Security Analysis of Learning Management System Using Penetration Testing with ISSAF Framework

Rusydi Umar 1, Imam Riadi 2, Sonny Abriantoro Wicaksono 3,*

* Correspondence Author: e-mail: sonny2008048044@webmail.uad.ac.id

1 Informatics Engineering; Ahmad Dahlan University; Yogyakarta; (0274) 511830; e-mail: rusydi@mti.uad.ac.id
sonny2008048044@webmail.uad.ac.id
2 Information System; Ahmad Dahlan University; Yogyakarta; (0274) 511830; e-mail: imam.riadi@is.uad.ac.id

Abstract

The development of Information Technology must be balanced with security in the system in the face of hacking threats that have an impact on information leakage or service disruptions. Without the security on the system, many hackers will easily take over the system. In an effort to solve security problems, a method that ensures security is needed. In this study using the Penetration Testing method using the ISSAF frameworks. The results of this research are expected to find out the security gaps in the LMS that is currently used.

Keywords: Security, LMS, Pentest, Kali Linux

1. Introduction

In the current era of Globalization, the development of Information Technology is very rapid (Desy Ria & Budiman, 2021). In its development, apart from Information Technology, Communication Technology is also developing very rapidly (Huda, 2020). Where this technology is able to improve performance quickly, efficiently and accurately. Apart from being effective in the world of work, Information Technology is an important part of running the education system. With Information and Communication Technology, it can make it easier for us to learn and get the information we need anywhere and at any time (Asmawi et al., 2019).

The education system is a strategy and method used in the teaching and learning process which aims to direct students to develop their potential (Risdianto, 2019). In the field of education, the role of Information Technology cannot be underestimated, since ancient times people have used technology as a tool in learning, starting from whiteboards, laptops, and LCD projectors. If you pay attention, learning is currently not carried out completely using conventional models or directly, because currently many people are using technology as a medium for delivering material. And Information Technology currently offers new learning methods called Learning Management System (LMS). The presence of LMS brings better hopes in the world of education (Sinnun, 2017). LMS allows material to be delivered to teaching participants via the internet, intranet or other computer network media. This learning system is a new method in the teaching and learning process, so that teaching participants can learn anywhere and at any time without having to sit and listen to the material delivered directly. There are many LMS platforms that can be used, such as LMS, Edmodo, Moodle, and Google Classroom (Sulistyorini & Anistyasari, 2020).

Currently, the Bekasi Muhammadiyah Business Institute has an LMS that can provide services to lecturers and students in the teaching and learning process such as the availability of syllabus, learning materials, assignments, UTS/UAS exam questions, and attendance. Since this system was published, security testing has never been carried out on the LMS system. As an important asset, system security is one of the main...
issues in the current development of information and communication technology (Ardan et al., 2021). Without security, there will be many hackers who can easily take over the system used. This creates openness in accessing personal data for an institution, especially at the Bekasi Muhammadiyah Business Institute. Seeing this condition, a method for analyzing security in the LMS is needed.

In an effort to solve security problems, it is necessary to implement methods that can guarantee data security. In this research, researchers used the Penetration Testing (Pentest) method using the ISSAF Framework (Khan et al., 2023; Utoro et al., 2020). Pentest is the right method to use in analyzing vulnerabilities in the system. Pentest is a security service provider that uses common language with deep coverage (Fauzan & Syukhri, 2021). Pentest is a framework that was built in 2010 by providing a structured and detailed testing guide, and is able to provide a reference for users regarding the quality of the tests carried out. Currently, many studies use Penetration Testing (Pentest) as a standard in information system security testing. Pentest uses attack simulations to determine risks related to security breaches (Anggraeni et al., 2022; Wardhana & Seta, 2021). In this Pentest simulation, a controlled attack is carried out which helps identify vulnerabilities to applications, networks and operating system branches. This penetration test analyzes all potential vulnerabilities in the system, including weak and inappropriate system configurations, gaps in software or hardware, as well as operational weaknesses in the process or technical handling. Pentest is used when the security system conditions find threats from outside (Haeruddin & Kurniadi, 2021; Nabila et al., 2023). In general, the steps for carrying out a Pentest can be seen in Figure 1.

