

EVALUATION OF DATA CONFIDENTIALITY SECURITY USING THE OWASP ON THE XYZ WEB APPLICATION

SKRIPSI



**PROGRAM STUDI ILMU KOMPUTER (S1)
JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KEJURUAN
UNIVERSITAS PENDIDIKAN GANESHA**



- 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 VeryDS oleh BSrE
- Cetakan dokumen ini merupakan salinan dari file dokumen bertandatangan elektronik yang keabsahannya dapat diakses melalui scan QRCode yang terdapat pada sertifikat ini.



- 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 BSR E - BSSN, validitas dokumen elektronik ini bisa dicek menggunakan aplikasi mobile VeryDS oleh BSR E
- Cetakan dokumen ini merupakan salinan dari file dokumen bertandatangan elektronik yang keabsahannya dapat diakses melalui scan QRCode yang terdapat pada sertifikat ini.

SKRIPSI

DIAJUKAN UNTUK MELENGKAPI TUGAS DAN MEMENUHI SYARAT-SYARAT UNTUK MENCAPAI GELAR SARJANA KOMPUTER



| | |
|---------------|---|
| Pembimbing I | Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D. NIP.197803242005011001 |
| Pembimbing II | Ir. I Ketut Resika Arthana, S.T., M.Kom. NIP.198412012012121002 |

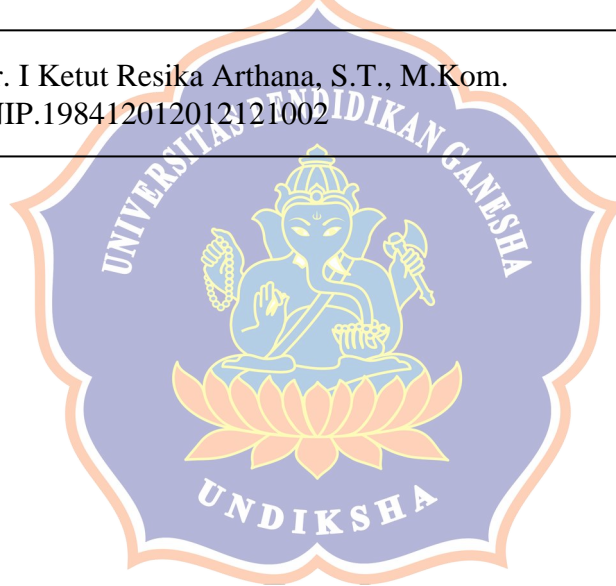


- UU ITE No. 11 Tahun 2008 Pasal 5 Ayat 1 "Informasi Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah"
- Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan BSrE - BSSN, validitas dokumen elektronik ini bisa dicek menggunakan aplikasi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

Skripsi oleh I Komang Wahyu Ambara Putra ini
telah dipertahankan di depan dewan penguji
Pada tanggal 23 April 2026

Dewan Penguji

| | |
|---------|---|
| Ketua | I Ketut Purnamawan, S.Kom., M.Kom. NIP.197905112006041004 |
| Anggota | Ir. Ketut Agus Seputra, S.ST.,M.T. NIP.199008152019031018 |
| Anggota | Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D. NIP.197803242005011001 |
| Anggota | Ir. I Ketut Resika Arthana, S.T., M.Kom. NIP.198412012012121002 |



- 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 VeryDS oleh BSrE
- Cetakan dokumen ini merupakan salinan dari file dokumen bertandatangan elektronik yang keabsahannya dapat diakses melalui scan QRCode yang terdapat pada sertifikat ini.

Diterima oleh Panitia Ujian Fakultas Teknik dan Kejuruan
Universitas Pendidikan Ganesha
guna memenuhi syarat-syarat untuk mencapai gelar Sarjana Komputer

Menyetujui

| | |
|------------------|---|
| Ketua Ujian | Ir. Made Windu Antara Kesiman, S.T., M.Sc., Ph.D. NIP.198211112008121001 |
| Sekretaris Ujian | I Nyoman Saputra Wahyu Wijaya, S.Kom., M.Cs. NIP.198910262019031004 |



- 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 VeryDS oleh BSrE
- Cetakan dokumen ini merupakan salinan dari file dokumen bertandatangan elektronik yang keabsahannya dapat diakses melalui scan QRCode yang terdapat pada sertifikat ini.

