

**PENETRATION TESTING FOR CROSS-SITE SCRIPTING
(XSS) DETECTION USING PENETRATION TESTING
EXECUTION STANDARD (PTES) METHODOLOGY: A CASE
STUDY OF INFORMATION SYSTEMS IN UNIVERSITAS
PENDIDIKAN GANESHA**



**BY
NABILA AULIA AZIZAH
2215091040**

**INFORMATION SYSTEM STUDY PROGRAM
DEPARTMENT OF INFORMATICS ENGINEERING
FACULTY OF ENGINEERING AND VOCATIONAL
UNIVERSITAS PENDIDIKAN GANESHA
SINGARAJA**

2026

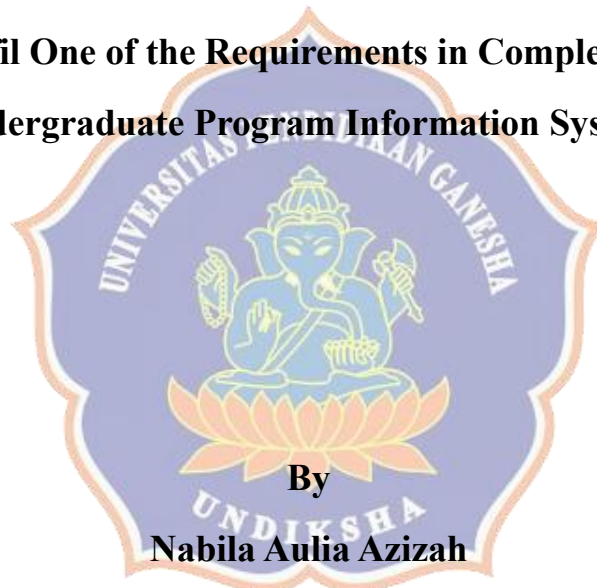
**PENETRATION TESTING FOR CROSS-SITE SCRIPTING
(XSS) DETECTION USING PENETRATION TESTING
EXECUTION STANDARD (PTES) METHODOLOGY: A CASE
STUDY OF INFORMATION SYSTEMS IN UNIVERSITAS
PENDIDIKAN GANESHA**

UNDERGRADUATE THESIS

Submitted to

Universitas Pendidikan Ganesha

**To fulfil One of the Requirements in Completing the
Undergraduate Program Information Systems**



By

Nabila Aulia Azizah

221509104

**INFORMATION SYSTEM STUDY PROGRAM
DEPARTMENT OF INFORMATICS ENGINEERING
FACULTY OF ENGINEERING AND VOCATIONAL
UNIVERSITAS PENDIDIKAN GANESHA**

SINGARAJA

2026

UNDERGRADUATE THESIS

**SUBMITTED IN FULFILLMENT OF THE
REQUIRED ACADEMIC WORK AND IN
COMPLETION OF THE REQUIREMENTS TO
OBTAIN THE DEGREE OF BACHELOR OF
COMPUTER SCIENCE**

Approved By

Supervisor I	Ir. Gede Arna Jude Saskara, S.T.,M.T NIP.199105152020121003
Supervisor II	Dr. Gede Saindra Santyadiputra, S.T., M.Cs. NIP.198708022014041001