![Pentest Steps](source)

Source: Research's Result (2023)

Figure 1. Pentest Steps

2. Research Method

The Penetration Testing stage is a testing stage in the form of successive attacks on the system. Based on the definition, Penetration Testing is a method for evaluating the security of a system or network (Sahren et al., 2019). Penetration Testing in this research begins with a literature study regarding the tests carried out and conducting interviews with system managers. Next, testing was carried out using the ISSAF Framework. After testing is carried out, it then provides recommendations to improve security in the LMS, using the ISSAF Framework (Sanjaya, Sasmita, & Arsa, 2020).
A. Information Gathering
The Information Gathering stage is a general search and collection stage of information carried out on the target (Eko Prasetyo & Hassanah, 2021). In this case, what is collected is hardware and software in the form of domain information and network information (Burhani & Priyawati, 2024).

B. Network Mapping
After the information has been successfully obtained, then TCP and UDP port scanning is carried out on the system (Silmina et al., 2022).

C. Vulnerability Identification
This stage is the stage of scanning the system on the target to find out security vulnerabilities in it (Silmina et al., 2022). In this research, Vega Vulnerability Tools are used as a scanning process to determine security vulnerabilities on websites.

D. Penetration
The penetration stage is the stage of simulating an attack to gain illegal access to a target with the aim of obtaining gaps in system security (Ashar, 2022; Herman et al., 2023). The types of attacks carried out at this stage are Cross-Site attacks (XSS) and SQL Injection attacks carried out on the target website.

E. Gaining Access and Privilege Escalation
The gaining access and privilege escalation stage is a testing stage by trying to access the target system (Sanjaya, Sasmita, & Made Sri Arsa, 2020). The type of access carried out in this research is access to the admin user system and access to the Cpanel system.

F. Enumerating Further
This stage searches for and solves all information regarding the password obtained from the target (Sanjaya, Sasmita, & Made Sri Arsa, 2020).

G. Compromise Remote User/Sites
The remote user/sites compromise stage is a testing stage by exploiting access to the root user via a remote connection to the system using the local administrator password (Pektas & Basaranoglu, 2017).

H. Maintaining Access
After gaining system access, the system can then be exploited by looking for other common devices that are vulnerable (Yaacoub et al., 2023).

I. Covering Tracks
Covering Tracks is the final stage of penetration testing, this stage of testing involves deleting attack logs that have been carried out in the previous stage (Sanjaya, Sasmita, & Made Sri Arsa, 2020).

3. Results and Analysis
In this chapter, the security testing stages of the ISSAF Framework will be carried out in each phase, then the results that have been tested will be made into reports and recommendations for each stage.

3.1. Information Gathering
In the initial stage to get the IP address of the target, at this stage the tool used is Nikto which is accessed via the Linux operating system. The processes carried out at this stage are SSL, DNS, Domain Info, and CMS.

Pada tahap awal untuk mendapatkan IP Address pada target, tahap ini tools yang digunakan adalah nikto yang diakses melalui sistem operasi Linux. Proses pada tahap ini yang dilakukan adalah SSL, DNS, Info Domain, dan CMS.

3.1.1. Get the Target IP Address
At this stage, scan the IP Address that has been obtained using Nikto tools on the Linux Operating System. The results of scanning can be seen in Figure 2.

3.1.2. Domain Info

After scanning the IP address using Nikto, the next step is to look for domain information. At this stage the tool used is whois. Can be seen in Figure 3.

3.1.3. Security Socket Layer (SSL)

To find out SSL on the lms.ibm.ac.id domain, use Linux in Figure 4.
3.1.4. Domain Name Server

In this test, testing was carried out on the nslookup tool on the Linux operating system, which can be seen in Figure 5.

