



UNDERGRADUATE THESIS

SECURITY ANALYSIS USING THE HYBRID OWASP AND NIST SP 800-115 METHOD IN THE EAST JAVA DISKOMINFO SUBDOMAIN

MOCH WAHYU SAMPURNO UTOMO

NPM 22081010046

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

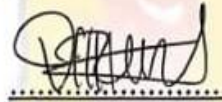
**SECURITY ANALYSIS USING THE HYBRID OWASP AND NIST SP 800-115
METHOD IN THE EAST JAVA DISKOMINFO SUBDOMAIN**

By :
MOCH WAHYU SAMPURNO UTOMO
NPM. 22081010046

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 April 22, 2026:

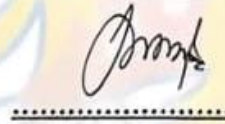
Approved,

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



(Advisor I)

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



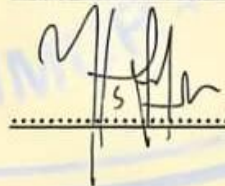
(Advisor II)

Eva Yulia Puspaningrum, S.Kom., M.Kom
NIP.19890705 202121 2 002



(Head Assessor)

Yisti Vita Via, S.ST., M.Kom.
NIP.19860425 202121 2 001



(Assessor I)

Acknowledge by,

Dean of the Faculty of Computer Science



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

APPROVAL SHEET

**SECURITY ANALYSIS USING THE HYBRID OWASP AND NIST SP 800-115
METHOD IN THE EAST JAVA DISKOMINFO SUBDOMAIN**

By:
MOCH WAHYU SAMPURNO UTOMO
NPM. 22081010046

Approved to proceed to the Thesis Examination

Approved by,

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



Dr. Intan Yuniar Purbasari, S.Kom., M.Sc
NIP.198006022 025212 029

STATEMENT OF ORIGINALITY

I am the undersigned:

Student Name : Moch Wahyu Sampurno Utomo
NPM : 22081010046
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, April 22, 2026
Declarant,



Moch Wahyu Sampurno Utomo
NPM. 22081010046

ABSTRACT

Student Name / NPM: Moch Wahyu Sampurno Utomo/22081010046
Thesis Title: SECURITY ANALYSIS USING THE HYBRID OWASP
AND NIST SP 800-115 METHOD IN THE EAST JAVA
DISKOMINFO SUBDOMAIN
Supervisor: 1. Henni Endah Wahanani, ST., M.Kom
2. Achmad Junaidi, S.Kom., M.Kom

Government agencies' increasing reliance on web technology has raised the risk of cyber threats. According to the 2023 report from the National Cyber and Crypto Agency, Indonesia experienced more than 370 million cyber incidents in 2022, with government institutions among the primary targets. This study aims to identify security vulnerabilities, evaluate security control compliance, and provide mitigation recommendations for the website of the Trenggalek Regional Forest Service Branch under Dinas Komunikasi dan Informatika of East Java Province.

This research applies a grey-box penetration testing approach using a hybrid framework that integrates OWASP Top Ten 2021, OWASP WSTG, OWASP ASVS Level 2, NIST SP 800-115, and CVSS v3.1. The testing process consists of Planning, Discovery, Attack, and Reporting stages. Tools used include Nmap, Burp Suite, SQLMap, OWASP ZAP, Nuclei, and Wappalyzer.

The results identified ten vulnerabilities mapped to the OWASP Top Ten 2021 categories. High-risk vulnerabilities were found in Broken Access Control, Cryptographic Failures, Identification and Authentication Failures, Software and Data Integrity Failures, and Security Logging and Monitoring Failures, with CVSS scores ranging from 7.3 to 8.8. Medium-risk vulnerabilities were also identified in several categories. This study demonstrates that the proposed hybrid framework provides a comprehensive and systematic approach for evaluating government website security.

Keywords: *penetration testing, web application security, OWASP, NIST SP 800-115, CVSS, Diskominfo Jawa Timur, grey-box testing.*

ACKNOWLEDGEMENTS

Praise be to Allah SWT for all His graces, guidance, and gifts to the author so that the thesis proposal with the title "**SECURITY ANALYSIS USING THE HYBRID OWASP AND NIST SP 800-115 METHOD IN THE EAST JAVA DISKOMINFO SUBDOMAIN** " can be completed properly.

