AssassinGo: 基于Go的高并发可拓展式Web渗透框架

Amyang / 2018-05-29 22:37:44 / 浏览数 5430 安全工具 工具 顶(1) 踩(0)

AssassinGo是一款使用Golang开发，集成了高可用信息收集、基础攻击向量探测、Google-Hacking综合搜索和PoC自定义添加并对目标进行批量检测等功能的自动化Web

项目网址： https://assassin-go.ink

Github： https://github.com/AmyangXYZ/AssassinGo

Assassin Go

功能

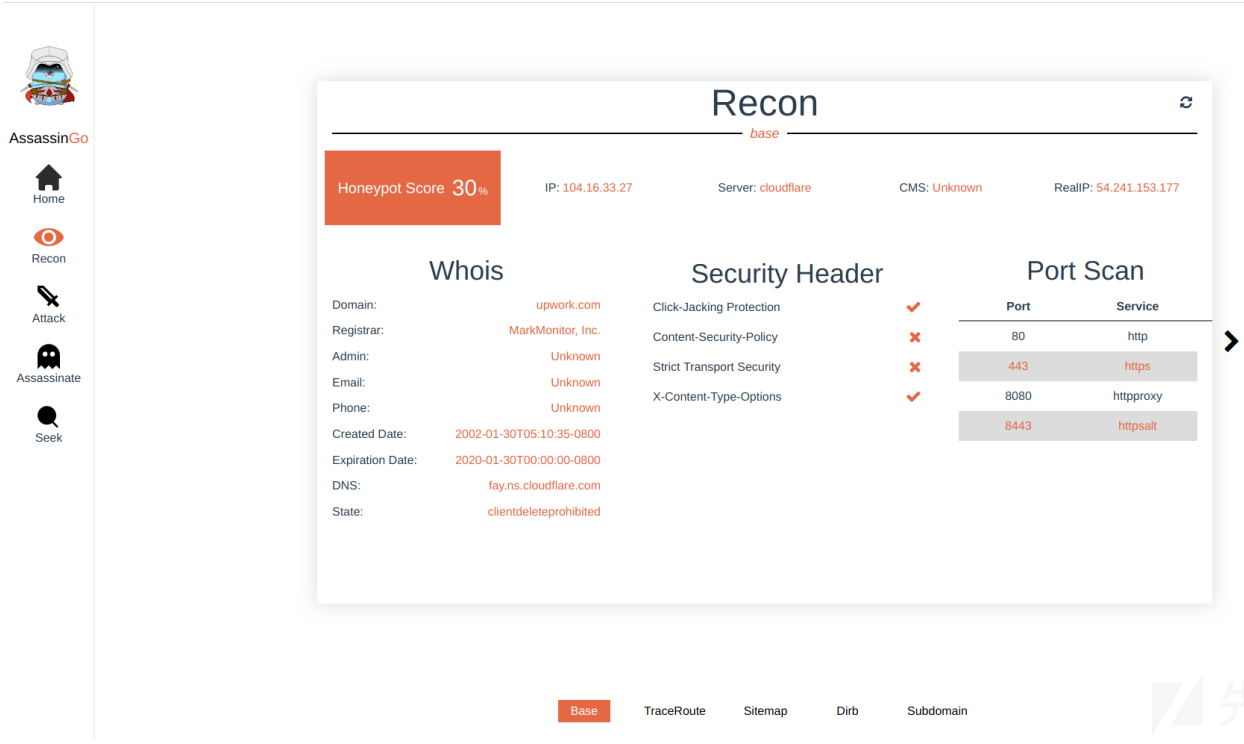
信息收集部分

- HTTP安全头部检查
- 服务器识别
- CMS版本识别
- 蜜罐概率检测
- CloudFlare绕过并检测Real IP
- 路由节点跟踪并在googlemap上做可视化标记
- 端口扫描
- 目录爆破和可视化的sitemap
- Whois信息
- 子域名扫描

