COMPARISON ANALYSIS OF THE WEB SECURITY PTES, ISSAF AND OWASP IN DISKOMINFO, BANDUNG CITY

Tio Revolino Syarif [1,] Didit Andri Jatmiko [2]

[1,2] Universitas Komputer Indonesia

Jl. Dipatiukur No. 112-116, Bandung 40132

E-mail : tio.revolino.syarif@email.unikom.ac.id [1], didit@email.unikom.ac.id [2]

ABSTRACT

Currently the development of technology in the field of information has spread to remote parts of the country, both in villages, sub-districts, regencies and cities have begun to have divisions that implement a system of information dissemination to the public by using the website and one of the parties responsible for the dissemination service information in the city of Bandung is Diskominfo. However, with the use of the website as a public information service media by the government, it would be very possible if the website could be attacked by irresponsible people who could cause loss and disruption of government information services to the public. One effort to prevent this is Penetration Testing. Penetration Testing, or can also be called Pen Testing, is an attempt to find vulnerabilities in computer systems, computer networks, or web applications, which can be exploited by attackers. In this study, we will compare three Penetration Testing Frameworks, namely PTES, ISSAF, and OWASP. The results of this study are expected to help the DISKOMINFO in Bandung to manage the website and provide an understanding of the differences to the three Frameworks.

Keywords: PTES, OWASP, ISSAF, Penetration Testing, website vulnerability, Reporting

1. INTRODUCTION

Dinas Komunikasi dan Informatika Bandung city is an agency responsible for processing information in the city of Bandung. Website is also a very important requirement in government agencies, especially the Office of Communication and Information, Bandung. Benefits of the Website include, as a medium for delivering information, as a medium of interaction, as a measure of whether or not active government activities, as a place for people to express their aspirations, and as a place for promotion.

But, behind the many benefits, there are also threats that can occur. Based on data obtained from the Directorate of Cyber Crime Indonesia, in 2015-2016 in Indonesia there were 2880 cases of Cyber Crime [1]. In May 2017, there was a cyber attack of Ransomware Wannacry which caused disruption to companies and hospitals in more than 150 countries [2]. The attack opened the eyes of the world and became the first step to cooperate in cyber security.

Computer Security Systems can be said to be a method that is made to secure the functions, data, performance, or processes that exist on a computer system. An experiment must be carried out to find out whether a website is safe or not from dangerous actions carried out by the attacker [3]. One way to find out whether our system is safe or not is to do Penetration Testing.

Penetration Testing can be said to be a legal and official way to find and exploit computer systems that aim to make the system safer [4]. But in some cases, vulnerabilities obtained from Penetration Testing are actually used by irresponsible parties. Therefore it is very important to ask permission to the party who wants Penetration Testing [5].

Penetration Testing Execution Standard (PTES) has recently emerged as one of the Frameworks for Penetration Testing. Although this Framework is still in the development stage, it provides a highly structured method to motivate the community that aims to identify what the Security Assessment is

The Information Systems Security Assessment Framework (ISSAF) is a structured framework of the Open Information System Security Grop that classifies the assessment of system security information into several domains and assesses specific details or testing criteria for each domain [6].

The Open Web Application Security Project (OWASP) is a free and open community throughout the world focused on improving the security of application software. OWASP's mission is to make security applications "visible", so that people and organizations can make decisions about application security risks. The results of this OWASP test will be mapped using the Risk Rating rating parameter. Risk Rating is a valuation parameter used to measure the level of a risk. In this methodology, risk is the result of likelihood with impact. The results of these tests will be used as a parameter to assess how high the level of security of a web.

Based on the problems that occur, this research is carried out which is expected to be able to help the DISKOMINFO of Bandung City, in maintaining the security of the website, and determine what framework is right to use.

2. THEORY BASIS

At this stage a discussion of the theories used in the study will be conducted.