DECLARATION

I hereby declare that the written work titled "Evaluation of Data Confidentiality Security Using the OWASP on the XYZ Web Application" and its entirety are genuinely my original work, created without engaging in plagiarism or improper citation practices that violate the ethical standards of the scientific community. By making this declaration, I accept full responsibility for any sanctions that may be imposed if any violations of scientific ethics or challenges to the authenticity of my work are later discovered.

Singaraja, April 13, 2026

The one that makes a statement



I Komang Wahyu Ambara Putra
NIM 2215101055

FOREWORD

The author expresses highest gratitude to God Almighty for His blessings and grace, which enabled the author to complete this undergraduate thesis titled "Evaluation of Data Confidentiality Security Using the OWASP on the XYZ Web Application". This thesis is submitted to fulfill the requirements for obtaining a Bachelor's degree in Computer Science at Universitas Pendidikan Ganesha.

The author realizes that the completion of this thesis would not have been possible without the support, guidance, and assistance from various parties. Therefore, the author would like to express profound appreciation and gratitude to:

1. Prof. Dr. I Wayan Lasmawan, M.Pd., as the Rector of Universitas Pendidikan Ganesha, for providing the educational facilities and supportive environment at the university.
2. Prof. Dr. Kadek Rihendra Dantes, S.T., M.T., as the Dean of the Faculty of Engineering and Vocational, for the motivation and facilities provided within the faculty.
3. Dr. Putu Hendra Suputra, S.Kom., M.Cs., as the Head of the Informatics Engineering Department, for the guidance and departmental support.
4. I Nyoman Saputra Wahyu Wijaya, S.Kom., M.Cs., as the Coordinator of the Computer Science Study Program, for the motivation, facilities, and valuable inputs that contributed to improving this research.
5. Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D, as the first advisor and academic advisor, who has provided patience, motivation, continuous guidance, and direction to the author in completing this thesis.
6. Ir. I Ketut Resika Arthana, S.T., M.Kom., as the second advisor, who has given valuable advice, technical guidance, and motivation throughout the writing process.
7. I Ketut Purnamawan, S.Kom., M.Kom., as the first examiner, for the constructive feedback and suggestions that have significantly improved the quality of this research.
8. Ir. Ketut Agus Seputra, S.ST.,M.T., as the second examiner, who have provided valuable input and advice in improving the research conducted.

9. The Head and Staff of UPA TIK XYZ University, who provided the opportunity for the author to conduct the internship and research, as well as facilitated access to the system for testing purposes.
10. All lecturers in the Informatics Engineering Department and Computer Science Study Program for the knowledge and experience shared during the author's studies.
11. The author's beloved parents, I Nyoman Arsil and Desak Alit Malini, and the author's siblings, Ni Putu Poni Aprilia Cahya and I Kadek Angga Mahendra for their endless prayers, material support, and encouragement which served as the author's greatest motivation.
12. All friends from the Computer Science Class of 2022 for the togetherness, discussions, and support during college life.
13. All parties who have assisted the author, whom cannot be mentioned one by one.

The author acknowledges that this undergraduate thesis is far from perfect and may contain shortcomings due to the author's limited knowledge and experience. Therefore, constructive criticism and suggestions are highly appreciated to improve this work. Hopefully, this thesis will be beneficial for the development of science and for those who require it.