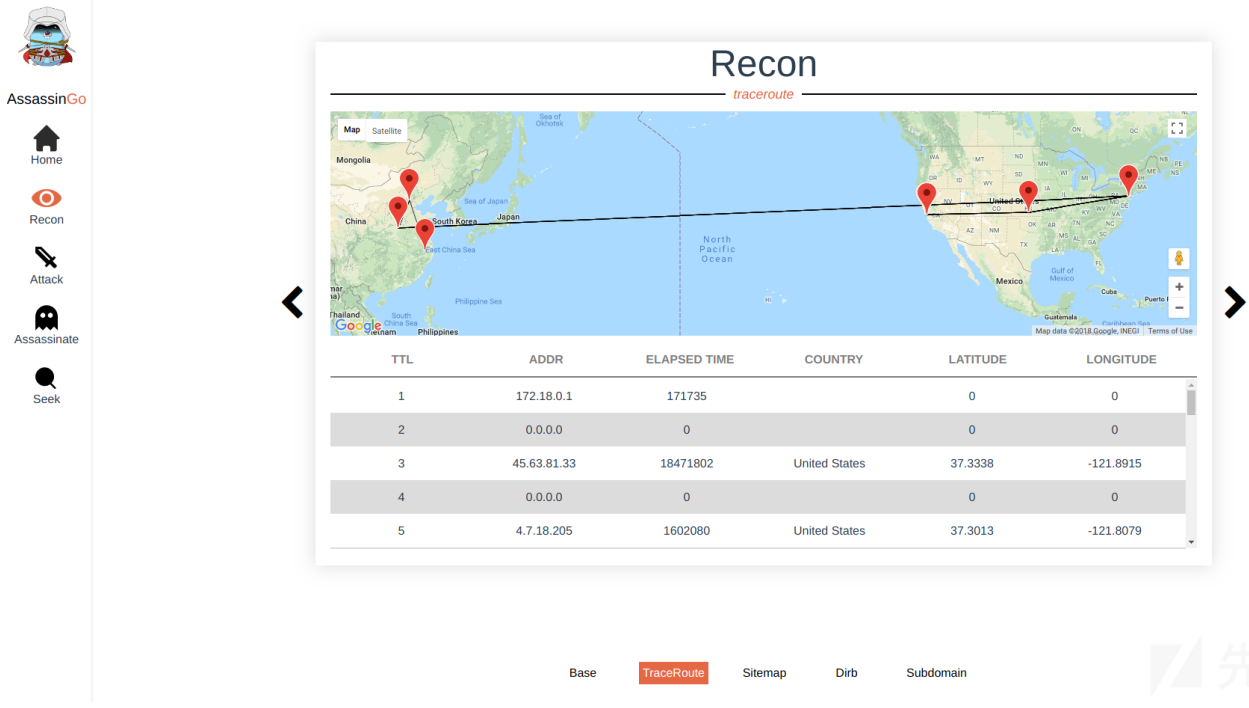
精准的的蜜罐概率检测、并发式的爆破、完美可视化的拓扑以及强大的CloudFlare 绕过并检测真实IP等功能 或许能让使用者在真实的渗透过程中如虎添翼

