FAZSCAN:

Cross-Platform Software Application as Scanner of Information and Security of Websites

M.Fazri Nizar (mfazri.lpb2021@gmail.com) (SMA Negeri 4 OKU)
Supervisor: Sri Lorita, M.Pd.

CENTER FOR YOUNG SCIENTISTS
APCYS 2022

INTRODUCTION

Users safety while browsing websites and websites security concern. The internet penetration rate was at 73.7 percent of total population of Indonesia. That means, there were about 204.7 million of internet users in Indonesia in the beginning of 2022. The cyber security becomes a concern, both for users and websites.

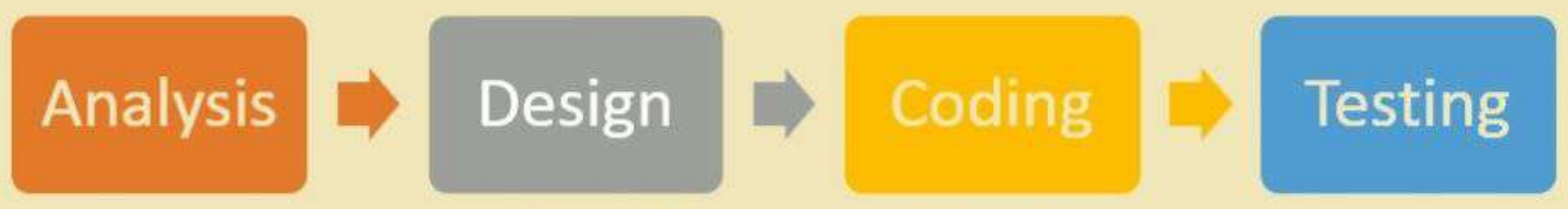
Flutter was used in the development as the framework of the software application. It is expected to provide ease of use, ease-to-read website security scan results and the usability in many platforms (cross-platform ability of Flutter).

PROBLEM FORMULATIONS

1. How does FazScan work?
2. How ease of use is FazScan for common users?
3. Is FazScan effective for analyzing the information and security of websites?

