



UNDERGRADUATE THESIS

**EVALUATION OF MAJADIGI WEB APPLICATION
VULNERABILITIES BASED ON VAPT
FRAMEWORK WITH MITRE ATT&CK MAPPING
AND CVSS ASSESSMENT**

BELIA PUTRI SALSABILA
NPM 22081010311

THESIS ADVISORS

Henni Endah Wahanani, ST. M.Kom
Achmad Junaidi, S.Kom., M.Kom

**MINISTRY OF HIGHER EDUCATION, SCIENCE, AND TECHNOLOGY
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAWA TIMUR
FACULTY OF COMPUTER SCIENCE
INFORMATICS STUDY PROGRAM
SURABAYA
2026**

APPROVAL SHEET

EVALUATION OF MAJADIGI WEB APPLICATION VULNERABILITIES BASED ON VAPT FRAMEWORK WITH MITRE ATT&CK MAPPING AND CVSS ASSESSMENT

By:
BELIA PUTRI SALSABILA
NPM. 22081010311

Has been defended before, and accepted by, the Board of Assessors of the Thesis Examination of the Informatics Study Program, Faculty of Computer Science, Universitas Pembangunan Nasional Veteran Jawa Timur, on May 22, 2026:

Approved,

Henni Endah Wahanani, ST. M.Kom
NIP. 19780922 202121 2 005


.....

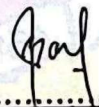
(Advisor I)

Achmad Junaidi, S.Kom., M.Kom.
NIP. 19781110 202521 1 048


.....

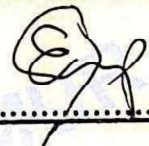
(Advisor II)

Made Hanindia Prami Swari, S.Kom, M.Cs
NIP. 19800205 201803 2 001


.....

(Head Assessor)

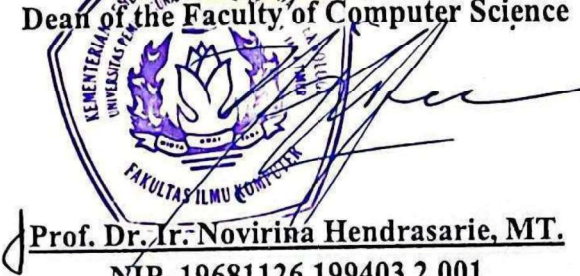
Eka Prakarsa Mandyartha, S.T., M.Kom
NIP. 19880525 201803 1 001


.....

(Assessor I)

Acknowledge by,

Dean of the Faculty of Computer Science


.....

Prof. Dr. Ir. Novirina Hendrasarie, MT.
NIP. 19681126 199403 2 001

APPROVAL SHEET

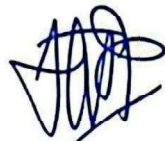
**EVALUATION OF MAJADIGI WEB APPLICATION
VULNERABILITIES BASED ON VAPT FRAMEWORK WITH MITRE
ATT&CK MAPPING AND CVSS ASSESSMENT**

By:
BELIA PUTRI SALSABILA
NPM. 22081010311

Approved to proceed to the Thesis Examination

Approved by,

**Coordinator of Informatics Study Program
Faculty of Computer Science**



Dr. Intan Yuniar Purbasari, S.Kom. MSc.

NIP. 19800602 202521 2 029

STATEMENT OF ORIGINALITY

I am the undersigned:

Student Name : Belia Putri Salsabila
NPM : 22081010311
Degree Program : Bachelor (S1)
Study Program : Informatics
Faculty : Faculty of Computer Science

Hereby declares that this undergraduate thesis contains no part of any other scientific work that has been submitted to obtain an academic degree at any higher education institution. Furthermore, it does not contain any work or opinions previously written or published by others, except for those which are explicitly cited in this thesis and listed completely in references.

And I declare that this scientific document is free from elements of plagiarism. If in the future indications of plagiarism are found in this Thesis, I am willing to accept sanctions in accordance with the applicable laws and regulations.

Thus, I made this statement without any coercion from anyone and to be used as it should.



Surabaya, June 08, 2026
Declarant,



BELIA PUTRI SALSABILA
NPM. 22081010311

ABSTRACT

Student Name / NPM : Belia Putri Salsabila/22081010311
Thesis Title : Evaluation of MAJADIGI Web Application Vulnerabilities Based on VAPT Framework with MITRE ATT&CK Mapping and CVSS Assessment
Supervisor : 1. Henni Endah Wahanani, ST. M.Kom
2. Achmad Junaidi, S.Kom., M.Kom

Cybersecurity threats against e-government portals continue to escalate, yet integrated security evaluations of public service systems in Indonesia remain scarce. MAJADIGI (majadigi.jatimprov.go.id), a web application owned by the Department of Communication and Informatics of East Java Province, serves as a Single Sign-On portal managing citizen's personal data through a centralized authentication service, yet has never undergone systematic security assessment.

