Abstract No: SC-25 **Smart Computing**

Web application securing methods

***B. K. T. P. Wickramasinghe and N. Wedasinghe**

Faculty of Computing, General Sir John Kotelewala Defence University, Sri Lanka
**wickramasinghe95@gmail.com*

Abstract

Web applications are one of the most prevalent platforms for information and services delivery over Internet today. As they are increasingly used for critical services, web applications become a popular and valuable target for security attacks. Although a large body of techniques have been developed to fortify web applications and mitigate the attacks toward web applications, there is little effort devoted to drawing connections among these techniques and building a big picture of web application security research. The main objective of this paper is to point out the possible vulnerabilities in a content serving web application and propose suitable security techniques to protect the site from the attack and provide significant help to the developer of a web application. This research paper organizes the existing research works on securing web applications into three categories based on their design philosophy: security by construction, security by verification and security by protection. Finally, this research paper summarizes the lessons learnt and discuss future research opportunities in this area.

Keywords: Cross-site scripting, SQL injection, Web application

Introduction

Today, almost every enterprise conducts business online. As the applications that run online businesses spread out over technologies and platforms, the security risks also increase. In 2012 alone, there were more than 800 reported hacking incidents, and 70% of those were perpetrated through web application flaws. The web is the new perimeter for enterprise IT security, and it is not nearly as easy to lock down as a network (Hoff, 2013). As web applications are increasingly used to deliver security critical services, they become a valuable target for security attacks. Many web applications interact with back-end database systems, which may store sensitive information (e.g., financial, health), the compromise of web applications would result in breaching an enormous amount of information, leading to severe economic losses, ethical and legal consequences. Current widely-used web application development and testing frameworks, on the other hand, offer limited security support. Secure web application development is an error-prone process and requires substantial efforts, which could be unrealistic under time to-market pressure and for people with insufficient security skills or awareness. As a result, a high percentage of web applications deployed on the Internet are exposed to security vulnerabilities. According to a report by the Web Application Security Consortium, about 49% of the web applications being reviewed contain vulnerabilities of elevated risk level and more than 13% of the websites can be compromised completely automatically.

According to (Gordeychik, 2010) the most widespread vulnerabilities are Cross-Site Scripting, Information Leakage, SQL Injection, Insufficient Transport Layer Protection, Fingerprinting, HTTP Response Splitting (Figure 2).

Many of the available techniques make assumptions on the web technologies used in the application development and only address one security flaw. This paper, surveys