

Analysis of Selection of PHP Frameworks that Meet OWASP Criteria Using the AHP Method

John Swatrahadi Permana¹, Hendrana Tjahjadi², Rinaldi Munir³, Gunawan Wibisono⁴, Hetly Brinner Yussak Kawet⁵

¹Cyber Defense Engineering
Republic of Indonesia Defense University
Jakarta, Indonesia
john.permana@idu.ac.id

²Faculty of Science and Defense Technology
Republic of Indonesia Defense University
Jakarta, Indonesia
hendrana@idu.ac.id

³School of Electrical Engineering and Informatics
Bandung Institute of Technology
Bandung, Indonesia
rinaldi@staff.stei.itb.ac.id

⁴Faculty of Science and Defense Technology
Republic of Indonesia Defense University
Jakarta, Indonesia
weebegoen@gmail.com

⁵Faculty of Science and Defense Technology
Republic of Indonesia Defense University
Jakarta, Indonesia
hetlykawet@gmail.com



Abstract— The rapid advancement of information technology has opportunities and threats that compete with each other to be the winner. The government takes advantage of advances in information technology to improve people's welfare and build partnerships with the private sector through the implementation of e-government, as mandated in Presidential Instruction no. 3 of 2003 concerning National Policy and Strategy for E-Government Development. Through this Presidential Instruction, government organizations must be more open to forming partnerships with the business world (public-private partnership). In this strategy the government implements several G2G, G2B, C2C strategies. The government is developing a strategy by opening public services online, a network of supporting organizations (back-office), electronic documents, basic applications such as e-literacy, e-billing, e-procurement, e-reporting and also giving the role of the private sector. in the business world where most of these applications currently use web-based applications, although some have switched to a mobile basis. Where there are opportunities there, you also don't want to be left behind, the threat of crime is also getting heavier with various motives and sharing techniques to threaten to take advantage of these opportunities to gain profit. Cyber loggers are not standing still in taking advantage of what the Government is currently operating in the form of a web application that operates in cyber space. Cybercriminals also want to take advantage of this opportunity for personal gain or damage the government's reputation. Criminals try to get data of economic value to sell to other parties on the dark web. Criminals also seek to

undermine the government's authority by damaging its reputation through hacking activities on portals operated by government organizations. The government cannot remain silent, belittling the activities of these cybercriminals. One of the strategies that the government can implement in maintaining security in cyberspace is to build secure web applications known as secure programming or secure coding. Implementation of secure programming in web application development can be analyzed using the Analytical Hierarchy Process.

Keywords— WEB Based Application, Secure Programming, Secure Coding, AHP.

I. INTRODUCTION

The government really wants the administration to take advantage of advances in information technology by implementing e-government. On the other hand, digital criminals target the weaknesses in e- government to obtain personal gain through unauthorized activities such as hacking portals, selling valuable information on the dark web and other activities. The government goes the extra mile to implement e-government that is guaranteed to be safe from crime in cyberspace. One way that needs to be done is to build an application system in the form of a web that is used in e-government with a secure-programming development method or there is also something called secure coding.

The government in developing web-based applications can implement secure programming or secure coding according to one of the reference standards for web- based software development. The implementation of web application development standards such as OWASP can mitigate the risk of cyber threats that can occur at any time by government organizations. Some of the components in the standard include 1. Input validation, 2. Encoding output 3. Authentication and password management, 4. Access control, 5. Cryptographics practices, 6. Error handling and logging. 7. Data protection, 8. Communication security, 9. System configuration, 10. Database security, 11. File management, 12. Memory management, 13 general coding prantices. The problem faced by application developers is the many and complex applications of secure web programming that must be met in addition to meeting the main functionality needs of web applications with a short schedule. The problem can be solved with several mathematical approaches. Mathematical method approaches that can be used to solve these problems include analytical hierarchy process, analytical network process and game theory. In this research, an analysis of these three methods can be carried out in the problem solving strategy for developing web- based applications that apply security standards. With the analysis of this research, it is hoped that the government can find out the technical problems in the implementation of secure programming by providing technical solutions that are part of the strategy in anticipating the threat of cybercrime.

