



UNDERGRADUATE THESIS

SECURITY ANALYSIS OF THE WESKONEK ERP SYSTEM USING A HYBRID MITRE AND PTES METHOD

KEN NARENDRA EKAMARTHA
NPM 22081010083

THESIS ADVISOR

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 OF THE WESKONEK ERP SYSTEM USING A
HYBRID MITRE AND PTES METHOD

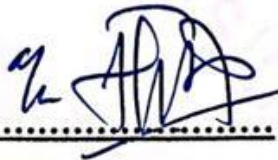
By:
KEN NARENDRA EKAMARTHA
NPM. 22081010083

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 July 10, 2026:

Approved,

Henni Endah Wahanani, ST. M.Kom.

NIP. 19780922 202121 2 005



(Advisor I)

Achmad Junaidi, S.Kom, M.Kom.

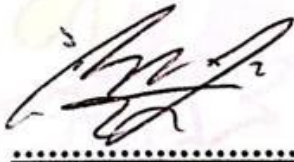
NIP. 19781110 202521 1 048



(Advisor II)

Budi Nugroho, S.Kom. M.Kom.

NIP. 19800907 202121 1 005



(Head Assessor)

Ardhon Rakhmadi, S.Tr.T., M.Kom.

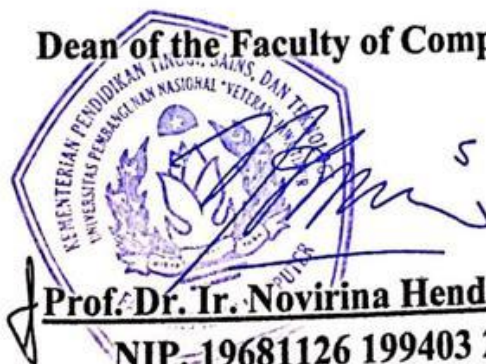
NIP. 19910805 202406 1 002



(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 OF THE WESKONEK ERP SYSTEM USING A HYBRID MITRE AND PTES METHOD

By:
KEN NARENDRA EKAMARTHA
NPM. 22081010083

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 : Ken Narendra Ekamartha
NPM : 22081010083
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, July 10, 2026



Declarant,

A handwritten signature in black ink, written over the official stamp and the word 'Declarant'.

KEN NARENDRA EKAMARTHA

NPM. 22081010083

ABSTRACT

Student Name/ NPM : Ken Narendra Ekamartha / 22081010083
Thesis Title : SECURITY ANALYSIS OF THE WESKONEK
ERP SYSTEM USING A HYBRID MITRE AND
PTES METHOD
Advisor : 1. Henni Endah Wahanani, ST, M.Kom
2. Achmad Junaidi, S.Kom, M.Kom

The web-based Enterprise Resource Planning (ERP) system centrally stores an organization's operational data but is vulnerable to security threats if not adequately protected. This study aims to analyze the security of the Weskonek ERP System owned by PT Tekno Konek Solusi using a Grey-Box Penetration Testing approach. The applied hybrid method combines the PTES phases, weakness classification with CWE, attack mapping using MITRE ATT&CK, and severity assessment through CVSS v3.1. Testing was conducted using tools such as OWASP ZAP, Burp Suite, SQLmap, and Nmap. The results identified vulnerabilities including SQL Injection, Cross-Site Scripting (XSS), Brute Force on the Login Page, and Active Session Misuse, impacting the system's confidentiality, integrity, and availability. This study provides mitigation including strengthening input validation, managing authentication, securing sessions, configuring cookies, and limiting login attempts.

Keywords: ERP, penetration testing, PTES, CWE, MITRE ATT&CK, CVSS, web application security

ACKNOWLEDGEMENTS

Praise and gratitude are expressed by the author to Allah SWT for His endless blessings, guidance, and grace, enabling the author to complete the undergraduate thesis entitled "**SECURITY ANALYSIS OF THE WESKONEK ERP SYSTEM USING A HYBRID MITRE AND PTES METHOD**" successfully.

This thesis was prepared as one of the requirements to obtain a Bachelor of Computer Science degree in the Informatics Study Program, Faculty of Computer Science, Universitas Pembangunan Nasional "Veteran" Jawa Timur. During the preparation process, the author received various forms of assistance, guidance, support, and motivation from many individuals. Therefore, on this occasion, the author would like to express the deepest gratitude to all parties who have contributed to the completion of this thesis.