This study proposes an integrated evaluation approach combining Vulnerability Assessment and Penetration Testing (VAPT) with MITRE ATT&CK Enterprise mapping and CVSS v3.1 scoring simultaneously a combination that has rarely been applied to provincial-level e-government systems. Grey-box testing was conducted under official authorization from the East Java Provincial Department of Communication and Informatics using OWASP ZAP, Nessus, Burp Suite, SQLmap, Nmap, and several supporting tools.

Values of the 12 vulnerability indications detected, manual validation confirmed 9 True Positives distributed across three OWASP Top 10:2021 categories: A05:2021-Security Misconfiguration in 6 findings, A01:2021-Broken Access Control in 2 findings, and A07:2021-Identification and Authentication Failures in 1 finding. MITRE ATT&CK mapping identified two interconnected attack chains, while CVSS v3.1 scoring yielded a score range of 4.3-6.9 at Medium risk level. The JWT in Browser localStorage finding, with a score of 6.9, was designated the highest mitigation priority due to its potential to expose user's personal data protected under Indonesian Law No. 27 of 2022 on Personal Data Protection. The results demonstrate that the integrated approach produces a more comprehensive security evaluation compared to single-framework methods, while also generating structured and technically validated mitigation recommendations.

Keywords: VAPT, OWASP Top 10:2021, MITRE ATT&CK, CVSS v3.1, web application security, e-government

ACKNOWLEDGEMENTS

Praise and gratitude be to Allah SWT for His grace, mercy, and ease granted throughout this journey, enabling the author to complete this thesis titled **“Evaluation of MAJADIGI Web Application Vulnerabilities Based on VAPT Framework with MITRE ATT&CK Mapping and CVSS Assessment.”** This thesis is submitted as a partial fulfillment of the requirements for the degree of Bachelor of Computer Science at the Informatics Study Program, Faculty of Computer Science, Universitas Pembangunan Nasional “Veteran” East Java.

The author recognizes that this work could not have been accomplished without the involvement, guidance, and support of many parties. With great sincerity, the author would like to extend heartfelt gratitude to:

1. Mrs. Prof. Dr. Ir. Novirina Hendrasarie, M.T., Dean of the Faculty of Computer Science, Universitas Pembangunan Nasional “Veteran” East Java, for providing the academic policies, facilities, and a conducive environment that have supported students throughout their studies.
2. Mrs. Dr. Intan Yuniar Purbasari, S.Kom., M.Sc., Coordinator of the Informatics Study Program, Faculty of Computer Science, Universitas Pembangunan Nasional “Veteran” East Java, for her direction and dedication in maintaining the academic standards of the program.
3. Mrs. Henni Endah Wahanani, S.T., M.Kom., Thesis Advisor I, who with great patience and diligence has devoted her time to providing guidance, constructive feedback, and both technical and methodological direction that have been invaluable in the development and completion of this research.
4. Mr. Achmad Junaidi, S.Kom., M.Kom., Thesis Advisor II, for his critical perspective, thoughtful suggestions, and consistent encouragement that have meaningfully contributed to the quality of this research.
5. Mrs. Made Hanindia Prami Swari, S.Kom., M.Cs., Head Assessor, for her thorough evaluation and scholarly input during the examination process, which helped sharpen the depth and rigor of this thesis.