In order to support the decision-making process, Prof. Thomas L. Saaty, a professor of mathematics from the University of Pittsburg, developed a decision support method called the Analytical hierarchy process (AHP). According to Saaty (1990), complexity in decision making because the criteria are many. AHP is a method of solving a complex unstructured situation into several components in a hierarchical arrangement, by giving a subjective value of the relative importance of each variable and establishing which variable has the highest priority to influence the outcome of the situation. The AHP method model can be described as a hierarchical structure consisting of components of objectives, criteria, sub-criteria and alternative solutions or decisions that can be taken, as in the following figure:

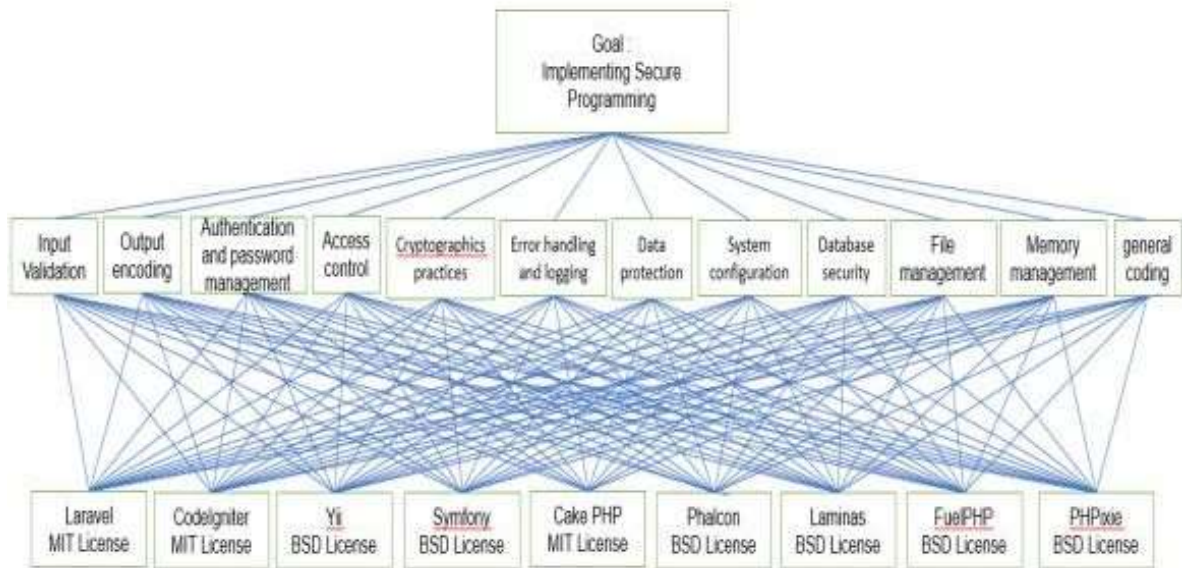


Fig. 1. Goal Implementing Secure Programming

The goal to be achieved using this AHP method is to select a php programming framework that applies secure programming. PHP frameworks include: 1. Laravel, 2. Codeigniter, 3. Yii, 4. Symfony, 5.CakePHP, 6. Phalcon, 7. Laminas, 8. FuelPHP, 9. PHPixie. 10. Zend Among these frameworks which one comes closest to meeting the criteria of OWASP secure programming.

II. RESEARCH METHODS

In this study, the method that will be used to solve the problem of choosing a php framework with OWASP standard criteria uses the process hierarchy analysis method. In addition to determining the selection of framework php use the method also to analyze how the use of the right method compares in determining the choice that is closest to standard secure programming.

This research method uses a quantitative research process. This research process goes through a series of sequential processes from beginning to end. This research process goes through the following processes: 1. Finding, identifying, limiting and formulating problems, 2. Compiling theoretical foundations / studies, 3. Formulating hypotheses, 4. Establishing samples and populations including the development of research instruments, 5. Collection data, 6. Data analysis and discussion and conclusions and suggestions. Results and Discussion Some steps or procedures that must be done in the application of the AHP method, namely by selecting a structure chart to facilitate illustration, have been done previously in the introduction, then is to make a pairways comparison matrix.