The author would like to thank Mrs. Henni Endah Wahanani, ST. M.Kom as Supervisor I and Mr. Achmad Junaidi, S.Kom., M.Kom. as Supervisor 2 who are willing to take their time to provide guidance, advice and motivation to the author. In addition, during the preparation of the thesis proposal, the author also received a lot of assistance from various parties. For this the author would like to thank the:

1. Mrs. Prof. Dr. Ir. Novirina Hendrasarie, M.T. as the Dean of the Faculty of Computer Science, National Development University "Veteran" East Java.
2. Mrs. Dr. Intan Yuniar Purbasari, S.Kom., M.Sc. as the Coordinator of the Informatics Study Program, Faculty of Computer Science, National Development University "Veteran" East Java.
3. Mrs. Fetty Tri Anggraeny, S.Kom., M.Kom. as the author's academic advisor, who has provided guidance, motivation, support, and attention throughout the author's academic journey.
4. All lecturers of the Data Science and Informatics Study Program, National Development University "Veteran" East Java, for their knowledge, guidance, valuable experiences, and life lessons throughout the author's education.
5. The author's beloved parents, who have become the greatest reason for the author to keep striving and moving forward until this point. Thank you for the endless love, prayers, sacrifices, moral and financial support, and sincerity that can never be repaid. Thank you for always being a place to return to, a source of comfort, and the greatest strength whenever the author felt tired and almost gave up. This achievement is dedicated to both of them.
6. The author's beloved younger brother, Bayu, for always providing encouragement, support, and happiness throughout the author's college years and thesis completion process. His presence and care mean so much to the author.
7. The author's cousins Pretty, Betty, and Renty, who have continuously provided support, motivation, care, and encouragement throughout the author's academic journey and thesis completion.
8. Belia Putri Salsabila, who has always accompanied the author through every situation during the thesis process. Thank you for the patience, support, help,

care, and time given to the author. Thank you for always being there whenever the author felt exhausted, confused, and close to giving up.

9. The Densus family, namely Mas Bregas, Basroil, Paskal, Kadek, Manda, Stefi, and Hanna, for being part of the author's college journey. Thank you for the togetherness, support, laughter, assistance, and encouragement that made this long journey feel lighter and more memorable.
10. Ibnu, the author's best friend and companion since junior high school, who has always provided support, help, and encouragement throughout various phases of life until the completion of this thesis.
11. The Mamski family, for their companionship, support, encouragement, and togetherness during the thesis preparation process, making the author feel less alone throughout the journey.
12. Dinas Komunikasi dan Informatika for granting research permission, support, and assistance during the research process.
13. The members of HIMATIFA for the experiences, lessons, support, and togetherness shared throughout the author's college years.
14. All Informatics students from various batches who have become part of the author's journey throughout college. Thank you for the support, help, experiences, and memories shared during the academic years and thesis completion process.

The author realizes that in the preparation of the following thesis there are many shortcomings. For this reason, constructive criticism and suggestions from all parties are highly expected for the perfection of writing the following thesis. Finally, with all the limitations that the author has, hopefully the following report can be useful for all parties in general and the author in particular.

Surabaya, 22 April 2026



Author

LIST OF CONTENTS

APPROVAL SHEET	i
APPROVAL SHEET	ii
STATEMENT OF ORIGINALITY	iii
ABSTRACT	iv
ACKNOWLEDGEMENTS.....	v
LIST OF CONTENTS	vii
LIST OF FIGURES	xii
LIST OF TABLES	xvi
CHAPTER I INTRODUCTION.....	1
1.1. Background	1
1.2. Problem Formulation	5
1.3. Research Objectives	5
1.4. Research Benefits.....	6
1.5. Research Limitations.....	6
CHAPTER II LITERATURE REVIEW.....	8
2.1. General Overview of the Institution.....	8
2.2. Previous Research.....	8
2.2.1. Institutional Profile	10
2.2.2. Organizational Structure	12
2.3. Penetration Testing.....	14