6. Mr. Eka Prakarsa Mandyartha, S.T., M.Kom., Assessor I, for his critical questioning and substantive recommendations that strengthened the analytical framework and overall structure of this thesis.
7. Mr. Andreas Nugroho Sihananto, S.Kom., M.Kom. and the entire Thesis PIC team, for their coordination, administrative support, and assistance that ensured the thesis process ran smoothly and in an orderly manner.
8. All lecturers and staff of Universitas Pembangunan Nasional “Veteran” East Java, whose dedication in sharing knowledge and providing academic services has been an important foundation throughout the author’s years of study.
9. The author’s beloved Mother and Father, who have been the greatest source of strength and steadiness throughout this entire journey. Every prayer offered in the quiet hours of the night, every small question asked about progress and well-being, and every sacrifice made without a word of complaint has amounted to a support that cannot be measured or repaid. The author may never be able to return all that has been given, except by continuing to grow and to give the very best in return.
10. The author’s beloved younger sister and younger brother, and the extended family, whose presence and encouragement whether through a short message, a moment of laughter, or simply being there have always served as a quiet reminder that there is a far greater reason behind every effort the author has chosen to keep making, especially on the days when moving forward felt difficult.
11. Moch. Wahyu Sampurno Utomo, a partner whose sincerity, patience, and care have accompanied the author through every phase of this research through the most demanding and uncertain moments, and through the quieter ones alike. His presence during this process has been one of the things the author is most grateful for.
12. Densus, Fat Free, BLJ Naraya and Kriya Vikas HIMATIFA, and Zfordda, for the shared experiences, laughter, and support that have colored the author’s days throughout university life. The time spent together in the midst of working through things and in the moments of simply being present for one another is a part of this journey that the author will carry with genuine gratitude.

The author acknowledges that this thesis is not without limitations. Constructive criticism and suggestions are sincerely welcomed for the purpose of future improvement. It is hoped that this thesis may offer a meaningful contribution to the field of cybersecurity research and serve as a useful reference for readers and researchers with shared interests in the subject.

Surabaya, May 19th 2026

Author

TABLE OF CONTENTS

APPROVAL SHEET	i
APPROVAL SHEET	ii
STATEMENT OF ORIGINALITY	iii
ABSTRACT	iv
ACKNOWLEDGEMENTS.....	v
TABLE OF CONTENTS.....	viii
LIST OF FIGURES	xiii
LIST OF TABLES	xvii
CHAPTER I INTRODUCTION.....	1
1.1. Background	1
1.2. Problem Formulation.....	4
1.3. Research Objectives	4
1.4. Research Benefits	5
1.5. Research Limitations.....	5
CHAPTER II LITERATURE REVIEW	7
2.1. Previous Studies	7
2.2. Overview of the Institution	9
2.2.1. Institutional Profile.....	9
2.2.2. Organizational Structure	11
2.3. Vulnerability Assessment and Penetration Testing (VAPT).....	12
2.3.1. Vulnerability Assessment.....	14
2.3.2. Penetration Testing.....	14
2.4. MITRE ATT&CK.....	15

2.4.1. Structure of MITRE ATT&CK.....	16
2.4.2. MITRE ATT&CK Domains.....	17
2.4.3. Tactics in MITRE ATT&CK Enterprise.....	17
2.4.4. Mitigations dalam MITRE ATT&CK.....	18
2.5. CIA Triad	18
2.6. Google Dorking.....	19
2.7. OWASP Top 10	20
2.7.1. A01:2021-Broken Access Control	21
2.7.2. A02:2021- Cryptographic Failures.....	21
2.7.3. A03:2021 - Injection	21
2.7.4. A04:2021 - Insecure Design.....	22
2.7.5. A05:2021 - Security Misconfiguration	22
2.7.6. A06:2021 - Vulnerable and Outdated Components	22
2.7.7. A07:2021 - Identification and Authentication Failures.....	23
2.7.8. A08:2021 - Software and Data Integrity Failures	23
2.7.9. A09:2021 - Security Logging and Monitoring Failures.....	23
2.7.10. A10:2021 - Server-Side Request Forgery (SSRF)	23
2.8. OWASP Cheat Sheet Series.....	23
2.9. Common Weakness Enumeration (CWE).....	24
2.10. Common Vulnerabilities and Exposures (CVE).....	24
2.11. Common Vulnerability Scoring System (CVSS).....	25
2.11.1. Components of the Common Vulnerability Scoring System (CVSS)	26
2.12. Tools and Utilities	31
2.12.1. Kali Linux	31
2.12.2. Wappalyzer.....	32

2.12.3. Owasp ZAP	33
2.12.4. Nessus.....	33
2.12.5. SQLmap	34
2.12.6. Nmap	35
2.12.7. BurpSuite.....	35
2.12.8. Whois	36
2.12.9. Nslookup	36
2.12.10. Dirsearch	37
2.12.11. cURL	37
2.12.12. Webhook.Site	38
CHAPTER III SYSTEM DESIGN AND IMPLEMENTATION	40
3.1 Research Methodology.....	40
3.2 Planning & Scope.....	43
3.2.1. Research Objects	44
3.2.2. System Design.....	45
3.3. Information Gathering.....	46
3.4. Vulnerability Scanning.....	49
3.5. Validation & Controlled Exploitation	56
3.6. Vulnerability Analyze	62
3.7. Reporting & Mitigation Recommendation.....	66
CHAPTER IV TESTING AND ANALYSIS	69
4.1. Planning & Scope Results.....	69
4.2. Information Gathering Results	70
4.2.1. Wappalyzer.....	71
4.2.2. Nslookup	74
4.2.3. Whois	75

