Detection, Avoidance, and Attack Pattern Mechanisms in Modern Web Application Vulnerabilities: Present and Future Challenges

Shashank Gupta, Department of Computer Engineering, National Institute of Technology Kurukshetra, India
B. B. Gupta, Department of Computer Engineering, National Institute of Technology Kurukshetra, India

ABSTRACT

In this paper, we present comprehensive survey of secured web application by identifying numerous serious threats faced by several-related organizations. Based on this, we have summarized the statistics of all emerging web application vulnerabilities by referring several-linked vulnerabilities and their classifications like US-CERT, CVE, CWE, NVD, OWASP etc. In addition, we present a comprehensive survey of the emerging web application weaknesses and discuss how to avoid, detect and attack pattern mechanisms of all critical web threats. Moreover, a detailed comparison has also been presented for all emerging web application exposures corresponding to certain threat agents, which indicates the level of the threat for a recognized vulnerability. In addition, we discuss numerous precautions that can be taken while defining lifecycle of web applications with hacking tools and describe ways to launch & utilize safety procedures and regular security controls in a recursive manner.

KEYWORDS

CERT, CWE, Vulnerability Catalogs, Web Application Attacks, Web Application Vulnerabilities

INTRODUCTION

In the contemporary era of the World Wide Web (WWW), online Internet facilities are accessible by users in real-time, regardless of geographical locations. A continued boom of social networking sites, online shopping sites, Internet banking and other widespread modern web applications provide dynamic access of contents to the users and this has increased utilization of user generated HTML contents (Van, 2015), (Huang, 2016), (Balasubramanian, 2016). Moreover, web applications are often implemented by the web developers with a short development time which works against the implementation of good security architectures. Web developers often lack knowledge about detecting and eliminating web vulnerabilities (McClure, 2002), (Abliz, 2011), (Kleiman, 2009), (Janczewski, 2007), ((Lawton, 2007). Today modern web applications are being developed under advanced technologies (e.g., JavaScript (Flanagan, 2006), AJAX (MacDonald, 2005) etc.) and this has changed the complexity of programs. Moreover, these compound programs are now no longer restricted to execution on the web server-side. As web applications incorporate a considerable amount of JavaScript

DOI: 10.4018/IJCAC.2017070101

Copyright © 2017, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
code, this has to be transferred and executed on the client-side of the web browser. However, web applications are becoming the simplest possible target for the attackers in performing malicious activities, such as session hijacking, stealing session ids, etc. According to reports published in the Common Vulnerabilities Exposure (CVE) database (CVE, 2013), web application flaws are the main cause of most vulnerability.

In addition, the World Wide Web (WWW) has been transformed into a multifaceted network, incorporating a wide variety of components and technologies, including client-side technologies (JavaScript etc.), server-side technologies, HTTPS protocol and a wide variety of other technologies. Web applications developed on these platforms accommodate a wide range of users, and offer access to a wide range of advanced technologies. However, discrepancies among these tools create a challenge of providing defensive security measure for safe development of web applications, even though, current defensive schemes offer limited support for the web application platform. Hence, it is clear that significant efforts are needed for deploying the defensive security measures for a significant number of Internet–based vulnerable web applications. A recent report (WhiteHat, 2013) offers awareness of current issues in the security of web applications and the concerns that industries typically face when performing online business in a secured way. This website has been distributing security statistics report relating to the current state of website security for the following popular domains: Banking, Financial Services, Health Care, Insurance, and Retail business (Haddad, 2009), (Almuhimedi, 2008), (Balduzzi, 2010a), (Balduzzi, 2010b), (Bowen, 2009) since 2006.

**MOTIVATION**

Now-a-days, large multinational corporations depend on the web application to extend and span their business comprising public sector, banking sector, e-commerce, IT sector, etc. All these web applications are built using advanced web technologies like AJAX, JavaScript and are hosted by the cloud servers. While, these are crucial for the business, but at the same time, they are also vulnerable to the various types of cyber-attacks. Consequently, it leads to the reputation damage, loss of sensitive information, financial loss, etc. Figure 1 illustrates the percentage of web application system developed using different programming languages as reported by the Web Application Vulnerability Statistics (2013) (Web application Vulnerability statistics, 2013). It is stated by the report that PHP and Java are the most popular web application development technologies. ‘Other’ category may include less popular languages like perl, python, etc.

There are several vulnerabilities that have infected a large number of web applications of almost every field. Figure 2 shows the statistics for these vulnerabilities that are commonly found in the web applications as reported by the White Hat Security (2015) (White Hat, 2015).

Escalation of JavaScript-based browser-side programming has caused increased security problems interrelated to modern web applications. According to the survey done by the OWASP (OWASP, 2013) in 2013, the problem causing greatest infection is the Cross-Site Scripting (XSS) attack and is accordingly the third top most weakness among the top ten susceptible threats. Figure 3 shows widespread vulnerabilities discovered in web applications tested by the IBM Hosted Application Security Management(HASM) service in contrast to the OWASP Top 10 vulnerabilities presented in 2013 (OWASP, 2013). The OWASP is a community that facilitates organizations for developing and maintaining the modern web applications that can be trusted. It also lists and describes OWASP’s Top 10 vulnerabilities observed in the modern web applications.

It is also shown in report by Web Application Vulnerabilities Statistics (2013) (Web application Vulnerability statistics, 2013) (as shown in Figure 4), that about 76% PHP based web application comprise dangerous vulnerabilities, 70% of java based web application and 55% of ASP.Net based web application comprise dangerous vulnerabilities.
Cloud Computing in Local Government: From the Perspective of Four London Borough Councils
www.igi-global.com/article/cloud-computing-local-government/75113?camid=4v1a

Software-as-a-Service using Heterogeneous Distributed System for User Specific Applications
www.igi-global.com/article/software-as-a-service-using-heterogeneous-distributed-system-for-user-specific-applications/111145?camid=4v1a