第5章 移动安全快速入门

5.1 常用工具介绍

本节着重介绍两款常用的安全测试和代码分析工具：JADX 和 Burp Suite。JADX 是一款开源的反编译工具，能够将安卓应用的 DEX 文件和 APK 文件转换为 Java 代码，便于用户理解和分析安卓应用。Burp Suite 作为一款网络应用安全测试工具，具备检测和修改网络流量等功能。本节将详细介绍这两款工具的功能特点以及应用方法，以案例实践的方式带领读者体验移动安全分析的基本流程，为读者在安全测试和代码分析方面提供实用的指导。

5.1.1 JADX

JADX(dex to java decompiler)是一款开源的反编译器，主要用于将安卓应用的 DEX 文件和 APK 文件转换成 Java 源代码。对于安全研究人员而言，对安卓应用的源代码进行分析可以帮助发现潜在的安全漏洞、恶意行为以及隐私问题。JADX 同时支持命令行和图形界面，能够以简便的方式完成 APK 文件的反编译操作，从而帮助开发者深入理解安卓应用和所用库的代码逻辑。

JADX 的主要功能如下。

(1) 反编译：JADX 可以将来自 APK 和 DEX 等文件直接反编译为较为易读的 Java 源代码。

(2) 解析：JADX 可以解析 APK 文件中的 AndroidManifest.xml 配置文件以及 resources.arsc 中包含的二进制资源文件。

(3) 代码优化：JADX 可以对复杂的 Java 代码进行优化，使其更加简洁和易于理解，这包括使用其自带的反混淆器以简化控制流、消除无效代码等。

除了命令行工具，JADX 还提供了图形用户界面，称为 jadx-gui。该界面进一步完善了分析反编译代码的过程，可以查看带有突出显示的反编译代码，并集成了代码编辑器常见的函数跳转、交叉引用查找、字符串搜索等功能，可以快速查找特定函数或代码片段，极大地增强了代码定位和理解能力。此外，jadx-gui 集成了 Smali 调试器，允许用户查看和调试安卓应用的中间表示形式——Smali 代码，这一功能对于深入理解和分析安卓应用的底层逻辑尤为重要。

1. JADX 的安装

根据用户的操作系统和偏好，安装 JADX 可以通过几种不同的方法进行。以下是一些常见的安装 JADX 的方法。

1）下载预编译的二进制文件

该安装方法适用于所有主要的操作系统（Windows、macOS、Linux）。

（1）下载及解压：访问 JADX 官方的 GitHub 主页（https://github.com/skylot/jadx），单击页面右侧的 Release 链接，在打开的页面中找到最新版本，下载适用于用户操作系统的预编译压缩文件（如.zip 文件或.tar.gz 文件）并解压文件到用户选择的目录。

（2）运行可执行文件：解压完成后，在解压目录的 bin 文件夹下，有两个文件，jadx（命令行版本的应用）和 jadx-gui（图形界面版本的应用）。通过直接运行可执行文件（在 Windows 操作系统上是.bat 文件，在 Linux 操作系统和 macOS 操作系统上是.sh 文件）即可启动 JADX。

注：为了启动 JADX，请确保已经安装了 64 位的 Java 11 或更高的版本。

2）通过包管理器安装

对于某些操作系统，用户可以直接使用系统对应的包管理器来安装 JADX。

（1）Arch Linux：sudo pacman -S jadx。

（2）Debian/Ubuntu：sudo apt-get install jadx。

（3）macOS：brew install jadx。

（4）Flathub：flatpak install flathub com.github.skylot.jadx。

这些命令会自动下载和安装 JADX 及其所有依赖项，安装好的 JADX 会被添加到系统路径下，可以从任何位置通过命令行直接启动。对于某些操作系统（如 macOS 操作系统），系统路径可能不会自动更新，可能需要手动将 JADX 的安装路径添加到系统的环境变量中。

