I. J. Computer Network and Information Security, **2019, 7, 8-12**
Published Online July 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.07.02

Open Source Intelligence Testing Using the OWASP Version 4 Framework at the Information Gathering Stage (Case Study: X Company)

I Putu Agus Eka Pratama
Udayana University, Bali, Indonesia
E -mail: eka.pratama@unud.ac.id

Anak Agung Bagus Arya Wiradarma
Udayana University, Bali, Indonesia
E-mail: 9egungwira5@gmail.com

Received: 09 April 2019; Accepted: 19 May 2019; Published: 08 July 2019

***Abstract*—**The application of technology in various fields makes mobility even higher, one of them is by making a website for exchange and manage information. However, with information disclosure causing security and protection issues to be considered. One of the website security techniques can be done by using the penetration testing method to know the vulnerability of the system. This study will implement tools with the Open Source Intelligence concept, namely Maltego as a medium for conducting security testing and using the OWASP version 4 framework as a standardization of steps taken when security test goes on. This study will focus on information gathering security testing of important factor of the X Company's website. The results of testing and analysis with the OWASP version 4 framework with the Testing for Information Gathering module show that the web application system used by X Company has information vulnerability of the used web server version, GET and POST requests, URL systematics, website framework, website builder component, and the outline of the website architecture. The researcher gave several recommendations related to the vulnerability of the website which later can be used by X Company website administrators to improve website security and protection.

***Index Terms*—**Information Gathering, Maltego, OSINT, OWASP, Penetration Testing, Website.

I. Introduction

The application of technology is very helpful in various fields and has a positive impact on human life, one of which is the dissemination of information through the Internet through a Website. But the disclosure of information on a Website can be a weak point of an organization that uses the website as an information medium. Security enhancements on the website can be done by testing the vulnerability of the website, one of which is the penetration testing method. The steps to do penetration testing consist of various stages, one of which is the information gathering stage where the attacker will gather information such as domain names, IP addresses, port information, and so on. Penetration testing has several frameworks that can be used, one of which is OWASP (Open Web Application Security Project) which focuses on web application security.

The OWASP Framework used in this study is the OWASP framework version 4 of 2015 using the framework module: 4.2 Testing for Information Gathering where the module is dedicated to performing information gathering stages. The software / tools used are tools with the OSINT category. OSINT (Open Source Intelligence) One of the tools with the OSINT concept is Maltego. This study will use Maltego as the main tool in carrying out information gathering processes on case studies of X companies with outputs of evaluation report results that will be used as a reference for action recommendations to minimize the level of vulnerability of existing systems.

II. Literature Study

A. Open Source Intelligence

OSINT (Open Source Intelligence) is a part of intelligence disciplines that are related to intelligence generated from the availability of information for the public that is collected, exploited, and disseminated in a timely manner to the right audience for the purposes of handling certain information and intelligence needs [5,7]. The main function of the use of OSINT is in the functions of national security, law enforcement, and business intelligence and is valuable for analysts who use non-sensitive intelligence in answering classified, non-classified, and proprietary intelligence requirements in all previous intelligence disciplines [8,9]. The purpose of OSINT in the context of penetration testing is to gather as much information as possible about the attacks that will

be carried out. Specific testing agreements that involve organizations and clients allow some information to be released before the testing itself [6].

B. Maltego

Maltego is a software developed by Paterva and is used by professionals or experts in the field of security and forensic investigators to collect and analyze open source information for intelligence purposes specifically. Maltego can also be used for handling evidence that is useful because of the large amount of data generated by the method of penetration testing accidentally during the attack on the target [9]. A very important feature in Maltego is the ability to search for deeper information using reference information that has been collected regarding OSINT sources [4]. Maltego can easily collect information from various sources and use various kinds of transformations to process and produce results in graphical form so that it is easier for users to understand. Processing of the information has been embedded in Maltego and can also be adjusted based on user needs [12]. Maltego is developed in the Java programming language and runs on the Kali Linux operating system. Users are required to register to be able to use Maltego for free. After registered users, users can already use Maltego to collect targeted digital information on the internet.

