

Fortify SCA

产品使用手册

道普云（山东）智能科技有限公司
技术支持：18266417701
客服微信：daopuyun

目录

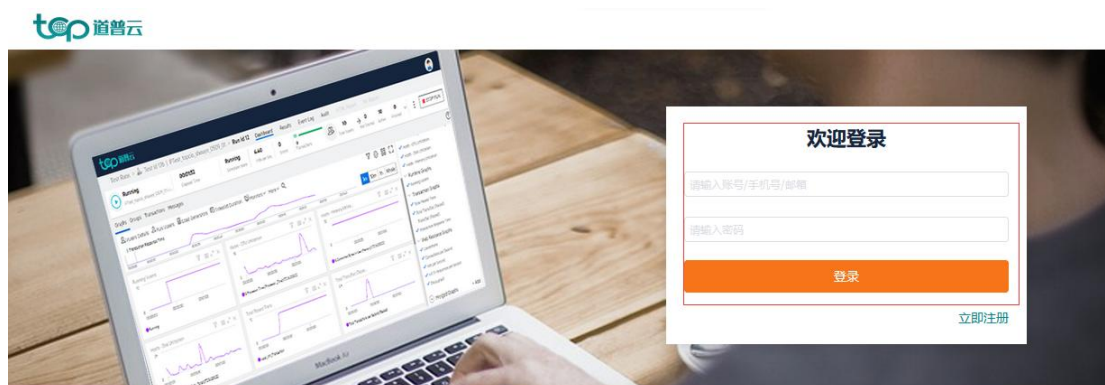
1. 总体使用流程	3
2. 用户登录	3
3. 创建测试用户	3
4. 创建代码测试项目	4
5. 使用代码测试工具	5
5.1. 通过 “Audit Workbench” 进行测试	8
5.2. 通过 “Scan Wizard” 进行测试	12
5.3. 通过命令行进行测试	16
5.3.1. Linux 项目测试	17
5.3.2. iOS 项目测试	17
6. 测试报告生成	17
6.1. 通过 “Audit Workbench” 生成测试报告	17
6.2. 通过 “Scan Wizard” 生成测试报告	19
6.3. 通过命令行生成测试报告	19

1. 总体使用流程

用户登录-创建测试用户-创建测试项目域-创建测试项目-使用代码测试工具 Fortify SCA-同步测试数据

2. 用户登录

- (1) 打开平台首页并输入登录用户名和密码



3. 创建测试用户

- (1) 打开测试用户新增页面



- (2) 输入测试用户信息

新增用户

* 用户名

tester01

* 登录账号(创建后不可修改)

tester01

* 手机号

13712345678

* 密码

••••••••

👁

* 再次输入密码

••••••••

👁

邮箱

* 用户组

默认组

▼

* 角色

客户方管理员

▼

* 状态

正常

▼

确定

4. 创建代码测试项目

(1) 打开测试项目域新增页面



(2) 输入测试项目域名称

项目域

域名称

Q

×

+ 增加

域名称	项目数	操作
代码测试	0	<div>🗑</div> <div>✎</div>

取消 保存

(3) 打开测试项目新增页面



- (4) 输入测试项目信息，包括基本信息、测试类型，点击保存，平台返回 Fortify SCA 工具所在云主机 IP 地址信息

基本信息

* 项目名称: XX软件代码测试项目

* 项目域: 代码测试

开始日期: 2020-07-01

结束日期: 2020-07-10

项目编号: 请输入项目编号

* 是否同步到本地: ☒ 是 ☐ 否

测试类型

* 测试类型: Fortify

安全测试

产品名称: Fortify SCA 20.1 及Host-试用

IP地址: 121.40.186.87(10.0.14.153)

取消 保存

5. 使用代码测试工具

- (1) 点击 Fortify SCA 产品信息，查看已购买或试用的产品信息



- (2) 点击产品 ID，进入产品详情页

Fortify SCA 20.1 及Host-试用产品列表

+ 新购产品				
购买产品备注	产品ID	状态	有效期	操作
请输入产品备注	请输入产品ID	请选择		
Fortify SCA 20.1 及Host-试用	766705094652616704	正常	2020-10-16 16:52:19-2020-10-30 16:52:42	续费

共 1 条 10条/页 < 1 > 前往 1 页

(3) 在产品详情页，点击“查看初始密码”

产品详情

Fortify SCA 20.1 及Host-试用

766705094652616704

续费

创建时间

2020-10-16 16:52:19

到期时间

2020-10-30 16:52:42 到期

Fortify SCA 20.1

购买产品备注 Fortify SCA 20.1

产品名称

Fortify SCA 20.1

许可数量

1

Fortify Host

购买产品备注 Fortify Host

实例id: i-bp1l1dx7h32v98dpp2oa

IP地址: 121.40.186.87(10.0.14.153)

备注:

查看初始密码

重置密码

产品名称

fortify-host

区域ID

华东1 (杭州)

实例资源规格

ecs.g6e.xlarge

公网带宽

1Mbit/s

系统盘类型

ESSD云盘

系统盘大小

(4) 从弹出窗口查看“初始密码”

产品详情

Fortify SCA 20.1 及Host-试用

766705094652616704

续费

创建时间 2020-10-16 16:52:19

到期时间 2020-10-30 16:52:42 到期

Fortify SCA 20.1

购买产品备注 Fortify SCA 20.1

产品名称Fortify SCA 20.1许可数量

Fortify Host

购买产品备注 Fortify Host

实例id: i-bp1l1dx7h32v98dpp2oaIP地址: 121.40.186.87(10.0.14.153)

