

目录

前言	1.1
Xposed简介	1.2
VirtualXposed	1.2.1
太极Magisk	1.2.2
安装Xposed	1.3
使用Xposed	1.4
Xposed心得	1.5
附录	1.6
参考资料	1.6.1

强大的安卓破解辅助工具：Xposed框架

- 最新版本：[v0.6](#)
- 更新时间：[20200904](#)

简介

介绍用于安卓破解的辅助工具：Xposed框架的基本概念和具体用法以及相关心得。

源码+浏览+下载

本书的各种源码、在线浏览地址、多种格式文件下载如下：

Gitbook源码

- [crifan/crack_assistant_xposed_framework: 强大的安卓破解辅助工具：Xposed框架](#)

如何使用此Gitbook源码去生成发布为电子书

详见：[crifan/gitbook_template: demo how to use crifan gitbook template and demo](#)

在线浏览

- [强大的安卓破解辅助工具：Xposed框架 book.crifan.com](#)
- [强大的安卓破解辅助工具：Xposed框架 crifan.github.io](#)

离线下载阅读

- [强大的安卓破解辅助工具：Xposed框架 PDF](#)
- [强大的安卓破解辅助工具：Xposed框架 ePUB](#)
- [强大的安卓破解辅助工具：Xposed框架 Mobi](#)

版权说明

此电子书教程的全部内容，如无特别说明，均为本人原创和整理。其中部分内容参考自网络，均已备注了出处。如有发现侵犯您版权，请通过邮箱联系我 [admin 艾特 crifan.com](mailto:admin@crifan.com)，我会尽快删除。谢谢合作。

鸣谢

感谢我的老婆陈雪的包容理解和悉心照料，才使得我 [crifan](#) 有更多精力去专注技术专研和整理归纳出这些电子书和技术教程，特此鸣谢。

[crifan.com](#), 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2020-09-08
21:09:23

Xposed简介

- Xposed
 - 是什么：本身是一个框架
 - 所以也称： Xposed框架
 - = Xposed Framework
 - 适用对象：安卓手机
 - 作用：可以在Xposed中安装各种插件，实现各种高级功能
 - 引申：常被用来配合破解安卓应用
 - 前提：需要安卓手机有 root权限
 - 特点
 - 开源
 - 支持插件
 - 安装插件后，可以实现各种原本很难实现的效果

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2020-09-04
22:51:38

VirtualXposed

- TODO
 - 【未解决】小米9中安装VirtualXposed
 - 【未解决】小米9中无法运行VirtualXposed会崩溃一闪而过
 - 【已解决】VirtualXposed是否真的免Root和支持哪些插件
 - 【已解决】网易MuMu中安装VirtualXposed
 - 【未解决】网易MuMu中VirtualXposed中安装和使用JustTrustMe
-

- VirtualXposed
 - 一句话简介：Use Xposed with a simple APP, without needing to root, unlock the bootloader, or flash a system image
 - 介绍：一个类似于Xposed框架
 - 但
 - 优点
 - 无需Root
 - 缺点
 - 有些其他的限制？
 - 主页
 - Download | VirtualXposed
 - <https://vxposed.com>

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2020-09-04
22:51:38

太极Magisk

- 太极·虚拟框架
 - 一句话简介：免解锁,免Root,就能使用Xposed框架
 - 一个可以免 Root 运行的类 Xposed 框架
 - 资料
 - 官网
 - <https://www.taichi-app.com/>
 - <https://taichi.cool/zh/>
 - 文档
 - 介绍 | 太极
 - <https://taichi.cool/zh/doc/>
 - 下载
 - <https://taichi.cool/zh/download.html>
 - 模块下载
 - 太极官网-太极app, 开启全新的XPOSED模块使用体验
 - <https://www.taichi-app.com/#/download/alipay>

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2020-09-04
22:51:38

安装Xposed

TODO:

- 【已解决】Mac中夜神安卓模拟器中安装Xposed框架
- 【记录】给二手已root小米4设置Charles代理和安装Charles证书和启用Xposed
- 【已解决】Mac中夜神模拟器中安装Xposed模块: JustTrustMe
- 【已解决】用WrBug的DumpDex从app中hook导出dex文件
- 【未解决】小米4中尝试安装最新3.1.5的Xposed Installer去解决2.6版本提示的不兼容的问题
- 【已解决】mac中试用FDex2去hook导出安卓app的dex等文件
- 【已解决】Android 4.4.4的小米4Xposed Installer出错: Xposed目前不兼容Android SDK版本19或您的处理器架构 armeabi-v7a
- 【已解决】Mac中夜神模拟器中安装Xposed框架
- 【已解决】Mac中夜神模拟器中安装Xposed模块: JustTrustMe
- 【已解决】价格便宜但支持root的Android手机
- 【已解决】如何确定此二手小米4是否的确已经root
- 【记录】二手已root的小米4安卓手机照片和信息
- 【已解决】小米4的MIUI系统自动升级导致清楚已有root权限后如何恢复root权限
- 【已解决】小米4中重新安装Xposed Installer和激活Xposed框架

