Maliki Interdisciplinary Journal (MIJ)
Volume 2, Issue 11, 2024 pp. 1545-1562
eISSN: 3024-8140
http://urj.uin-malang.ac.id/index.php/mij/index

Analisis keamanan *Learning Management System* (LMS) *Moodle* dengan metode *vulnerability scanning*

Diah Ayu Rahma[1]*, Fina Maslahatul Firhah[2], Muhammad Ainul Yaqin[3]
[1,2,3]Program Studi Teknik Informatika, Universitas Islam Negeri Maulana Malik Ibrahim Malang
*e-mail: *220605110006@student.uin-malang.ac.id*

Kata Kunci:
learning management system;
vulnerability scanning;
kerentanan keamanan

Keywords:
learning management system;
vulnerability scanning;
security vulnerabilities

A B S T R A K

Learning Management System (LMS) merupakan platform e-learning yang sangat penting dalam mengelolapembelajaran online. Salah satu LMS yang populer digunakan saat ini adalah Moodle, yang bersifat open source dan memiliki beragam fitur yang dapat disesuaikan dengan kebutuhan pengguna. Keamanan menjadi aspek krusial dalam LMS karena platform ini menyimpan data sensitif seperti informasi pengguna dan materi pembelajaran. Penelitian ini bertujuan untuk melakukan analisis keamanan pada Moodle, dengan menggunakan metode Vulnerability Scanning menggunakan tools OWASP-ZAP. Hasil analisis mencakup identifikasi kerentanan keamanan, tingkat keparahan kerentanan, dan perbandingan dengan LMS Moodle versi lain. Rekomendasi untuk meningkatkan keamanan Moodle juga akan disampaikan. Penelitian ini ditujukan untuk administrator Moodle, praktisi keamanan, dan peneliti di bidang keamanan informasi. Diharapkan hasil penelitian ini dapat meningkatkan kesadaran akan pentingnya keamanan dalam LMS, memberikan panduan untuk melakukan vulnerability scanning pada Moodle, serta membantu administrator dalam mengidentifikasi dan mengatasi potensi kerentanan keamanan pada platform Moodle.

A B S T R A C T

The Learning Management System (LMS) is a crucial e-learning platform for managing online education. One popular LMS used today is Moodle, which is open source and oflers various customizable features to meet users' needs. Security is a critical aspect of LMS because it stores sensitive data such as user information and learning materials. This research aims to analyze the security of Moodle using the Vulnerability Scanning method with OWASP-ZAP tools. The analysis include identifying security vulnerabilities, assessing their severity, and comparing them with other versions of the Moodle LMS. Recommendations for enhancing Moodle's security will also be provided. This research targets Moodle administrators, security practitioners, and researchers in the field of information security. The expected outcomes of this research are to raise awareness of the importance of security in LMS, provide guidance forconducting vulnerability scanning on Moodle, and assist administrators in identifying and addressing potential security vulnerabilities in the Moodle platform.

Pendahuluan

Learning Management System merupakan platform e-learning yang digunakan untuk mengelola pembelajaran online. LMS menyediakan berbagai fitur yang dapat mendukung proses pembelajaran. Ada banyak sekali jenis LMS,salah satunya adalah Moodle. Moodle merupakan LMS yang populer digunakansaat ini. Moodle bersifat *open source* dan memiliki banyak fitur yang dapat disesuaikan dengan kebutuhan (Pratama &

Cahyaningsih, 2021).

Keamanan merupakan aspek yang penting dalam LMS, sebab platform LMS menyimpan berbagai data sensitif seperti informasi pengguna dan materi pembelajaran. Melakukan analisis keamanan pada LMS merupakan hal yang diperlukan, dengan melakukan analisis maka dapat diketahui potensi kerentanan keamanan dalam sistem LMS tersebut (Pargaonkar, 2023).

Vulnerability scanning merupakan metode yang akan digunakan untuk mengidentifikasi kerentanan keamanan sistem LMS Moodle versi terbaru menggunakan tools OWASP-ZAP. Hasil analisis menggunakan vulnerability scanning akan dipaparkan, termasuk jenis kerentanan yang ditemukan dan tingkat keparahannya. Kemudian berdasarkan hasil analisis, akan dilakukan perbandingan dengan LMS Moodle versi lain dan memberikan rekomendasi untuk peningkatan keamanan Moodle (Aslan et al., 2023).

Penelitian ini ditujukan untuk administrator Moodle, praktisi keamanan, dan peneliti di bidang keamanan informasi. Dengan hasil penelitian ini diharapkan dapat meningkatkan kesadaran tentang pentingnya keamanan dalam LMS, memberikan panduan untuk melakukan vulnerability scanning pada Moodle, dan membantu administrator untuk mengidentifikasi dan mengatasi potensi kerentanan keamanan pada Moodle.

Beberapa penelitian mengenai Moodle hanya berfokus pada versi tertentu, sehingga belum ada gambaran menyeluruh tentang keamananMoodle di berbagai versi. Kemudian penelitian yang kurang membandingkan keamanan Moodle dengan LMS jenis lain membuat sulit untuk menentukan di posisi mana Moodle dalam bidang keamanan secara keseluruhan.

Penelitian yang sudah ada umumnya hanya berfokus pada kerentanan yang muncul ketika penelitian dilakukan saja tanpa melakukan identifikasi. Diperlukan penelitian lain yang berkelanjutan untuk mengidentifikasi dan menganalisis kerentanan baru yang muncul seiring waktu. Hal seperti ini diperlukan guna memastikan bahwa solusi keamanan yang diterapkan tetap efektif dalam menghadapi ancaman baru pada keamanan.

Faktor-faktor yang mempengaruhi keamanan Moodle masih belum dipaparkan. Diperlukan penelitian lebih lanjut mengenai penjelasan faktor seperti apa yang dapat mempengaruhi tingkat keamanan Moodle. Dengan memahami faktor-faktor yang telah dipaparkan, developer dapat mengembangkan solusi yang lebih efektif untuk meningkatkan keamanan Moodle.

