Burp 插件分享：图形化版的重算 sign 和参数加解密插件

作者：bit4@Mottoin Team

0x00 前言

之前在 freebuf 分享过自己学习 burp 插件开发的一些小收获：

BurpSuite 插件开发 Tips：请求响应参数的 AES 加解密

后来断断续续尝试写了图形化的版本，也对纯代码版本进行了改进，现做简单描述分享给大家，链接在末尾。

0x01 工具介绍

- 适用场景：

  有些 App 产生的请求有对参数进行加密处理或者添加 sign 字段，导致不能直接*判断参数内容和修改参数值*。

  在知道具体算法的前提下，该插件可以实现请求参数的自动加解密操作（Para Encrypter）、在修改参数后自动重新计算 sign（Resign）。

- 前提条件：

  需要知道具体的签名或者加解密算法。这可能需要逆向或者其他手段去获取。

- 插件特性：

  1.可以控制插件生效的组件，包括 proxy、scanner、intruder、repeater。

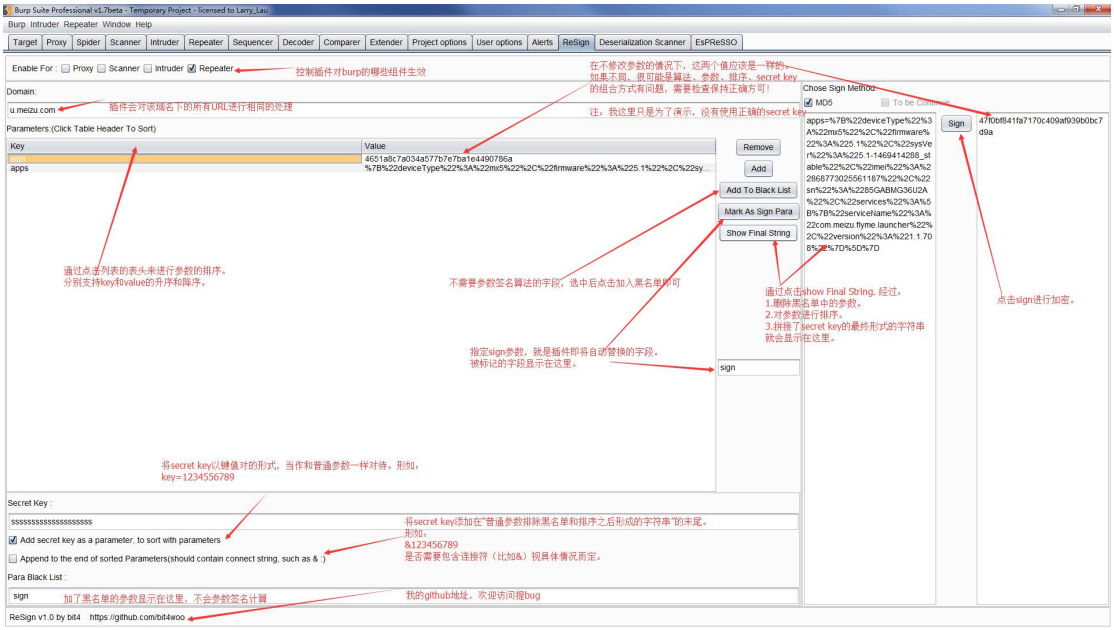
  2.可以控制插件生效的域名和参数。

  3.目前 Resign 支持 md5 的 sign 算法，Para Encrypter 支持 AES、Base64。

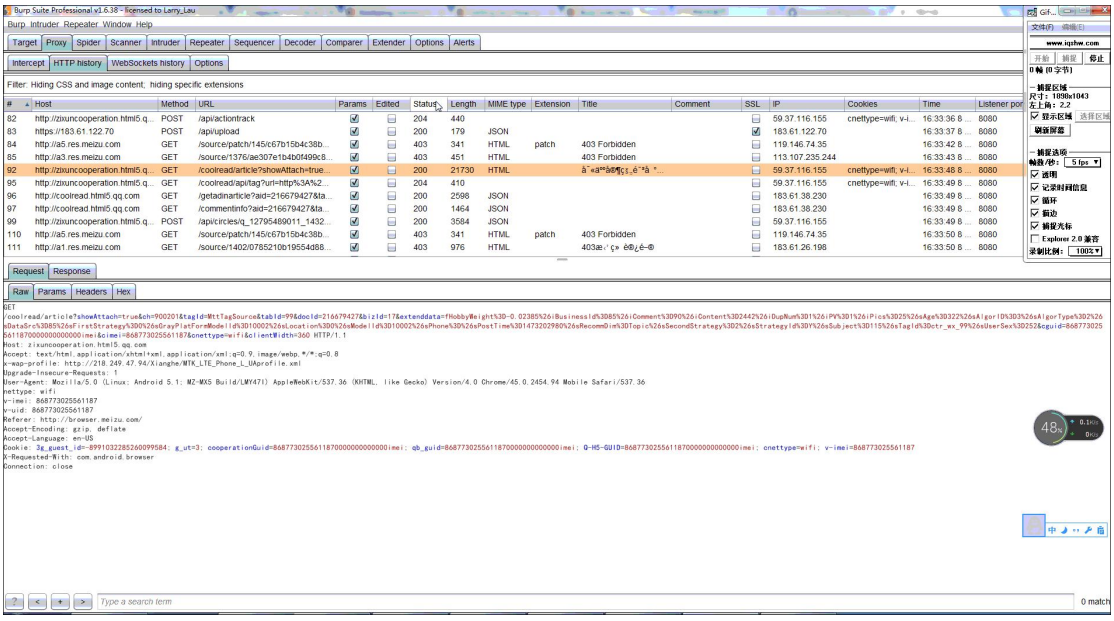
  4.支持右键"发送到"插件的功能。

0x02 界面和使用

