



**CYBERATTACK PREVENTION THROUGH THE DEVELOPMENT OF A
MULTI-VULNERABILITY SCANNER**

UNDERGRADUATE THESIS

**Submitted as one of the requirements to obtain
Sarjana Komputer (S.Kom.)**

By:

ELGINO TANTO JAYA

001202200143

FACULTY OF COMPUTER SCIENCE

INFORMATICS STUDY PROGRAM

CIKARANG

AUGUST, 2025

SIMILARITY INDEX REPORT

Turnitin-Elgino Tanto Jaya

ORIGINALITY REPORT

6%

SIMILARITY INDEX

3%

INTERNET SOURCES

2%

PUBLICATIONS

3%

STUDENT PAPERS

PRIMARY SOURCES

1

Submitted to Asia Pacific University College of
Technology and Innovation (UCTI)

Student Paper

1%

2

www.coursehero.com

Internet Source

1%

3

myfik.unisza.edu.my

Internet Source

<1%

4

Submitted to Universiti Malaysia Pahang

Student Paper

<1%

5

Submitted to Pukyong National University

Student Paper

<1%

6

Submitted to Macao Polytechnic Institute

Student Paper

<1%

7

docslib.org

Internet Source

<1%

8

Submitted to KDU College Sdn Bhd

Student Paper

<1%

9

Submitted to Sim University

Student Paper

<1%

Screenshot of GPT Zero

- Chapter 1

 **GPTZero** Version 2025-06-02-beta

CHAPTER 1 - 7/21/2025

AI Report

We predict this text is

Human Generated

AI Probability

11%

This number is the probability that the document is AI-generated, not a percentage of AI text in the document.

Plagiarism

?

The plagiarism scan was not run for this document. Go to gptzero.me to check for plagiarism.

CHAPTER 1 - 7/21/2025

ELGINO TANTO JAYA

- Chapter 2

 **GPTZero** Version 2025-06-02-beta

CHAPTER 2 - 7/21/2025

AI Report

We predict this text is

Human Generated

AI Probability

4%

This number is the probability that the document is AI-generated, not a percentage of AI text in the document.

Plagiarism

?

The plagiarism scan was not run for this document. Go to gptzero.me to check for plagiarism.

CHAPTER 2 - 7/21/2025

ELGINO TANTO JAYA

- Chapter 3

 Version 2025-06-02 beta

CHAPTER 3 - 7/21/2025

AI Report

We predict this text is

Human Generated

AI Probability

3%

This number is the probability that the document is AI-generated, not a percentage of AI text in the document.

Plagiarism

?

The plagiarism scan was not run for this document. Go to [gptzero.me](#) to check for plagiarism.

CHAPTER 3 - 7/21/2025

ELGINO TANTO JAYA

- Chapter 4

 Version 2025-06-02 beta

CHAPTER 4 - 7/21/2025

AI Report

We predict this text is

Human Generated

AI Probability

0%

This number is the probability that the document is AI-generated, not a percentage of AI text in the document.

Plagiarism

?

The plagiarism scan was not run for this document. Go to [gptzero.me](#) to check for plagiarism.

CHAPTER 4 - 7/21/2025

ELGINO TANTO JAYA

- Chapter 5

 Version 2025-06-02 beta

CHAPTER 5 - 7/21/2025

AI Report

We predict this text is

Human Generated

AI Probability

3%

This number is the probability that the document is AI-generated, not a percentage of AI text in the document.

Plagiarism

?

The plagiarism scan was not run for this document. Go to [gptzero.me](#) to check for plagiarism.