RESEARCH METHODOLOGY

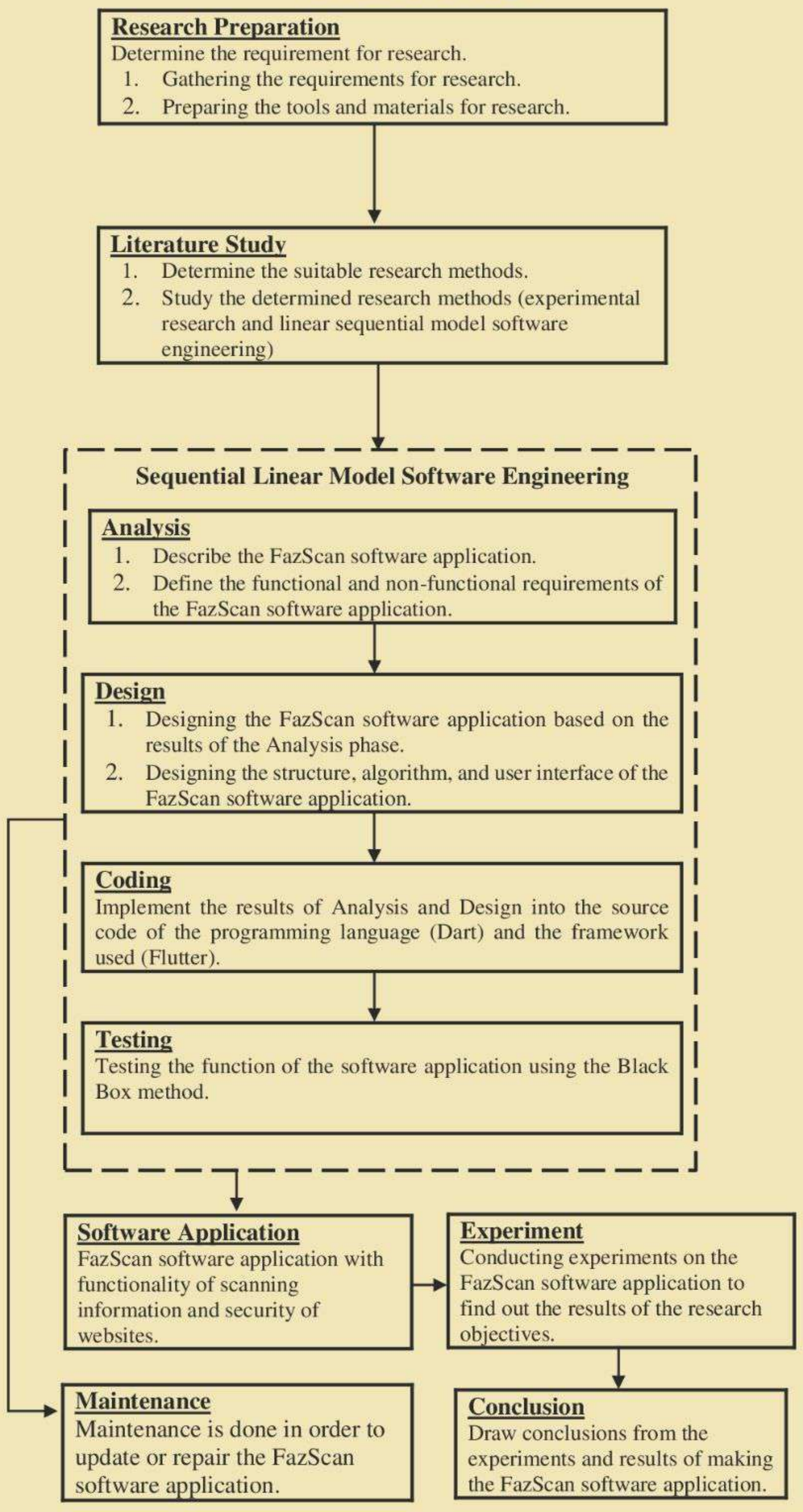
1. Literature Study/Review.
2. Experimental Research.
3. Linear Sequential Model Software Engineering.



Linear Sequential Model

The research methods consisted of the data collection process, the software development/engineering process, and the experimental process. In this research, the data collection method is study literature from credible sources. The data collected are regarding software, programming language, Dart programming language, framework, Flutter framework, operating system, website scanning, and cross-platform. The software development/engineering process was carried out using the linear sequential model. The linear sequential model is a continuity software development process, where the progress is seen as a waterfall flowing down through the phases of analysis, design, coding, and testing (Pressman, 1994). The experimental process was conducted to test the effectivity of FazScan vulnerability scanning to various websites.

Research Design



Research Preparation
Determine the requirement for research.
1. Gathering the requirements for research.
2. Preparing the tools and materials for research.

Literature Study
1. Determine the suitable research methods.
2. Study the determined research methods (experimental research and linear sequential model software engineering)

Sequential Linear Model Software Engineering

Analysis
1. Describe the FazScan software application.
2. Define the functional and non-functional requirements of the FazScan software application.

Design
1. Designing the FazScan software application based on the results of the Analysis phase.
2. Designing the structure, algorithm, and user interface of the FazScan software application.

Coding
Implement the results of Analysis and Design into the source code of the programming language (Dart) and the framework used (Flutter).

Testing
Testing the function of the software application using the Black Box method.

Software Application
FazScan software application with functionality of scanning information and security of websites.

Experiment
Conducting experiments on the FazScan software application to find out the results of the research objectives.

Maintenance
Maintenance is done in order to update or repair the FazScan software application.

Conclusion
Draw conclusions from the experiments and results of making the FazScan software application.

RESULT & ANALYSIS

The algorithm structure of the FazScan software application in brief is to scan the URL of the target website as input from user then process the scanned content with various algorithms and then display it in the form of a user interface (see program flowchart).

