软件需求规格说明书

——交互式恶意代码特征查询系统

2.1小组

|  |  |  |
| --- | --- | --- |
| **文件状态**  **[ ] 草稿**  **[ ] 讨论稿**  **[ ] 正式发布** | **文档类型** | 软件需求规格说明书 |
| **文件标识** |  |
| **版 本** | V1.1.001 |
| **作 者** | 邹欢欢 |
| **完成日期** | 2016.09.02 |

文档修订：

|  |  |  |  |
| --- | --- | --- | --- |
| **版本** | **日期** | **更改人** | **描述（注明修改的条款或页）** |
|  |  |  |  |

目录

[软件需求规格说明书 1](#_Toc460662445)

[——交互式恶意代码特征查询系统 1](#_Toc460662446)

[1.引言 4](#_Toc460662447)

[1.1 编写目的 4](#_Toc460662448)

[1.2 软件需求分析背景 4](#_Toc460662449)

[1.3 软件需求分析目标 4](#_Toc460662450)

[1.4 参考文献 4](#_Toc460662451)

[2.系统概述 5](#_Toc460662452)

[2.1 产品描述 5](#_Toc460662453)

[2.2 系统总体功能 5](#_Toc460662454)

[3.软件功能需求说明 5](#_Toc460662455)

[3.1功能需求 5](#_Toc460662456)

[3.2 UML图 6](#_Toc460662457)

[3.3.1用例图 6](#_Toc460662458)

[3.3.2类图 6](#_Toc460662459)

[4.软件非功能性需求 7](#_Toc460662460)

[4.1 运行环境 7](#_Toc460662461)

[4.2 可用性 7](#_Toc460662462)

[4.3 可靠性 7](#_Toc460662463)

[4.4 可维护性，可扩展性 8](#_Toc460662464)

[4.5 灵活性 8](#_Toc460662465)

[4.6 安全性 8](#_Toc460662466)

# 1.引言

* 1. 编写目的

为明确软件需求、安排项目规划与进度、组织软件开发与测试，撰写本文档。

本文档主要用于说明交互式恶意代码特征查询系统的功能需求分析、数据库分析、运行环境等。主要用于开发人员进行项目设计，同时也为后续的数据库维护工作提供了良好的使用说明和标准规范，也可以作为未来版本升级时的重要参考资料。

* 1. 软件需求分析背景

恶意代码，也称为恶意软件，在大多数计算机入侵事件中都扮演了重要角色。任何以某种方式来对用户、计算机或网络造成破坏的软件，都可以被认为是恶意代码，包括计算机病毒、木马、蠕虫、内核套件、勒索软件、间谍软件，等等。

对于这些大量的恶意代码数据，我们需要有一个能够方便进行查询的系统来管理如此多的恶意代码数据，这也就是我们开发此交互式恶意代码特征查询系统的缘由所在。

* 1. 软件需求分析目标

软件需求分析的主要实现目标：

1) 对实现软件的功能做全面的描述，帮助用户判断实现功能的正确性、一致性和完整性，促使用户在软件设计启动之前周密地、全面地思考软件需求；

2) 了解和描述软件实现所需的全部信息，为软件设计、确认和验证提供一个基准；

3) 为软件管理人员进行软件成本计价和编制软件开发计划书提供依据

* 1. 参考文献

# 2.系统概述

2.1 产品描述

恶意代码的分类整理是一件繁琐的事，对于如此多种类的恶意代码，如何对已经进行了静态以及动态分析，特征提取分类的恶意代码进行有效管理，则需要一个有友好用户界面，功能齐全，有效的系统进行恶意代码的管理查询。

