Web漏洞扫描之AppScan

IBM® Security AppScan® 是一个适合安全专家的Web应用程序和Web服务渗透测试解决方案。
国外商业漏扫产品中，少有的能支持中文的漏扫，运行于Windows平台；
界面清晰、配置简单丰富的中文和产品文档，详细的漏洞说明和修复建议；
支持丰富的扫描报告，包括安全性、行业标准、合规一次性报告。

https://www.ibm.com/developerworks/cn/downloads/r/appscan/

1. 功能及特点

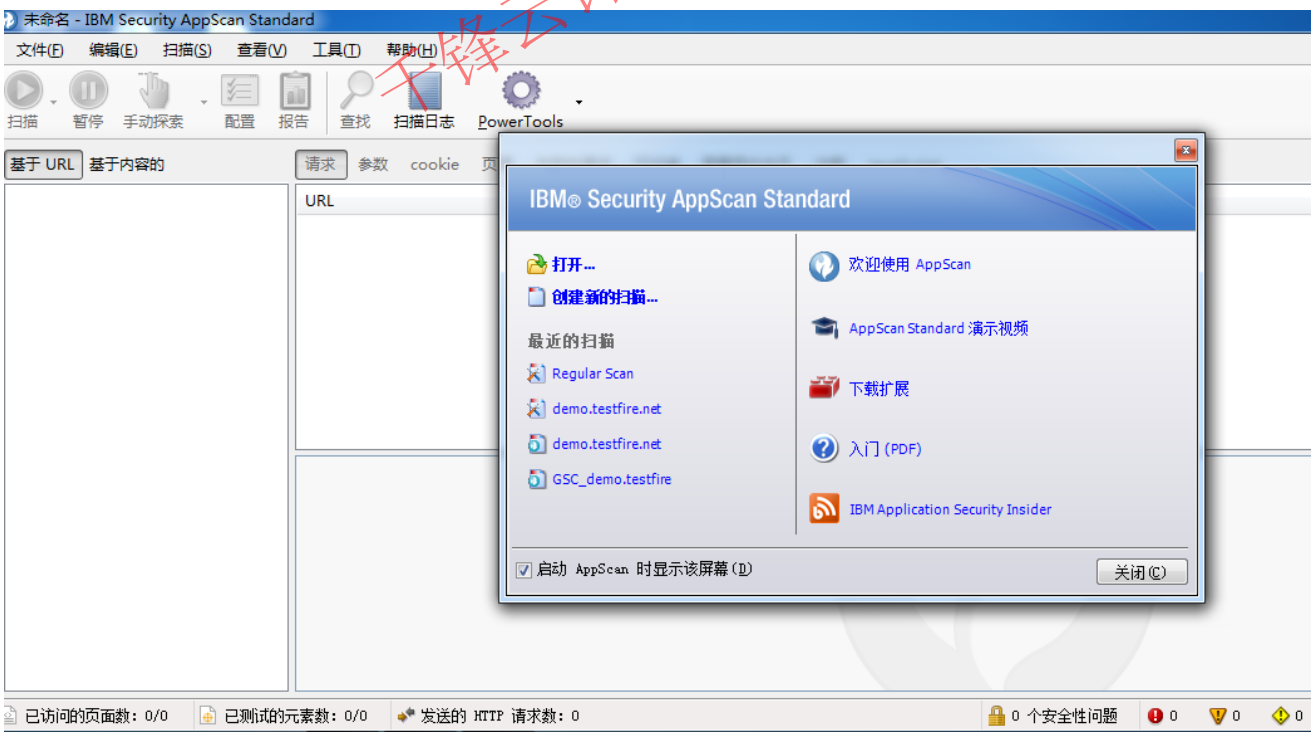
a) 对现代 Web 应用程序和服务执行自动化的动态应用程序安全测试 (DAST) 和交互式应用程序安全测试 (IAST)。支持Web2.0、JavaScript和AJAX框架的全面的JavaScript执行引擎。
b) 涵盖XML和JSON基础架构的SOAP和REST Web服务测试支持WS-Security标准、XML加密和XML签名。
详细的漏洞公告和修复建议。
c) 40多种合规性报告，包括支付卡行业数据安全标准(PCI DSS)、支付应用程序数据安全标准(PA-DSS)、ISO 27001和ISO 27002，以及Basel II。
d) IBM Security AppScan eXtensions Framework提供的自定义功能和可扩展性。