产品名称fortify-host区域ID华东1 (杭州)实例资源规格ecs.g6e.xlarge

公网带宽1Mbit/s系统盘类型ESSD云盘系统盘大小

查看初始密码

操作系统名称: Windows Server 2019 数据中心版 64位中文版

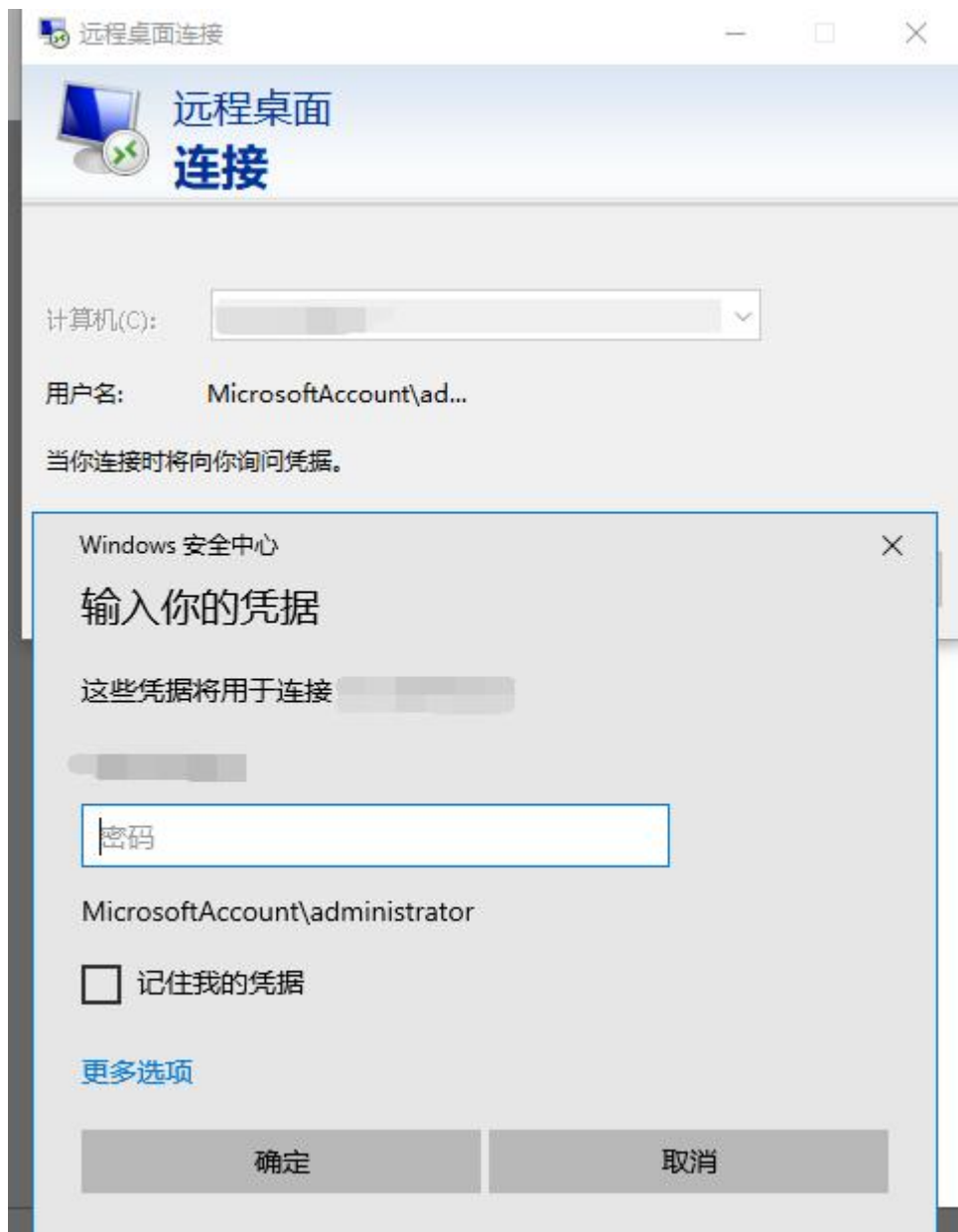
用户名:

密码:

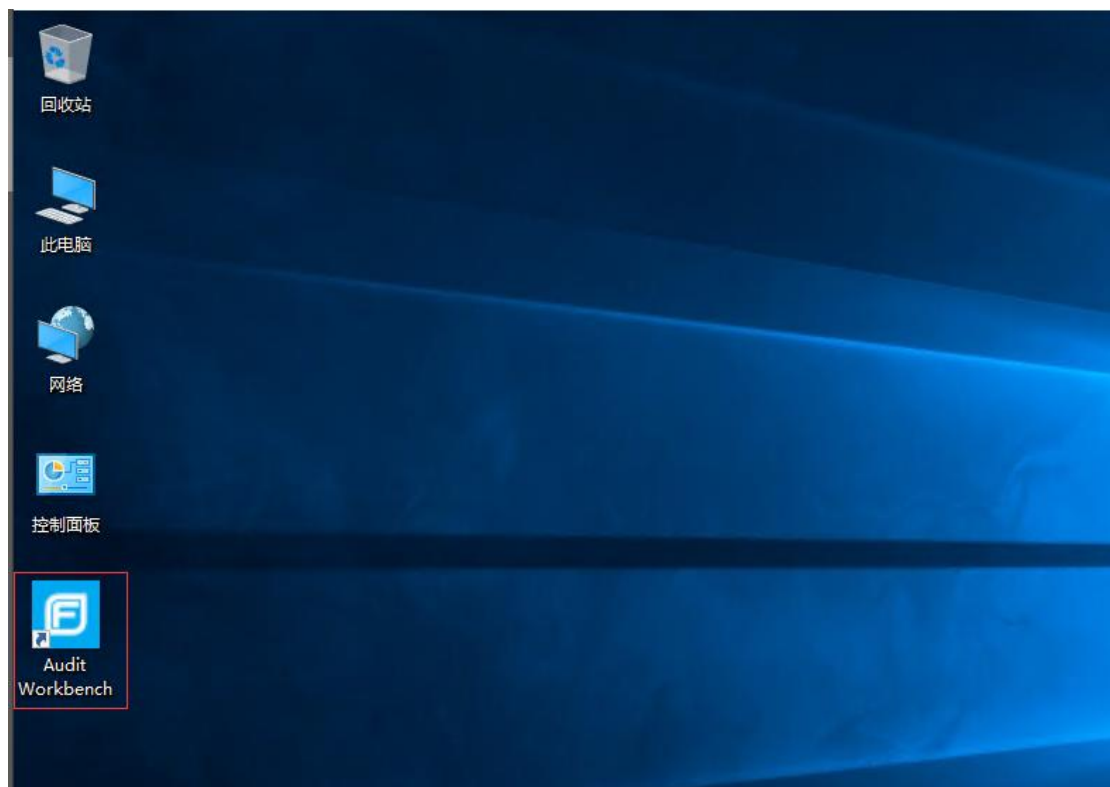
关闭

重置密码

(5) 根据获取的 Fortify SCA 云主机 IP 地址、用户名和口令，远程登录到该云主机



(6) 打开桌面 Fortify SCA 20.1 代码审计引擎

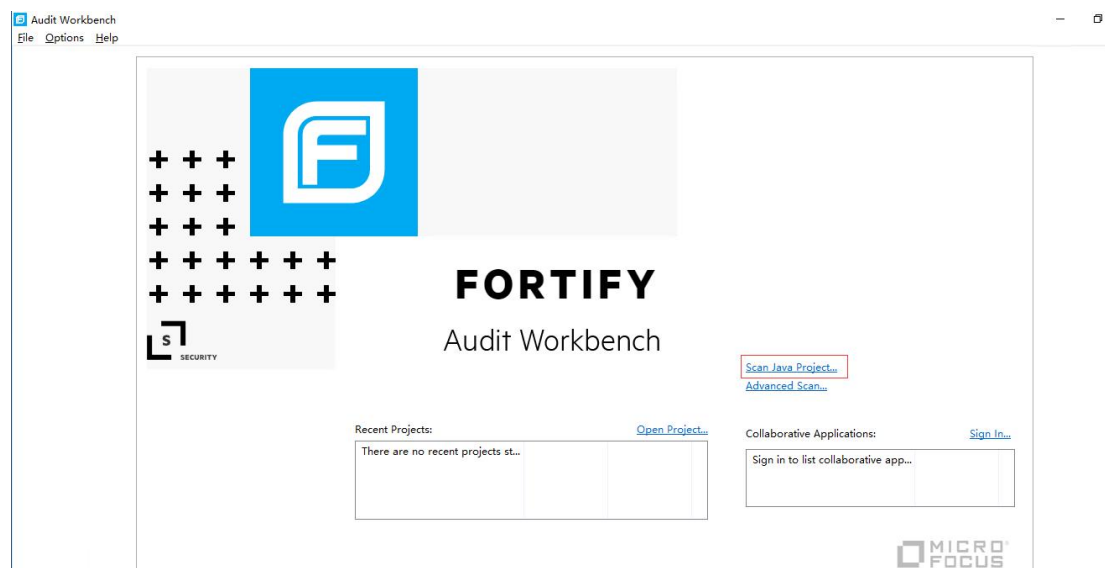


5.1. 通过 “Audit Workbench” 进行测试

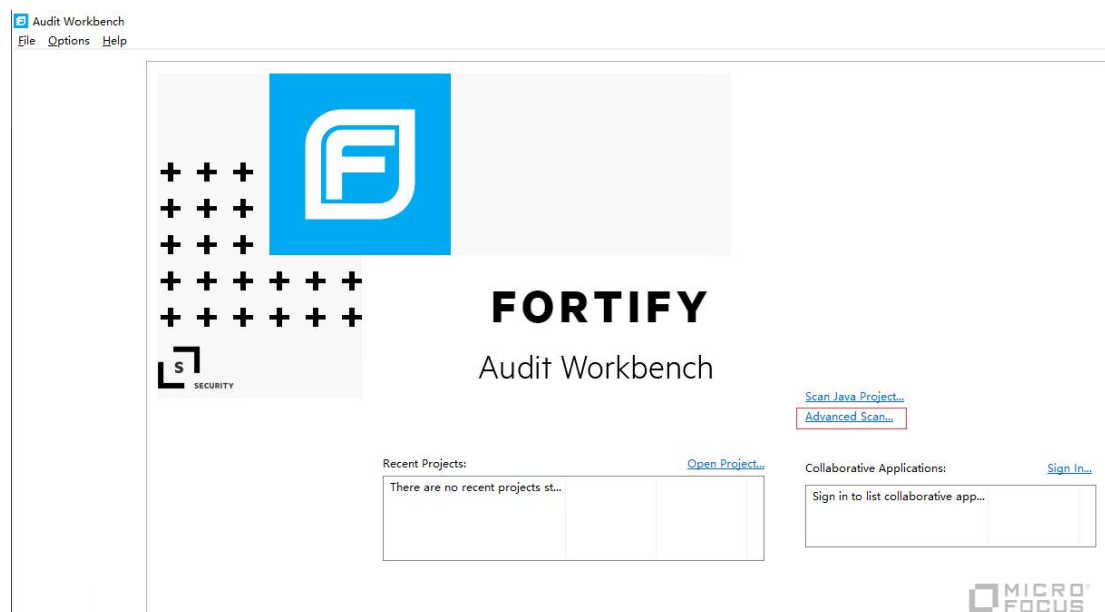
“Audit Workbench” 支持 Java 语言源代码的测试。

(1) 在主页面选择代码测试语言类型

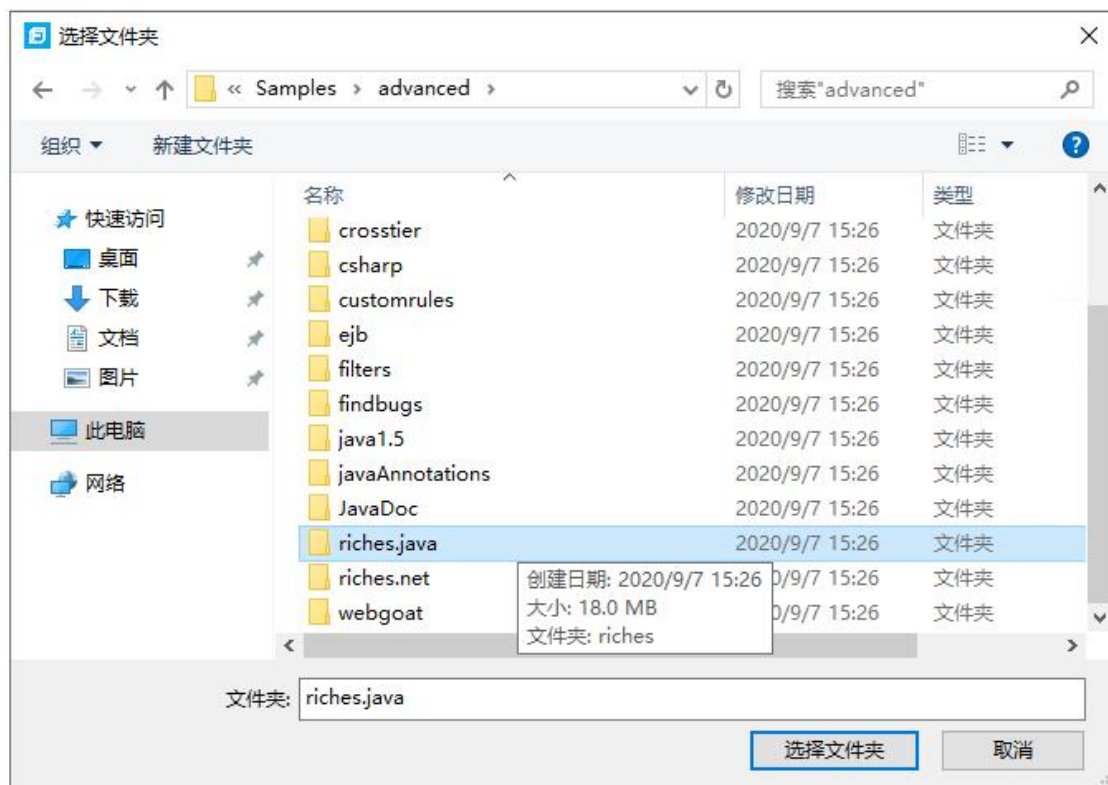
1) 选择 “Scan Java Project”



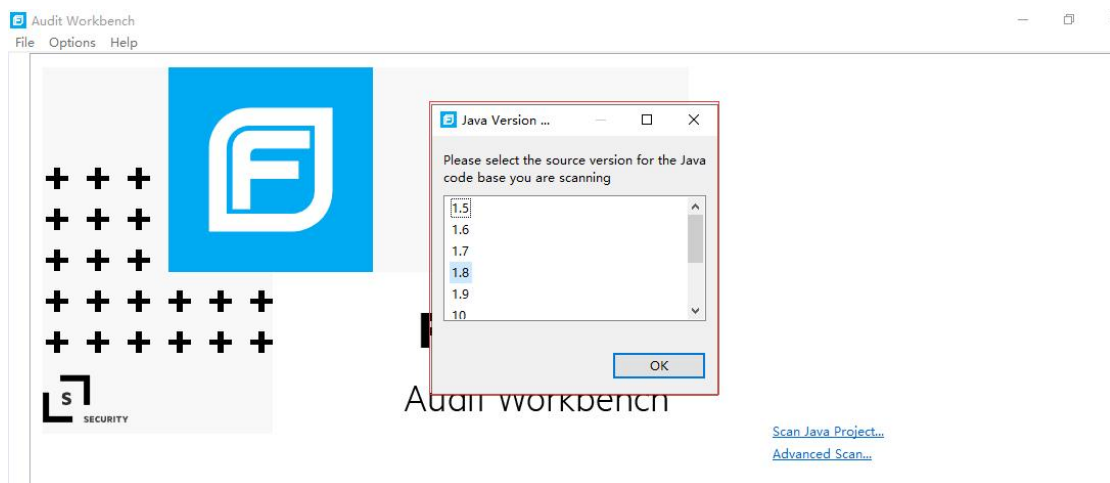
2) 如果是非 Java 语言，选择 “Advanced Scan”