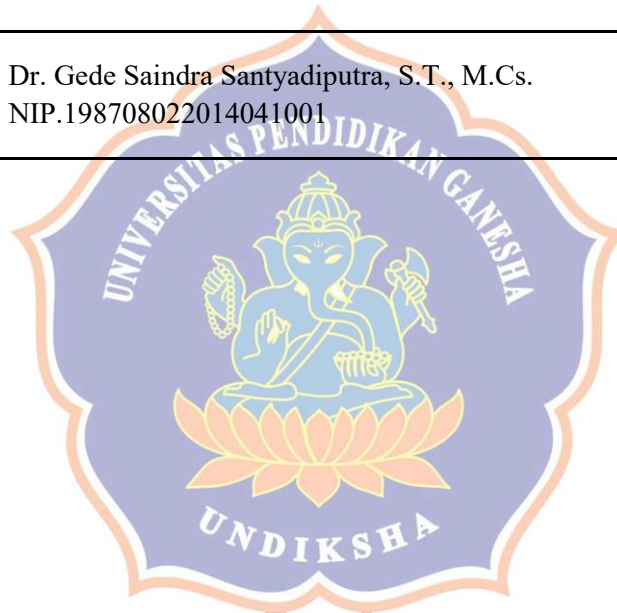


- UU ITE No. 11 Tahun 2008 Pasal 5 Ayat 1 "Informasi Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah"
- Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan BSrE - BSSN, validitas dokumen elektronik ini bisa dicek menggunakan aplikasi mobile YeryDS oleh BSrE
- Cetakan dokumen ini merupakan salinan dari file dokumen bertandatangan elektronik yang keabsahannya dapat diakses melalui scan QRCode yang terdapat pada sertifikat ini.

Undergraduate Thesis by Nabila Aulia Azizah
Has been defended before the Board of Examiners
on the date of May 20, 2026

Board of Examiners

Chairperson	Ir. Kadek Teguh Dermawan, S.Pd., M.Korn. NIP.199406132025061003
Member	Dr. Bagus Gede Krishna Yudistira, M.Korn. NIP.199208122024061003
Member	Ir. Gede Arna Jude Saskara, S.T.,M.T NIP.199105152020121003
Member	Dr. Gede Saindra Santyadiputra, S.T., M.Cs. NIP.198708022014041001



- UU ITE No. 11 Tahun 2008 Pasal 5 Ayat 1 "Informasi Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah"
- Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan BSrE - BSSN, validitas dokumen elektronik ini bisa dicek menggunakan aplikasi mobile YeryDS oleh BSrE
- Cetakan dokumen ini merupakan salinan dari file dokumen bertandatangan elektronik yang keabsahannya dapat diakses melalui scan QRCode yang terdapat pada sertifikat ini.

Accepted by the Examination Committee of the Faculty of Engineering and Vocational
Universitas Pendidikan Ganesha
to fulfill the requirements to obtain the undergraduate degree of bachelor of computer science

Approved By

Chairperson of the Examination	Ir. Made Windu Antara Kesiman, S.T., M.Sc., Ph.D. NIP.198211112008121001
Secretary of the Examination	Ir. I Made Dendi Maysanjaya, S.Pd., M.Eng. NIP.199005152019031008

Endorsed,
Dean of the Faculty of Engineering and Vocational



- UU !TE No. 11 Tahun 2008 Pasal 5 Ayat 1 "Informasi Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah"
- Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan BSrE • BSSN, validitas dokumen elektronik ini bisa dicek menggunakan aplikasi mobile YeryDS oleh BSrE
- Cetakan dokumen ini merupakan salinan dari file dokumen bertandatangan elektronik yang keabsahannya dapat diakses melalui scan QRCode yang terdapat pada sertifikat ini.

STATEMENT OF AUTHENTICITY

I hereby declare that this academic work entitled “Penetration Testing for Cross-Site Scripting (XSS) Detection Using Penetration Testing Execution Standard (PTES) Methodology: A Case Study of Information Systems in Universitas Pendidikan Ganesha” and all its contents are truly my own work, and I have not committed plagiarism or cited in ways inconsistent with the ethics prevailing in the academic community. I am prepared to bear any risk/sanction imposed on me if violations of academic ethics are found in this work, or if there are claims against its authenticity.



Singaraja, 09 June 2026

Statement made by



A handwritten signature in black ink, appearing to read 'Nabila Aulia Azizah'.

Nabila Aulia Azizah

Student ID. 2215091040

MOTTO

“There is no another chance in this life. Do it now or never.”



