
基于 Web 指纹识别的漏洞扫描工具设计

Design of Vulnerability Scanning Tool Based on Web Fingerprint Identification

摘要

当今世界，移动互联网、云计算等技术在持续进步中，许多行业进行了数字化的革新，而在互联网的广泛应用之下也出现了众多的 Web 安全问题。为了提高 Web 应用的安全性，人们通常在 Web 应用系统上线前会对其进行渗透测试，从而发现并修复 Web 应用中的安全漏洞，提高 Web 应用的安全性。漏洞扫描则是渗透测试过程中必不可少的环节，漏洞扫描可以发现 Web 应用中的脆弱点，渗透测试人员可以根据扫描的结果有针对性地进行渗透测试，迅速定位 Web 应用中的漏洞。高效的漏洞扫描可以在不触发目标站点安全策略的前提下迅速发现 Web 应用的漏洞，如何高效进行漏洞扫描是网络安全研究的重要内容。

本文旨在研究设计一种高效的漏洞扫描方案，高效地检测 Web 应用中的漏洞。该方案基于 Web 应用指纹识别技术，可以有针对性地选择漏洞利用脚本，减少扫描的漏洞数量，提高漏洞扫描的效率。最终使用这个方案设计出了一款基于 Web 指纹识别的漏洞扫描工具，该工具利用 Web 应用指纹识别技术识别出 Web 应用的各种信息，并利用这些信息对漏洞库中的漏洞利用脚本进行筛选，最后利用选出的漏洞利用脚本进行漏洞扫描并输出漏洞扫描报告，实现了高效地进行漏洞扫描的研究目标。

关键词：Web 应用漏洞 Web 漏洞扫描 Web 指纹识别 XSS 跨站脚本 JBoss 反序列化

Abstract

In today's world, mobile Internet, cloud computing and other technologies are in continuous progress. Many industries have made digital innovations, and under the widespread use of the Internet, many Web security problems have also appeared. With the help of penetration testing technology, it is possible to find hidden security risks of Web applications before the attacker, deploy defensive measures in advance, and improve the security of Web applications. Vulnerability scanning is a necessary part of the penetration testing process. Vulnerability scanning can find vulnerabilities in Web applications. Penetration testers can conduct targeted penetration testing based on the results of the scan to quickly locate vulnerabilities in Web applications. How to conduct vulnerability scanning efficiently is an indispensable part of network security research. Efficient vulnerability scanning can quickly find vulnerabilities in Web applications without triggering the security policy of the target site.

This article aims to study and design an efficient vulnerability scanning scheme to efficiently detect vulnerabilities in Web applications. This scheme is based on Web application fingerprint identification technology, which can selectively select vulnerability exploit scripts, reduce the number of scanned vulnerabilities, and improve the efficiency of vulnerability scanning. Finally, using this scheme, a vulnerability scanning tool based on Web fingerprint identification was designed. This tool uses Web application fingerprint identification technology to identify various information of Web applications, and uses this information to filter vulnerability exploit scripts in the vulnerability library. Finally, the selected vulnerability exploit script is used to perform vulnerability scanning and output a vulnerability scanning report, thereby achieving the research goal of efficiently performing vulnerability scanning.

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：

<https://d.book118.com/728130114033006137>