申报书

|  |
| --- |
| **一、项目简介：**（200字以内）：  本项目针对互联网发展趋势以及安全形势问题进行探索，利用分布式的扫描，高效的实现网站信息采集、分析及漏洞检测。 本项目能对互联网现有网站进行资产信息收集分析，得到网站的类别及内容倾向，分析出目前互联网的发展趋势和服务导向。 本项目能将互联网批露出的POC、EXP、API进行整理归纳，运用Python编写插件型的漏洞扫描器进行漏洞扫描，分析互联网的安全现状。 |

|  |
| --- |
| **二、申请理由：**（立项依据、自身及团队具备的知识、特长、前期准备等）  **立项依据：**  随着互联网的高速发展与普及，大大小小的商业网站与个人网站如雨后春笋般的搭建了起来，其中蕴含着大量可参考的数据信息，加之中小型网站与个人网站的站长安全意识薄弱，网站的安全性低，存在极大的安全风险与安全隐患。  基于此，本项目将设计分布式的网站信息分析及漏洞扫描平台，调用中间件对返回信息进行处理，调用Python插件对疑似存在风险的网站进行试探性的扫描，最后对数据进行整理，分析目前的服务导向与发展，预估互联网发展状态。  该平台的意义与特点主要有以下几点：  （1）分布式扫描：  由于单机系统性能以及带宽等限制，当需要收集分析与扫描大量主机时显得力不从心。  分布式扫描采用多台主机进行操作，突破系统性能限制，必要时进行分工，专司其职，减少软件本身在系统内竞争产生的资源浪费。  （2）基于中间件的处理数据  用专门的中间件处理数据，增大收集分析数据的准确性。降低维护成本，使项目后期更轻松。  （3）基于python插件的设计  利用插件式的功能处理，把不同的功能模块化，降低它们之间的耦合性，便于后期的维护，以及更容易定制开发新功能插件。  （4）层级处理  利用层级思想，把项目平台递进分类，不满足前置层的要求就不进行下一层次的处理，减少系统的能耗。  **前期准备：**  1.扫描器的框架设计与编写    编写了相应的扫描器主体Demo，对相关常规漏洞的POC以及EXP进行了收集归纳，并大体编写了相应插件。  2. 理清接下来要解决的技术问题与实现难题   （1）运用BootStrap编写Web界面，以及JS实现界面的动态交互；   （2）运用中间件处理与归纳收集的信息；   （3）运用分布式方法与Redis数据库解决信息的收集与存储；   （4）解决高效性的收集与扫描的性能问题；   （5）收集网站信息处理的相关词库，提高网站信息解析归纳的准确性。 |

|  |
| --- |
| **三、项目方案与进度安排：**  **该项目按以下步骤有序的推进：**  第一阶段(2019.5--2019.8)：  **（1）**编写前端界面框架；  **（2）**编写与平台自身交互的API接口文件；  **（3）**编写URL收集器；  **（4）**编写漏洞扫描器。  第二阶段(2019.8--2019.12)：  **（1）**编写漏洞收集中间件；  **（2）**编写信息处理中间件；  **（3）**搭建分布式服务器；  **（4）**处理数据库的存储问题。  第三阶段(2020.1--2020.4)：  **（1）**解决扫描的效率问题；  **（2）**解决代码的容错性处理问题；  **（3）**开始扫描收集，入库等操作；  **（4）**编写相应界面呈现项目想达到的目的效果。 |

|  |
| --- |
| **四、项目特色与创新：**：   本项目能高效的实现信息采集与分析以及漏洞检测，避免重复性的劳作，同时能分析网站的服务导向与发展，尝试感知未来互联网的发展态势。  本项目同时在技术层面有如下特色与创新：   1.突破传统的扫描方式，采用层级和分布式的扫描策略，突破单机的扫描效率限制以及传统的防火墙策略局限；   2.采用Python插件式技术进行漏洞扫描器开发，定制属于自己的扫描工具；   3.采用中间件的处理形式，使数据的处理更加高效。 |
| **五、预期成果：**  设计一套分布式的网站信息分析及漏洞扫描平台,该平台具有如下基本功能: 1.获得网站以及主机的资产信息，分成数十个小类，分析其构成，将结果以柱状、饼状图的形式呈现出来，通过线性变化感知未来互联网的发展趋势。 2.通过简单漏洞的检测结果，获得当前互联网上存在的安全风险与安全隐患态势。 |