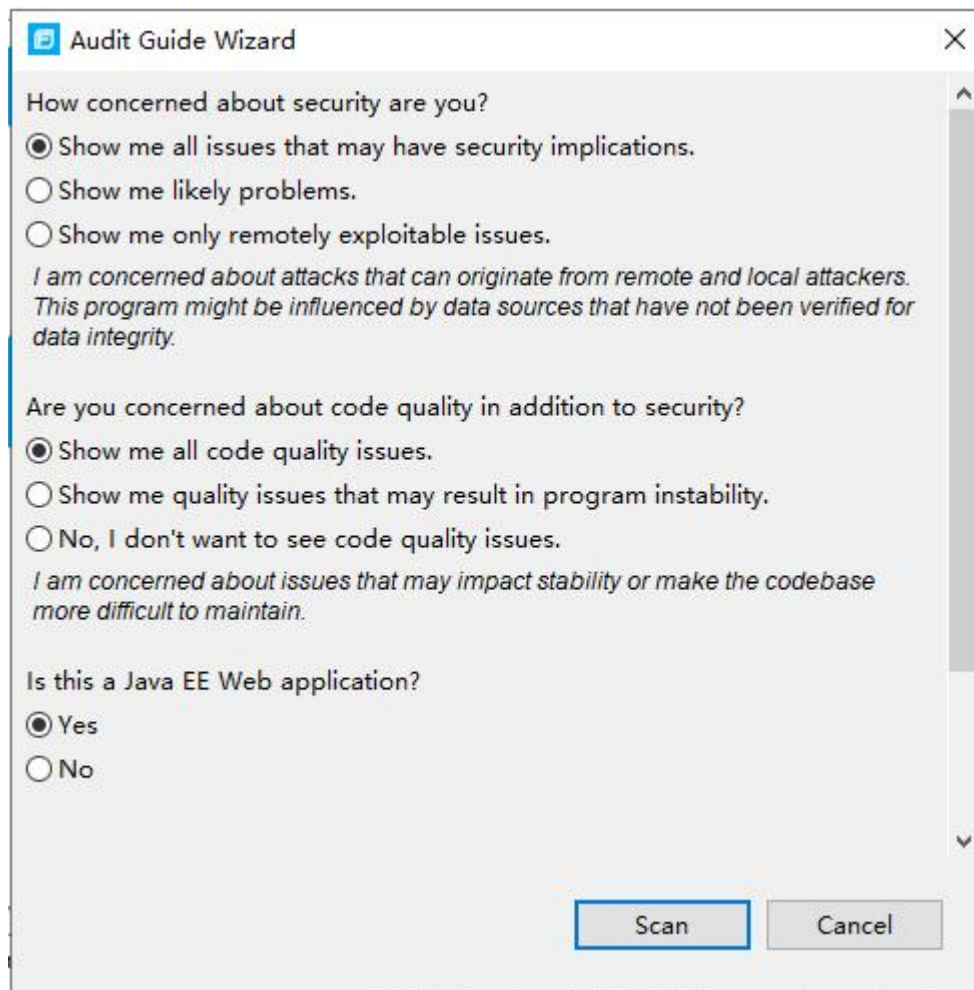
(2) 选择被测试代码所在目录



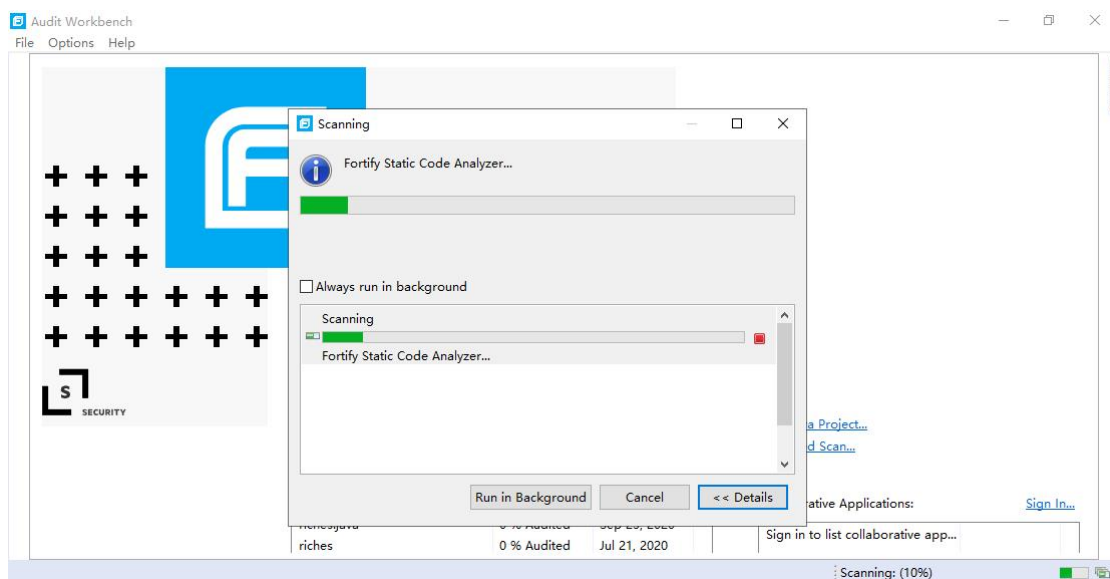
(3) 选择 Java 版本



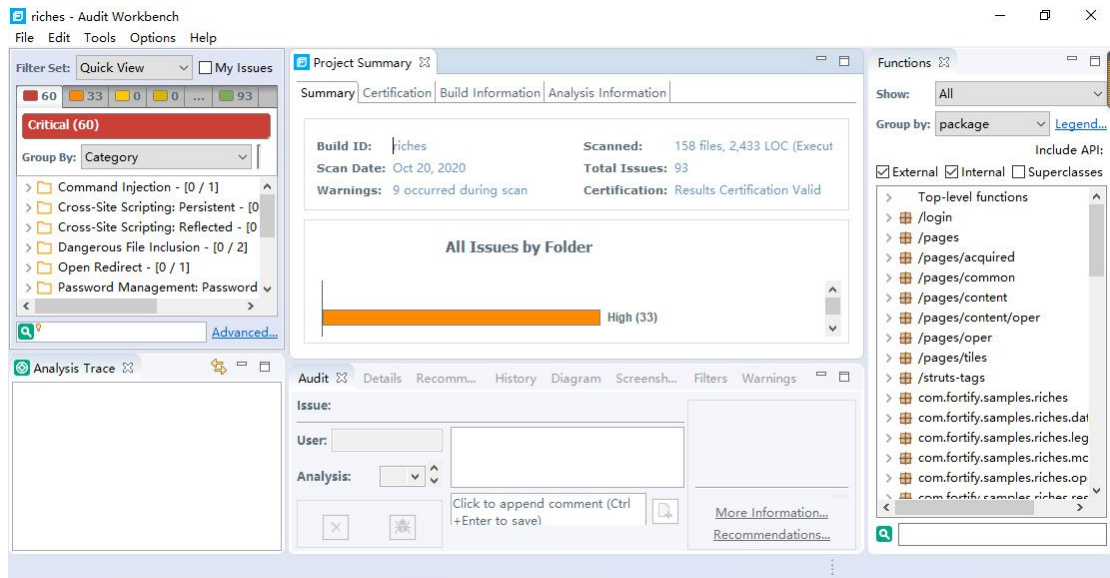
(4) 进行代码测试配置



(5) 运行代码测试



