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

Vulnerability Assessment for Basic Data of Education Website in Regional Government X – A Black Box Testing Approach

Atho' Novian Awlarijal[1*], Ahmad Almaarif[2], and Avon Budiono[3]

[1 2 3] School of Industrial and System Engineering, Telkom University, Bandung - INDONESIA

Corresponding author email: athonovian@student.telkomuniversity.ac.id, ahmadalmaarif@telkomuniversity.ac.id, avonbudi@telkomuniversity.ac.id

Abstract

The development of technology in the current era is growing more rapidly. One example is the spread of information is no longer using the print media but uses web media. The Department of Education in Regional Government X uses the website to disseminate information to outside parties. The Department of Education uses the web to manage basic data of education (*Dapodik*). In the current era, information is very crucial. According to the Open Web Application Security Project (OWASP) in 2017 there are several vulnerabilities that often occur on websites such as injection flaws, sensitive data exposure, cross-site scripting (XSS), etc. This will impact the attacker in exploiting the system, retrieving information or important data on the web. Therefore, security must be ensured to maintain the integrity of the information on the website. One way to maintain the integrity of information on a website is by conducting vulnerability assessment. Vulnerability assessment is a series of actions to identify and analyze the possibility of security vulnerabilities in the system (ISACA, 2017). This paper provides a black box testing for vulnerability assessment of web application by mean of analyzing and using combined set tool to detect vulnerabilities. This black box testing using OWASP-ZAP dan OpenVAS for vulnerability scanning.

Keywords: information, security, web application, vulnerability assessment, black box testing

1. Introduction

Today, people have started to depend on the internet in everyday life. It can be concluded from increasing number of internet users in Indonesia. According to a survey conducted by the Indonesian Internet Service Providers Association (APJII 2017) internet users in Indonesia totaled 143.26 million people or around 54.68% of the total population of 262 million people. Internet users increased by around 10 million from 132.7 million the previous year. Internet users are predicted to continue to increase every year.

The government also uses the development of internet technology for basic data of education (*Dapodik*). Basic data of education (*Dapodik*) is a data collection system managed by the Ministry of Education and Culture which contains data on education units, students, educators, and education substance whose data is sourced from education units that are continuously updated online (Minister of Education and Culture 2015).

With the increase of internet users in Indonesia, more and more information will be obtained from the internet. This must be accompanied by a security system. Website security is needed to maintain the integrity of the information on the website. According to the Open Web Application Security Project (OWASP), there are ten vulnerabilities that often occur in web application (OWASP 2017). By taking advantage of these vulnerabilities, the attacker can exploit the system and retrieve sensitive information from system. One way to maintain the integrity of information on a website is by conducting a vulnerability assessment.

2. Literature review

2.1. Information Security

Information security is protecting information, data or other assets from access, disruption, or modification from unauthorized parties. In information security to ensure that information is said to be safe is known as the concept of Confidentiality, Integrity, and Availability, or commonly called the CIA Triad (Andress 2014)

Confidentiality is a part of information privacy that refers to the ability to safeguard information from irresponsible parties and only can be accessed by those who have access (Andress 2014). Confidentiality is protection of data from unauthorized access. In other words, only people who are authorized to do so can gain access to sensitive data. A failure to maintain confidentiality that means the secret data has been revealed and no way to un-reveal it.

Integrity is preventing the information or data from being change, modified or destroyed by unauthorized party and ensure the authenticity of information (Nieles, Dempsey and Pillitteri 2017). Data integrity is the content or property part of data that has not been illegally changed. Data integrity not only ensures that the data received is the same as the data sent, but also includes the process of sending from the sender and receiver, the data when stored in storage and processing on a computer. Maintaining data integrity can be done with authorization. Example of mechanism to control or maintaining data integrity are in the file system of Linux implement permission that restrict for preventing unauthorized changes.

Availability is ensuring information can be access reliable and timely (Nieles, Dempsey and Pillitteri 2017). In other words, availability is the ability to provide information when authorized party needs that information. Loss of availability may occur due to many reasons such as power loss, application or operating system problems, network attacks, or other problems.

2.2. Web Application Vulnerabilities

Web application vulnerabilities are some of the most common flaws in website. This paper describes some of the most common web application vulnerabilities based on OWASP Top 10 2017. OWASP Top 10 is valuable document for web application security from collaboration of security expert who shared their expertise to produce top ten list web application vulnerabilities (OWASP 2017). The OWASP Top 10 2017 has listed ten vulnerabilities below:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring

Injection, sensitive data exposure, and cross-site scripting (XSS) are the most popular vulnerabilities exploited by attacker. Injection flaws occurs when untrusted information or data sent to web application as part of command or query such command OS, query SQL, etc. Cross-site scripting (XSS) occur when web application input untrusted information or data without validation or update an existing web page with user supplied data like tag script html or JavaScript. XSS allow attacker to execute script in web browser. Sensitive data exposure occurs when there is no additional protection between client-server connections such as encryption.

