

**ANALYSIS AND IMPLEMENTATION OF THE SHA-256 ALGORITHM
ON WEB SECURITY AGAINST SQL INJECTION ATTACKS**

UNDERGRADUATE THESIS



arranged by

R. Allail Sukma Kamandanu

15.61.0045

**DEGREE PROGRAM
STUDY PROGRAM INFORMATICS
FACULTY OF COMPUTER SCIENCE
AMIKOM UNIVERSITY YOGYAKARTA
YOGYAKARTA
2019**

**ANALYSIS AND IMPLEMENTATION OF THE SHA-256 ALGORITHM
ON WEB SECURITY AGAINST SQL INJECTION ATTACKS**

UNDERGRADUATE THESIS

to fulfill some requirements to achieve a Bachelor's degree
in the Informatics Study Program



arranged by

R. Allail Sukma Kamandanu

15.61.0045

**BACHELOR DEGREE
STUDY PROGRAM INFORMATICS
FACULTY OF COMPUTER SCIENCE
AMIKOM UNIVERSITY YOGYAKARTA
YOGYAKARTA
2019**

APPROVAL

THESIS

**ANALYSIS AND IMPLEMENTATION OF THE SHA-256 ALGORITHM
ON WEB SECURITY AGAINST SQL INJECTION ATTACKS**

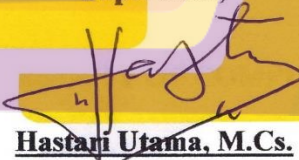
prepared and compiled by

R. Allail Sukma Kamandanu

15.61.0045

has been approved by the Thesis Supervisor
on February 11, 2019

Supervisor,



Hastari Utama, M.Cs.

NIK. 190302230

ATTESTATION

THESIS

**ANALYSIS AND IMPLEMENTATION OF THE SHA-256 ALGORITHM
ON WEB SECURITY AGAINST SQL INJECTION ATTACKS**

prepared and compiled by

R. Allail Sukma Kamandanu

15.61.0045

has been maintained in front of the Board of Examiners

on February 22, 2019

Board of Examiners

Examiners

Signature

Windha Mega Pradnya D, M.Kom.

NIK. 190302185

Erni Seniwati, S.Kom, M.Cs.

NIK. 190302231

Anggit Dwi Hartanto, M.Kom.

NIK. 190302163



This thesis has been accepted as one of the requirements to obtain a Bachelor of
Computer degree on March 4, 2019

DEAN OF THE FACULTY OF COMPUTER SCIENCE



Krisnawati, S.Si, M.T.

NIK. 190302038

STATEMENT

I, the undersigned, hereby declare that, this thesis is my own (ORIGINAL) work, and the contents of this thesis do not have works submitted by others to obtain an academic degree at any higher education institution, and as long as my knowledge is not works or opinions that have been written and / or published by others, except those written in this text and mentioned in the bibliography.

Everything related to the manuscript and the work that has been made is my personal responsibility.

Yogyakarta, 01 March 2019



R.Allail Sukma Kamandanu

NIM. 15.61.0045

MOTTO

“How stupid a human being is, he destroys the present while worrying about the future, but cries in the future by remembering his past.”

(Ali bin Abi Thalib)

“I have no special talent. I just have a passionate curiosity.”

(Albert Einstein)

“I always want to be someone else. But now I realize I should have been more specific.”

(Lily Tomlin)

“You will live longer when you realize that spending time grieving is useless.”

(Ruth E. Renki)

DEDICATION

I thank Allah God Almighty for giving His blessings, mercy and guidance so that I can finish this Thesis well. I also feel grateful to the people around me who have directly or indirectly helped me in working on this Thesis. . I present this thesis to :

1. My father, R. Pamungkas Sulisty H, My mother, Marga Ruliati, and my younger brother R. Zidane Damar Jatmiko and my little one brother, R. Handaru Adiwira who always prayed for, encouraged, and supported me.
2. Mr Hastari Utama, M.Cs. as a supervisor who always provides input and guidance in completing the Thesis.
3. To Ripto Sudiarno as a best friend and mentor who has given his knowledge to help conduct research.
4. My DotD friends, Aziz Naufal Alauddin Nadian, Abdul Aziz Istanto Wibowo, and Gema Kumara Riskianto Putra, who always give encouragement and motivation to immediately complete the Thesis.
5. My friends Rasyiid Indra Parmadi, Dhismas Haryo, Raka Putra Wicaksana, Mukhlis Purnama, Enrico Praditya, and Fachruddin Sujatmiko who always help entertain and help in distress.
6. 15BCI classmates, AMIKOM assistants, public relations, and organizations that have become my friends during college.

