Forensic Investigation of SEO Manipulation in Moodle LMS: Uncovering Illegal Content in Educational Platforms

T Rochmadi[*1], V P Widartha[2], T A Sarmento[3], A A Harahap[4], I Ajis[5]

[1,4,5]Information System, Universitas Alma Ata, Indonesia

[2]Department of Information System, Pulyong National University, South Korea

[3]Informatics Engineering, Institute of Business, East Timor

E-mail: trirochmadi@almaata.ac.id[1], vandhapw@pukyong.ac.kr[2], tito.sarmentu@iob.edu.tl[3], avrillaila@almaata.ac.id[4], 223100292@almaata.ac.id[5]

Abstract. Learning Management Systems (LMS) like Moodle are frequently targeted by covert cyberattacks that exploit the credibility of academic domains for illicit purposes. This study uncovers an SEO-based attack method that infiltrates hidden links to gambling sites through Moodle's public directory. Digital forensic methodology was used to trace the perpetrators' footprints from server logs, HTML/JS files, and activity in Google Search Console. The results revealed a comprehensive exploit: fake admin accounts, redirect file injection, and Google indexing manipulation. This research not only highlights an under-researched threat but also offers a mitigation framework based on the ISO/IEC 27001 standard. Key contributions include identifying SEO-based attack techniques in LMSs, analyzing digital artifacts for perpetrator attribution, and strengthening cybersecurity governance in educational institutions.

Keywords: Moodle; Black-hat SEO; Cyberattacks LMS; Digital Forensic.

1. Introduction

In the era of digitalization of higher education, which is indicated by rapid progress in internet access [1], the use of Learning Management System (LMS) platforms has become a key element in the delivery of teaching materials, academic communication, and learning process management [2] to increase efficiency and service in flexible internet use [3], [4]. Among the various available platforms, Moodle holds a strategic position as an open-source LMS widely adopted [5] by educational institutions due to its flexibility and extensive developer community. However, high dependence on LMSs poses serious implications for cybersecurity [6] in educational environments [7].

Cyber threats to educational institutions are becoming increasingly prevalent [8]. Various reports indicate that the education sector is now the target of increasingly complex attacks, ranging from data theft to the infiltration of illegal content, one of which was reported by Id-SIRTII/CC – BSSN, 2024 [9]. One form of attack that has not been widely discussed in academic literature is the misuse of LMS as a medium to spread hidden links to online gambling sites through Search Engine Optimization (SEO) manipulation techniques [10]. In this context, cybercriminals infiltrate malicious files into the Moodle directory, then use black-hat SEO techniques to redirect traffic from search engines to illegal sites, leveraging the high academic domain reputation.

The case study in this research reveals that the attack was carried out systematically, starting with the creation of fake accounts with administrator rights, the insertion of HTML and JavaScript files into the LMS directory, and the manipulation of Google indexing through the Google Search Console feature. This attack not only tarnishes the digital integrity of the institution but also demonstrates the exploitation of public trust in educational domains as a means of legitimizing illegal content. Unfortunately, there is still a gap in research specifically examining the integration of digital forensics, SEO manipulation, and LMS systems in the context of higher education. Most forensic studies focus on major incidents such as data breaches, ransomware, or email-based fraud. In contrast, the exploitation of LMS for hidden purposes such as increasing gambling site traffic remains minimally explored academically.

To address this gap, this study aims to conduct a digital forensic investigation into SEO-based cyberattacks on the Moodle platform. The main focus of this research includes identifying attack techniques and paths, analyzing time-series digital activity, and attributing perpetrators based on digital artifacts, such as server logs, file metadata, and data from Google Webmaster Tools. The main contribution of this study is to strengthen the understanding of covert LMS exploitation techniques and mitigation measures that other educational institutions can apply.

2. Related Work

2.1. Cybersecurity Threats in Moodle-Based LMS

Moodle, as an open-source LMS platform, is widely used across higher education institutions due to its flexibility and customizable architecture. However, this openness also poses security vulnerabilities. Research by Akacha & Awad, 2023 [11], Dandotiya et al., 2023 [12] identified various common risks in Moodle, such as SQL injection, cross-site scripting (XSS), and privilege escalation. Rochmadi et al., 2024 [13] confirmed that in Indonesian university environments, vulnerabilities often arise from improper access control configurations or outdated system components [14].

