Proceedings of the 2nd Faculty of Industrial Technology International Congress
International Conference
Bandung, Indonesia, January 28-30, 2020
ISBN 978-623-7525-37-0

ANALYSIS OF POTENTIAL SECURITY ISSUES IN REGIONAL GOVERNMENT X WEBSITE USING SCANNING METHOD IN KALI LINUX

Jelita Putri Deviarinda[1*], Avon Budiyono[2], and Ahmad Almaarif[3]

[1 2 3] Department of Information System, Telkom University, Bandung - INDONESIA

* Corresponding author e-mail: jelitaputrid@student.telkomuniversity.ac.id, avonbudi@telkomuniversity.ac.id, ahmadalmaarif@telkomuniversity.ac.id

Abstract

The importance of website security is a top priority after data leakage or damage occurs. Website is a web page that is interconnected and contains a collection of information and can be accessed through the home page using a browser and internet network. According to the ministry of communications and information, 50% of the government's website is under threat from hacker attacks that can harm private information. Vulnerability assessment or process of identifying the weaknesses of a system can be an effective way to control and prevention against risks that occur. Given these problems, it is necessary to analyze the potential vulnerabilities on websites with vulnerability assessments aimed at preventing security vulnerabilities. In this study the analysis of potential website security loopholes was performed using scanning methods. The test is carried out with a vulnerability assessment using tools that are available on Linux and run on a virtual machine. Kali Linux is an operating system that has many tools including penetration testing, ethical hacking and network security assessment. This research was conducted using uniscan and nmap tools by scanning the target URL and assisted by using a web browser. The result of testing is to find a security vulnerability using a scanning method with tools and then giving the solution of the vulnerability it acquired.

Keywords: Security, Website, Vulnerability Assessment, Scanning, Kali Linux

1. Introduction

The development of technology in the current era is developing very rapidly. Information technology is a technology that can be used to process, obtain good data information, which is relevant, accurate information (Uno & Lamatenggo, 2011). The existence of information technology has enabled people to exchange information using Internet. Internet (Interconnected Network) is a network of computers that connect between networks globally, the Internet can also be called a natural network of a wide network (Sibero A. F., 2013). According to (APJII, 2018) Internet user in Indonesia has increased to 143.26 million people in 2017 or equivalent to 54.7 percent. The internet has a lot of information, one of which can be channeled through the website. Website is a web page that is interconnected and contains a collection of information and can be accessed through the home page using a browser and internet network. Based on the communication and Informatics White Book report in 2016 that a number of security incidents through Internet network in the domain of government is go.id often done cheating or data leakage (Iskandar, 2016). According to the Ministry of Communication and Informatics Office, 50% of Indonesia's government website is threatened by hacker attacks that can harm public personal data information.

Government is an agency to provide services to the community. There are many services provided by one of the online services which is a website that will facilitate the public in accessing information about the agencies in the government. Based on the report of the Communication and Informatics White Book year 2016 data obtained website with the domain go.id need a strong security to avoid attacks from outside Therefore, the purpose of this research is to find vulnerabilities and conduct analysis to prevent the occurrence of security vulnerabilities on government websites.

2. **Literature review**

2.1. Website

Website is a collection of information pages provided through Internet channels so that it can be accessed all over the world while connected to the Internet network without limited time and space (Suryayusra, 2014). According to Raharjo (Raharjo, 2011) website, is a service within the network of information space. As with Sibero (Sibero A. , 2013) website is a system related to documents and generally to display information in the form of text or images on the Internet network.

2.2. Website Security

Website security is important in building a website, good safety development is done at the beginning of the design of the website by the developer. Developers should follow the trend of attacks from hackers who always evolve with the development of Technology (Gultom & Mawaddah, 2015).

2.3. Vulnerability Assessment

Vulnerability Assessment (VA) is a process to identify or scan a system or software or network to find out defects and weaknesses. It also includes a series of systematic actions that are used to review and prioritize security vulnerabilities in network or communications systems or application services (Yaqoob, et al., 2017). Vulnerability Assessment is a systematic examination to determine the vulnerability to the information system and take precautions to minimize threats and reduce the risk of (Technology, 2013).

