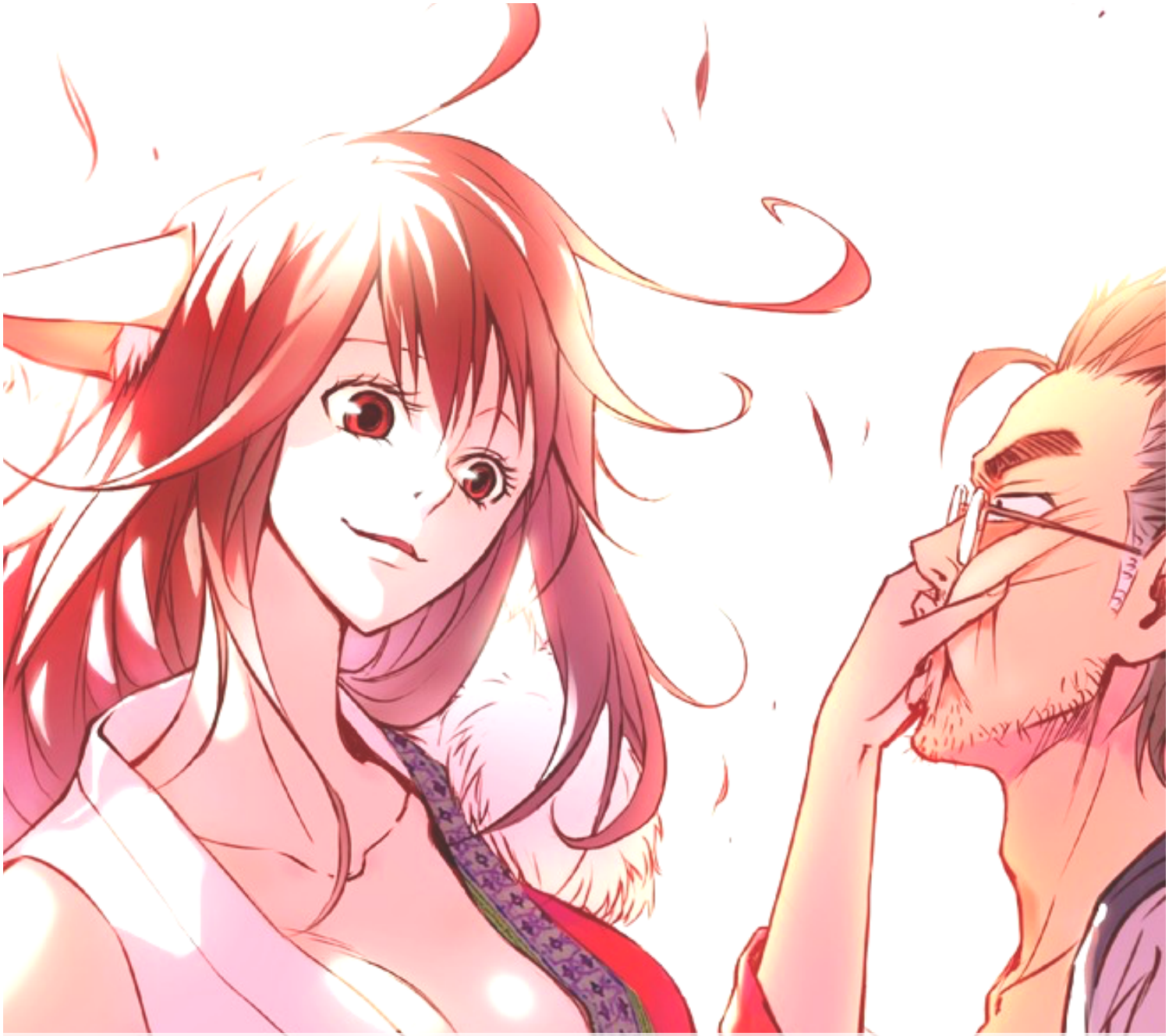

Frida 框架简介(一)

译者：lockdown(看雪 ID：小调调)

原文链接：http://www.frida.re/docs/home/

原文作者：Rotlogix

微信公众号：看雪 iOS 安全小组 我们的微博：weibo.com/pediyiosteam

我们的知乎：zhihu.com/people/pediyiosteam

Frida 简介

Welcome

本网站旨在成为 Frida 的综合指南。 我们将介绍一些主题，例如从命令行执行交互函数的跟踪、基于 Frida 的 API 构建您自己的工具、为您将来参与 Frida 开发提供一些建议等等。

So what is Frida, exactly?

它是原生程序的 Greasemonkey，可投入更多专业的项目中。它是一个动态代码工具。它允许你在 Windows、Mac、Linux、iOS、Android 和 QNX 的应用中插入 JavaScript 的代码片段。Frida 还为您提供了一些基于 Frida API 开发的简单工具。可以按原样使用，也可以根据你的需求做调整，或者作为 API 使用的范例。

Why do I need this?

好问题，我们将通过一些事例来说明：

- 有个热门的应用，它只适用于 IOS 的系统，然而你想与他进行互操作。你发现它使用了网络加密协议，像 Wireshark 这类的工具没办法分析它。此时你可以选择使用 Frida，并将其用于 API 跟踪。

- 当你构建一个桌面应用程序时——这个应用已经部署在客户的网站上——发现了一个问题：内置的日志代码不够详细。所以你可能需要给你客户一个定制的程序，写很多耗时费力的日志代码。此时你可以使用 Frida 构建一个特定的应用程序工具、添加你需要的所有诊断模块——这些诊断模块仅仅几行 Python 代码。无需向客户发送新的自定义版本，你只需要在现有的框架下，更新所需模块来完成版本更新。

- 你想要构建一个加强版 Wireshark——能嗅探加密网络协议的功能，甚至会篡改函数调用来伪造网络环境，这样的话你就不需要再建一个测试实验室。

- 可用于程序内部的黑盒测试，不会影响源代码，只需要出现异常时的逻辑流程。

Why a Python API, but JavaScript debugging logic?

Frida 的核心是用 C 语言编写的，并将谷歌的 V8 引擎（JavaScript 引擎）注入到目标进程中，你的 JS 就可以访问所有的内存数据，挂函数钩子，甚至调用程序内部的函数。有一个双向通信通道，用于应用程序（Python）和在目标进程中运行的 JS 之间进行通信。

在这个 C 语言编写的核心之上，有多种语言绑定，例如，Node.js，Python，Swift，.NET，Qml 等，并且很容易为其他语言和环境构建额外的绑定。

ProTips™, Notes, and Warnings

在本指南中，有一些小而方便的信息，可以使 Frida 变得更容易使用、更有趣，更安全。

如果上面所提到的没有你想知道的内容，或者你有更好的想法或建议，请提交给我们，我们将把它添加到该指南里。