Neptunus : Jurnal Ilmu Komputer Dan Teknologi Informasi
Volume. 3, Nomor. 3, Agustus 2025
e-ISSN : 3031-898X, p-ISSN : 3031-8998; Hal. 21-36
DOI: https://doi.org/10.61132/neptunus.v3i3.887
Available online at: https://journal.arteii.or.id/index.php/Neptunus

Analisis Keamanan *Website E-learning* ILMU2 Menggunakan Metode *Open Web Application Security Project ZAP* (OWASP ZAP)

Shalsabila Titanie Harianto[1*], Zahrah Aliyah Rachman[2], Aliyyah Nabiilah Farahdita[3], Fahryan Putra Ramadi[4], Agung Brastama[5] , Siti Mukaromah[6]
[1-6] Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jawa Timur, Indonesia
Email : 22082010091@student.upnjatim.ac.id[1], 22082010103@student.upnjatim.ac.id[2], 22082010122@student.upnjatim.ac.id[3], 22082010189@student.upnjatim.ac.id[4], agungbp.si@upnjatim.ac.id[5], sitimukaromah.si@upnjatim.ac.id[6]*

Alamat: JL. Rungkut Madya No.1, Gn. Anyar, Kec. Gn. Anyar, Surabaya, Jawa Timur
Korespondensi penulis: 22082010091@student.upnjatim.ac.id

Abstract. *The development of e-learning platforms has transformed the landscape of education by providing flexible and accessible learning methods. However, security threats targeting web-based applications pose significant risks to the confidentiality, integrity, and availability of academic data. This research aims to analyze the security vulnerabilities of the ILMU2 e-learning website at UPN "Veteran" Jawa Timur using the Web Application Security Project Zed Attack Proxy (OWASP ZAP) methodology. The study applies a black-box testing approach to simulate attacks and identify potential weaknesses in the website's security mechanisms. Expected findings include the identification of vulnerabilities such as cross-site scripting (XSS), SQL injection, and security misconfigurations. The results are intended to provide insights for improving the security posture of the ILMU2 platform and contribute to the broader discourse on securing educational technology in higher education institutions.*

Keywords: *E-learning, OWASP ZAP, security analysis, system vulnerability, web application*

Abstrak. Perkembangan *platform e-learning* telah memberikan kemudahan akses terhadap proses pembelajaran, khususnya di lingkungan perguruan tinggi. Namun, keberadaan celah keamanan dalam aplikasi *web* seperti situs *e-learning* ILMU2 UPN "Veteran" Jawa Timur menimbulkan risiko serius terhadap kerahasiaan, integritas, dan ketersediaan data akademik. Penelitian ini bertujuan untuk menganalisis keamanan situs *e-learning* ILMU2 menggunakan metode *Web Application Security Project Zed Attack Proxy (OWASP ZAP)*. Metode yang digunakan adalah pengujian *black-box* untuk mensimulasikan serangan dan mendeteksi kerentanan pada sistem. Hasil yang diharapkan mencakup temuan kerentanan seperti *cross-site scripting (XSS)*, *SQL injection*, serta kesalahan konfigurasi keamanan. Temuan ini diharapkan dapat memberikan rekomendasi perbaikan serta berkontribusi terhadap peningkatan keamanan sistem informasi dalam lingkungan pendidikan tinggi.

Kata kunci: *e-learning*, kerentanan sistem, OWASP ZAP, pengujian keamanan, aplikasi *web*

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam sektor pendidikan, khususnya melalui pemanfaatan *platform e-learning*. Sistem *e-learning* memungkinkan proses pembelajaran dilakukan secara daring, memfasilitasi interaksi antara dosen dan mahasiswa tanpa batasan ruang dan waktu. UPN "Veteran" Jawa Timur merupakan salah satu institusi yang telah mengimplementasikan *platform* pembelajaran daring bernama ILMU2. *Platform* ini menjadi sistem utama dalam menunjang kegiatan belajar mengajar secara digital, termasuk pengelolaan tugas, materi kuliah, dan hasil evaluasi pembelajaran.