C. Penetration Testing

The penetration testing method or often called "pentest" is the practice of computer system, network, or web application security testing to find security vulnerabilities that can be exploited by attackers by providing stages of system attacks to the system [1]. The penetration testing method can be facilitated by using tools or done manually [10]. The processes contained in the penetration testing method include information gathering, identifying penetration points, and also reporting the results of testing. Implementation of security testing with the penetration testing method is recommended to use a related framework so that the stages of attack carried out towards the system have standardization that has been developed and recognized by certain organizations that are experts in the field of security testing [2]. The main purpose of penetration testing is to identify system security weaknesses. In addition, it can also be used to test organizational security policies, awareness of organizational employees on security requirements, and the ability of organizations to identify and respond to security incidents [11]. The results of system security testing evaluations from the penetration testing method that have been successfully identified or exploited will be collected and provided to administrators, organizational owners, or organizational system managers with the aim of giving them recommendations for making decisions and prioritizing efforts to improve system security and protection [3].

D. OWASP

OWASP is a non-profit organization that focuses on improving software security [4]. OWASP provides many tools, guides and testing methodologies for cyber security under an open source license, specifically the OWASP Testing Guide (OTG) [14]. The OTG is divided into three main parts including the OWASP testing framework for web application development, web application testing methodology, and system evaluation reporting. The web application testing methodology can be used independently, or can be used as a testing framework. A web application developer can use the framework to build web applications by considering the protection and security aspects followed by security testing with the penetration testing method to test the system security of the web application developed [16]. The OWASP Testing Guide Framework has a strong focus on the level of security of web applications in all software development lifecycles aspect that different with other penetration testing security testing frameworks, such as ISSAF and OSSTMM, which is both of them are intended to test the security from implementation. The OWASP Testing Guide is specifically targeted to a single scope of domain, which as web applications [2].

III. Research Methodology

The research methodology begins with conducting a literature study that aims to understand the application of research concepts. After conducting a literature study, researchers will start a search and analysis of information related to the case studies used. The information gathering phase was conducted with the aim of gathering detailed information about the case study website. After completion, an evaluation report will be made to find out recommendations that can be given by the researcher. The following is a sequence of research methods.

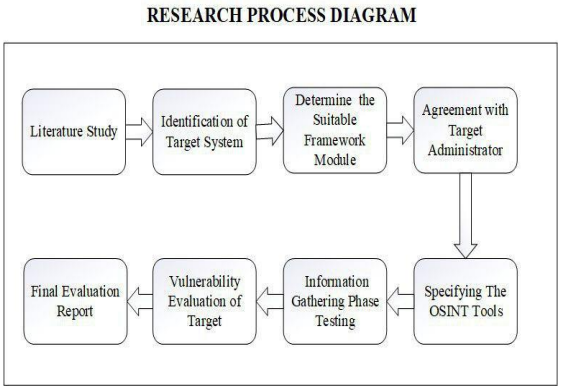

Fig.1. Research Process Diagram

IV. Test Results

The use of Open Source Intelligence tools in testing results and discussion of the research will be displayed in 3 parts, which as the results of testing, testing analysis, and testing recommendations.

A. Maltego as Tool

Testing the information gathering phase is done by using Open Source Intelligence tools with specific functions to gather information on the target. This research used Maltego as a media tool to support the research stage. The following figure is the appearance of the startup from Maltego which runs on Ubuntu Linux OS 18.04

B. Testing Results of OWASP Framework Version 4

Testing phases are carried out on the web application target using the Testing for Information Gathering module which consists of 10 phases to find information as complete as possible from the target as the purpose of the information gathering stage. The following table shown below is a table of test results.