	1	2	3	4	5	6	7	8	9	10	11	12	13
1	1	5.00	0.14	0.20	7.00	7.00	1.00	0.50	5.00	0.50	7.00	7.00	0.50
2	0.20	1	0.20	0.14	0.50	1.00	0.14	0.20	0.50	0.14	0.50	0.50	0.14
3	7.00	5.00	1	2.00	5.00	7.00	5.00	1.00	7.00	5.00	5.00	9.00	1.00
4	5.00	7.00	0.50	1	5.00	7.00	7.00	3.00	5.00	3.00	5.00	9.00	0.50
5	0.14	2.00	0.20	0.20	1	1.00	1.00	0.14	1.00	0.14	1.00	1.00	0.14
6	0.14	1.00	0.14	0.14	1.00	1	0.50	0.14	3.00	0.14	3.00	3.00	0.14
7	1.00	7.00	0.20	0.14	1.00	2.00	1	0.33	5.00	0.50	5.00	5.00	0.14
8	2.00	5.00	1.00	0.33	7.00	7.00	3.00	1	5.00	2.00	3.00	7.00	1.00
9	0.20	2.00	0.14	0.20	1.00	0.33	0.20	0.20	1	0.14	3.00	3.00	0.14
10	2.00	7.00	0.20	0.33	7.00	7.00	2.00	0.50	7.00	1	7.00	7.00	0.50
11	0.14	2.00	0.20	0.20	1.00	0.33	0.20	0.33	0.33	0.14	1	3.00	0.14
12	0.14	2.00	0.11	0.11	1.00	0.33	0.20	0.14	0.33	0.14	0.33	1	0.14
13	2.00	7.00	1.00	2.00	7.00	7.00	7.00	1.00	7.00	2.00	7.00	7.00	1

Fig. 2. Result

With C1 : Input validation, C2: Output encoding, C3: Authentication and password management, C4 : Access control, C5 : Cryptographics practices, C6: Error handling and logging, C7 : Data protection, C8: Communication security, C9: System configuration, C10: Database security, C11: File management, C12: Memory management, C13: General coding obtained pairways comparison matrix as follows :

Table 1. OWASP standard

Cat		Priority	Rank	(+)	(-)
1	Input validation	7.9%	6	4.3%	4.3%
2	Output encoding	1.6%	12	0.8%	0.8%
3	Authentication and password management	19.6%	1	13.3%	13.3%
4	Access control	17.1%	2	10.3%	10.3%
5	Cryptographics practices	2.2%	10	1.0%	1.0%
6	Error handling and logging	2.6%	8	1.6%	1.6%
7	Data protection	5.3%	7	2.9%	2.9%
8	Communication security	11.8%	4	4.3%	4.3%
9	System configuration	2.3%	9	1.3%	1.3%
10	Database security	9.9%	5	4.0%	4.0%
11	File management	2.1%	11	1.1%	1.1%
12	Memory management	1.4%	13	0.6%	0.6%
13	General coding	16.3%	3	7.3%	7.3%

Based on the ranking of the highest categories, the 3rd, 4th and 13th categories were selected. The criteria are authentication and password management, access control and general coding to facilitate the calculation of the three highest categories will be calculated compare way Furthermore, create a pairwise comparison matrix and priority weights (eigen vector) between alternatives in relation to the criteria and measure the consistency of the logi. There should be 3 x 9 components and alternatives that need to be taken into account. However, this research will be limited to only 4 frameworks, namely 1. Laravel, 2.Codeigniter, 3. Symphony and 4. Zend.

The calculation of authentication and password management criteria in 4 php alternative frameworks is as follows:

	1	2	3	4
1	1,00	5,00	5,00	2,00
2	0,20	1,00	4,00	2,00
3	0,20	0,25	1,00	2,00
4	0,50	0,50	0,50	1,00

The table multiplied by the same table yields

	1	2	3	4	jml	Bbt Pr
1	4	12,25	31	24	71,25	0,56
2	2,2	4	10	12,4	28,6	0,23
3	1,45	2,5	4	4,9	12,85	0,10
4	1,2	3,63	5,5	4	14,33	0,11
jml	8,85	22,38	50,5	45,3	127,03	

Showing the most priority alternative options is the 1st alternative that is right to choose based on authentication and password management criteria. The calculation of access control criteria in 4 alternativeframework options is shown by a matrix as below:

	1	2	3	4
1	1,00	3,00	3,00	4,00
2	0,33	1,00	4,00	2,00
3	0,20	0,25	1,00	2,00
4	0,25	0,50	0,50	1,00

The table multiplied by the same table will produce priority weights as in the table below :

	1	2	3	4	Jml	Pri
1	3,60	8,75	20,00	20,00	52,35	0,50
2	1,97	4,00	10,00	13,33	29,30	0,28
3	0,98	2,10	3,60	5,30	11,98	0,12
4	0,77	1,88	3,75	4,00	10,39	0,10
J	7,32	16,73	37,35	42,63	104,03	