2.3. Black Box

Black box testing is technique of testing web application without knowledge of internal web application conditions. It only examines the basic of aspects of system and no relevance or has little relevance to internal logical structure of the system (Khan and Khan 2012). Black box approach can use a web vulnerability scanner tools or manual penetration testing.

2.4 Vulnerability Assessment

A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source (National Institute of Standards and Technology 2012). Vulnerability assessment is a series of actions to identify and analyze the possibility of security vulnerabilities in

the system. Vulnerability assessments are usually carried out using automated scanning tools to carry out discovery, testing, analysis and reporting of system vulnerabilities through network-based or host-based (ISACA 2017).

Weaknesses that are owned by the system can occur due to internal and external factors. Internal factors occur due to lack of administrator awareness in managing the system. While external factors due to the weakness of the system made so that the attacker can easily exploit the system. Risks due to internal or external effects cannot be eliminated but vulnerability assessment can reduce existing vulnerabilities or security holes. According to OWASP, there are three vulnerability assessment cycles, namely detection, report and remediation (OWASP 2019).

3. Methodology

As mentioned earlier, the methodology used is a black box test for vulnerability assessment of web applications using a set of combined tools to examine various security issues (Awang and Manaf 2013). This paper experimented web application testing uses a combination of OWASP-ZAP and OpenVAS. OWASP-ZAP and OpenVAS choosen because the software are free and easy to use. Using different tool to increase the probability of finding various types of vulnerability.

Fig. 1: Vulnerability Assessment Process

Fig. 1 explains process for vulnerability assessment test on web application target through four phases namely Information Gathering, Vulnerability Scanning, Result Analysis, and Reporting (Doshi and Trivedi 2015). Information Gathering – Define scope target and basic information about web application. Vulnerability Scanning – Begin with define tools uses for scanning, installing, and configure tool. After that, scanning web application target using vulnerability scanner tools. Result Analysis – After scanning complete with tools, analyze result of detection from tools and test manual to ensure result of detection from tools vulnerability scanning.

4. Test Result and Analysis

The focus on testing is to find vulnerabilities that may exist in educational basic data web applications. So that security recommendations will be given to improve the web application. The first step is to determine the target scope. After that using Nmap for gathering information.

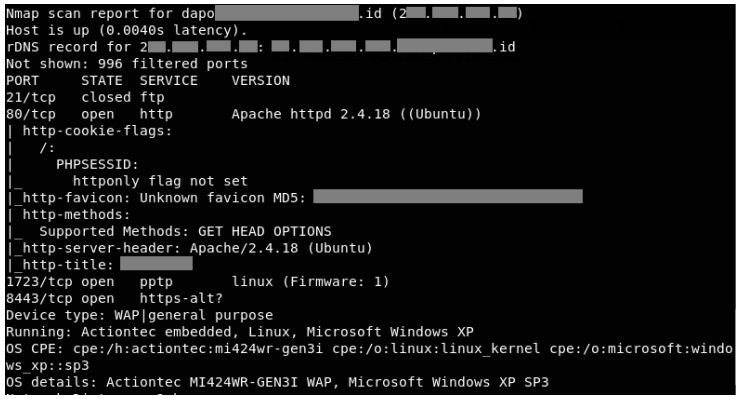

Fig. 2: Nmap Information Gathering

Fig. 2 shows that the web application DNS Record with IPv4 2xx.xxx.xxx.xxx and several port are open such port 80 for http service, port 1723 for pptp service, etc. Other information from Nmap are like device type, OS details, etc. After get some information, begin vulnerability scanning with tools namely OWASP-ZAP and OpenVAS. The black box vulnerability testing using Kali Linux as operating system.

4.1 Vulnerability scanner uses OWASP-ZAP

The Open Web Application Security Project Zed Attack Proxy (OWASP-ZAP) is one of popular open source free vulnerability security scanner tools and is actively development by an international team of volunteers. OWASP can find security vulnerabilities in web applications automatically. OWASP-ZAP is tool for penetration tester (pentester) to use for security testing. OWASP-ZAP also use while developing and testing a web application. Here is the result of vulnerability scanning basic educational data.

Table 1: Summary of detection on OWASP-ZAP

Risk Level	Total
High	1
Medium	2
Low	3
Informational	0

Table 1 shows the information after vulnerability scanning basic educational data web application using OWASP-ZAP. Total result of vulnerability scanning indicate that security system is insecure because there are many detected vulnerabilities and some of detection is high and medium level.