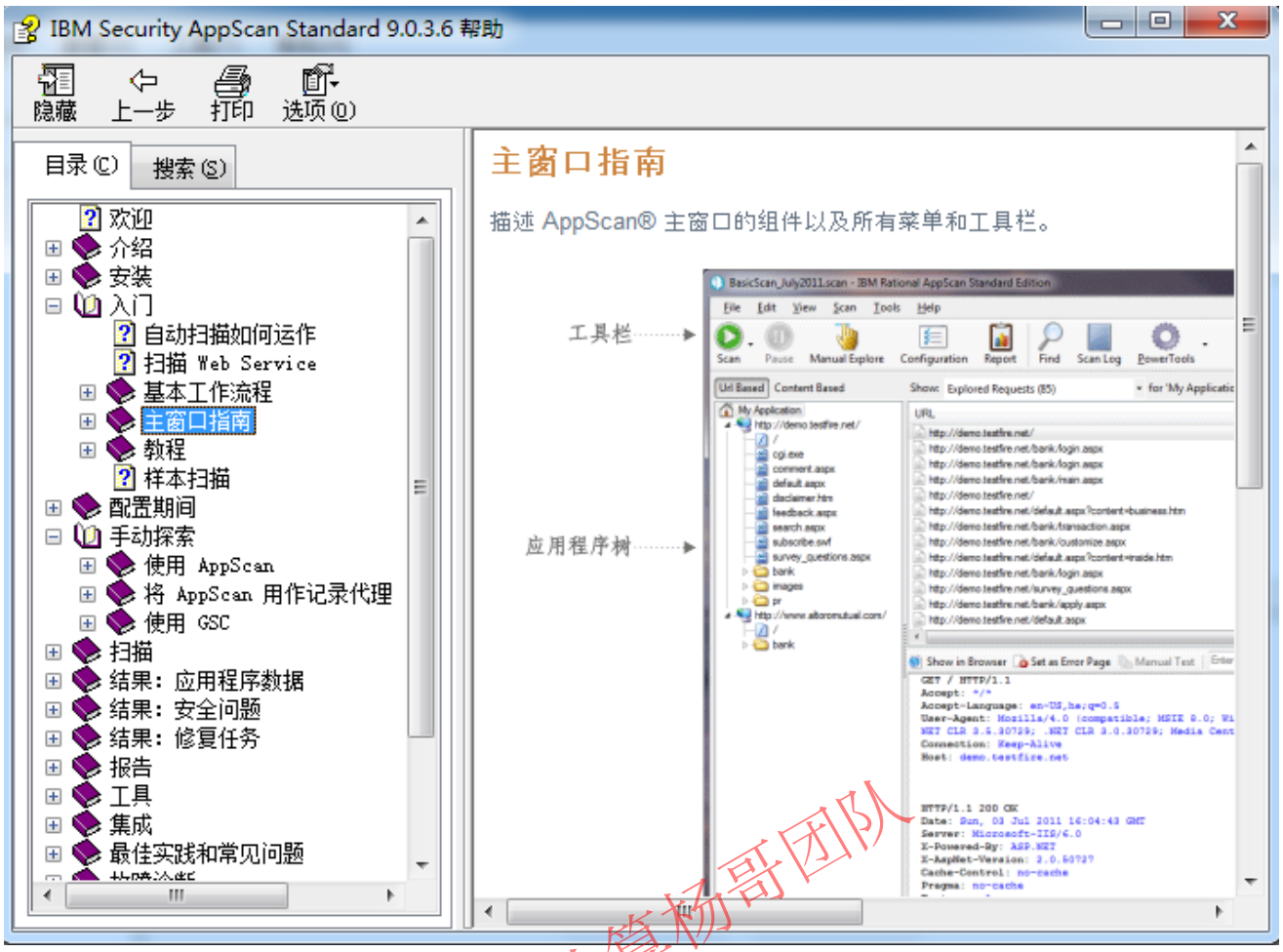
2. 项目实现环境

目标靶机：OWASP_Broken_Web_Apps_VM_1.2
测试渗透机：win7

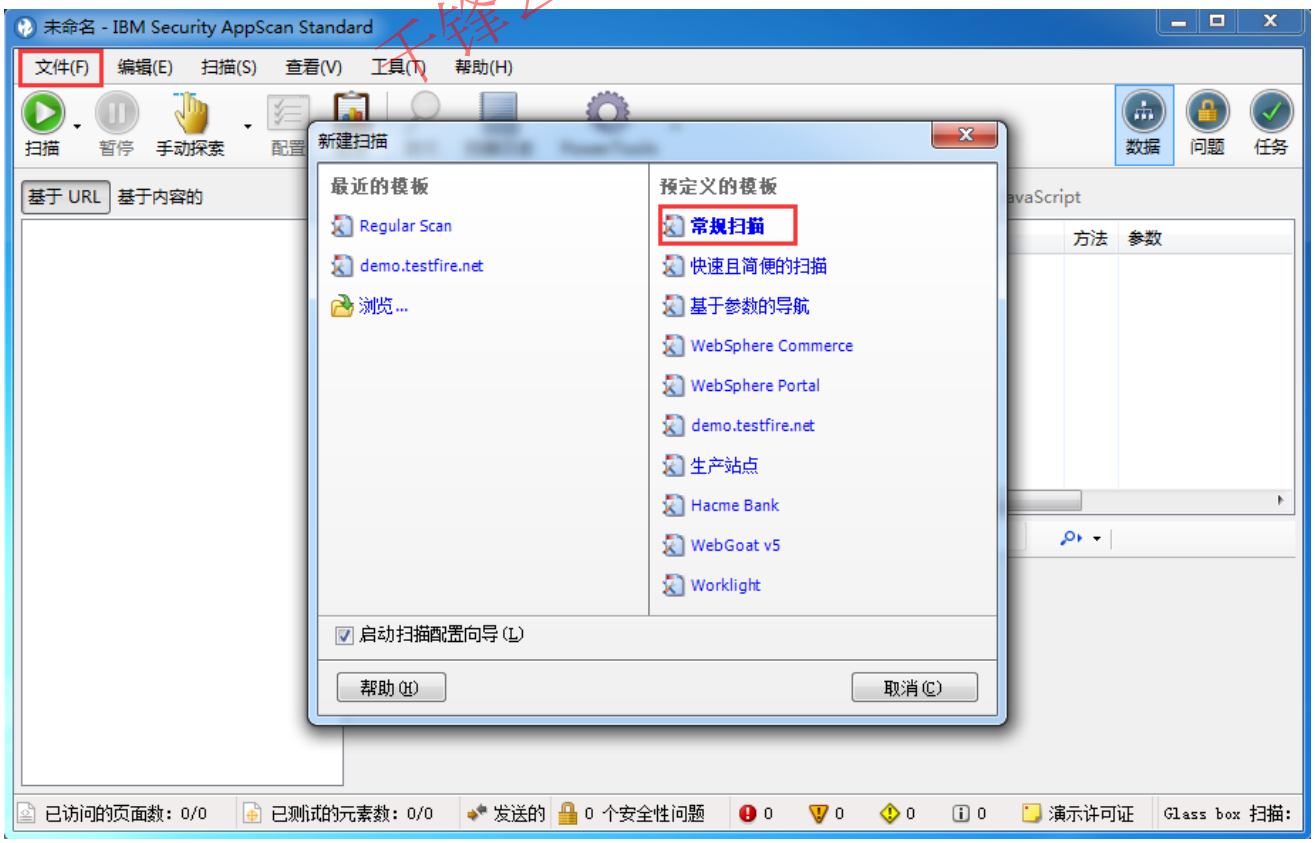
3. AppScan安装


IBM
Security AppScan Standard
版本 9.0.3.6
Licensed Materials - Property of IBM. 5724-T59 © Copyright IBM Corporation and its licensors 2000, 2017. All Rights Reserved.U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.Watchfire, AppScan and the Flame logo are trademarks of IBM Corporation in the United States, other countries, or both. A current list of IBM trademarks is available at http://www.ibm.com/legal/copytrade.shtml. Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.Other company product or service names may be trademarks or service marks of others.
构建： 10344 安全规则版本： 10344
正在装入: ActionBasedLib
Java


未命名 - IBM Security AppScan Standard
文件(F) 编辑(E) 扫描(S) 查看(V) 工具(T) 帮助(H)
扫描 暂停 手动探索 配置 报告 查找 扫描日志 PowerTools
基于 URL 基于内容的
请求 参数 cookie
URL
IBM® Security AppScan Standard
打开...
创建新的扫描...
最近的扫描
Regular Scan
demo.testfire.net
demo.testfire.net
GSC_demo.testfire
欢迎使用 AppScan
AppScan Standard 演示视频
下载扩展
入门 (PDF)
IBM Application Security Insider
启动 AppScan 时显示该屏幕(D)
关闭(C)
已访问的页面数: 0/0
已测试的元素数: 0/0
发送的 HTTP 请求数: 0
0 个安全性问题
0
0
0