However, most studies focus on direct violations such as data theft or DoS (Denial of Service) attacks. Few studies have highlighted the stealthy use of LMS as a means of spreading illegal links through SEO manipulation techniques. This creates a research gap in the LMS security forensics literature that has not been widely explored.

2.2. Black-Hat SEO Techniques in Cybersecurity Attacks

Black-hat SEO is a manipulative technique used to illegally boost a website's ranking in search engines [15]. These practices include keyword stuffing, cloaking, doorway pages, and backlink exploitation [16]. A study by Tazi et al., 2023 [17] shows that cybercriminals are now exploiting high-reputation domains, including educational sites that organizations consider to be of little security concern [13]. This poses a threat to data privacy [18] or, in the case of this research, could be used to insert hidden pages with links to illegal gambling or drug sites.

However, security analysis approaches generally still focus on detecting malware or phishing, rather than detecting SEO anomalies as latent threats. This means that harmful SEO techniques have not been fully mapped as part of a comprehensive digital forensics model.

2.3. The Role of Google Webmaster Tools and Log Analysis in Digital Forensics

Google Search Console (formerly Google Webmaster Tools) offers comprehensive features that provide important insights into crawl behavior analysis, page indexing, and traffic anomalies [19]. Azahari & Balzarotti, 2024 [20] shows that a combination of server logs and webmaster data can be used to reconstruct the trail of SEO attacks and attribute perpetrators. However, most studies still discuss this tool technically, not as part of an integrated forensic methodology. In other words, the potential of Google Search Console in supporting the digital forensics investigation process, especially in the context of SEO abuse, is still underutilized in formal academic literature.

A report from Id-SIRTII/CC – BSSN, 2024 [9] notes that university websites in Indonesia are targets of cyberattacks. HTML files that appear legitimate are often uploaded unknowingly by website

administrators, containing links to illegal content or defacing the website. However, most documentation of these cases is in the form of guidelines or technical reports, not indexed scientific publications. Filling this gap is important, as the integration of LMS vulnerabilities, black-hat SEO, and forensic analysis addresses an underexplored intersection that is increasingly exploited in higher education cybercrime.

3. Research Method

This study uses a digital forensic case study approach to investigate cyberattacks on the Moodle Learning Management System (LMS) at a higher education institution. The main objective of this approach is to identify the methods of attack, the digital traces of the perpetrators, and to understand how SEO manipulation was used to infiltrate online gambling content into the academic system.

A qualitative digital forensics approach was selected because the investigation required contextual interpretation of digital artifacts, such as server logs, script patterns, and SEO anomalies, to reconstruct the sequence and intent of the attack tasks that quantitative metrics alone cannot adequately address. The overall investigation process in this study follows a digital forensic workflow, as illustrated in Figure 1, which outlines the stages from data collection to reporting and recommendation mitigation.

