burpsuite 之 Scanner

1、简介

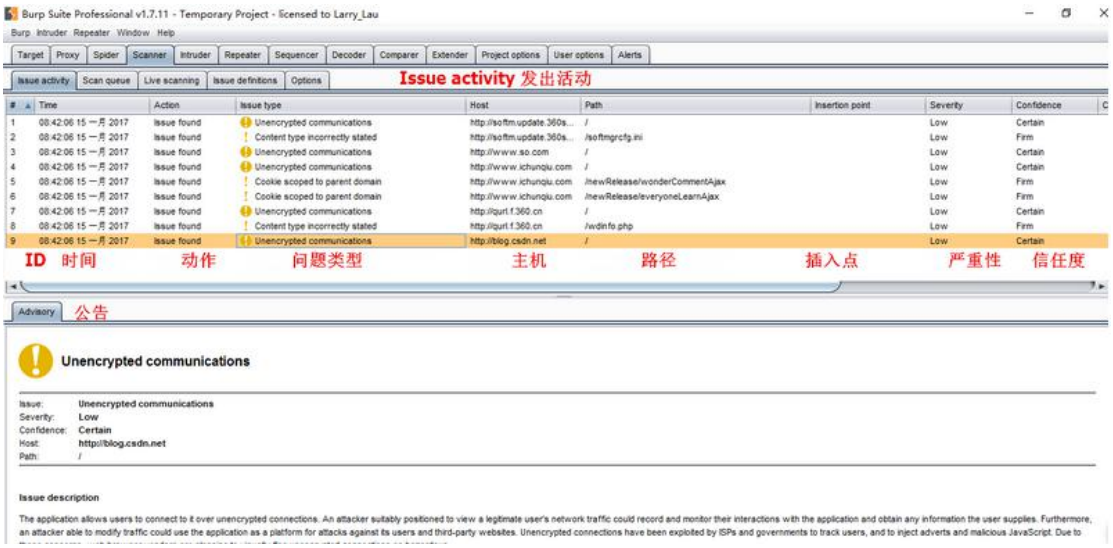
Burp Scanner 是一个进行自动发现 web 应用程序的安全漏洞的工具。它是为渗透测试人员设计的，并且它和你现有的手动执行进行的 web 应用程序半自动渗透测试的技术方法很相似。

使用的大多数的 web 扫描器都是单独运行的：你提供了一个开始 URL，单击||go||,然后注视着进度条的更新直到扫描结束，最后产生一个报告。Burp Scanner 和这完全不同，在攻击一个应用程序时它和你执行的操作紧紧的结合在一起。让你细微控制着每一个扫描的请求，并直接反馈回结果。

Burp Scanner 可以执行两种扫描类型：主动扫描(Active scanning)，被动扫描(Passive scanning)。

2、模块说明

2.1：Issue activity



2.2：Scan queue　　扫描队列，这里将显示扫描队列的状态 进度 结果等。

主要包含以下内容：

1. 索引号的项目，反映该项目的添加顺序。

2. 目的地协议，主机和 URL 。

3. 该项目的当前状态，包括完成百分比。

4. 项目扫描问题的数量（这是根据所附的最严重问题的重要性和彩色化） 。

5. 在扫描项目的请求数量进行。

6. 网络错误的数目遇到的问题。

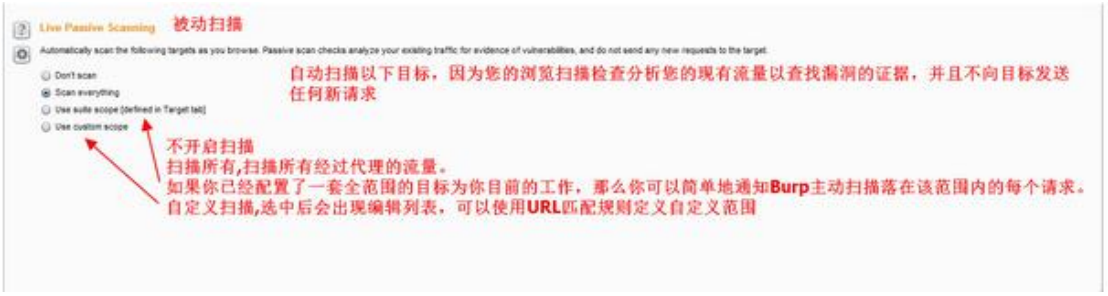
7. 为项目创建的插入点的数量。

2.3：Live scanning

实时扫描可让您决定哪些内容通过使用浏览器的目标应用，通过 BurpProxy 服务器进行扫描。您可以实时主动扫描设定 live active scanning(积极扫描)和 live passive（被动扫描）两种扫描模式。

Live Active Scanning：积极扫描。当浏览时自动发送漏洞利用代码。

Live Passive Scanning：被动扫描。只分析流量不发送任何请求。



2.4：Issue Definitions

漏洞列表，列出了 burp 可以扫描到的漏洞详情

3：Options

包含 Burp 扫描选项进行攻击的插入点，主动扫描引擎，主动扫描优化，主动扫描区和被动扫描区域。

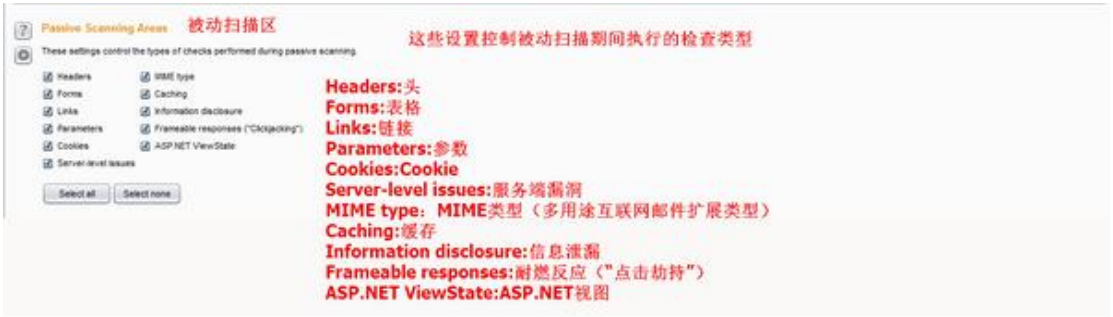
3.1：Attack Insertion Points

3.2：Active Scanning Engine

3.3：Active Scanning Optimization

3.4：Active Scanning Areas

3.5：Passive Scanning Areas



3.6：Static Code Analysis