Tinjauan Pustaka

Penelitian terkait dengan analisis keamanan (LMS) moodle dengan metode vulnerability scanning telah dilakukan oleh beberapa peneliti diantaranya studi tentang Pengujian Keamanan Learning Management System Tutor LMS (Prasetyo et al., 2022). Penelitian ini merujuk pada metode penelitian yang diuji secara langsung dengan mengidentifikasi kerentanan terkait kontrol akses rusak pada platform tersebut.Dalam proses pengujian melalui tindakan langsung sebagai sebagai pengunjung yang

melakukan akses pada platform tersebut dan secara langsung mengidentifikasi dan mendokumentasikan kerentanan terhadap platform LMS. Dengan tujuan memberikan wawasan kepada pemilik platform untuk dapat memberikan kontrol akses yang aman untuk pengguna.

Analisa keamanan website open journal system menggunakan metode vulnerability assessment (Riadi et al., 2020). Penelitian ini merujuk pada vulnerability scanning sebagai metode yang digunakan untuk analisa keamanan. Penelitian ini menggunakan metodologi Open Web Application Security Project (OWASP) dalam pengujian, yang bertujuan untuk mengidentifikasi berbagai kerentanan keamanan di situs web OJS, termasuk kerentanan tinggi, sedang, dan rendah Rekomendasi dari penelitian ini mencakup penggunaan versi terbaru OJS yang dirilis oleh OJS Public Knowledge Project (PKP) sebagai langkah untuk mengatasi kerentanan yang teridentifikasi.Metode ini melibatkan pengujian sistem OJS tanpa pengetahuan sebelumnya tentang struktur sistem, dengan tujuan mengidentifikasi kerentanan atau kelemahan keamanan untuk tujuan remediasi yang cepat.

Moodle Learning Management System Utilization Assessment: Lenses on Its Accessibility, Security, and Usability (Gumiran, 2022). Penelitian ini merujuk pada Moodle yang menjadi Learning Management System dengan menganalisis dari segi keamanan dan manfaat yang didapatkan. Penelitian ini menggunakan Metode pengumpulan dan analisis data yang diterapkan adalah kuantitatif menggunakan survei online dengan instrumen yang dikembangkan oleh peneliti untuk mengumpulkan data, dengan pemilihan responden yang ditargetkan.

Tabel 1. Tabel Tinjauan Pustaka

No.	Nama peneliti	Tujuan Penelitian	Metode Penelitian	Hasil	Perbedaan
1.	Imam Riadi, et al.	Mengidentifikasi kerentanan pada situs web OJS.	Melakukan penilaian kerentanan dan pengujian penetrasi.	70 kerentanan tinggi, 1929 menengah, dan 4050 rendah pada OJS 2.4.7.	Objek pengujian menggunakan website open source E-Learning.
2.	Irene Cabauatan Gumiran	Menganalisis manfaat Moodle	Metode Kuantitatif Analisis data responden dan penelitian sebelumnya	Moodle dirancang untuk pengguna yang lebih mahir (expert), aksesibilitas tinggi, keamanan dan kegunaan dinilai sangat efisien dan	Objek perbandingan menggunakan dua versi Moodle

				sukses	
3.	Stefanus Eko Prasetyo, et al.	Mengidentifikasi dan mendokumentasikan kerentanan pada platform LMS	Melakukan metode penelitian tindakan dan pengujian penetrasi	Tutor LMS rentan terhadap akses pengunjung dan kelemahan dalam kontrol sistem Sedangkan Desain REST API LMS Cukup mudah digunakan pengunjung untuk mengambil konten kursus dan informasi tanpa otentikasi dan otorisasi	Pengujian dilakukan menggunakan OWASP-ZAP

Metode Penelitian

Penelitian ini akan mengadopsi metode vulnerability scanning untuk menganalisis keamanan Moodle Learning Management System (LMS) versi terbaru. Data yang digunakan meliputi konfigurasi Moodle, pengaturan keamanan, pengguna yang ada, serta perangkat lunak dan tools seperti OWASP-ZAP. Variabel yang diamati mencakup jenis-jenis kerentanan keamanan, tingkat keparahan, dan rekomendasi untuk meningkatkan keamanan Moodle (Kurniawan, 2021). Dengan menggunakan tool OWASP-ZAP pendeteksian keamanan pada Moodle Learning Management System (LMS) dapat dilakukan analisis kerentanan yang nantinya dapat diambil kesimpulan agar dapat menjadiacuan untuk memperbaiki sistem Moodle Learning Management System (LMS) yang telah ada (Priyawati et al., 2022).

Data Penelitian

Data yang akan digunakan dalam penelitian ini berasal dari beberapa sumber yang relevan dengan melakukan analisis keamanan Learning Management System (LMS) Moodle menggunakan metode Vulnerability Scanning. Hal pertama yang perlu dilakukan ialah melakukan konfigurasi Moodle baik itu versi lama maupun versi baru yang nantinya akan dibuat perbandingan. Kemudian melakukan konfigurasi pengaturan keamanan, serta profil pengguna dengan beberapa peran yang ada dalam sistem. Selain itu, data yang akan digunakan dalam penelitian juga mencakup informasi mengenai alat yang akan digunakan, seperti OWASP-ZAP, termasuk versi, konfigurasi, dan fitur yang nantinya akan digunakan.

Data mengenai jenis-jenis kerentanan keamanan yang sering ditemukan pada Moodle juga dikumpulkan melalui beberapa sumber, termasukliteratur dan penelitian sebelumnya. Jenis-jenis kerentanan umumnyamencakup Injection Vulnerabilities (SQL Injection dan LDAP Injection),Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), dan jenis kerentanan lainnya. Kemudian data hasil scanning menggunakan OWASP-ZAP meliputi detail dari kerentanan yang ditemukan, lokasi dimana kerentanan tersebut ditemukan, tingkat keparahannya, dan rekomendasi perbaikan yang dapat dilakukan (Ally, 2022).