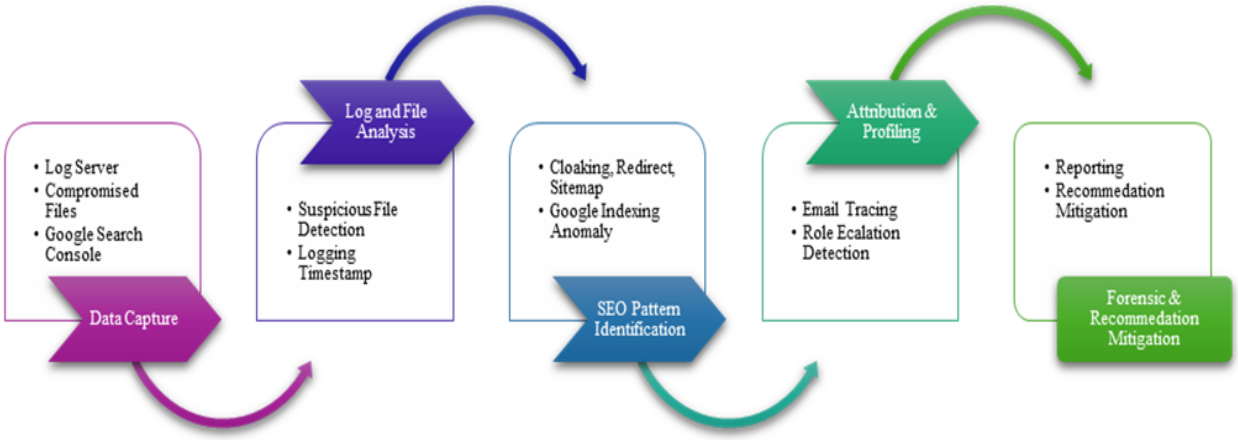

Figure 1. Stages of Digital Forensic Research Approach

The research object is a higher education institution whose identity has been concealed to maintain confidentiality and information security. The LMS platform used is Moodle version 3.6, which is self-hosted on the institution's server. The incident analyzed occurred over a short period from May 26 to June 7, 2025, and included a series of file infiltration activities, traffic redirection, and administrator account deletion.

Data was collected from various digital sources as follows:

- Moodle Server Logs: including user access, file upload activities, and access rights changes.
- Infected Files: HTML/JS files found in the Moodle directory and analyzed manually.
- Google Search Console: used to trace traffic anomalies, inbound links, and keywords leading to the site.

The analysis process was carried out through the following stages:

1. Server Log Forensic Analysis
2. Analysis of the Content and Structure of Compromised Files
3. Google Webmaster Console Analysis
4. Attribution of the Perpetrator

This methodology directly addresses the study's objectives by tracing the entire attack lifecycle, including identifying specific attack techniques used by attackers, and linking these findings to actionable mitigation strategies aligned with ISO/IEC 27001 best practices.

4. Results

4.1. Compromised Files

The analysis results showed that the modified file in index.html contained scripts that led to online gambling, Figure 2, and several scripts commonly used for SEO purposes, Figure 3. The need to accelerate SEO fetch sitemap.xml, Figure 4.

```
$brand = strtolower($BRAND);
$baseAuthor = $BRAND;
$URL  = "https://ampyuksini.online/?pages=$BRAND";
$PAGEURL = "https://ampyuksini.online/?pages=$BRAND";
$AMP = "https://ampyuksini.online/?pages=$BRAND";
$DAFTAR = "https://mplay.shop//";
$BANNER =
"https://i.pinimg.com/736x/a9/56/67/a95667acadcc3d13df66389c030cd634.jpg";
$LOGO =
"https://i.pinimg.com/736x/35/7d/0d/357d0d0335d3521d483352d49d22da
```

Figure 2. Script Embedded in index File

```
$tunnel = "pages";
$filename = "melati.txt";

if (isset($_GET[$tunnel])) {
    $lines = file($filename, FILE_IGNORE_NEW_LINES | FILE_SKIP_EMPTY_LINES);
    $target_string = strtolower($_GET[$tunnel]);

    foreach ($lines as $value=>$item) {
      if (strtolower($item) === $target_string) {
          $BRAND = strtoupper($target_string);
          $NUMLIST = $value+1;
```

Figure 3. Script that Calls melati.txt

```
<?xml version="1.0" encoding="UTF-8"?>
<urlset xmlns="http://www.sitemaps.org/schemas/sitemap/0.9">
  <url>
    <loc>https://elearning.[redacted]id/?pages=Logo303</loc>
    <lastmod>2025-05-28</lastmod>
    <changefreq>daily</changefreq>
    <priority>0.8</priority>
  </url>
  <url>
    <loc>https://elearning.[redacted]ac.id/?pages=Bendera88</loc>
    <lastmod>2025-05-28</lastmod>
    <changefreq>daily</changefreq>
    <priority>0.8</priority>
  </url>
  <url>
    <loc>https://elearning.[redacted]id/?pages=Intan4D</loc>
    <lastmod>2025-05-28</lastmod>
    <changefreq>daily</changefreq>
    <priority>0.8</priority>
  </url>
  <url>
    <loc>https://elearning.[redacted]ac.id/?pages=Casper88</loc>
    <lastmod>2025-05-28</lastmod>
    <changefreq>daily</changefreq>
    <priority>0.8</priority>
  </url>
  <url>
```

Figure 4. Script in sitemap.xml Modified with Online Gambling Terms

Figure 2 shows a script redirecting to an online gambling website with the addresses listed in $URL and $REGISTER. The script also manipulates slugs to increase Google's indexing and retrieves the same $BRAND variable from the melati.txt file in Figure 3. The melati.txt file contains hundreds of terms that serve as additional keywords related to online gambling to avoid tracking or disguising terms.