CHAPTER 5 - 7/21/2025

ELGINO TANTO JAYA

ABSTRACT

This study presents the development of a user-friendly web-based scanning tool designed to detect cybersecurity threats from three common sources: executable (.exe) files, URLs, and email messages (.eml). The objective of this study is to provide an accessible and effective cybersecurity solution for users of all technical backgrounds by enabling real-time threat detection, persistent scan history tracking, user-generated feedback, and comprehensive analytical reports with preventive recommendations. The methodology involves applying distinct threat detection techniques personalized to each input type and utilizing the Agile Kanban methodology to implement each step of the software design process, enabling flexible adaptation and visual tracking of development progress. For URLs, detection is performed using a machine learning approach that combines an XGBoost classifier with domain reputation assessments to identify malicious links. Email threat analysis is conducted through multi-layered inspection, including header analysis, attachment scanning, and content classification using a Support Vector Machine (SVM) trained on Word2Vec-generated feature vectors. Executable file analysis combines cryptographic hash verification, signature pattern matching, heuristic rule evaluation, and external threat intelligence via the VirusTotal API to identify potential threats. The results of the experiments demonstrate that the system is able to detect a wide range of threats while also maintaining usability and performance, which contributes to greater cybersecurity awareness and resilience for the typical user.

TABLE OF CONTENTS

	Page
ABSTRACT	v
DEDICATION	vi
ACKNOWLEDGMENTS	vii
CHAPTER I.....	1
INTRODUCTION	1
1.1 Problem Formulation	1
1.1.1 Background	1
1.1.2 Problem Statement	2
1.1.3 Objective	2
1.1.4 Problem from a Customer Perspective	3
1.2 Problem Constraint Analysis	3
1.2.1 Accessibility	3
1.2.2 Accuracy	3
1.2.3 Security	4
1.3 Problem Functional Analysis.....	4
1.3.1 Multi Vulnerability Scanner Login & Sign-up Explanations	4
1.3.2 Multi Vulnerability Scanner Home Page Explanations.....	4
1.3.3 Multi Vulnerability Scanner Result Page Explanations	5
1.3.4 Multi Vulnerability Scanner History Page Explanations.....	5
1.4 Solution Selection	5
1.4.1 Alternative Solution 1.....	5
1.4.2 Alternative Solution 2.....	6
1.4.3 Alternative Solution 3.....	6
1.4.4 Solution Selection.....	6
1.5 Solution Usage Scenarios	6
1.5.1 Access with and without Login.....	6
1.5.2 Selecting Scanner	7
1.5.3 Scanning Process.....	7
1.5.4 Managing Scan Results.....	7
1.5.5 Repeated User	8

1.6	Development Effort.....	8
1.6.1	Man-months	8
1.6.2	Machine-months.....	8
1.6.3	Development Tools	8
1.6.4	Test Equipment	8
1.6.5	Timelines	9
CHAPTER II		10
SPECIFICATIONS		10
2.1	Existing and Proposed System	10
2.1.1	Existing Business Process.....	10
2.1.2	Proposed Business Process	11
2.2	Global Description of the Product	12
2.2.1	Main Functionality	12
2.2.2	User Characteristics.....	12
2.2.3	Constraints	13
2.2.4	Product Development Environment	14
2.2.5	Product Operational Environment.....	14
2.3	Requirement Analysis	15
2.3.1	External Interface	15
2.3.2	Functional Description	16
2.3.3	Data Requirement from user's perspective.....	20
2.3.4	Functional Requirement from user's perspective.....	22
2.3.5	Non-Functional Requirement.....	25
2.4	Specification Testing.....	26
CHAPTER III.....		27
DESIGN		27
3.1	Alternative Design Solutions Design.....	27
3.1.1	Alternative Solution 1: Multi Vulnerability Scanner Website.....	27
3.1.2	Alternative Solution 2: Multi Vulnerability Scanner API	29
3.1.3	Alternative Solution 3: Multi Vulnerability Scanner Application	31
3.2	Rational/Systematic Design.....	33
3.2.1	Comparison Table	33
3.2.2	Quantitative Solution Selection.....	34
3.2.3	Solution Selection.....	38