2.4. Technique of Vulnerability Assessment

Some of the Vulnerability Assessment techniques (Goel & Mehtre, 2015):

- Static Analysis

This technique do not run test cases or exploit. Static analysis is in this technique analyze the contents of the system and find out the types of vulnerabilities that exist and do not exploit the system. Weakness in this technique is requiring a lot of time for testing.

- Manual Testing

This technique do not require any tools or software to know the vulnerability. This technique tests by setting up a test plan manually or without a testing plan. On this technique do not use tools for testing and this technique is very less than on other techniques.

- Automated Testing

Automated testing technique uses automated vulnerability testing tool to determine vulnerabilities in the system. Accuracy in this technique is very good than other techniques. In this test use a scanner to test.

- Fuzz Testing

Known as fuzzing. Fuzz testing is done by inserting invalid data or any data into the system and then looking for crashes and failures. This technique can be used to determine the vulnerability of zero day.

4.1. Kali Linux

Kali Linux is a Linux security audit that is ready for companies based on Debian GNU or Linux. Security professionals usually use Linux times to do penetration testing, forensic analysis, and security audits. Kali Linux is a rolling distribution, meaning it will receive daily updates. The Menu on Kali Linux makes it easy to get tools for various tasks and activities including: Vulnerability analysis, Web application analysis, database assessment, password attack, sniffing and spoofing, forensics (Raphaël Hertzog & Aharoni, 2017).

3. **Methodology**

The research methods used in this study use testing method research (Hambling & Goethem, 2018), there are five phases in the study which is the cycle of testing. Start from Test Planning and Control, Test Analysis and Design, Test Implementation and Execution, Evaluating Exit Criteria and Reporting, and Test Closure Activities.

Fig. 1: Testing Methodology (Hambling & Goethem, 2018)

Fig. 1 explains the phase flow of the vulnerability testing methodology in research. Here is an explanation of each phase:

- Test Planning and Control

Test planning is to create vulnerability criteria during testing. Criteria is when the testing process will end. The controls are what will be done if they do not match the plan as described in the test planning, after which the adjustments are made.

- Test Analysis and Design

Test analysis and design focus on the details of what to test and how to combine it with a test case. Test analysis and Design is a bridge that connects between planning and execution.

- Test Implementation and Execution

Implementation of testing and implementation involving test execution, and preparation before testing. This stage in execution using the uniscan and nmap tools and assisted by the Web browser.

- Evacuating Exit Criteria and Reporting

At the stage of Evaluating Exit Criteria and Reporting will be evaluated on the outcome of the test execution, then it will be determined whether the testing expires or continues.

- Test Closure Activities

The closure activity of the focus test to ensure that everything has been running well, the report is completed and bugs are closed.

This research will use all phases to test the vulnerability on target.

4. Experimental Result and Analysis

On this research focuses on the discovery of the vulnerabilities that exist on the target site X district and will provide recommendations to address the vulnerabilities found. The first step is test planning and control is planning the process will begin and expire. Next prepare the target website and test the vulnerability by using nmap, uniscan and assisted web browser tools that aim to get more information about the vulnerabilities that are on the website. The testing process is done on a virtual machine and uses operating system linux.

4.1. Vulnerability Assessment with Nmap Tools

Nmap is a port scanner that retrieves the IP address of the target machine or the hostname and then finds the basic information associated with it.