下面是部分功能截图：

（1）基础信息收集：



（2）路由探测并在地图上可视化标记：

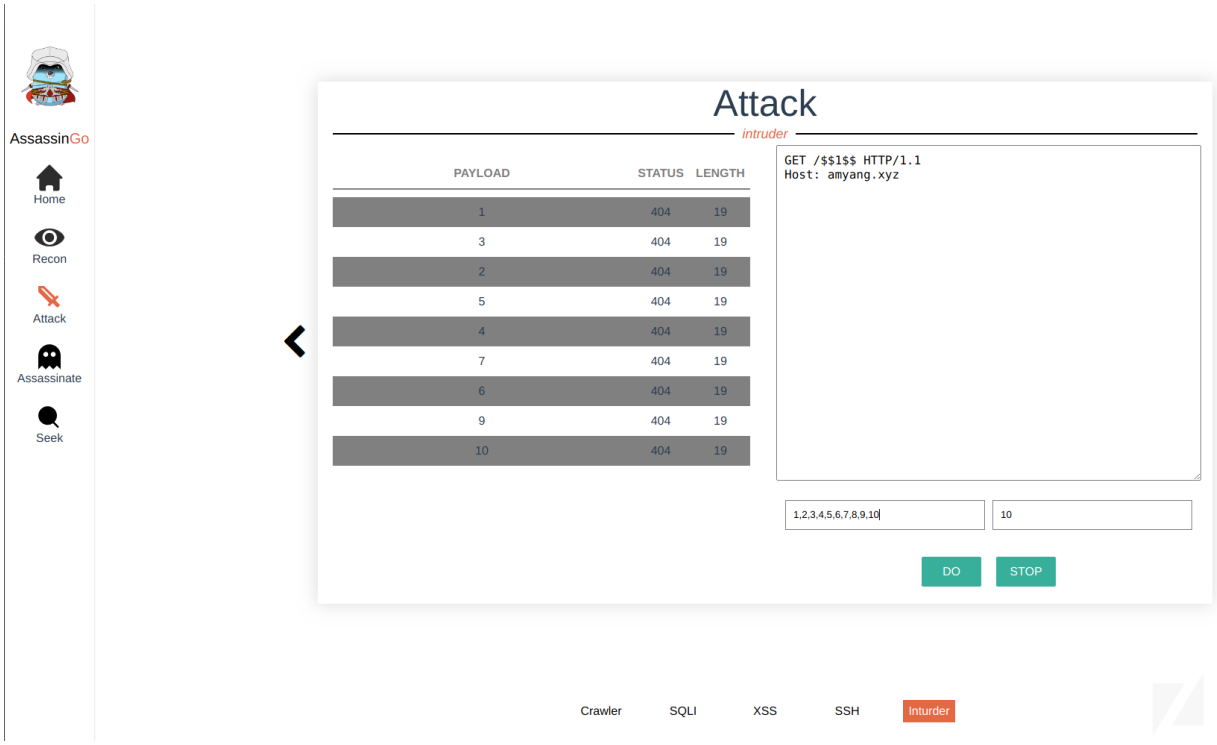


基础攻击部分

- 整站爬虫
- SQLi检测
- 反射型xss
- Intruder
- SSH爆破

以下是部分功能截图：

Intruder

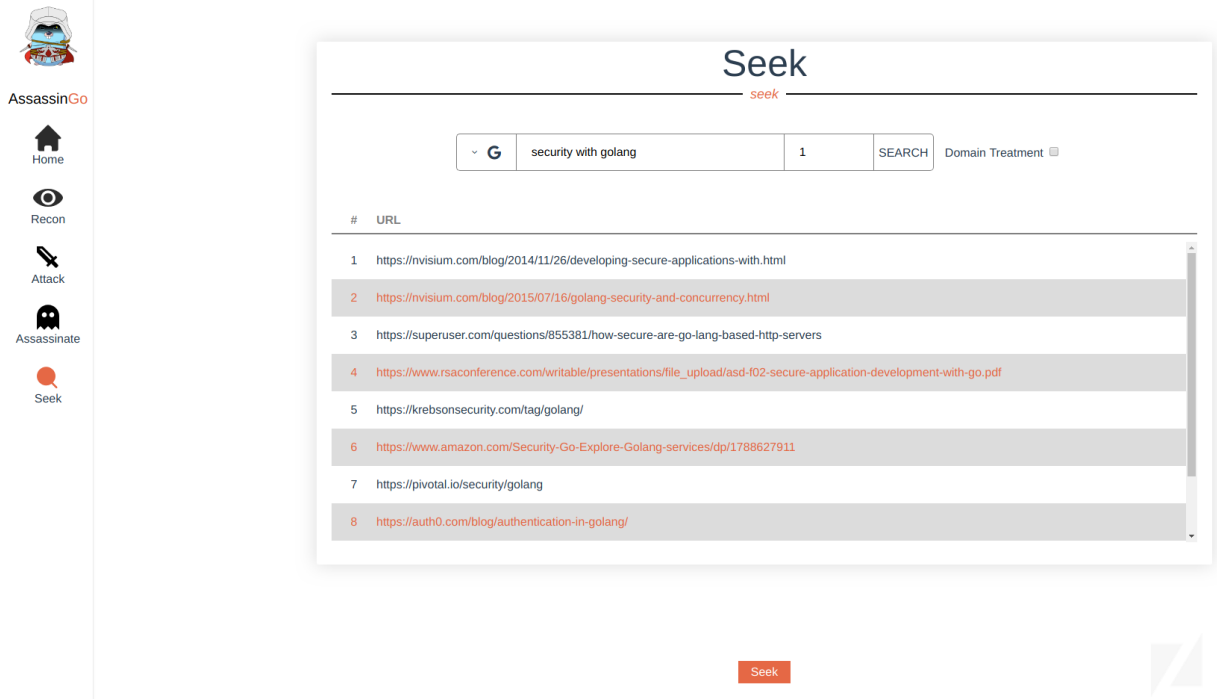


下个版本会将爬虫和XSS检测也升级成headless-chrome版本

Google-Hacking

后端调用Headless-Chrome爬取google或bing搜索结果，完全支持google-hacking语法，而且不会被反爬虫检测。这也可以说是一大特色，利用其强大的搜索能力以及详