3）从源代码编译

如果需要使用最新的开发版本或添加自定义功能的 JADX，可以选择从源代码编译，其步骤如下。

（1）安装 JDK（Java development kit）：确保安装了 11 版本或以上的 JDK。

（2）克隆 JADX 的 GitHub 仓库：git clone https://github.com/skylot/jadx.git。

（3）进入克隆的仓库目录：cd jadx。

（4）编译并构建项目：./gradlew dist（注：在 Windows 操作系统上，使用 gradlew.bat 而非 gradlew）。

构建完成后，用于运行 JADX 的可执行脚本位于 build/jadx/bin，并打包到 build/jadx-<version>.zip。

2. JADX 的使用

JADX 提供了两种主要使用方式来满足不同用户的需求：命令行工具（jadx）和图形用户界面（jadx-gui）。以下是对这两种使用方法的详细介绍：

1) JADX 命令行工具

JADX 的命令行版本适用于习惯在终端或命令行界面工作的用户。其优点是可以快速反编译 APK 或 DEX 文件，并将输出保存为 Java 源代码文件，使用方式非常直接，适用于自动化脚本或批量处理任务。

需要反编译名为 example.apk 的安卓应用并将输出保存在当前目录，用户可以使用命令：jadx example.apk。这将在当前目录下创建一个名为 example 的文件夹，其中包含了反编译生成的 Java 源代码。另外，如果用户想将输出保存到特定目录，比如，名为 output_dir 的文件夹，可以使用 jadx -d output_dir example.apk 命令。

运行上述 JADX 命令反编译一个 APK 文件后，JADX 会在用户选择的目录下生成一个新的文件夹，其名称通常是根据 APK 文件的名称来命名的，如本例中将得到 example 文件夹。在 example 文件夹中，存在两个主要的子文件夹，resources 文件夹和 sources 文件夹。这两个文件夹分别承载了应用的不同组成部分，提供反编译后的详细信息。

(1) resources 文件夹：该文件夹包含了 APK 文件中的所有资源文件，通常包括图片(如 PNG 文件、JPG 文件)、布局文件(XML 文件)、字符串资源、样式定义等。

(2) sources 文件夹：该文件夹包含从 APK 文件中反编译得到的 Java 源代码，主要体现了应用的逻辑和功能。

除了这两个主要的文件夹，AndroidManifest.xml 清单文件也是安全分析的重要信息来源，它包含了应用的基本信息，如权限声明、定义的活动和服务等。

2) JADX 图形用户界面

jadx-gui 将复杂的反编译过程封装在一个易于导航和使用的图形界面中，使得分析反编译代码更加便捷。接下来介绍其常见使用步骤。

(1) 启动 jadx-gui。jadx-gui 通常附带一个名为 jadx-gui.sh(Linux 操作系统或 macOS 操作系统)或 jadx-gui.bat(Windows 操作系统)的可执行启动脚本文件。运行该文件即可启动 jadx-gui。此外，若 JADX 的安装路径已经添加到了系统环境变量中，也可以直接在命令行窗口中输入 jadx-gui 命令来启动 JADX 的图形界面。

(2) 打开目标文件。在 jadx-gui 的界面顶部，单击 File 菜单，然后选择 Open files 选项。将打开一个对话框，让用户浏览并选择需要反编译的 APK 文件或 DEX 文件。一旦选择了文件，JADX 将自动执行反编译流程，并加载文件内容。

(3) 浏览和分析代码。jadx-gui 会以树状结构展示反编译结果，其中包括了所有检测到的包、类、方法和资源文件，该结构使得导航和定位特定部分代码变得简单直观。同时，用户可以使用 jadx-gui 中的搜索功能来查找特定的类名、方法名或字段。此外，JADX 支持在代码中的方法和类名之间跳转，这对于理解代码逻辑和依赖关系非常有帮助。

(4) 导出代码。如果需要保存反编译的源代码，可以通过选择 File→Save all 选项来实现。这将导出整个项目的源代码，通常是以 Java 文件的形式保存在指定目录中，方便用户进一步进行后续分析。