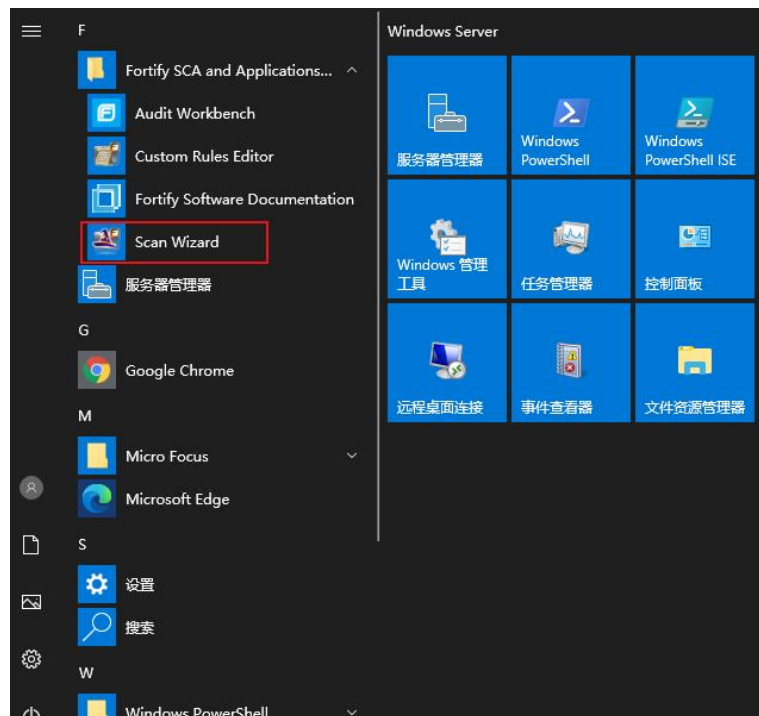
(6) 查看代码测试结果



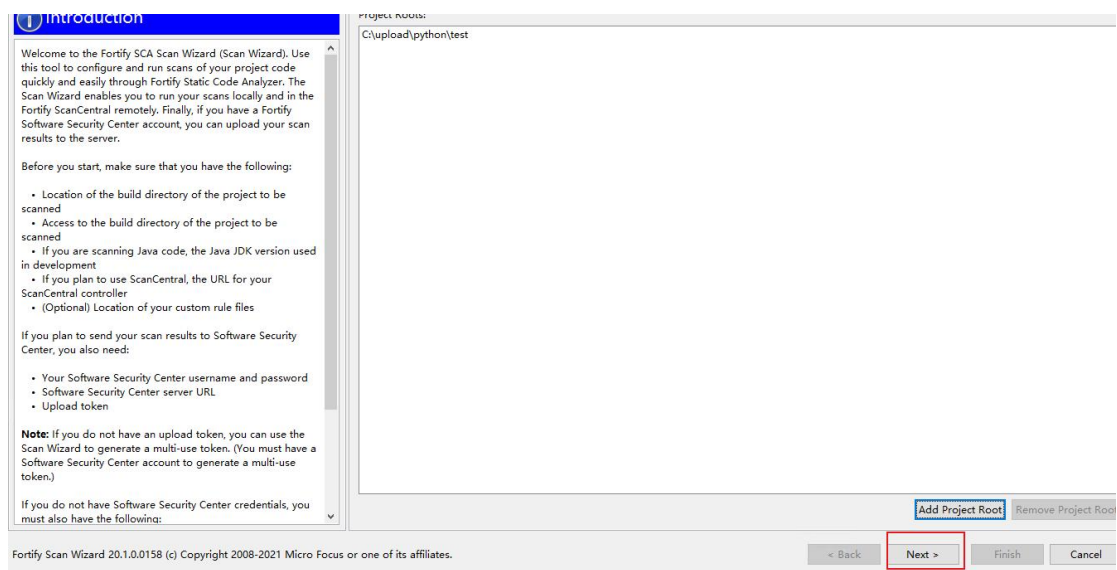
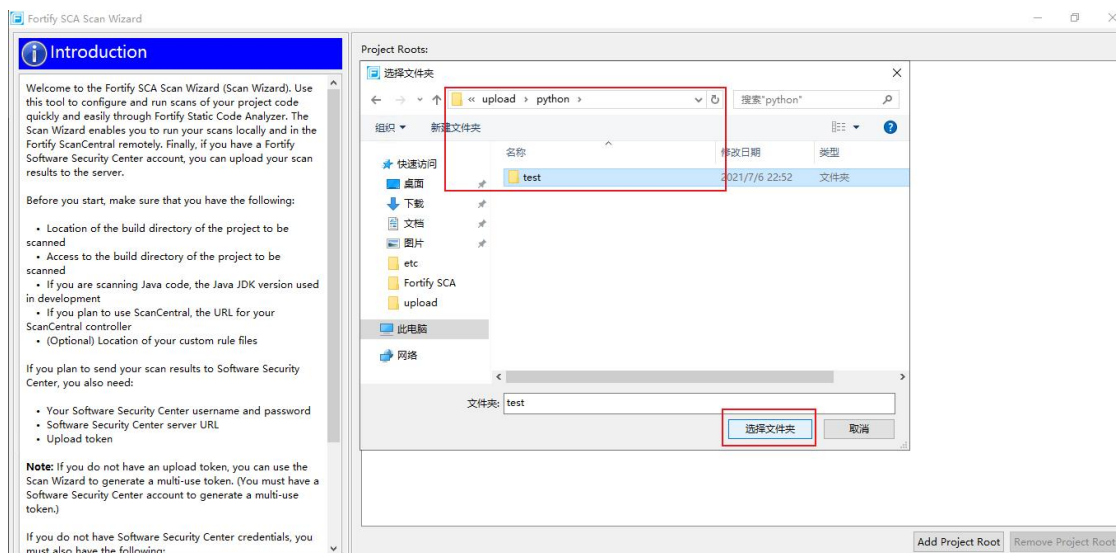
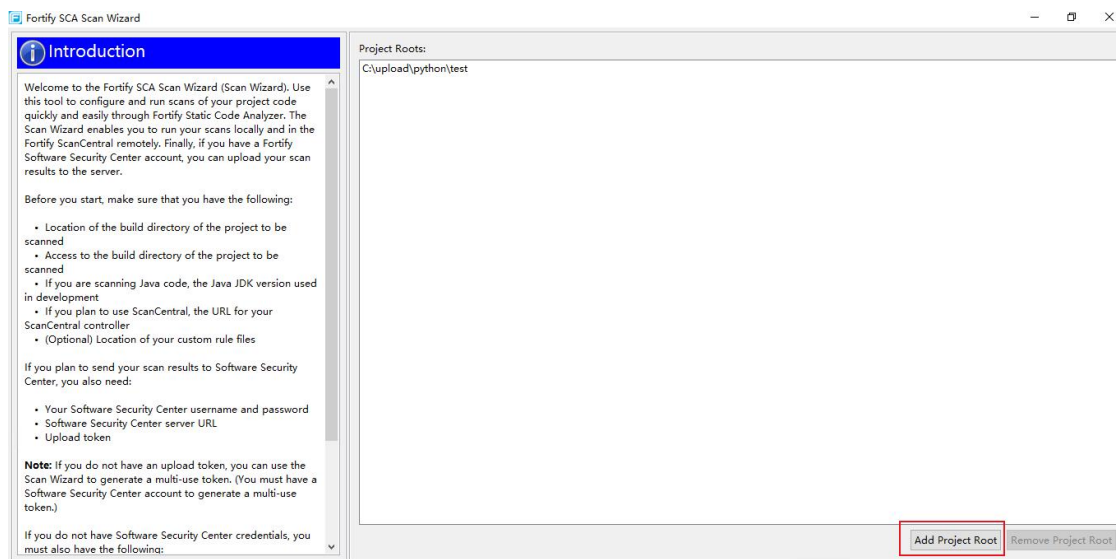
5.2. 通过“Scan Wizard”进行测试