Seluruh data yang telah disebutkan sebelumnya akan menjadi dasar untuk melaksanakan metodologi dasar yang telah disusun, termasuk pengembangan instrumen pengumpulan data, pengumpulan data melalui konfigurasi Moodle, serta proses scanning menggunakan OWASP-ZAP, melakukan analisis berdasarkan hasil scanning, dan penyusunan rekomendasi dan kesimpulan. Dengan menggunakan data ini, penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai kerentanan keamanan Moodle dan memberikan rekomendasi yang berguna untuk meningkatkan keamanan secara keseluruhan.

Desain Penelitian

Desain penelitian ini menggunakan desain penelitian eksperimental yang merupakan sebuah pendekatan penelitian yang digunakan untuk menguji efek dari satu atau lebih variabel bebas terhadap satu atau lebih variabel terikat dengan cara yang terkontrol. Dalam konteks penelitian ini, desain penelitian eksperimental akan digunakan untuk menguji efek dari penggunaan OWASP-ZAP sebagai alat scanning terhadap keamanan Moodle. Desain ini melibatkan instalasi dan konfigurasi Moodle versi terbaru sebagai kelompok perlakuan, di mana perlakuan tersebut adalah penggunaan OWASP-ZAP untuk melakukan scanning terhadap Moodle tersebut.

Langkah - langkah yang akan digunakan adalah :

1. Literature review
   a) Meninjau literatur tentang Moodle, OWASP-ZAP,dan vulnerability scanning.
   b) Mengidentifikasi jenis-jenis kerentanan keamananyang umum ditemukan pada Moodle.
   c) Mempelajari penelitian sebelumnya tentanganalisis keamanan Moodle.
2. Pengembangan instrumen pengumpulan data
   a) Membuat daftar periksa kerentanan keamanan berdasarkanhasil literatur review.
   b) Mengumpulkan informasi tentang kerentanan moodle daripenelitian penelitian sebelumnya
3. Pengumpulan data
   a) Menginstal dan mengkonfigurasi Moodle versi terbaru danversi lama
   b) Melakukan scanning terhadap Moodle dengan OWASP-ZAP.
   c) Mengidentifikasi jenis-jenis kerentanan keamananyang ditemukan.

d) Mengisi daftar periksa kerentanan keamanan.

4. Analisis data

a) Menganalisis data yang dikumpulkan dari scanning.

b) Menentukan tingkat keparahan kerentanan keamanan yangditemukan.

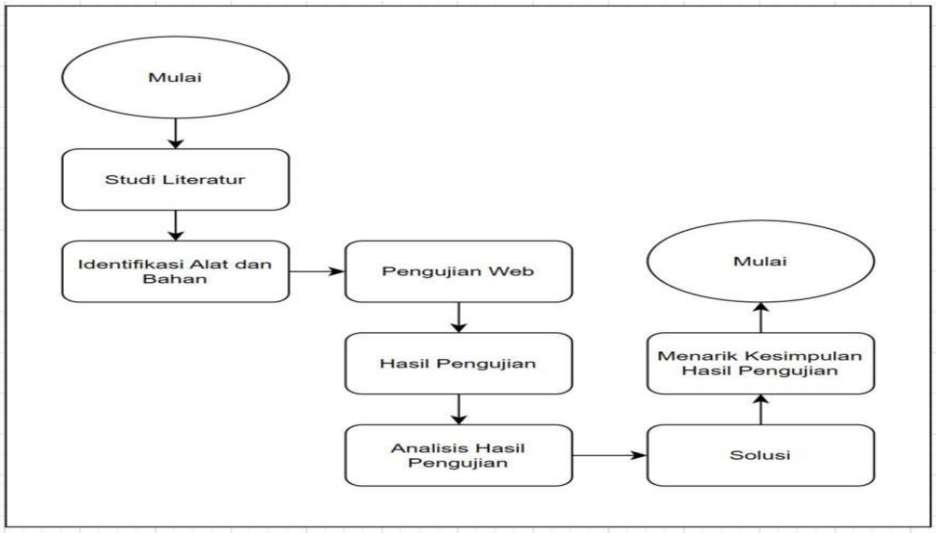
c) Mengidentifikasi penyebab kerentanan keamanan.

5. Rekomendasi dan kesimpulan

a) Memberikan rekomendasi untuk meningkatkan keamananMoodle berdasarkan hasil analisis data.

b) Menarik kesimpulan tentang keamanan Moodle versi terbaru.

Gambar 1. Alur Penelitian



Desain Eksperimen

Desain eksperimen yang akan digunakan untuk penelitian ini mencakup beberapa tahapan yang cukup sistematis. Berikut merupakan penjelasan dari diagram tahapan tersebut:

1) Generate tools

Langkah pertama adalah mengunduh dan menginstal OWASP ZAP. OWASP ZAP adalah alat pemindai kerentanan web open source yang dapat digunakan untuk menemukan kerentanan keamanan pada aplikasi web.

2) Input URL

Masukkan URL LMS Moodle yang ingin dianalisis. OWASP ZAPakan memindai URL ini untuk mencari kerentanan keamanan.

3) Autoscanning

OWASP ZAP akan secara otomatis memindai URL yang dimasukkan. Proses pemindaian dapat memakan waktu beberapa menit, tergantung pada kompleksitas aplikasi web.

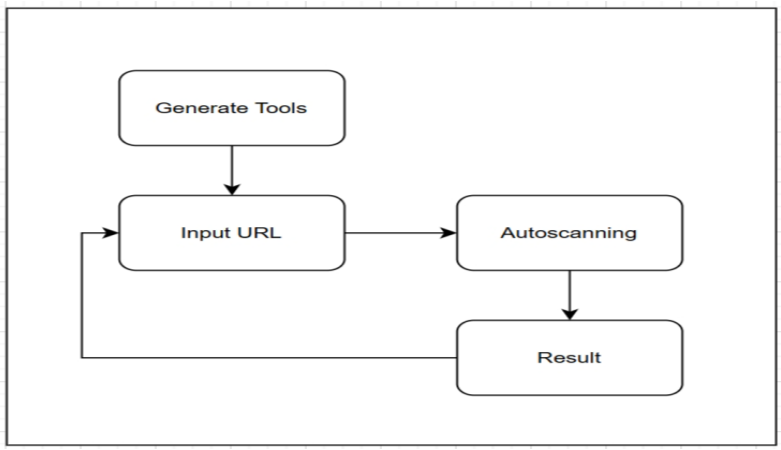
4) Result

OWASP ZAP akan menampilkan hasil pemindaian dalam format laporan. Laporan ini akan berisi daftar kerentanan keamanan yang ditemukan, serta informasi tentang kerentanan tersebut, seperti tingkat keparahan, dampak, dan solusi.

