Chapter 1: Introduction

1.1. Introduction:

The *World Wide Web* (WWW) is the extension of the Internet, which began in late of 1970s with *ARPANET* as an experimental wide-area network created by the U.S Department of Defense. The WWW is a repository of information spreading all over the world.

1.2. Motivation:

The explosive growth of the Internet has brought many good things: e-commerce, e-banking, e-mail, stores of reference material …etc. As technology advances, a dark side starts to reveal itself; criminal hackers (attackers). Anyone can download hacking tools and use them to attempt to break into computers anywhere in the world.

Attackers try to compromise Web applications from their clients, their servers, and/or their networks. Web application software development has several vulnerabilities that are hard to detect and solve. To prevent hacking, security is required for the Web application itself, Web servers, Web browsers, operating systems, and transmission networks and protocols.

There is little emphasis on the security of the Web application itself because the security professionals focus on network and operating system security, but not on the security of Web applications which, got focus from the 11th of September 2001 **[1, 2]**.

The security assessment of Web application has several challenges:

- It is always a complicated process that is hard to realize because security is a process, not an event or product, which is a chain and any single weak link can break the entire Web application security **[3]**.

- It depends on the experience of the security assessment team so that there is no methodology for testing the target of evaluation (TOE).
- It covers a full spectrum of the *target of evaluation* (TOE) vulnerabilities **[4]**.
- It takes a long time to do research and develop appropriate security testing tools.
- It needs to determine the security testing baseline that is required to protect TOE against threats **[4]**.
- It should be done to gain maximum results and with minimal disruption to normal operations **[5]**.
- Security needs are different for each TOE **[5]**.

1.2.1. Thesis Objectives:

The main objective of this thesis is to explore how to enhance the security assessment methodology of Web application based on penetration testing, pen-testing, techniques.

There are several techniques, methods and tools for performing pen-testing which makes it difficult to follow certain methodology. This thesis is based on creating a methodology for doing a security assessment of Web applications according to a developed methodology based on pen-testing.

The thesis attempts to answer the following questions:

- What are the different *security standards* and which of these could be used as a baseline to determine the *testing criteria* of Web applications?
- What are the hacking techniques/tools that are used to exploit the vulnerabilities and manipulate Web applications?
- How to perioterize the security assessment process according to the risk of the Web application attacks?

- How to enhance the security assessment and risk assessment using knowledge about the hacking tools which are classified in a developed tool matrix and the proposed enhanced OSSTMM pen-testing methodology?
- What is the security assessment methodology that is used to test the Web application security controls especially the Web authentication?

This thesis uses the pen-testing as one of the security assessment techniques of Web applications. Existing pen-testing methods suffers from limitations, but this thesis proposes a solution by creating a methodology based on:

- Understanding the different security standards for using one of them as a baseline to determine 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 controls.
- 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.

1.2.2. Thesis Structure:

This thesis outlines is as follow:

- **Chapter Two:** *Overview of Web Applications & Common Security Problems*. It gives a brief about Web origin, Web pages and Web application, Web application authentication and its attacks.
- **Chapter Three:** *the Security testing techniques*. It gives the security lifecycle, the current security standard, the security testing methodologies, the security assessment techniques, the comparison between security testing techniques, and uses the pen-testing methodology. It gives the pen-testing overview its goal, then the successful criteria of pen-testing.
- **Chapter Four:** *The Proposed Web Application Security Assessment Methodology*. It gives a proposed methodology for the security assessment of Web application based on an enhancement for the OSSTMM pen-testing methodology, attack tree, and tool matrix as a risk assessment methodology.
- **Chapter Five:** *Case Study*. It is applied on Web application authentication. It uses the Webgoat project as a target of evaluation (TOE).
- **Chapter Six:** Conclusion and Future Work

After the outlines of the security assessment challenges, the thesis objects and the thesis outline are discussed in more detail, the next chapter discusses the Web application fundamentals and a specific Web application security mechanism; authentication attacks.