

# Security Assessment Using Nessus Tool to Determine Security Gaps on the Repository Web Application in Educational Institutions

Chayadi Oktomy Noto Susanto<sup>1</sup>, Kauka Noor Fathur Rizko<sup>1</sup> and Dwijoko Purbohadi<sup>1\*</sup>

<sup>1</sup>Universitas Muhammadiyah Yogyakarta, Jln.Brawijaya, Tamantirto, Kasihan, Bantul, Yogyakarta 55183, Indonesia

\*Corresponding author: [purbohadi@yahoo.com](mailto:purbohadi@yahoo.com)

## Abstract

*This research aims to determine security holes and risks that may arise in the educational institution's repository web application. The repository web application contains research data, journals, articles, and papers from lecturers and students at the institution. This web application does not yet have documentation about security holes and risks in it. It causes a sense of concern on the part of educational institutions. Therefore, it is necessary to have a security assessment to conduct a risk-oriented assessment that might occur if an attack is attempted. The Vulnerability Assessment and Penetration Testing (VAPT) method was utilized to conduct a security assessment and test educational institutions' repository web application. Several vulnerabilities found with the Nessus tool could still be exploited and resulted in findings in legal access rights when the researchers performed a test simulation on the repository web application. This research was used as a report to the educational institution, particularly as a material for the evaluation process to increase its web application security. This research was carried out within the educational institution environment. Hence, it did not fully describe the possibility of actual attacks originating from outside the educational institution environment.*

**Keywords:** Security Assessment, Vulnerability Assessment and Penetration Testing, and Nessus

## 1. Introduction

Information technology was built to ease humans to manage and disseminate public and confidential information [1]. Information managed and disseminated must have integrity or can be trusted. Therefore, information security is crucial because it can affect the image of the educational institution. Threats to information can come from anywhere. To identify and minimize security threats that can cause risks, it is necessary to measure these risks. A security assessment is a series of activities to assess the security of a web application. The assessment carried out on the security assessment is risk-oriented [2]. This assessment aims to identify security gaps and risks arising from attempted attacks in a web application. The resulting risk can be in the form of taking essential information or attempts to thwart the ongoing information technology process. This activity is deemed necessary to improve the mechanism for protecting confidential information security. The steps taken are in the form of prevention, detection, and response [3].

Observations on the repository web application reveal that the web application has never been made to measure security gaps that can pose a risk or be called a security assessment. It is a particular concern for researchers if an attack occurs because the web contains information about research conducted by lecturers and students. Therefore, it is necessary to have a security assessment on the repository web application. This activity is carried out using the Vulnerability Assessment and Penetration Testing (VAPT) method, which consists of two main activities, Vulnerability Assessment and Penetration Testing aiming to obtain essential information on a web application [4].

Vulnerability Assessment is a search for system security gaps that can lead to failure of the information technology process. Once attackers find the loophole, they determine how to access it. Thus, the threat to the confidentiality of the application increases. Attackers use tools to identify application vulnerabilities [5]. One tool for identifying application vulnerabilities is Nessus, employed to discover security holes in software or web pages. This tool allows attackers to find a way to bypass the security of a software or web page [6]. After finding a security hole, then the Penetration Testing is performed. Penetration Testing is a way to identify security holes in the implementation of a system's security mechanisms. This activity is carried out by attacking a computer system to find security weaknesses, potentially gaining access to its functions and data [7]. These attack simulation results are then documented and presented as a report to the relevant stakeholders. Educational institutions can use this paper as an evaluation material to improve security on their repository web application.

## 2. Method

This security assessment utilized the Vulnerability Assessment and Penetration Testing (VAPT) method in the educational institution repository web application. Vulnerability Assessment scanned the web application to look for security holes that attackers might use to access essential information. Penetration Testing is a simulation of penetration or entry into a system by exploiting security holes [4]. The steps performed in this method are as follows [8]:

1. Scope

This stage determined the scope of the research. Researchers determined the limited coverage of the repository web application of the educational institution. The result achieved was access rights to enter the repository web application.