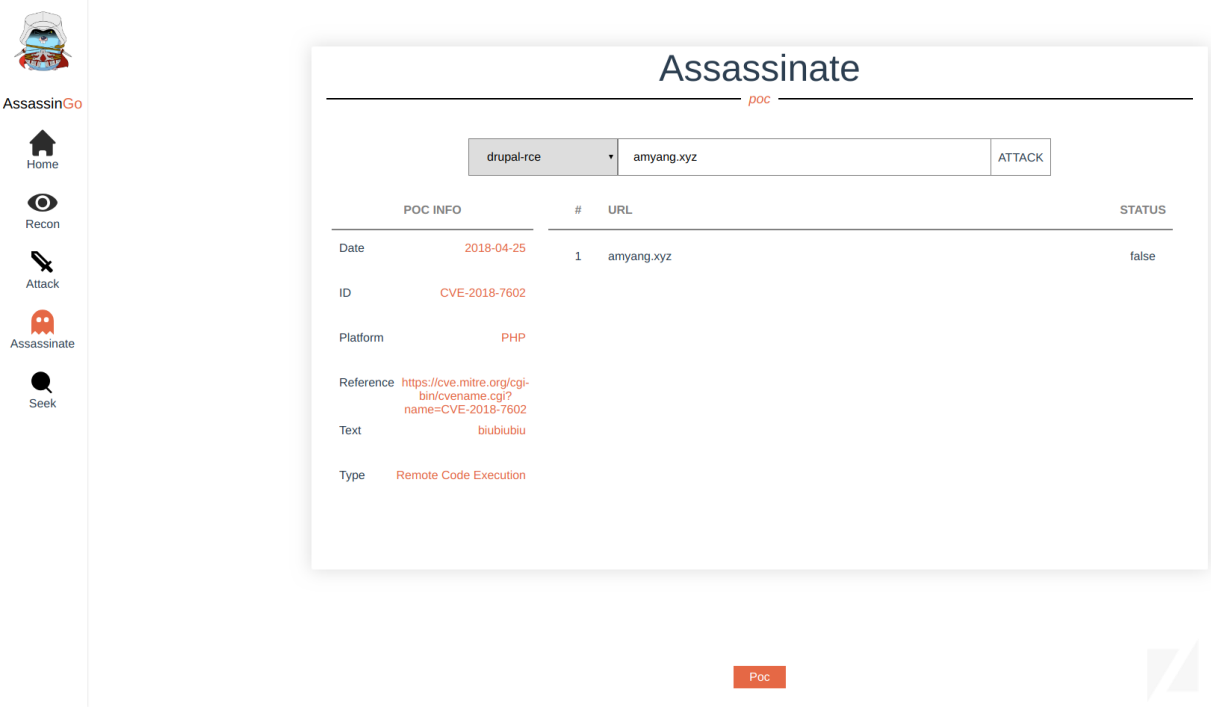
详细的Google-Hacking语法文档将引用团队成员精心整理的git项目，下面是项目地址：
https://github.com/K0rz3n/GoogleHacking-Page