2.1. PTES (Penetration Testing Execution Standard)

Penetration Testing Execution Standard (PTES) is a new standard designed by businesses and security service providers using a common language with a range of penetration testing. PTES began in early 2009 and began with a meeting between founding members while talking about the current interests or weaknesses in penetration testing [7]. The PTES phase was designed to explain a Penetration Testing and ensure that a business level of standardization will be extended to Penetration Testing. by everyone who does this type of assestment [8]. 7 steps in doing penetration testing execution:

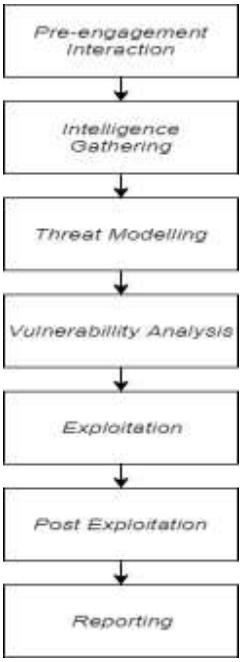

Figure 1 STEPS PTES

2.2. ISSAF (Information System Security Assesment Framework)

ISSAF is a structured framework that categorizes information system security assessments into various domains and details of specific evaluations or testing criteria for each domain [9]. This aims to provide input on security assessments based on the actual scenario. Adequacy of using ISSAF to fulfill security assessment requirements in an organization and can be used as a reference to fulfill other information security. ISSAF includes important aspects of security processing, assessment, and helps to get a complete picture of possible vulnerabilities. Following are the steps in the ISSAF (Information System Security Assessment Framework):

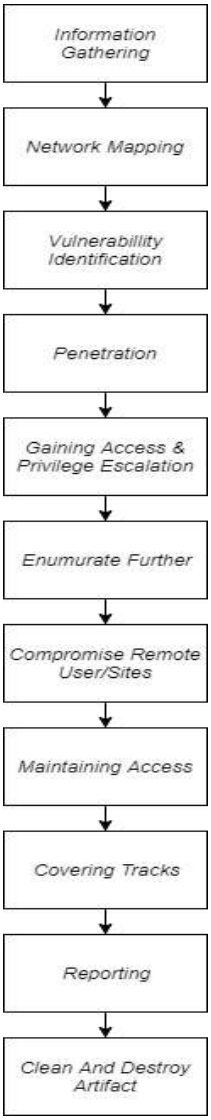

Figure 2 STEPS ISSAF

2.3. OWASP (Open Web Application Security Project)

The Open Web Application Security Project (OWASP) is a free and open community dedicated to enabling organizations to develop, buy and maintain trustworthy applications, all tools, documents, forums used by OWASP are free and open to anyone interested to improve application security [10]. The following are the stages of the Open Web Application Security Project (OWASP) framework:

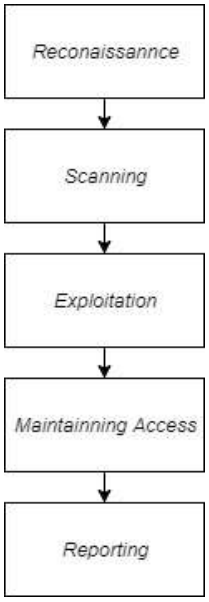

Figure 3 STEPS OWASP

3. RESEARCH METHOD

The research methodology used is qualitative research methods, namely research on research that is descriptive and tends to use analysis. The following is the flow of research conducted in this study:

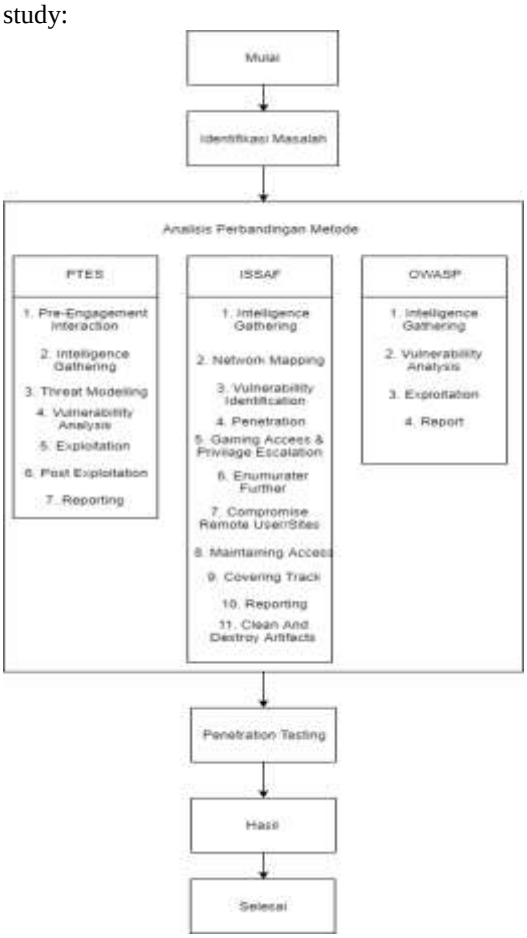

Figure 4 Research Flow

1. Problem Identification

At this stage, the researchers worked with DISKOMINFO to identify the problems found on the Bandung DISKOMINFO website.

2. Comparison Analysis Method

The researcher made a comparison between the three methods used.

3. Penetration Testing

In this stage the researcher will test the vulnerability on the specified website. Examination of vulnerabilities is done using tools that will be adjusted.

4. Result

In this stage, the tester gets the results from a comparison of the three methods and gets the results from Penetration Testing

4. RESULT AND DISCUSSION

- **PTES (Penetration Testing Execution Standard)**

1. Pre-Engagement Interaction

In the Pre-Engagement Interaction phase, discussions will be held with parties from Diskominfo, Bandung. This discussion was conducted to determine the process to be carried out in this study. The agreement that was successfully produced at this stage is as follows:

1. Identify Research Contacts
2. Confirm the scope of the research, approach and explanation of the method to be used in testing vulnerabilities at diskominfo.bandung.go.id
3. Request data in the form of domains managed by Diskominfo, Bandung

2. Intelligence Gathering

At this stage, information about the domain diskominfo.bandung.go.id will be searched, here are the results of the search using Whois Domain and Zenmap:

Figure 5 Whois diskominfo.bandung.go.id

The following is the results table for the whois domain diskominfo.bandung.go.id

Table 1 Whois Diskominfo.bandung.go.id

Diskominfo.bandung.go.id	
Domain ID	PANDI-DO282184
Domain Name	BANDUNG.GO.ID
Created On	10-May-2000
Expiration Date	31-Jan-2020
Status	OK

Furthermore, information will be sought about Network Mapping by using Zenmap for the diskominfo.bandung.go.id domain. Here are the results of Zenmap for the diskominfo.bandung.go.id domain:

Table 2 Zenmap diskominfo.bandung.go.id

diskominfo.bandung.go.id		
Port	***Status***	***Services***
80	Open	http
443	Open	https

3. Vulnerabillity Analysis

The following are the results of Vulnerability Analysis using the Accunetix scanning vulnerability tools, namely Application Error Message (CWE-209), Error Message On Page (CWE-200), Vulnerable Javascript Library (CWE-16).

4. Exploitation

Exploitation is one of the stages in the Framework Penetration Execution Standard (PTES) where at this stage the examiner will penetrate the tested website to see whether the domain diskominfo.bandung.go.id has a security gap. The following is the result of exploitation using SQLmap*:*

Figure 6 Sqlmap diskominfo.bandung.go.id

Based on Figure 6, the diskominfo.bandung.go.id domain does not have a SQL Injection slot.

5. Reporting

At this stage the researcher will also give a Risk Rating to the domain diskominfo.bandung.go.id. This level of Risk Rating refers to the Risk Rating provided by the Penetration Testing Execution Standard (PTES) framework. The following is an illustration of the Risk Rating.

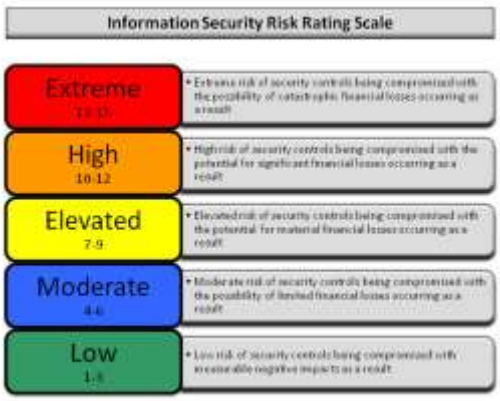

Figure 7 Risk Rating Scale

Based on the research that has been done, the Risk Score for the website diskominfo.bandung.go.id for now is 6, this refers to the possibility that there are weaknesses in security controls that can cause limited financial losses.