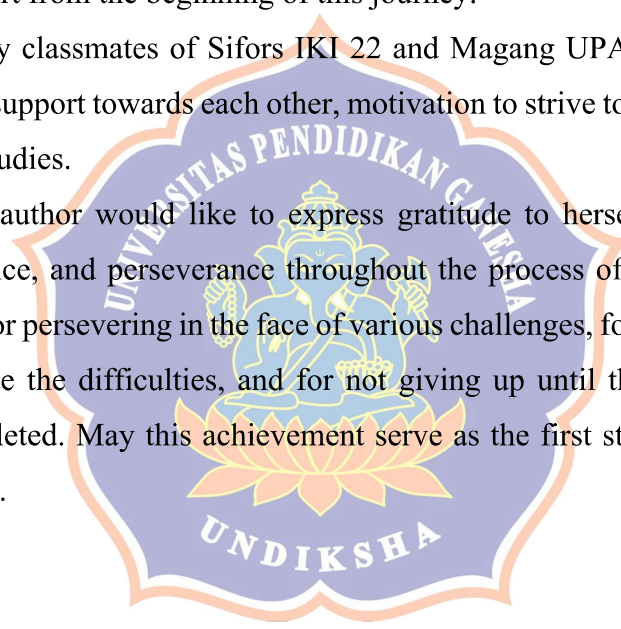
PREFACE

The author would like to express sincere gratitude to the Almighty of God for His blessings and grace, which encourage the author to complete this undergraduate thesis entitled “Penetration Testing For Cross-Site Scripting (XSS) Detection Using Penetration Testing Execution Standard (PTES) Methodology: A Case Study of Information Systems In Universitas Pendidikan Ganesha.”

This undergraduate thesis is submitted to fulfill of the requirements for obtaining a Bachelor’s degree in Computer Science at Universitas Pendidikan Ganesha. During the research, the author has been encountered several obstacles and challenges. However, the author would like to express sincere gratitude and appreciation to:

1. Prof. Dr. I Wayan Lasmawan, M.Pd., Rector of Universitas Pendidikan Ganesha, who has provided the author with the opportunity to pursue higher education in the Information Systems Study Program, Department of Informatics, Faculty of Engineering and Vocational Studies.
2. Prof. Dr. Kadek Rihendra Dantes, S.T., M.T., as the Dean of the Faculty of Engineering and Vocational, which enabled the to complete the study.
3. Ir. Gede Arna Jude Saskara, S.T.,M.T., as the First Supervisor, who has provided guidance, advices, feedbacks, and believe that the author can accomplish this research.
4. Dr. Gede Saindra Santyadiputra, S.T., M.Cs., as the Second Supervisor, who has provided valuable guidance, suggestions, advices, support, and knowledge to broader perspective that helped the author to develop understanding and explore various aspect within this research.
5. Ir. Kadek Teguh Dermawan, S.Pd., M.Kom., as the First Examiner, for the valuable suggestions, guidance, direction, and motivation provided to the author throughout the preparation of this thesis, as well as for the extensive knowledge shared with the author during the course of study.
6. Dr. Bagus Gede Krishna Yudistira, M.Kom., as the Second Examiner, for the valuable insights, suggestions, guidance, and motivation to this research.

7. All the lecturers in Information System Study Program, who have given insights and advices to the author during the study.
8. Staffs in UPA TIK and mentor in security division, Ketut Wawan Arimbawa, S.Kom., who involved directly to helps this research.
9. Beloved parents, siblings, and other family for their endless support, prayers, motivation, and unconditional love given to the author.
10. To someone, Angga, who always encouraged the author to take this topic a well as his endless support during this journey.
11. To my best friend in this journey, Artini, Dian, April, Putri, Utta, Eva, Ilfi, Irbah, Vika, Berlian, and Icha, for their encourgamenet, motivation, and support from the beginning of this journey.
12. To my classmates of Sifors IKI 22 and Magang UPA TIK 2025/2026 for their support towards each other, motivation to strive together in completing our studies.
13. Last, author would like to express gratitude to herself for all the effort, patience, and perseverance throughout the process of this journey. Thank you for persevering in the face of various challenges, for continuing to strive despite the difficulties, and for not giving up until this work was finally completed. May this achievement serve as the first step toward a brighter future.