Figure 4 shows a script in the sitemap.xml page used to facilitate Google's crawling and indexing in search engines. The sitemap has been modified by adding the slug /?pages= to facilitate index fetching in Google Search Console. This fetch feature in Google Search Console speeds up indexing in Google search engines. Therefore, if the script in Figure 1, including $AMP, is linked to the online gambling website, clicks on the index in Google, even though the Moodle LMS has been repaired.

4.2. Google Search Console Verification

Through forensic access to Google Search Console, it was observed that the attacker had successfully claimed ownership of the institution's LMS subdirectory by injecting a verification meta tag, Figure 5. This allowed the attacker to manipulate indexing behavior and monitor traffic. Figure 6 illustrates that the attacker's account has administrative privileges over the Search Console configuration. The visualization of the indexing activity timeline (Figure 7) shows a sharp increase in search engine activity immediately after the injection of the suspicious file.

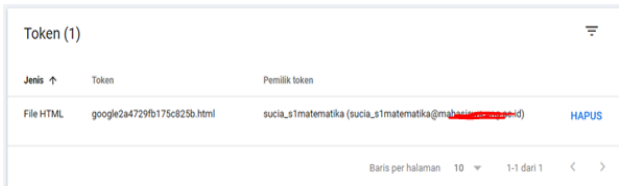

Figure 5. Ownership Change in Search Console

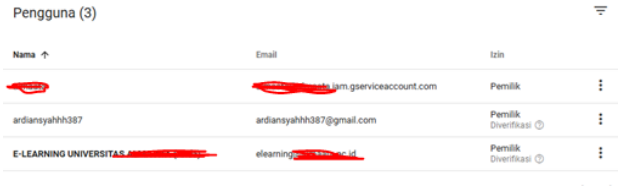

Figure 6. Attacker Successfully Becomes Admin

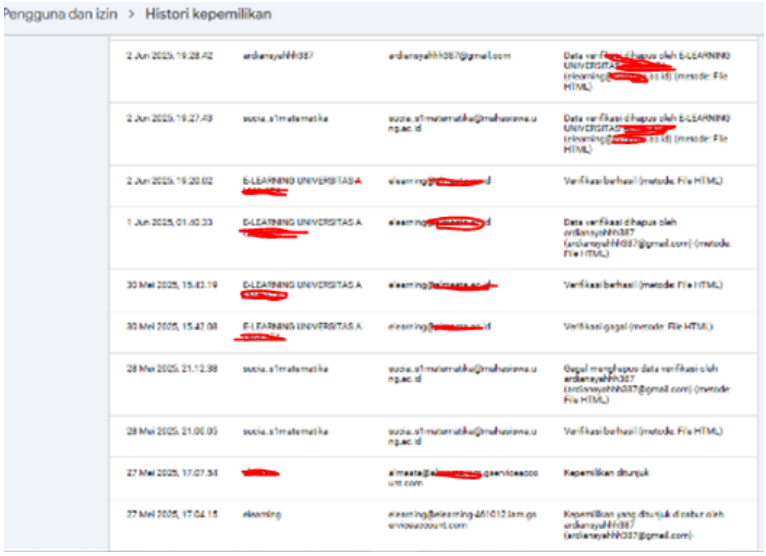

Figure 7. Attacker History on Web Master Google (Google Search Console)

Table 1 summarizes the chronology of the main attack activities, from the creation of a fake admin account to search engine manipulation and the deletion of the administrator account.

Table 1. Chronology of the Attack on LMS

Date	Activity	Description
May 26, 2025	Creation of fake admin account	An account with an email address similar to the institution's domain was created with administrator access rights.
May 27, 2025	Insertion of index.html file	An HTML file containing a redirect script to a gambling site was inserted into the LMS public directory.
May 29, 2025	Access to Google Search Console	The perpetrator verifies site ownership via HTML meta-tags
May 30, 2025	Addition of manipulative sitemap	A sitemap is inserted to accelerate the indexing of illegal pages.
June 2, 2025	Traffic spikes sharply	A surge in traffic from gambling-related keywords (active SEO)
June 7, 2025	Original admin account deleted	Legitimate administrator access removed from the system.