2.3.1.	Penetration Testing Stages.....	15
2.3.2.	Penetration Testing Approaches	17
2.4.	CIA Triad	18
2.5.	OWASP Top 10	20
2.5.1.	Broken Access Control (A01:2021 / A05:2017)	23
2.5.2.	Cryptographic Failures (A02:2021 / Sensitive Data Exposure A03:2017).....	23
2.5.3.	Injection (A03:2021 / A01:2017)	23
2.5.4.	Insecure Design (A04:2021).....	24
2.5.5.	Security Misconfiguration (A05:2021 / A06:2017)	24
2.5.6.	Vulnerable and Outdated Components (A06:2021 / A09:2017)	24
2.5.7.	Identification and Authentication Failures (A07:2021 / Broken Authentication A02:2017)	25
2.5.8.	Software and Data Integrity Failures (A08:2021)	25
2.5.9.	Security Logging and Monitoring Failures (A09:2021 / Insufficient Logging & Monitoring A10:2017)	25
2.5.10.	Server-Side Request Forgery (SSRF) (A10:2021)	25
2.6.	NIST SP 800-115	25
2.6.1.	Main Approaches of NIST SP 800-115.....	26
2.6.2.	Implementation Phases of NIST SP 800-115	27
2.7.	OWASP Web Security Testing Guide (WSTG).....	29
2.8.	OWASP Application Security Verification Standard (ASVS).....	30
2.8.1.	ASVS Structure and Levels.....	30
2.8.2.	Main Categories in OWASP ASVS	31

- 2.9. Common Vulnerability Scoring System 33
 - 2.9.1. Main Structure of CVSS 34
- 2.10. Auxiliary Tools 40
 - 2.10.1. Mozilla Firefox 40
 - 2.10.2. Wappalyzer 41
 - 2.10.3. Virtualbox 42
 - 2.10.4. Kali Linux 44
 - 2.10.5. Burp Suite 45
 - 2.10.6. Nessus 46
 - 2.10.7. Nmap (Network Mapper)..... 48
 - 2.10.8. Dirsearch..... 49
 - 2.10.9. Nuclei..... 50
 - 2.10.10. SQLMap..... 51
 - 2.10.11. Gobuster..... 52
 - 2.10.12. cURL (Client URL)..... 53
 - 2.10.13. OWASP ZAP (Zed Attack Proxy)..... 54
 - 2.10.14. Dalfox 56
- CHAPTER III METHODOLOGY 58**
 - 3.1. Research Design..... 58
 - 3.2. Planning..... 60
 - 3.2.1. Research Object 60
 - 3.2.2. System Functionality 62

- 3.3. Discovery 68
 - 3.3.1. Vulnerability Scanning 71
- 3.4. Attack 85
- 3.5. Reporting..... 92
 - 3.5.1. Risk Analysis Methodology..... 96
- 3.6. Research Tools 98
- CHAPTER IV RESULTS AND DISCUSSION 100**
- 4.1. Planning Phase 100
- 4.2. Discovery Phase 102
 - 4.2.1. Dirsearch..... 102
 - 4.2.2. Wappalyzer 105
 - 4.2.3. Nmap..... 107
 - 4.2.4. Nuclei..... 109
 - 4.2.5. Gobuster..... 115
- 4.3. Attack Phase..... 117
 - 4.3.1. T1 - Broken Access Control 118
 - 4.3.2. T2 - Cryptographic Failures..... 123
 - 4.3.3. T3 - Injection 127
 - 4.3.4. T4 - Insecure Design/Business Logic 131
 - 4.3.5. T5 - Security Misconfiguration..... 136
 - 4.3.6. T6 - Vulnerable & Outdated 141
 - 4.3.7. T7 - Identification & Authentication Failures 144