From the table shows but the 1st alternatic i.e. Laravel which is the top of the order. Finally, the general coding comparison calculation is shown bythe matrix calculation as below:

	1	2	3	4
1	1,00	5,00	7,00	5,00
2	0,20	1,00	4,00	2,00
3	0,20	0,25	1,00	2,00
4	0,20	0,50	0,50	1,00

The table multiplied by the same table will produce priority weights as in the table below :

	1	2	3	4	Jml	B.
1	5,32	12,25	32,5	33	83,07	0,63
2	1,83	3,6	9,6	12,8	27,83	0,21
3	0,98	2,1	3,6	5,3	11,98	0,09
4	0,72	1,73	3,6	3,8	9,84	0,07
J	8,85	19,68	49,3	54,9	132,73	

The table also shows the 1st alternatic, namely Laravel which is the top order for general coding criteria. An important aspect in the application of the AHP method is the calculation of the consistency of the assessment. The Consistency Ratio CR measurement of the three criteria produces the 1st criterion value= 0,059749, 2nd criterion = 0,052388 and 3rd criterion = 0,099871. Of the three criteria, it shows that the filling of the matrix assessment is valid or consistent and can be accepted as a decision- making analysis.

Global priority is obtained by multiplying the priority weight of each criterion with the priority weight of each alternative. Calculation of global priority can be demonstrated by the following calculations :

	A	B	C
1	0,44405	0,50	0,63
2	0,292007	0,28	0,21
3	0,164121	0,12	0,09
4	0,099822	0,10	0,07

Multiplied by the highest priority criterion 3 normalization, namely:

0,369811
0,476323
0,454039

The global priority table is obtained as follows

Pilihan 1	Laravel	0,688084355
Pilihan 2	Codeigniter	0,337365221
Pilihan 3	Symphony	0,156558348
Pilihan 4	Zend	0,092904323

From the table it can be described the structure of the AHP method in outline is as follows :

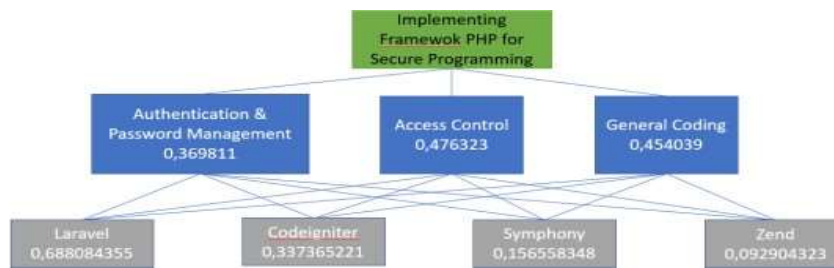


Fig. 3. Implementing Framework PHP for Secure Programming

III. CONCLUSION

Laravel is the framework php that best meets the criteria of OWASP standards based on selection using hierarchy process analysis. The AHP method in addition to being able to be used to select one alternative framework php that is best in meeting OWASP standards can also provide a ranking order of several alternatives that are taken into account. The AHP method can be used for decision making analysis that contains many criteria such as the OWASP standard which can involve 13 criteria. The limitation of this study is not that all criteria are taken into account through only the 3 most important criteria that are continued to be calculated. Including alternative solution options are not entirely calculated but only popular ones, namely Laravel, CI, Symfony and Zend.

REFERENCES

- [1] Dr. Drs. Marsono, M.Si (2019). Quantitative research methods. Bogor : In Media
- [2] Dr. Drs. Marsono, M.Si. (2020). The use of the Analytical Hierarchy Process method. Bogor : In Media
- [3] The OWASP Foundation, (2010), OWASP Secure Coding Practices Quick Reference Guide
- [4] Presidential Instruction number 3 of 2003 concerning national policies and strategies for e-government development
- [5] Presidential Regulation number 82 of 2022 protection of vital information infrastructure
- [6] Law number 11 of 2008 concerning information and electronic transactions
- [7] Government regulation number 82 of 2012 concerning the implementation of electronic systems and transactions
- [8] Solica, Verra (2016) microsoft excel on analytical hierarchy process method for choosing delivery services. Information Management for educators and professionals Vol.1, No. 1, December 2016