Table 1 presents the chronology of the attack, revealing a deliberate escalation strategy by the perpetrator. The sequence begins with the creation of a fake administrator account (May 26, 2025), which immediately grants privileged access to the LMS environment. This foothold is followed by the insertion of a malicious index.html file (May 27, 2025) designed to redirect users to gambling sites an early indication of the economic motive. The subsequent verification of site ownership in Google Search Console (May 29, 2025) marks a critical turning point, enabling the attacker to manipulate indexing behavior and monitor traffic at scale. By May 30, 2025, the addition of a custom sitemap accelerated the visibility of illicit pages in search results. The sharp traffic surge on June 2, 2025, indicates the successful activation of the black-hat SEO campaign, which continued until the final disruptive act: deleting the legitimate administrator account (June 7, 2025), effectively locking out institutional control. This timeline demonstrates not only the technical capabilities of the attacker but also the exploitation of LMS vulnerabilities in a carefully staged manner to maximize persistence and impact.

4.3. Manipulated Search Results

The results of black-hat SEO manipulation are visible in Figure 8, where Google search results begin to display gambling-related keywords and links under the university domain. This shows that the attack successfully exploited the institution's high domain authority to boost the ranking of illegal content, thereby abusing the reputation of the educational domain for illicit economic gain.

Figure 8. Moodle LMS Sample Hit by Black-hat SEO Attack

Table 2 presents a comparative view of Google indexing metrics before and after the incident, highlighting the impact of black-hat SEO on the institution's domain.

Table 2. Comparative View of Google indexing

Parameter	Before	After	Change (%)
Indexed Pages	152	236	+55.26%
Backlinks	37 domain	89 domain	+140.54%
Gambling-Related Keywords	0	23	N/A
URLs with Active Redirects	0	17	N/A
LMS Traffic Bounce Rate	42%	89%	+111.90%

Table 2 quantifies the operational success of the attack by comparing Google indexing metrics before and after the incident. Indexed pages rose 55.26%, reflecting the injection and rapid indexing of illicit content. Backlinks increased dramatically 140.54%, signaling the attacker's use of automated link-building or affiliate networks to strengthen search rankings. The sudden appearance of gambling-related keywords and URLs with active redirects both previously nonexistent confirms the precision of the SEO manipulation in targeting specific search traffic. The bounce rate's jump from 111.90% further suggests that the majority of visits originated from irrelevant or deceptive search results, a hallmark of cloaking and keyword stuffing strategies. Collectively, these metrics illustrate not only the efficiency of the black-hat SEO techniques but also their measurable disruption to the LMS's normal operational profile.

5. Discussion

5.1 Interpretation of Results: Economic Motives and LMS Vulnerability

The main motive behind these attacks is economic, to generate traffic and user clicks to online gambling platforms, which typically operate on an affiliate marketing model with high commissions. The use of Moodle, an open-source LMS that is often poorly protected, provides fertile ground for exploitation. Many institutions fail to implement strict access controls, file integrity monitoring, or directory indexing prevention, leaving web-accessible directories vulnerable to file injection.

5.2 SEO Exploitation in the Context of Educational Institutions

This case illustrates how attackers exploit public trust associated with .ac.id or .edu domains to gain an SEO advantage. Educational websites often have high domain authority and credibility in the eyes of search engines. When these domains are manipulated to present hidden links to gambling sites, search engines give them high rankings, misleading users and damaging the integrity of the institution. The attacker's methods, including hiding, keyword stuffing, and automatic sitemap submission, are classic examples of black hat SEO techniques adapted to abuse institutional trust.

5.3 Implications for Digital Security in the Education Sector

This case highlights the urgent need for proactive cybersecurity strategies in educational institutions. LMS platforms are no longer passive tools for learning, but have become potential entry points for broader cyber threats. The findings indicate that many institutions may remain unaware of such SEO-based attacks due to the covert nature of the methods used. Routine SEO audits, log analysis, and web integrity monitoring should be integrated into the digital governance framework.

5.4 Recommendations

To strengthen digital resilience in educational institutions, several proactive measures should be considered based on the findings of this study. First, it is important to conduct regular audits of publicly accessible directories in LMS such as /mod/resource/ and /course/ to detect unauthorized file injections. Automated scanning tools can be used to identify suspicious file types, such as standalone .html or .js files, which are typically not part of standard Moodle content.

Second, institutions should integrate SEO audit mechanisms into their cybersecurity protocols. This includes routine analysis of sitemap submissions, backlink profiles, and indexed pages using tools like Google Search Console, Ahrefs, or other SEO monitoring platforms. By proactively monitoring SEO anomalies, institutions can identify harmful indexing behavior before it escalates.

