



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:

MIKAIL WHANGYEE

001202200097

FACULTY OF COMPUTER SCIENCE

INFORMATICS STUDY PROGRAM

CIKARANG

AUGUST, 2025

SIMILARITY INDEX REPORT

Capstone Individual Report_Mikail
Whangyee_Informatics_2022.pdf

ORIGINALITY REPORT

6%	3%	3%	4%
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	afrjcict.net Internet Source	<1%
3	Submitted to University of Greenwich Student Paper	<1%
4	Submitted to University of Northumbria at Newcastle Student Paper	<1%
5	Lu, Cheng-Kuan. "Wireless Bi-directional Bio-potential Recording and Stimulation System.", Case Western Reserve University, 2020 Publication	<1%
6	Submitted to Sim University Student Paper	<1%
7	Submitted to KDU College Sdn Bhd Student Paper	<1%
8	Submitted to Higher Education Commission Pakistan Student Paper	<1%
9	repository.sustech.edu Internet Source	<1%

GPTZero Result

- CHAPTER I

 Version 2025-08-11-base

CHAPTER I - 8/20/2025

AI Report

We predict this text is

Human Generated

<div>AI Probability</div> <div>10%</div> <div><small>This number is the probability that the document is AI generated, not a percentage of AI text in the document.</small></div>	<div>Plagiarism</div> <div></div> <div><small>The plagiarism scan was not run for this document. Go to gptzero.me to check for plagiarism.</small></div>
---	--

CHAPTER I - 8/20/2025

Mikail

- CHAPTER II

 Version 2025-08-11-base

CHAPTER II - 8/20/2025

AI Report

We predict this text is

Human Generated

<div>AI Probability</div> <div>4%</div> <div><small>This number is the probability that the document is AI generated, not a percentage of AI text in the document.</small></div>	<div>Plagiarism</div> <div></div> <div><small>The plagiarism scan was not run for this document. Go to gptzero.me to check for plagiarism.</small></div>
--	--

CHAPTER II - 8/20/2025

Mikail

- CHAPTER III

 Version 2025-08-11-base

CHAPTER III - 8/20/2025

AI Report

We predict this text is

Human Generated

<div>AI Probability</div> <div>0%</div> <div><small>This number is the probability that the document is AI generated, not a percentage of AI text in the document.</small></div>	<div>Plagiarism</div> <div></div> <div><small>The plagiarism scan was not run for this document. Go to gptzero.me to check for plagiarism.</small></div>
--	--

CHAPTER III - 8/20/2025

Mikail

- CHAPTER IV

 Version 2025-08-11-base

CHAPTER IV - 8/20/2025

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 IV - 8/20/2025

Mikail

- CHAPTER V

 Version 2025-08-11-base

CHAPTER V - 8/20/2025

AI Report

We predict this text is

Human Generated

AI Probability

1%

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 V - 8/20/2025

Mikail

ABSTRACT

The growing number of cyber threats, especially malware and phishing, poses serious risks to both personal and sensitive information in today's digital world. This research aims to develop a user-oriented web application to assist individuals in identifying and mitigating cybersecurity threats originating from various digital inputs such as URLs, emails, and file attachments. The system was developed using the Agile methodology, which enabled iterative development, continuous user feedback, and flexible refinement throughout the project lifecycle. The system combines machine learning, reputation analysis, and external service integration to detect suspicious behaviour effectively. Designed to be accessible for all users, the application provides a simple interface and clear, interactive scan results. It also helps users recognize threats hidden in the digital content they commonly interact with. Testing shows that the system can detect different types of threats accurately and supports user awareness of digital security.

TABLE OF CONTENTS

	Page
ABSTRACT.....	v
DEDICATION.....	vi
ACKNOWLEDGMENTS	vii
LIST OF TABLES.....	xii
LIST OF FIGURES	xiii
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.....	15
2.2.5	Product Operational Environment	16
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.....	22
2.3.4	Functional Requirement from user's perspective	24
2.3.5	Non-Functional Requirement.....	28
2.4	Specification Testing	29
CHAPTER III		31
DESIGN		31
3.1	Alternative Design Solutions Design.....	31
3.1.1	Alternative Solution 1: Multi Vulnerability Scanner Website	31
3.1.2	Alternative Solution 2: Multi Vulnerability Scanner API	34
3.1.3	Alternative Solution 3: Multi Vulnerability Scanner Application.....	36
3.2	Rational/Systematic Design.....	39
3.2.1	Comparison Table.....	39
3.2.2	Quantitative Solution Selection	40
3.2.3	Solution Selection	45
3.3	Hierarchical/Iterative Design.....	46
3.3.1	Data Flow Diagram of Multi Vulnerability Scanner	46
3.3.2	Global Variable / Message Passing Interface	47
3.3.3	Agile Kanban Methodology to Implement Steps in Software Engineering.....	48
3.3.4	Detail of Component and Library Used.....	49
3.3.5	Unified Modeling Language 2.0	52
3.4	Verification Demonstration and Proof of Design Process.....	55
3.5	Standard Used	57