Received: Mei 24, 2025; Revised: Juni 08, 2025; Accepted: Juni 22, 2025; Online Available: Juni 26, 2025

Namun, seiring meningkatnya penggunaan sistem *e-learning*, ancaman terhadap keamanan informasi menjadi isu krusial yang perlu diperhatikan secara serius. Banyak sistem informasi pendidikan menjadi target serangan siber yang memanfaatkan celah keamanan dari aplikasi berbasis *web* (Sharma & Mishra, 2023). Berdasarkan penelitian Alshamrani et al. (2020), ancaman seperti *SQL injection*, *cross-site scripting (XSS)*, dan *broken authentication* sering kali ditemukan dalam sistem pendidikan daring. Oleh karena itu, penting bagi institusi pendidikan untuk melakukan evaluasi keamanan sistem secara berkala guna mengidentifikasi dan memperbaiki potensi kerentanan sebelum disalahgunakan oleh pihak yang tidak bertanggung jawab.

Beberapa penelitian sebelumnya telah menyoroti pentingnya pengujian keamanan aplikasi *web* dalam konteks pendidikan tinggi. Misalnya, penelitian oleh Kaur & Kaur (2021) menunjukkan bahwa banyak institusi belum secara rutin melakukan uji penetrasi atau pengujian kerentanan, yang menyebabkan sistem informasi mereka rentan terhadap serangan. Alat bantu seperti OWASP ZAP *(Zed Attack Proxy)* telah terbukti efektif dalam mendeteksi berbagai celah keamanan, termasuk dalam simulasi pengujian terhadap sistem informasi akademik (Sari & Prasetyo, 2021). Penggunaan alat ini dapat memberikan pemahaman menyeluruh mengenai jenis dan tingkat risiko yang dihadapi oleh sistem *e-learning*.

Meskipun OWASP ZAP telah banyak digunakan dalam berbagai studi untuk menguji aplikasi *web* berbasis pendidikan, belum ditemukan penelitian yang secara spesifik menganalisis keamanan *platform* ILMU2 milik UPN "Veteran" Jawa Timur. Hal ini menciptakan *gap* penelitian yang perlu dijembatani, terutama mengingat pentingnya menjaga integritas dan kerahasiaan data akademik yang dikelola oleh sistem tersebut. Analisis keamanan berbasis metodologi OWASP dapat membantu institusi pendidikan merancang strategi mitigasi risiko yang lebih efektif. Lebih lanjut, hasil dari pengujian ini dapat menjadi referensi untuk pengembangan kebijakan keamanan sistem informasi secara berkelanjutan di lingkungan kampus.

Penelitian ini bertujuan untuk melakukan analisis keamanan terhadap *website* ILMU2 UPN "Veteran" Jawa Timur dengan menggunakan metode pengujian OWASP ZAP. Fokus utama penelitian adalah mengidentifikasi potensi kerentanan sistem berdasarkan kategori OWASP, serta memberikan rekomendasi teknis terhadap temuan yang diperoleh. Dengan pendekatan ini, penelitian diharapkan mampu memberikan kontribusi nyata dalam penguatan sistem keamanan informasi di sektor pendidikan tinggi. Selain itu, hasil penelitian ini juga dapat dijadikan rujukan bagi institusi lain yang menggunakan sistem *e-learning* dalam menghadapi tantangan keamanan digital yang semakin kompleks.