5) Analisis

Berdasarkan desain eksperimen ini, dapat disimpulkan bahwa OWASP ZAP dapat digunakan untuk menganalisis kerentanan keamanan pada LMS Moodle versi 3 dan 4. OWASP ZAP adalahalat yang mudah digunakan dan efektif untuk menemukan kerentanan keamanan pada aplikasi web.

Gambar 2. Alur Pengujian

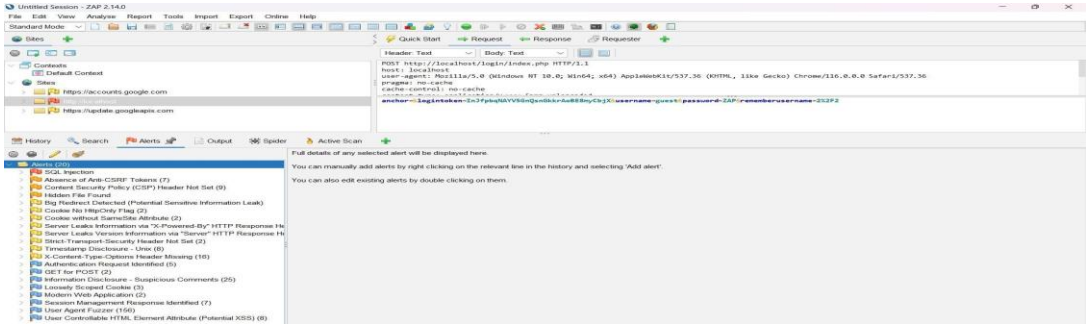


Tahap pengujian website menggunakan perangkat lunak Open Web Application Security Project (OWASP) dan OWASP Zed Attack Proxy (ZAP) yang ditunjukkan pada Gambar 2. Website yang diuji adalah website LMS Moodle versi 3 dan versi 4. Hasil yang diperlukan disesuaikan dengan keperluan yang menunjukkan jenis ancaman, peringkat risiko, confidence, evidence, source, CWE ID, dan WASC ID. Common Weakness Enumeration (CWE) merupakan daftar yang berisi jenis celah keamanan dan kerentanan yang dikategorikan untuk mengidentifikasi, memperbaiki, dan mencegah kerentanan.

Pembahasan

LMS Moodle Versi 3

Gambar 3. Hasil *scanning* pada LMS Moodle Versi 3 menggunakan OWASP-ZAP

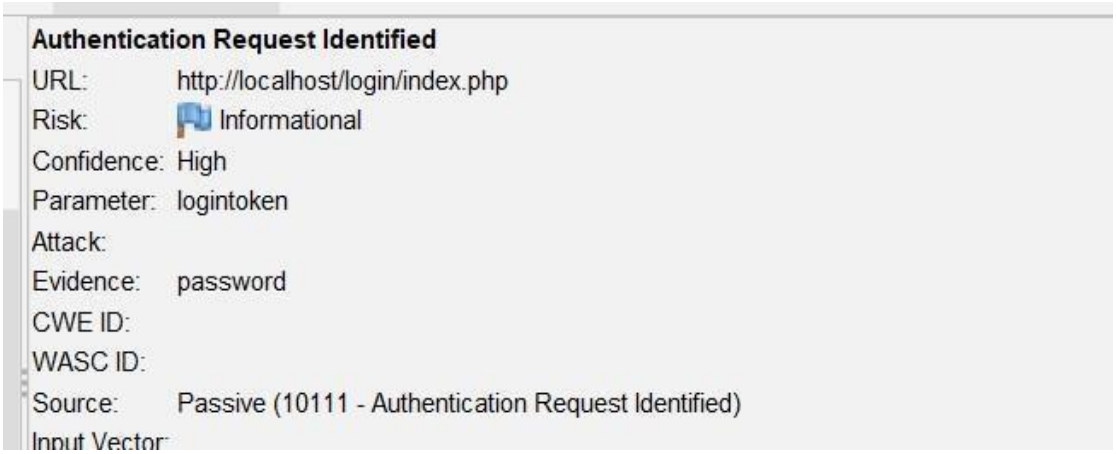


1. Autentikasi dan otorisasi

Gambar 4. Hasil *scanning* pada Autentikasi dan Otorisasi

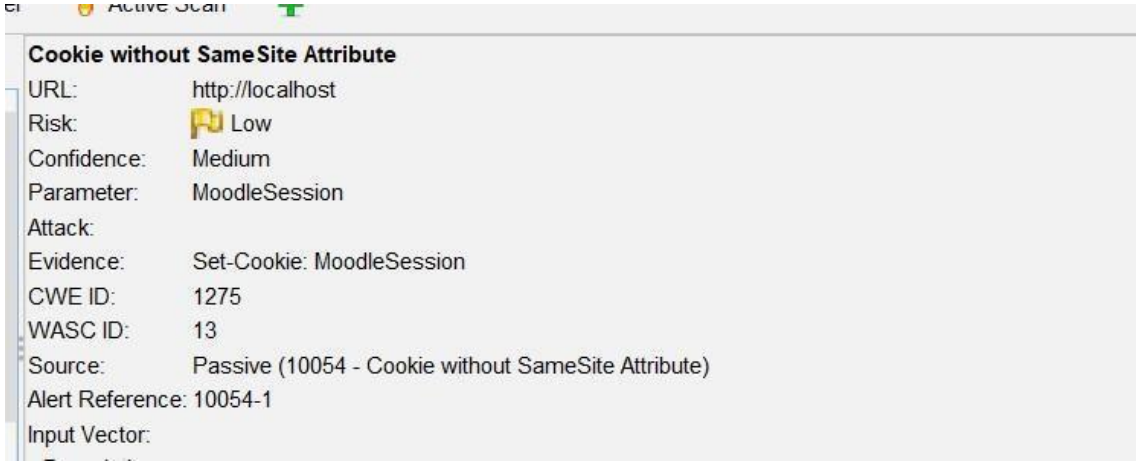
Cross-Site Request Forgery (CSRF) adalah jenis serangan web disebabkan oleh kurangnya token anti-CSRF pada formulir login. Token anti-CSRF adalah nilai acak yang dihasilkan oleh server dan dikirim ke browser klien. Saat pengguna mengirimkan formulir login, token anti-CSRF harus disertakan dalam permintaan.