4.2.4. Google Dorking.....	77
4.2.5. Nmap	79
4.2.6. Dirsearch	80
4.3. Vulnerability Scanning Results.....	82
4.4. Validation & Controlled Exploitation Results	84
4.4.1. Finding #1 SQL Injection.....	85
4.4.2. Finding #2 SQL Injection - SQLite (Time Based).....	88
4.4.3. Finding #3 Absence of Anti-CSRF Tokens	89
4.4.4. Finding #4 CSP: Failure to Define Directive with No Fallback	99
4.4.5. Finding #5 CSP: Wildcard Directive	106
4.4.6. Finding #6 CSP: script-src unsafe-inline	112
4.4.7. Finding #7 CSP: style-src unsafe-inline.....	118
4.4.8. Finding #8 Content Security Policy (CSP) Header Not Set.....	124
4.4.9. Finding #9 Cross-Domain Misconfiguration	130
4.4.10. Finding #10 Information Disclosure - JWT in Browser localStorage	136
4.4.11. Finding #11 Missing Anti-clickjacking Header	141
4.4.12. Finding #12 Session ID in URL Rewrite	146
4.4.13. Validation Results Summary.....	150
4.5. Vulnerability Analyze Results	154
4.5.1. Classification Recapitulation Based on OWASP Top 10:2021 and CWE- ID.....	154
4.5.2. MITRE ATT&CK Mapping Recapitulation	156
4.5.3. CVSS v3.1 Assessment Recapitulation.....	159
4.6. Reporting & Mitigation Recommendation Results.....	160
4.6.1. High Priority.....	164
4.6.2. Medium Priority	166

4.6.3. Normal Priority	190
4.6.4. Mitigation Recommendation Testing Results	193
CHAPTER V CONCLUSION	197
5.1. Conclusion.....	197
5.2. Recommendations for Future Development	199
BIBLIOGRAPHY	201
APPENDIX	207

LIST OF FIGURES

Figure 2. 1 East Java Diskominfo Logo.....	10
Figure 2. 2 Organizational Structure of East Java Diskominfo.....	11
Figure 2. 3 CIA Triad.....	19
Figure 2. 4 OWASP Top 10 differences 2017 vs 2021.....	20
Figure 2. 5 Base Score Calculator CVSS 3.1.....	26
Figure 2. 6 Temporal Score Calculator CVSS 3.1.....	29
Figure 2. 7 Environmental Metrics Calculator CVSS 3.1.....	30
Figure 2. 8 Kali Linux Logo.....	32
Figure 2. 9 Wappalyzer Logo.....	32
Figure 2. 10 OWASP ZAP Logo.....	33
Figure 2. 11 Nessus Logo.....	34
Figure 2. 12 Sqlmap Logo.....	34
Figure 2. 13 Nmap logo.....	35
Figure 2. 14 BurpSuite Logo.....	36
Figure 2. 15 Whois Logo.....	36
Figure 2. 16 Nslookup Logo.....	37
Figure 2. 17 Dirsearch Logo.....	37
Figure 2. 18 cURL Logo.....	38
Figure 2. 19 Page Webhook.Site.....	38
Figure 3. 1 Research Flowchart.....	41
Figure 3. 2 Mitre Att&ck Mapping.....	42
Figure 3. 3 Main Portal of MAJADIGI Website.....	45
Figure 3. 4 Use Case Diagram Website MAJADIGI.....	46
Figure 3. 5 OWASP ZAP Results.....	50
Figure 3. 6 Nessus Results.....	53
Figure 3. 7 Mapping of vulnerability risk analysis results.....	63
Figure 3. 8 CVSS v3.1 Base Score Calculator.....	65
Figure 3. 9 Structure of the Mitigation Recommendation Report.....	66
Figure 4. 1 Wappalyzer Results.....	72