Singaraja, 28 May 2026

Author

TABLE OF CONTENTS

STATEMENT OF AUTHENTICITY	v
PREFACE	i
ABSTRACT	iii
ABSTRAK	iv
TABLE OF CONTENTS	v
LIST OF TABLES	xi
LIST OF FIGURES	xv
LIST OF APPENDICES	xvi
CHAPTER I INTRODUCTION	1
1.1. Research Background	1
1.2. Problem Identification	4
1.3. Research Objectives.....	5
1.4. Research Limitations	5
1.5. Research Significances	6
CHAPTER II THEORETICAL FRAMEWORK	8
2.1. Literature Review	8
2.2. Theory Background	21
2.2.1. Information System	21
2.2.2. Information System Security	21
2.2.3. Web Application Vulnerability	22
2.2.4. Penetration Testing	22
2.2.5. Penetration Testing Execution Standard	24
2.2.6. Cross-Site Scripting	25
2.2.7. Risk Assessment	26
2.2.8. OWASP Risk Rating Methodology.....	26

CHAPTER III RESEARCH METHODOLOGY	28
3.1. Type of Research	28
3.2. Research Stage.....	29
3.3. Data Collection Method.....	30
3.4. Penetration Testing Execution Standard	32
3.4.1. Pre-Engagement Interactions Phase.....	32
3.4.2. Intelligence Gathering Phase	33
3.4.3. Threat Modeling Phase.....	33
3.4.4. Vulnerability Analysis Phase	33
3.4.5. Exploitation Phase	35
3.4.6. Post-Exploitation Phase.....	35
3.4.7. Reporting Phase.....	35
3.5. Data Verification and Analysis.....	35
3.6. Data Validation.....	39
3.7. Tools	40
CHAPTER IV FINDINGS AND DISCUSSION	42
4.1. Research Findings.....	42
4.1.1. Pre-Engagement Interactions.....	42
4.1.2. System A.....	44
4.1.2.1. Intelligence Gathering	44
4.1.2.2. Threat Modeling.....	45
4.1.2.3. Vulnerability Analysis	47
4.1.2.4. Exploitation	49
4.1.2.5. Post-Exploitation	49
4.1.2.6. Reporting.....	49
4.1.3. System B.....	49
4.1.3.1. Intelligence Gathering	49

4.1.3.2.	Threat Modeling.....	50
4.1.3.3.	Vulnerability Analysis.....	51
4.1.3.4.	Exploitation.....	52
4.1.3.5.	Post-Exploitation.....	52
4.1.3.6.	Reporting.....	53
4.1.4.	System C.....	53
4.1.4.1.	Intelligence Gathering.....	53
4.1.4.2.	Threat Modeling.....	54
4.1.4.3.	Vulnerability Analysis.....	55
4.1.4.4.	Exploitation.....	57
4.1.4.5.	Post-Exploitation.....	59
4.1.4.6.	Reporting.....	60
4.1.4.7.	Data Analysis.....	61
4.1.5.	System D.....	85
4.1.5.1.	Intelligence Gathering.....	85
4.1.5.2.	Threat Modeling.....	86
4.1.5.3.	Vulnerability Analysis.....	87
4.1.5.4.	Exploitation.....	88
4.1.5.5.	Post-Exploitation.....	89
4.1.5.6.	Reporting.....	90
4.1.5.7.	Data Analysis.....	90
4.1.6.	System E.....	102
4.1.6.1.	Intelligence Gathering.....	102
4.1.6.2.	Threat Modeling.....	103
4.1.6.3.	Vulnerability Analysis.....	105
4.1.6.4.	Exploitation.....	106

