网站漏洞扫描器

项目文档(Version 0.1)

2019年10月5日

最后修改：2019年10月5日

目录

[第1章 项目目录说明](#_Toc28530_WPSOffice_Level1) [3](#_Toc28530_WPSOffice_Level1)

[1.1 项目结构](#_Toc9127_WPSOffice_Level2) [3](#_Toc9127_WPSOffice_Level2)

[1.2 程序运行](#_Toc25720_WPSOffice_Level2) [4](#_Toc25720_WPSOffice_Level2)

[第2章 程序设计需求](#_Toc9127_WPSOffice_Level1) [5](#_Toc9127_WPSOffice_Level1)

[2.1 程序简介](#_Toc20591_WPSOffice_Level2) [5](#_Toc20591_WPSOffice_Level2)

[2.2 设计需求](#_Toc204_WPSOffice_Level2) [5](#_Toc204_WPSOffice_Level2)

[2.2.1 敏感目录扫描](#_Toc9127_WPSOffice_Level3) [5](#_Toc9127_WPSOffice_Level3)

[2.2.2 端口扫描](#_Toc25720_WPSOffice_Level3) [5](#_Toc25720_WPSOffice_Level3)

[第3章 参数说明](#_Toc25720_WPSOffice_Level1) [6](#_Toc25720_WPSOffice_Level1)

[3.1 参数文档](#_Toc25811_WPSOffice_Level2) [6](#_Toc25811_WPSOffice_Level2)

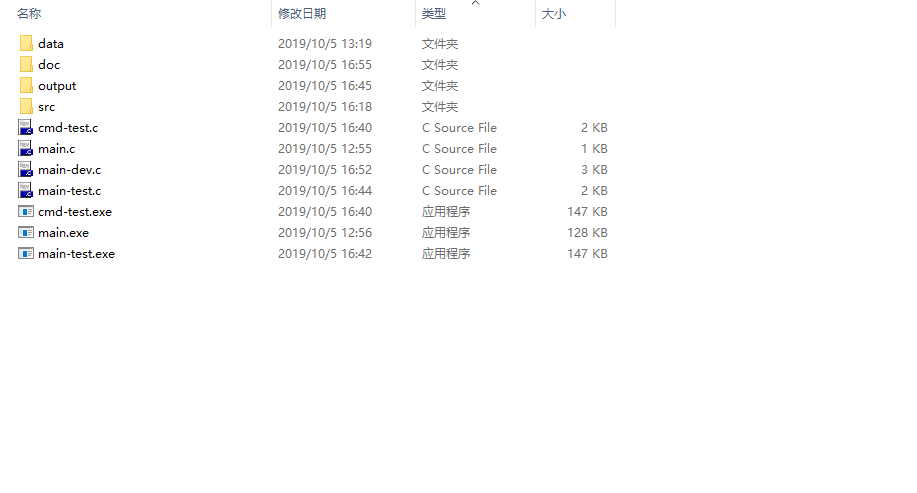
[3.2 参数详情](#_Toc18836_WPSOffice_Level2) [6](#_Toc18836_WPSOffice_Level2)

[常见问题及解决方法](#_Toc31128_WPSOffice_Level1) [7](#_Toc31128_WPSOffice_Level1)

[文档日志](#_Toc17584_WPSOffice_Level1) [8](#_Toc17584_WPSOffice_Level1)

# 第1章 项目目录说明

## 1.1 项目结构



|  |  |  |
| --- | --- | --- |
| 名称 | 类型 | 说明 |
| data | 目录 | 数据文件夹，存放如后台目录、敏感端口 |
| doc | 目录 | 文档文件夹 |
| output | 目录 | 输出文件夹，存放程序输出结果 |
| src | 目录 | C头文件夹 |
| cmd-test.c | 文件 | 解析命令行参考代码 |
| main.c | 文件 | 主代码（全英文注释，编译最终程序） |
| main-dev.c | 文件 | 主代码-开发版（有必要英文注释，编译测试程序） |
| main-test.c | 文件 | 主代码-测试版（允许没有注释，用于调试错误） |

## 1.2 程序运行

目前(2019.10.5),main.c没有实质内容，测试程序由main-dev.c编译，程序位于根目录的main-dev.exe。

可以实现帮助和版本命令（-h,--help,-v,--version），打印输入的url,lang和port字符。效果如下图：

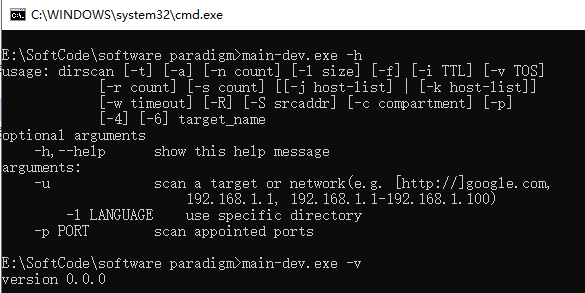


图1-2 打印help和version信息



图1-3 打印参数信息

# 第2章 程序设计需求

## 2.1 程序简介

扫描器用于收集目标网站的敏感目录和端口。根据实际情况，还可以再添加子域名扫描，开发语言自动识别，建站模板识别等。

## 2.2 设计需求

### 2.2.1 敏感目录扫描

敏感目录具体指网站后台，robots.txt，网站配置文件，git文件，网站备份压缩包。现有两个指令控制目录扫描，分别为url和lang。对应扫描网站的url地址和建站语言，建站语言参数将指定对应的目录字典。字典来源于github

### 2.2.2 端口扫描

敏感端口指3389（远程桌面），3306（MySQL 端口），8080（tomcat 端口）等。需要准备一份默认扫描字典。

# 第3章 参数说明

## 3.1 参数文档

参数文档位于data和doc文档，分别用于打印help指令和保存文档。

## 3.2 参数详情

usage: dirscan [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]

[-r count] [-s count] [[-j host-list] | [-k host-list]]

[-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]

[-4] [-6] target\_name

optional arguments

-h,--help show this help message

-v,--version show the version of this program

arguments:

-u scan a target or network(e.g. [http://]google.com,

192.168.1.1, 192.168.1.1-192.168.1.100)

-l LANGUAGE use specific directory

-p PORT scan appointed ports

# 常见问题及解决方法

# 文档日志

* 2019年10月5日

完成第一版(v0.1)的编写工作