As well as all those who have helped and supported me that I cannot mention one by one.

ACKNOWLEDGEMENTS

Thank you we pray to Allah SWT for His blessings and gifts so that the writer can complete the thesis report in time with the title "ANALYSIS AND IMPLEMENTATION OF THE SHA-256 ALGORITHM ON WEB SECURITY AGAINST SQL INJECTION ATTACKS" This thesis was prepared to complete the final assignment of college and fulfill the graduation requirements of the Bachelor Informatics Education program at Amikom University Yogyakarta. During the education of Bachelor Informatics up to the Thesis completion process, various parties have provided facilities, assisted, fostered, and guided the writer for that especially to:

1. Mr. Prof. Dr. M. Suyanto, MM as Chancellor of the Amikom University in Yogyakarta who has provided many facilities in completing education..
2. Mr. Hastari Utama, M.Cs. as a supervisor who has spent a lot of time and energy guiding the author during the preparation of this thesis..
3. Mr / Mrs. Lecturer at Amikom University Yogyakarta who has provided writers with several useful disciplines..
4. Friends in arms of Bachelor Informatics Students in 2015, who have discussed and collaborate with writers during their education..

The author realizes, this thesis still has many weaknesses and weaknesses. Therefore, constructive criticism and suggestions will be welcomed, hopefully, the existence of this thesis can be useful and increase our insight, especially about Web Security.