Singaraja, April 13, 2026

Author,

TABLE OF CONTENTS

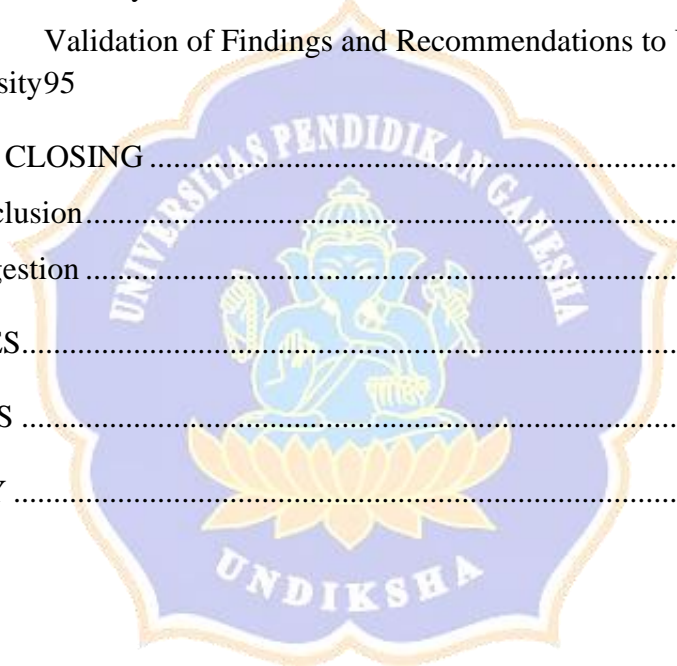
| | |
|---|------|
| FOREWORD | i |
| TABLE OF CONTENTS | iii |
| LIST OF TABLES | viii |
| LIST OF FIGURES | xi |
| LIST OF APPENDICES | xiii |
| CHAPTER I INTRODUCTION | 1 |
| 1.1 Background | 1 |
| 1.2 Research Scopes | 3 |
| 1.3 Research Questions | 3 |
| 1.4 Research Objectives | 3 |
| 1.5 Research Benefits | 4 |
| CHAPTER II LITERATURE REVIEW | 5 |
| 2.1 Related Research | 5 |
| 2.2 Information System | 8 |
| 2.3 CIA Triad | 9 |
| 2.4 Data Confidentiality | 10 |
| 2.5 Vulnerability | 11 |
| 2.6 OWASP | 11 |
| 2.7 OWASP WSTG | 12 |
| 2.8 OWASP Top 10 | 14 |
| 2.9 OWASP Risk Rating Methodology | 16 |
| 2.10 Authentication Testing | 22 |
| 2.11 Authorization Testing | 22 |
| 2.12 Session Management Testing | 23 |
| 2.13 Weak Cryptography Testing | 23 |
| 2.14 Grey Box Testing | 23 |
| CHAPTER III METHODOLOGY | 26 |
| 3.1 Research Approach | 26 |

| | | |
|--|---|----|
| 3.2 | Research Object and Focus | 26 |
| 3.3 | Research Stages | 26 |
| 3.3.1 | Tools Installation..... | 27 |
| 3.3.2 | Initial Analysis and Reconnaissance | 27 |
| 3.3.3 | System Testing Execution..... | 28 |
| 3.3.4 | Proof of Concept (PoC)..... | 32 |
| 3.3.5 | Documentation of Results | 32 |
| 3.3.6 | Vulnerability Evaluation | 32 |
| 3.4 | Data Collection Techniques | 35 |
| 3.5 | Research Timeline | 36 |
| CHAPTER IV RESULT AND DISCUSSION | | 39 |
| 4.1 | Initial Analysis and Reconnaissance | 39 |
| 4.1.1 | XYZ Web Application | 39 |
| 4.1.2 | ABC Web Application | 40 |
| 4.2 | System Testing Result | 40 |
| 4.2.1 | Authentication Testing | 40 |
| 4.2.2 | Authorization Testing..... | 44 |
| 4.2.3 | Session Management Testing..... | 46 |
| 4.2.4 | Weak Cryptography Testing | 50 |
| 4.2.5 | Recapitulation of System Testing Results..... | 51 |
| 4.3 | Vulnerability Proof of Concept (PoC)..... | 53 |
| 4.3.1 | Authentication Bypass via Logic Flaw in Parameter Validation in the Login Function of the XYZ Web Application | 54 |
| 4.3.2 | No Account Lockout Mechanism Allows Brute Force Attacks on the XYZ Web Application Login Function | 54 |
| 4.3.3 | IDOR in the Graduation Ticket Functionality of the XYZ Web Application..... | 55 |
| 4.3.4 | IDOR in the Final Project Topic Offering Details Functionality of the XYZ Web Application | 56 |
| 4.3.5 | IDOR in the Lecturer Performance Questionnaire Functionality of the XYZ Web Application | 57 |
| 4.3.6 | Improper Session Management Due to Failure of Server-Side Session Expiration Enforcement on the XYZ Web Application | 58 |

