TABLE OF CONTENTS

Table of Contents vi

List of Figures ix

List of Tables xii

List of Terms xiii

Chapter I Introduction 1

I.1 Background 1

I.2 Problem Statement 2

I.3 Research Objectives 2

I.4 Research Scopes 3

I.5 Research Benefits 3

Chapter II LITERATURE REVIEW 4

II.1 Previous Study 4

II.2 Website 4

II.3 Web Hosting 5

II.4 Website Vulnerabilities 6

II.5 Vulnerability Assessment and Penetration Testing (VAPT) 8

II.5.1 Vulnerability Assessment and Penetration Testing Technique 9

II.6 Kali Linux 10

II.7 Owasp Web Security Testing Guide Version 4 11

II.8 Owasp Risk Rating Methodology 11

II.9 Security Hardening 11

II.9.1 Pre-Hardening 12

Chapter III METHODS 13

III.1 Stages of Problem Solving 13

III.1.1 Problem Statement 14

III.1.2 Planning 14

III.1.3 Simulation 14

III.1.4 Analysis 14

III.1.5 Final Phase 14

III.2 Data Collection 15

III.3 Evaluation Methods 15

III.4 Justification of Methods 15

Chapter IV EXPERIMENTAL SYSTEM 16

IV.1 Experimental System 16

IV.1.1 Hardware 16

IV.1.2 Software 16

IV.2 Testing Scenario Implementation of Attack Tools 19

IV.3 OWASP Testing Guide 20

IV.3.1 Information Gathering 20

IV.3.2 Data Validation Testing 22

IV.3.3 Client Side Testing 24

Chapter V EXPERIMENTAL DATA TESTING AND ANALYSIS 26

V.1 Experimental Data Testing and Analysis 26

V.1.1 Information Gathering Result 26

V.1.2 Data Validation Testing Result 34

V.1.3 Client Side Testing Result 55

V.2 Testing Result 66

V.3 Analysis 66

V.3.1 Threat Agent Factor 66

V.3.2 Vulnerability Factor 68

V.3.3 Technical Impact 69

V.3.4 Business Impact 71

V.3.5 Overall Risk Severity 72

V.4 Recommendation 74

Chapter VI CONCLUSION AND SUGGESTION 75

VI.1 Conclusion 75

VI.2 Suggestion 75

REFERENCES 76