● 如何安装

- 一般是通过 `Xposed Installer` = `Xposed安装器` 来安装 `Xposed`框架， 安装到安卓系统中
 - `Xposed Installer`
 - 可以理解为是一个特殊的安卓的应用
 - 专门用来安装Xposed框架
- 被安装的安卓系统
 - 可以用 安卓模拟器
 - 安卓模拟器有很多，不是所有的都能成功安装
 - 尝试过
 - 网易MuMu
 - 运行速度不错，但不支持设置Wifi代理
 - 详见
 - 【未解决】Mac中用Charles抓包网易MuMu安卓模拟器中Android的app
 - Andy
 - 安装后无法正常运行
 - 详见
 - 【未解决】Mac中尝试用Andy安卓模拟器去供Charles抓包Android中app的数据
 - 最终跑通的路是
 - Mac版 夜神安卓模拟器
 - 基于 Android 4.4.2
 - -> 找到了匹配的 2.7 (或更低的 2.6 等) 版本的 `Xposed Installer`，即可安装
 - 注：更高的 3.x 版本，比如 3.5.1，不支持 Android 4.4，只支持 Android 5
 - 详见
 - 【已解决】Mac中夜神安卓模拟器中安装Xposed框架
 - 【已解决】Mac中夜神模拟器中安装Xposed模块: JustTrustMe
 - 也可以用 安卓真机
 - 但前提是：安卓手机要有root权限
 - 但（2019年及之后）很难买到支持root权限的手机

- 之前跑通的路是
 - 淘宝上买的二手的已root的小米4，型号：MI 4LTE-CU，系统：Android 4.4.4
 - 注意：
 - 在无端被 MIUI 自动升级（从 5.8.5 升级为 7.5.12.17）而丢失了卖家预装好的 Xposed Installer 之后，再去费了番功夫想办法重新安装可用的 Xposed，最终思路是：
 - 网上找到了某大神 SolarWarez 修改后的 2.6 的版本的 Xposed：
 - XposedInstaller_v2.6.1_by_SolarWarez_20151129.apk
 - 才得以成功安装
 - 激活Xposed后，即可正常安装 JustTrustMe 等模块
 - 最终实现 SSL pinning 的绕开/禁止的效果
 - 就可以全部看到https解密后的明文了
 - 详见
 - 【已解决】小米4中重新安装Xposed Installer和激活Xposed框架
 - 【记录】给二手已root小米4设置Charles代理和安装Charles证书和启用 Xposed

注意手机有变砖可能

刷Xposed框架会修改系统文件，所以可能会导致手机变砖，系统崩溃。以及刷成功后系统变卡变慢。并且不保证每台机器都可以刷成功，请自行评估在决定是否安装

- » 不建议在自己的（常用）手机中装Xposed，因为很容易导致变砖
- » 建议在安卓模拟器上，或者其他开发专用的安卓机上装 Xposed
- » 或者也可以在自己手机或开发专用安卓机中免root安装 VirtualXposed 或 太极Magisk

因为免root不会导致系统崩溃或手机变砖

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2020-09-04
22:51:38

使用Xposed

安装了Xposed后，对于Xposed的使用，主要是：

- 安装各种插件
- 使用各种插件
 - 实现特定的目的和效果

比如：

- 【整理Book】好用的安卓模拟器：夜神Nox

中就有涉及到：

- 安装XPosed框架
 - 【已解决】Mac中夜神安卓模拟器中安装Xposed框架
- 在XPosed中安装JustTrustMe
 - 【已解决】Mac中夜神模拟器中安装Xposed模块：JustTrustMe
 - 然后就可以去用Charles抓包了，而绕开https了，实现了破解https的目的
 - 【整理Book】app抓包利器：Charles