3.6	Implementation and Testin Plans.....	58
3.6.1	Gantt Chart.....	58
3.6.2	S-Chart	58
CHAPTER IV.....		59
IMPLEMENTATION		59
4.1	Design Implementation.....	59
4.1.1	Function/Procedure/Class Implementation.....	59
4.1.2	Database Implementation.....	68
4.1.3	Integration Among Every Module	69
4.1.4	Implementation Verification	70
4.2	Product Display.....	72
4.2.1	Login Page	73
4.2.2	Register Page	73
4.2.3	Home Page / Dashboard.....	74
4.2.4	Email Scanner Page	76
4.2.5	URL Scanner Page.....	77
4.2.6	File Scanner Page.....	77
4.2.7	History Page.....	78
4.2.8	Full Report Page	79
4.2.9	Result Page.....	81
4.2.10	Tips Page.....	83
4.2.11	Comment Modal	84
4.2.12	Email Scanner Plugin.....	84
4.2.13	Email Scanner Plugin Result and Full Report	85
4.3	Component Cost Analysis.....	86
4.4	Manual Guide.....	86
4.4.1	System Build Documentation from the Source	86
4.4.2	System Installation.....	88
4.4.3	User Guide per User Role	89
4.5	Video Demonstration	90
CHAPTER V		91
Testing.....		91
5.1	Functional Testing	91
5.1.1	Testing Results of Every Function in the Specification.....	91
5.1.2	Present Qualitative Testing	93
5.1.3	Detail the Test Procedures	95
5.1.4	Procedures for the Demo	99
5.2	Testing Other Specifications.....	102
5.2.1	Non-Functional Specifications.....	102
5.2.2	Photos and Recording of the Test	104
APPENDIX.....		118

LIST OF TABLES

TABLE	Page
Table 1.6.1-1 Man Months.....	9
Table 2.2.2-1 User Characteristic	14
Table 2.3.2-1 Use Case Scenario for Register of Multi Vulnerability Scanner.....	18
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 Scanners of.....	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	21
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	23
Table 3.2.1-1 Comparison Between Alternative Solutions	40
Table 3.2.2-1 The Rubrics of Criteria and Scale	41
Table 3.2.2-2 Quantitative Selection for Alternative Solution 1	42
Table 3.2.2-3 Quantitative Selection for Alternative Solution 2	43
Table 3.2.2-4 Quantitative Selection for Alternative Solution 3	44
Table 3.3.5-1 Verification Demonstration for Multi Vulnerability Scanner	55
Table 3.3.5-1 Standard Used of Multi Vulnerability Scanner	57
Table 4.1.4-1 Implementation Verification	70
Table 4.2.11-1 Component Cost Analysis of Multi Vulnerability Scanner.....	86
Table 5.1.1-1 Problem Functional Analysis Testing Results.....	91
Table 5.1.1-2 Functional Description Testing Results.....	92
Table 5.1.2-1 Present Qualitative Testing.....	94
Table 5.2.1-1 Non-Functional Specifications Testing	102

LIST OF FIGURES

FIGURE	Page
Figure 1.6.5-1 Timelines for Developing 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	22
Figure 2.3.4-1 Context Diagram of Multi Vulnerability Scanner.....	24
Figure 2.3.4-2 Activity Diagram of Multi Vulnerability Scanner	25
Figure 2.3.4-3 Data Flow of Multi Vulnerability Scanner.....	26
Figure 3.1.1-1 Block Diagram Level 0 of Multi Vulnerability Scanner Website.....	31
Figure 3.1.1-2 Block Diagram Level 1 of Multi Vulnerability Scanner Website.....	32
Figure 3.1.2-1 Block Diagram Level 0 of Multi Vulnerability Scanner API	34
Figure 3.1.2-2 Block Diagram Level 1 of Multi Vulnerability Scanner API	35
Figure 3.1.3-1 Block Diagram Level 0 of Multi Vulnerability Scanner Application.....	36
Figure 3.1.3-2 Block Diagram Level 1 of Multi Vulnerability Scanner Application.....	37
Figure 3.2.2-1 Formula for Quantitative Selection.....	42
Figure 3.3.1-1 Data Flow Diagram Level 0 of Multi Vulnerability Scanner	46
Figure 3.3.1-2 Data Flow Diagram Level 1 of Multi Vulnerability Scanner	46
Figure 3.3.3-1 Kanban Board for Multi Vulnerability Scanner.....	49
Figure 3.3.5-1 Use Case Diagram for Multi Vulnerability Scanner	52
Figure 3.3.5-2 Activity Diagram of Multi Vulnerability Scanner	53
Figure 3.3.5-3 Class Diagram of Multi Vulnerability Scanner.....	54
Figure 3.3.5-4 Sequence Diagram of Multi Vulnerability Scanner	54
Figure 3.3.5-5 ERD for Multi Vulnerability Scanner	55
Figure 3.6.1-1 Gantt Chart for Developing Multi Vulnerability Scanner.....	58
Figure 3.6.2-1 S-Chart for Developing Multi Vulnerability Scan	58
Figure 4.1.1-1 Block Diagram Level 0	59
Figure 4.1.1-2 A Glimpse Before Scan Controller Function Code.....	60
Figure 4.1.1-3 A Glimpse Before Scan Section View Code.....	61
Figure 4.1.1-4 Scan Look Up Function Code	62
Figure 4.1.1-5 Data Flow Diagram Level 2 File Scanner Process.....	63
Figure 4.1.1-6 File Scanner Script	64
Figure 4.1.1-7 File Scanner Controller Code.....	66
Figure 4.1.1-8 File Scanner View Page Code.....	67