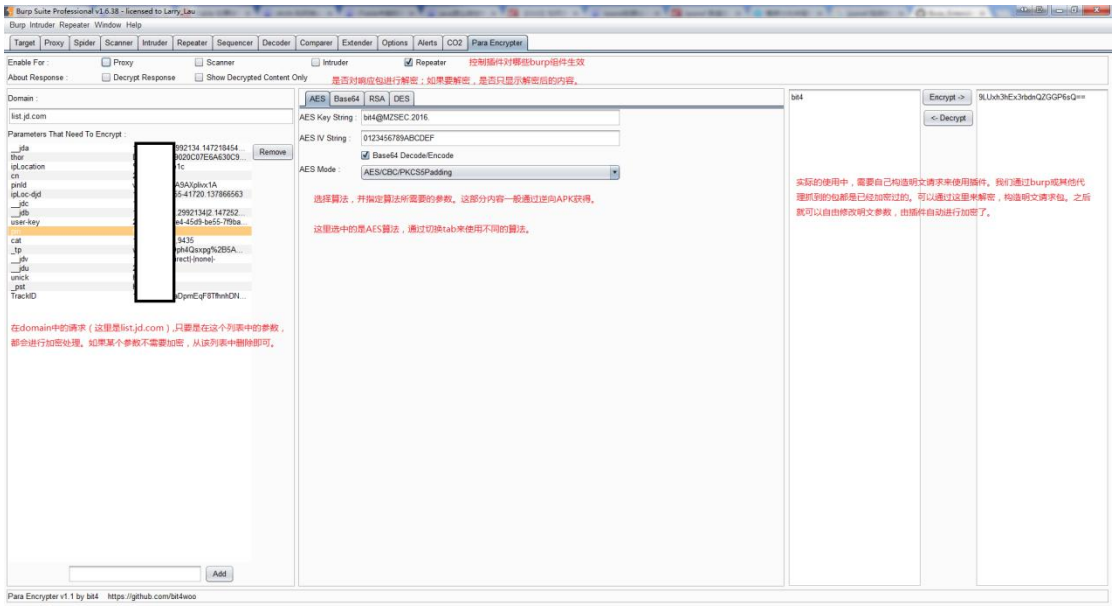
- Resign 界面展示及说明



- Resign 使用演示



- Para Encrypter 界面展示及说明



- Para Encrypter 使用演示

  和 resign 插件类似，不再重复

- 和 SQLMAP 的配合

  sqlmap.py -u "http://www.test.com/a.php?id=1" --proxy=http://127.0.0.1:8080 --skip-urlencode

  通过以上方法，sqlmap 的请求也可以通过 burp 进行进行处理，好基友有通过此方法成功找到过 SQL 注入。--proxy 参数就是 burp 的代理地址；--skip-urlencode 是为了保证在 burp 对参数进行处理前参数还是原始明文，没有经过 URL 编码。

0x03 纯代码版本

其实我个人是更倾向使用这个版本的，它的灵活性是图像版本没有办法比的，可以自由修改代码然后从新打包使用。

熟悉 Java 的朋友建议使用该版本，进行自己的修改和调整。源码中都有较为详细的注释，欢迎 fork 阅读。

0x04 源码和下载

在 github 上分享相应的源码：

Resign 图形版
Para Encrypter 图形版
纯代码版（包括 Resign 和 Para Encrypter）

使用中如有问题，欢迎在 github 上给我提 issue。