

第 6 章

Xposed 框架介绍

作为比 Frida 框架更早的 Hook 框架，Xposed 在 Android 安全领域颇负盛名，在 Frida 未出现之前更是在 App 安全测试过程中必不可少的工具。基于 Xposed 框架开发的微信/QQ 抢红包、运动记录作弊、消息防撤回等插件现在仍旧备受欢迎，本章将对这款框架进行介绍。

6.1 Xposed 框架简介

Xposed 框架（Xposed Framework）是一套开源的、在 Android root 模式下运行的框架，它可以在不修改 App 源码的情况下通过 Hook 方式去影响程序的运行。与 Frida 一样，Xposed 广泛用于 Android 安全测试中，不管是针对特定 API 的监控、恶意代码的分析还是对系统功能的自定义，Xposed 框架都能够以对 Java 代码 Hook 的方式游刃有余地完成。可惜的是，Xposed 最后的发行版是 v89，发行时间是 2017 年 12 月 18 日，如图 6-1 所示。

查看相应的代码提交记录，这个版本适配的是 Nougat 代号的 Android，通过 Android 官网提供的“代号、标记和 Build 号”对照表可知这个代号对应的 Android 版本为 Android 7.1 和 7.0，如图 6-2 所示，也就是 Xposed 在 7 之后再也没有发行过正式的版本（release 版本）。

到 2020 年，从 Xposed 官方 Framework 的网址可以得知 sdk26 以及 27 版本（Android 8.0 和 8.1）的 Xposed 还是处于 beta 版本的状态，如图 6-3 所示。