由于本次分布式应用系统实践的课题我们致力于恶意代码的分类管理查询，所以所设计的系统全是游客状态，不需要建立注册者信息数据库。系统所实现的功能如下所述。

系统性质：网站。

系统使用者：网站登录者。

系统运行环境：网络运行。

2.2 系统总体功能

2.2.1.能够对恶意代码信息条件查询，（如根据域名，IP等）

2.2.2.能够实现树形图形可视化

2.2.3.对于树状结构的结点，能够显示其信息

# 3.软件功能需求说明

3.1功能需求

3.3.1 能够针对域名进行IP分析

3.3.2 能够针对域名展示其WHOIS信息

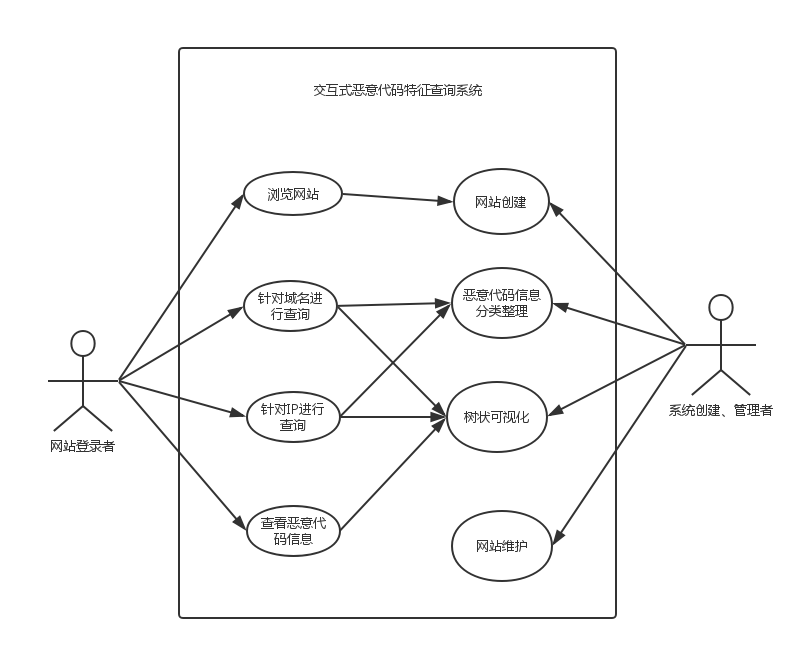
3.3.3 能够对域名进行可视化分析展示

3.3.4 能够真的IP进行IP反查

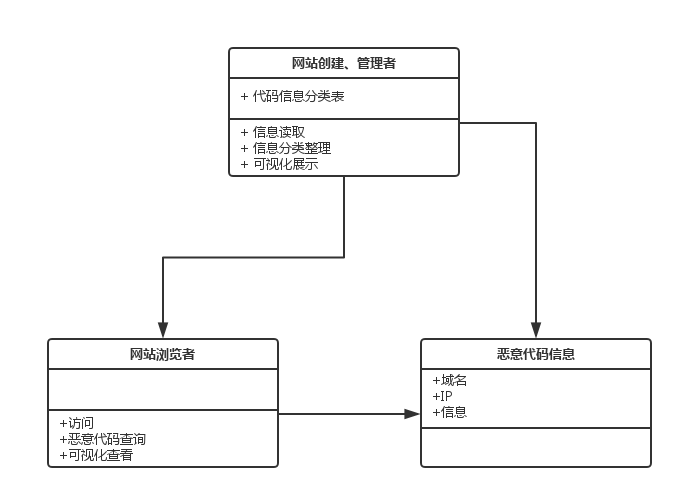
3.3.5 能够展示恶意代码的通信样本信息

3.2 UML图

3.3.1用例图



3.3.2类图



# 4.软件非功能性需求

4.1 运行环境

Firefox，Google chrome等各大类浏览器。

4.2 可用性

在这一部分应从客户使用的合理性和方便性等角度进行描述。例如：

基于最受欢迎的屏幕尺寸和分辨率设计，打造极致用户体验。

• 能够应对应用在运作时可能随时被外界干扰所中断的情况

• 适合用户点击的元素截面尺寸、元素的按键效果（视觉、听觉、触觉）、同步副本和对移动应用运行的影响

4.3 可靠性

本系统的最终用户涉及面广， 因此，整体系统运行要求稳定，有很强的防错、抗错能力，保证数据传输、上报工作正常进行。

4.4 可维护性，可扩展性

应用从设计上尽量考虑到后期拓展，如需添加功能也可做二次开发。从功能上具有通用性，易于修改和扩展。系统具有开放性，是指统计、分析内容的可修改、可扩展性。

4.5 灵活性

计划或者进度改变的时候所有人员听从实验室安排，尽量完成预定目标。若实在力不能及，集体会议商议如何更改项目内容满足时间进度。

4.6 安全性

软件系统自身能不具有的病毒检查能力，对经过服务系统的文件资料不能进行是否携带病毒的检查。解决的方法可以使用其它外部病毒防护软件与系统结合。