3. 高级功能

JADX 的图形用户界面提供了一些高级的代码分析功能，使得理解和审查反编译的

代码更为高效，以下是对这些功能的详细介绍。

（1）搜索功能。JADX 内置了强大且灵活的搜索功能，支持多种匹配模式。如图 5-1 所示，通过单击 Navigation 菜单来打开搜索框，可以搜索特定的类、方法、属性、代码片段、文件，甚至是代码中的注释。这意味着，无论是需要查找一个特定的方法实现，还是寻找特定的 API 调用，JADX 的搜索功能都能够帮助精确定位。

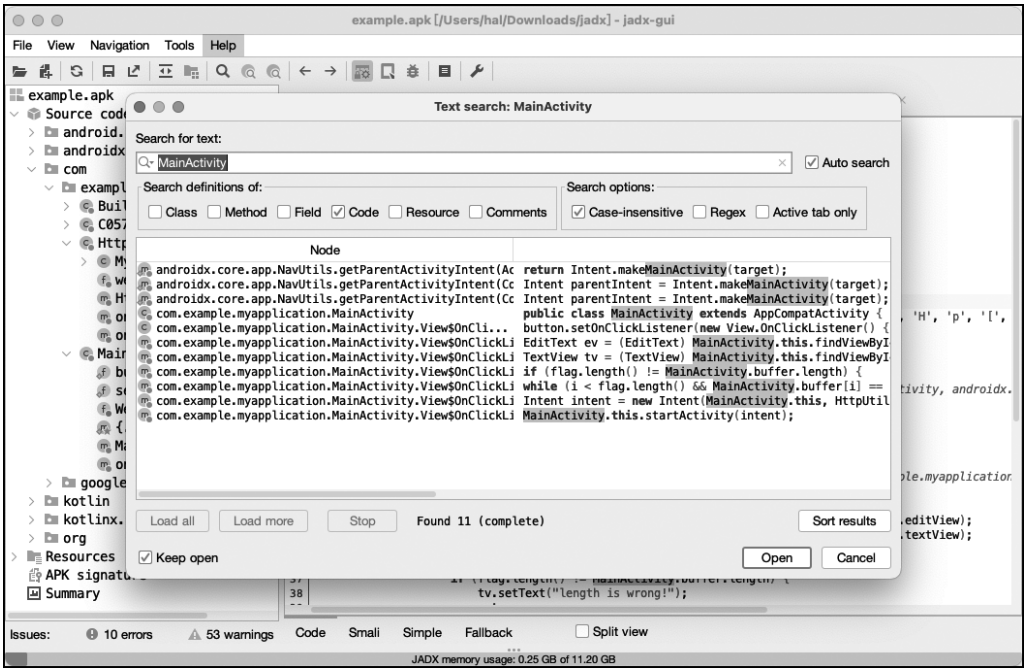

图 5-1　JADX 搜索功能

（2）声明/定义跳转。当需要查找类、方法或字段的声明/定义位置时，JADX 可以直接使用 Ctrl 键＋单击的方式，跳转到光标下符号的声明/定义位置。另一种方式是在鼠标选中指定的符号后按 D 键，或者右击，在弹出的快捷菜单中选择 Go to declaration 选项，可以直接跳转到所选符号的声明/定义处。

（3）交叉引用查找。JADX 支持快速定位代码中特定类、变量或方法的所有位置，如图 5-2 所示，这对于理解类和方法的调用关系和依赖关系非常有帮助。先在代码中选中一个类、变量或方法，再按 x 键或右击并在弹出的快捷菜单中选择 Find Usage 选项，JADX 会显示该符号的引用位置列表。

（4）添加注释。为了更好地理解或记录代码的特定内容，JADX 允许用户直接在源代码中添加个性化的注释。在想要添加注释的代码位置上，右击并在弹出的快捷菜单中，选择 Comment 选项，即可在弹出的对话框中输入任意的注释文本。

（5）反混淆。通常在发布一个 APK 文件之前，为了增强项目的安全性，开发者进行代码混淆，其目的是防止代码被轻易地逆向和破解，从而保护知识产权和阻拦攻击者利用潜在的安全漏洞发动攻击，关于该技术的详细内容将在第 6 章介绍。经过混淆的代码在功能上是没有变化的，但是去掉了部分语义信息。JADX 提供了代码的反混淆功能，以提