2. KAJIAN TEORITIS

E-Learning

E-learning merupakan salah satu sarana yang dimanfaatkan dalam kegiatan pembelajaran di institusi pendidikan tinggi yang dapat berfungsi sebagai alternatif untuk memenuhi interaksi yang tidak dapat dilaksanakan langsung di ruang kelas. (Retnoningsih, 2017). Dalam bidang pendidikan, internet dapat dimanfaatkan sebagai media untuk belajar. Proses belajar ini berbentuk pendidikan elektronik yang lebih dikenal sebagai *e-learning*. (Hasan, H. Hafidz, & Nashihin, H., 2023). Dengan kemajuan yang terus-menerus dalam teknologi informasi dan komunikasi saat ini, terutama dalam hal internet, sangat memungkinkan untuk menciptakan cara-cara belajar yang lebih efektif yang sejalan dengan perkembangan zaman dan sesuai dengan keperluan para pelajar. (Nashihin, H., Efendi, R., & Salmiyatun, S, 2020)

Keamanan Aplikasi Web

Aktivitas kejahatan siber semakin meningkat dari hari ke hari dan mengeksploitasi situs *web* karena tidak adanya keamanan dalam infrastruktur jaringan. Perlindungan data adalah tingkat prioritas tertinggi saat ini sehingga pekerjaan yang menonjol adalah menemukan kelemahan keamanan dalam jaringan dan aplikasi *web* (Nurdin, Salman, & Kadang, O., M, 2024). Keamanan aplikasi *web* adalah upaya untuk melindungi aplikasi berbasis *web* dari berbagai ancaman siber yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan data.

Ancaman tersebut bisa berupa pencurian data, akses tidak sah, atau manipulasi informasi yang umumnya terjadi akibat celah pada sistem autentikasi, pengolahan input, atau konfigurasi yang tidak aman. Oleh karena itu, penting bagi pengembang untuk memahami risiko keamanan sejak awal dan menerapkan langkah-langkah pencegahan, seperti validasi data, penggunaan protokol yang aman, serta pengujian keamanan secara berkala. Salah satu pendekatan yang sering digunakan adalah dengan memanfaatkan alat bantu seperti OWASP ZAP untuk mengidentifikasi potensi kerentanan dalam aplikasi secara otomatis dan membantu memastikan sistem berjalan dengan aman sebelum digunakan oleh pengguna.

OWASP (*Open Web Application Security Project*)

OWASP (*Open Web Application Security Project*) adalah sebuah organisasi nirlaba global yang fokus pada peningkatan keamanan perangkat lunak, khususnya aplikasi berbasis *web*. *Open Web Application Security Project* (OWASP) adalah sebuah framework bersifat *open source* yang menyediakan berbagai sumber daya terbuka dan

gratis, seperti dokumentasi, alat uji keamanan, panduan pengembangan aman, serta daftar kerentanan umum dalam aplikasi *web* (Kusuma, G., 2022). Tujuan utama OWASP adalah membantu pengembang, peneliti, dan organisasi memahami serta mengimplementasikan praktik terbaik dalam membangun aplikasi yang aman. Dengan adanya OWASP, komunitas teknologi memiliki referensi yang kredibel untuk mengidentifikasi, menganalisis, dan memperbaiki potensi celah keamanan dalam siklus pengembangan perangkat lunak.

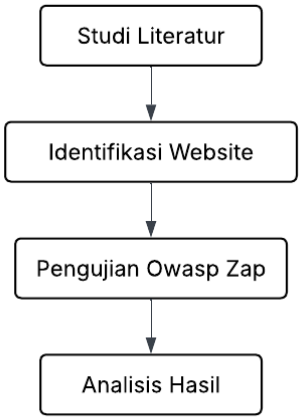
OWASP ZAP (*Zed Attack Proxy*)

OWASP ZAP (*Zed Attack Proxy*) adalah salah satu alat *open-source* yang dikembangkan oleh OWASP untuk melakukan pengujian keamanan pada aplikasi *web*. ZAP dirancang untuk membantu pengembang dan penguji keamanan dalam menemukan celah atau kerentanan pada aplikasi secara otomatis maupun manual. ZAP yang dikenal dengan "proxy man-in-the-middle" ini berdiri diantara *browser* penguji dan aplikasi *web* sehingga dapat menyegat dan memeriksa pesan yang dikirim antar *browser* dan aplikasi *web* (Kuncoro, A. W., & Rahma, F., 2022). Alat ini memiliki berbagai fitur seperti *spidering* (menelusuri halaman web), *active scanning* (pemindaian aktif untuk mendeteksi kerentanan), *passive scanning*, *man-in-the-middle proxy*, dan fitur untuk pengujian autentikasi.