- **ISSAF (Information System Security Assesment Framework)**

1. Information Gathering

At this stage information will be searched for the website to be examined, here are the results of the search using Whois Domain*:*

Figure 8 Whois diskominfo.bandung.go.id

The following is the results table for the whois domain diskominfo.bandung.go.id

Table 3 Whois diskominfo.bandung.go.id

Diskominfo.bandung.go.id	
Domain ID	PANDI-DO282184
Domain Name	BANDUNG.GO.ID
Created On	10-May-2000
Expiration Date	31-Jan-2020
Status	OK

2. Network Mapping

Network mapping will be done with the help of the Zenmap tool, the following are the results of the Port-Port search using Zenmap:

Table 4 Zenmap diskominfo.bandung.go.id

diskominfo.bandung.go.id		
Port	***Status***	***Services***
80	Open	http
443	Open	https

3. Vulnerability Identification

After the Information Gathering stage, the next stage is Vulnerability Identification, at this stage scanning of the website will be done to see whether the website has a vulnerability or not, and how severe the website has vulnerabilities. If there is a vulnerability, the examiner will use the vulnerability to carry out the next testing step. The following are the results of Vulnerability Analysis using the Accunetix scanning vulnerability tools, namely Application Error Message (CWE-209), Error Message on Page (CWE-200), and Vulnerable Javascript Library (CWE-16).

4. Penetration

Penetration is one of the stages in the Information System Security Assessment Framework (ISSAF) where at this stage the examiner will penetrate the tested website. In this stage the examiner will test whether this website has a vulnerability to SQL Injection by using a tool called SQLmap. Here is a screenshot of the results of testing using SQLmap*:*

Figure 9 SQLmap diskominfo.bandung.go.id

Based on Figure 9, it can be seen that the diskominfo.bandung.go.id website does not have a SQL Injection vulnerability.

5. Reporting

- **Management Summary**

Based on the research that has been carried out from the initial stage to the final stage, there are several vulnerabilities found in the diskominfo.bandung.go.id domain. This vulnerability is Application Error Message, Error Message on Page, Vulnerable Javascript Library (CWE-16).

- **Scope of The Project**

Scope of the project is a report on the scope that researchers took. This scope itself has actually been taken by the researcher based on the agreement of the researcher and the party being tested. The scope taken by researchers is a web application.

- **Vulnerabillity Scan Report**

Vulnerability scan reports are the report stage based on the analysis process in the second phase of the ISSAF method plus the implementation that has been done. The following is a table report:

Table 5 Vulnerabillity Scan Report

No	**Common Weakness Enumeration**	***CWE -209***	***CWE -444***	***CWE -260***
	Domain			
1	Diskominfo.bandung.go.id	✓	✓	✓

- **OWASP (Open Web Application Security Project)**

1. Reconaissance

At this stage a search for information about the website to be investigated will be carried out, here are the results of the search using Whois Domain and Zenmap*:*

Figure 10 Whois diskominfo.bandung.go.id

The following is the results table for the whois domain diskominfo.bandung.go.id

Table 6 Whois diskominfo.bandung.go.id

Diskominfo.bandung.go.id	
Domain ID	PANDI-DO282184
Domain Name	BANDUNG.GO.ID
Created On	10-May-2000
Expiration Date	31-Jan-2020
Status	OK

Next will be an information search about Network Mapping. Here are the results of Zenmap for the diskominfo.bandung.go.id domain:

Table 7 Zenmap diskominfo.bandung.go.id

diskominfo.bandung.go.id		
Port	***Status***	***Services***
80	Open	http
443	Open	https

2. Scanning

The next stage is Scanning, at this stage scanning of the website will be seen to see whether the website has a vulnerability or not, and how severe the vulnerability that the website has, Here are the results of scanning using Accunetix vulnerability scanning tools, namely Application Error Message (CWE-209), Error Message On Page (CWE-200), Vulnerable Javascript Library (CWE-16). Application Error Message (CWE-209).