Figure 4.1.1-9 File Result Report Template Code.....	67
Figure 4.1.2-1 Database Implementation.....	68
Figure 4.1.3-1 Data Flow Diagram Level 1	69
Figure 4.2.1-1 Login Page of Multi Vulnerability Scanner	73
Figure 4.2.2-1 Register Page of Multi Vulnerability Scanner	73
Figure 4.2.3-1 Dashboard Page (Main Interface) of Multi Vulnerability Scanner	74
Figure 4.2.3-2 Dashboard Page (A Glimpse Before Scan) of Multi Vulnerability Scanner	74
Figure 4.2.3-3 Dashboard Page (Scan Lookup) of Multi Vulnerability Scanner	75
Figure 4.2.3-4 Dashboard Page (Scanner Selection) of Multi Vulnerability Scanner.....	75
Figure 4.2.4-1 Email Scanner Page of Multi Vulnerability Scanner	76
Figure 4.2.5-1 URL Scanner Page of Multi Vulnerability Scanner.....	77
Figure 4.2.6-1 File Scanner Page of Multi Vulnerability Scanner	77
Figure 4.2.7-1 History Page of Multi Vulnerability Scanner.....	78
Figure 4.2.8-1 Full Report Page (URL) of Multi Vulnerability Scanner.....	79
Figure 4.2.8-2 Full Report Page (File) of Multi Vulnerability Scanner	79
Figure 4.2.8-3 Full Report (Email) of Multi Vulnerability Scanner.....	79
Figure 4.2.9-1 Result Page (Safe) of Multi Vulnerability Scanner.....	81
Figure 4.2.9-2 Result Page (Not Safe) of Multi Vulnerability Scanner.....	81
Figure 4.2.9-3 Result Page (Suspicious) of Multi Vulnerability Scanner	82
Figure 4.2.10-1 Tips Page of Multi Vulnerability Scanner	83
Figure 4.2.11-1 Comment Modal of Multi Vulnerability Scanner	84
Figure 4.2.12-1 Email Scanner Plugin of Multi Vulnerability Scanner	84
Figure 4.2.13-1 Email Scanner Plugin Result of Multi Vulnerability Scanner	85
Figure 4.2.13-2 Email Scanner Plugin Full Report of Multi Vulnerability Scanner	85
Figure 5.2.2-1 Login Page Testing	104
Figure 5.2.2-2 Register Page Testing.....	104
Figure 5.2.2-3 Dashboard Page (Main Interface) Testing	105
Figure 5.2.2-4 Dashboard Page (A Glimpse Before Scan) Testing.....	105
Figure 5.2.2-5 Dashboard Page ((Search Scan Section) Testing.....	105
Figure 5.2.2-6 Dashboard Page (Select Scanner Type) Testing	106
Figure 5.2.2-7 URL Scanner Page Testing	106
Figure 5.2.2-8 File Scanner Page Testing.....	107
Figure 5.2.2-9 Email Scanner Page Testing.....	107
Figure 5.2.2-10 Result Page (Safe) Testing.....	108
Figure 5.2.2-11 Result Page (Not Safe) Testing	108
Figure 5.2.2-12 Result Page (Suspicious) Testing.....	108
Figure 5.2.2-13 Full Report Page (File) Testing.....	109
Figure 5.2.2-14 Full Report Page (URL) Testing	109
Figure 5.2.2-15 Full Report Page (Email) Testing	110

Figure 5.2.2-16 Tips Page Testing.....	111
Figure 5.2.2-17 History Page Testing	112
Figure 5.2.2-18 Comment Modal Testing.....	112
Figure 5.2.2-19 Email Scanner Plugin Test.....	113
Figure 5.2.2-20 Email Scanner Plugin Result Test.....	113
Figure 5.2.2-21 Email Scanner Plugin Full Report Test.....	114