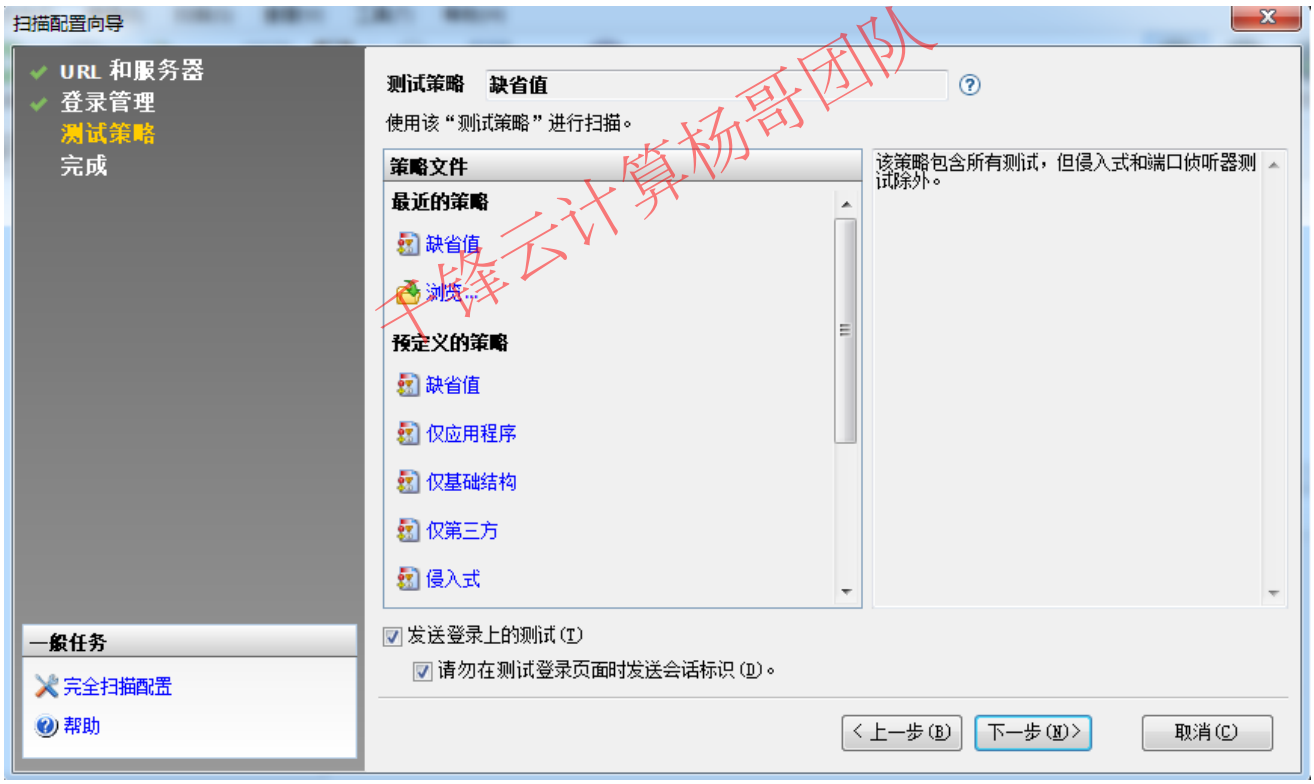
4. 创建扫描



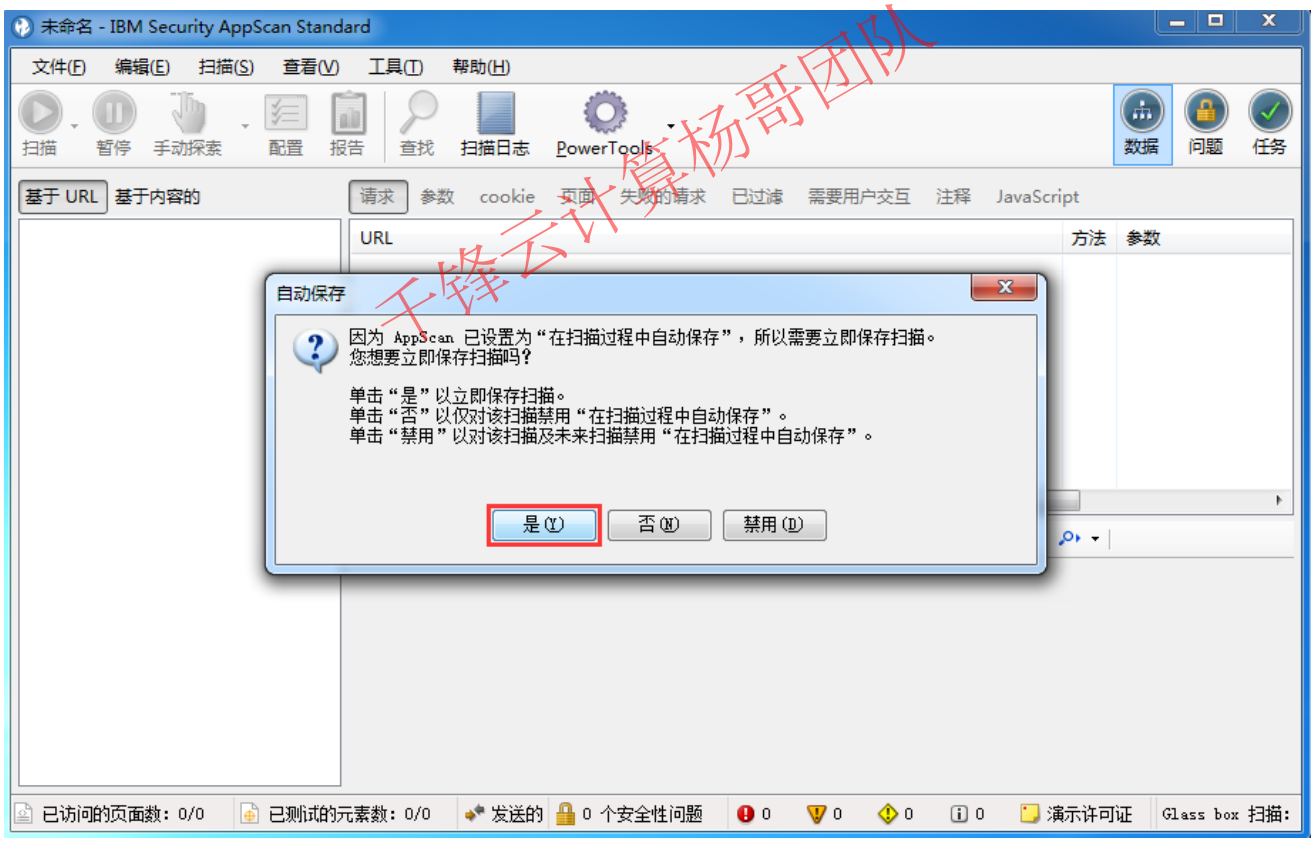

扫描配置向导
IBM
欢迎使用"配置向导"
"配置向导"将帮助您配置一个以扫描模板为基础的新扫描：常规扫描
我想要使用以下方法探索站点：
AppScan（自动或手动）
外部设备/客户机（AppScan 作为记录代理）
通用服务客户机 (WSDL)
未安装 GSC Web Services 记录器。 立即下载 GSC
我应选择哪个选项？
一般任务
完全扫描配置
帮助
< 上一步(B)
下一步(N)>
取消(C)

