

TABLE OF CONTENTS

COVER	i
UNDERGRADUATE THESIS	ii
APPROVAL PAGE	iii
STATEMENT	iv
DEDICATION PAGE.....	v
PREFACE	vi
TABLE OF CONTENTS.....	viii
LIST OF FIGURES	xii
LIST OF TABLES	xiii
LIST OF APPENDIXES.....	xiv
ABSTRACT.....	xv
CHAPTER I.....	1
1.1. Background Problem	1
1.2. Research Problem	2
1.3. Research Constraints.....	2
1.4. Research Objective	3
1.5. Research Benefits.....	3
1.6. Research Method	3
1.7. Thesis Organization.	4
CHAPTER II.....	6
CHAPTER III	9
3.1. Web Application	9
3.2. Security Audit Standard	10
3.2.1. OWASP Application Security Verification Standard 3.0	10
3.3. Ethical Hacking.....	12
3.3.1. Types of Attack.....	12
3.3.2. Scope and Limitation	13
3.3.3. Web Application Attack	13
3.4. Google Hacking	19
3.5. Tools	20

3.5.1.	Zed Proxy Attack	20
3.5.2.	FoundstoneSitedigger 3.0	21
3.5.3.	Wappalyzer	22
CHAPTER IV		23
4.1.	Pre-Assumption	23
4.2.	Methodology	23
4.2.1.	Data Collection	27
4.2.2.	Search Engine Discovery	28
4.2.3.	Vulnerability Scanning	29
4.2.4.	Data Analysis	30
4.2.5.	Designing Technical Solution and Requirement.....	31
4.2.6.	Design Implementation	31
4.2.7.	Design Testing	32
CHAPTER V		33
5.1.	Data Collection	33
5.2.	Search Engine Discovery	35
5.3.	Vulnerability Scanning	43
5.4.	Design of the Solution	56
5.5.	Design Implementation	62
5.5.1.	Specification of Website	63
5.5.2.	Setting Content Security Header	63
5.5.3.	Setting X-Frame-Option Header	64
5.5.4.	Setting X-Content-TypeOption Header	65
5.5.5.	Enable Web Browser XSS Protection.....	65
5.5.6.	Hide Server's version information via "Server"HTTP Response	66
5.5.7.	Hide Server's Information via "X-Powered-By" HTTP Response.....	67
5.5.8.	Setting Cache-control in HTTP Response Header	67
5.6.	Testing	69
5.6.1.	Header Confirmation	69
5.6.2.	Vulnerability Scanning	69
CHAPTER VI		71
6.1.	Experiment Results and Discussion	71

6.1.1.	Security Header Report.....	71
6.1.2.	HTTP Response Message	72
6.1.3.	Vulnerabilities and URLs	73
CHAPTER VII.....		81
7.1.	Conclusion	81
7.2.	Future Works	82
BIBLIOGRAPHY		83