Chapter 18
Detecting Vulnerabilities in Web Services: Can Developers Rely on Existing Tools?

Nuno Antunes
University of Coimbra, Portugal

Marco Vieira
University of Coimbra, Portugal

ABSTRACT
Although web services are becoming business-critical components, they are often deployed with software bugs that can be maliciously exploited. Numerous developers are not specialized on security and the common time-to-market constraints limit an in-depth testing for vulnerabilities. In this context, vulnerability detection tools have a very important role helping the developers to produce less vulnerable code. However, developers usually select a tool to use and rely on its results without knowing its real effectiveness. This chapter presents two case studies on the effectiveness of several well-known vulnerability detection tools and discusses their strengths and limitations. Based on lessons learned, the chapter also proposes a benchmarking technique that can be used to select the tool that best fits a specific scenario. The main goal is to provide web service developers with information on how much they can rely on widely used vulnerability detection tools and on how to select the most adequate tool.

INTRODUCTION
Ranging from on-line stores to large corporations, web services are increasingly becoming a strategic vehicle for data exchange and content distribution (Chappell & Jewell, 2002). As addressed in Chapter 15, web services are so widely exposed that any existing security vulnerability will most probably be uncovered and exploited by hackers. Moreover, hackers are moving their focus to applications’ code, often improperly implemented, searching for vulnerabilities by exploring appli-
Detecting Vulnerabilities in Web Services

cations’ inputs with specially tampered values. These values can take advantage of existing vulnerabilities representing considerable danger to the application’s owner, for instance, by giving to an attacker access to read, modify or destroy reserved resources.

To prevent vulnerabilities developers must apply best coding practices, perform security reviews, execute penetration testing, use code vulnerability detectors, etc. Still, many times developers focus on the implementation of functionalities and on satisfying the customer’s requirements and disregard security aspects. Additionally, most developers are not security specialists and the common time-to-market constraints limit an in-depth search for vulnerabilities. In this context, vulnerability detection tools have a very important role helping the developers to produce less vulnerable code.

Although there are several techniques for vulnerability detection in web applications (see chapters 7 and 15), in practice, there are two main approaches to test web services for vulnerabilities (Stuttard & Pinto, 2007):

- **Static code analysis**: “white-box” approach that consists of the analysis of the web application source code. This can be done manually or by using automatic tools. The problem is that exhaustive source code analysis may be difficult and may not find all security flaws due to the complexity of the code.

- **Penetration testing**: “black-box” approach that consists of the analyses of the web application execution in search for vulnerabilities. In this approach, the scanner (either a human or a software tool) does not know the internals of the web application and it uses fuzzing techniques over the web HTTP requests.

Due to time constraints or resource limitations, developers frequently have to select a specific tool from the large set of tools available and strongly rely on that tool to detect potential security problems in the code being developed. The problem is that this is usually done without really knowing how good each tool is. This way, developers urge the definition of a practical approach that helps them comparing alternative tools concerning their ability to detect vulnerabilities.

This chapter introduces some penetration testing and static code analysis tools that are widely used to detect vulnerabilities in web services. The strengths and limitations of both techniques are discussed in the context of the results of two case studies, conducted to understand the effectiveness of the existing tools in real scenarios. Based on the lessons learned, we then present a benchmarking technique that can be applied to select the best tools for specific development settings (i.e., according to the objectives of the developers). The main goal is to provide web service developers with information on how much they can rely on the existing vulnerability detection tools and on how to select and use those tools to obtain the most benefit possible.

**VULNERABILITY DETECTION TECHNIQUES AND TOOLS**

Penetration testing and static code analysis are the two techniques most used by web service developers to detect security vulnerabilities in their code (Stuttard & Pinto, 2007). Penetration testing consists of stressing the application from the point of view of an attacker (“black-box” approach) using specific malicious inputs. On the other hand, static code analysis is a “white-box” approach that consists of analyzing the source code of the application (without executing it) looking for potential vulnerabilities (among other types of software defects). Both penetration testing and static code analysis can be performed manually or automatically. However, automated tools are the
Related Content

Moving from Waterfall to Agile: Perspectives from IT Portuguese Companies
[www.igi-global.com/article/moving-from-waterfall-to-agile-perspectives-from-it-portuguese-companies/216858?camid=4v1a](www.igi-global.com/article/moving-from-waterfall-to-agile-perspectives-from-it-portuguese-companies/216858?camid=4v1a)

The Role of Individual-Media Relationship and Consumer Personal Factors on Spanish Teenagers’ Mobile Social Networking Sites Usage
Carla Ruiz-Mafé, Silvia Sanz-Blas and José Martí-Parreño (2014). *International Journal of E-Services and Mobile Applications* (pp. 18-33).
[www.igi-global.com/article/the-role-of-individual-media-relationship-and-consumer-personal-factors-on-spanish-teenagers-mobile-social-networking-sites-usage/118192?camid=4v1a](www.igi-global.com/article/the-role-of-individual-media-relationship-and-consumer-personal-factors-on-spanish-teenagers-mobile-social-networking-sites-usage/118192?camid=4v1a)

Does Technology Acceptance Change the Way from CRM to Customer Loyalty?: An Empirical Study on the Banking Industry
[www.igi-global.com/chapter/does-technology-acceptance-change-way/65943?camid=4v1a](www.igi-global.com/chapter/does-technology-acceptance-change-way/65943?camid=4v1a)

The Degree of Internationalization and the Use of Social Media in Marketing Communication: The Case of SMEs in Poland