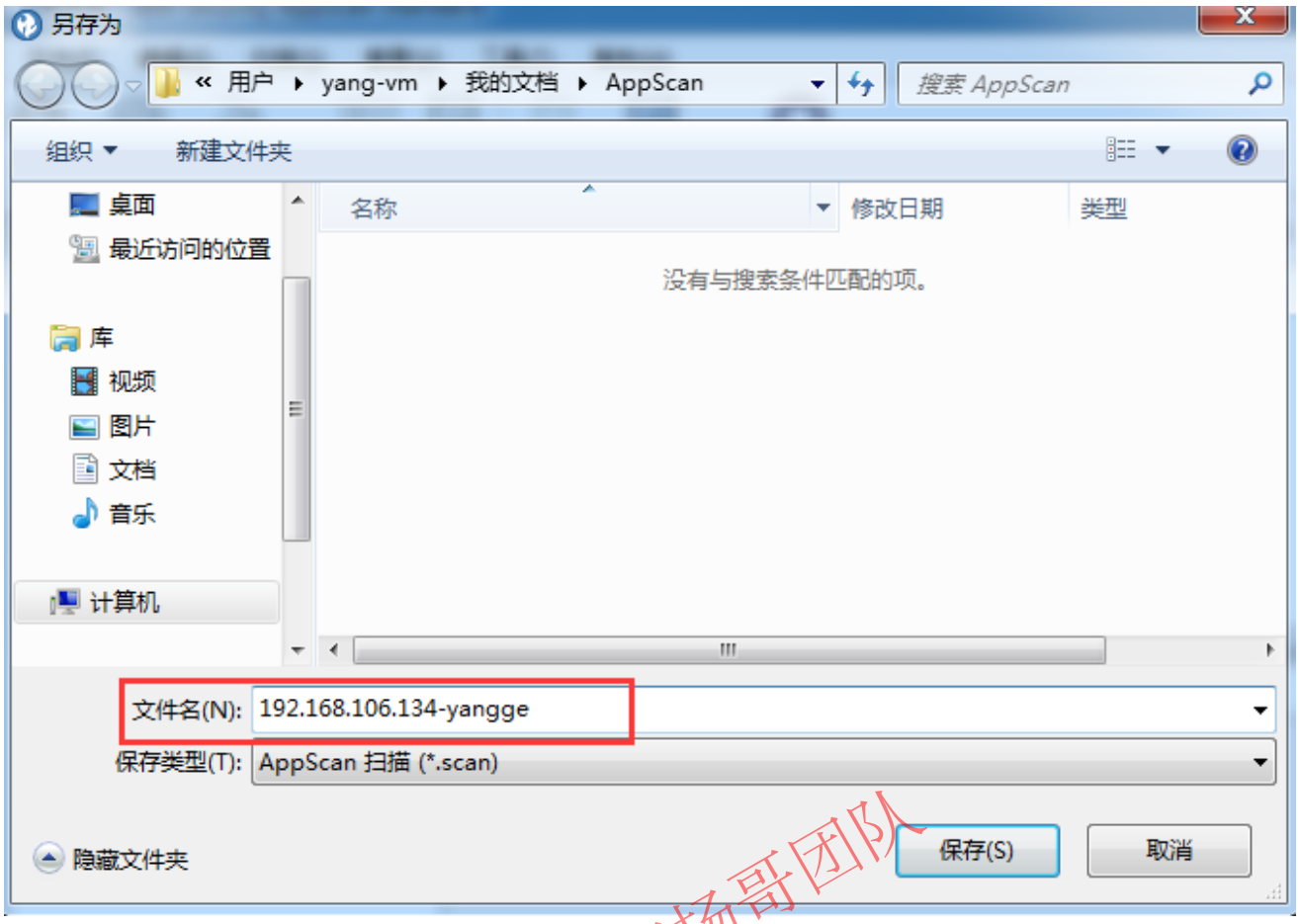

扫描配置向导
URL 和服务器
登录管理
测试策略
完成
起始 URL
从该 URL 启动扫描：
http://192.168.106.134/mutillidae/
已连接到服务器
重要信息：如果要扫描生产站点，首先阅读以下准则：
扫描实时生产站点
仅扫描此目录中或目录下的链接(L)
将所有路径作为区分大小写来处理（Unix、Linux 等）(T)
其他服务器和域
我需要配置其他连接设置（代理、HTTP 认证）(A)
一般任务
完全扫描配置
帮助
< 上一步(B)
下一步(N)>
取消(C)

