Burpsuite自带小功能分享

5ecu**** / 2018-03-01 13:46:42 / 浏览数 3511 安全工具 工具 顶(0) 踩(0)

1.1.简要描述

Burpsuite作为web测试中的利器大家都知道，除了其核心的功能外还有部分小功能也是非常的不错，和大家分享一下。（小功能如使用错误,敬请指出,不胜感激。）下面以1

1.2.Infiltrator

这个功能可能大家不怎么使用不熟悉，我在官网中找到了相关的一些介绍。（注意请勿在生产环境中进行测试！）
Infiltrator让Burp 能够检测输入到服务器端可能存在问题的api，既last (交互式应用程序安全测试)。
从Burp菜单中选择 Burp Infiltrator 选项，选择应用程序类型后保存，在安装和运行Infiltrator之前不要运行应用程序。
将Infiltrator安装程序复制到应用程序的根文件夹中进行赋权并执行，执行交互完成后正常启动应用程序，最终在扫描过程中会触发一些安全报告。

1.3.Clickbandit

Clickjacking中文即为点击劫持，攻击者使用多个透明或不透明的图层来欺骗用户在不知情中点击另一页面上的按钮或链接。Clickbandit可以迅速的生成相关poc以验证是否
在打开的对话框上,单击"copy clickbandit to
clipboard"按钮。复制此代码到控制台中（火狐为例），相关poc即覆盖在浏览器窗口的顶部,原始页面将在一个框架内重新加载(如果你不想在录制过程中菜单进行跳转,单选
click actions")。再简单地执行你希望受害者执行的点击顺序后进行保存到本地，点击即可看到是否存在此漏洞。

1.4.Collaborator

Collaborator是1.6.15版本添加的新功能，用于检测部分无法直接回显的漏洞。相关描述大家可以在百度中找到。
找到Project Options >Misc> Burp collaborator
Server中进行配置，第一项是默认的burp给你分配的地址，第二选项是不使用这个功能，第三个是使用一个私有的collaborator服务。
默认配置后scanner功能会在扫描的过程中随机的插入一些子域名，我们选定一个把他固定下来。打开Burp > Burp collaborator client ，选择copy to
clipboard可以看到burp分配的子域名，单选私有服务器后填入进行通信的检查。在能访问互联网的情况下都会提示都成功。

接下去正常扫描即可，所探测到的漏洞都进行报告：

但部分测试是需要在不联网的情况下进行的，下面我们执行相关命令把collaborator进行本地化:
java -jar burpsuite_pro_v1.7.31.jar --collaborator-server
单选私有服务器后填入ip地址，这边有个问题是通信测试后dns和https是无法使用的，但不影响http的使用。

欢迎各位大佬来公众号"5ecurity"拍砖 ^_^

点击收藏 | 1 关注 | 2

上一篇：wmi与vbs 下一篇：Jmeter_RMI漏洞复现—【C...

1. 1 条回复

finger 2018-06-18 09:14:24

应该直接上二维码的

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 关于社区 友情链接 社区小黑板