4.1.6.5.	Post-Exploitation	107
4.1.6.6.	Reporting.....	107
4.1.7.	System F	107
4.1.7.1.	Intelligence Gathering.....	107
4.1.7.2.	Threat Modeling.....	108
4.1.7.3.	Vulnerability Analysis.....	110
4.1.7.4.	Exploitation	111
4.1.7.5.	Post-Exploitation	111
4.1.7.6.	Reporting.....	111
4.1.8.	System G	112
4.1.8.1.	Intelligence Gathering.....	112
4.1.8.2.	Threat Modeling.....	113
4.1.8.3.	Vulnerability Analysis.....	115
4.1.8.4.	Exploitation.....	118
4.1.8.5.	Post-Exploitation.....	118
4.1.8.6.	Reporting.....	118
4.1.9.	System H	118
4.1.9.1.	Intelligence Gathering.....	118
4.1.9.2.	Threat Modeling.....	119
4.1.9.3.	Vulnerability Analysis.....	121
4.1.9.4.	Exploitation	122
4.1.9.5.	Post-Exploitation	123
4.1.9.6.	Reporting.....	123
4.1.10.	System I.....	123
4.1.10.1.	Intelligence Gathering.....	123
4.1.10.2.	Threat Modeling.....	124

4.1.10.3. Vulnerability Analysis.....	126
4.1.10.4. Exploitation	128
4.1.10.5. Post-Exploitation.....	130
4.1.10.6. Reporting.....	131
4.1.10.7. Data Analysis.....	132
4.1.11. System J.....	154
4.1.11.1. Intelligence Gathering.....	154
4.1.11.2. Threat Modeling.....	155
4.1.11.3. Vulnerability Analysis.....	158
4.1.11.4. Exploitation	160
4.1.11.5. Post-Exploitation.....	165
4.1.11.6. Reporting.....	167
4.1.11.7. Data Analysis.....	169
4.1.12. System K.....	223
4.1.12.1. Intelligence Gathering.....	223
4.1.12.2. Threat Modeling.....	224
4.1.12.3. Vulnerability Analysis.....	226
4.1.12.4. Exploitation	228
4.1.12.5. Post-Exploitation.....	229
4.1.12.6. Reporting.....	230
4.1.12.7. Data Analysis.....	230
4.1.13. System L.....	241
4.1.13.1. Intelligence Gathering.....	241
4.1.13.2. Threat Modeling.....	242
4.1.13.3. Vulnerability Analysis.....	244
4.1.13.4. Exploitation	245

4.1.13.5. Post-Exploitation.....	246
4.1.13.6. Reporting.....	246
4.2. Discussions	246
CHAPTER V CONCLUSION.....	258
5.1. Conclusions.....	258
5.2. Recommendation	259
REFERENCES	262
APPENDICES.....	266



LIST OF TABLES

Table 3.1 List of the Testing Target.....	30
Table 3.2 List references of CVE's	33
Table 3.3 Risk Severity.....	39
Table 3.4 Overall Risk Severity.....	39
Table 3.5 Tools	40
Table 4.1 Intelligence Gathering of System A.....	44
Table 4.2 Threat Modeling of System A (Reflected XSS).....	45
Table 4.3 Threat Modeling of System A (DOM-Based XSS).....	46
Table 4.4 Automated Scanning Result of System A.....	47
Table 4.5 Manual Testing Result of System A (Reflected XSS)	48
Table 4.6 Manual Testing Result of System A (DOM-Based XSS)	48
Table 4.7 Testing Summary Report of System A	49
Table 4.8 Intelligence Gathering of System B.....	49
Table 4.9 Threat modeling of system B (Reflected XSS).....	50
Table 4.10 Automated Scanning Result of System B.....	52
Table 4.11 Manual Testing Result of System A (Reflected XSS).....	52
Table 4.12 Testing Summary Report of System B	53
Table 4.13 Intelligence Gathering of System C.....	53
Table 4.14 Threat Modeling of System C (Reflected XSS)	54
Table 4.15 Automated Testing Result of System C.....	56
Table 4.16 Manual Testing Result of System C (Reflected XSS)	56
Table 4.17 Exploitation of System C.....	57
Table 4.18 Report of System C (C.R01).....	60
Table 4.19 Report of System C (C.R03).....	60
Table 4.20 OWASP Risk Rating and Recommendation (C.R01).....	61
Table 4.21 OWASP Risk Rating and Recommendation (C.R03).....	73
Table 4.22 Intelligence Gathering of System D.....	85
Table 4.23 Threat Modeling of System D (Reflected XSS)	86
Table 4.24 Threat Modeling of System D (DOM-Based XSS)	86
Table 4.25 Automated Scanning Result of System D.....	87
Table 4.26 Manual Testing Result of System D.....	88