Third, tightening access controls and privilege management is essential. All administrative accounts should be secured with multi-factor authentication (MFA), and the principle of least privilege should be enforced to minimize lateral movement in the event of an account breach.

Finally, institutions should consider aligning their cybersecurity practices with international standards such as ISO/IEC 27001, with a focus on controls such as A.12.4.1 for event logging and monitoring, A.9.2.3 for managing privileged access, and A.14.2.1 for secure system engineering. Embedding these

standards into the LMS governance structure will help ensure consistent risk management and system integrity over time.

6. Conclusion

This study has shown that Learning Management Systems (LMS), particularly Moodle, can be exploited as an entry point for sophisticated cyber attacks involving SEO manipulation and the promotion of illicit content. Through digital forensic case studies, it was discovered that attackers infiltrated the LMS by injecting HTML and JavaScript files into public directories, which redirected search engine traffic to online gambling websites. The misuse of Google Search Console to verify ownership and manipulate site indexing further highlights the diverse nature of the threat.

The incidents analyzed in this study reveal a shift in attackers' tactics from open data breaches to covert SEO exploitation, leveraging the institutional credibility of educational domains for economic gain. The results confirm that Moodle's default configuration, if not hardened, presents exploitable vulnerabilities that can jeopardize not only system integrity but also institutional reputation.

The study's main contributions are threefold. First, it highlights a new vector of LMS abuse SEO-based manipulation that is largely underrepresented in the literature. Second, it demonstrates the forensic value of combining internal server logs with external SEO data to reconstruct cyber events. Third, it proposes a security awareness model emphasizing SEO audits as a component of digital governance in education.

To mitigate these risks, institutions should implement proactive defense mechanisms, including routine log audits, file upload permission restrictions, integration of web integrity monitoring tools, and SEO anomaly detection systems. Furthermore, compliance with cybersecurity frameworks such as ISO/IEC 27001 should be prioritized to formalize risk management practices and ensure the resilience of educational digital infrastructure.

Future research could expand this investigation by applying machine learning techniques to detect unusual SEO behavior across various LMS platforms. Longitudinal studies involving multiple institutions could also offer a broader perspective on how these threats evolve and how defense patterns can be standardized across the education sector.

7. References

[1] S. A. Nugroho and T. Rochmadi, "Analisis Keamanan Sistem Informasi Pusaka Magelang Menggunakan Open Web Application Security Project (OWASP) dan Information Systems Security Assessment Framework (ISSAF)," *CyberSecurity dan Forensik Digital*, vol. 7, no. 1, pp. 56–61, Aug. 2024, doi: 10.14421/csecurity.2024.7.1.4555.

[2] G. Slavko and S. Serhiienko, "Optimization of LMS Moodle configuration and Education Technologies on the Example of Electrical Engineering Education," in *2021 IEEE International Conference on Modern Electrical and Energy Systems (MEES)*, 2021, pp. 1–5. doi: 10.1109/MEES52427.2021.9598719.

[3] S. Nugroho and T. Rochmadi, "Analysis of Information Security Readiness Using the Index KAMI," *DECODE: Jurnal Pendidikan Teknologi Informasi*, vol. 4, no. 3, pp. 881–886, Nov. 2024, doi: 10.51454/decode.v4i3.602.

[4] A. G. P. Sidhawara, "An Evaluation of UAJY Learning Management System's Usability using USE Questionnaire and Eye-tracking," *Indonesian Journal of Information Systems (IJIS*, vol. 4, no. 2, pp. 174–188, Feb. 2022, doi: 10.24002/ijis.v4i2.5273.

[5] X. Tan, J. She, S. Chen, S. Ohno, and H. Kameda, "Analysis of Student Learning Behavior Based on Moodle Log Data," in *2021 14th International Conference on Human System Interaction (HSI)*, Gdańsk: IEEE, Sep. 2021, pp. 1–4. doi: 10.1109/HSI52170.2021.9538680.

[6] Đ. Milošević, K. Kuk, B. Popović, and P. Čisar, "Endangered data in Moodle platform with malicious plugins," in *2022 21st International Symposium INFOTEH-JAHORINA (INFOTEH)*, East Sarajevo: IEEE, Apr. 2022, pp. 1–5. doi: 10.1109/INFOTEH53737.2022.9751251.