Karena antarmukanya yang intuitif dan kemampuannya yang kuat, OWASP ZAP banyak digunakan baik oleh pemula maupun profesional di bidang keamanan aplikasi. Selain itu, ZAP mendukung integrasi dengan alat atau proses pengembangan lain sehingga cocok digunakan dalam siklus pengembangan perangkat lunak berbasis DevSecOps. Dengan OWASP ZAP, proses identifikasi dan mitigasi risiko keamanan dapat dilakukan secara lebih cepat dan efisien, sehingga membantu menjaga keamanan aplikasi *web* sejak tahap pengembangan awal.

3. METODE PENELITIAN

Metode yang digunakan dalam proses analisis autentikasi pada website *E-Learning* ILMU2 yang dimiliki oleh UPN "Veteran" Jawa Timur terdiri dari beberapa tahap yang akan digambarkan pada *flowchart* berikut.



Gambar 1. *Flowchart* Metode Penelitian

Studi Literatur

Tahap studi literatur ini bertujuan untuk menjelaskan kajian pustaka dari teori-teori yang digunakan untuk mendukung penelitian yang diperoleh dari jurnal, buku, artikel, situs internet, maupun penelitian terdahulu. Studi literatur dilakukan sebagai landasan teoritis untuk memperkuat pemahaman peneliti terhadap topik yang dikaji. Dalam tahap ini, peneliti mengumpulkan dan menelaah berbagai referensi yang relevan untuk memperoleh gambaran menyeluruh mengenai konsep, variabel, dan hasil penelitian sebelumnya yang berkaitan.

Identifikasi *Website*

Sistem informasi *e-learning* ILMU2 yang diterapkan di UPN "Veteran" Jawa Timur merupakan sebuah *platform* yang dirancang untuk menunjang proses pembelajaran berbasis digital di lingkungan perguruan tinggi. Melalui sistem ini, dosen dapat mengunggah materi, memberikan tugas, serta melakukan evaluasi pembelajaran, sementara mahasiswa dapat mengakses materi, mengikuti perkuliahan secara daring, dan mengumpulkan tugas. Sistem ini mendukung efisiensi dan fleksibilitas proses belajar mengajar yang tidak terbatas oleh ruang dan waktu.

Pengujian Owasp Zap

Pengujian menggunakan OWASP ZAP (*Zed Attack Proxy*) dilakukan untuk mendeteksi potensi kerentanan pada aplikasi *website*, seperti celah keamanan yang termasuk dalam OWASP *Top* 10, antara lain SQL *Injection*, *Cross Site Scripting* (XSS), dan *Security Misconfiguration*. Alat ini bekerja dengan memindai sistem secara otomatis melalui tahapan seperti *spidering* dan *active scan* untuk mengidentifikasi titik

lemah yang dapat dieksploitasi. Hasil dari pengujian ini digunakan sebagai acuan dalam perbaikan sistem agar lebih aman dan terlindungi dari ancaman siber.