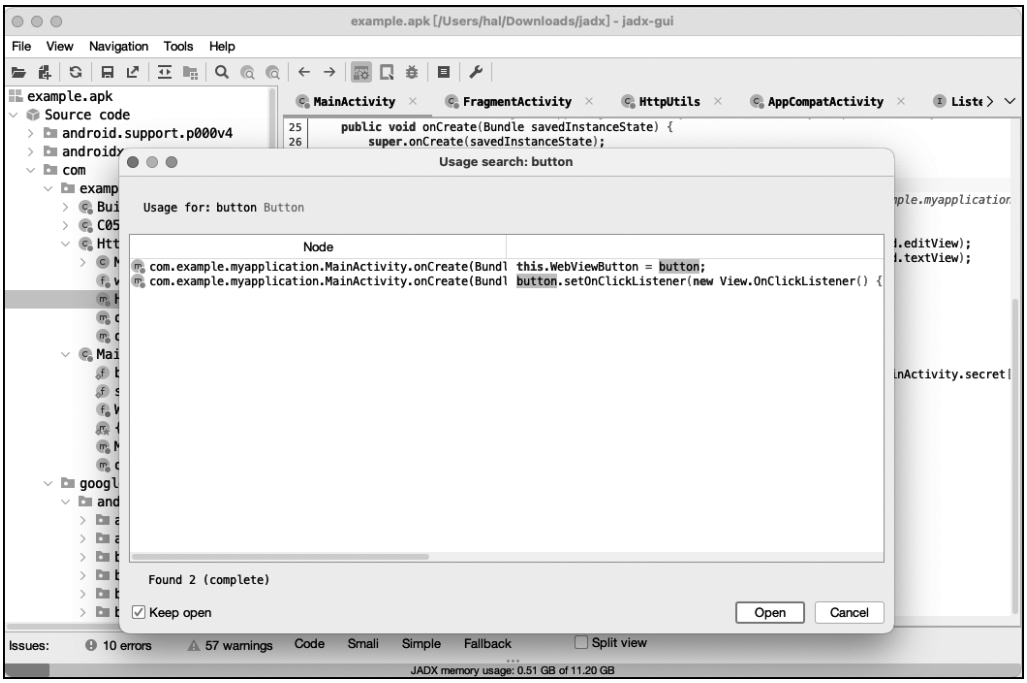

图 5-2　JADX 交叉引用查找

高代码的易读性。在 JADX 的图形用户界面中，选择 Tools→Deobfuscation 选项，可以执行代码的反混淆处理。这一功能可以将混淆后的标识符替换成更具可读性的形式，从而帮助开发者更好地理解和分析代码的逻辑和功能。

5.1.2　Burp Suite

Burp Suite 是 Web 应用渗透测试集成平台，它包含了许多工具，并为这些工具设计了许多接口，为安全研究人员和渗透测试人员提供了全面的功能套件。

移动应用通常由前端（客户端）和后端（服务端）组成，两者之间通过网络进行交互通信，以实现复杂的业务逻辑和数据交换。前端负责提供用户界面和满足用户需求，包括数据输入、页面展示和用户交互。后端则处理核心逻辑，如数据存储、身份验证、授权和数据处理等。这两部分通常通过常见的超文本传输协议（hypertext transfer protocol，HTTP）或超文本传输安全协议（hyper transfer protocol secure，HTTPS）进行通信，与 Web 应用类似。因此，前后端的交互成为移动应用安全测试的重点，Burp Suite 工具的强大功能和灵活架构使其能够在移动应用安全测试中发挥重要作用。

通过其集成的各种模块，Burp Suite 能够拦截、检查和修改移动应用与服务器之间的通信，帮助用户发现并利用应用中的漏洞。其功能包括拦截器、代理服务器、扫描器、重放器等，使安全分析人员能够对移动应用的各方面进行深入审查和测试。

