如何编写burpsuite联动sqlmap的插件

山东安云 F 2016-03-28 共421117人围观 ，发现 33 个不明物体

工具

0×00 引言

burpsuite和sqlmap是渗透测试中最常用到的两大神器。最中意的功能是利用burpsuite拦截http请求，然后用sqlmap的r参数读取。但每次重复这个动作有点烦，特别是Mac下默认不能右击新建文件。所以一直在找联动burpsuite和sqlmap的插件。在找到的方案中，gason已经很久没更新了；freebuf发的这个插件很不错，但是不适配Mac；比较好的是bapp中的co2，但是调用的不是sqlmap的r参数，而是u参数，无法实现对http请求的全部利用。趁着有时间，自己用Python开发了一个

环境

> 操作系统: Mac OS X 10.11.4
>
> Python解释器: Jython 2.7
>
> Burpsuite: 1.6.38
>
> sqlmap: 1.0.3.4(已经添加到环境变量中)

0×01 开发

新的插件希望能够满足三个要求:

1.能通过burpsuite最简单的调用sqlmap

2.能够用sqlmap r参数读取请求文件

3.能够重复的利用sqlmap请求，比如校验漏洞后继续获取请求的数据，表，列，内容等

基于以上三个需求大致梳理了一下流程

1.在的Proxy页面右键触发插件

2.burpsuite将拦截的http请求全部保存到一个文件中

3.弹出mac的终端调用sqlmap -r $fileName

然后是源代码

```
#必须导入的库
from burp import IBurpExtender
from burp import IContextMenuFactory
from burp import IBurpExtenderCallbacks
from burp import IHttpRequestResponse
from burp import IHttpListener
from burp import IProxyListener


#导入java库
from javax.swing import JMenuItem


#Python原生模块
import os
import subprocess
import time
import re
```

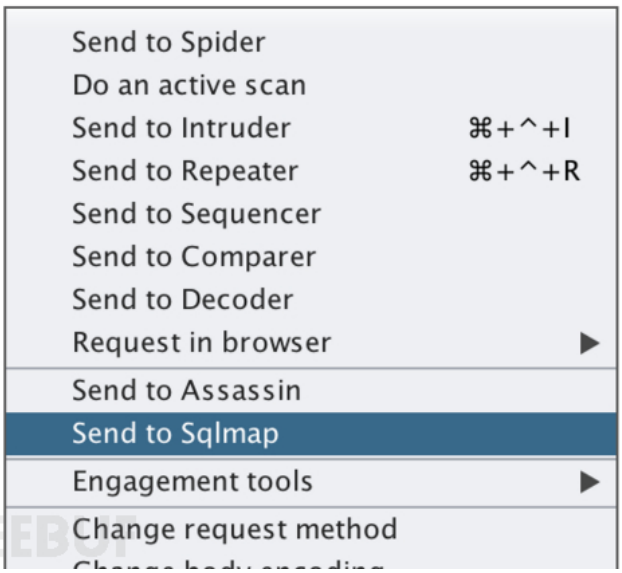
其中IBurpExtender是编写插件必须导入的接口，IContextMenuFactory是用来控制右键菜单的，IHttpRequestResponse，IHttpListener，IProxyListener用来控制http请求流量

```
class BurpExtender(IBurpExtender, IHttpListener, IContextMenuFactory, IProxyListener, IHttpRequestResponse, IBurpExtenderCallbacks):
    #必须引用的主函数,完成初始化设置
    def registerExtenderCallbacks(self, callbacks):
        #右键触发扫描
        self._actionName = "Send to Sqlmap"
        self._helers = callbacks.getHelpers()
        self._callbacks = callbacks
        #插件名字
        callbacks.setExtensionName("Burp2sqlmap")

        callbacks.registerHttpListener(self)
        callbacks.registerContextMenuFactory(self)
        callbacks.registerProxyListener(self)

        return
```

然后是初始化设置，定义右键Menu的字段以及插件的名字

```
#创建菜单右键
def createMenuItems(self, invocation):
    menu = []
    responses = invocation.getSelectedMessages()
    if len(responses) == 1:
        menu.append(JMenuItem(self._actionName, None, actionPerformed=lambda x, inv=invocation: self.sqlmapShell(inv)))
        return menu
    return None
```

直接摘抄前辈的，定义右键菜单以实现右键触发。如图



```
#主函数
def sqlmapShell(self, invocation):

    invMessage=invocation.getSelectedMessages()
    request = invMessage[0].getRequest().tostring()

    hostDomain=re.findall(r"Host: (.+?)\r\n", request)[0].replace('.', '_').replace(':', '_')

    dirList = os.listdir(os.getcwd())

    if hostDomain not in dirList:
        os.mkdir(hostDomain)
        os.chdir(hostDomain)
    else:
        os.chdir(hostDomain)

    #定制时间戳,以下划线分割分别是月份_日分_小时_分钟_秒
    timeName=time.strftime("%m_%d_%H_%M_%S", time.localtime())

    fullName = hostDomain + "_" + timeName + ".txt"
    fileObj = open(fullName, "w")
    fileObj.write(request)
    fileObj.close()

    os.chdir(httpPath)
```