The author would like to express appreciation and gratitude to:

1. My beloved father, mother, and younger sibling, who have always provided endless love, prayers, support, and encouragement. All forms of sacrifice, attention, and motivation given have become the greatest source of strength for the author to continue striving until this thesis was completed.
2. Mrs. Henni Endah Wahanani, S.T., M.Kom. and Mr. Achmad Junaidi, S.Kom., M.Kom., as thesis supervisors who have patiently dedicated their time, energy, and knowledge to provide guidance, direction, constructive criticism, and valuable suggestions throughout the research and thesis preparation process.
3. My fellow students who participated in the proposal seminar and research seminar, namely Nabil Ramadhani, Abraham Danar Jovian, Dimas Aji Primadiansyah, M. Maulana Falihuddin, and Ryan Bagus Bimantoro, who have continuously provided support, motivation, and companionship throughout the academic journey until the completion of this thesis. The experiences, discussions, and collaborations shared together have become meaningful memories for the author.
4. My friends from Mamino, namely Kupluk, Basroil, Fadika, Rizki, Alip, Nanta, Yasir, Kepin, Ojan, Wahyu, Leon, Erlang, Irfan, and Slotong, who

have brought many stories, laughter, and memorable moments that made the university journey more meaningful. Thank you for the support, information, and various experiences shared throughout the academic process until the completion of this study.

5. All parties who have provided assistance, support, prayers, and other contributions throughout the author's academic journey and the completion of this thesis, both directly and indirectly, who cannot be mentioned individually. May all kindness and support given receive abundant rewards from Allah SWT.

The author realizes that this thesis still has various limitations and is far from perfect. Therefore, constructive criticism and suggestions are highly appreciated as valuable input for future improvements. The author sincerely hopes that this thesis can provide benefits, both for the development of knowledge and for readers who may require related information.

Surabaya, July 10th 2026



Ken Narendra Ekamartha

TABLE OF CONTENTS

APPROVAL SHEET	i
APPROVAL SHEET	iii
STATEMENT OF ORIGINALITY	v
ABSTRACT	vii
ACKNOWLEDGEMENTS	ix
TABLE OF CONTENTS	xi
LIST OF FIGURES	xv
LIST OF TABLES	xvii
CHAPTER I INTRODUCTION	1
1.1 Background	1
1.2 Problem Formulation.....	3
1.3 Problem Limitations	3
1.4 Goal	4
1.5 Benefit	5
CHAPTER II LITERATURE REVIEW	7
2.1 Previous Research	7
2.2 Company Profile.....	10
2.2.1 Bussiness Field	11
2.3 <i>Enterprise Resource Planning</i> (ERP).....	12
2.4 CIA Triad	12
2.4.1 <i>Confidentiality</i>	13
2.4.2 <i>Integrity</i>	13
2.4.3 <i>Availability</i>	14
2.5 <i>Penetration Testing</i> Execution Standard (PTES)	15
2.5.1 Pre-Engagement Planning.....	15
2.5.2 Intelligence Gathering.....	16
2.5.3 Threat Modeling	16
2.5.4 Vulnerability Analysis	17
2.5.5 Exploitation.....	17
2.5.6 Post-Exploitation	18

2.5.7 Reporting	18
2.6 Common <i>Weakness</i> Enumeration	19
2.6.1 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20
2.6.2 CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21
2.6.3 CWE-352: Cross-Site Request Forgery (CSRF)	22
2.6.4 CWE-862: Missing Authorization	23
2.6.5 CWE-787: Out-of-bounds Write	24
2.6.6 CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24
2.6.7 CWE-416: Use After Free	25
2.6.8 CWE-125: Out-of-bounds Read	26
2.6.9 CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	27
2.6.10 CWE-94: Improper Control of Generation of Code ('Code Injection')	28
2.6.11 CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29
2.6.12 CWE-434: Unrestricted Upload of File with Dangerous Type	30
2.6.13 CWE-476: NULL Pointer Dereference	31
2.6.14 CWE-121: Stack-based Buffer Overflow	32
2.6.15 CWE-502: Deserialization of Untrusted Data	33
2.6.16 CWE-122: Heap-based Buffer Overflow	34
2.6.17 CWE-863: Incorrect Authorization	34
2.6.18 CWE-20: Improper <i>Input validation</i>	35
2.6.19 CWE-284: Improper Access Control	36
2.6.20 CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	37
2.6.21 CWE-306: Missing <i>Authentication</i> for Critical Function	37
2.6.22 CWE-918: Server-Side Request Forgery (SSRF)	38
2.6.23 CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')	39
2.6.24 CWE-639: Authorization Bypass Through User-Controlled Key	40