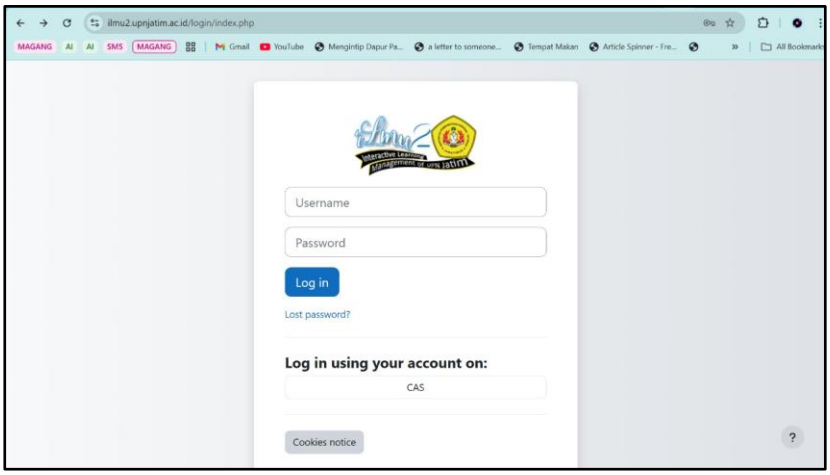
Analisis Hasil

Analisis hasil dilakukan untuk menganalisis temuan yang diperoleh setelah melakukan proses pengujian sistem ILMU2 menggunakan Owasp Zap. Setiap kerentanan yang terdeteksi dianalisis berdasarkan tingkat risikonya, mulai dari rendah, sedang, hingga tinggi, guna menentukan prioritas penanganan. Hasil analisis ini memberikan gambaran menyeluruh mengenai aspek keamanan sistem yang perlu diperbaiki serta menjadi dasar rekomendasi tindakan perbaikan. Dengan demikian, proses ini bertujuan untuk memastikan bahwa sistem yang dianalisis memenuhi standar keamanan yang layak.

4. HASIL DAN PEMBAHASAN

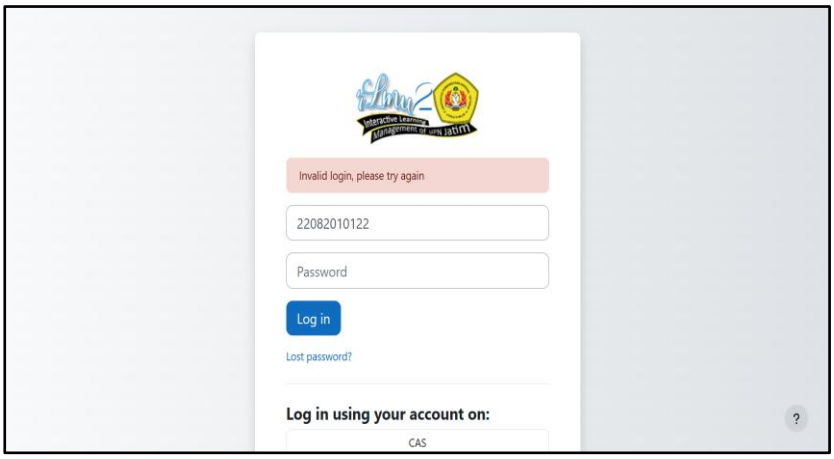
*Website e-learnin*g ILMU2 Universitas Pembangunan Nasional "Veteran" Jawa Timur merupakan *platform* yang digunakan untuk mendukung pembelajaran daring hingga membantu pengelolaan dalam pengumpulan tugas mahasiswa. Maka dari itu untuk mengetahui tingkat keamanan *website* dilakukan analisis dengan melalui proses pengumpulan data dan pengujian langsung menggunakan *tools* OWASP ZAP (Zed Attack Proxy) terhadap keseluruhan sistem pada *website e-learning* ILMU2 Universitas Pembangunan Nasional "Veteran" Jawa Timur yang dilaksanakan pada bulan Mei 2025. Selama proses analisis ini pendekatan yang digunakan adalah metode *black-box testing*, metode ini tidak memiliki akses ke kode sumber sistem, melainkan hanya mengandalkan interaksi melalui antarmuka web (Sugara & Sriyasa, 2024).