2. Reconnaissance

Reconnaissance aimed to find basic information such as operating system, IP address, port and web server used on the web application repository. It was carried out using the Nmap Version 7.70 tool on the Kali Linux operating system.

3. Vulnerability Detection

This phase aimed to look for security holes on the repository web application using the Nessus 7.1.2 on the Google Chrome browser application for the Windows operating system.

4. Information Analysis and Planning

This step analyzed the findings of security holes obtained at the vulnerability detection stage and determined methods or techniques of attacks by exploiting these gaps. The findings of security gaps were used to simulate attacks include:

- a. Transmit Cleartext Credential Web Server

This security hole's findings described that session data running on the repository web application were not encrypted. Hence, session data to and from the webserver could be known in plaintext, including username and password. Arspooft version 2.4 and SSLStrip version 0.9 on the Kali Linux operating system were employed to simulate the attacks.

- b. SYN Scanner

The vulnerability findings described the open ports on the repository web application. Researchers used one of the open ports, port 5432, to enter the PostgreSQL port database. Metasploit version 4.17.2-dev was utilized to simulate the attacks.

5. Penetration Testing

Simulated attacks were carried out on the repository web application using predetermined tools to obtain information in accounts used on the web application.

6. Privilege Escalation

It utilized account access rights obtained from the attack simulation step. Access rights were used to explore features on the web application.

7. Report

This security assessment was written in a report and reported to the educational institution.

### 3. Results

A Security Assessment was carried out on the repository web application of educational institutions using the VAPT method. The application's determination was based on previous research discussing the list of critical assets belonging to educational institutions. The repository ranked second with a high vulnerability level because the web application stored essential information, and it was reported to have frequent attempted attacks [9]. After determining the research scope, the next step was to look for security holes on the web application. The finding of a gap entitled Web Server Transmit Cleartext Credential was obtained at the Vulnerability Assessment stage using the Nessus tool. This security gap existed because the web application was not configured to use the HTTPS protocol. The HTTPS protocol encrypted session data using the Secure Socket Layer (SSL) or the Transport Layer Security (TLS) protocols. Both protocols protected from the man in the middle attacks [10]. The protocol used in this web application was the HTTP protocol. It did not encrypt the session data journey. Thus, this web application could still be attacked using the man in the middle attack technique. This activity succeeded in recording an account as an admin on the web application. The results of these activities are described in Figure 1.