“Scan Wizard”支持 Java、Python、C/C++、.Net、Go、PHP、Flex、Action Script、HTML、XML、JavaScript、TypeScript、Kotlin、SQL、ABAP、ColdFusion 语言或框架源代码的测试。

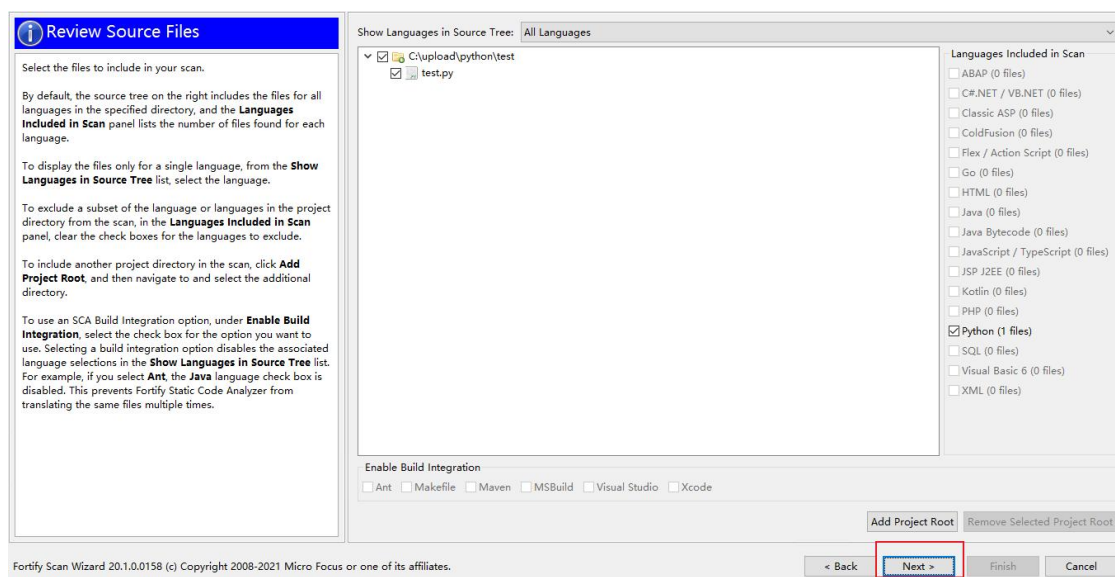
(1) 打开 Scan Wizard



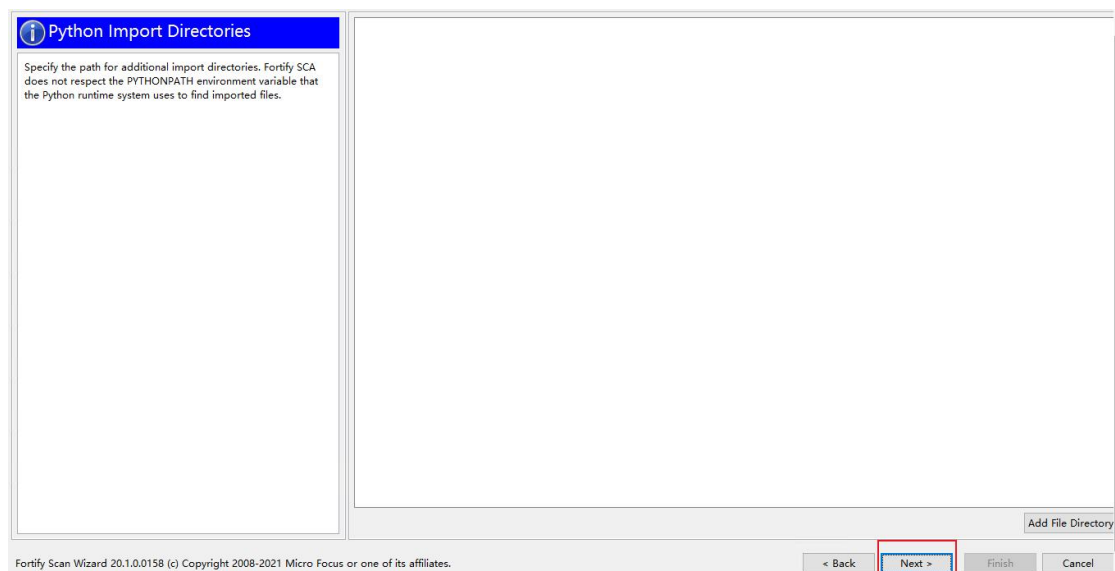
(2) 选择 Python 文件所在目录



(3) 确认测试工具自动识别内容



(4) 选择库文件



(5) 生成脚本文件

Translation and Scan

Specify how to run your scan and how to handle the output.

Windows Script: Select this check box to generate a script formatted for Windows. In the **Script file location** box, enter the directory in which to store the script.

Unix Script: Select this check box to generate a script formatted for Unix or a Unix-like operating system. In the **Script file location** box, enter the directory in which to store the script.

Scan phase: Select this check box to initiate an SCA scan of the translated data.

Scan result name: To use a file name other than the default shown in the **Scan result name** box, type a name for the FPR file produced by the scan. Make sure that you include the .fpr file extension in the file name.

Quick Scan: Select this check box to scan the project in Quick Scan mode.

Upload scan to SSC: Select this check box to upload the FPR file to Software Security Center.

ScanCentral scan: Select this check box to use ScanCentral to execute the scan phase remotely.

Include custom rules: Select this check box to include custom rules in your scan.