3.3	Hierarchical/Iterative Design.....	39
3.3.1	Data Flow Diagram of Multi Vulnerability Scanner.....	39
3.3.2	Global Variable / Message Passing Interface	40
3.3.3	Agile Kanban Methodology to Implement Steps in Software Engineering	41
3.3.4	Detail of Component and Library Used.....	42
3.3.5	Unified Modeling Language 2.0	44
3.4	Verification Demonstration and Proof of Design Process	47
3.5	Standard Used.....	48
3.6	Implementation and Testing Plans.....	50
3.6.1	Gantt Chart.....	50
3.6.2	S-Chart.....	50
CHAPTER IV.....		51
IMPLEMENTATION		51
4.1	Design Implementation	51
4.1.1	Function/Procedure/Class Implementation.....	51
4.1.2	Database Implementation	62
4.1.3	Integration Among Every Module	63
4.1.4	Implementation Verification	65
4.2	Product Display	67
4.2.1	Login Page	67
4.2.2	Register Page.....	67
4.2.3	Home Page / Dashboard	68
4.2.4	Email Scanner Page.....	70
4.2.5	URL Scanner Page	70
4.2.6	File Scanner Page.....	71
4.2.7	History Page	72
4.2.8	Full Report Page.....	72
4.2.9	Result Page.....	74
4.2.10	Tips Page.....	75
4.2.11	Comment Modal.....	76
4.3	Component Cost Analysis	78
4.4	Manual Guide	78
4.4.1	System Build Documentation from the Source.....	78

4.4.2	System Installation	80
4.4.3	User Guide per User Role	80
4.5	Video Testing	82
CHAPTER V		83
TESTING		83
5.1	Functional Testing	83
5.1.1	Testing Results of Every Function on the Specification	83
5.1.2	Present Qualitative Testing	85
5.1.3	Detail the Test Procedures	86
5.1.4	Procedures for the Demo	90
5.2	Testing Other Specifications	92
5.2.1	Non-Functional Specifications	92
5.2.2	Photos and Recording of the Test	93

LIST OF TABLES

TABLE	Page
1.1 Man Months	8
2.1 User Characteristics	12
2.2 Use Case Scenario for Register of Multi Vulnerability Scanner	16
2.3 Use Case Scenario for Login of Multi Vulnerability Scanner	17
2.4 Use Case Scenario for Scanners of Multi Vulnerability Scanner	Error! Bookmark not defined.
2.5 Use Case Scenario for Comment of Multi Vulnerability Scanner	19
2.6 Use Case Scenario for Scan History of Multi Vulnerability Scanner	19
2.7 Users Data Dictionary of Multi Vulnerability Scanner	20
2.8 Scans Data Dictionary of Multi Vulnerability Scanner	20
2.9 Comment Data Dictionary of Multi Vulnerability Scanner	21
3.1 Comparison Between Alternative Solutions	34
3.2 The Rubrics of Criteria and Scale.....	35
3.3 Quantitative Selection for Alternative Solution 1	36
3.4 Quantitative Selection for Alternative Solution 2	37
3.5 Quantitative Selection for Alternative Solution 3	37
3.6 Verification Demonstration for Multi Vulnerability Scanner	47
3.7 Standard Used of Multi Vulnerability Scanner	49
4.1 Implementation Verification	65
4.2 Component Cost Analysis of Multi Vulnerability Scanner	78
5.1 Problem Functional Analysis Testing Results.....	83
5.2 Functional Description Testing Results	84
5.3 Present Qualitative Testing	86
5.4 Non Functional Specifications Testing	92

