

Contents

List of Tables	iv
List of Figures.....	v
Abstract.....	vi
Acronyms.....	ix
Chapter 1: Introduction	3
1.1. Introduction:.....	3
1.2. Motivation:.....	3
1.2.1. Thesis Objectives:.....	4
1.2.2. Thesis Structure:	6
Chapter 2: Overview of Web Applications & Common Security Problems	9
2.1. Introduction:.....	9
2.2. The Web Origin:	9
2.2.1 Markup Languages:	9
2.2.2 Web Pages and Web Sites:	11
2.3. Web Applications:	11
2.3.1 The Anatomy of Web Applications:.....	11
2.3.2 Universal Resource Locator (URL):.....	15
2.3.3 The Hypertext Transfer Protocol (HTTP):	16
2.3.4 Web Services:	18
2.4. Web Application Security:.....	20
2.4.1. Web Application Authentication:	22
2.4.2. Web Application Authentication Mechanisms:.....	23
2.4.2.1. Mechanisms that Do Not Require User Credentials:.....	23
2.4.2.2. Authentication Mechanisms That Require User Credentials:.....	24
a. Basic Authentication:.....	24
b. Digest Authentication:	26
c. Form Based Authentication:	27
2.4.3. Web Authentication Attacks:.....	28
a. Basic Authentication Vulnerabilities:.....	29
b. Digest Authentication Vulnerabilities:	30
c. Form-Based Authentication Vulnerabilities:	31
Chapter 3: The Security Testing Techniques.....	34
3.1. Introduction:.....	34
3.2. Security Lifecycle:	34
1. <i>Security Definition Stage:</i>	35
2. <i>Security Testing Stage:</i>	35
3. <i>Remediation/Mitigation of Risk Findings Stage:</i>	35
4. <i>Ongoing Control and Review Stage:</i>	35
3.3. Security Testing:	36
3.3.1 The Techniques of Security Testing:.....	36
3.3.2 Comparison Between Testing Techniques:	38
3.4. Security Assessment Goals:.....	39
3.4.1 Security Assessment Types:	39
3.4.2 The Security Assessment Testing Criteria:.....	40
3.5. Web Application Security Assessment:.....	42
3.5.1 Manual Inspections & Reviews:	43
3.5.2 Attack Modeling:	43