Figure 4. 2 Nslookup Results	74
Figure 4. 3 Whois Results	76
Figure 4. 4 Google Dorking Validation Results.....	78
Figure 4. 5 Nmap Scan Results	79
Figure 4. 6 Dirsearch Results	81
Figure 4. 7 Favicon Directory Validation Results.....	81
Figure 4. 8 Contents of the Favicon Directory.....	82
Figure 4. 9 Test the cURL Baseline with API Key	85
Figure 4. 10 Response Baseline - HTTP 200 with News Data	86
Figure 4. 11 Error-Based Test with Single Quote.....	86
Figure 4. 12 Boolean-Based TRUE/FALSE Test	87
Figure 4. 13 SQLmap Scan Results	87
Figure 4. 14 SQLmap Results Details - All Not Injectable Parameters.....	87
Figure 4. 15 Time-Based Blind Test	88
Figure 4. 16 SSO Authentication Endpoint GET and Response Header Response	90
Figure 4. 17 Confirmation of the Absence of CSRF Token on the HTML Response Form Login SSO	91
Figure 4. 18 POST Request to SSO Authentication Endpoint.....	92
Figure 4. 19 CSRF PoC Generator on Burp Suite.....	93
Figure 4. 20 CSRF PoC Execution from External Domains.....	94
Figure 4. 21 CSRF PoC Results	95
Figure 4. 22 CVSS v3.1 Score Assessment on Absence of Anti-CSRF Tokens ..	97
Figure 4. 23 GET Request to SSO Authentication Endpoint.....	99
Figure 4. 24 CSP Header Response on SSO Login Page.....	100
Figure 4. 25 Simulating Attacks on CSP Failure	101
Figure 4. 26 Confirmation of Data Receipt on Webhook.site.....	102
Figure 4. 27 CVSS Score Assessment v3.1 on CSP No Fallback.....	104
Figure 4. 28 CSP Header Response on SSO Login Page.....	106
Figure 4. 29 Example of External Resource Proof on SSO Login Page	108
Figure 4. 30 Simulation Results of External Script Loading from SSO Page	109
Figure 4. 31 CVSS Score Assessment v3.1 on CSP Wildcard Directive	110

Figure 4. 32 Confirm Active Script Blocks on the HTML Response SSO Login Page	113
Figure 4. 33 Inline Script Injection Simulation Results	114
Figure 4. 34 Web Elements of Injection Simulation Results	115
Figure 4. 35 CVSS v3.1 Score Assessment on unsafe-inline script-src CSP.....	117
Figure 4. 36 Confirm Inline Style and External Stylesheet	119
Figure 4. 37 Inline Style Injection Simulation Results	120
Figure 4. 38 CVSS v3.1 Score Assessment on CSP style-src unsafe-inline.....	122
Figure 4. 39 CSP validation on the Endpoint account list	124
Figure 4. 40 Validate the Consistency of the Absence of CSP on Multiple Endpoints	125
Figure 4. 41 Simulation Results of Three Vector Attacks on the Main Domain	126
Figure 4. 42 Confirmation of Data Receipt on Webhook.site.....	127
Figure 4. 43 Simulated Web Elements on the Main Domain.....	127
Figure 4. 44 CVSS v3.1 Score Assessment on CSP Header Not Set.....	129
Figure 4. 45 Request GET ke Endpoint API /menu-footer	131
Figure 4. 46 Response API with CORS Header	131
Figure 4. 47 Results of Simulation of Cross-Origin Request to MAJADIGI API	133
Figure 4. 48 CVSS v3.1 Score Assessment on Cross-Domain Misconfiguration	134
Figure 4. 49 JWT Token on the localStorage Browser	136
Figure 4. 50 JWT Token Structure of localStorage	137
Figure 4. 51 JWT Token Header Analysis.....	137
Figure 4. 52 JWT Token Payload Analysis User Data	138
Figure 4. 53 CVSS v3.1 Score Assessment on JWT in Browser localStorage ...	139
Figure 4. 54 Validate Header Response Consistency on Two Endpoints	142
Figure 4. 55 Page View Before Clickjacking Simulation	143
Figure 4. 56 Views After Clickjacking Simulation.....	143
Figure 4. 57 CVSS v3.1 Score Assessment on Missing Anti-clickjacking Header	145
Figure 4. 58 OWASP ZAP Detected Parameters.....	147