Gambar 5. Hasil *scanning* pada Autentikasi dan Otorisasi



Mampu mengenali permintaan autentikasi dan membaca informasi tambahan (seperti nama pengguna) yang disertakan dalam bagian "Other Info". Informasi ini disusun dalam bentuk pasangan key-value (kunci-nilai) untuk membantu mengidentifikasi detail penting dari permintaan.Jika sistem keamanan diatur untuk melakukan deteksi metode autentikasi secara otomatis ("Auto-Detect"), maka akan menyesuaikan metode autentikasi yang digunakan agar sesuai dengan jenis permintaan yang teridentifikasi. Hal ini memungkinkan sistem keamanan untuk menangani beragam jenis permintaan login dengan lebih fleksibel dan efisien.

Gambar 6. Hasil *scanning* pada Autentikasi dan Otorisasi



Jika cookie dibuat tanpa atribut Same Site, cookie tersebut dapat dikirim sebagai respons terhadap permintaan lintas situs (cross-site request), yang dapat membuka risiko keamanan seperti Cross-Site Request Forgery(CSRF), Cross-Site Script Inclusion (XSSI), dan serangan waktu (timing attacks).

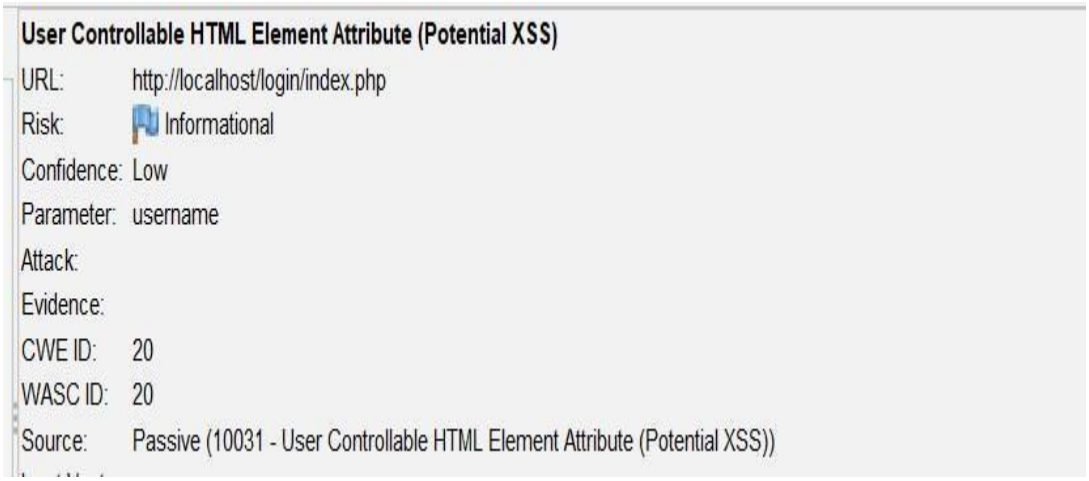
2. Manjamen user

Gambar 7. Hasil *scanning* pada Manajemen User

Peringatan ini muncul karena ada kemungkinan komentar tertinggal dalam kode program yang bisa dimanfaatkan penyerang. Komentar ini, meskipun tidak dieksekusi, bisa berisi informasi tentang cara kerja program, kelemahan yang sedang diperbaiki (tapi belum dihapus).

3. Assessment

Gambar 8. Hasil *scanning* pada Assessment



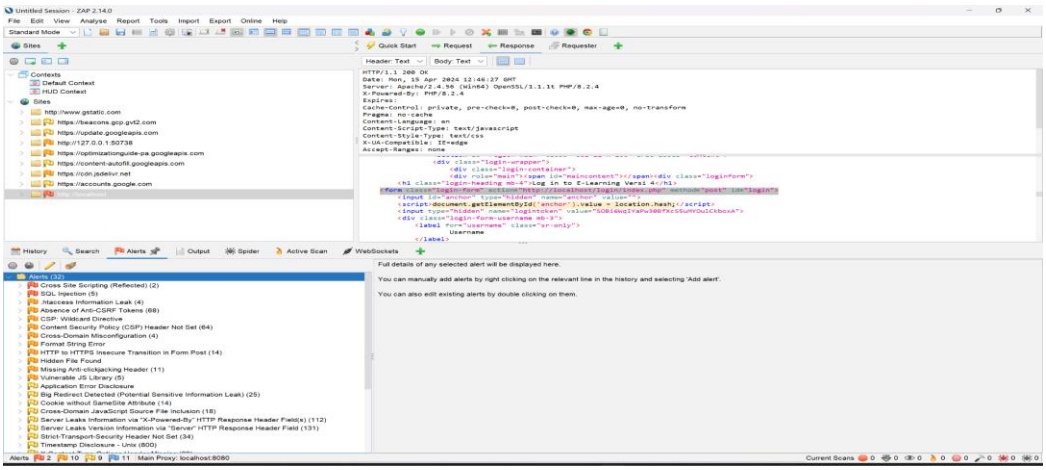
Pemeriksaan ini bertujuan untuk menemukan titik lemah potensial terhadap serangan Cross-Site Scripting (XSS) dengan memeriksa input pengguna yang diberikan melalui parameter query string dan data POST untuk mengidentifikasi dimana nilai atribut HTML tertentu mungkin dapat dikendalikan. Ini memberikan deteksi titik rawan untuk XSS (cross-site scripting).

