Web安全 -- BurpSuite插件实战

小峰 / 2018-01-03 18:19:56 / 浏览数 4779 新手 入门资料 顶(0) 踩(0)

简述

今天主要介绍些常用Brup插件，以及某些插件如何在burp上安装、使用。文章早就出来了，年底工作比较忙，一直就没有给大家更新。新年第一篇，视频周末给大家放出。

1.1详细介绍

1.1.4 extender功能：

可通过商店添加某些插件，同样也可以添加自己或第三方的插件。

可添加java、Python、ruby类型的插件，若安装失败会提示异常情况。

同样burp提供了api接口，可创建自定义插件。

1.2实战篇

1.2.1 sqlipy使用

由于sqlmap是Python语言编写的，而burp是java编写的所以需要先下载jython-standalone-2.7.0.jar文件，然后进行使用。下载地址：http://www.jython.org/downloac

在options下加载jar包。

到burp的应用商店下载sqlipy并安装。

安装成功，会显示状态，如果安装失败会在error菜单提示出错信息。

安装好后会显示该插件，由于在使用过程中会用到很多插件，但在开启burp时会加载所以插件，建议将插件关闭，下次使用时在开启。

下面介绍如何使用burp+sqlmap发现sql注入漏洞

首先需要先设置sqlmapapi监听端口，执行sqlmapapi.py –s可以看到该服务的端口。

在插件中监听该端口，也就是8775。

下面使用burp抓取数据包，并右键发送到sqlipy。

可以看到将url,cookie,user-agent参数填写到了对应功能处。

同样，他默认设置了对数据包的扫描情况，也可以自定义需要扫描。

在sqlmap logs下可查看扫描的情况。

在target栏可以看到对参数的测试payload数据。

同样，当想停止对某个请求进行扫描时，可在sqlmap scan stop模块暂停扫描。

1.2.2 co2使用

由于sqlmap是Python语言编写的，而burp是java编写的所以需要先下载jython-standalone-2.7.0.jar文件，然后进行使用 。
下载地址：http://www.jython.org/downloads.html

在options下加载jar包。

C02工具调用sqlmap，初学者可使用该工具进行SQL注入。

发送到sqlmapper功能。

 可以选扫描的级别，扫描请求头，post参数。

 选择要扫描方式。

 调用sqlmap进行扫描。

1.2.3 xssValidator使用

 首先，下载安装xssValidator插件，也可通过https://github.com/nVisium/xssValidator

安装成功后，可以看到需要执行phantomjs xss.js

Phantomjs下载：http://phantomjs.org/download.html

PhantomJS是一个基于webkit的JavaScript
API。它使用QtWebKit作为它核心浏览器的功能，使用webkit来编译解释执行JavaScript代码。任何你可以在基于webkit浏览器做的事情，它都能做到。它不仅是个隐
Web 测试、页面访问自动化等。

在插件安装目录的xss-detector子目录下有一个xss.js的文件，使用phantomjs运行该文件，进行监听。

 执行phantomjs xss.js进行检讨8093端口，当执行扫描xss时，会在cmd下显示扫描状态。

 使用burp抓取数据包，并选择要进行测试的参数。

 首先设置payload类型：

 选择Extension-generated为xssvalidator插件。

 标注xss漏洞成功的状态。

 设置payload processingp。

 设置匹配字符。

 显示xss注入状态。

 排序xss_result可以看到排序成功。

1.2.4 bypass waf使用

 首先简单看下bypass waf有哪些功能

 1、用户可以修改在每个请求中发送的X-Originating-IP，X-Forwarded-For，X-Remote-IP，X-Remote-Addr头，
将WAF配置为信任自己（127.0.0.1）来绕过目标。

 2、“Content-Type”通过修改该选项来查看是否对该类型进行验证。

 3、也可以修改”主机”标题。 配置不当的WAF可能配置为仅根据此标头中找到的主机的正确FQDN来评估请求，这是此绕过目标。

 4、请求类型选项允许Burp用户仅对”GET”或”POST”的给定请求方法使用剩余的旁路技术，或将其应用于所有请求。

5、路径注入功能可以不修改请求，注入随机路径信息信息（/path/to/example.php/randomvalue?restofquery），或注入随机路径参数（/path/to/example.php;rando
这可以用于绕过依赖于路径信息的编写不良的规则。

 6、路径混淆功能将路径中的最后一个正斜杠修改为随机值，或者默认情况下不做任何操作。
最后一个斜杠可以修改为许多值中的一个，在许多情况下导致仍然有效的请求，但是可以绕过依赖于路径信息的写得不好的WAF规则。

 7、参数混淆特征是语言特定的。
PHP将在每个参数的开始处丢弃一个+，但是可能会为特定的参数名称写入写得不好的WAF规则，因此在开头忽略带有+的参数。
类似地，ASP在每个参数的开始处丢弃一个%。

在应用商店中安装bypass插件

 设置该插件规则。

 设置对哪些菜单可进行bypass。

1.2.5 logger++使用

 Burpsuite自带的日志只记录了HTTP
Proxy的请求，无法查看Repeater、Intruder等模块的历史记录，Logger++增加了这方面的功能，可以方便的筛选查看各模块历史记录。

 在view logs功能处可看到历史记录。

 可通过关键次进行搜索某些特定的请求。

 右击查看某个请求，可在view logs下查看该请求。

点击收藏 | 0 关注 | 0

上一篇：BLE-GATT浅析 下一篇：内存动态执行DLL的介绍与应用

1. 0 条回复
   - 动动手指，沙发就是你的了！