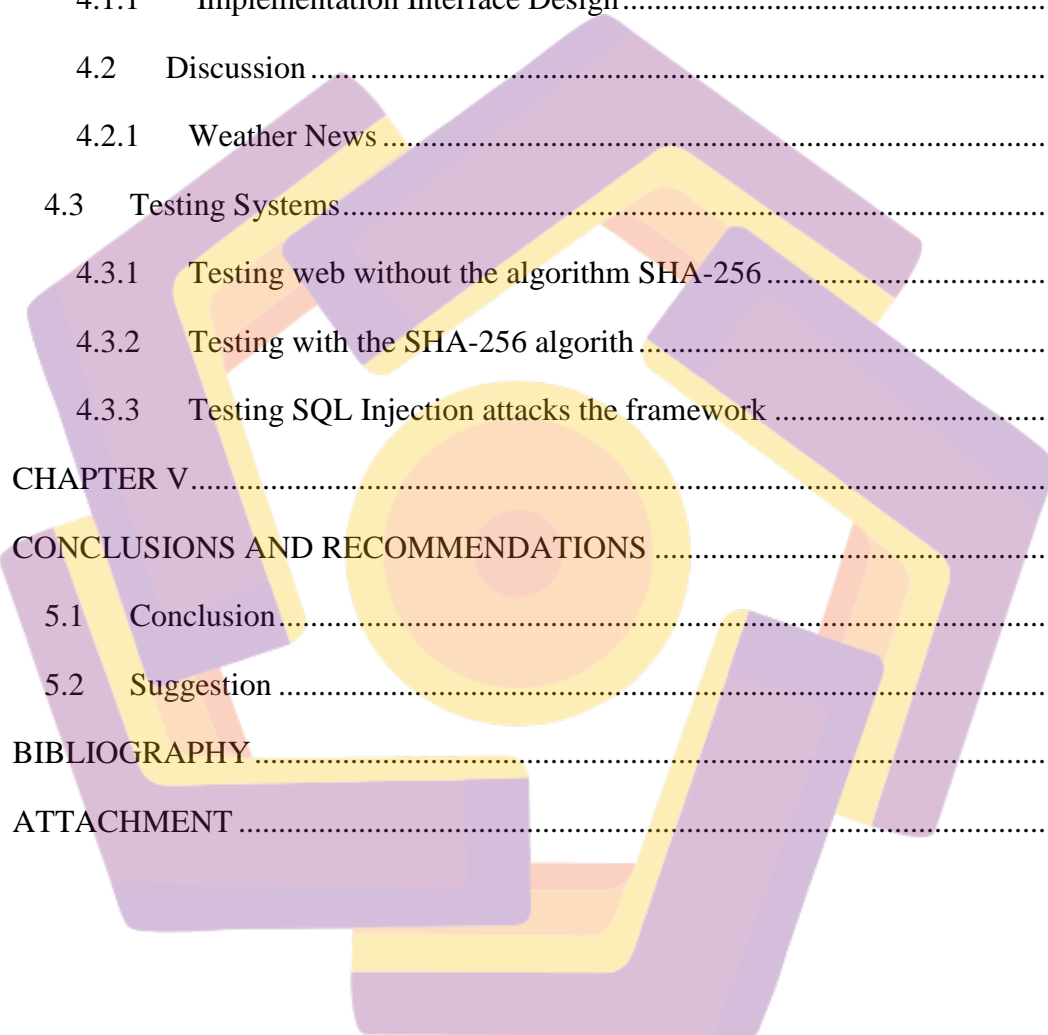
Yogyakarta, February 2019

Author

TABLE OF CONTENTS

COVER	i
TITLE.....	ii
APPROVAL THESIS.....	<u>iii</u>
ATTESTATION THESIS.....	iv
STATEMENT.....	v
MOTTO	vi
DEDICATION.....	vii
ACKNOWLEDGEMENTS	viii
TABLE OF CONTENTS.....	ix
LIST OF TABLES	xii
LIST OF FIGURES	xiii
ABSTRACT.....	xv
CHAPTER I.....	1
1.1 Background	1
1.2 Formulation of the problem.....	2
1.3 Initial hypothesis	3
1.4 Scope of problem.....	3
1.5 Research methods.....	3
1.6 Writing system	5

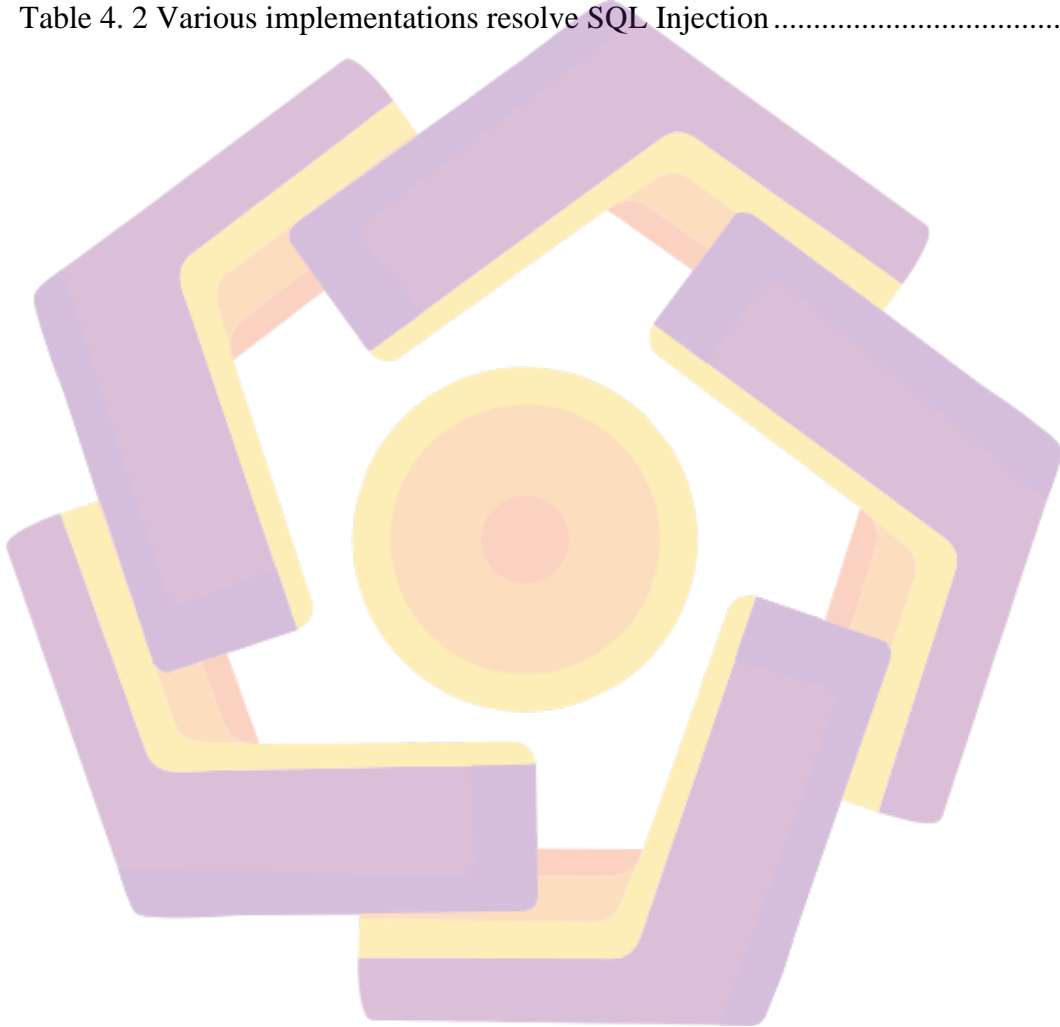
CHAPTER II.....	6
LITERATURE AND THEORETICAL BASIS	6
2.1 Literature review	6
2.2 Theoretical basis.....	7
2.2.1 System Security.....	7
2.2.2 Cryptography	9
2.2.2 Hash Function	15
2.2.3 Web Based Application.....	18
2.2.4 SQL Injection.....	19
2.2.5 Secure Hash Algorithm 2 (SHA-256).....	21
CHAPTER III	29
3.1 Flow Research	29
3.1.1 Determining the topic of research.....	30
3.1.2 Conducting literature study and determination of the theoretical basis	30
3.1.3 Data Collection and Analysis.....	30
3.1.4 Define Problems.....	30
3.1.5 System Design and Implementation System.....	31
3.1.6 Testing System.....	31
3.1.7 Conclusions and recommendations.....	33
3.2 Analysis	34
3.2.1 Analysis of Needs	34
3.2.2 Process Analysis Hash	35
3.2.3 Analysis method.....	42



