

## **Contents**

<b>Chapter 1: Introduction</b>	<b>1-3</b>
1.1 Computer Network	
1.2 Internet	
1.3 World Wide Web (WWW)	
1.4 Web Application	
1.5 Popularity of Web Application	
1.6 Security threats in Web Application	
1.7 Web-Graph	
<b>Chapter 2: Security Threats in Web Application</b>	<b>4-7</b>
2.1 About OWASP	
2.2 Top Ten OWASP Attacks (A Report)	
<b>Chapter 3: About Cross Site Request Forgery (CSRF)</b>	<b>8-18</b>
3.1 What is CSRF	
3.2 Sequence diagram to explain CSRF attack	
3.3 Example Scenario of a Typical CSRF attack	
3.4 Present Practice to Address CSRF	
3.5 Present practice to Mitigate CSRF	
3.5.1 Token Validation	
3.5.2 Referrer Test	
3.5.3 Captcha Code	
3.6 Observation and Motivation	

<b>Chapter 4: Problem selection</b>	<b>19-25</b>
4.1 Problem Selection Based on Motivation	
4.2 Preparation of Test Bed	
4.2.1 Architecture of proposed system based on	
4.3 About Web-Graph	
4.3.1 What is Web-Graph	
4.3.2 In general web graph is used for several purposes	
4.3.3 Web-graph in preparing access behavioral model	
4.3.4 How web graph is used to identify a legitimate user	
<b>Chapter 5: Proposed Detection Method</b>	<b>26-29</b>
5.1 Algorithm to Create Web-Graph	
5.2 Algorithm to Identify Legitimate User	
5.3 Experimental results and data sets	
<b>Chapter 6: Conclusion and Future Work</b>	<b>30</b>
<b>Appendix A: Bibliography</b>	<b>31</b>
<b>Appendix B: GUI Interface and Snapshots</b>	<b>32-35</b>