4.2 Vulnerability scanner uses OpenVAS

The Open Vulnerability Assessment System (OpenVAS) is an open-source application that is used to scan for vulnerabilities. OpenVAS capabilities such as authenticated testing, various internet protocols, performance tuning, etc. OpenVAS was developed and managed by Greenbone Network since 2009. OpenVAS is open source under the GNU General Public License (GNU GPL) license.

Table 2: Summary of detection on OpenVAS

Risk Level	Total
High	2
Medium	29
Low	1
Informational	40

Table 2 shows the vulnerability information that was detected using OpenVAS. The vulnerability scanning results using OpenVAS more than OWASP-ZAP. These results indicate that web applications are not safe because there are many detected even many high and medium level vulnerabilities, including low and informational logs.

4.3 Analysis Result

Table 3: Some Vulnerabilities Detected by The Application

Description	Nmap	OWASP-ZAP	OpenVAS
Cross-Site Scripting (Reflected)		✓	
Clear text transmission via HTTP			✓
Directory Browsing		✓	✓
Missing 'httpOnly' Cookie Attribute		✓	✓
Open Port	✓	✓	✓
Web Server Identification	✓		✓

Table 3 shows some vulnerability information detected through different applications. The result of vulnerability scanning can be used as parameter to minimize all forms attack from attacker. After get result from vulnerability scanning, next phase is result analysis. The analysis uses for validation that the detection from vulnerability scanner tools is valid. This paper analyzes several detections in high level not all detection result because too much. The first vulnerability detection found are cross-site Scripting (XSS), as a result of cross-site scripting injection, an attacker can bypass security on the client side, obtain sensitive information, and even insert dangerous

applications. So, the first step to validation is access the link that indicate XSS. After that, try inject with code in the search form, for example:

< h4 >< script > alert("coba XSS! "); </script >< h4 >

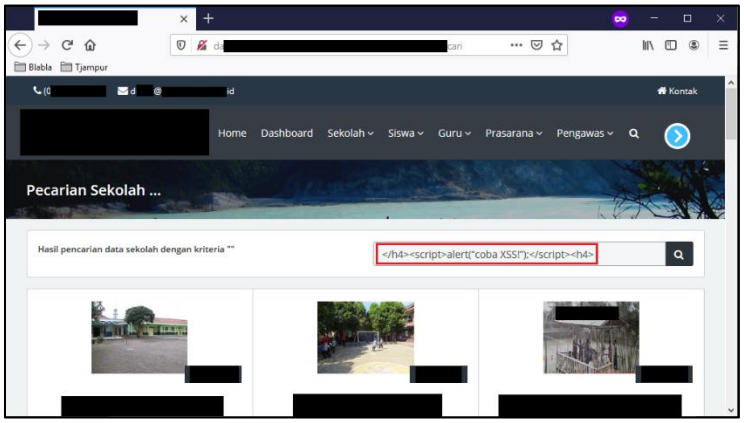

Fig. 3: Try XSS

After input inject code to search form, web application will respond by appearing in a pop up like figure 4 below.

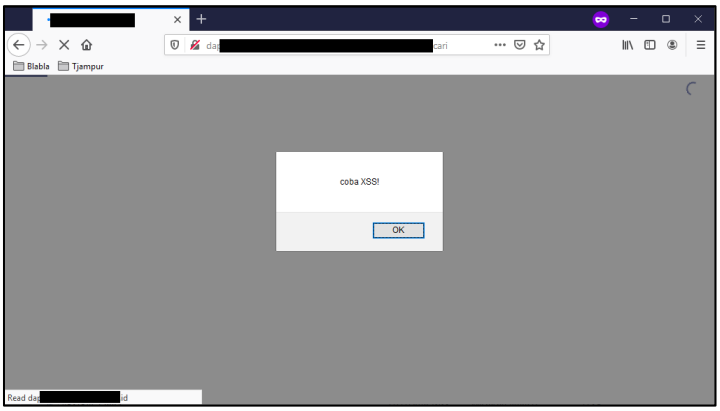

Fig. 4: After submit XSS

Another vulnerability detection found is clear text transmission. Clear text transmission is dangerous if accessed via public network such as café, airport, or others places that result in other parties can eavesdropping through a switch or router. So for first step is access the link that indicate clear text transmission. After that try to fill the form like figure 5 below

