裁决 / 2019-09-10 08:53:56 / 浏览数 3755 安全工具 工具 顶(1) 踩(0)

# burpsuite插件之AutoRepeater

# 0x01 AutoRepeater介绍

Burp Suite是一个拦截HTTP代理,它是执行Web应用程序安全测试的事实工具。虽然Burp

Suite是一个非常有用的工具,但使用它来执行授权测试通常是一项涉及"更改请求和重新发送"循环的繁琐工作,这可能会漏掉漏洞并减慢测试速度。AutoRepeater是一个开 Suite扩展,旨在减轻这种努力。AutoRepeater可自动化和简化Web应用程序授权测试,并为安全研究人员提供易于使用的工具,可在Burp Suite中自动复制,修改和重新发送请求,同时快速评估响应的差异。

AutoRepeater仅重新发送由定义的替换更改的请求。当AutoRepeater收到与给定选项卡设置的条件匹配的请求时, AutoRepeater将首先将每个已定义的基本替换应用于请

项目地址: https://github.com/nccgroup/AutoRepeater

下载地址: https://github.com/nccgroup/AutoRepeater/blob/master/AutoRepeater.jar

### 0x02 AutoRepeater特点

没有AutoRepeater,基本的Burp Suite Web应用程序测试流程如下:

- 1. 用户面对Web应用程序,直到找到有趣的请求
- 2. 用户将请求发送到Burp Suite的"Repeater"工具
- 3. 用户在"Repeater"中修改请求并将其重新发送到服务器
- 4. 重复步骤3,直到找到甜蜜漏洞
- 5. 从第1步开始,直到用户用完测试时间或者可以退出bug赏金收入

虽然此测试流程有效,但测试任何请求中可能存在的问题尤为繁琐。例如,更改电子邮件地址,帐户身份,角色,URL和CSRF令牌都可能导致漏洞。目前,Burp Suite不会在Web应用程序中快速测试这些类型的漏洞。

#### 现有一些Burp

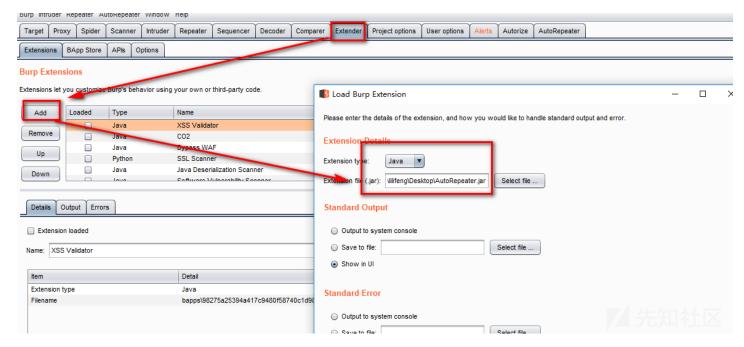
Suite插件(AuthMatrix,Authz和Autorize)可以使授权测试更容易,但每个插件都有限制其实用性的问题。AuthMatrix和Authz要求用户向插件发送特定请求,并设置授 Suite熟悉的用户界面,并将它们组合在一起以创建最简化的授权测试插件。

AutoRepeater提供了一种通用解决方案,用于简化Web应用程序中的授权测试。AutoRepeater提供以下功能:

- 自动复制,修改和重新发送任何请求
- 有条件的替代品
- 快速标题, Cookie和参数值替换
- 拆分请求/响应查看器
- 原始与修改的请求/响应差异查看器
- 基本替换中断CSRF令牌和会话cookie等请求的值
- Renamable标签
- 记录
- 出口
- 切换激活
- 从其他Burp Suite工具"发送到AutoRepeater"