Gambar 9. Hasil *scanning* pada Assessment

Timestamp dapat digunakan untuk melacak aktivitas pengguna dan mengidentifikasi potensi kerentanan keamanan biasanya terekspos saatwaktu suatu peristiwa terjadi atau data dimodifikasi, secara tidak sengaja terekspos.

LMS Moodle Versi 4

Gambar 10. Hasil *scanning* pada LMS Moodle Versi 4 menggunakan OWASP-ZAP



1. Autentikasi dan otorisasi

Gambar 11. Hasil *scanning* pada Autentikasi dan Otorisasi

Absence of Anti-CSRF Tokens	
URL:	http://localhost/login/index.php
Risk:	Medium
Confidence:	Low
Parameter:	
Attack:	
Evidence:	<form class="login-form" action="http://localhost/login/index.php" method="post" id="login">
CWE ID:	352
WASC ID:	9
Source:	Passive (10202 - Absence of Anti-CSRF Tokens)

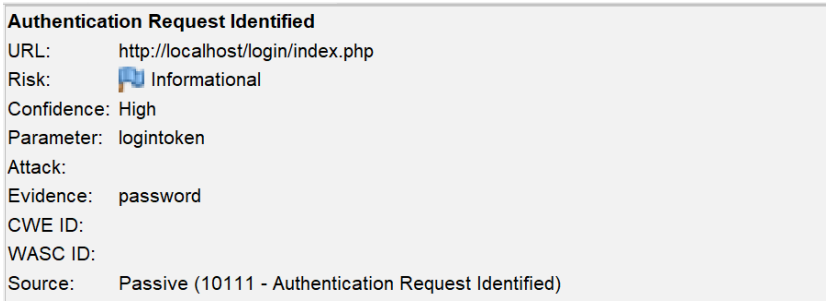
Serangan CSRF atau Cross-Site Request Forgery dapat terjadi saat melakukan login pada situs web. Penyerangan dapat dilakukan untuk mengubah pengaturan akun dan menghapus data. CSRF bisa saja terjadi karena LMS ini tidak memiliki perlindungan khusus.

Gambar 12. Hasil *scanning* pada Autentikasi dan Otorisasi

Cookie without SameSite Attribute	
URL:	http://localhost
Risk:	Low
Confidence:	Medium
Parameter:	MoodleSession
Attack:	
Evidence:	Set-Cookie: MoodleSession
CWE ID:	1275
WASC ID:	13
Source:	Passive (10054 - Cookie without SameSite Attribute)

Cookie merupakan data kecil yang disimpan oleh situs web pada perangkat pengguna. Kurangnya atribut SameSite pada cookie merupakan celah keamanan yang bisa dimanfaatkan oleh penyerang.

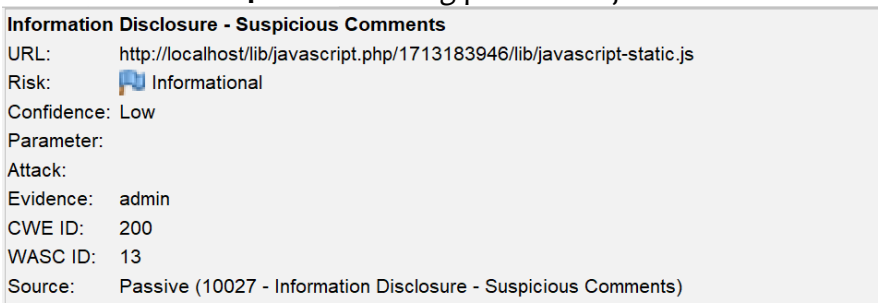
Gambar 13. Hasil *scanning* pada Autentikasi dan Otorisasi



Informasi mengenai permintaan yang diberikan telah diidentifikasi sebagai permintaan autentikasi. Dalam LMS ini berarti ketika seseorang mengakses situs dan memerlukan login, maka sistem akan mendeteksi permintaan tersebut dan memahami jenis autentikasi yang digunakan. Kemudian karena sistem menerapkan "Deteksi otomatis" maka sistem akan menyesuaikan diri untuk menerima jenis autentikasi yang digunakan, yaitu username dan password.

2. Manajemen user

Gambar 14. Hasil *scanning* pada Manajemen User



Komentar yang ada dalam kode program dapat mengandung informasimengenai cara pengelolaan data pengguna atau fungsi internal sistem.

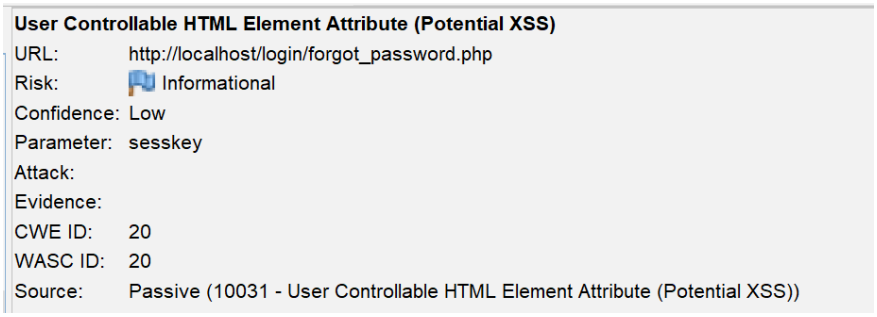
3. Assessment

Gambar 15. Hasil *scanning* pada Assessment

Kerentanan keamanan dapat terjadi pada web yang berbasis Unix. Kerentanan keamanan yang dimaksud adalah kebocoran informasi mengenai timestamp. Timestamp bukan masalah yang terlalu sensitif tetapi penyerang tetap saja bisa

memanfaatkan kebocoran ini untuk mencari informasi lain yang sifatnya lebih sensitif. Selain itu, dengan menggunakan timestamp, penyerang dapat memprediksi pola aktivitas server dan melancarkan serangan pada saat yang tepat.

Gambar 16. Hasil *scanning* pada Assessment



Pemeriksaan ini berfokus pada data yang dimasukkan ke data program untuk mencari dimana input pengguna bisa mempengaruhi nilai atribut pada HTML. Apabila input tersebut bisa mempengaruhi nilai atribut HTML maka hal ini merupakan indikasi awal potensi serangan XSS.