CHAPTER IV	51
IMPLEMENTATION AND DISCUSSION.....	51
4.1 Implementation.....	51
4.1.1 Implementation Interface Design.....	51
4.2 Discussion	52
4.2.1 Weather News	53
4.3 Testing Systems.....	56
4.3.1 Testing web without the algorithm SHA-256	57
4.3.2 Testing with the SHA-256 algorithm.....	60
4.3.3 Testing SQL Injection attacks the framework	62
CHAPTER V.....	65
CONCLUSIONS AND RECOMMENDATIONS	65
5.1 Conclusion.....	65
5.2 Suggestion	65
BIBLIOGRAPHY.....	66
ATTACHMENT	69

LIST OF TABLES

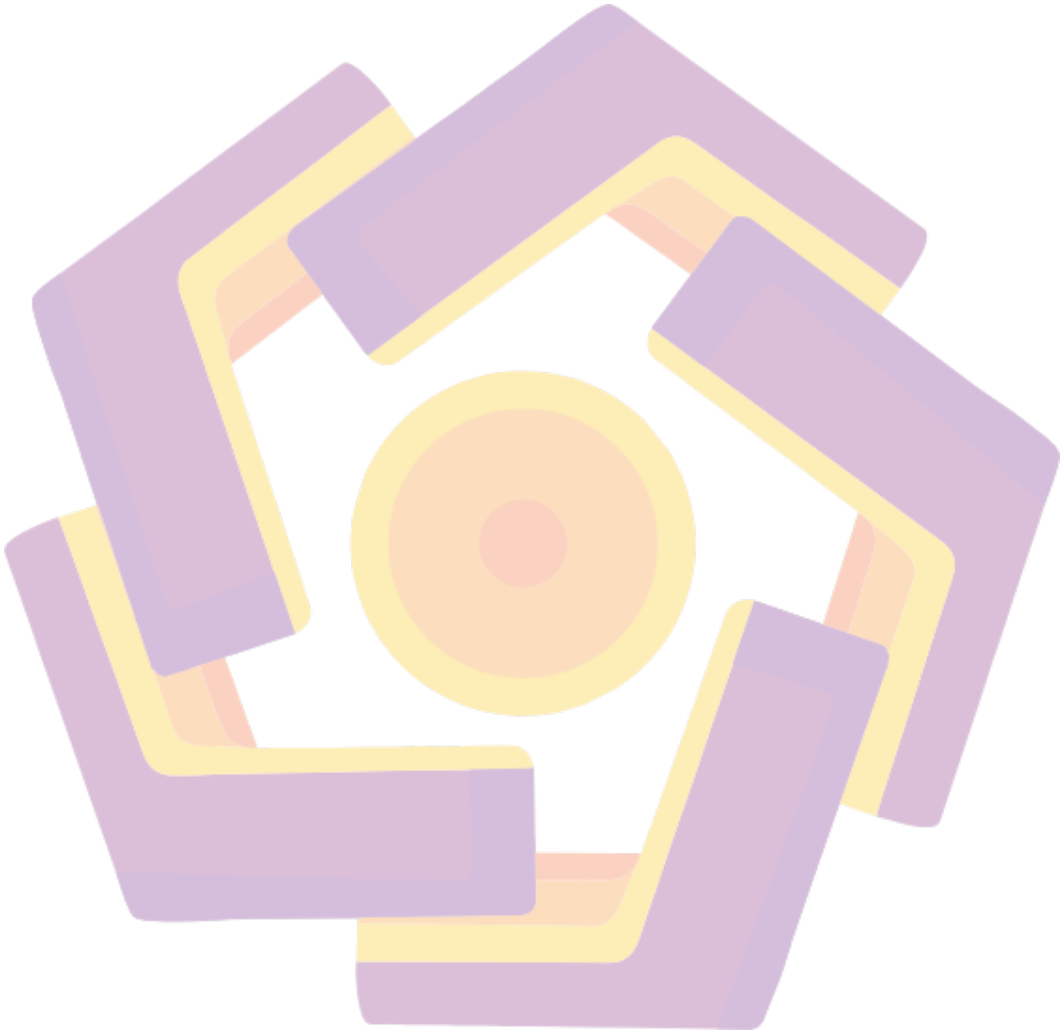
Table 4. 1 Types of test query SQL Injection	61
Table 4. 2 Various implementations resolve SQL Injection	64



LIST OF FIGURES

Figure 2. 1 Systems Web Applications	8
Figure 2. 2 Surveys Web Application Attacks.....	9
Figure 2. 3 Web Application Attacks Per 3 Months Year 2017	10
Figure 2. 4 Process Encryption / Decryption Algorithm Symmetric	14
Figure 2. 5 Process Encryption / Decryption Algorithm Asymmetric.....	14
Figure 2. 6 Testing the integrity of the message with the hash function	16
Figure 2. 7 Hash functions with iterations	17
Figure 2. 8 Preprocessing stages on SHA-256.....	25
Figure 2. 9 Computation on SHA-256 hash stage.....	27
Figure 3. 1 Flowchart Flow Research	30
Figure 3. 2 Web Test Dummy Flowchart.....	32
Figure 3. 3 Flowchart Web SHA-256	33
Figure 3. 4 Flowchart Client Server	35
Figure 3. 5 Process Approach Waterfall	43
Figure 3. 6 Hashing process id news with SHA-256 algorithm.....	48
Figure 3. 7 Interface design news pages	50
Figure 4. 1 Main Display Image Web.....	51
Figure 4. 2 When the Web Image Data Not Found.....	52
Figure 4. 3 Code Page News	53
Figure 4. 4 Connection With Salt.....	54
Figure 4. 5 Code To Get User Log.....	55
Figure 4. 6 Character Regular Expression	55
Figure 4. 7 Testing SQL Injection Union Select.....	57
Figure 4. 8 Error When Url inserted Quote Marks	57
Figure 4. 9 Preliminary Results From Union Select Query	59

Figure 4. 10 Results Union Select..... 59
Figure 4. 11 Preview of Final Results From Union Select 60
Figure 4. 12 Value Log Attacker..... 60



ABSTRACT

With the rapid advancement of information technology development, especially in the aspects of web security. A web, of course, has data that should be safeguarded by web security. But the development of technology is also growing techniques aimed at entry or hacking a website, one of which is SQL Injection Union Select. This will be a big problem if the problem can not be resolved.

This study will make a web security system, particularly in the Get parameter using the SHA-256 in order to prevent their access to the database by a hacker. SHA-256 algorithm is a cryptographic algorithm that has great capability in security aspects.

The end result of the SHA-256 algorithm implementation on web security generates the security parameter of the Get preventing attacks people who do not have the authority.

Keywords: SHA-256, Web Security, SQL Injection, Union Select, and Cryptography