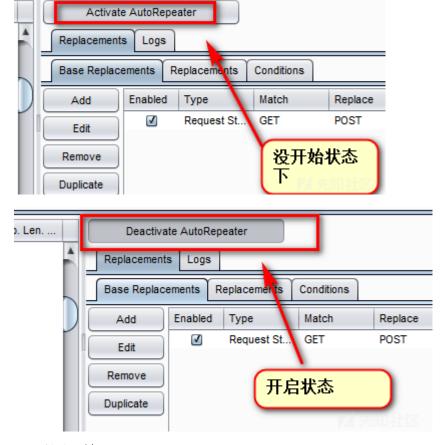
# 0x03 AutoRepeater安装方法

下载插件,在extender模块添加【商店里面也可以,但是慢而且你也需要确定是最新的】



# 0x04 AutoRepeater使用注意事项

1. 没开始的时候,不要开启



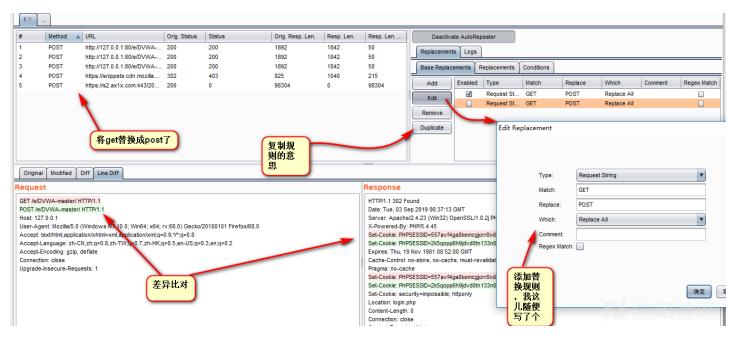
2. cookie jar别点

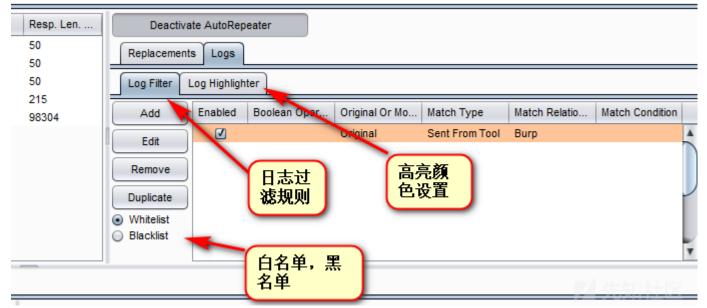


3. 重启之后,数据会丢失,规则配置还在

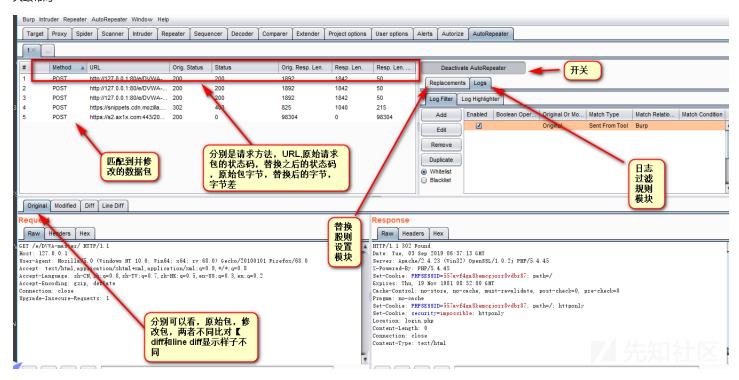
# 0x05 AutoRepeater使用方法

流程:先点开关,在replacements添加替换规则,之后logs一般默认即可,接下来将数据包发送到AutoRepeater就可以分析了,我这里面为了直观,替换规则是"将GET换 replacements