4.3.8.	T8 - Software & Data Integrity Failures.....	148
4.3.9.	T9 - Security Logging & Monitoring Failures.....	152
4.3.10.	T10 - Server-Side Request Forgery/API Security	155
4.3.11.	Summary of Validation Results.....	158
4.4.	Reporting Phase	159
4.4.1.	T1 Mitigation Report	160
4.4.2.	T2 Mitigation Report	163
4.4.3.	T3 Mitigation Report	166
4.4.4.	T4 Mitigation Report	169
4.4.5.	T5 Mitigation Report	173
4.4.6.	T6 Mitigation Report	176
4.4.7.	T7 Mitigation Report	180
4.4.8.	T8 Mitigation Report	182
4.4.9.	T9 Mitigation Report	187
4.4.10.	T10 Mitigation Report	191
CHAPTER V CLOSING.....		195
5.1.	Conclusion.....	195
5.2.	Suggestion.....	196
BIBLIOGRAPHY		200
ATTACHMENT.....		205

LIST OF FIGURES

Figure 2. 1 Diskominfo Logo.....	12
Figure 2. 2 Diskominfo organizational structure	14
Figure 2. 3 CIA Triad.....	19
Figure 2. 4 OWASP Top 10 2021 Changes	21
Figure 2. 5 NIST SP 800-115 Research Flow.....	27
Figure 2. 6 CVSS Logo.....	33
Figure 2. 7 Base Metrics CVSS	35
Figure 2. 8 Temporal Metrics CVSS.....	37
Figure 2. 9 Environmental Metrics CVSS	39
Figure 2. 10 Mozilla Firefox Logo.....	40
Figure 2. 11 Wappalyzer Logo.....	41
Figure 2. 12 Wappalyzer View	42
Figure 2. 13 VirtualBox Logo.....	43
Figure 2. 14 VirtualBox View.....	43
Figure 2. 15 Kali Linux Logo	44
Figure 2. 16 Kali Linux View	45
Figure 2. 17 Burp Suite Logo.....	45
Figure 2. 18 Burp Suite View	46
Figure 2. 19 Nessus Logo.....	47
Figure 2. 20 Nessus View	47
Figure 2. 21 Nmap Logo.....	48

Figure 2. 22 Nmap View.....	49
Figure 2. 23 Dirsearch Logo	49
Figure 2. 24 Dirsearch View	50
Figure 2. 25 Nuclei Logo	50
Figure 2. 26 Nuclei View	51
Figure 2. 27 SQLMap Logo	52
Figure 2. 28 SQLMap View.....	52
Figure 2. 29 Gobuster Logo	53
Figure 2. 30 Gobuster View	53
Figure 2. 31 cURL (Client URL) Logo.....	54
Figure 2. 32 cURL (Client URL) View	54
Figure 2. 33 OWASP ZAP Logo	55
Figure 2. 34 OWASP ZAP View	56
Figure 2. 35 Dalfox Logo.....	56
Figure 2. 36 Dalfox View.....	57
Figure 3. 1 Hybrid Framework Integration.....	58
Figure 3. 2 Home Page of the Trenggalek Regional Forestry Service Branch Website	60
Figure 3. 3 Use Case for the Trenggalek Regional Forestry Service Branch Website	63
Figure 3. 4 Example of scanning results using OWASP ZAP	73
Figure 3. 5 Example of scanning results using Nessus	81
Figure 3. 6 Output Summary.....	92

Figure 3. 7 Executive Summary.....	93
Figure 3. 8 Summary of Vulnerability Findings.....	93
Figure 3. 9 Summary of Mitigation Recommendations.....	95
Figure 3. 10 Risk Analysis Process.....	96
Figure 3. 11 Examples of Using CVSS Base Matrices.....	97
Figure 4. 1 Dirsearch Results.....	103
Figure 4. 2 Wappalyzer Results.....	106
Figure 4. 3 Nmap Results.....	108
Figure 4. 4 Nuclei Results.....	110
Figure 4. 5 Nuclei 2 Results.....	111
Figure 4. 6 Nuclei 3 Results.....	112
Figure 4. 7 Nuclei 4 Results.....	113
Figure 4. 8 Directory & File Discovery Results with Gobuster.....	116
Figure 4. 9 Test Horizontal Privilege Escalation Results.....	119
Figure 4. 10 Test Request Vertical Privilege Escalation.....	120
Figure 4. 11 Response Vertical Privilege Escalation.....	120
Figure 4. 12 Score CVSS T1 - Broken Access Control.....	121
Figure 4. 13 Header Verification Using Nmap.....	123
Figure 4. 14 Check Password.....	124
Figure 4. 15 Score CVSS T2 - Cryptographic Failures.....	125
Figure 4. 16 Initiate SQL Injection Scanning with SQLMap.....	127
Figure 4. 17 Final Results of SQLMap Scan.....	128