Perbandingan Hasil Analisa Moodle Versi 3 dan Moodle Versi 4

Tahap Analisa hasil pengujian yang di dapat dilakukan setelah hasil pengujian telah diperoleh dimana tahapan ini melalui beberapa tahapan yaitu identifikasi masalah, dampak, dan keparahan risiko pada website, dan menyesuaikan peringkat risiko. Risiko terdapat 4 level kategori risiko yang ditunjukkan pada Tabel 2.

Tabel 2. Tabel Kategori Risiko

Risk
Low
Medium
High
Informational

1. Absence of anti-CSRF token

Tabel 3. Tabel Perbandingan LMS Moodle Versi 3 dan 4 dalam Absence of Anti-CSRF Token

	Versi 3	**Versi 4**
Risk	Medium	Medium
Confidence	Low	Low

Evidence	<form class="mt-3" action "http://localhost/login/index.php" method="post" id="login">	<form class="login-form"action="http://localhost/login/index.php" method="post"id="login">
CWE ID	352	352
WASC ID	9	9
Source	Passive (10202 - Absence of Anti-CSRF Tokens)	Passive (10202 - Absence of Anti-CSRF Tokens)

Solusi: Menggunakan token unik untuk setiap sesi dapat memberikan keamanan tambahan tanpa bergantung pada header Referer. Ini mencegah permintaan palsu yang berasal dari sumber yang tidak dikenali kemudian memastikan bahwa pengguna yang mengirim permintaan telah otentikasi dengan benar dan menggunakan data lain dalam permintaan (seperti headercustom, token, atau parameter URL) untuk memverifikasi bahwa permintaanberasal dari sumber yang diinginkan.

1. Authentication request identified

Tabel 4. Tabel Perbandingan LMS Moodle Versi 3 dan 4 dalam Authentication Request Identified

	Versi 3	**Versi 4**
Risk	Informational	Informational
Confidence	High	High
Evidence	Password	password
CWE ID	-	-
WASC ID	-	-
Source	Passive (10111-Authentication Requestidentified)	Passive (10111-Authentication Requestidentified)

Solusi : Peringatan informasi adalah jenis pesan yang memberi tahu Anda tentang sesuatu yang mungkin memerlukan perhatian, tetapi tidak menunjukkan adanya ancaman atau kerentanan keamanan yang nyata namun tetap saja harus menyadari kapan dan mengapa peringatan ini muncul, sehingga Anda siap jika ada perubahan atau eskalasi setelah itu dicatat dan analisa tentang kerentanan yang ada untuk melakukan perbaikanpada keamanan.

2. Cookie without samesite attribute

Tabel 5. Tabel Perbandingan LMS Moodle Versi 3 dan 4 dalam Cookie without SameSite

	Versi 3	**Versi 4**
Risk	Low	Low
Confidence	High	Medium
Evidence	Set-Cookie: MoodleSession	Set-Cookie: MoodleSession

CWE ID	1275	1275
WASC ID	13	13
Source	Passive (10054 - Cookie without SameSite Attribute)	Passive (10054 - Cookie without SameSite Attribute)

Solusi: Atribut SameSite pada cookie menentukan bagaimana cookie diperlukan dalam permintaan lintas situs, penting untuk mencegah serangan seperti Cross-Site Request Forgery (CSRF). Jika Same Site diatur ke 'lax', cookie hanya dikirim dalam permintaan lintas situs yang melibatkan interaksi pengguna seperti mengklik tautan. Jika diatur ke 'strict', cookie hanya dikirim dalam permintaan yang berasal dari domain yang sama, yang paling aman. Untuk meningkatkan keamanan, evaluasi kebutuhan aplikasi , konfigurasi cookie dengan atribut Same Site yang tepat, lalu uji dan validasi untuk memastikan fungsionalitas tidak terganggu. Dengan mengatur SameSite pada 'lax' atau 'strict', Maka dapat meminimalkan risiko serangan lintas situs dan melindungi aplikasi serta pengguna.

3. Information disclosure – suspicious comments

Tabel 6. Tabel Perbandingan LMS Moodle Versi 3 dan 4 dalam Information Disclosure

	Versi 3	**Versi 4**
Risk	Low	Low
Confidence	High	Medium
Evidence	Set-Cookie: MoodleSession	Set-Cookie: MoodleSession
CWE ID	1275	1275
WASC ID	13	13
Source	Passive (10054 - Cookie without SameSite Attribute)	Passive (10054 - Cookie without SameSite Attribute)

Solusi : Untuk menjaga keamanan sistem dengan mencari kode programyang ada komentarnya yang berisi informasi sensitif atau petunjuk yang dapat dimanfaatkan penyerang. Hapus atau ubah komentar yang dapat memberikan wawasan tentang kerentanan, konfigurasi sistem, atau informasi penting lainnya. Jika komentar mengacu pada masalah atau bug, perbaiki masalah tersebut sebelum menghapus komentar.

4. User controllable HTML element attribute (potential XSS)

Tabel 7. Tabel Perbandingan LMS Moodle Versi 3 dan 4 dalam Potential XSS

	Versi 3	**Versi 4**
Risk	Informational	Informational
Confidence	Low	Low
Evidence	-	-
CWE ID	20	20

WASC ID	30	20
Source	Passive (10031) - User controllable HTML Element Attribute (potential XXS)	Passive (10031) - User controllable HTML Element Attribute (potential XXS)

Solusi : dengan membersihkan data validasi pengguna sebelum ditampilkan di halaman web. Ini mencegah penyerang menyisipkan kode berbahaya (seperti skrip) yang bisa mencuri informasi atau merusak website Anda.