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2020-09-04 22:51:38

Xposed心得

安卓破解可能会涉及到Xposed

注意到：

【已解决】 mac版JD-GUI查看并导出jar包的java源代码

和：

【已解决】 搞懂安卓app混淆和加固常见做法和相关逻辑

中都有个： XposedCheck

```

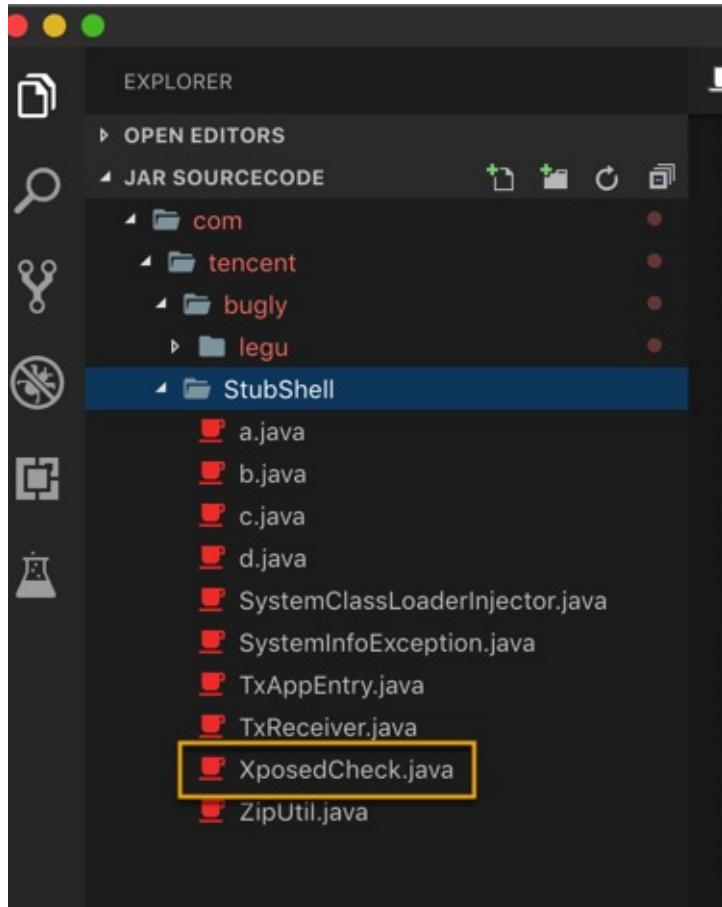
TxAppEntry.class - Java Decomplier
xiao huashengv3.6.9_downcc.com-dex2jar.jar

com.tencent
  StubShell
    SystemClassLoaderInjector.class
    SystemInfoException.class
    TxAppEntry.class
  TxReceiver.class
    TX_RECEIVER : String
    TxReceiver()
    onReceive(Context, Intent) :
      XposedCheck.class
    ZipUtil.class
    a.class
    b.class
    c.class
    d.class
  bugly.legu
    crashreport
    proguard
    Buggy.class
    BuggyStrategy.class
    CrashModule.class
    a.class
    b.class

TxAppEntry.class
private static String g;
private static String h;
private static String i = "";
private static boolean j = false;
private static String mOldAPPName;
public static Object mPClassLoader;
private static String mPKName;
private static String mSocPath;
private static String mSrcPath;
private static String mVerFilePath;
private static boolean mbVerCheck = false;
private static final String version = "a97e1a6e0a991683d921b464ea34";
private Handler k = null;

static
{
    try
    {
        j = "__TRUE__".equals(c);
        d = 0;
        e = false;
        return;
    }
    catch (Throwable localThrowable)
    {
        for (;;)
        {
            Log.w("SecShell", localThrowable);
        }
    }
}

public static void a(Intent paramIntent)
  
```



- » 看来是安卓apk加固方案内部用到了：去check检测Xposed相关的逻辑
- » 说明软件加固的破解中，有些是借助Xposed去破解安卓的
- » 实际情况的确也是，Xposed之类的框架，是帮助破解安卓的利器

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新：2020-09-04
22:51:38

附录

下面列出相关参考资料。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2020-09-04 22:51:38

参考资料

- [原创]Xposed 安装记录-『Android安全』 -看雪安全论坛
- Android APK脱壳--腾讯乐固、360加固一键脱壳 | 辉天神龙
- Difference between Xposed and VirtualXposed · android-hacker/VirtualXposed Wiki
- How does VirtualXposed work · android-hacker/VirtualXposed Wiki
- 不需要 Root, 也能用上强大的 Xposed 框架: VirtualXposed - 少数派
- 安卓应用的安全和破解
- Xposed框架概况 - Xposed框架中文站
- Xposed框架 - 维基百科, 自由的百科全书
- Xposed框架中文站 - 超多Xposed框架模块介绍与下载
- 【Android】Xposed 框架解析 - 简书
-

crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2020-09-04
22:51:38