1. Burp Suite 的安装

安装 Burp Suite 主要通过下载并运行其官方软件安装包来完成。用户可以根据自己

的实际需求选择合适的版本进行安装。以下是详细步骤。

(1) 下载 Burp Suite。访问 PortSwigger 官方网站(https://portswigger.net/burp),单击页面上方的 Products 可以选择下载最新版本的 Burp Suite,其提供两个版本:社区版和专业版。社区版是免费的,适合初学者进行基础的安全测试,可直接下载使用。而专业版则提供更全面的功能,包括高级扫描器、更广泛的漏洞检测能力和自动化工具等,需要购买许可证使用。用户可以根据 Burp Suite 版本及设备对应的操作系统选择对应的软件安装包进行下载。

(2) 安装 Burp Suite。运行上一步所下载的安装包,按照指引完成安装 Burp Suite。若下载版本为 Burp Suite 专业版,需要输入购买的许可证密钥。根据指引安装完成后,即可使用 Burp Suite。

2. Burp Suite 核心功能

由于 Burp Suite 是一个工具集成平台,在启动 Burp Suite 后,其窗口内将展示多个选项卡,每个选项卡提供不同的功能和工具,接下来将对 Burp Suite 的部分功能和工具进行详细介绍。

1) 代理(proxy)

Burp Proxy,作为浏览器与目标应用之间的 Web 代理服务器,提供了拦截、检查和修改双向传输流量的能力,其中也包括对 HTTPS 应用的测试。作为 Burp Suite 平台中的关键组件,Burp Proxy 允许用户利用 Burp Suite 的其他工具对请求进行深入分析,极大地提升了安全测试的灵活性和效率。

2) 入侵器(intruder)

Burp Intruder 用于对应用执行自动化定制攻击。通过配置攻击,可以在反复发送相同 HTTP 请求的同时,将不同的实际攻击代码(即有效载荷)插入预先定义的位置。该工具特别适用于大规模测试,如穷举攻击、输入验证测试和安全性评估,从而高效地识别和利用应用的潜在弱点。通过灵活配置不同的有效载荷和目标位置,入侵器能够针对 Web 应用的特定功能或参数实施精确的测试。

3) 重放器(repeater)

Burp Repeater 专为重复修改和发送特定 HTTP 等消息而设计。它广泛应用于各种场景,如发送具有变化参数值的请求,依照特定顺序发送一连串 HTTP 请求。

重放器允许同时在多个独立的标签页处理多条消息,每个标签页的修改都会被存储在历史记录中。对于 HTTP 请求,还可在每个标签页上添加注释,以强化信息的追踪和管理。这种灵活的操作方式和细致的控制手段,使得重放器尤其适用于需要精确调整和观察请求结果的复杂场景。

4) 定序器(sequencer)

Burp Sequencer 是分析一组令牌随机性质量的工具,通常用于检测访问令牌是否可预测、密码重置令牌是否可预测等场景,通过定序器的数据样本分析,可以很好地降低关键数据被伪造的风险。

这类分析在确定诸如会话管理等关键功能的有效性方面至关重要,有助于识别和修

正因随机性质量不足而引发的潜在安全漏洞。通过对令牌样本的综合评估，定序器能够提供有关其随机性质量的详细信息，从而有助于增强应用的整体安全性。

5）解码器（decoder）

Burp Decoder 可用于将数据转换成常见编码格式和对数据进行解码，其主要用途包括：手动解码数据，自动识别并解码常见的编码格式，以及将原始数据转换成不同的编码和散列格式。

解码器可以对同一数据进行多层转换，以解开或实施复杂的编码方案。例如，为了生成用于攻击的正确格式数据，可以先依次进行统一资源定位符（uniform resource locator，URL）解码、超文本标记语言（hypertext markup language，HTML）解码，并编辑解码后的数据，然后重新进行 HTML 编码、URL 编码，以转换为可以用于攻击的正确格式数据。

执行转换操作时，可以从各种工具中的消息编辑器发送数据到解码器，并使用其进行数据转换。

6）扩展（extensions）

Burp Extensions 提供了自定义 Burp Suite 行为的功能。用户可以使用社区中其他人开发的 Burp 扩展，也可以自行编写扩展。

大多数高质量 Burp Suite 扩展可以从 BApp Store 下载，这些扩展由 Burp Suite 的第三方用户编写和维护，并由官方对其进行安全性审核，但不对其特定用途的适用性作出任何保证。扩展为用户提供了更广泛的测试和自定义选项，从而增强了 Burp Suite 的灵活性，这使得用户能够根据自己的特定需求和偏好，为 Burp Suite 增添新的维度和功能。