5. Timestamp disclosure – unix

Tabel 8. Tabel Perbandingan LMS Moodle Versi 3 dan 4 dalam Timestamp Disclosure

	Versi 3	**Versi 4**
Risk	Low	Low
Confidence	Low	Low
Evidence	1713183946	1713183946
CWE ID	200	200
WASC ID	13	13
Source	Passive (10096 - Timestamp Disclosure)	Passive (10096 - Timestamp Disclosure)

Solusi: Pemeriksaan atau verifikasi secara manual perlu dilakukanterhadap data timestamp untuk memastikan bahwa data tersebut tidak sensitif dan tidak dapat digunakan untuk memperlihatkan pola aktivitas server yang dapat dieksploitasi oleh penyerang. Verifikasi manual dapat dilakukan dengan cara mengumpulkan data timestamp, melakukan analisis sensitivitas data, mengevaluasi risiko, dan mendokumentasi hasil analisis.

Kesimpulan

Berdasarkan analisis keamanan menggunakan metode VulnerabilityScanning pada Learning Management System (LMS) Moodle dengan menggunakan tools OWASP-ZAP, ditemukan beberapa kerentanan keamanan yang perlu diperhatikan. Kerentanan tersebut meliputi masalah pada autentikasi dan otorisasi, manajemen pengguna, serta kerentanan pada assessment. Meskipun tingkat keparahan kerentanan bervariasi, dari rendah hingga sedang, potensi eksploitasi oleh penyerang dapat menyebabkan masalah keamanan yang serius.

Terdapat perbedaan dalam kerentanan antara versi Moodle 3 dan versi Moodle 4, meskipun tingkat risiko yang terkait relatif sama. Sebagai rekomendasi, disarankan untuk menerapkan langkah-langkah perbaikan seperti penggunaan token anti-CSRF, konfigurasi cookie dengan atribut SameSite yang tepat, serta pembersihan komentar yang mencurigakan dari kode program. Langkah-langkah ini diharapkan dapat meningkatkan keamanan Moodle secara keseluruhan dan mengurangi risiko potensial

terhadap pengguna dan data sensitif yang disimpan didalamnya.

Daftar Pustaka

Aapio, T. (2021). Nmap scanning basics -kurssin rakentaminen metropolian Moodleympäristöön: Metropolia Ammattikorkeakoulu Insinööri (AMK) Information and Computer Technology IoT and Cloud Computing. https://www.theseus.fi/bitstream/handle/10024/508832/Aapio_Tomi.pdf?sequence=2

Abdullah, H. S. (2020). Evaluation of open source web application vulnerability scanners. *Academic Journal of Nawroz University*. https://journals.nawroz.edu.krd/index.php/ajnu/article/view/532

Allo, A. K. (2023). Analisis keamanan website SIASAT menggunakan teknikfootprinting dan vulnerability scanning. *Universitas Kristen Satya Wacana Institutional Repository.* https://repository.uksw.edu/handle/123456789/32212

Ally, S. (2022). Review of online examination security for the moodle learning management system. *IJEDICT: International Journal of Education and Development using Information and Communication Technology, 18(1).* https://files.eric.ed.gov/fulltext/EJ1345408.pdf

Al'Am'yubi, M. R. S., & Wijayanto, D. (2023). Analisis sistem keamanan website XYZ menggunakan framework OWASP ZAP. *JUIK : Jurnal Ilmu Komputer,* 3(1). https://journal.umgo.ac.id/index.php/juik/article/download/1974/1223

Aslan, Ö., Aktuğ, S. S., Okay, M. O., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333

Asmiyunda, A., Sanova, A., & Ekaputra, F. (2023). Pelatihan pemanfaatan aplikasi platform open course berbasis moodle dalam mengelola pembelajaran daring. *Jurnal Pengabdian UNDIKMA*, 4(2), 362. https://doi.org/10.33394/jpu.v4i2.7216

Gumiran, I. C. (2022). Moodle learning management system utilization assessment: Lenses on its accessibility, security, and usability. *IJRISS : International Journal of Research and Innovation in Social Science,* 6(8), 468–471. https://doi.org/10.47772/IJRISS.2022.6820

Kalaani, C. (2023). OWASP ZAP vs snort for SQLi vulnerability scanning. digitalcommons.georgiasouthern.edu. https://digitalcommons.georgiasouthern.edu/cgi/viewcontent.cgi?article=3820&context=etd

Kurniawan, S. (2021). Apa Itu Moodle? Niagahoster. https://www.niagahoster.co.id/blog/moodle-adalah/

Nurbojatmiko., Lathifah, A., Amri, F. B., & Rosidah, A. (2022). Security vulnerability analysis of the sharia crowdfunding website using OWASP-ZAP. *IEEE Xplore.* https://dx.doi.org/10.1109/CITSM56380.2022.9935837

Pargaonkar, S. (2023). Advancements in security testing: A comprehensive review of methodologies and emerging trends in software quality engineering. *IJSR : International Journal of Science and Research*, 12(9), 61–66. https://doi.org/10.21275/SR23829090815

Prasetyo, S. E., Hasanah, N., & Wijaya, G. (2022). Pengujian keamanan Learning

Management System Tutor LMS terhadap kerentanan insecure design dan broken access control. *Telcomatics : Telecommunication, Control, Information Technology and Electronic*, 7(2). https://doi.org/10.37253/telcomatics.v7i2.7357

Pratama, I. G. I., & Cahyaningsih, I. G. A. (2021). Melawat ke dunia virtual transformasi guru sejarah biasa menjadi guru memesona abad 21 di masa pembelajaran jarak jauh. *Candra Sangkala*, 3(1), 11. https://doi.org/10.23887/jcs.v3i1.33919

Priyawati, D., Rokhmah, S., & Utomo, I. C. (2022). Website vulnerabilitytesting and analysis of website application using OWASP. *IJCIS : International Journal of Computer and Information System*, 3(3). https://doi.org/10.29040/ijcis.v3i3.90

Riadi, I., Yudhana, A., & Yunanri, W. (2020). Analisis keamanan website open journal system menggunakan metode vulnerability assessment. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 7(4), 853–860. https://doi.org/10.25126/jtiik.2020701928

Sahida, N. N., Rokmanah, S., & Syachruroji, A. (2023). Literature review: Pemanfaatan teknologi dalam pembelajaran di sekolah dasar. *PENDAS: Jurnal Ilmiah Pendidikan Dasar, 8(3)*. https://journal.unpas.ac.id/index.php/pendas/article/view/10583