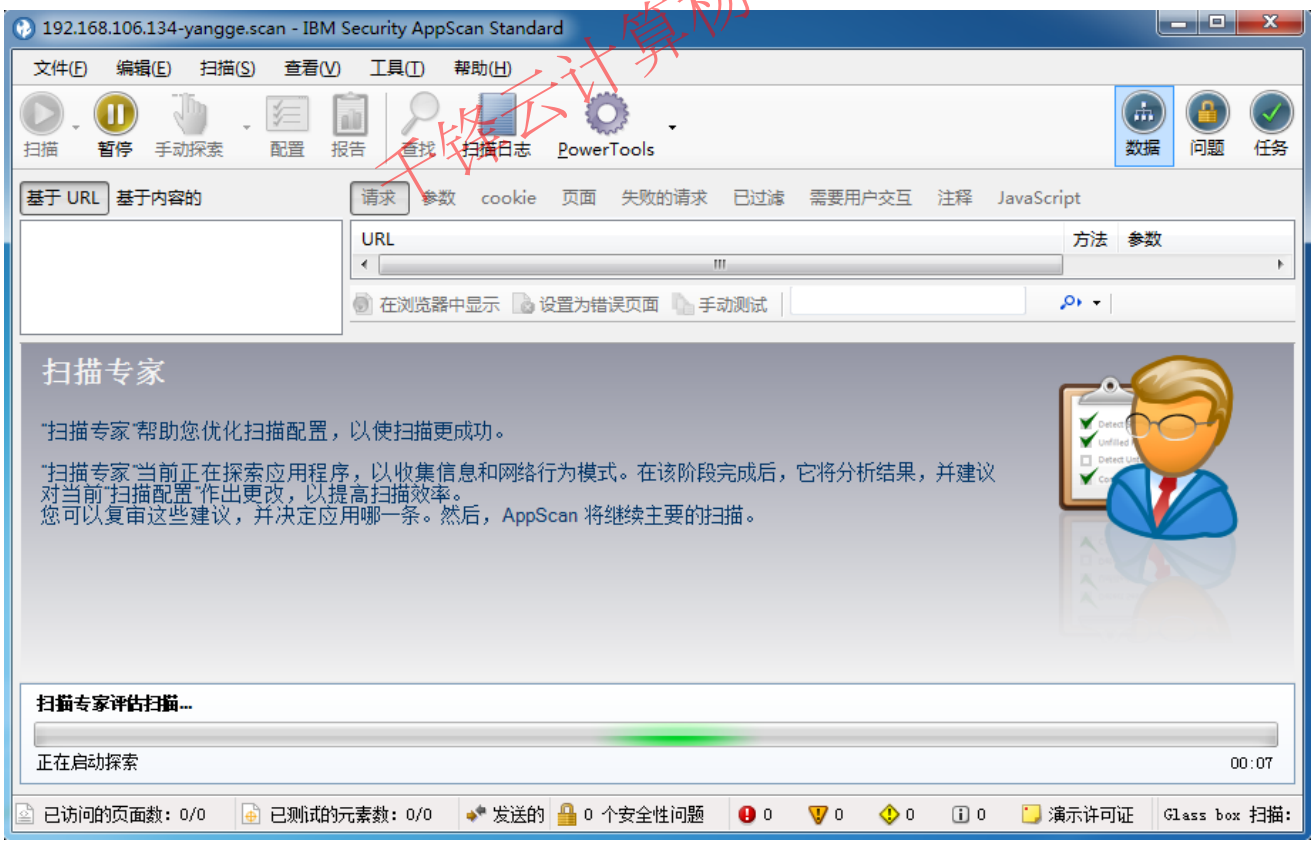

扫描配置向导
URL 和服务器
登录管理
测试策略
完成
登录方法
使用以下方法，以登录应用程序。
记录（推荐）(E)
提示(P)
自动(A)
无(O)
记录(R)
使用已记录的登录序列来登录到应用程序。
尚未记录登录
一般任务
完全扫描配置
帮助
我想要配置“会话中检测”选项(S)
< 上一步(B)
下一步(N)>
取消(C)