Figure 4. 59 Simulating the Use of Tokens from URLs	148
Figure 4. 60 Token Simulation Results.....	149
Figure 4. 61 Distribution of Validation Results of 12 Vulnerability Findings ...	151
Figure 4. 62 Distribution of Validation Results by Top 10:2021 OWASP Categories	151
Figure 4. 63 Mitigation Priority Distribution	161
Figure 4. 64 Distribution of Mitigation Priorities and CVSS Scores Finding	161
Figure 4. 65 Code Before Implementation on AdonisJS (HttpOnly Cookie)	193
Figure 4. 66 Code After Implementation on AdonisJS (HttpOnly Cookie)	193
Figure 4. 67 Code Before Implementation on JavaScript Storage Logic.....	194
Figure 4. 68 Code After Implementation on JavaScript Storage Logic	194
Figure 4. 69 Simulation Results Before Mitigation Implementation	194
Figure 4. 70 Simulation Results After Mitigation Implementation	195

LIST OF TABLES

Table 2. 1 CVSS v3.1 Rating Categories and Scores.....	25
Table 3. 1 Integration of Frameworks within the Security Evaluation Framework	42
Table 3. 2 Information and Data Collection Planning	47
Table 3. 3 Summary of OWASP ZAP Findings and OWASP Top 10:2021 Classification.....	51
Table 3. 4 Summary of Nessus Essentials Findings.....	54
Table 3. 5 List of Indicated Vulnerabilities for Validation.....	56
Table 3. 6 Validation & Controlled Exploitation Design.....	58
Table 3. 7 Vulnerability Mapping Design to MITRE ATT&CK Enterprise	60
Table 3. 8 CVSS v3.1 Metrics and Their Implementation in This Research.....	64
Table 3. 9 Structure of the Security Evaluation Report	67
Table 4. 1 Testing Scope.....	69
Table 4. 2 System Technology Scanning Results Using Wappalyzer	72
Table 4. 3 Nslookup Results	74
Table 4. 4 System Infrastructure Scan Results Using Whois.....	76
Table 4. 5 Google Dorking Parameter Results.....	78
Table 4. 6 Nmap Results	80
Table 4. 7 Dirsearch Results	81
Table 4. 8 Comparison of Time-Based SQLi Testing Responses.....	89
Table 4. 9 CVSS v3.1 Assessment Details - Absence of Anti-CSRF Tokens	97
Table 4. 10 Analysis of CSP Directives Without Fallback	100
Table 4. 11 CVSS v3.1 Assessment Details - CSP: Failure to Define Directive with No Fallback	104
Table 4. 12 CSP Wildcard Directive Analysis.....	107
Table 4. 13 Detailed CVSS v3.1 Assessment for CSP: Wildcard Directive.....	111
Table 4. 14 CVSS v3.1 Scoring Details - CSP: script-src unsafe-inline.....	117
Table 4. 15 Detailed CVSS v3.1 Assessment - CSP: style-src unsafe-inline	122

Table 4. 16 Detailed CVSS v3.1 Assessment - Content Security Policy (CSP) Header Not Set	129
Table 4. 17 CORS Configuration Analysis.....	132
Table 4. 18 CVSS v3.1 Scoring Details - Cross-Domain Misconfiguration.....	134
Table 4. 19 CVSS v3.1 Scoring Details - Information Disclosure: JWT in Browser localStorage.....	140
Table 4. 20 Anti-Clickjacking Header Analysis on MAJADIGI Endpoints.....	142
Table 4. 21 CVSS v3.1 Scoring Details - Missing Anti-clickjacking Header	145
Table 4. 22 Analysis of Google Analytics Request Parameters.....	147
Table 4. 23 Summary of Validation Results	152
Table 4. 24 Classification Recapitulation Based on OWASP Top 10:2021 and CWE-ID	155
Table 4. 25 MITRE ATT&CK Mapping Recapitulation.....	157
Table 4. 26 CVSS v3.1 Assessment Recapitulation.....	159
Table 4. 27 Mitigation Priority of Findings	162
Table 4. 28 Disclosure of Mitigation Recommendation Information - JWT in the localStorage Browser	165
Table 4. 29 CSP Header Not Set Mitigation Recommendations	167
Table 4. 30 CSP Mitigation Recommendations: unsafe-inline script-src	170
Table 4. 31 CSP Mitigation Recommendations: style-src unsafe-inline	174
Table 4. 32 CSP Mitigation Recommendations: No Fallback Directive	176
Table 4. 33 CSP Mitigation Recommendations: Wildcard Directive	180
Table 4. 34 Recommendations for Mitigating the Absence of Anti-CSRF Tokens	184
Table 4. 35 Missing Anti-clickjacking Header Mitigation Recommendations...	188
Table 4. 36 Recommendations for Mitigating Cross-Domain Misconfiguration	191