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:

GHIFARI PRAYUGA GUNAWAN

001202200050

FACULTY OF COMPUTER SCIENCE

INFORMATICS STUDY PROGRAM

CIKARANG

AUGUST, 2025

Individual Reports_Ghifari Prayuga.docx

ORIGINALITY REPORT

6%	3%	2%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Asia Pacific University College of Technology and Innovation (UCTI) Student Paper	1%
2	myfik.unisza.edu.my Internet Source	<1%
3	Submitted to Universiti Malaysia Pahang Student Paper	<1%
4	Song, Jiajun. "Optimization of Shape and Control of Linear and Nonlinear Wave Energy Converters.", Michigan Technological University, 2020 Publication	<1%
5	Submitted to International American University Student Paper	<1%
6	Submitted to University of Greenwich Student Paper	<1%
7	www.ir.juit.ac.in:8080 Internet Source	<1%
8	afrjcict.net Internet Source	<1%
9	Submitted to KDU College Sdn Bhd Student Paper	<1%
10	repository.sustech.edu Internet Source	<1%
11	www.coursehero.com Internet Source	<1%

GPT ZERO RESULT

Chapter 1

GPTZero Version 2025-06-02-base CHAPTER I - 7/20/2025

AI Report

We predict this text is

Human Generated

AI Probability

9%

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 I - 7/20/2025

GHIFARI GUNAWAN

CHAPTER I

INTRODUCTION

1.1 Problem Formulation

1.1.1 Background

Chapter 2

GPTZero Version 2025-06-02-base CHAPTER I - 7/20/2025

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 I - 7/20/2025

GHIFARI GUNAWAN

CHAPTER II

Specifications

1.1 Existing and Proposed System

1.1.1 Existing Business Process

Chapter 3

GPTZero Version 2025-06-02-base CHAPTER I - 7/20/2025

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 I - 7/20/2025

GHIFARI GUNAWAN

CHAPTER III

Design

1.1 Alternative Design Solutions Design

1.1.1 Alternative Solution 1: Multi Vulnerability Scanner Website

Chapter 4

GPTZero Version 2025-06-02-base CHAPTER I - 7/20/2025

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 I - 7/20/2025

GHIFARI GUNAWAN

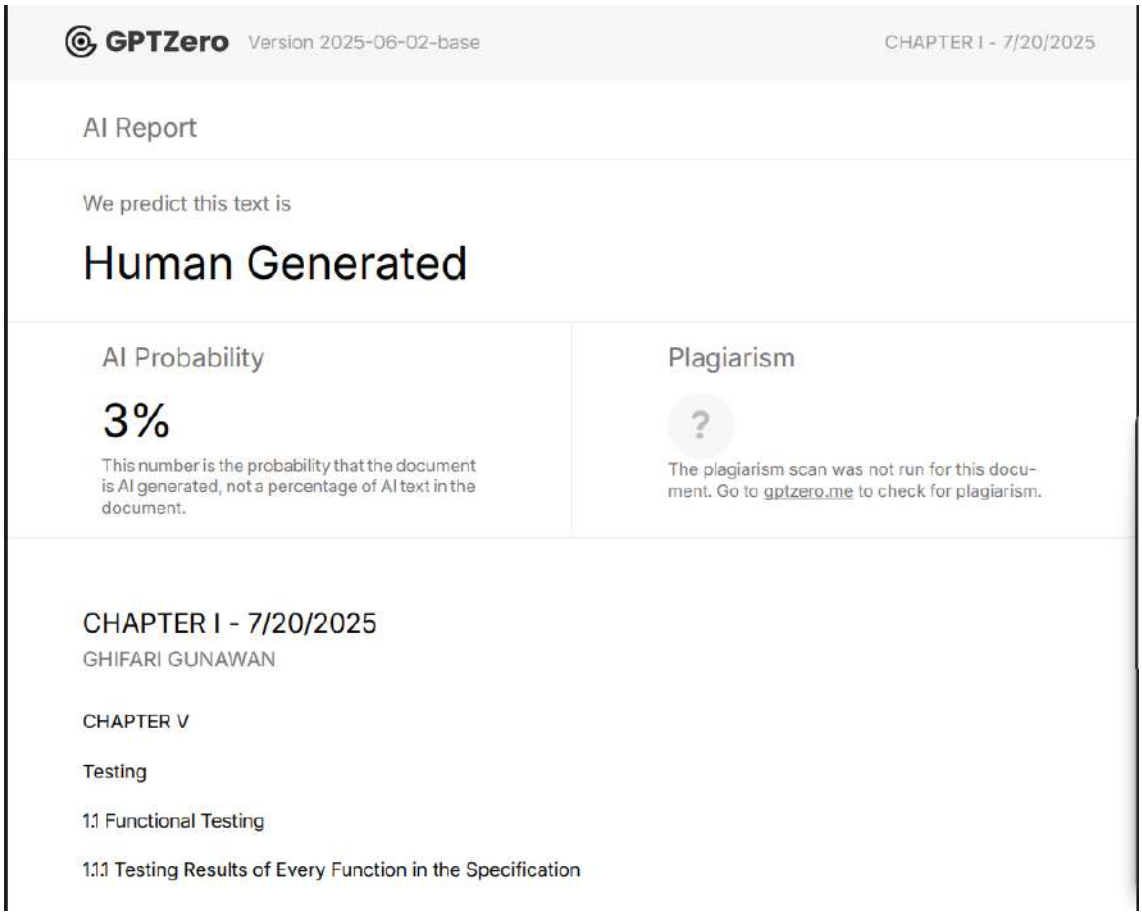
for Developing Multi Vulnerability Scanner

