The Fifth Information Systems International Conference 2019

Web Vulnerability Assessment and Maturity Model Analysis on Indonesia Higher Education

IGN Mantra[a,]*, Muhammad Syarif Hartawan[b], Hoga Saragih[c], Aedah Abd Rahman[d]

[a]Perbanas Institute, Jakarta, Indonesia
[b]University Of Krisnadwipayana, Jakarta, Indonesia
[c]Bakrie University, Jakarta, Indonesia
[d]Asia e University, Kuala Lumpur, Malaysia

Abstract

College websites are websites that are used as media and means of campus information. Since the website is widely accessible, the level of security on the website must always be maintained. To see the level of web security, it can be done by testing the security vulnerability of the web. The test results using the tools Nessus and Skipfish, on the websites of several universities in Jakarta, show that there are still several vulnerabilities. This vulnerability will affect the maturity level of the web site security. The results of vulnerability testing show that as many as 60% of the total 33 web sites have a maturity level below number 3. This indicates that the level of vulnerability on the web site is still high.

Keywords: Website; Vulneraiblity Assesment; Maturity Level

1. Introduction

The website is basically a collection of documents that contain data and information that can be accessed via the internet. The website is now the main source of information and is used for many activities, one of which is activities for academic purposes in universities. At present there are frequent attacks on web sites, including the college web

* Corresponding author. Tel.: +62-81-580-095-75.
E-mail address: ign.mantra@perbanas.id

site. Attacks on web sites are intended to steal data / information, change data, or also intended to deactivate services provided by the websites. Web-based applications allow users to share and manipulate information by using various platforms [1]. The confidentiality, integrity and availability of services of a website can depend on the security of web applications [2]. The Web Application Security Consortium (WASC) defines web applications as software applications run by web servers that respond to dynamic requests via HTTP [3]. They consist of scripts that are on a web server and interact with databases or other dynamic content sources [1]. Typical deployments consist of browser clients, web servers, application servers, and database servers [1]. As web application complexity and connectivity increases, the challenge of securing it grows exponentially [1]. One way to maintain website security is to do vulnerability testing regularly. The purpose of the vulnerability test is to assess the level of maturity (security) that is owned by a web site. The security properties of a web application are similar to other software system security, which includes data confidentiality, data integrity, and application availability. A vulnerability is a weakness in the application, which can be a design error implementation, which can harm the stakeholders of the application. Stakeholders include the application owner, application users, and other entities that rely on the application. The term "vulnerability" is often used very loosely. However, here we need to distinguish threats, attacks, and countermeasures. Testing for vulnerability, whether manual or automatic, is considered a key component of every effort to improve security. This assessment allows organizations to know the status of information security and their infrastructure, and is designed to identify whether an activity that threatens security will occur in the form of a hack attack that will disrupt infrastructure security measures and will exploit any vulnerable assets of the organization. Violations of security parameters result in compromises in the confidentiality, availability and integrity of information that is sacred to business activities [4].

Vulnerability assessment is a process that defines, identifies, classifies security gaps (vulnerabilities) on computers, networks, or communication infrastructure. In addition, vulnerability analysis can estimate the effectiveness of the proposed preventive actions and evaluate their actual effectiveness after they are implemented. The results of a vulnerability assessment activity can be used to determine the maturity level of the security of the web site. This maturity level can be used to measure the extent to which the implementation of security controls has been applied to the web site, so that it can take corrective actions to deal with threats that can be caused by security vulnerabilities on the web site. Analysis of several maturity models shows that many models differ based on their characteristics. But at the same time there are also a number of similarities in these models, which have been found which can partly be explained by the fact that many originators of maturity models only create models based on their predecessor models without much thinking about the suitability of the designs they spark. This shows that the maturity modeling concept must be reviewed and reassessed. In general, maturity models are a tool to assess the effectiveness of an organization in achieving certain goals. The model allows organizations to identify security practices that are weak or not taken seriously and which security practices are truly embedded in business activities. In the context of cyber security, maturity models can help organizations distinguish where security is made, within an organization or only entrusted to other parties. One of the main reasons that the maturity model is used is that improvements throughout the organization can take time; in cyberspace security the maturity model gives organizational leaders a way to measure the progress made in instilling securing into strategic operations and daily operations. The maturity model is based on the premise that people, organizations, functional areas, processes, etc., evolve through a process of development or growth towards more advanced maturity, through a number of different levels. The level in the model is the basis from which evolution to a higher level of maturity can be planned and implemented [5]. The purpose of the maturity model is to measure the activities carried out, make them measurable and develop in other words to make them mature over time, namely [6]. Besides making their own maturity models, institutions usually adopt several parts COBIT, ITIL, PMI, CMMI, ISO.