| | | |
|--------|---|----|
| 4.3.7 | Session Fixation in the CASAuth Cookie Parameters of the XYZ Web Application | 59 |
| 4.3.8 | Weak Account Lockouts Allowing Automatic and Manual Bypasses on the ABC Web Application | 60 |
| 4.3.9 | Broken Access Control in the Reset Password Function of the ABC Web Application | 61 |
| 4.3.10 | Password Changes Without Old Password Verification on the ABC Web Application | 62 |
| 4.3.11 | Old Password Reset Links Not Deactivated After Use on the ABC Web Application | 62 |
| 4.3.12 | Recapitulation of PoC Results | 63 |
| 4.4 | Categorizing Vulnerabilities on OWASP Top 10 | 63 |
| 4.5 | Vulnerability Risk Calculation Using OWASP Risk Rating | 65 |
| 4.5.1 | Authentication Bypass via Logic Flaw in Parameter Validation in the Login Function of the XYZ Web Application | 65 |
| 4.5.2 | No Account Lockout Mechanism Allows Brute Force Attacks on the XYZ Web Application Login Function | 66 |
| 4.5.3 | IDOR in the Graduation Ticket Functionality of the XYZ Web Application..... | 67 |
| 4.5.4 | IDOR in the Final Project Topic Offering Details Functionality of the XYZ Web Application | 68 |
| 4.5.5 | IDOR in the Lecturer Performance Questionnaire Functionality of the XYZ Web Application | 69 |
| 4.5.6 | Improper Session Management Due to Failure of Server-Side Session Expiration Enforcement on the XYZ Web Application | 71 |
| 4.5.7 | Session Fixation in the CASAuth Cookie Parameters of the XYZ Web Application | 72 |
| 4.5.8 | Weak Account Lockouts Allowing Automatic and Manual Bypasses on the ABC Web Application | 73 |
| 4.5.9 | Broken Access Control in the Reset Password Function of the ABC Web Application | 74 |
| 4.5.10 | Password Changes Without Old Password Verification on the ABC Web Application | 75 |
| 4.5.11 | Old Password Reset Links Not Deactivated After Use on the ABC Web Application | 76 |
| 4.5.12 | Recapitulation of Vulnerability Risk Calculation..... | 78 |

| | | |
|--------|---|----|
| 4.6 | Vulnerability Discussion | 79 |
| 4.6.1 | Authentication Bypass via Logic Flaw in Parameter Validation in the Login Function of the XYZ Web Application | 80 |
| 4.6.2 | No Account Lockout Mechanism Allows Brute Force Attacks on the XYZ Web Application Login Function | 81 |
| 4.6.3 | IDOR in the Graduation Ticket Functionality of the XYZ Web Application..... | 81 |
| 4.6.4 | IDOR in the Final Project Topic Offering Details Functionality of the XYZ Web Application | 82 |
| 4.6.5 | IDOR in the Lecturer Performance Questionnaire Functionality of the XYZ Web Application | 82 |
| 4.6.6 | Improper Session Management Due to Failure of Server-Side Session Expiration Enforcement on the XYZ Web Application | 83 |
| 4.6.7 | Session Fixation in the <i>CASAuth</i> Cookie Parameters of the XYZ Web Application | 83 |
| 4.6.8 | Weak Account Lockouts Allowing Automatic and Manual Bypasses on the ABC Web Application | 84 |
| 4.6.9 | Broken Access Control in the Reset Password Function of the ABC Web Application | 84 |
| 4.6.10 | Password Changes Without Old Password Verification on the ABC Web Application | 85 |
| 4.6.11 | Old Password Reset Links Not Deactivated After Use on the ABC Web Application | 85 |
| 4.7 | Formulation and Validation of Recommendations | 86 |
| 4.7.1 | Authentication Bypass via Logic Flaw in Parameter Validation in the Login Function of the XYZ Web Application | 86 |
| 4.7.2 | No Account Lockout Mechanism Allows Brute Force Attacks on the XYZ Web Application Login Function | 87 |
| 4.7.3 | IDOR in the Graduation Ticket Functionality of the XYZ Web Application..... | 88 |
| 4.7.4 | IDOR in the Final Project Topic Offering Details Functionality of the XYZ Web Application | 88 |
| 4.7.5 | IDOR in the Lecturer Performance Questionnaire Functionality of the XYZ Web Application | 89 |
| 4.7.6 | Improper Session Management Due to Failure of Server-Side Session Expiration Enforcement on the XYZ Web Application | 90 |