CHAPTER III

Implementation

1.1 Design Implementation

Chapter 5



GPTZero Version 2025-06-02-base CHAPTER I - 7/20/2025

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 I - 7/20/2025

GHIFARI GUNAWAN

CHAPTER V

Testing

1.1 Functional Testing

1.1.1 Testing Results of Every Function in the Specification

ABSTRACT

With the fast development of digital technology, cyber threats by malware and phishing attacks have gradually grown to be a regular and harmful occurrence. Most of these attacks focus on vital data, which comprise Personally Identifiable Information (PII), including Sensitive PII (SPII). The objective of this study is to develop a web-based Multi Vulnerability Scanner to help users identify threats originating from URLs, files, and emails in an accessible and user-friendly manner, even for those with minimal technical background. The system performs threat detection across multiple input types by analyzing URLs using a supervised machine learning model using XGBoost, inspecting email components such as domain reputation, suspicious links, and sender Ips using SVM, and evaluating uploaded files through hash matching and entropy analysis. The system successfully detects threats and provides detailed results and recommendations to users. This solution helps increase cybersecurity awareness and offers an effective way to protect against attacks via .exe files, emails and URLs

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 4
1.2.1 Accessibility 4
1.2.2 Accuracy 4
1.2.3 Security 4
1.3 Problem Functional Analysis 5
1.3.1 Multi Vulnerability Scanner Login & Sign-up Explanations 5
1.3.2 Multi Vulnerability Scanner Home Page Explanations 5
1.3.3 Multi Vulnerability Scanner Result Page Explanations 5
1.3.4 Multi Vulnerability Scanner History Page Explanations 6
1.4 Solution Selection 6
1.4.1 Alternative Solution 1 6
1.4.2 Alternative Solution 2 6
1.4.3 Alternative Solution 3 7
1.4.4 Solution Selection 7
1.5 Solution Usage Scenarios 7
1.5.1 Access with and without Login 7
1.5.2 Selecting Scanner 8
1.5.3 Scanning Process 8
1.5.4 Managing Scan Results 8
1.5.5 Repeated User 9
1.6 Development Effort 9
1.6.1 Man-months 9
1.6.2 Machine-months 9
1.6.3 Development Tools 10
1.6.4 Test Equipment 10