2. Research methods

Vulnerability testing was carried out in 33 university-owned web sites in the Jakarta area, and was held for a period of 2 months from 1 September to 31 October 2018. Due to the security of the website url, the IP address and name of the website owner was omitted in this study. For this reason, the number one (1) to thirty-three (33) alias on the web site is used as their name. Vulnerability analysis is the art of finding vulnerabilities in software. The idea is to find vulnerabilities before the application is deployed or before the attacker can find vulnerabilities. To do vulnerability

analysis, tools are used that can automatically find vulnerabilities in software. The purpose of using this tool is to find all possible vulnerabilities in an application. Some examples of causes of vulnerability on websites include:

- Weakness of the input validation process
- Weakness of login mechanisms.

Error handling. It is imperfect to terminate the connection to the database. The methodology used for this research is the constructive research method which is to test the vulnerability of college web site security and then record and collect responses from web security vulnerability tests. The test tool uses several tools that are available in the Kali Linux operating system, namely Nessus and Skipfish.

2.1. Nessus

Nessus was created by Renaud Deraison in 1998. Nessus is one of the network security scanners that must be used by system administrators. Nessus is a scanning software, which can be used to audit security of a system, such as vulnerability, misconfiguration, security patches that have not been applied, default passwords, and denial of service, Nessus serves to monitor network traffic. Because the function of Nessus can be used to detect weaknesses or defects from a system, Nessus becomes one of the mainstay tools when conducting a security audit of a system. Before Nessus version 3, this application was open source and became one of the prima done in the open source world. But now, starting with Nessus version 3 by Tenable Security it is used as a proprietary and closed source application. Neessus display can be seen in Fig. 1.
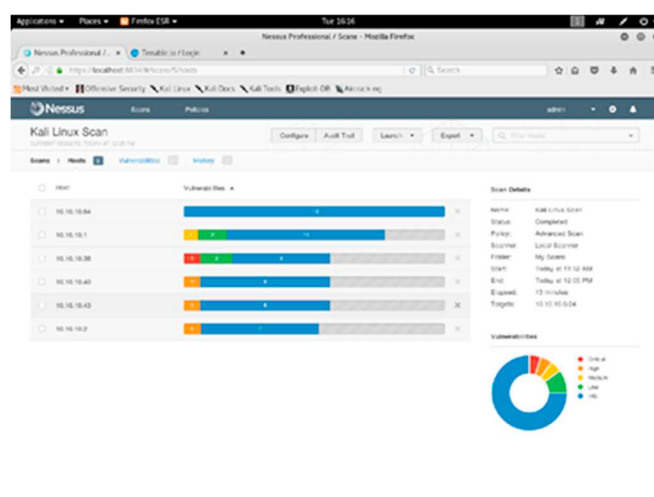

Fig. 1. Nessus display.

2.2 Skipfish

Skipfish is a new open source web application scanner, written in C programming, developed by Google. The purpose of Skipfish is similar to the purpose of previous web security hole scanners such as Nmap and Nessus, this allows web developers to scan their applications or sites for possible security problems that might lurk. Skipfish can be used as an automated web application security tool, which has been designed to find vulnerabilities in web applications before a hacker finds and exploits them. Skipfish can operate on cross platforms such as Linux, BSD, MAC and windows. Skipfish can be used to determine whether the codes on a web site are vulnerable to common attacks such as cross-site scripting (XSS), SQL, and XML injection attacks. After Skipfish finishes scanning, it will continue by preparing interactive site maps for targeted sites by doing repeated browsing and dictionary-based

searches. The final report produced by this tool is intended to function as a basis for security assessment of web applications (See Fig. 2).

Fig. 2. Skipfish display.

In this study the domain used to determine the value of the maturity level is the vulnerability that has been detected by the Nessus and skipfish tools. The number of vulnerabilities correlates with the maturity level. While for the maturity model, a Cyber Security Maturity Model approach is used. This model was chosen because web sites are very vulnerable to cyber-attacks. This model classifies the maturity level into 5 levels, as shown in Fig. 3. Explanations of each level are as follows:

- Level 1: Reactive & Manual, this security set-up is primitive and consists of minimum controls, such as firewalls and anti-virus software at the endpoint, that are signature-based and ineffective in mitigating sophisticated attacks. The threat level is also characterized by the lack of dedicated network security staff and frequent "firefighting" to eradicate malware and restore business operations using manual processes.
- Level 2: Tools based, the organization has invested and implemented a variety of security tools. However, the solutions are usually adopted on a piecemeal basis rather than as a fully integrated approach. Adoption of security processes and ensuring the skill sets of security professionals remain weak as well. As a result, the threat mitigation level is only slightly better due to the use of more tools, providing a greater degree of automation to detect and respond to cyber-attacks. There is also ample room for improvements in integration for better threat mitigation.
- Level 3: Integrated Picture, the organization has a series of aligned security operations, capabilities and processes that begins with the ability to "see" broadly and deeply across the IT environment, and ends with the ability to quickly mitigate and recover from a security incident. There is a tighter integration with security controls alongside the stringent adoption of security processes and dedicated security staff trained to handle common cyber-attacks. There is also greater emphasis on interoperability among security controls, and adoption of standards- based data exchange of threat intelligence.
- Level 4: Active Defense, these organizations are predictive and agile; establishing fully-equipped Cyber Security Operations Centers leveraging security intelligence and analytics tools to illuminate potential threat events, assisting the operator in detecting threats and remediation the cyber-attack promptly. However, its lack of sophisticated capabilities of mitigating advanced targeted attacks using new threat vectors or social engineering techniques could still result in adverse effects on enterprise operations.
- Level 5: Resilient Enterprise, Organizations attaining this security level have a tightly integrated set-up of efficient security tools that are empowered by full visibility of threats across Information Technology (IT) and Operational Technology (OT) systems. It will also have the right processes and skill sets which are continually updated to

combat advanced attacks and all possible types of threat scenarios. These organizations adopt cyber security best practices and emphasize security awareness as a shared responsibility among all employees, by regularly providing training on how to stay safe online to prevent any disruptions to their business.

Fig. 3. Skipfish display   Cyber Security Maturity Model [7].

3. Results

From the scan results Vulnerability uses Nessus with the target IP of a college (University6) there are some security gaps as shown in Fig. 4. The vulnerability is described as follows:

- 5 with an orange high category
- 24 categories of medium colored yellow
- 11 low-colored green categories
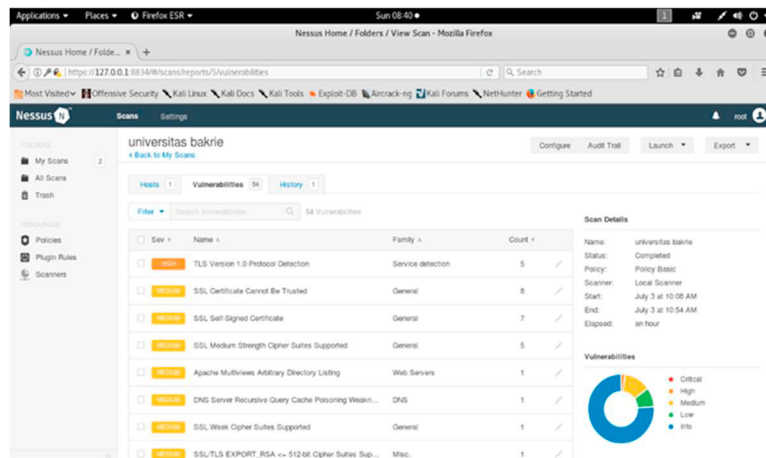- 123 in the info category in blue.

Fig. 4. Vulnerability obtained by Nessus on the web site.

The report obtained by Nessus tools from the university web site1 has the highest level of security loopholes, namely the TLS Version 1.0 Protocol Detection, which the payment card industry data security standard (PCI)

stipulates that the TLS 1.0 encryption protocol can no longer be used to secure. The Skipfish tool can display the contents of a folder from a web site. Fig. 4 is a display of Skipfish for the University6 folder. The folder in it still contains folders and files from the collection of Scanning results and parts of the Tools. The image appears in the index.html file. which is the result of scanning obtained from the Tool.
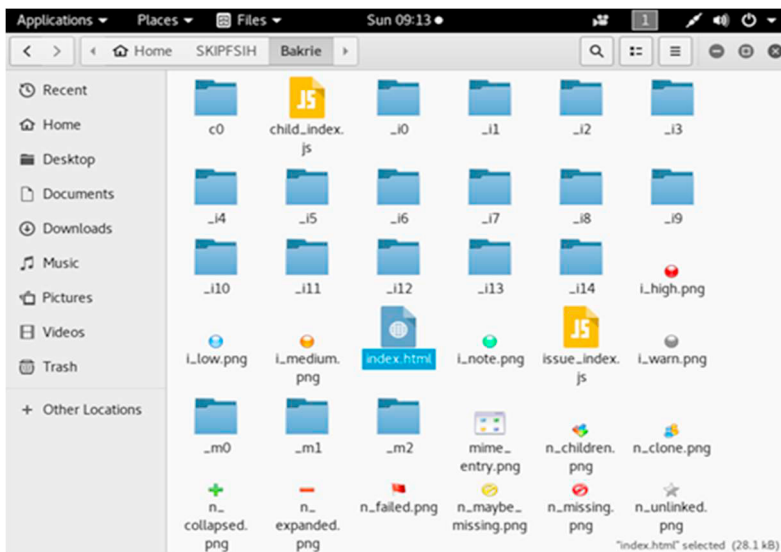

Fig. 5. The appearance of Skipfish illustrating a college web site folder.