Metode *black-box testing* dilakukan dengan mensimulasikan perilaku pengguna yaitu mahasiswa tanpa mengetahui struktur *internal* dari sistem. Dalam konteks ini, pengujian dimulai dari halaman *login website* ILMU2 yang berfungsi sebagai gerbang utama akses pengguna. Penguji mencoba melakukan *input* data login serta menelusuri berbagai fitur untuk mengamati bagaimana sistem merespons permintaan, validasi input, serta perlindungan terhadap potensi serangan seperti *SQL injection* dan CSRF.



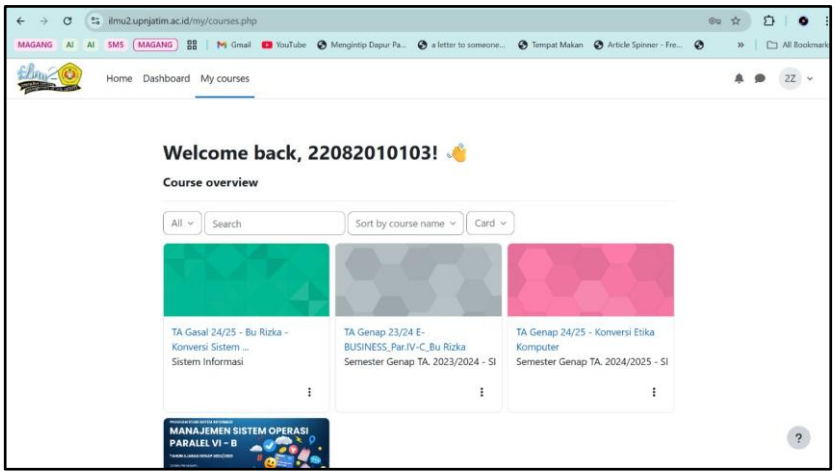
Gambar 2. Tampilan *Login Website* ILMU2

Gambar 2. menunjukkan halaman *login* dari *website e-learning* ILMU2 yang menjadi objek awal dalam proses pengujian menggunakan metode *black-box*. Halaman ini merupakan titik masuk utama bagi pengguna yaitu mahasiswa, sehingga penting untuk dilakukan analisis guna melihat bagaimana sistem menangani permintaan autentikasi dan *input* dari pengguna.



Gambar 3. Tampilan *Invalid Login Website* ILMU2

Pada Gambar 3. memperlihatkan hasil dari percobaan *input login* yang gagal. Pengujian ini dilakukan sebagai bagian dari validasi sistem terhadap *input* tidak sah, seperti simulasi serangan SQL *injection* maupun *brute force*. Tahapan ini bertujuan untuk mengetahui sejauh mana sistem mampu mendeteksi dan menangani *input* yang mencurigakan.



Gambar 4. Halaman Utama Setelah *Login Website* ILMU2

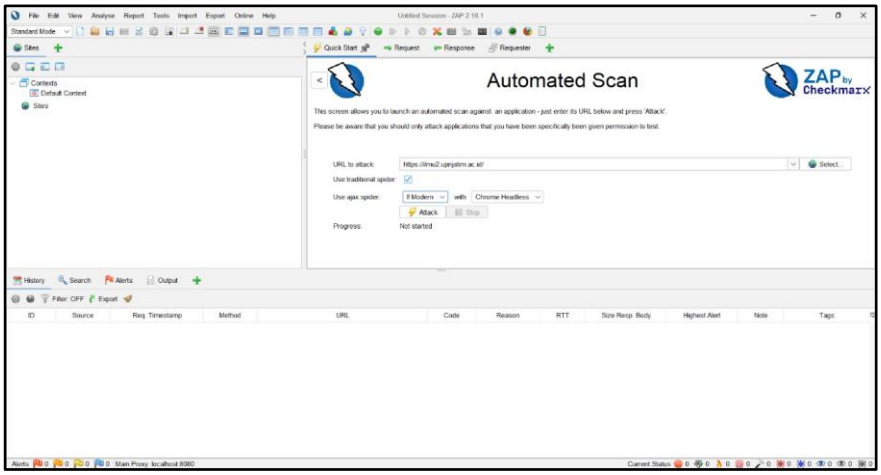
Selanjutnya pada Gambar 4. menampilkan tampilan halaman utama setelah proses *login* berhasil. Bagian ini diuji untuk mengevaluasi pengelolaan sesi pengguna dan memastikan bahwa hanya pengguna yang berhasil melewati proses autentikasi yang dapat mengakses halaman tersebut. Pengamatan terhadap alur ini membantu dalam mengidentifikasi kelemahan pada kontrol akses dan manajemen sesi. Ketiga tahapan ini dilakukan berurutan untuk mengamati bagaimana sistem merespon *input* pengguna dari awal hingga berhasil masuk ke dalam sistem. Seluruh proses ini menjadi dasar penting sebelum dilakukan pemindaian otomatis menggunakan OWASP ZAP untuk mendeteksi kerentanan secara menyeluruh.