2.6.25 CWE-770: Allocation of Resources Without Limits or Throttling	41
2.7 MITRE ATT&CK	42
2.7.1 MITRE ATT&CK Structure	43
2.7.2 MITRE ATT&CK Domains	44
2.8 Common Vulnerability Scoring <i>System</i> (CVSS).....	45
2.8.1 Base Metrics	46
2.8.2 Temporal Metrics.....	49
2.8.3 Environmental Metrics	51
2.9 Testing Tools and Environment	52
2.9.1 Kali Linux	52
2.9.2 Mozilla Firefox	54
2.9.3 Burp Suite	55
2.9.4 OWASP Zap	56
2.9.5 Nmap.....	57
2.9.6 Nuclei.....	58
2.9.7 SQLmap.....	59
2.9.8 ParamSpider.....	60
2.9.9 Curl	61
2.9.10 Dirsearch.....	62
2.9.11 Wappalyzer	63
2.9.12 Gobuster.....	64
CHAPTER III METHODOLOGY	67
3.1 Research Design	67
3.2 Pre-Engagement Interactions	72
3.2.1 Research Object	72
3.2.2 System Functionality	73
3.3 Intelligence Gathering	76
3.4 Threat Modeling	81
3.4.1 Weskonek ERP System Vulnerability Scanning With OWASP ZAP..	82
3.5 Vulnerability Analysis.....	89
3.6 Exploitation	93
3.7 Post-Exploitation	100

3.8 Reporting	104
CHAPTER IV RESULTS AND DISCUSSION	111
4.1 Pre-Engagement Interactions	111
4.2 Intelligence Gathering.....	113
4.2.1 Application Technology Identification using Wappalyzer	113
4.2.2 Network Infrastructure Scanning using Nmap.....	114
4.2.3 Application Parameter Enumeration using ParamSpider.....	116
4.2.4 Directory Enumeration using Gobuster.....	117
4.2.5 Initial Vulnerability Identification using Nuclei	118
4.3 Threat Modeling	120
4.4 Vulnerability Analysis	122
4.5 Exploitation.....	126
4.5.1 <i>SQL Injection</i>	134
4.5.2 <i>Cross-Site Scripting (XSS)</i>	135
4.5.3 <i>Brute Force Login Page</i>	136
4.5.4 Risk of Active Session Misuse.....	137
4.6 Post-Exploitation	138
4.6.1 <i>SQL Injection</i>	139
4.6.2 <i>Cross-Site Scripting (XSS)</i>	140
4.6.3 <i>Brute Force Login Page</i>	142
4.6.4 Risk of Active Session Misuse.....	144
4.7 Reporting	146
CHAPTER V CLOSING.....	149
5.1 Conclusion	149
5.1.1 Suggestion.....	151
BIBLIOGRAPHY	153
ATTACHMENT.....	157

LIST OF FIGURES

Figure 2. 1 Tekno Konek Solusi Logo	10
Figure 2. 2 Tekno Konek Solusi Tagline	11
Figure 2. 3 CIA Triad.....	13
Figure 2. 4 PTES Methodology	15
Figure 2. 5 Common Weakness Enumeration Logo	19
Figure 2. 6 CWE-79	20
Figure 2. 7 CWE-89	21
Figure 2. 8 CWE-352	22
Figure 2. 9 CWE-862	23
Figure 2. 10 CWE-787	24
Figure 2. 11 CWE-22	25
Figure 2. 12 CWE-416	26
Figure 2. 13 CWE-125	27
Figure 2. 14 CWE-78	28
Figure 2. 15 CWE-94	29
Figure 2. 16 CWE-120	30
Figure 2. 17 CWE-434	31
Figure 2. 18 CWE-476	32
Figure 2. 19 CWE-502	33
Figure 2. 20 CWE-863	35
Figure 2. 21 CWE-20	36
Figure 2. 22 CWE-306	38
Figure 2. 23 CWE-918	39
Figure 2. 24 CWE-77	40
Figure 2. 25 CWE-770	41
Figure 2. 26 MITRE ATT&CK Logo	42
Figure 2. 27 CVSS Logo.....	45
Figure 2. 28 Base Metrics CVSS 3.1 Example	47
Figure 2. 29 Temporal Metrics Example	50
Figure 2. 30 Environmental Metrics Example	51
Figure 2. 31 Kali Linux.....	53