3. Exploitation

Exploitation is one of the stages in the Open Web Application Security Project (OWASP) where at this stage the examiners will penetrate the tested website. Here is a screenshot of the results of testing using SQLmap*:*

Figure 11 SQLmap diskominfo.bandung.go.id

Based on Figure 11, it can be seen that the diskominfo.bandung.go.id website does not have a SQL Injection vulnerability.

4. Reporting

In the Reporting phase, OWASP (Open Web Application Security Project) has a method namely OWASP Risk Rating Methodolgy. OWASP Risk Rating Methodology is a method used to determine the risk classification on the website.

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Figure 12 Likelihood dan Impact Level

After calculation, the diskominfo.bandung.go.id domain has a Likelihood score of 5, so it has a Medium rating. While the Impact score is 4, and also has a Medium rating. After that, determine the risk classification based on the formula from the OWASP Risk Rating Methodology and adjust it to figure 13

Figure 13 Overall Risk Severity

Based on Figure 13, it can be seen that the Diskominfo.bandung.go.id subdomain has a Medium risk level.

5. CONCLUSION

Based on the results of this study, according to the authors that the appropriate Framework for use in DISKOMINFO in Bandung is the Framework for Penetration Testing Execution Standard (PTES) and the Open Web Application Security Project (OWASP), because the assessment of this framework uses levels that can be understood by users who are not only people who are experienced with Penetration Testing, but can also be understood by users who also do not have experience in the field of Penetration Testing. While the framework of the Information System Security Assessment Framework (ISSAF) can only be understood by users who are experienced in the field of Penetration Testing, because reporting on this framework does not have levels as in the other two frameworks. The advice that the researcher can give is:

- Provide a report format on vulnerabilities based on the three Frameworks, Penetration Testing Execution Standard (PTES), Information System Security Assessment Framework (ISSAF), and the Open Web Applicatin Security Project (OWASP) that can be used for future research.
- Maintaining a Website by using references from the results of reports that have been carried out and hoping to prevent future vulnerabilities.

6. BIBLIOGRAPHY

[1] H. Djanggih, The Effectiveness of Law Enforcement on Child Protection for Cybercrime Victims in Indonesia, *IOP Conf. Series: Journal of Physics: Conf. Series 1028 (2018) 021292, 2018*

[2] M. J. Islami, TANTANGAN DALAM IMPLEMENTASI STRATEGI KEAMANAN SIBER NASIONAL INDONESIA DITINJAU DARI PENILAIAN GLOBAS CYBERSECURITY INDEX, Puslitbang Aptika dan IKP, Badan Litbang SDM, Kemenkominfo,2017

[3] E.B.Setiawan, A Setiyadi, Web Vulnerabillity Analysis and Implementation, *IOP Conf. Series: Materials Science and Engineering 407 (2018) 012081, 2018*

[4] Patrick Engebretson, The Basic of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy, Elsevier, 2010

[5] Vibhurushi Chotaliya, Fiyona Mistry, New Era of Web Security By Implementing of Penetration Testing, International Journal of Trend in Scientific Research and Development, 2018

[6] Shorunke Muyiwa Musaddiq. Penetration Testing in WI-FI network. *International Journal of Computer Science Engineering,Vol 4 issues 4*, pp.115

[7] The Penetration Execution Standard, *Penetration Execution Standard-The FAQ, http://www.pentest-standard.org/index.php/FAQ*, 26 Februari 2018 19.45

[8] D. Kennedy, J. O'Gorman, D. Kearns, M. Aharoni, "METASPLOIT The Penetration Tester's Guide", No Starch Press, pp. 2, 2011

[9] Jajang Ruhiyat, Angga Setiyadi, Sistem Monitoring Website Dengan Metode ISSAF Di Dinas Komunikasi dan Informatika Kabupaten Tangerang, Unikom, 2018

[10] OWASP, "OWASP Top 10 – 2013 : The ten most Critical Web Application Security Risk", OWASP, pp.2