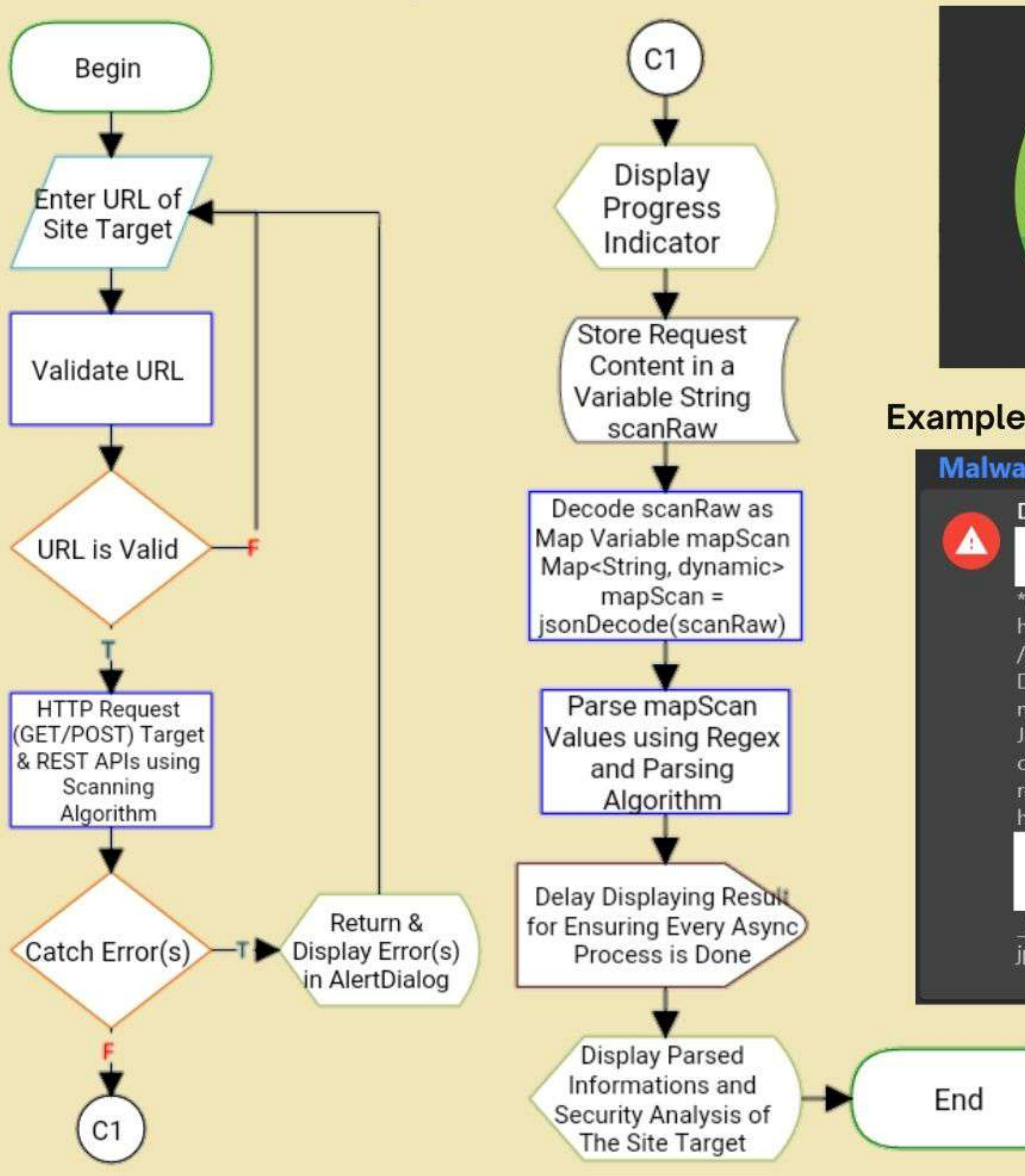
Risk Name	Range	Detection
Minimal	0-0.5	General Info
Low	0.5-1.5	Recommendation Security Informations
Medium	1.5-2.5	Outdated Systems, No SSL
High	2.5-3.5	Malware/Hacked Warns
Malicious	3.5-4.0	Domain Blacklisted

As a conclusion of scanning result, FazScan will display a Risk Meter graph with the information shown on the table above. The classifications of risk level as a result of security vulnerability detection are based on CVE & CWE report.