1.6.5 Timelines 10

CHAPTER II 11

Specifications 11
2.1 Existing and Proposed System 11
2.1.1 Existing Business Process 11
2.1.2 Proposed Business Process 13
2.2 Global Description of the Product 13
2.2.1 Main Functionality 13
2.2.2 User Characteristics 14
2.2.3 Constraints 15
2.2.4 Product Development Environment 16
2.2.5 Product Operational Environment 17
2.3 Requirement Analysis 17
2.3.1 External Interface 17
2.3.2 Functional Description 18
2.3.3 Data Requirement from user's perspective 23
2.3.4 Functional Requirement from user's perspective 25
2.3.5 Non-Functional Requirement 29
2.4 Specification Testing 30

CHAPTER III 32

Design 32
3.1 Alternative Design Solutions Design 32
3.1.1 Alternative Solution 1: Multi Vulnerability Scanner Website 32
3.1.2 Alternative Solution 2: Multi Vulnerability Scanner API 35
3.1.3 Alternative Solution 3: Multi Vulnerability Scanner Application 37
3.2 Rational/Systematic Design 40
3.2.1 Comparison Table 40
3.2.2 Quantitative Solution Selection 42
3.2.3 Solution Selection 46
3.3 Hierarchical/Iterative Design 47
3.3.1 Data Flow Diagram of Multi Vulnerability Scanner 47
3.3.2 Global Variable / Message Passing Interface 48
3.3.3 Agile Kanban Methodology to Implement Steps in Software Engineering . 50
3.3.4 Detail of Component and Library Used 51
3.3.5 Unified Modeling Language 2.0 54
3.4 Verification Demonstration and Proof of Design Process 58
3.5 Standard Used 60
3.6 Implementation and Testing Plans 61
3.6.1 Gantt Chart 61
3.6.2 S-Chart 62

CHAPTER IV **63**

Implementation **63**
4.1 Design Implementation 63
4.1.1 Function/Procedure/Class Implementation 63
4.1.2 Database Implementation 75
4.1.3 Integration Among Every Module 77
4.1.4 Implementation Verification 79
4.2 Product Display 82
4.2.1 Login Page 82
4.2.2 Register Page 82
4.2.3 Home Page / Dashboard 83
4.2.4 Email Scanner Page 86
4.2.5 URL Scanner Page 87
4.2.6 File Scanner Page 87
4.2.7 History Page 88
4.2.8 Full Report Page 89
4.2.9 Result Page 91
4.2.10 Tips Page 93
4.2.11 Comment Modal 94
4.2.12 Email Scanner Plugin 94
4.2.13 Email Scanner Plugin Result and Full Report 95
4.3 Component Cost Analysis 96
4.4 Manual Guide 97
4.4.1 System Build Documentation from the Source 97
4.4.2 System Installation 98
4.4.3 User Guide per User Role 99
4.5 Video Testing 101

CHAPTER V **102**

Testing **102**
5.1 Functional Testing 102
5.1.1 Testing Results of Every Function in the Specification 102
5.1.2 Present Qualitative Testing 105
5.1.3 Detail the Test Procedures 106
5.1.4 Procedures for the Demo 111
5.2 Testing Other Specifications 115
5.2.1 Non-Functional Specifications 115
5.2.2 Photos and Recording of the Test 116