POC 批量精准探测

本框架可内置大量的精心选择的最新的POC，并且会显示Poc的详细的信息。我们提供了非常方便的接口供使用者自定义添加POC，使用者可以根据前面功能搜索到的或批量

下面是功能截图：



网站服务

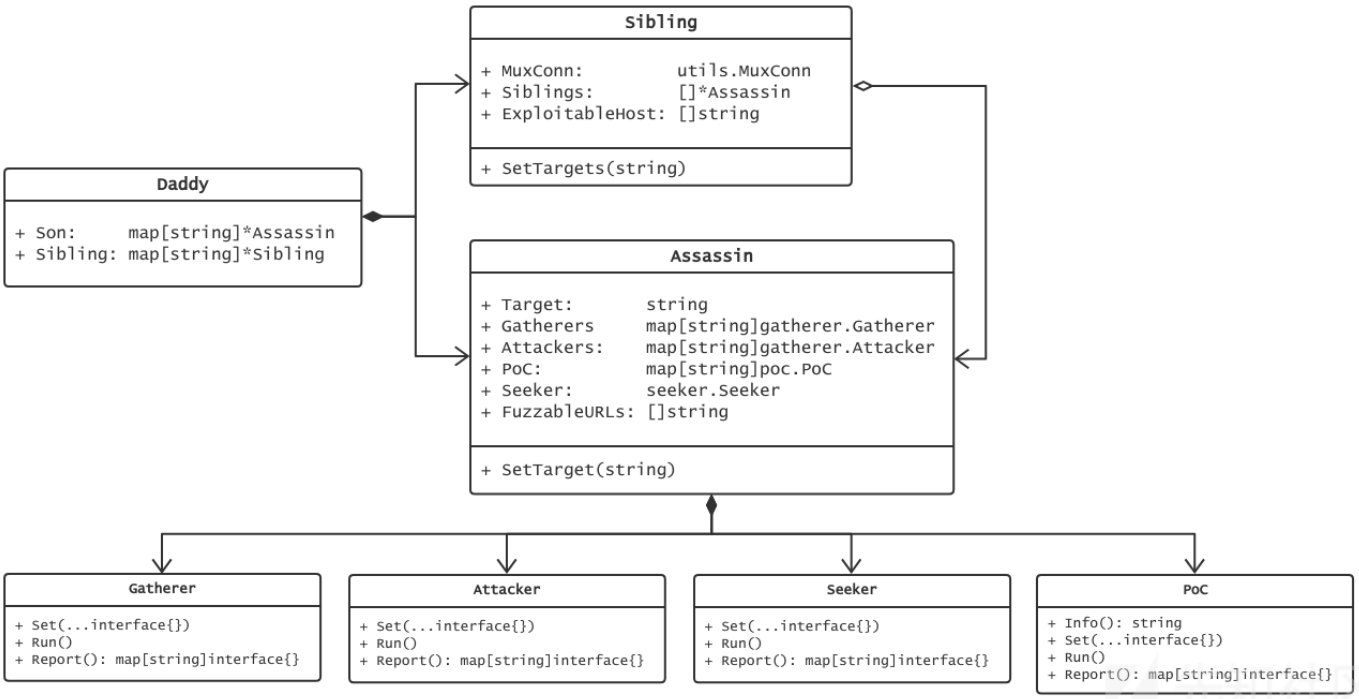
后端基于[sweetygo]

前端基于Vue。

前后端交互大量使用WebSocket，使扫描结果即时展示在前台。

设计概要

后端实现选用组合模式。



信息收集接口Gatherer、基本攻击接口Attacker、漏洞PoC验证接口基本相同，均包含下列三种方法：

Set(...interface{})：设置本函数或PoC所必需的参数，如目标、端口、并发数量等等。

Run()：函数启动入口。

Report() map[string]interface{}：返回执行结果，为后续生成报告准备。

而POC接口还需要额外实现Info() string方法，返回该漏洞的基本信息。

当添加新的功能或更新PoC时仅需编写一个新的.go文件并实现对应接口的方法。

例如当新公布出一个远程代码执行漏洞的PoC时，我们可直接新建一个xx-rce.go文件（参考已写好的几个POC），实现上述接口，重新编译整个项目之后（Go语言的编译时

项目进度

基本功能已开发完，部署了一个demo版本，

由于服务器性能有限，并未开放注册，大家想体验可以联系我手动注册（amyang.xyz@gmail.com），

或者在自己本地搭建，必要的shell脚本和docker-compose已写好。

由于团队人手十分有限，很多地方不是很完善，POC也没有积攒几个，希望大家体谅。

致谢

在这个项目的开发完成过程中团队成员都付出了辛勤的努力，在此表示衷心的感谢。

@Amyang @U1in @K0rz3n，同样，我们也期待你的加入。

上一篇：DnsLogSqlinj Tool... 下一篇：Bundle风水——Android...

1. 4 条回复

Tu9Oh0st 2018-05-31 18:08:18

大佬，问下，如何才能参与这个项目的开发呢？

0 回复Ta

Tu9Oh0st 2018-05-31 18:09:16

@Tu9Oh0st 或者说是需要什么前提条件（语言，还是渗透经验之类的

0 回复Ta


Amyang 2018-05-31 19:12:35

@Tu9Oh0st 有一定开发经验和Go基础，能实现我们的接口扩展功能和PoC就ok

0 回复Ta


小鲜肉懵逼了 2019-07-20 21:54:52

收藏了，可以自己建站了

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