The scanning results are (if detected) General Informations (Input, Site, Domain, IP, CMS, CDN, and Hosting), Blacklist/Whitelist Informations (including Kominfo TrustPositif), System Details (System Error, System Info, and System Notice), WebApp Informations (WebApp Info, WebApp Notice, and WebApp Name & Version), Outdated Informations, Recommendation Security Informations, Malware Security Warnings, Link Lists (IFrame, JS External, JS Local, and URL), and JS Library Vulnerability.

The malicious risk classification of blacklisted domain of websites is based on the fact that mostly the websites are detected for doing malicious activity (e.g. phishing, illegal pornography, etc.) or severe infection of malware (e.g. malicious JS library that conducts cryptojacking).

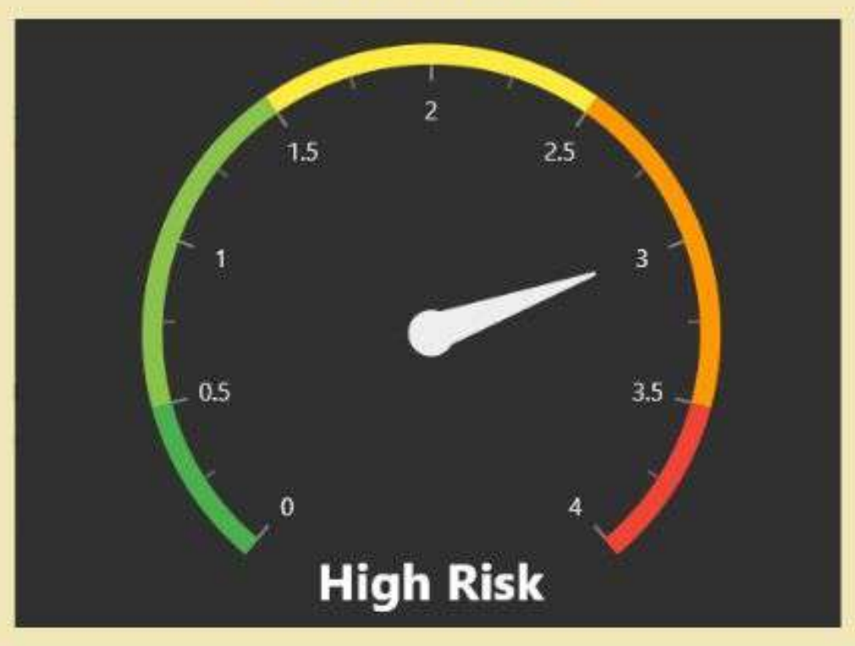
Program Flowchart



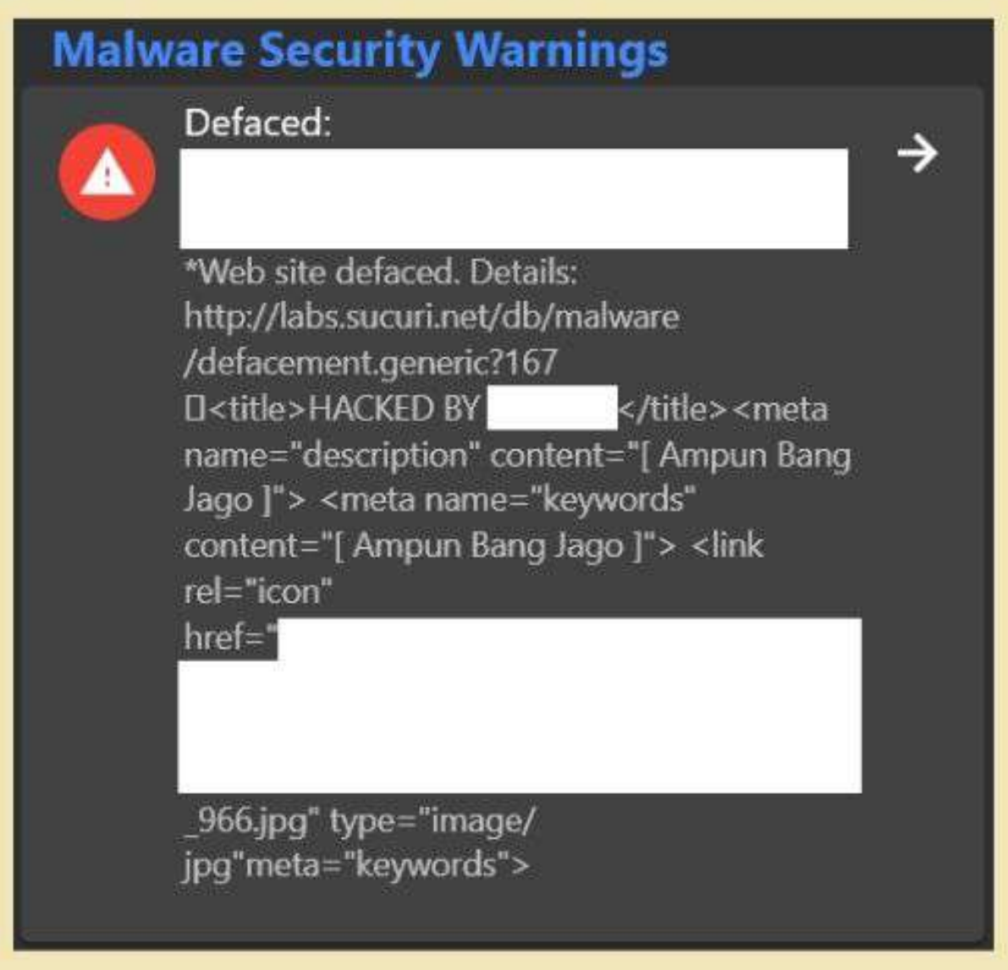
Begin
Enter URL of Site Target
Validate URL
URL is Valid
F
T
HTTP Request (GET/POST) Target & REST APIs using Scanning Algorithm
Catch Error(s)
T
Return & Display Error(s) in AlertDialog
F
C1

C1
Display Progress Indicator
Store Request Content in a Variable String scanRaw
Decode scanRaw as Map Variable mapScan Map<String, dynamic> mapScan = jsonDecode(scanRaw)
Parse mapScan Values using Regex and Parsing Algorithm
Delay Displaying Result for Ensuring Every Async Process is Done
Display Parsed Informations and Security Analysis of The Site Target
End

Risk Meter