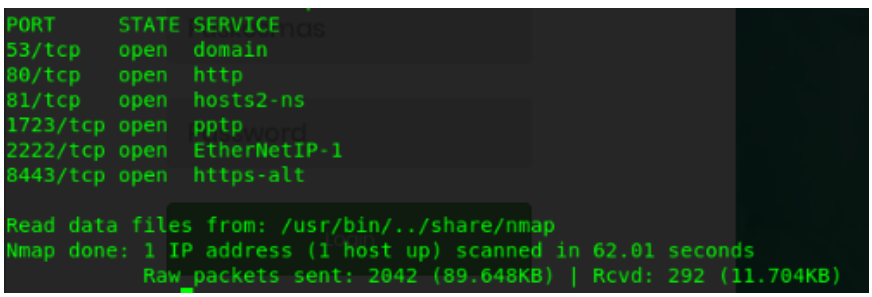

Fig. 2: Scanning Nmap Port Result

Fig. 2 is the result of the scanning of nmap on the target website. The following information that can be obtained:

- Port 53/tcp is a domain that has open port status.
- Port 80/tcp is a http that has open port status.
- Port 81/tcp is a hosts2-ns that has open port status.
- Port 1723/tcp is a pptp that has open port status.
- Port 2222/tcp is a EtherNetIP-1 that has open port status.
- Port 8443/tcp is a https-alt that has open port status.

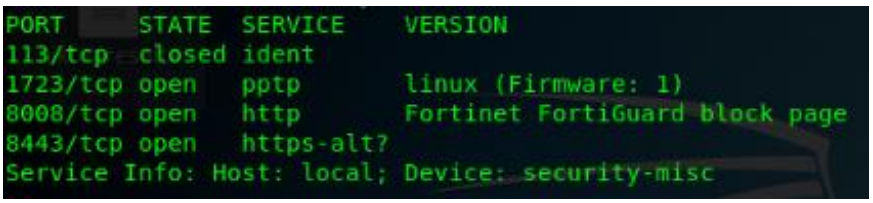

Fig. 3: Scanning Nmap Port Result

Fig. 3 is Nmap port result scanning, in different command with Fig. 2 information that can be obtained is as follows:

- Port 113/tcp is a ident that has closed port status.
- Port 8008/tcp is a http Fortinent Fortiguard block page that has open port status.

4.2. Vulnerability Assessment with Uniscan Tools

Uniscan is an open-source penetration testing tool. Uniscan can scan vulnerabilities on target websites, folders, and security issues. Meanwhile, the administrator panel of the target website can be found through a directory check with Uniscan.

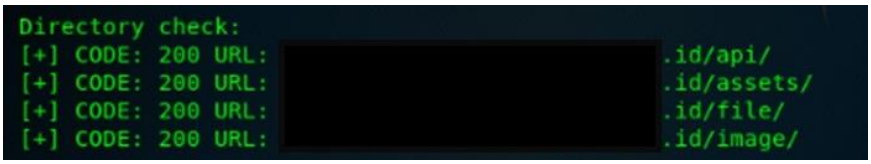

Fig. 4: Directory Check Uniscan Result

Fig. 4 is the result of scanning Uniscan that displays the directory check on the target website it is .id/api, .id/assets, .id/file, .id/image.

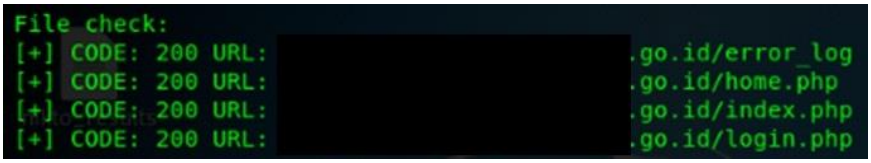

Fig. 5: File Check Uniscan Result

Fig. 5 is the result of scanning Uniscan that displays the file check on the target website it is .id/error_log, .id/home.php, .id/index.php, .id/login.php.

4.3. Directory Check and File Check Uniscan in the Web Browser

Web browsers are software to receive and present information over the Internet. At this stage the Web browser used chrome to check directories and files that have been testing on Uniscan tools.

Fig. 6: Directory Check File

Fig. 6 is a test in Web browser based testing on Uniscan that is in the Directory Check file section. In the Directory Check file section there is a file contents manual book.