主函数，获取http的请求流量并写到一个文件中

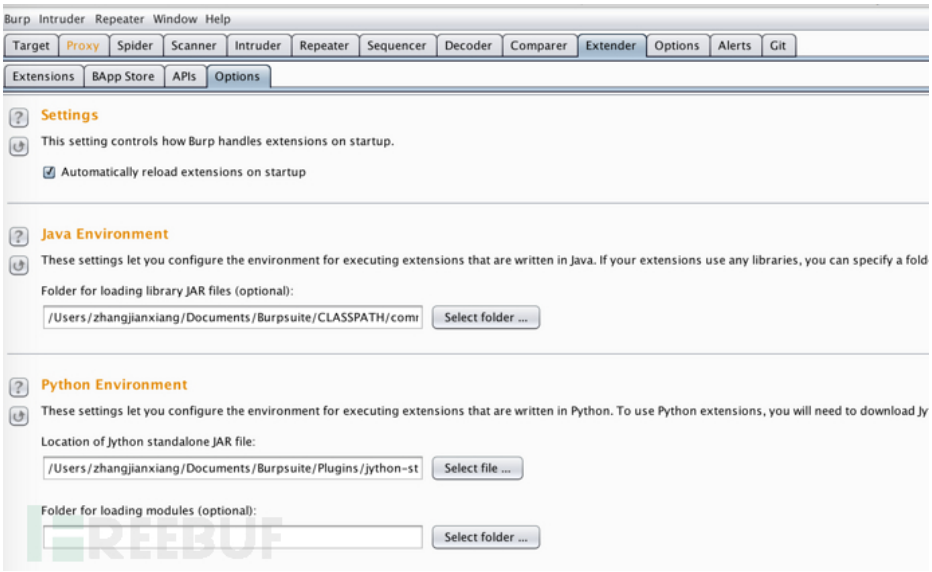
```
#cmdBase="tell application \"Terminal\" \n\tactivate\n\tdo script \" " + pythonPath + " " + sqlmapPath + "  " + "-r " + full
cmdBase="tell application \"Terminal\" \n\tactivate\n\tdo script \" sqlmap -r " + fullPathName + " --batch --threads 3 --tam

proc = subprocess.Popen(['osascript', '-'], stdin=subprocess.PIPE, stdout=subprocess.PIPE)
stdout_output = proc.communicate(cmdBase)
```

调用Mac的终端执行sqlmap。python没有直接调用Mac App的方法，通过Python调用Applescript打开终端

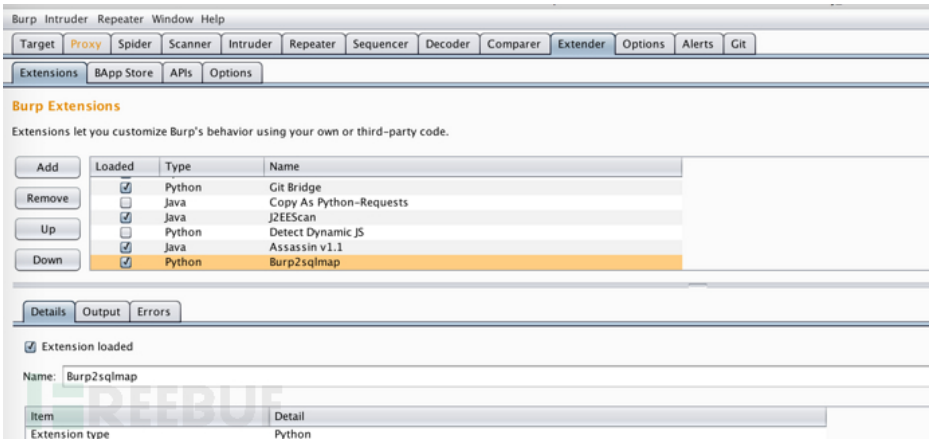
完整的源代码在:https://github.com/5ir1us/Burpsuite4Extender

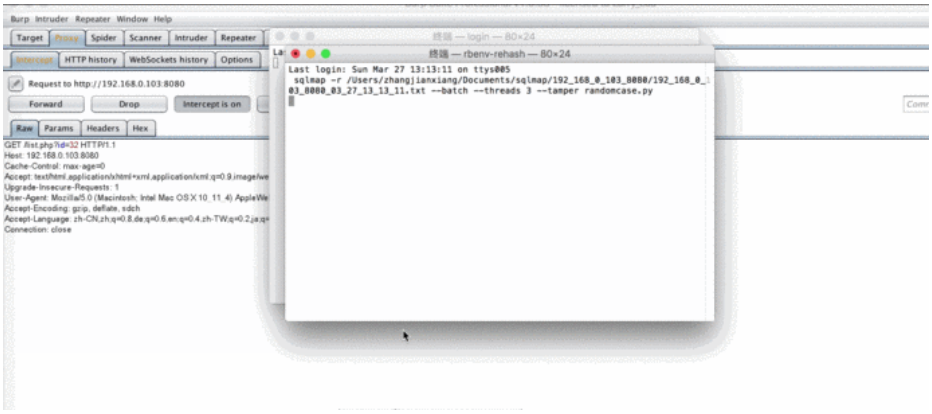
0×02 安装

首先下载[Jython 2.7.0 – Standalone Jar](#)文件，然后在Burpsuite的Extender页面导入该解释器，如图



然后即可导入该插件





0×03 参考

http://drops.wooyun.org/papers/3962

http://blog.stalkr.net/2015/04/creating-burp-extensions-in-python.html

http://blog.nsfocus.net/burpsuite-plugin-development-rsa-encryption-decryption/

http://www.moonsos.com/Article/penetration/107.html

http://www.secpulse.com/archives/44241.html

https://portswigger.net/burp/extender/

http://xlixli.net/?p=431