Web 应用安全漏洞扫描技术研究

摘　要

随着Web2.0的崛起，社交网络、短视频平台，甚至不少移动端APP都采用Web作为基础平台，企业与政府的信息化建设也首选Web技术，甚至将Web接口作为唯一的公网接口，Web技术的地位得到前所未有的提升，及时发现Web安全漏洞并对其补救成为重中之重。Web安全问题的层出不穷使运营者认识到漏洞的防护成本十分高昂：Web防御是一个巨大且广泛的方面，往往由使用的技术种类、技术实例数量决定其防御成本；而攻击仅仅只是某个防御方面上的一个点，如果一个点被攻破了，无论整体的其他部分做得有多好，依然于事无补。在此思想的影响下，攻击性防护应运而生，即站在攻击者的角度审视整个Web系统，Web应用安全漏洞扫描技术便在此列。其本质是程序基于HTTP协议，构建恶意或畸形数据测试系统功能的鲁棒性与安全性，从而实现发现漏洞、评估漏洞、补救漏洞的闭环。

本文将从三个方面研究Web应用安全扫描技术并解决Web安全问题：1）研究并分析主流安全问题并刨析主流Web应用安全扫描器程序思路；2）通过编程的方式设计并实现对SQL注入及XSS跨站脚本等主流漏洞的扫描；3)研究主流Web安全防护技术，提出Web安全问题的解决方案。基于这些研究，本文开发出了一种新的漏洞扫描器，和国内已有的漏洞扫描器相比，它具有良好的可移植性、可扩展性，并实现了扫描器的爬虫化和漏洞扫描插件化。

关键字：Web安全；漏洞分析；SQL注入；XSS漏洞；漏洞扫描

Abstract

With the rise of the Web, social networking, a short video platform, even many mobile APP using the Web as foundation platform, enterprises and the government's information construction also preferred Web technology, Web interface as the only public interface, even the status of the Web technology to improve on an unprecedented scale, timely find Web security vulnerabilities and its remedy become a top priority. The emergence of Web security issues makes operators realize that the cost of vulnerability protection is very high: Web defense is a huge and extensive aspect, which is often determined by the type of technology used and the number of technical instances; And an attack is just a point in a defense, and if a point is breached, it doesn't matter how well the rest of the whole is doing. Under the influence of this idea, offensive protection came into being, that is, to view the whole Web system from the perspective of the attacker, and Web application security vulnerability scanning technology is one of them. The essence of the program is to build the robustness and security of the malicious or malformed data testing system based on HTTP protocol, so as to realize the closed loop of discovering, evaluating and remediation vulnerabilities.

This paper will study the Web application security scanning technology and solve the Web security problems from three aspects: 1) study and analyze the mainstream security problems and analyze the mainstream Web application security scanner program thinking; 2) design and realize the scanning of mainstream vulnerabilities such as SQL injection and XSS cross-site scripting through programming; 3) study mainstream Web security protection technologies and propose solutions to Web security problems. Based on these studies, a new vulnerability scanner is developed in this paper. Compared with the existing domestic vulnerability scanner, it has good portability and expansibility, and realizes the crawler and plug-in of the scanner.

Keywords: Web security; Vulnerability analysis; SQL injection. XSS holes; Vulnerability scanning