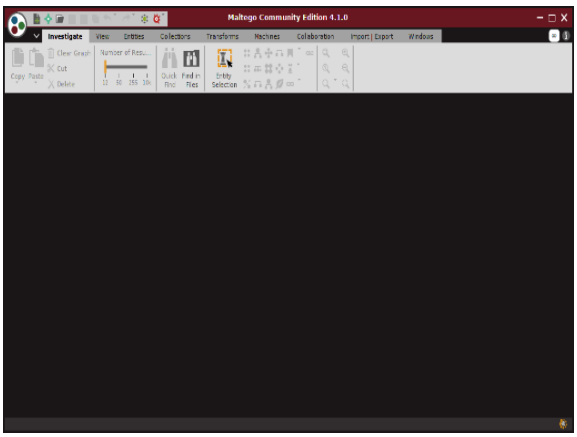

Fig.2. First Appearance of Maltego

Table 1. Testing Results of OWASP Version 4

Number	Module	Objective	Result
4.2.1	*Conduct Search Engine Discovery and Reconnaissance for Information Leakage (OTG-INFO-001)*	Understanding the design and configuration information from applications/systems/ organizations that can be accessed openly either directly (on the organization's website) or indirectly (on third party websites).	Success
4.2.2	*Fingerprint Web Server (OTG-INFO-002)*	Find the version and type of web server used by the target to find out the weaknesses and types of exploits that are suitable for use during testing.	Fail
4.2.3	*Review Webserver Metafiles for Information Leakage (OTG-INFO-003)*	Knowing the leakage of information from the directory of the web application	Success
4.2.4	*Enumerate Applications on Webserver (OTG-INFO-004)*	Calculate applications on the target web server range	Success
4.2.5	*Review Webpage Comments and Metadata for Information Leakage (OTG-INFO-005)*	View comments on the designate web page target and find metadata to had better knowledge of the target and to find information leaks.	Success
4.2.6	*Identify Application Entry Points (OTG-INFO-006)*	Understanding how requests and responses were formed from target	Fail
4.2.7	*Map Execution Paths Through Application (OTG-INFO-007)*	Make the mapping of the target website and understand the main workflow	Fail
4.2.8	*Fingerprint Web Application Framework (OTG-INFO-008)*	Knowing the type of the used framework from the target website so the tester will have a better understanding of the security testing methodology.	Fail
4.2.9	*Fingerprint Web Application ((OTG-INFO-009)*	Identify the version of the target website to determine weaknesses and exploitation methods that are suitable for use during testing	Fail
4.2.10	*Map Application Architecture (OTG-INFO-010)*	Identify and know the overall architecture of the target website	Fail

C. Testing Analysis of OWASP Framework Version 4

Based on the results of testing using OWASP version 4 in table 1 shows that the web application successfully passed in the phase (OTG-INFO-001), (OTG-INFO-003), (OTG-INFO-004), (OTG-INFO-005) and fail the test in phase (OTG-INFO-002), (OTG-INFO-006), (OTG-INFO-007), (OTG-INFO-008), (OTG-INFO-009), (OTG-INFO- 0010). The definition of failing in this study is when the testers can find information related to the description of the Testing for Information Gathering module on the OWASP framework within the scope of the mentioned phases. Modules that do not pass the testing can provide vulnerability to the website applications because testers are played as same role as the attacker that can find information needed to penetrate further on the next stage.

D. Testing Recommendations of OWASP Framework Version 4

The test results on modules that fail the Testing for Information Gathering modules will be displayed with the effect that will be appear from the attacker and recommendations that can be use by the web application administrator in table 2.

Table 2. Testing Recommendations of OWASP Version 4

Number	Module	Effect	Recommendation
4.2.2	*Fingerprint Web Server (OTG-INFO-002)*	An attacker who knows the type of web server can explore further the weakness of the web server and the type of attack that suitable for use	Use related modules available on the web server (Apache, IIS, etc.) to hide the web server version when making a request on an internet connection
4.2.6	*Identify Application Entry Points (OTG-INFO-006)*	Attackers can find out GET and POST requests made by the target website with the detail of data exchange	Using the HTTPS protocol with SSL to morely secure the connections on the web server and encrypt the GET and POST data sent by the web server
4.2.7	*Map Execution Paths Through Application (OTG-INFO-007)*	The attacker can find out the entire URL flow used along with their respective functions on the target website	Implementing Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) which functions is to detect and prevent attacks
4.2.8	*Fingerprint Web Application Framework (OTG-INFO-008)*	Attackers can find out the type of framework that used to build the target websites to learn weaknesses and attacks that are suitable for use on the framework	Organizing the advanced encrypt on the framework used to build websites so that attackers cannot penetrate and fully control the framework
4.2.9	*Fingerprint Web Application ((OTG-INFO-009)*	Attackers who know the version of the website builder component can learn more about the weaknesses and types of attacks that are suitable for use	Using the modules provided on website builder components (Apache, Jquery, etc.) to hide the version that used when the attacker tries to gather information
4.2.10	*Map Application Architecture (OTG-INFO-010)*	Attackers who know the main architecture of the website can gather important information to be studied further to carry out attacks on the target website	Administrators can build the security as strong as possible to secure sensitive information from the used web architecture when hackers start the scanning progress. Proxy servers and encryption can be used as a solution to secure website information

V. Conclusions

The results of testing and analysis on the website which is used as a case study (target) by using the Testing for Information Gathering module on OWASP framework version 4, shows that the website builder components can still be penetrated and analyzed by the attackers. This statement can be determined from the results of the penetration tests that show unsuccessful or fail results in certain modules. Some recommendations were given by researchers to improve website security to be better and safer and not easily attacked by irresponsible parties and attackers.