Scan memory: Specify the amount of memory SCA uses for scanning.

Windows Script

☒ Generate Script for Windows

Script file location:

Unix Script

☐ Generate Script for Unix

Script file location:

☒ Scan phase (in addition to translation phase)

Scan Options

Scan result name:

☒ Quick Scan

☐ Upload scan to SSC

☐ ScanCentral scan

☐ Include custom rules

Scan memory: / 15854 Mb

Fortify Scan Wizard 20.1.0.0158 (c) Copyright 2008-2021 Micro Focus or one of its affiliates.

< Back **Next >** Finish Cancel

(6) 完成脚本文件生成

Summary

Thank you for using the **Fortify SCA Scan Wizard**.

Important: You cannot run a script generated on a Windows machine on a non-Windows machine. Likewise, you cannot run a script generated on a non-Windows system on a Windows system.

To use this script, copy it to the relevant directory and run it. The script translates (and scans, if selected) the files you specified when you generated the script.

Successfully created script "C:\upload\python\test\Fortifytest.bat":

```

@echo off
REM #####
REM Script generated by Fortify SCA Scan Wizard (c) 2011-2021 Micro Focus or one of its affiliates
REM Created on 2021/07/06 23:03:23
REM #####
REM Generated for the following languages:
REM Python
REM #####
REM DEBUG - if set to true, runs SCA in debug mode
REM SOURCEANALYZER - the name of the SCA executable
REM FPR - the name of analysis result file
REM BUILDID - the SCA build id
REM ARGFILE - the name of the argument file that's extracted and passed to SCA
REM BYTECODE_ARGFILE - the name of the argument file for Java Bytecode translation that's extracted and passed to SCA
REM MEMORY - the memory settings for SCA
REM SCANSWITCHES - parameters to be passed to the analysis phase of SCA
REM LAUNCHERSWITCHES - the launcher settings that are used to invoke SCA
REM OLDFILENUMBER - this defines the file which contains the number of files within the project, it is automatically generated
REM FILENOMAXDIFF - this is the percentage of difference between the number of files which will trigger a warning by the script
REM #####

set DEBUG=false
set SOURCEANALYZER=sourceanalyzer
set FPR="Fortifytest.fpr"
set BUILDID="test"
set ARGFILE="Fortifytest.bat.args"
set BYTECODE_ARGFILE="Fortifytest.bat.bytecode.args"
set MEMORY=-Xmx14268M -Xms400M -Xss24M
set LAUNCHERSWITCHES=""
set SCANSWITCHES=""
set OLDFILENUMBER="Fortifytest.bat.fileno"
set FILENOMAXDIFF=10
set ENABLE_BYTECODE=false
        
```

Fortify Scan Wizard 20.1.0.0158 (c) Copyright 2008-2021 Micro Focus or one of its affiliates.

< Back Next > **Finish** Cancel

(7) 执行生成的脚本文件

此电脑 > 本地磁盘 (C:) > upload > python > test

名称	修改日期	类型	大小
Fortifytest	2021/7/6 23:04	Windows 批处理...	6 KB
test.py	2021/7/6 22:52	PY 文件	1 KB

5.3. 通过命令行进行测试

命令行方式支持各语言源代码的测试。

5.3.1. Linux 项目测试

以 Linux 下 C/C++ 程序代码测试为例：

1. 代码编译

在代码测试执行前, 首先需要进行 C/C++ 程序代码的编译, 如下面的示例:

```
gcc -l. -o hello.o -c helloworld.c
```

通过 gcc 编译器将代码进行编译。

2. 代码测试

在代码编译后, 使用 sourceanalyzer 命令进行代码文件测试。

```
sourceanalyzer -b <build_id> gcc -l. -o hello.o -c helloworld.c
```

3. 代码扫描结果文件生成

在代码测试后, 使用 sourceanalyzer 命令进行代码文件扫描及结果文件生成。

```
sourceanalyzer -b <build_id> -scan -f hello.fpr
```

其中, 本命令中的<build_id>与第 2 步命令中的<build_id>相同。成功生成结果文件后, 可以基于该结果文件生成测试报告。

4. 代码扫描结果文件生成

在代码测试后, 使用 sourceanalyzer 命令进行代码文件扫描及结果文件生成。

5.3.2. iOS 项目测试

1. iOS 项目测试条件

- (1) iOS 项目需要使用 non-fragile Objective-C runtime 模式 (ABI version 2 或 3)
- (2) 使用 Apple “xcode-select command-line tool” 设置 Xcode path, 同时供 Fortify 使用。
- (3) 确保项目相关依赖库文件已经包含在项目中。
- (4) 针对 Swift 代码, 确保所有第三方模块都已经被包含, 包括 Cocoapods。
- (5) 如果项目中包含二进制的属性列表文件, 需要将它们转化为 XML 格式, 通过 Xcode 的 `putil` 命令进行转换。
- (6) 针对 Objective-C 项目, 需要保证头文件能够被获取。
- (7) 针对 WatchKit 应用, 需要同时转化 iPhone 应用和 WatchKit 扩展目标。

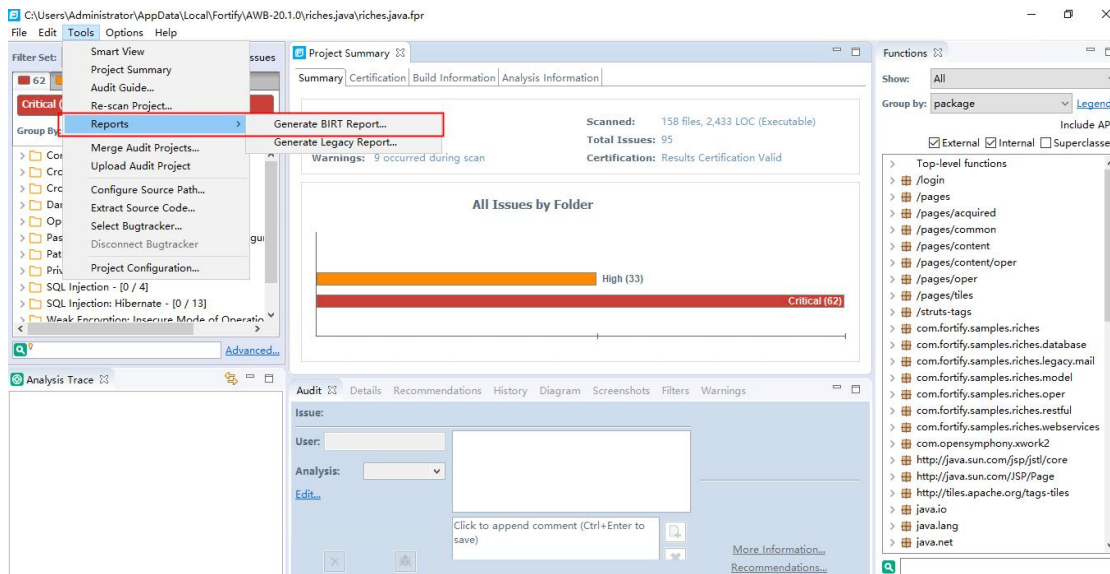
2. iOS 代码测试执行

```
sourceanalyzer -b <build_id> xcodebuild [<compiler_options>]
```