Table 4.27 Exploitation of System D.....	88
Table 4.28 Report of System D (D.R01)	90
Table 4.29 OWASP Risk Rating and Recommendation (D.R01).....	90
Table 4.30 Intelligence Gathering of System E.....	102
Table 4.31 Threat Modeling of System E (Reflected XSS).....	103
Table 4.32 Threat Modeling of System E (DOM-Based XSS)	104
Table 4.33 Automated Scanning Result of System E.....	106
Table 4.34 Manual Testing Result of System E.....	106
Table 4.35 Testing Summary Report of System E.....	107
Table 4.36 Intelligence Gathering of System F	107
Table 4.37 Threat Modeling of System F (Reflected XSS).....	108
Table 4.38 Threat Modeling of System F (DOM-Based XSS).....	109
Table 4.39 Automated Scanning Result of System F	110
Table 4.40 Manual Testing Result of System F.....	111
Table 4.41 Testing Summary Report of System F.....	111
Table 4.42 Intelligence Gathering of System G.....	112
Table 4.43 Threat Modeling of System G (Reflected XSS)	113
Table 4.44 Threat Modeling of System G (Stored XSS)	113
Table 4.45 Threat Modeling of System G (DOM-Based XSS)	114
Table 4.46 Automated Scanning Result of System G.....	115
Table 4.47 Manual Testing Result of System G (Reflected XSS)	116
Table 4.48 Manual Testing Result of System G (Stored XSS).....	117
Table 4.49 Testing Summary Report System G.....	118
Table 4.50 Intelligence Gathering of System H.....	118
Table 4.51 Threat Modeling of System H (Reflected XSS)	119
Table 4.52 Threat Modeling of System H (DOM-Based XSS)	120
Table 4.53 Automated Scanning Result of System H.....	121
Table 4.54 Manual Testing Result of System H (Reflected XSS)	122
Table 4.55 Testing Summary Report of System H.....	123
Table 4.56 Information Gathering of System I.....	123
Table 4.57 Threat Modeling of System I (Reflected XSS).....	124
Table 4.58 Threat Modeling of System I (Stored XSS).....	125

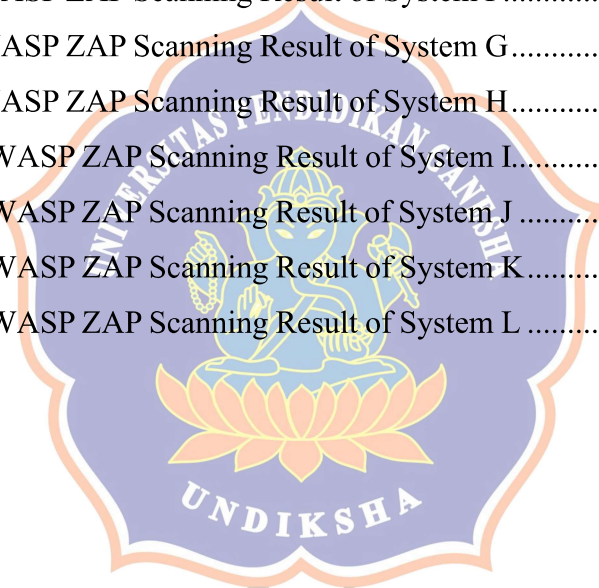
Table 4.59 Threat Modeling of System I (DOM-Based XSS).....	125
Table 4.60 Automated Scanning Result of System I	126
Table 4.61 Threat Modeling of System I (Reflected XSS).....	127
Table 4.62 Manual Testing Result of System I (Stored XSS)	127
Table 4.63 Exploitation of System I.....	128
Table 4.64 Testing Summary Report of System I (I.S01).....	131
Table 4.65 Testing Summary Report of System I (I.S02).....	131
Table 4.66 OWASP Risk Rating and Recommendation (I.S01)	132
Table 4.67 OWASP Risk Rating and Recommendation (I.S02)	143
Table 4.68 Intelligence Gathering of System J.....	154
Table 4.69 Threat Modeling of System J (Reflected XSS).....	155
Table 4.70 Threat Modeling of System J (Stored XSS)	156
Table 4.71 Threat Modeling of System J (DOM-Based XSS)	156
Table 4.72 Automated Scanning Result of System J.....	158
Table 4.73 Manual Testing Result of System J (Reflected XSS).....	159
Table 4.74 Manual Testing Result of System J (Stored XSS)	159
Table 4.75 Exploitation of System J.....	160
Table 4.76 Report of System J (J.R01).....	167
Table 4.77 Report of System J (J.R04).....	167
Table 4.78 Report of System J (J.S01)	168
Table 4.79 Report of System J (J.S02).....	168
Table 4.80 Report of System J (J.OS3)	168
Table 4.81 OWASP Risk Rating and Recommendation (J.R01).....	169
Table 4.82 OWASP Risk Rating and Recommendation (J.R04).....	180
Table 4.83 OWASP Risk Rating and Recommendation (J.S01)	191
Table 4.84 OWASP Risk Rating System J and Recommendation (J.S02).....	201
Table 4.85 OWASP Risk Rating and Recommendation (J.S03)	212
Table 4.86 Intelligence Gathering of System K.....	223
Table 4.87 Threat Modeling of System K (Reflected XSS)	224
Table 4.88 Threat Modeling of System K (Stored XSS)	225
Table 4.89 Threat Modeling of System K (DOM-Based XSS)	225
Table 4.90 Automated Scanning Result of System K.....	226