| | | |
|-------------------------|---|-----|
| 4.7.7 | Session Fixation in the <i>CASAuth</i> Cookie Parameters of the XYZ Web Application | 90 |
| 4.7.8 | Weak Account Lockouts Allowing Automatic and Manual Bypasses on the ABC Web Application | 91 |
| 4.7.9 | Broken Access Control in the Reset Password Function of the ABC Web Application | 92 |
| 4.7.10 | Password Changes Without Old Password Verification on the ABC Web Application | 93 |
| 4.7.11 | Old Password Reset Links Not Deactivated After Use on the ABC Web Application | 94 |
| 4.7.12 | Implications of Findings for the Information Systems Ecosystem at XYZ University | 94 |
| 4.7.13 | Validation of Findings and Recommendations to UPA TIK XYZ University | 95 |
| CHAPTER V CLOSING | | 96 |
| 5.1 | Conclusion | 96 |
| 5.2 | Suggestion | 96 |
| REFERENCES | | 99 |
| APPENDICES | | 103 |
| BIOGRAPHY | | 105 |



LIST OF TABLES

| | |
|---|----|
| Table 2.1 Related Research..... | 5 |
| Table 2.2 Threat Agent Factors (OWASP, 2023)..... | 17 |
| Table 2.3 Vulnerability Factors (OWASP, 2023)..... | 17 |
| Table 2.4 Technical Impact Factors (OWASP, 2023) | 19 |
| Table 2.5 Business Impact Factors (OWASP, 2023)..... | 20 |
| Table 3.1 Authentication Testing Aspects | 29 |
| Table 3.2 Authorization Testing Aspects..... | 30 |
| Table 3.3 Session Management Testing Aspects | 31 |
| Table 3.4 Weak Cryptography Testing Aspects | 32 |
| Table 3.5 Research Timeline..... | 37 |
| Table 4.1 Initial Analysis and Reconnaissance of XYZ Web Application..... | 39 |
| Table 4.2 Initial Analysis and Reconnaissance of ABC Web Application..... | 40 |
| Table 4.3 Recapitulation of Authentication Testing Results | 52 |
| Table 4.4 Recapitulation of Authorization Testing Results..... | 52 |
| Table 4.5 Recapitulation of Session Management Testing Results | 53 |
| Table 4.6 Recapitulation of Weak Cryptography Testing Results..... | 53 |
| Table 4.7 Recapitulation of PoC Results | 63 |
| Table 4.8 Vulnerability Categorization Based on OWASP Top 10..... | 63 |
| Table 4.9 Likelihood of Authentication Bypass via Logic Flaw in Parameter Validation in the Login Function of the XYZ Web Application | 65 |
| Table 4.10 Impact Factors of Authentication Bypass via Logic Flaw in Parameter Validation in the Login Function of the XYZ Web Application | 66 |
| Table 4.11 Likelihood of No Account Lockout Mechanism Allows Brute Force Attacks on the XYZ Web Application Login Function | 66 |
| Table 4.12 Impact Factors of No Account Lockout Mechanism Allows Brute Force Attacks on the XYZ Web Application Login Function | 67 |
| Table 4.13 Likelihood of IDOR in the Graduation Ticket Functionality of the XYZ Web Application | 68 |
| Table 4.14 Impact Factors of IDOR in the Graduation Ticket Functionality of the XYZ Web Application | 68 |