LIST OF TABLES

TABLE Page
Table 1.6.1-1 Man Months 9
Table 2.2.2-1 User Characteristics 14
Table 2.3.2-1 Use Case Scenario for Register of Multi Vulnerability Scanner 19
Table 2.3.2-2 Use Case Scenario for Login of Multi Vulnerability Scanner 19
Table 2.3.2-3 Use Case Scenario for URL and File Scanner of Multi Vulnerability Scanner 20
Table 2.3.2-4 Use Case Scenario for Email Scanner of Multi Vulnerability Scanner 20
Table 2.3.2-5 Use Case Scenario for Comment of Multi Vulnerability Scanner 21
Table 2.3.2-6 Use Case Scenario for Scan History of Multi Vulnerability Scanner 22
Table 2.3.3-1 Users Data Dictionary of Multi Vulnerability Scanner 23
Table 2.3.3-2 Scans Data Dictionary of Multi Vulnerability Scanner 23
Table 2.3.3-3 Comment Data Dictionary of Multi Vulnerability Scanner 24
Table 3.2.1-1 Comparison Between Alternative Solutions 41
Table 3.2.2-1 The Rubrics of Criteria and Scale 42
Table 3.2.2-2 Quantitative Selection for Alternative Solution 1 43
Table 3.2.2-3 Quantitative Selection for Alternative Solution 2 44
Table 3.2.2-4 Quantitative Selection for Alternative Solution 3 45
Table 3.3.5-1 Verification Demonstration for Multi Vulnerability Scanner 58
Table 3.3.5-1 Standard Used of Multi Vulnerability Scanner 60
Table 4.1.4-1 Implementation Verification 79
Table 4.2.11-1 Component Cost Analysis of Multi Vulnerability Scanner 96
Table 5.1.1-1 Problem Functional Analysis Testing Results 102
Table 5.1.1-2 Functional Description Testing Results 103
Table 5.1.2-1 Present Qualitative Testing 105

LIST OF FIGURES

FIGURE Page
Figure 1.6.5-1 Timelines for Developing the System 10
Figure 2.1.1-1 Existing Email Threat Scanner Flow 11
Figure 2.1.1-2 Existing URL Threat Scanner Flow 12
Figure 2.1.1-3 Existing File Threat Scanner Flow 12
Figure 2.1.2-1 Proposed System Flow 13
Figure 2.3.2-1 Use Case Diagram of Multi Vulnerability Scanner 18
Figure 2.3.3-1 ERD of Multi Vulnerability Scanner 23
Figure 2.3.4-1 Context Diagram of Multi Vulnerability Scanner 25
Figure 2.3.4-2 Activity Diagram of Multi Vulnerability Scanner 26
Figure 2.3.4-3 Data Flow of Multi Vulnerability Scanner 27
Figure 3.1.1-1 Block Diagram Level 0 of Multi Vulnerability Scanner Website 32
Figure 3.1.1-2 Block Diagram Level 1 of Multi Vulnerability Scanner Website 33
Figure 3.1.2-1 Block Diagram Level 0 of Multi Vulnerability Scanner API 35
Figure 3.1.2-2 Block Diagram Level 1 of Multi Vulnerability Scanner API 36
Figure 3.1.3-1 Block Diagram Level 0 of Multi Vulnerability Scanner Application 37
Figure 3.1.3-2 Block Diagram Level 1 of Multi Vulnerability Scanner Application 38
Figure 3.2.2-1 Formula for Quantitative Selection 43
Figure 3.3.1-1 Data Flow Diagram Level 0 of Multi Vulnerability Scanner 47
Figure 3.3.1-2 Data Flow Diagram Level 1 of Multi Vulnerability Scanner 48
Figure 3.3.3-1 Kanban Board for Multi Vulnerability Scanner 51
Figure 3.3.5-1 Use Case Diagram for Multi Vulnerability Scanner 54
Figure 3.3.5-2 Activity Diagram of Multi Vulnerability Scanner 55
Figure 3.3.5-3 Class Diagram of Multi Vulnerability Scanner 56
Figure 3.3.5-4 Sequence Diagram of Multi Vulnerability Scanner 57
Figure 3.3.5-5 ERD for Multi Vulnerability Scanner 58
Figure 3.6.1-1 Gantt Chart for Developing Multi Vulnerability Scanner 61
Figure 3.6.2-1 S-Chart for Developing Multi Vulnerability Scanner 62
Figure 4.1.1-1 Data Flow Diagram Level 0 63
Figure 4.1.1-2 Data Flow Diagram Level 2 Authentication Process 64
Figure 4.1.1-3 Register Function Block Code 65
Figure 4.1.1-4 Login Function Block Code 66
Figure 4.1.1-5 Data Flow Diagram Level 2 URLs Scanner Process 67
Figure 4.1.1-6 URL Scanner Script Block Code 69
Figure 4.1.1-7 URL Scanner API Block Code 71
Figure 4.1.1-8 URL Scanner Controller Block Code 73
Figure 4.1.1-9 URL Scanner Result Block Code 74