Figure 2. 32 Mozilla Firefox Logo	54
Figure 2. 33 Burp Suite	55
Figure 2. 34 OWASP Zap	57
Figure 2. 35 Nmap Logo	58
Figure 2. 36 Nuclei	59
Figure 2. 37 SQLmap	60
Figure 2. 38 ParamSpider	61
Figure 2. 39 Curl Logo	62
Figure 2. 40 Dirsearch	63
Figure 2. 41 Wappalyzer	64
Figure 2. 42 Gobuster	65
Figure 3. 1 Hybrid Mitre PTES & CVSS Framework.....	68
Figure 3. 2 Weskonek Dashboard.....	72
Figure 3. 3 Use Case Weskonek ERP System.....	74
Figure 3. 4 OWASP ZAP Scanning Example	84
Figure 3. 5 Vulnerability Risk Analysis Results Mapping.....	101
Figure 3. 6 CVSS Calculator Example.....	103
Figure 3. 7 Data Integration and Verification	104
Figure 3. 8 Executive Summary	105
Figure 3. 9 Finding Details and Proof of Concept.....	106
Figure 3. 10 CIA Triad	107
Figure 3. 11 Risk Classification	108
Figure 3. 12 Mitigation Recommendations	109
Figure 4. 1 SQL Injection Vulnerability Evidence.....	135
Figure 4. 2 XSS Vulnerability Evidence	136
Figure 4. 3 Brute Force Vulnerability Evidence.....	137
Figure 4. 4 Risk of Active Session Misuse Vulnerability Evidence	138
Figure 4. 5 SQL Injection CVSS 3.1 Score.....	140
Figure 4. 6 Cross-Site Scripting CVSS 3.1 Score	142
Figure 4. 7 Brute Force CVSS 3.1 Score.....	144
Figure 4. 8 Risk of Active Session Misuse CVSS 3.1 Score	146
Figure 4. 9 Report of Findings Example	147

LIST OF TABLES

Table 2. 1 CVSS Score Category	46
Table 3. 1 Tool Mapping Across PTES Phases	69
Table 3. 2 Intelligence Gathering Tools Planning	77
Table 3. 3 OWASP ZAP Findings	84
Table 3. 4 Threat Mapping Based on OWASP Findings	86
Table 3. 5 CWE List Based on OWASP ZAP Scan Results.....	90
Table 3. 6 CWE Mapping to MITRE ATT&CK Tactics and Techniques.....	94
Table 3. 7 Exploitation Test Matrix	97
Table 4. 1 Target Testing Information	112
Table 4. 2 Rules of Engagement for Penetration Testing	112
Table 4. 3 Website Technology Stack Identification	114
Table 4. 4 Website Port List.....	115
Table 4. 5 ParamSpider Enumeration Results.....	116
Table 4. 6 Gobuster Enumeration Results.....	117
Table 4. 7 Nuclei Identification Results.....	118
Table 4. 8 OWASP ZAP Active Scanning Results.....	120
Table 4. 9 Vulnerability Mapping	121
Table 4. 10 Mapping of OWASP ZAP Findings to CWE	122
Table 4. 11 Exploitation Testing Matrix Validation Results	126
Table 4. 12 Mapping of Exploitation Findings to MITRE ATT&CK	131
Table 4. 13 SQL Injection Vulnerability Details	134
Table 4. 14 Cross-Site Scripting (XSS) Vulnerability Details.....	135
Table 4. 15 Brute Force Vulnerability Details	136
Table 4. 16 Active Session Misuse Risk Vulnerability Details	137
Table 4. 17 Exploitation Results Mapping.....	138
Table 4. 18 CVSS v3.1 Assessment of SQL Injection Vulnerability	139
Table 4. 19 CVSS v3.1 Assessment of Cross-Site Scripting (XSS) Vulnerability	141

Table 4. 20 CVSS v3.1 Assessment of Brute Force Login Page Vulnerability .. 142

Table 4. 21 CVSS v3.1 Assessment of Active Session Misuse Risk Vulnerability
..... 144