Example of Malware/Hacked Detection



Malware Security Warnings

Defaced:
[redacted]
*Web site defaced. Details: http://labs.sucuri.net/db/malware/defacement.generic?167
□<title>HACKED BY [redacted]</title><meta name="description" content="[Ampun Bang Jago]"> <meta name="keywords" content="[Ampun Bang Jago]"> <link rel="icon" href="[redacted]_966.jpg" type="image/jpg"meta="keywords">

CONCLUSION

1. Simple ways of working, FazScan scans the target URL of the website that is inputted by user then display the scanning result to the user interface screen.
2. FazScan is easy to use and be operated by users because the researcher keep the user interface clean and simple.
3. FazScan is effective on fast-analyzing the security vulnerability scanning result of website and conclude it into Risk Meter.

FUTURE WORK

1. Expand cross-platform ability to reach other operating systems users.
2. Implementing new security vulnerability scanning functions (SQLi, CSRF, etc.).
3. Performing performance analysis on FazScan.

REFERENCES

[1] Chaudhuri, A. B. 2020. *Flowchart and Algorithm Basics: The Art of Programming*. Dulles: Mercury Learning & Information.

[2] Gao, J., et al. 2003. *Testing and Quality Assurance for Component-based Software*. Norwood: Artech House, Inc.

[3] Pressman, R. S. 1994. *Software Engineering: A Practitioner's Approach*. New York City: New York McGraw-Hill, Inc.

[4] Zammetti, F. 2019. *Practical Flutter*. New York City: Apress.