Figure 4.1.2-1 Database Implementation of Multi Vulnerability Scanner 75
Figure 4.1.3-1 Data Flow Diagram Level 1 of Multi Vulnerability Scanner 77
Figure 4.2.1-1 Login Page of Multi Vulnerability Scanner 82
Figure 4.2.2-1 Register Page of Multi Vulnerability Scanner 83
Figure 4.2.3-1 Dashboard Page (Main Interface) of Multi Vulnerability Scanner 84
Figure 4.2.3-2 Dashboard Page (A Glimpse Before Scan) of Multi Vulnerability Scanner 84
Figure 4.2.3-3 Dashboard Page (Scan Lookup) of Multi Vulnerability Scanner 84
Figure 4.2.3-4 Dashboard Page (Scanner Selection) of Multi Vulnerability Scanner 85
Figure 4.2.4-1 Email Scanner Page of Multi Vulnerability Scanner 86
Figure 4.2.5-1 URL Scanner Page of Multi Vulnerability Scanner 87
Figure 4.2.6-1 File Scanner Page of Multi Vulnerability Scanner 87
Figure 4.2.7-1 History Page of Multi Vulnerability Scanner 88
Figure 4.2.8-1 Full Report Page (URL) of Multi Vulnerability Scanner 89
Figure 4.2.8-2 Full Report Page (File) of Multi Vulnerability Scanner 89
Figure 4.2.8-3 Full Report (Email) of Multi Vulnerability Scanner 90
Figure 4.2.9-1 Result Page (Safe) of Multi Vulnerability Scanner 91
Figure 4.2.9-2 Result Page (Not Safe) of Multi Vulnerability Scanner 91
Figure 4.2.9-3 Result Page (Suspicious) of Multi Vulnerability Scanner 92
Figure 4.2.10-1 Tips Page of Multi Vulnerability Scanner 93
Figure 4.2.11-1 Comment Modal of Multi Vulnerability Scanner 94
Figure 4.2.12-1 Email Scanner Plugin of Multi Vulnerability Scanner 94
Figure 4.2.13-1 Email Scanner Plugin Result of Multi Vulnerability Scanner 95
Figure 4.2.13-2 Email Scanner Plugin Full Report of Multi Vulnerability Scanner 96
Figure 5.2.2-1 Login Page Testing 116
Figure 5.2.2-2 Register Page Testing 116
Figure 5.2.2-3 Dashboard Page (Main Interface) Testing 117
Figure 5.2.2-4 Dashboard Page (A Glimpse Before Scan) Testing 117
Figure 5.2.2-5 Dashboard Page ((Search Scan Section) Testing 118
Figure 5.2.2-6 Dashboard Page (Select Scanner Type) Testing 118
Figure 5.2.2-7 URL Scanner Page Testing 119
Figure 5.2.2-8 File Scanner Page Testing 119
Figure 5.2.2-9 Email Scanner Page Testing 119
Figure 5.2.2-10 Result Page (Safe) Testing 120
Figure 5.2.2-11 Result Page (Not Safe) Testing 120
Figure 5.2.2-12 Result Page (Suspicious) Testing 121
Figure 5.2.2-13 Full Report Page (File) Testing 121
Figure 5.2.2-14 Full Report Page (URL) Testing 122
Figure 5.2.2-15 Full Report Page (Email) Testing 122
Figure 5.2.2-16 Tips Page Testing 123

Figure 5.2.2-17 History Page Testing 124
Figure 5.2.2-18 Comment Modal Testing..... 124
Figure 5.2.2-19 Email Scanner Plugin Test 125
Figure 5.2.2-20 Email Scanner Plugin Result Test..... 125
Figure 5.2.2-21 Email Scanner Plugin Full Report Test..... 126