The data from the vulnerability test also found that the number of vulnerabilities found on each college's web site also varied. The number of vulnerabilities on a web site can be assumed that the maturity of the web is low. Maturity for each college web can be seen in Fig. 5. To determine the maturity level, it is determined based on Table 1.

Table 1. Maturity level assessment.

Number of types of vulnerabilities	Maturity level
Less than 2	5
2 to 4	4
5 to 7	3
8 to 10	2
More than 10	1

From Fig. 6, it can be seen that the number of web sites that have a higher maturity level is relatively small. Table 2 shows the percentage of the maturity level value of 33 websites that have vulnerabilities. A high maturity level can be interpreted that the website has a low vulnerability.
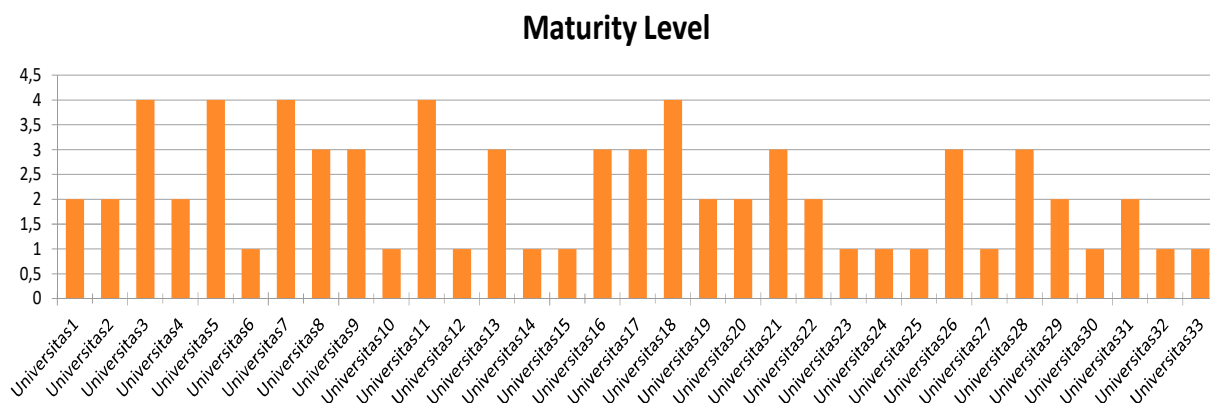
Maturity Level

Fig. 6. Maturity level.

The number of web sites that have level 4 maturity values is only 15% of the total 33 websites. This means that almost all websites have a low maturity level. Some of the causes of this low maturity level must be a serious concern for website owners. The possible cause of lower maturity level is the lack of implementation of security controls on the website, both during development and implementation. Therefore, the application of appropriate and strict controls must be carried out. The implementation of these controls must also be accompanied by periodic vulnerability testing.

Table 2. Maturity level assessment.

Maturity level	Prosentase
1	0.36
2	0.24
3	0.24
4	0.15
5	0

4. Conclusion

By testing the vulnerability of the web site, there will be some weaknesses found on the web site. These weaknesses can pose a security threat to the assets of the organization that owns the web site. To test vulnerabilities, you can use tools that are available in open source, where the tool can perform the vulnerability test process automatically and runs on various operating systems. The results obtained from the VA process on several web sites showed that there were still many vulnerabilities on these web sites. The number of vulnerabilities causes a lower maturity level of the web site. Most of the college websites in Jakarta have low maturity levels.

Reference

[1] El Idrissi, S, N. Berbiche, F. Guerouate, and M. Sbihi. (2017) "Performance Evaluation of Web Application Security Scanners for Prevention and Protection against Vulnerabilities." *International Journal of Applied Engineering Research* **12 (21)**: 11068-11076.

[2] Ferreira, A.M., and H. Kleppe. (2011) "Effectiveness of Automated Application Penetration Testing Tools".

[3] Web Application Security Consortium. (2009) "Web Application Security Scanner Evaluation Criteria." Available from: www.webappsec.org.

[4] Shrestha. (2012) "Security Assessment via Penetration Testing: A Network and System Administrator's Approach." [Master's Thesis], Oslo University.

[5] Santos, R.S., M.R.S. Borges, J.H. Canós, and J.O. Gomes. (2011) *The Assessment of Information Technology Maturity in Emergency Response Organizations*, Springer Science+Business Media B.V. pp. 593-613.

[6] CMMI Product Team. (2002) *Capability Maturity Model® Integration (CMMISM), Version 1.1*, Carnegie Institute Pittsburgh, PA 15213-3890. **Aug**.

[7] Forst, A, and Suvillan. (2017) *Exploring Cyber Security Maturity in Asia A study of Enterprise Corporate Executives, IT Executives & IT Practitioners' Perceptions towards Cyber Security Readiness in Asia-Pacific,* LogRhythm.