3. Burp Suite 的使用

由于移动应用中存在大量的前后端数据交互行为，该过程通常也是漏洞出现的高频场景。因此，安全研究人员常常通过监控触发某些操作时的数据交互网络流量，来了解数据的发送、接收方式以及使用的数据格式等。此外，通过拦截并修改流量中的参数，并观察其响应，研究人员能够测试后端是否存在身份验证绕过漏洞、不当的输入验证等问题。下面将详细介绍如何利用 Burp Proxy 拦截和修改网络流量。

1）拦截请求

Burp Proxy 能够拦截通过 Burp 浏览器与目标服务器进行通信的 HTTP 请求和响应，这一功能使得用户可以观察，并分析在进行各种操作时网站的响应和行为模式，以下是详细的步骤。

（1）启动 Burp 浏览器。首先，在 Burp Suite 窗口中选择 Proxy 选项卡下的 Intercept 标签，单击 Intercept 选项卡上的 Intercept is off 按钮，以激活拦截功能，使其变为 Intercept is on。一旦开启拦截，浏览网页或与 Web 应用交互时产生的所有网络流量都会通过 Burp Suite 处理，包括发送到服务器的每个请求和从服务器接收的每个响应。接下来，单击 Open Browser 按钮以开启一个新的窗口，即集成浏览器。该浏览器已预先配置，可直接与 Burp Suite 协同工作。

（2）拦截请求。拦截请求的目的是在流量被转发到目标服务器之前，对其进行审查和修改。当使用 Burp Proxy 时，浏览器向服务器发出的 HTTP 请求会被先拦截下来。

因此，使用该浏览器尝试访问网站 https://portswigger.net 时，网站无法加载。

(3) 转发请求。为了在 Burp 浏览器中加载完整页面，需要多次单击 Forward 按钮来逐一发送被拦截的请求及其后续请求。每次单击 Forward 按钮时，当前拦截的请求会被发送至目标服务器，随后 Burp Proxy 会继续拦截下一个请求。通过反复执行此操作，直到所有被拦截的请求都得到处理并发送，最终页面才能够在浏览器中完全加载和显示出来。

(4) 停止拦截。由于浏览器在访问网页时会发送大量的请求，通常不需要拦截每一个请求。因此，可以单击 Intercept is on 按钮将其变换为 Intercept is off 以关闭拦截功能。这样，网络流量可以在浏览器和服务器之间自由传输，从而大幅提高浏览速度和效率。

(5) 查看历史记录。在 Burp Suite 中，选择 Proxy→HTTP history 标签，可以查看所有经过 Burp Proxy 的 HTTP 通信记录。这一功能为分析过往的网络交互提供了便利，即使是在拦截功能关闭的情况下，也能回溯和审查每一次浏览器与服务器之间的请求和响应。通过这种方式，用户可以在保持正常网站浏览体验的同时，对 Burp 浏览器与服务器之间的交互进行后续分析。这种流畅浏览和详细分析相结合的方式，不仅在多数情况下更加方便高效，而且能确保用户在不受干扰的情况下浏览网站。同时，用户也能全面审查网络请求和响应，有效地揭示网络交互的细节和潜在问题。

2) 修改请求

成功拦截 HTTP 请求后，用户可以在请求编辑器中修改请求的任何部分，从而以网站非预期的方式操纵请求，并实时观察其响应结果。

(1) 编辑请求。在 Burp Proxy 的 Intercept 选项卡中，当请求被拦截后，选择需要修改的部分，并直接在请求编辑器中进行修改。该过程中，可以更改 URL、HTTP 方法、参数、Header 信息，甚至是 POST 请求的数据内容等。

(2) 重放请求。使用重放器发送修改后的请求，可以测试修改后请求的效果。右击拦截的请求，在弹出的快捷菜单中选择 Send to Repeater 选项，即可发送修改后的请求，并观察不同修改对服务器响应的具体影响。

