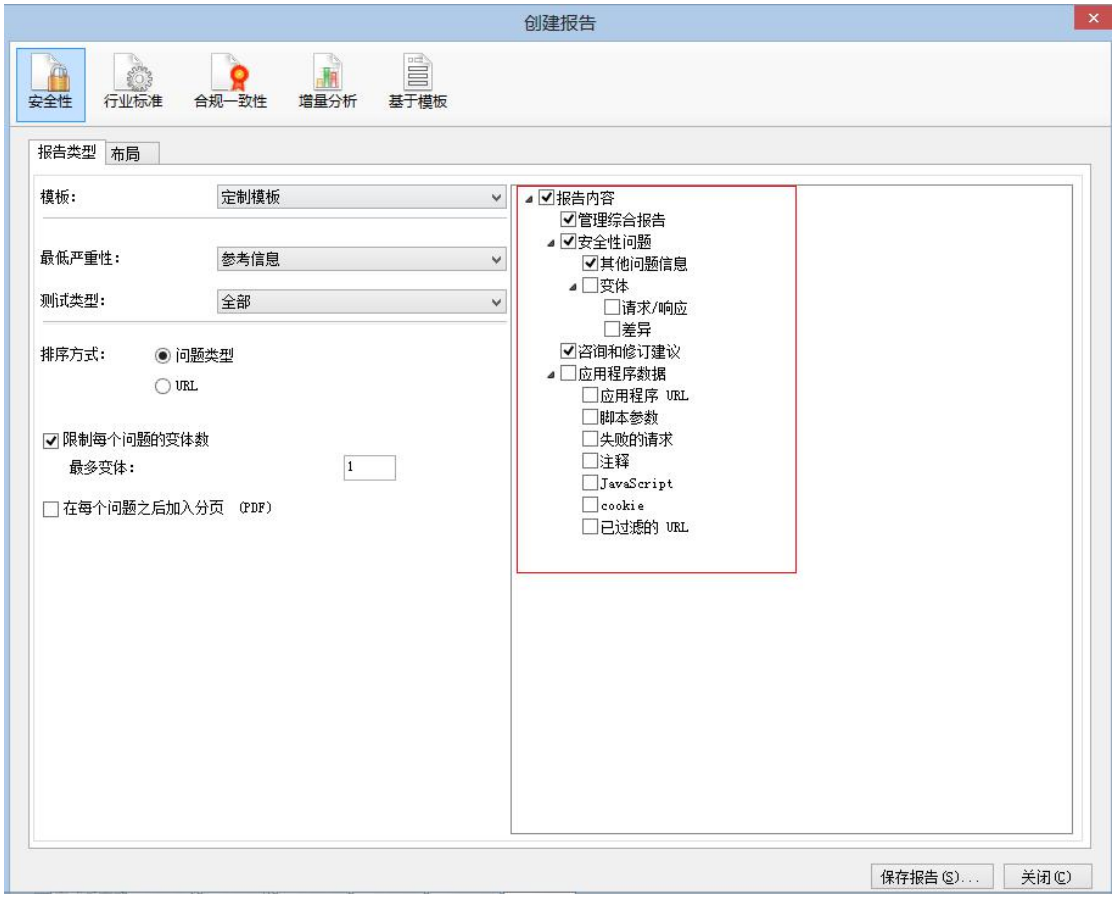


4.4 生成报告

扫描结束后，通过选择不同的参数，可以利用 AppScan 生成相应的报告。

点击工具栏中的报告选项，或菜单栏中的工具->报告。勾选报告内容中的参数，这里建议勾选管理摘要报告、咨询和修复建议、修复任务三项。

点击预览即可在报告查看器中查看扫描情况，点击保存则可以选择生成相应格式的报告，包括.pdf、.html 等。



选择上述参考项后，报告中将会显示以下内容：

- 管理摘要报告——对扫描结果的总结。
- 详细的安全性问题——具体说明哪些 URL 出现了哪些漏洞，并附上简单的修复意见。
- 修复任务——以列表的形式说明出现漏洞的 URL 的修复操作。
- 咨询和修复意见——提供详细的修复操作，包括详细的技术描述以及修复参考。