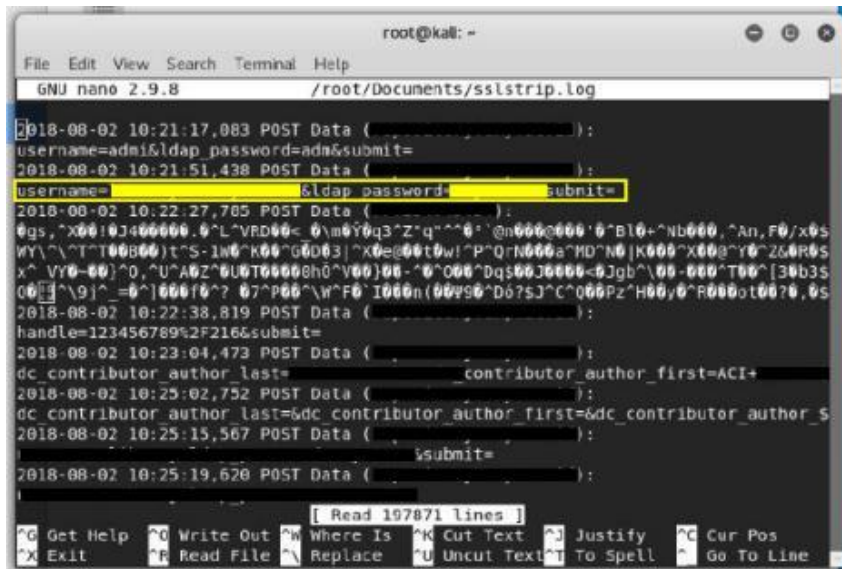
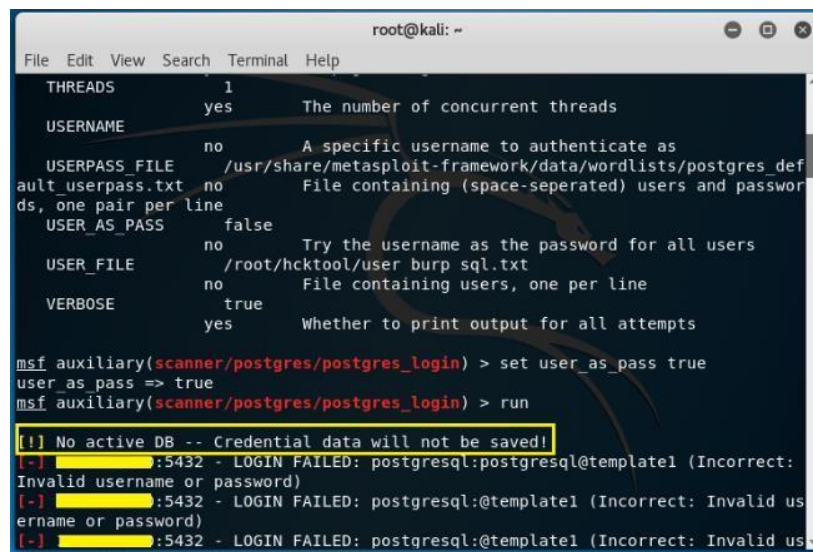


Figure 1. A Successful Penetration Attempt

This attack simulation activity used two tools, arpspoof and SSLStrip. Arpspoof is used to read session data on two hosts simultaneously [11], then the researchers can read the traffic between the two hosts connected to a local area network using the SSLStrip tool.

In the SSLStrip log, it is known that a username and password come from one of the end devices to the gateway on the local area network at the research location. This simulation attack succeeded in obtaining the account used on the repository web application of educational institutions. Researchers verified by logging into the repository web application using the username and password obtained.

The next attack simulation was carried out by exploiting a security hole entitled SYN Scanner. The information obtained from this vulnerability was a port used for PostgreSQL, namely port 5432. This attack simulation utilized the Metasploit tool with brute force attack techniques. Brute Force is an attack technique to find usernames and passwords that run automatically to find the correct username and password combination [12]. These activities are described in Figure 2.



```
root@kali: ~  
File Edit View Search Terminal Help  
THREADS 1 The number of concurrent threads  
USERNAME yes A specific username to authenticate as  
USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/postgres_def  
ault_userpass.txt no File containing (space-separated) users and passwor  
ds, one pair per line  
USER_AS_PASS false Try the username as the password for all users  
USER_FILE /root/hcktool/user_burp_sql.txt no File containing users, one per line  
VERBOSE true Whether to print output for all attempts  
msf auxiliary(scanner/postgres/postgres_login) > set user_as_pass true  
user_as_pass => true  
msf auxiliary(scanner/postgres/postgres_login) > run  
[!] No active DB -- Credential data will not be saved!  
[*] :5432 - LOGIN FAILED: postgresql:postgresql@template1 (Incorrect:  
Invalid username or password)  
[*] :5432 - LOGIN FAILED: postgresql:@template1 (Incorrect: Invalid us  
ername or password)  
[*] :5432 - LOGIN FAILED: postgresql:@template1 (Incorrect: Invalid us
```

**Figure 2. A Failed Penetration Attempt**

During the attack simulation, an error message of *[!] No active DB – Credential data will not be saved!* appears, as shown in Figure 2. This failure occurred because all requests directed to the web server first went through the firewall. The firewall functions to protect data and resources from damage caused by intruders entering a computer network [13]. This simulation attack was failed to enter the database on the repository web application of educational institutions.