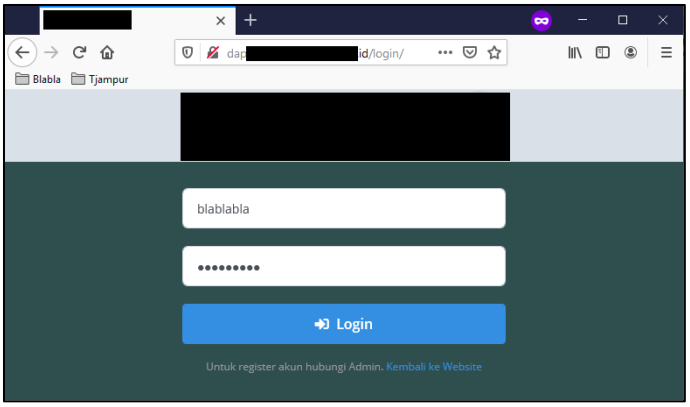

Fig. 5: Login clear text

Before submitting the form, start packet capture with Wireshark and see details in post method

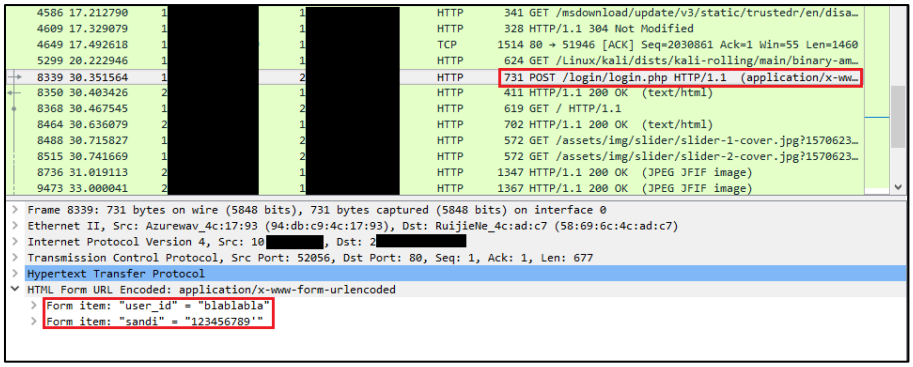

Fig. 6: Packet capture

5. Conclusion

This paper presents a black box testing approach for detection of vulnerabilities in web applications by selecting a set of tools in optimized and organized way. Based on the results of testing and analysis that has been done with the black box approach using a web vulnerability scanner tools shows that the basic data of education's website still has many vulnerabilities. The test results also show that scanning a web application using different tools will increase the probability of finding various types of vulnerability. High level of risks are found in this test, this indicate basic data of education website has high risk to be attacked. One solution for vulnerabilities found on this web application is by adding exception in source code in form section, such as login or search form. While the recommendations that can be done for Clear text transmission of sensitive information via HTTP is to use an SSL / TLS connection so that the communication between the client and the server is encrypted.

6. References

Andress, Jason. 2014. The Basics of Information Security Second Edition. Waltham: Syngress.

APJII. 2017. "Infografis Penetrasi & Perilaku Pengguna Internet Indonesia." APJII. Available at: https://apjii.or.id/survei2017/download/brDi5U0PaVndoR9vfu8msNG1gEAzCQ Accessed Desember 1, 2019.

Awang, Nor Fatimah, and Azizah Abd Manaf. 2013. "Detecting Vulnerabilities in Web Applications Using and Automated Black Box and Manual Penetration Testing." CCIS 381, 230-239.

Doshi, Jignesh, and Bhushan Trivedi. 2015. "Comparison of Vulnerability Assessment and Penetration Testing." International Journal of Applied Information Systems (IJAIS) 8, 51-54.

ISACA. 2017. *Vulnerability Assessment.* Rolling Meadows: ISACA.

Khan, Mohd. Ehmer, and Farmeena Khan. 2012. "A Comparative Study of White Box, Black Box and Grey Box Testing Techniques." International Journal of Advanced Computer Science and Applications (IJACSA), 12-15.

Minister of Education and Culture. 2015. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 79. Jakarta: Minister of Education and Culture.

National Institute of Standards and Technology. 2012. NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments. Gaithersburg: National Institute of Standards and Technology.

Nieles, Michael, Kelley Dempsey, and Victoria Yan Pillitteri. 2017. NIST Special Publication 800-12 Revision 1 - An Introduction to Information Security. Gaithersburg: National Institute of Standards and Technohlogy.

OWASP. 2017. "a" Category:OWASP Top Ten Project. Avalable at: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project. Accessed on December 1, 2019.

—. 2017. "b" "OWASP Top 10 2017." OWASP. Available at: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf. Accessed on December 1, 2019.

OWASP. 2019. Talk: OWASP Vulnerability Management Guide. May 1. Available at: https://www.owasp.org/index.php/Talk:OWASP_Vulnerability_Management_Guide#OWASP_Vulnerability_Management_Guide_v.1. Accessed on December 1, 2019.