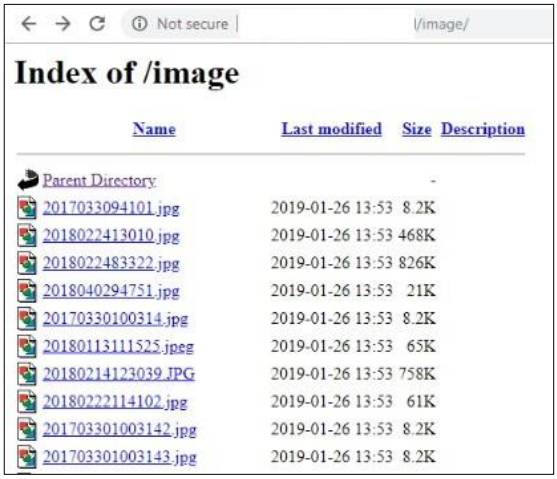

Fig. 7: Directory Check Image

Fig. 7 is a test in Web browser based testing on Uniscan that is in the directory check the image section. In the directory check the file section there are all images available on the target website and the size and last modified.

Fig. 8: File Check Error Log

Fig. 8 is a test in Web browser based testing on Uniscan that is in the file check error log. In the file check this section there are user information used with access time and modification.

5. Conclusion

Based on testing using different tools resulting in various kinds of vulnerabilities such as when conducting testing using uniscan tools and assisted with Web browsers is information obtained is found directory and files. Hackers can find out the information that is on the directory and files that are already in scanning. This information will be used by hackers in data retrieval. Testing using NMAP tools can show both open and closed ports and there are ports that need to be closed to avoid hackers use open ports to perform hacker and exploitations against the website. Website analysis by testing using Web browser is Google Chrome. The conclude on testing this hacker can find out the information the user name used. This information will be used by hackers in conducting tests using SQL Injection. Therefore it is recommended to immediately handle and upgrade the vulnerability because to minimize the occurrence of threats from outside.

6. References

APJII, A. P. (2018, March 22). *Penetrasi Internet di Indonesia Capai 143 Juta Jiwa.* Retrieved from https://apjii.or.id/downfile/file/BULETINAPJIIEDISI22Maret2018.pdf

Goel, J. N., & Mehtre, B. (2015). 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015). *Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology*, 712-713.

Gultom, L. M., & Mawaddah, H. (2015). Analisis Celah Keamanan Website Instansi Pemerinah Di Sumatera Utara. *Teknovasi*, 1.

Hambling, & Goethem. (2018). Testing Methodology. In L. J. Siagian, *Software Testing Automation* (pp. 6-8). Yogyakarta: Deepublish.

Iskandar, B. Y. (2016). *BUKU PUTIH KOMUNIKASI DAN INFORMATIKA 2016.* Jakarta: Badan Litbang, SDM Kementerian Komunikasi dan Informatika.

Raharjo, B. (2011). *Belajar Pemrograman Web.* Bandung: Modula.

Raphaël Hertzog, J. O., & Aharoni, M. (2017). *Kali Linux Revealed Mastering the Penetration Testing Distribution.* USA: Offsec Press .

Sibero, A. F. (2013). *Web Programming Power Pack.* Yogyakarta: MediaKom.

Suryayusra. (2014). Analisis Web Vulnerability pada Portal Pemerintahan Kota Palembang menggunakan Acunetix Vulnerability.

Technology, N. I. (2013). VULNERABILITY ASSESSMENT AND PENETRATION TESTING IN THE MILITARY AND IHL CONTEXT. *Security and Privacy Controls for Federal Information Systems and Organizations*, 53.

Uno, H. B., & Lamatenggo, N. (2011). *Teknologi Komunikasi dan Informasi.* Jakarta: PT Bumi Aksara, cet 2 .

Yaqoob, I., Hussain, S. A., Mamoon, S., Naseer, N., Akram, J., & Rehman, A. u. (2017). Penetration Testing and Vulnerability Assessment. 10-11.