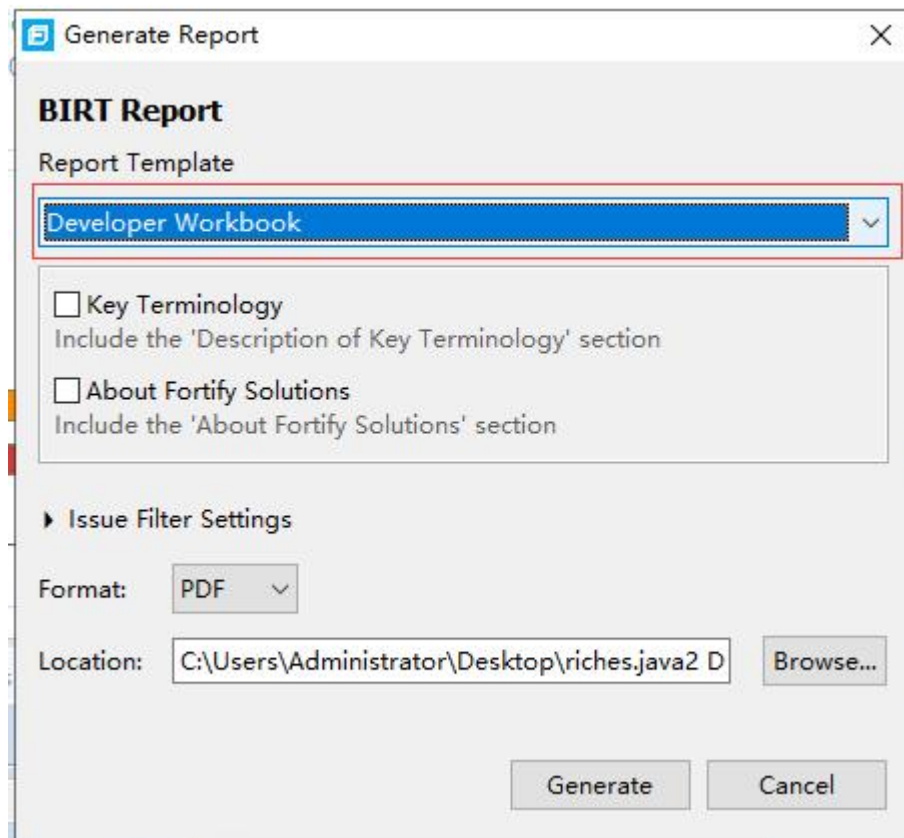
6. 测试报告生成

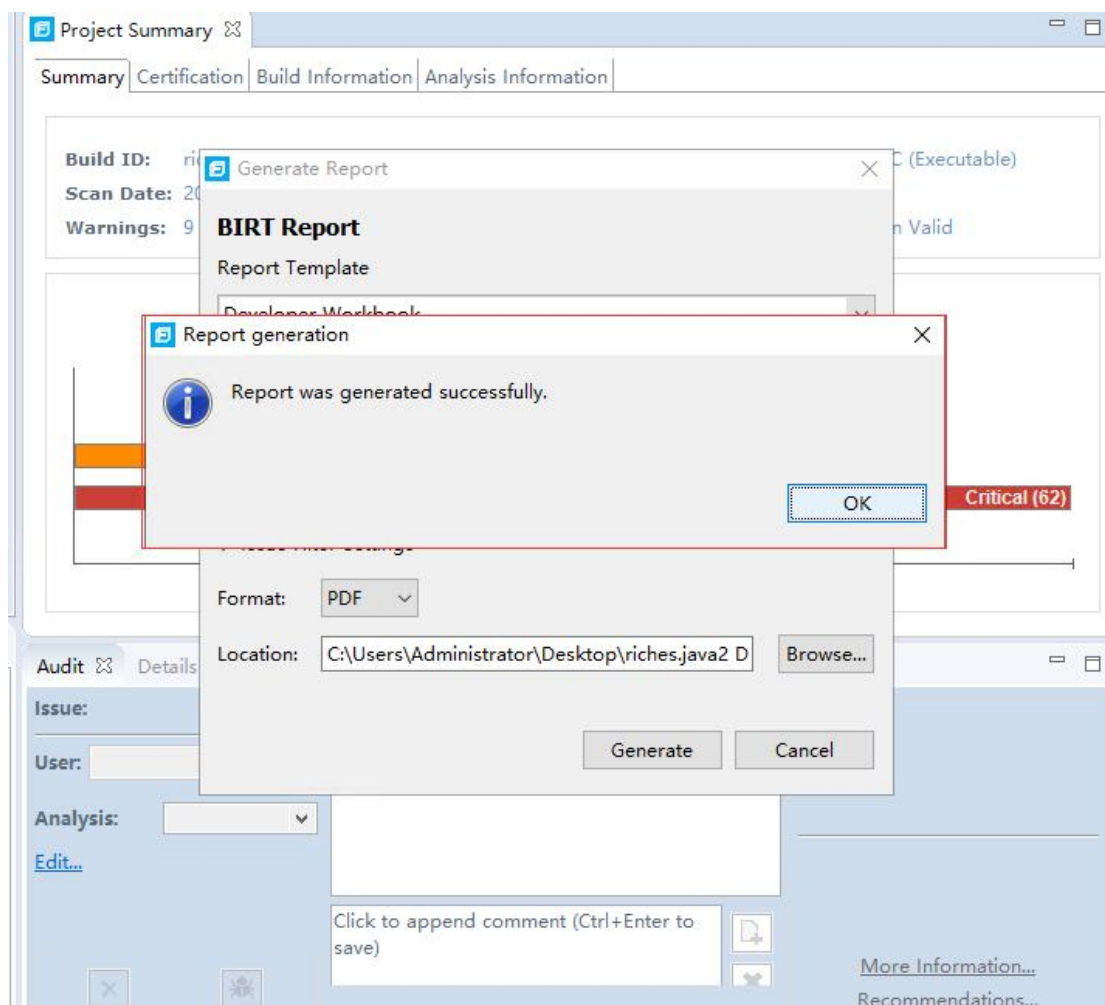
6.1. 通过 “Audit Workbench” 生成测试报告

1. 打开 “Audit Workbench” 中的 “Tools-Reports”, 选择 “Generate BIRT Report” 或者 “Generate Legacy Report”。



2.在报告模板“Report Template”中选择“Developer Workbook”，点击“Generate”按钮，工具会自动生成报告。





6.2. 通过“Scan Wizard”生成测试报告

通过“Scan Wizard”方式进行测试执行，会生成.fpr 测试结果文件，然后通过命令行方式基于测试结果文件生成测试报告文件。

6.3. 通过命令行生成测试报告

通过“Scan Wizard”方式或命令行方式生成测试结果文件后，可以基于“ReportGenerator”命令生成测试报告。

下面示例中，基于.fpr 结果文件生成 PDF 格式的测试报告。

```
ReportGenerator -format pdf -f <my_report>.pdf -source <my_results>.fpr
```

<my_report>.pdf 为命名的 PDF 格式测试报告名称，<my_results>.fpr 为测试结果

文件名称。