Pengujian ini berfokus pada autentikasi dan keseluruhan manajemen sesi, karena bagian ini menjadi titik krusial dalam menjaga akses terhadap data sensitif pengguna terutama mahasiswa. Data ini mencangkup informasi terkait bidang akademik, nilai, hingga materi pembelajaran. Melalui *scanning* otomatis menggunakan OWASP ZAP, berbagai data terkait yang berpotensi memiliki celah keamanan akan dikumpulkan untuk dianalisis. Hasil dari pengujian ini menjadi dasar dalam mengevaluasi efektivitas sistem serta mengidentifikasi komponen yang masih perlu ditingkatkan dari sisi keamanan *website*.

Session Management Testing

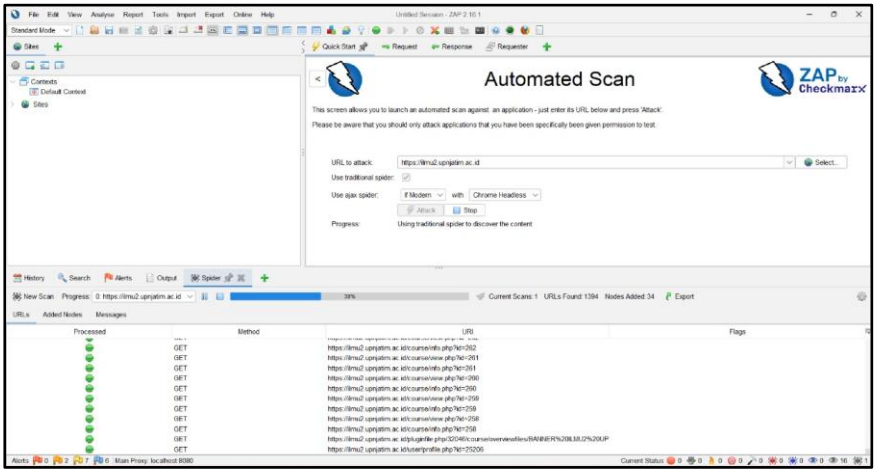
Pengujian terhadap *session management* pada *website e-learning* ILMU2 dilakukan menggunakan fitur *Active Scan* pada OWASP ZAP. Berikut merupakan tahapan pengujian dengan OWASP ZAP:

a) Pada Gambar 5. halaman utama program OWASP, pilih *automated scan* dan masukkan URL target serta *browser* yang akan digunakan. Lalu klik *attack* untuk melakukan pengujian