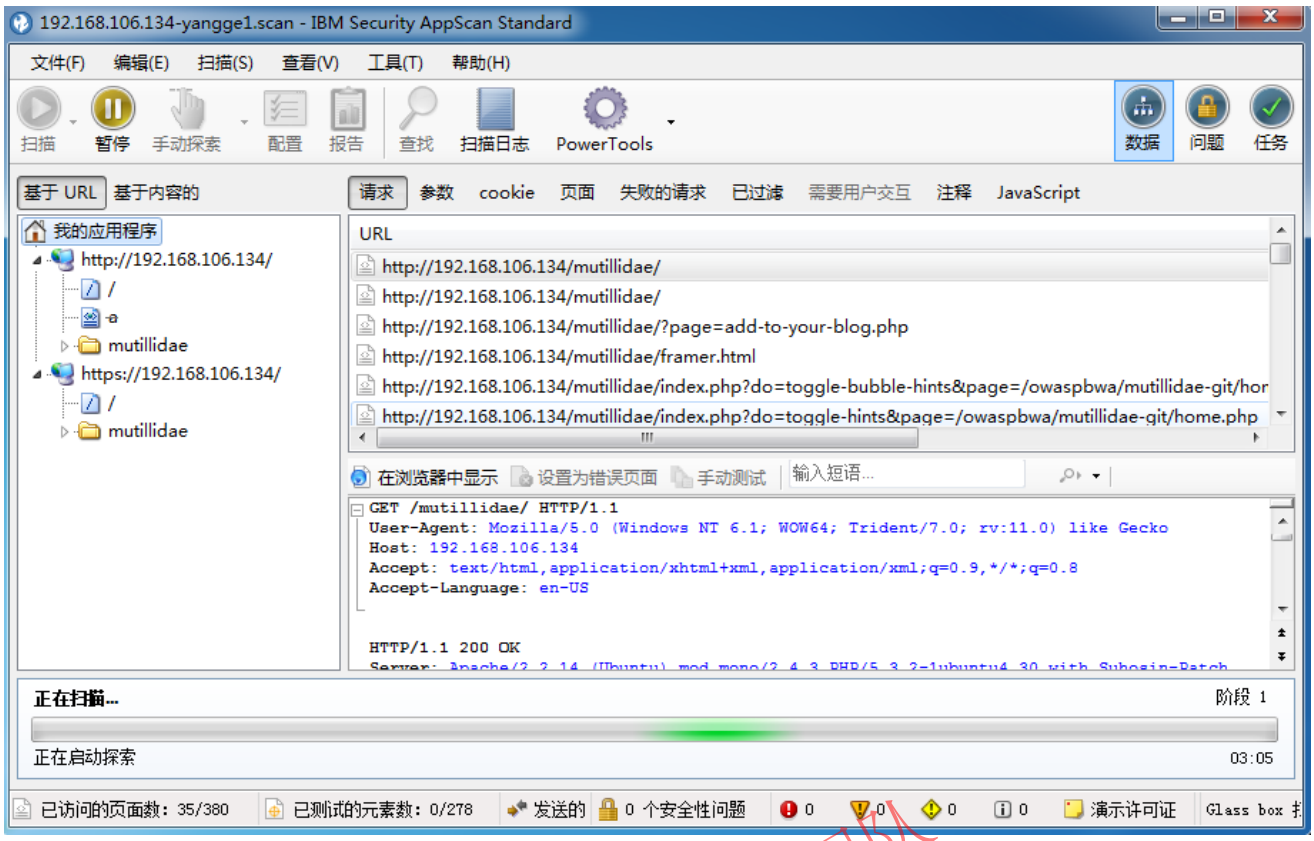

扫描配置向导
URL 和服务器
登录管理
测试策略
完成
测试策略
缺省值
使用该“测试策略”进行扫描。
策略文件
最近的策略
缺省值
浏览...
预定义的策略
缺省值
仅应用程序
仅基础结构
仅第三方
侵入式
该策略包含所有测试，但侵入式和端口侦听器测试除外。
一般任务
完全扫描配置
帮助
发送登录上的测试(T)
请勿在测试登录页面时发送会话标识(D)。
< 上一步(B)
下一步(N)>
取消(C)


扫描配置向导
URL 和服务器
登录管理
测试策略
完成
完成扫描配置向导
您已成功完成“扫描配置向导”。
您想要如何启动?
启动全面自动扫描(A)
仅使用自动“探索”启动(E)
使用“手动探索”启动(M)
我将稍后启动扫描(L)
完成“扫描配置向导”后启动“扫描专家”(S)
一般任务
完全扫描配置
帮助
< 上一步(B)
完成(F)
取消(C)


未命名 - IBM Security AppScan Standard
文件(F) 编辑(E) 扫描(S) 查看(V) 工具(T) 帮助(H)
扫描 暂停 手动探索 配置 报告 查找 扫描日志 PowerTools 数据 问题 任务
基于 URL 基于内容的
请求 参数 cookie 页面 失败的请求 已过滤 需要用户交互 注释 JavaScript
URL 方法 参数
自动保存
因为 AppScan 已设置为“在扫描过程中自动保存”，所以需要立即保存扫描。
您想要立即保存扫描吗?
单击“是”以立即保存扫描。
单击“否”以仅对该扫描禁用“在扫描过程中自动保存”。
单击“禁用”以对该扫描及未来扫描禁用“在扫描过程中自动保存”。
是(Y) 否(N) 禁用(D)
已访问的页面数: 0/0
已测试的元素数: 0/0
发送的
0 个安全性问题
演示许可证
Glass box 扫描:


另存为
« 用户 ▸ yang-vm ▸ 我的文档 ▸ AppScan
搜索 AppScan
组织
新建文件夹
桌面
最近访问的位置
库
视频
图片
文档
音乐
计算机
名称
修改日期
类型
没有与搜索条件匹配的项。
文件名(N): 192.168.106.134-yangge
保存类型(T): AppScan 扫描 (*.scan)
隐藏文件夹
保存(S)
取消


192.168.106.134-yangge.scan - IBM Security AppScan Standard
文件(F) 编辑(E) 扫描(S) 查看(V) 工具(T) 帮助(H)
扫描 暂停 手动探索 配置 报告 查找 扫描日志 PowerTools
数据 问题 任务
基于 URL 基于内容的
请求 参数 cookie 页面 失败的请求 已过滤 需要用户交互 注释 JavaScript
URL 方法 参数
在浏览器中显示 设置为错误页面 手动测试
扫描专家
"扫描专家"帮助您优化扫描配置，以使扫描更成功。
"扫描专家"当前正在探索应用程序，以收集信息和网络行为模式。在该阶段完成后，它将分析结果，并建议对当前"扫描配置"作出更改，以提高扫描效率。
您可以复审这些建议，并决定应用哪一条。然后，AppScan 将继续主要的扫描。
扫描专家评估扫描...
正在启动探索
00:07
已访问的页面数：0/0
已测试的元素数：0/0
发送的
0 个安全性问题
演示许可证
Glass box 扫描:



5. 保存扫描

6. 导出结果