Table 4.91 Manual Testing Result of System K (Reflected XSS)	227
Table 4.92 Manual Testing of System K (Stored XSS)	227
Table 4.93 Exploitation of System K.....	228
Table 4.94 Testing Summary Report of System K (K.S03).....	230
Table 4.95 OWASP Risk Rating and Recommendation (K.S03).....	230
Table 4.96 Intelligence Gathering of System L.....	241
Table 4.97 Threat modeling of System L (Reflected XSS)	242
Table 4.98 Threat Modeling of System L (Blind Stored XSS).....	243
Table 4.99 Threat Modeling of System L (DOM-Based XSS).....	243
Table 4.100 Automated Scanning Result of System L	244
Table 4.101 Manual Testing Result of System L (Reflected XSS)	245
Table 4.102 Manual Testing Result of System L (Blind Stored XSS)	245
Table 4.103 Testing Summary Report of System L.....	246
Table 5.1 Overall Testing Summary Result.....	247



LIST OF FIGURES

Figure 3.1 Research Stage	29
Figure 3.2 Venn Diagram of Testing Target	31
Figure 3.3 Venn Diagram of Testing Approach	32
Figure 4.1 Legal Authorization of Penetration Testing	42
Figure 4.2 OWASP ZAP Scanning Result of System A	47
Figure 4.3 OWASP ZAP Scanning Result of System B	51
Figure 4.4 OWASP ZAP Scanning Result of System C	55
Figure 4.5 OWASP ZAP Scanning Result of System D	87
Figure 4.6 OWASP ZAP Scanning Result of System E	105
Figure 4.7 OWASP ZAP Scanning Result of System F	110
Figure 4.8 OWASP ZAP Scanning Result of System G	115
Figure 4.9 OWASP ZAP Scanning Result of System H	121
Figure 4.10 OWASP ZAP Scanning Result of System I	126
Figure 4.11 OWASP ZAP Scanning Result of System J	158
Figure 4.12 OWASP ZAP Scanning Result of System K	226
Figure 4.13 OWASP ZAP Scanning Result of System L	244



LIST OF APPENDICES

Appendix 01. Research Data Request Letter.....	266
Appendix 02. Research Data Request Letter.....	267
Appendix 03. Legal Authorization and Validation of Penetration Testing.....	268
Appendix 04. Documentation of Data Validation in UPA TIK.....	269
Appendix 05. Official Report Of Document Handover.....	272
Appendix 06. Curriculum Vitae	274