References

[1] Abel Yeboah-Ofori, P. A. B. (2017). "Cyber Intelligence and OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media." International Journal of Cyber-Security and Digital Forensics 7(1): 11.

[2] Akhyar Lubis, A. T. (2017). "Security Assessment of Web Application Through Penetration System Techniques." International Journal of Recent Trends in Engineering & Research 03(01): 7.

[3] Aleatha Shanley, M. J. (2015). Selection of Penetration Testing Methodologies: A Comparison and Evaluation. 13th Australian Information Security Management Conference. Edith Cowan University Joondalup Campus, Perth, Western Australia, Edith Cowan University Research Online.

[4] Bahrun Ghozali, K., Sudarmawan and (2018). "Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) untuk Penilaian Risk Rating "Creative Information Technology Journal 4(4): 11.

[5] Benes, D. L. (2013). "OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm." Journal of Strategic Security 5(6): 15.

[6] Bert-Jaap Koops, J.-H. H., Ronald Leenes (2013). "Open-Source Intelligence and Privacy By Design." Computer Law & Security Review: 12.

[7] Deris Stiawan, M. Y. I., Abdul Hanan Abdullah, Fahad Aljaber, Rahmat Budiarto (2017). "Cyber-Attack Penetration Test and Vulnerability Analysis "International Journal of Online and Biomedical Engineering 13(1).

[8] Florian Schaurer, J. S. (2013). "The Evolution of Open Source Intelligence." Journal of U.S. Intelligence Studies 19: 4.

[9] Kawakita Masaru, S. S. (2018). "Detection, Auto Analysis of Cyber Threats Using Open Source Intelligence." NEC Technical Journal: Special Issue on Cybersecurity 12(2): 4.

[10] Mohammad Muhsin, A. F. (2015). "Penerapan Pengujian Keamanan Web Server Menggunakan Metode OWASP Versi 4 (Studi Kasus Web Server Ujian Online)." Multitek Indonesia 9(1): 9.

[11] Muhammad Zunnurain Hussain, M. Z. H., Muhammad Taimoor Aamer Chughtai (2017). "Penetration Testing In System Administration." INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH 6(6): 3.

[12] Petersen, R. L. (2017). Enhancing Identification and Reporting of Potentially Harmful Public Data on Danish Organization. Kongens Lyngby, Technical University of Denmark: 211.

[13] Pratama, I. P. A. E. (2018). Security Best Practice at Gianyar Smart Government Using Belati (An Indonesian OSINT Tool). CODEBALI International Cyber Security Conference and Exhibition, Padma Hotel, Legian, Bali, Indonesia.

[14] Raden Teduh Dirgahayu, Y. P., Adi Fajaryanto (2015). "Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server "Jurnal Imiah NERO 1(3): 7.

[15] Shivayogimath, C. N. (2014). "An Overview of Network Penetration Testing." International Journal of Research in Engineering and Technology 03(07): 5.

[16] Yunanri W, I. R., Anton Yudhana (2018). "Analisis Deteksi Vulnerability Pada Webserver Open Jurnal System Menggunakan OWASP Scanner." Jurnal Rekayasa Teknologi Informasi 2(1): 8.

Authors' Profiles

I Putu Agus Eka Pratama took his bachelor degree at Institut Teknologi Telkom and master degree at Institut Teknologi Bandung (ITB), both of them at Informatics. He has been working as a researcher and lecturer at Information Network and System (INS) Research Lab at ITB. At 2015 until now as a lecturer at Udayana University. His interest field are Smart City, Big Data, Computer Network and Security, Linux, Intelligent Transportation System. He is also an IT book writer and IT consultant.

Anak Agung Bagus Arya Wiradarma is the student and currently studying on information technology major in the Engineering Faculty of Udayana University. His research interests are mostly about computer network and network security management topics. Such as network centric principles, network programming, and network security application.

How to cite this paper: I Putu Agus Eka Pratama, Anak Agung Bagus Arya Wiradarma, "Open Source Intelligence Testing Using the OWASP Version 4 Framework at the Information Gathering Stage (Case Study: X Company)", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.7, pp.8-12, 2019.DOI: 10.5815/ijcnis.2019.07.02