[7] H. S. Lallie, A. Thompson, E. Titis, and P. Stephens, "Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector," *Computers*, vol. 14, no. 2, 2025, doi: 10.3390/computers14020049.

[8] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Working from Home During Covid-19 Crisis: a Cyber Security Culture Assessment Survey," *Security Journal*, vol. 35, no. 2, pp. 486–505, Feb. 2022, doi: 10.1057/s41284-021-00286-2.

[9] Id-SIRTII/CC – BSSN, "Lanskap Keamanan Siber Indonesia," 2024. Accessed: Oct. 01, 2024. [Online]. Available: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf

[10] S. B. Trivedi, *Chapter–19 Information Technology in Accounting Dr. Sunil B. Trivedi*. Crown Publishing, 2025.

[11] S. A.-L. Akacha and A. I. Awad, "Enhancing Security and Sustainability of e-Learning Software Systems: A Comprehensive Vulnerability Analysis and Recommendations for Stakeholders," *Sustainability*, vol. 15, no. 19, 2023, doi: 10.3390/su151914132.

[12] M. Dandotiya, P. Rahi, A. Khunteta, A. Anushya, and S. S. Ahmad, "SAFE: A Secure Authenticated & Integrated Framework for E-learning," in *Proceedings of the 4th International Conference on Information Management & Machine Intelligence*, in ICIMMI '22. New York, NY, USA: Association for Computing Machinery, 2023. doi: 10.1145/3590837.3590926.

[13] T. Rochmadi, A. Fadlil, and I. Riadi, "Tinjauan Pustaka Sistematis: Tantangan dan Faktor-Faktor Pengembangan Kesiapan Forensik Digital," *CyberSecurity dan Forensik Digital*, vol. 7, no. 2, pp. 81–89, Dec. 2024, doi: 10.14421/csecurity.2024.7.2.4861.

[14] T. M. Tran, R. Beuran, and S. Hasegawa, "Gamification-Based Cybersecurity Awareness Course for Self-Regulated Learning," *International Journal of Information and Education Technology*, vol. 13, no. 4, pp. 724–730, 2023, doi: 10.18178/ijiet.2023.13.4.1859.

[15] M. Shimamura, S. Matsugaya, K. Sakai, K. Takeshige, and M. Hashimoto, "An Analysis of the Relationship Between Black-Hat SEO Malware Families Leveraging Information from Redirected Fake E-Commerce Scam Sites," in *2024 IEEE Conference on Dependable and Secure Computing (DSC)*, Tokyo: IEEE, Nov. 2024, pp. 123–130. doi: 10.1109/DSC63325.2024.00025.

[16] K. Sellamuthu, S. Ranjithkumar, K. Kavitha, and S. Gowtham, "On Page SEO Techniques for Better Ranking in Search Engines," in *2022 8th International Conference on Smart Structures and Systems (ICSSS)*, Chennai: IEEE, Jun. 2022, pp. 1–6. doi: 10.1109/ICSSS54381.2022.9782182.

[17] F. Tazi, S. Shrestha, and S. Das, "Cybersecurity, Safety, & Privacy Concerns of Student Support Structure for Information and Communication Technologies in Online Education," *Proc. ACM Hum.-Comput. Interact.*, vol. 7, no. CSCW2, Oct. 2023, doi: 10.1145/3610055.

[18] T. Rochmadi and I. Y. Pasa, "Pengukuran Risiko dan Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi di BKD XYZ Berdasarkan ISO 27001 / SNI," *CyberSecurity dan Forensik Digital*, vol. 4, no. 1, pp. 38–43, May 2021, doi: 10.14421/csecurity.2021.4.1.2439.

[19] K. Arlitsch, J. Wheeler, M. T. N. Pham, and N. N. Parulian, "An Analysis of Use and Performance Data Aggregated from 35 Institutional Repositories," *Online Information Review*, vol. 45, no. 2, pp. 316–335, Mar. 2021, doi: 10.1108/OIR-08-2020-0328.

[20] A. Azahari and D. Balzarotti, "On the Inadequacy of Open-Source Application Logs for Digital Forensics," *Forensic Science International: Digital Investigation*, vol. 49, p. 301750, Jun. 2024, doi: 10.1016/j.fsidi.2024.301750.