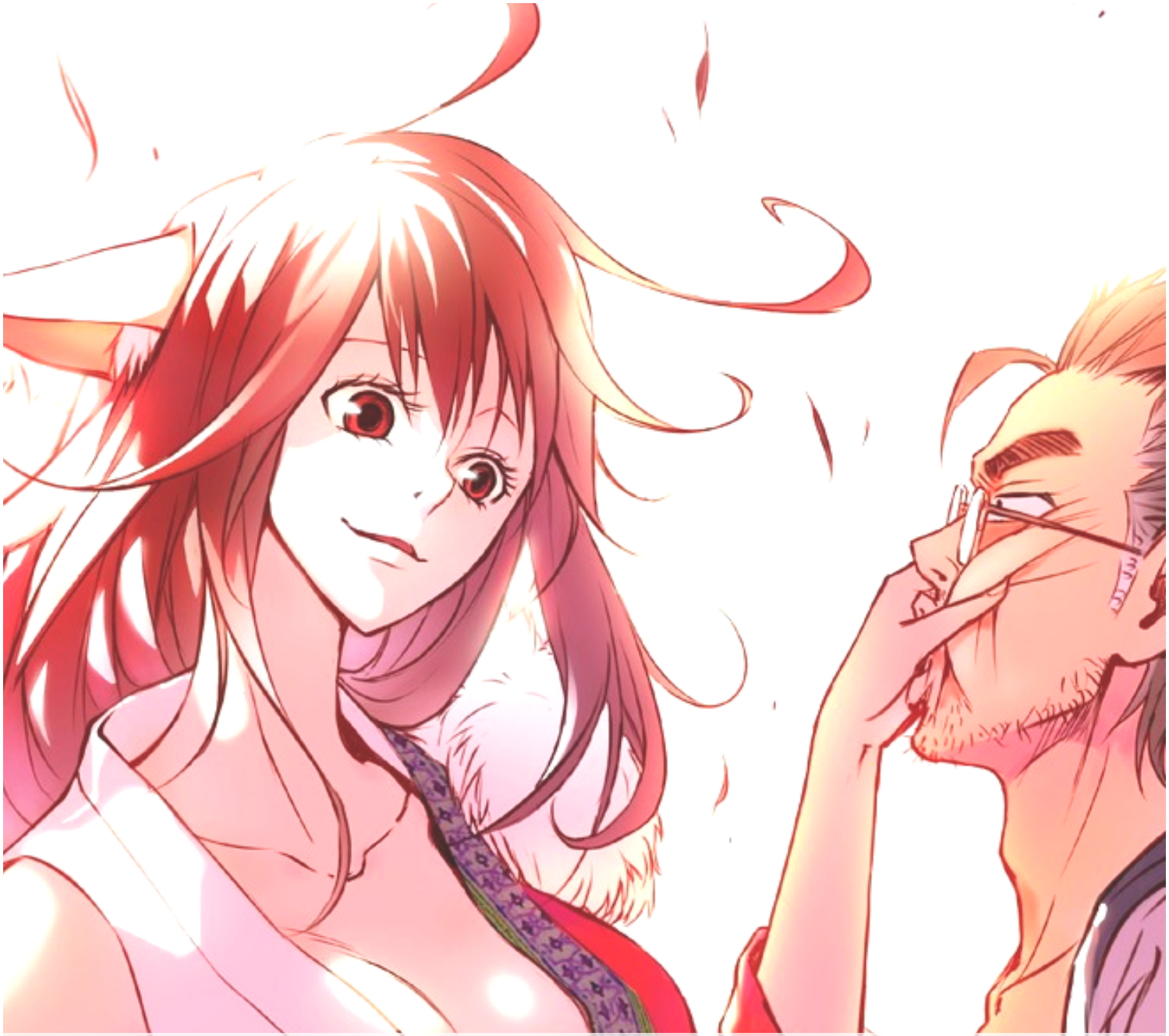

Frida 简介（安装）

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（安装）

Installation

Frida 从安装到配置只需要几分钟，如果你曾经遇到过比较蛋疼的问题，请提交 Issues（或 Pull request），描述一下你遇到的问题，然后我们讨论一下如何让这个过程变得更容易 。

Requirements for Python bindings

安装 Frida 非常简单和直接，但是安装之前你需要确保你的系统有以下环境：

- Python - 强烈推荐最新的 3.x
- Windows，Mac OS X 或 Linux

Install with pip

安装 Frida 的 Python bindings 的最好方法是通过 PyPI。在终端提示符下，只需运行以下命令来安装 Frida：

```
$ sudo pip install frida
```

所有 Frida 的 PyPI 依赖都是通过上面的命令自动安装的，所以你不必担心它们。 如果您在安装 Frida 时遇到问题，请查看故障排除页面或 report an issue，以便 Frida 社区可以改善每个人的体验。

Install manually

你也可以从这里获取预发布的二进制文件。

Testing your installation

启动一个可注入的程序：

```
$ cat
```

只需坐等输入。在 Windows 上，你可以使用 notepad.exe。

请注意，此示例将不适用于 Mac OS X El Capitan，因为它拒绝对系统二进制文件的访问 。详情请参阅这里。然而，如果你复制 cat 二进制到/tmp/cat 运行，此示例反而可以适用：

```
$ cp /bin/cat /tmp/cat
$ /tmp/cat
```

在另一个终端中，创建一个文件 example.py，其中包含以下内容：

```
import frida

session = frida.attach("cat")

print([x.name for x in session.enumerate_modules()])
```

如果您使用的是 Linux，请执行以下操作来调试非子进程（从 ubuntu10.10 开始，除非进程 B 是进程 A 的子进程，或者进程 A 为 root 运行，否则进程 A 不能调试进程 B）：

```
$ sudo sysctl kernel.yama.ptrace_scope=0
```

这时该拉 Frida 出来遛遛啦！我们运行 example.py 脚本看看它的魔力：

```
$ python example.py
```

输出应类似于此（取决于您的平台和库版本）：

```
[u'cat', …, u'ld-2.15.so']
```