LIST OF FIGURES

FIGURE	Page
1.1 Timelines for Developing the System	9
2.1 Existing Email Threat Scanner Flow	10
2.2 Existing URL Threat Scanner Flow	10
2.3 Existing File Threat Scanner Flow	11
2.4 Proposed System Flow	11
2.5 Use Case Diagram of Multi Vulnerability Scanner	16
2.6 ERD of Multi Vulnerability Scanner	20
2.7 Context Diagram of Multi Vulnerability Scanner	22
2.8 Activity Diagram of Multi Vulnerability Scanner	22
2.9 Data Flow of Multi Vulnerability Scanner	23
3.1 Block Diagram Level 0 of Multi Vulnerability Scanner Website	27
3.2 Block Diagram Level 1 of Multi Vulnerability Scanner Website	27
3.3 Block Diagram Level 0 of Multi Vulnerability Scanner API	30
3.4 Block Diagram Level 1 of Multi Vulnerability Scanner API	30
3.5 Block Diagram Level 0 of Multi Vulnerability Scanner Application	31
3.6 Block Diagram Level 1 of Multi Vulnerability Scanner Application	32
3.7 Formula for Quantitative Selection	36
3.8 Data Flow Diagram Level 0 of Multi Vulnerability Scanner	39
3.9 Data Flow Diagram Level 1 of Multi Vulnerability Scanner	39
3.10 Kanban Board for Multi Vulnerability Scanner	42
3.11 Use Case Diagram for Multi Vulnerability Scanner	44
3.12 Activity Diagram of Multi Vulnerability Scanner	45
3.13 Class Diagram of Multi Vulnerability Scanner	46
3.14 Sequence Diagram of Multi Vulnerability Scanner	46
3.15 ERD for Multi Vulnerability Scanner	47
3.16 Gantt Chart for Developing Multi Vulnerability Scanner	50
3.17 S-Chart for Developing Multi Vulnerability Scanner	50
4.1 Data Flow Diagram Level 0	51
4.2 History Controller Block Code	52
4.3 Comment Controller on Result Block Code	52
4.4 Comment Controller on History Block Code	53
4.5 Data Flow Diagram Level 2 Email Scanner Process	54
4.6 Email Scanner Controller Block Code	55
4.7 Email Scanner API Block Code	57
4.8 Email Scanner Header Block Code	59
4.9 Email Scanner Attachment Block Code	60
4.10 Email Scanner Content Block Code	61
4.11 Database Implementation of Multi Vulnerability Scanner	62
4.12 Data Flow Diagram Level 1 of Multi Vulnerability Scanner	63
4.13 Login Page of Multi Vulnerability Scanner	67
4.14 Register Page of Multi Vulnerability Scanner	67

4.15 Dashboard Page (Main Interface) of Multi Vulnerability Scanner	68
4.16 Dashboard Page (A Glimpse Before Scan) of Multi Vulnerability Scanner	68
4.17 Dashboard Page (Scan Lookup) of Multi Vulnerability Scanner	69
4.18 Dashboard Page (Scanner Selection) of Multi Vulnerability Scanner	69
4.19 Email Scanner Page of Multi Vulnerability Scanner	70
4.20 URL Scanner Page of Multi Vulnerability Scanner	70
4.21 File Scanner Page of Multi Vulnerability Scanner	71
4.22 History Page of Multi Vulnerability Scanner	72
4.23 Full Report Page (URL) of Multi Vulnerability Scanner	72
4.24 Full Report Page (File) of Multi Vulnerability Scanner	73
4.25 Full Report (Email) of Multi Vulnerability Scanner	73
4.26 Result Page (Safe) of Multi Vulnerability Scanner	74
4.27 Result Page (Not Safe) of Multi Vulnerability Scanner	74
4.28 Result Page (Suspicious) of Multi Vulnerability Scanner	74
4.29 Tips Page of Multi Vulnerability Scanner	75
4.30 Comment Modal of Multi Vulnerability Scanner.....	76
5.1 Login Page Testing	93
5.2 Register Page Testing	94
5.3 Dashboard Page (Main Interface) Testing	94
5.4 Dashboard Page (A Glimpse Before Scan) Testing	95
5.5 Dashboard Page ((Search Scan Section) Testing	95
5.6 Dashboard Page (Select Scanner Type) Testing	96
5.7 URL Scanner Page Testing	96
5.8 File Scanner Page Testing.....	96
5.9 Email Scanner Page Testing.....	97
5.10 Result Page (Safe) Testing	97
5.11 Result Page (Not Safe) Testing	98
5.12 Result Page (Suspicious) Testing	98
5.13 Full Report Page (File) Testing	99
5.14 Full Report Page (URL) Testing	99
5.15 Full Report Page (Email) Testing	99
5.16 Tips Page Testing	100
5.17 History Page Testing.....	101
5.18 Comment Modal Testing.....	101