burpsuite 插件之 Java Deserialization Scanner 使用方法

by:裁决

Java Deserialization Scanner 介绍

用于检测和利用 Java 反序列化漏洞的插件

项目地址: https://github.com/federicodotta/Java-Deserialization-Scanner

下载地址: https://github.com/federicodotta/Java-Deserialization-Scanner/releases

Ysoserial 介绍

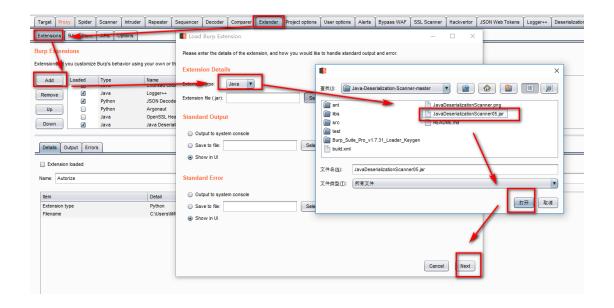
用于生成利用不安全 Java 对象反序列化的有效负载的概念验证工具

项目地址: https://github.com/frohoff/ysoserial

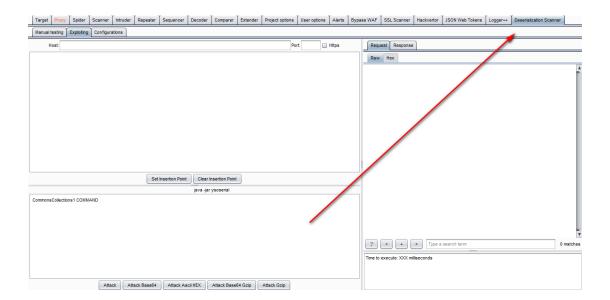
下载地址:

https://jitpack.io/com/github/frohoff/ysoserial/master-SNAPSHOT/ysoserial-master-SNAPSHOT/ysoser-Master-Master-Master-Master-Master-Master-Master-Master-Master-Master-Master-Master-Master-Master-Master-Master-Master-Master-M

Java Deserialization Scanner 安装



安装成功如下图

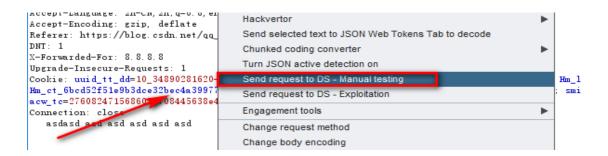


Yaoserial 安装

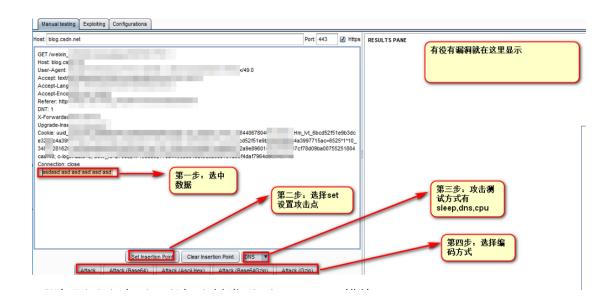


Java Deserialization Scanner 使用方法

1. 鼠标邮件发送要测试的反序列化数据到 Manual testing



2.选择测试方式,进行测试



3.假如测试出来了,鼠标右键发送到 exploiting 模块

| Connection: close asdasd asd asd asd asd | 044J0J0643D13CJ2660461U6014 | מו זיטטו עטטטאיטט זומט זומ |
|--|-----------------------------|----------------------------|
| | Send to Repeater | |
| | Send to Exploitation tab | |
| | | |

4.在 Exploitation tab 在确认下,下面那个输入框下 输入 ysoserial 的参数,假如检测出了 Apache Commons Collections 3,所以使用 CommonsCollections 3 COMMAD

| Connection: close asdasd asd asd asd asd | | |
|---|---|--|
| | Set Insertion Point Clear Insertion Point | |
| java -jar ysoserial | | |
| CommonsCollections1 calc | | |
| Attack | Attack Base64 | |

总结



关于插件还有很多功能性的介绍,同样我也懒得从 GitHub 上复制了,大家自己去看吧,我是可爱的老裁决,哈哈.gif

参考链接: https://www.cnblogs.com/yh-ma/p/10299289.html