Pen Testing for Web Applications

Ahmad Al-Ahmad, Yarmouk University, Jordan
Belal Abu Ata, Yarmouk University, Jordan
Abdullah H. S. Wahbeh, Dakota State University, USA

ABSTRACT

As many Web applications are developed daily and used extensively, it becomes important for developers and testers to improve these application securities. Pen testing is a technique that helps these developers and testers to ensure that the security levels of their Web application are at acceptable level to be used safely. Different tools are available for Pen testing Web applications; in this paper the authors compared six Pen testing tools for Web applications. The main goal of these tests is to check whether there are any security vulnerabilities in Web applications. A list of faults injected into set of Web pages is used in order to check if tools can find them as they are claimed. Test results showed that these tools are not efficient and developers should not depend solely on them.

Keywords: Developers, Faults Injection, Pen Testing, Security Vulnerabilities, Web Application, Web Pages

INTRODUCTION

Nowadays, Web applications are used worldwide by users for their personal needs but what make Web applications more and more important are the business intentions to use the Web. Web application become one of the most core business assists that must be surrounded by special security guards that are not less than any other assets as stated by Pan and Li (2009). Security issues may harm the benefits of businesses, but here comes the story; these are not ordinary guards, they are IT experts with high salaries, and the enemies here are also different, they are everywhere and nowhere, aided by the same defense methods you use that are Information technologies.

Currently, most of the businesses provide services to its customers using the Web and many of them depend on the Web to do their business in order to make benefits from the global accessibility of the Web. For example, E-commerce is a novel commerce model based on computer network; the E-commerce model depends mainly on money and whenever you find money in any filed, risks become higher and new type of attacker who have a mission to steal money from you not just for fun and self-motivation will be founded (Antunes & Vieira, 2009).

As demonstrated by Guo, Yu, and Chiueh (2005) the wide usage of Web applications and services poses new security challenges on developers and testers, hundreds of new

DOI: 10.4018/jitwe.2012070101
vulnerabilities are being discovered annually and dozens of new patches are being released monthly. So, sensitive data manipulated for these applications must be protected against the attackers who are trying to find vulnerabilities in this kind of applications; these vulnerabilities came from many sources starting from bad wiring code, servers used and firewall.

Keeping the data secure and ensuring that the application is available need extensive search over the test cases. Time challenges make it not practical to test the application code and find vulnerabilities using white box testing; even it’s the best way. Black box testing reduces testing effort and can be automatically repeated extensively to find new vulnerabilities beside the face its meets the time criteria needed by the Web application testing. Pen testing is black box testing method which tries to act like an attacker and use scientific method to find vulnerabilities before the attackers do this using tools and sometimes manually, as defined by Kwon et al. (2005): Pen testing is a goal-oriented method similar to “catch-the-flag” that attempts to gain privileged access to a system using pre-conditional means that a potential attacker could manipulate.

Several studies (Pan & Li, 2009; Antunes & Vieira, 2009; Orloff, Petukhov, & Kozlov, 2008; Zhao, Zheng, & Chen, 2009; Fonseca, Vieira, & Madeira, 2007) addressed web application vulnerabilities and Pen testing. Many Web vulnerabilities such as SQL Injection (Viera et al., 2009; Livshits & Lam, 2005; Halfond, Viegas, & Orso, 2006), XPath Injection (Viera, Antunes, & Madeira, 2009), Cross-site scripting (Livshits & Lam, 2005; Erlingsson, Livshits, & Xie, 2007), Path traversal (Livshits & Lam, 2005), HTTP response splitting (Livshits & Lam, 2005), and Command injection (Livshits & Lam, 2005; Jovanovic, Kruegel, & Kirda, 2006) exist and one of the useful solutions for such vulnerabilities is using Pen testing. Pen testing is new field of study highly needed and interesting for both technical and researcher. With many tools and no standards in this field it is complicated for the tester to start pen testing. Setting Pen testing steps and what is the information needed for each step along with the tools to aid testers in doing their job are ambiguous and still depend on the tester and the application framework used in the development process. Without code, setting as just a user is pen testing in practice. Repeating testing process many times beside all what has been discussed make the tools used in pen testing process very important and effect the overall testing process.

The main objective of this research is to conduct Pen testing on a selected Web application using several tools in order to compare the tools themselves, finding drawbacks in these tools and suggest solution for the testing process.

The remainder of the paper is organized as follows: Related works are described in the first section. The overall methodology followed is presented in the second section. Implementation, experimentation and results evaluation are expressed in third section. Finally, we close our paper with conclusion and future works in the last section.

**RELATED WORKS**

Pen testing for Web applications has been addressed by several researchers. In this section we review some related studies in the field of Pen testing and Web application security.

Orloff (2011) addressed Common Web security vulnerabilities such as cross-site scripting (XSS) and SQL injection. The authors demonstrated that it’s clear that it’s hard for ordinarily developer to take this task of finding vulnerabilities in Web application and this task need special knowledgeable team but with tools the developer can find many of vulnerabilities in Web application in an easy way. The authors studied open sourced tools (WebScrub and Paros) that help tester find vulnerabilities developed by Open Web Application Security Project (OWASP). Orloff (2011) demonstrated that testers also need manual checking to find vulnerabilities and they should insert SQL queries and scripts and find the result of such action. The author concluded that developers need to know what the attacker looks for and
Related Content

Research on the Information Construction of Accounting Audit Based on the Big Data of Computer

A Generic Model for Universal Data Storage and Conversion and Its Web Based Prototypical Implementation
[www.igi-global.com/article/generic-model-universal-data-storage/68966?camid=4v1a](www.igi-global.com/article/generic-model-universal-data-storage/68966?camid=4v1a)
Enabling Distributed Cognitive Collaborations on the Semantic Web
[www.igi-global.com/chapter/enabling-distributed-cognitive-collaborations-semantic/37650?camid=4v1a](www.igi-global.com/chapter/enabling-distributed-cognitive-collaborations-semantic/37650?camid=4v1a)

The Medical Semantic Web: Opportunities and Issues
[www.igi-global.com/article/medical-semantic-web/55381?camid=4v1a](www.igi-global.com/article/medical-semantic-web/55381?camid=4v1a)