

# CONTENTS

<b>1 Introduction</b>	<b>1-4</b>
1.1 Popularity of internet and web applications	
1.2 Security in web applications	
1.3 Harmfulness of typical threat Cross-site request forgery (CSRF)	
1.4 Present practices of defending web	
<b>2 Web Applications</b>	<b>5-6</b>
<b>3 Security Threats in Web Applications</b>	<b>7-9</b>
<b>4 Cross-Site Request Forgery</b>	<b>10-13</b>
4.1 Example scenario	
4.1 Conducting CSRF attacks	
4.3 Sequence Diagram	
<b>5 Prevention Measures for CSRF attacks</b>	<b>14-15</b>
<b>6 Problem Definition</b>	<b>16</b>
<b>7 Methodology</b>	<b>17-29</b>
7.1 Test bed	
7.2 Site Description	
7.3 CSRF attack demonstration	
7.4 Token method	
7.5 CAPTCHA method	
7.6 Graph based method	
<b>8 Comparative Study and Discussions</b>	<b>30-32</b>
<b>9 Conclusion</b>	<b>33</b>
<b>10 References</b>	<b>34-35</b>

# LIST OF FIGURES

2.1	Web Application Architecture	5
4.1	Sequential diagram showing a cross site request forgery attack	13
7.1	Login Page	18
7.2	User Profile Page	18
7.3	Transfer Page	19
7.4	Transaction Page	19
7.5	Attacker Site	20
7.6	Demonstration of attack	21
7.7	Token Algorithm	22
7.8	Transfer through Token page	23
7.9	CAPTCHA Algorithm	24
7.10	Transfer through CAPTCHA	25
7.11	Legitimate Profile	26
7.12	Legitimate profile web graph	27
7.13	Dynamic profile for a particular instance	27
7.14	Dynamic profile web graph for a particular instance	28
7.15	Attack Detected and Blocked	29
7.16	Graph based Algorithm	29