(3) 自动化测试。在理解如何手动修改和发送请求后，还可以利用入侵器进行自动化测试。通过配置攻击类型、载荷及其他相关选项，用户可以自动发送大量的修改请求，以发现应用可能存在的潜在问题。

4. Burp Suite 移动应用抓包

Burp Suite 的代理功能能够很好地适用于移动应用中 HTTP/HTTPS 流量拦截和分析，因此广泛应用于移动应用抓包。由于 HTTPS 流量是加密的，用户需在浏览器中安装 Burp Suite 提供的 SSL 证书，使得浏览器信任其代理服务器。完成这一步骤后，Burp Suite 即可解密 HTTPS 流量，使用户能够查看和修改加密的通信内容。配置流程如下。

(1) 设置代理监听器。如图 5-3 的步骤所示，在 Burp Suite 平台中，选择 Proxy→Options 选项，在弹出的 Settings 窗口中单击 Add 按钮以添加新的监听器。在弹出窗口的 Bind to port 文本框中输入 8082，并选中 Bind to address 选项组中的 All interfaces 单

选按钮，并单击 OK 按钮保存设置。这一步骤的目的是设置 Burp Suite 平台监听所有通过 8082 端口的流量，允许其捕获从安卓设备发出的请求。

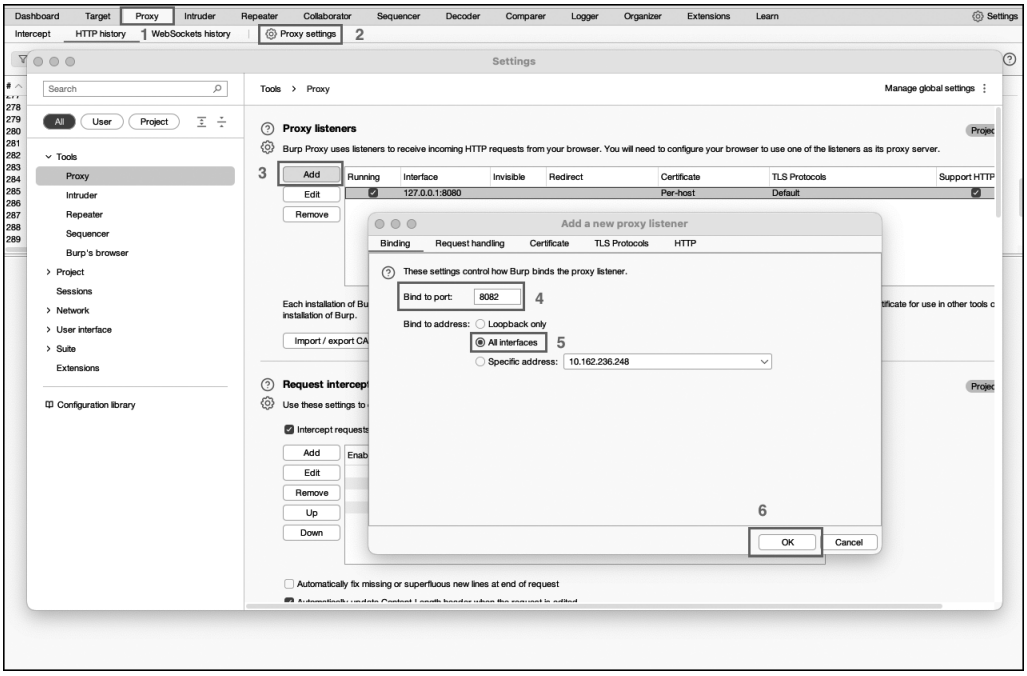

图 5-3　Burp Suite 抓包接口设置

（2）导出证书。由于用户需在浏览器中安装 Burp Suite 工具提供的安全套接层（secure socket layer，SSL）证书，使得浏览器信任其代理服务器，需要确认配置并导出证书授权（certificate authority，CA）证书，选择 DER 格式，保存为 burp.der，如图 5-4 所示。