#### 大致布局

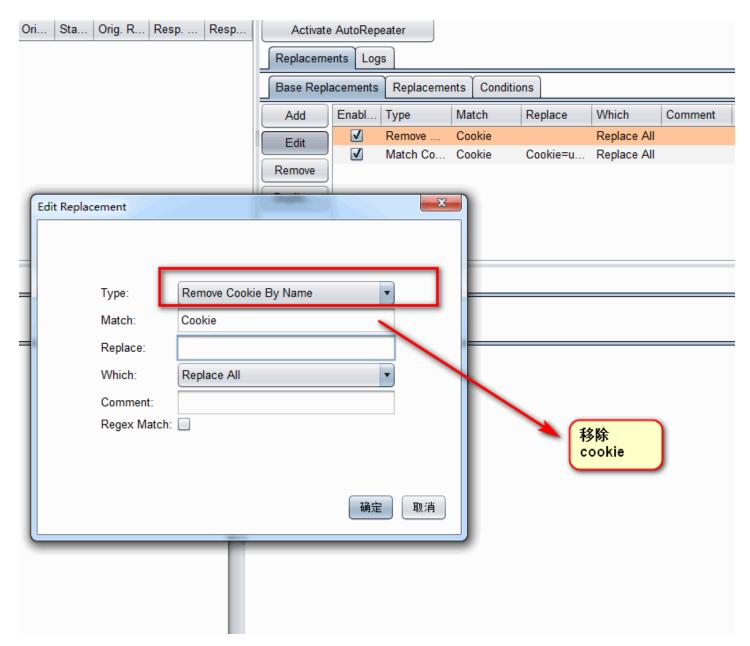


.....忘了标记顺序了,就这样吧

## 0x06 AutoRepeater替换规则举例

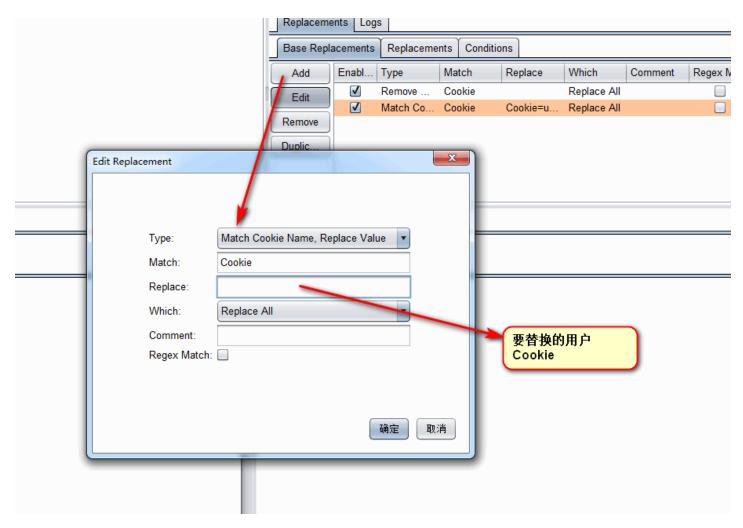
测试未经身份验证的用户访问

要测试未经身份验证的用户是否可以访问该应用程序(删除cookie],需要选择Remove Header By Name之后; Match选择Cookie



测试经过身份验证的用户访问【越权之类】

要测试越权之类【替换cookie值】的,需要在Base Replacements下为cookie配置一个规则, Match Cookie Name, Replace Value匹配cookie名称,替换为权限较低的用户的cookie值



0x07 总结

用了一下感觉还行,发现没有国内没说明就顺手写了个文档,大佬别喷

0x08 参考

AutoRepeater项目主页

AutoRepeater: Automated HTTP Request Repeating With Burp Suite

点击收藏 | 1 关注 | 1

上一篇: Asset Enumeration... 下一篇: windows样本分析之基础静态分析-三

1. 6 条回复



child 2019-09-10 22:10:24

比logger++多了好几个功能 ,感谢分享

0 回复Ta



<u>3\*\*\*\*</u> 2019-09-12 08:34:25

可以,支持

0 回复Ta



裁决 2019-09-12 20:26:53

@child 谢谢老哥,可以去https://github.com/lilifengcode/Burpsuite-Plugins-Usage看下是否还有其他有用的插件

0 回复Ta



裁决 2019-09-12 20:28:08

<u>@3\*\*\*\*</u> Thanks

0 回复Ta



drunkard > 2019-10-22 11:08:31

可以可以 感谢表哥输出

0 回复Ta



Eureka 2019-11-17 19:33:45

大佬,请问操作send to autorepeater时不成功,autorepeater下不显示任何请求怎么回事呀?

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS <u>关于社区</u> <u>友情链接</u> <u>社区小黑板</u>