Researchers carried out social engineering. Social engineering can be defined as the use of psychological tricks from hackers to obtain the information they need to gain access to the system or obtain the information required (for example, passwords) from someone, not by breaking into the system [14]. It was carried out through interviews focused on getting information on who had access rights to the web application. It was carried out on staff at the research location. The social engineering results revealed that the account obtained was the only admin account used for file management on the web application. This account has been used by more than one staff member at the research location. Accordingly, it can be a problem if a file management error, as it is difficult to find out which staff made a mistake because they use the same account to perform file management.

#### 4. Conclusions

The use of web applications to manage and publish journals and research from lecturers and students is a necessity. Some staff carried out information management in one room, and they used the same account to input data into the web application. However, if there is a data input error, it will be difficult to trace which staff made a mistake. This research report is based on security assessment activities using the Vulnerability Assessment and Penetration Testing (VAPT) method.

#### References

- [1] E. Indrayani, "Pengelolaan Sistem Informasi Berbasis Teknologi Informasi dan Komunikasi (TIK ) [Management of Information Systems Based on Information and Communication Technology]," vol. 12, no. 1, pp. 45–60, 2011.
- [2] A. Abdel-Aziz, "Scoping Security Assessments - A Project Management Approach," Security, 2011.
- [3] D. Dalalana Bertoglio and A. F. Zorzo, "Overview and open issues on penetration test," J. Brazilian Comput. Soc., vol. 23, no. 1, pp. 1–16, 2017.
- [4] J. N. Goel and B. M. Mehtre, "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology," Procedia Comput. Sci., vol. 57, pp. 710–715, 2015.
- [5] P. S. Shinde and S. B. Ardhapurkar, "Cyber Security Analysis Using Vulnerability Assessment and Penetration Testing," IEEE Spons. World Conf. Futur. Trends Res. Innov. Soc. Welf. (Startup Conclave), pp. 1–5, 2016.
- [6] H. Kumar, Learning Nessus for Penetration Testing. 2014.
- [7] I. Mukhopadhyay, S. Goswami, and E. Mandal, "Web Penetration Testing using Nessus and Metasploit Tool," IOSR J. Comput. Eng., vol. 16, no. 3, pp. 126–129, 2014.

- [8] B. C. Hidayanto, "Evaluasi Keamanan Aplikasi Sistem Informasi Menggunakan Framework VAPT (Studi Kasus : SISTER Universitas Jember) [Information System Application Security Evaluation Using VAPT Framework (Case Study: SISTER, University of Jember)]," 2017.
- [9] A. M. A. Yuhaz, "Risk Management Aset Teknologi Informasi Menggunakan Framework OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) dan FMEA (Failure Mode and Effect Analysis) di Institusi Pendidikan [Information Technology Asset Risk Management Using the OCTAVE Framework (Operationally Critical Threat, Asset and Vulnerability Evaluation) and FMEA (Failure Mode and Effect Analysis) in educational institutions]," Universitas Muhammadiyah Yogyakarta, 2018.
- [10] M. Oni, "Analisis Penggunaan Kriptografi dalam Online Banking [Analysis of the Use of Cryptography in Online Banking]," Anal. Pengguna. Kriptografi dalam Online Bank., no. 13508031, pp. 1–8, 2011.
- [11] S. Puangpronpitag and N. Masusai, "An efficient and feasible solution to ARP Spoof problem," 2009 6th Int. Conf. Electr. Eng. Comput. Telecommun. Inf. Technol., vol. 02, pp. 910–913, 2009.
- [12] A. Karawash, S. Ontario, S. Computing, I. Platform, I. C. View, and A. Karawash, "Brute Force Attack," no. November 2015, 2016.
- [13] S. Land and M. Breining, "United States Patent," vol. 1, no. 16, 2002.
- [14] S. Granger, "Social Engineering Fundamentals, Part I: Hacker Tactics | Symantec Connect," Soc. Eng. Fundam., vol. 1527, 2001.