| | |
|--|----|
| Table 4.15 Likelihood of IDOR in the Final Project Topic Offering Details Functionality of the XYZ Web Application..... | 69 |
| Table 4.16 Impact Factors of IDOR in the Final Project Topic Offering Details Functionality of the XYZ Web Application..... | 69 |
| Table 4.17 Likelihood of IDOR in the Lecturer Performance Questionnaire Functionality of the XYZ Web Application..... | 70 |
| Table 4.18 Impact Factors of IDOR in the Lecturer Performance Questionnaire Functionality of the XYZ Web Application..... | 70 |
| Table 4.19 Likelihood of Improper Session Management Due to Failure of Server-Side Session Expiration Enforcement on the XYZ Web Application | 71 |
| Table 4.20 Impact Factors of Improper Session Management Due to Failure of Server-Side Session Expiration Enforcement on the XYZ Web Application | 71 |
| Table 4.21 Likelihood of Session Fixation in the <i>CASAuth</i> Cookie Parameters of the XYZ Web Application | 72 |
| Table 4.22 Impact Factors of Session Fixation in the <i>CASAuth</i> Cookie Parameters of the XYZ Web Application..... | 73 |
| Table 4.23 Likelihood of Weak Account Lockouts Allowing Automatic and Manual Bypasses on the ABC Web Application | 73 |
| Table 4.24 Impact Factors of Weak Account Lockouts Allowing Automatic and Manual Bypasses on the ABC Web Application | 74 |
| Table 4.25 Likelihood of Broken Access Control in the Reset Password Function of the ABC Web Application..... | 75 |
| Table 4.26 Impact Factors of Broken Access Control in the Reset Password Function of the ABC Web Application..... | 75 |
| Table 4.27 Likelihood of Password Changes Without Old Password Verification on the ABC Web Application | 76 |
| Table 4.28 Impact Factors of Password Changes Without Old Password Verification on the ABC Web Application..... | 76 |
| Table 4.29 Likelihood of Old Password Reset Links Not Deactivated After Use on the ABC Web Application | 77 |
| Table 4.30 Impact Factors of Old Password Reset Links Not Deactivated After Use on the ABC Web Application | 77 |

Table 4.31 Recapitulation of Vulnerability Risk Calculation..... 78
Table 4.32 Recapitulation of the root cause of each vulnerability..... 79



LIST OF FIGURES

| | |
|--|----|
| Figure 2.1 Block Image of Interacting Information Systems (Hutahaeen, 2015)... | 9 |
| Figure 2.2 Changes from OWASP Top 10 2017 to 2021 (OWASP, 2021) | 15 |
| Figure 2.3 Security Gap Risk Likelihood and Impact Level (OWASP, 2022)..... | 20 |
| Figure 2.4 Calculation of Threat Agent Factor and Vulnerability Factor (OWASP, 2023) | 21 |
| Figure 2.5 Calculation of Technical Impact and Business Impact (OWASP, 2023) | 21 |
| Figure 2.6 Security Gap Risk Calculation (OWASP, 2023)..... | 21 |
| Figure 3.1 Research Stages | 27 |
| Figure 3.2 Stages in Vulnerability Risk Calculation..... | 33 |
| Figure 3.3 Stages of Formulating and Validating Recommendations | 35 |
| Figure 4.1 Execute POST Request Login to XYZ Web Application..... | 54 |
| Figure 4.2 Execute POST Request Login to XYZ Web Application | 55 |
| Figure 4.3 Login Attempts Results | 55 |
| Figure 4.4 Running the Program in Command Prompt | 55 |
| Figure 4.5 Details of Topics Offered | 56 |
| Figure 4.6 Accessing Details of Topics Offered by Other Study Programs | 57 |
| Figure 4.7 Account A POST Request | 57 |
| Figure 4.8 Account A POST Request | 57 |
| Figure 4.9 Account B Lecturer Performance Questionnaire in Account A's Browser | 58 |
| Figure 4.10 <i>Expires / Max-Age</i> on Cookie <i>CASAuth</i> | 58 |
| Figure 4.11 Modification of <i>Expires / Max-Age</i> on Cookie <i>CASAuth</i> | 58 |
| Figure 4.12 Modification of <i>Expires / Max-Age</i> on <i>CASAuth</i> Cookie Remains Valid..... | 59 |
| Figure 4.13 Account A's <i>CASAuth</i> Before Change..... | 59 |
| Figure 4.14 Account A's <i>CASAuth</i> After Change | 59 |
| Figure 4.15 Account B's <i>CASAuth</i> After Change | 59 |
| Figure 4.16 Account B's <i>CASAuth</i> After Change | 60 |
| Figure 4.17 Request Execution | 60 |
| Figure 4.18 Results of Successful Login Attempts | 60 |

Figure 4. 19 Locked Login Attempt..... 61
Figure 4.20 POST Request Before Modification 61
Figure 4.21 POST Request After Modification 61
Figure 4.22 Changing the Password in the Profile Menu 62



LIST OF APPENDICES

| | |
|--|-----|
| Appendix 1. Graduation Ticket Download Automation Script | 103 |
| Appendix 2. Presentation of Findings to the UPA TIK XYZ University Programmer Team..... | 103 |
| Appendix 3. Research Permit Letter | 104 |

