Abstract

Once a Web application is hosted in the Internet a window is opened through the local network that easily provides access to target of evaluation (TOE) valuable assets. There is a little emphasis on the security of the Web application itself because the security professionals focused on the security of the network, and the Web servers and browsers operating system. The security of Web applications got focus from the 11th of September 2001.

This thesis focuses on the security testing of the already developed Web application using an enhanced security assessment methodology based on the penetration testing techniques to investigate if there are vulnerabilities in Web application before potential attackers get them without damage the TOE and to check the applied security controls are valid or not for doing its role in security.

This thesis attempts to find a solution for some of the security assessment challenges based on:

- Understanding the different security standards for using one of them as a baseline for creating the Web application *Testing Criteria*.
- Using the *testing criteria* to provide a security assessment that can be applied to evaluate the different Web application security goals.
- Understanding the hacking techniques/testing tools that are used to exploit the vulnerabilities and manipulate Web applications, and to collect them in a tool matrix as a risk assessment methodology.
- Using the attack tree to enhance the accuracy of the security assessment methodology.
- Using the above methodology to check the security countermeasures for Web application authentication implementations.

This thesis is based on the security assessment of the Web application and puts a methodology for testing the software developing lifecycle (SDLC) after the implementation phase. The proposed methodology based on the pen-testing technique because it goes beyond the surface vulnerabilities, and it demonstrates how these vulnerabilities can be exploited using the hacking techniques. The proposed pen-testing is an enhancement for the *Open Source Security Testing Methodology Manual* (OSSTMM) by adding several phases; the scope phase, the information analysis and planning phase, the reporting phase, and the clean up phase.

This proposed methodology defines narrow security testing goals of OSSTMM by suggesting the scope phase which is essential to make the testing process more focused on the security goals because the pen-testing requires extensive work without more precise testing phase it becomes a complicated process. It enables the pen-testers sharing the process and spilt it among several persons, and it helps the organizations to apply the security best practice and evaluate their detection and response plans to minimize the damage associated with successful break-ins.

In addition to the *information analysis and planning phase* to organize the available data gathered about the TOE, and to define a roadmap for security testing effort. It also provides a periodic process for detecting for detecting the weakness that are present in the TOE in order to reduce the probability of a successful attack and to get more protection.

The proposed methodology still has limitations which are eliminated by using the created tool matrix and using of attack tree. The proposed tool matrix is a database that consists of five columns: pen-testing phase, the tool name, the tool feature, the Internet URL for download the tool, and the operating system for running the tool. The proposed tool matrix is based on the survey results of more than two thousand hacking tools. Sample of the tools is classified in a tool matrix according to the phases of pen-testing.

The proposed tool matrix adds several advantages to the pen-testing process like: it provides a baseline for security testing tools sorted in a database that is classified according to the pen-testing phases, it provides a *repository* for the

different exploitation/hacking tools, and it eliminates the dependence on pen-tester experience in the tool selection process. It reduces the searching time for suitable security testing tools for the pen-testing phases: information gathering phase, vulnerability detection and mapping phase, and vulnerability exploitation and penetration phase. Finally, it provides a hacking tool baseline for doing the TOE security testing with several tools for the same TOE vulnerability. But it still suffers from having no way to guarantee that a successful attack will not occur in the future; and there is no way to prioritize the pen-testing job.

The proposed methodology suggests a new usage for the attack tree with the pen-testing and the tool matrix. It makes the testing process more precise because the security testing depending on a particular security goal which is defined in the scope phase, creating a prioritization process for testing based on the risk assessment technique which is estimated from the number of the hacking tools in the updated tool matrix. It provides quantitative estimation based on the number of hacking tools in the up-to-date tool matrix and their potential impact on the TOE. Finally, it displays the potential attacks on the TOE in a hierarchical manner that simplifies navigation and helps making an easy security decision from the security perspective of the attackers. The proposed methodology is security compliance with ISO/IEC 27005.

This research is divided into six chapters: chapter 1 gives an introduction that includes the motivation for doing the thesis. Chapter 2 gives an overview of Web applications and common security problems. Chapter 3 gives the security testing techniques. Chapter 4 gives the proposed Web application security assessment methodology. Chapter 5 gives the case study, and finally chapter 6 gives conclusion and future work.