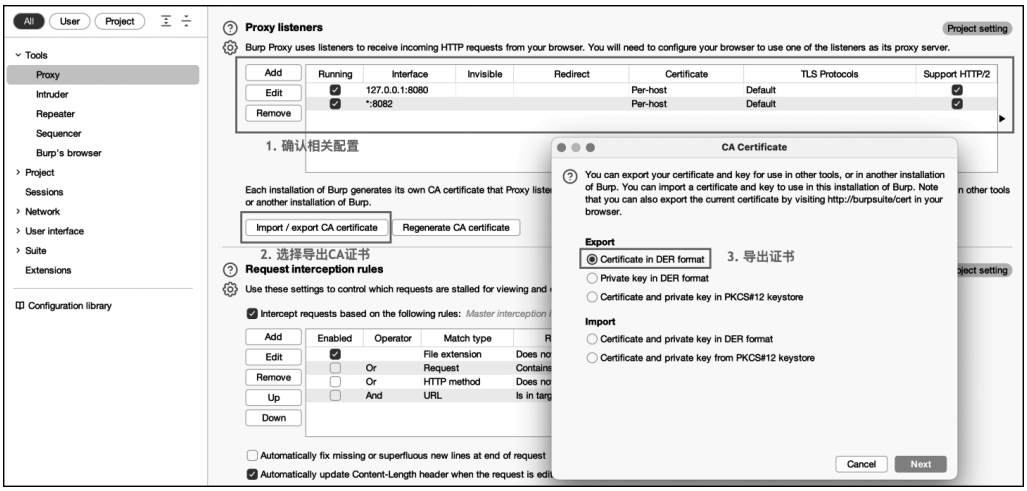

图 5-4　导出 Burp Suite 证书

（3）转换证书。导出证书后，需要使用 OpenSSL 工具转换证书格式，适应安卓系统

要求——证书必须是 PEM 格式，证书的文件名必须是证书的主题哈希值，且后缀为.0。具体转换命令如下。

```
1  openssl x509 -inform DER -in burp.der -out burp.pem
2  openssl x509 -inform PEM -subject_hash_old -in burp.pem |head -1
3  mv cacert.pem <hash_output>.0
```

(4) 安装证书。由于证书需要安装在系统文件目录/system 下，所以需要以超级用户权限运行 ADB 调试工具，并使系统分区可写。此后，需要将证书文件传输到安卓设备(或模拟器)，并将证书移动到系统证书目录，设置 644 权限，表示所有者有读取、写入的权限。

```
1  adb root
2  adb remount
3  adb shell
4  mv /sdcard/<hash >.0 /system/etc/security/cacerts
5  chmod 644 /system/etc/security/cacerts/<hash >.0
```

(5) 重启设备。在设备的“设置”中确认证书已安装，大致位置为“设置”→“安全”→“加密与凭据”→“信任的凭证”→“系统”(路径因设备系统不同可能存在差异)，若出现 PostSwigger CA 即为安装成功。

(6) 配置网络代理。这一步骤可以确保安卓设备的所有网络流量都通过 Burp Suite 代理，从而可以被捕获和分析，如图 5-5 所示。在安卓设备的设置中，找到网络选项，选择当前连接的 WiFi 网络，进入修改网络设置页面，设置代理为手动，并输入所连接计算机的 IP 地址和端口 8082(在 Burp Suite 中设置的监听端口)。

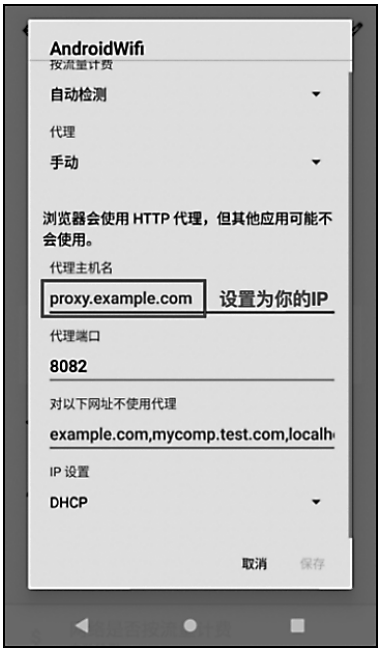

图 5-5　安卓设备代理配置