![Figure 5. Domain Name Server Test](image)

Source: Research's Result (2023)

3.1.5. Identifikasi CMS

This stage is carried out using WhatsApp tools, which can be seen in Figure 6.

![Figure 6. CMS Test](image)

Source: Research’s Result (2023)

3.2. Network Mapping

At this stage, it is carried out by scanning the Website port, the operating system used, and the services used by the Website.

3.2.1. Port Scanning

Scanning is carried out using the nmap tool by typing the nmap command on the Linux operating system, which can be seen in Figure 7.

![Figure 7. Port Scanner Hail](image)

Source: Research’s Result (2023)

3.2.2. Operation System Scanning

The scanner used by the Website is carried out using the nmap-v-A command on Kali Linux. Can be seen in Figure 8.
3.2.3. Service Scanning

At this stage, scanning uses the nmap tool by typing the nmap-sV command in kali linux. Can be seen in Figure 9.

Source: Research’s Result (2023)

Figure 9. Service Scanning Results
3.3 Vulnerability Identification

This stage is carried out using the ZAP tool, which is used to scan the target URL as in Figure 10.

![Automated Scan](image)

Source: Research’s Result (2023)

Figure 10. Results of ZAP Scanning Tools

After completing scanning on the website, flaws were found in the system from the results, which can be seen in Figure 11.

![Cross Site Scripting (Berbasis DQM)](image)

Source: Research’s Result (2023)

Figure 11. ZAP Scanning Results

It can be concluded from the scanning results that defects or vulnerabilities were found in the lms.ibm.ac.id domain. Some of the vulnerabilities that have been successfully obtained are as shown in Table 1.
Table 1. Scanning Results

<table>
<thead>
<tr>
<th>Scanning lms.ibm.ac.id</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross Site Scripting (DOM based)</td>
<td>High</td>
</tr>
<tr>
<td>Vulnerability JS Library</td>
<td>Medium</td>
</tr>
<tr>
<td>X-Frame-Options-Header Not Set</td>
<td>Medium</td>
</tr>
<tr>
<td>Anti-CSRF Token</td>
<td>Low</td>
</tr>
<tr>
<td>Cookie No HttpOnly Flag</td>
<td>Low</td>
</tr>
<tr>
<td>Cookie without SameSite Attribute</td>
<td>Low</td>
</tr>
<tr>
<td>Cross-Domain JS Source File Inclusion</td>
<td>Low</td>
</tr>
<tr>
<td>Incomplete or No Cache-Control Header Set</td>
<td>Low</td>
</tr>
<tr>
<td>X-Content-TypeOptions Missing</td>
<td>Low</td>
</tr>
<tr>
<td>Information Disclosure in UR - Sensitive</td>
<td>Informational</td>
</tr>
<tr>
<td>Information Disclosure in UR - Suspicious</td>
<td>Informational</td>
</tr>
<tr>
<td>Timestamp Disclosure - Unix</td>
<td>Informational</td>
</tr>
</tbody>
</table>

Source: Research's Result (2023)

4. Conclusion

The penetration testing method is a comprehensive system security test to test a complete computing base. The ISSAF framework is a penetration testing methodology designed to evaluate networks, systems and application controls. Penetration testing on IBM Bekasi's lms.ibm.ac.id using the ISSAF Framework was carried out through nine stages. From the research conducted in the absence of anti-clickjacking X-Frame Option, clickjacking is an attack technique so that targets can click in certain areas that are profitable for hackers.

Acknowledgements

I would like to thank the supervisors who have helped in preparing this article, and to IBM Bekasi for providing the opportunity to analyze the system. And to the PIKSEL journal team for taking the time to process this article review.

Author's Contribution

Rusydi Umar proposed the research. Rusydi Umar, Imam Riadi, and Sonny Abriantoro Wicaksono testing and analyzing the LMS.

Conflicts of Interest

The authors declare no conflict of interest.

References


https://doi.org/10.32722/multinetics.v6i2.3446


