申报作品情况（科技发明制作）

|  |  |  |
| --- | --- | --- |
| 作品全称 | 网站安全事件即时监测系统 | |
| 作作品设计、发明的目的和意义 | 随着计算机网络的发展，网站安全也逐渐引起国家和个人的重视。《网络安全法》的推出，从法律层面上保护了公民的权益，但是现实生活中仍然存在着网站被黑等现象。  为了维护安全和谐的网络环境，降低网站被黑风险，洞见研发组推出网络安全事件即时监测系统，能够即时有效发现网站是否被攻击以及攻击类型，并及时通告站长，给出相应的处理意见。解决网站安全事件发现滞后，漏报，新爆发的漏洞不能及时扫描发现的问题。  作为新一代大学生，我们积极响应国家号召，深刻学习习总书记关于“网络安全”的讲话，为祖国网络安全事业尽自己微薄之力。希望我们的作品也能发挥作用，时刻保护网站安全，维护网络安全。 | |
| 作品发明的创新点，技术关键和主要技术指标 | 1. 创新点   随着网站Web2.0前端框架的流行，越来越多的政府、学校等单位摆脱传统的前端架构，迭代为新的前端架构，在使得网站的界面更优美、使用更人性化的同时页给传统网站安全扫描器造成了扫描准确度下降的缺陷。传统的获取数据方式只是获取网站源码，没有将网站的内容加载展示。网站安全事件即时监测系统采用Google的Chrome内核模拟浏览器访问网站，拦截网站传输数据，对数据进行安全分析。突出网站数据完整性，与后台规则库匹配快速定位事件产生的原因。同时使用Chrome内核调用第三方搜索引擎百度、必应、360、Google等的接口。针对搜索引擎下的网站恶意SEO排名产生的劫持事件做特殊关键字搜索，对于此方式产生的网站劫持事件隐蔽性高，普通用户以及站长都很难发现。此平台对于被检测网站无攻击渗透行为，不影响网站线上功能。实现自动化安全测试，大大降低人工重复测试成本。  将被检测网站与监测数据结果在监测平台展示，实现统一管理，查询，用户不仅可以获取被检测网站的安全事件还能对网站事件进行溯源。   1. 技术关键 2. 调用Chrome内核拦截数据流量并做分析； 3. 平台展示系统采用Python语言Flask框架运用经典MVC架构设计； 4. Nginx服务器采用负载均衡支持上万并发扫描； 5. 一键Docker弹性部署，节点模块独立运行。易于拓展，智能评估监测，对于被监控网站数量较少情况下，能减少服务器资源； 6. 自动生成监测报告，微信、短信、邮件预警通告； 7. 技术指标   （1）监测平台的被检测网站任务并发数量  （2）数据存取的实时性与存取的效率  （3）网站监测结果的即时性、准确率、误报率、漏报率  （4）网站监测频率与流量 | |
| 实用性及推广前景的技术性说明及市场分析和经济效益预测 | **实用性及推广前景:**随着国家相关扶植政策的陆续出台，对信息安全方面支持力度越来越大。社会迅速的进入信息化时代，随之带来巨大的网络安全隐患。对网络攻击的监测及系统漏洞的发现及修复，成为当代网络安全的首要任务。  **推广技术与市场分析:**该项目分为监测与漏洞发现两部分，监测部分核心技术为基于谷歌内核的启发式爬虫技术与自主编写维护的威胁规则库。漏洞发现部分为集成了大量PoC文件的漏洞检测框架，能做到快速漏洞检测，自动化扫描，快速输出PoC.有高效，准确，自动化等特性。从近几年来看，因信息网络发展迅猛，网络安全人才也大量稀缺，理所当然一个好的安全监测产品也同样稀缺，特别对于教育政府机构的信息安全的监测更为重要。  **经济效益预测:**在当今市面上，高度集成的安全扫描系统服务费用是很高的。但许多商业性网站，服务器及一些机构单位对于信息安全也是必要的开销,安全产品亦会带来巨大的经济效益。 | |
| 作品进度  安排 | 2018年7月-2018年9月 产品需求分析，需求文档编写  2018年9月-2018年10月 产品功能实现  2018年10月-2018年11月 测试产品，开始对网站进行监测，获取分析数据，补充规则库  2018年12月-2019年02月 产品性能调优，部署上线，服务器性能调优  2019年02月-2019年03月 产品成型，包装、完善 | |
|  |  |  | |

作品附加材料(另附）