Figure 4. 18 XSS Vulnerability Scanning with Dalfox.....	128
Figure 4. 19 Parameter Validation Results on Dalfox	129
Figure 4. 20 Score CVSS T3 - Injection	130
Figure 4. 21 Visual Validation Evidence on User Interface	132
Figure 4.22 Intercept Process and Data Parameter Manipulation.....	133
Figure 4. 23 Request Manipulation Using Burp Suite	134
Figure 4. 24 Response Manipulation Using Burp Suite.....	134
Figure 4. 25 CVSS Score T4 - Insecure Design/Business Logic.....	135
Figure 4. 26 Gobuster Scan Results	137
Figure 4. 27 Manual Testing Results via curl	138
Figure 4. 28 HTTP Response Header Analysis	139
Figure 4. 29 Score CVSS T5 - Security Misconfiguration	139
Figure 4. 30 Zap Tech Results	141
Figure 4. 31 Wappalyzer.....	142
Figure 4. 32 CVE-2025-14178.....	142
Figure 4. 33 Score CVSS T6 - Vulnerable & Outdated.....	143
Figure 4. 34 Brute Force Attack Simulation on Login Panel.....	145
Figure 4. 35 Test Weak Password.....	146
Figure 4. 36 Forgot Password Test	146
Figure 4. 37 CVSS Score T7 - Identification & Authentication Failures	147

LIST OF TABLES

Table 2. 1 CVSS assessment categories v3.1	34
Table 3. 1 Planning for data and information collection.....	68
Table 3. 2 Results of data and information collection using OWASP ZAP	74
Table 3. 3 Mapping of OWASP ZAP scanning results.....	76
Table 3. 6 CVSS v3.1 assessment categories.....	94
Table 3. 7 Penetration Testing Research Tools.....	99
Table 4. 1 Scope of Testing.....	101
Table 4. 2 Directory Scan Results Using Dirsearch.....	104
Table 4. 3 Vulnerability Scanning Results Wappalyzer	107
Table 4. 4 Directory Scan Results Using Dirsearch.....	109
Table 4. 5 Vulnerability Scanning Results Using Nuclei	113
Table 4. 6 Directory and Endpoint Scanning Results Using Gobuster	117
Table 4. 7 CVSS Metrics Details for Broken Access Control	122
Table 4. 8 CVSS Metrics Details for Cryptographic Failures	125
Table 4. 9 CVSS Metrics Details for Injection	130
Table 4. 10 CVSS Metric Details for Insecure Design/Business Logic	135
Table 4. 11 CVSS Metrics Details for Security Misconfiguration	140
Table 4. 12 CVSS Metric Details for Vulnerable and Outdated Components.....	144
Table 4. 13 Details of CVSS v3.1 Metrics for Identification & Authentication Failures.....	147
Table 4. 14 CVSS Metric Details for Software and Data Integrity Failures.....	151

Table 4. 15 CVSS Metrics Details for Security Logging and Monitoring Failures.. 154

Table 4. 16 CVSS Metrics Details for Server-Side Request Forgery (SSRF)..... 157

Table 4. 17 Vulnerability Validation Results Summary 159

Table 4. 18 T1 Mitigation Report 160

Table 4. 19 T2 Mitigation Report 163

Table 4. 20 T3 Mitigation Report 167

Table 4. 21 T4 Mitigation Report 170

Table 4. 22 T5 Mitigation Report 174

Table 4. 23 T6 Mitigation Report 177

Table 4. 24 T7 Mitigation Report 180

Table 4. 25 T8 Mitigation Report 183

Table 4. 26 T9 Mitigation Report 187

Table 4. 27 T10 Mitigation Report 191