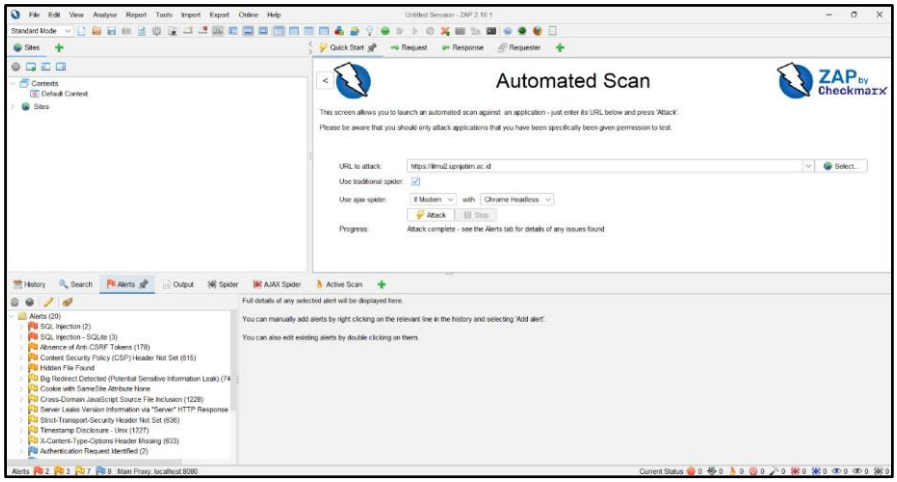
Gambar 5. Proses *Automated Scan* dengan OWASP ZAP

b) Proses *automated scan* berjalan seperti yang ditunjukkan pada Gambar 6. OWASP ZAP menggunakan fitur *spider* untuk secara otomatis menelusuri seluruh struktur halaman dan mendeteksi potensi kerentanan maupun ancaman pada URL target, yaitu *website* ILMU2. Setelah proses pemindaian selesai, OWASP ZAP akan menampilkan hasil temuan dalam bentuk daftar *alert* yang dikategorikan berdasarkan tingkat risikonya.



Gambar 6. Tampilan Proses *Scanning* pada OWASP ZAP

c) Pada Gambar 7. ditampilkan hasil pemindaian yang telah selesai, yang menunjukkan sejumlah celah keamanan atau ancaman yang terdeteksi pada *website e-learning* ILMU2. Hasil ini selanjutnya dianalisis untuk dilakukan pemetaan berdasarkan kategori kerentanan dan potensi dampaknya terhadap sistem. Analisis ini bertujuan untuk mengevaluasi tingkat keamanan website dan mengidentifikasi bagian-bagian yang rentan terhadap eksploitasi. Data yang diperoleh dari proses ini menjadi dasar dalam penyusunan rekomendasi perbaikan sekaligus menjadi hasil akhir dari penelitian ini.



Gambar 7. Hasil *Scanning* dengan OWASP ZAP

Hasil Penelitian

Hasil penelitian dari proses pemindaian yang telah dilakukan menggunakan metode *Open Web Application Security Project* (OWASP) menunjukkan sejumlah potensi celah keamanan pada *website e-learning* ILMU2. Temuan tersebut diklasifikasikan ke dalam empat kategori tingkat risiko, yaitu *High*, *Medium*, *Low*, dan *Informational*, berdasarkan tingkat dampak yang dapat ditimbulkan dari masing-masing kerentanan. Klasifikasi ini membantu dalam menentukan prioritas penanganan terhadap setiap celah yang terdeteksi. Rangkuman hasil pemindaian tersebut disajikan pada Tabel 1. sebagai *output* dari program OWASP ZAP yang akan dievaluasi.

Tabel 1. Hasil S*canning Report* dengan OWASP ZAP

Summary of Alerts	
Risk Level	*Number of Alerts*
High	2
Medium	3
Low	7
Informational	8

Alerts		
Name	*Risk Level*	*Number of Instance*

Content Security Policy (CSP) Header Not Set	*High*	615
Hidden File Found	*High*	1
Server Leaks Version Information via "Server" HTTP Response Header	*High*	1236
Strict Transport Security Header Not Set	*High*	636
Authentication Request Identified	*High*	2
GET For POST	*High*	2
SQL Injection	*Medium*	2
SQL Injection - SQLite	*Medium*	3
Big Redirect Detected (Potential Sensitive Information Leak)	*Medium*	74
Cookie with SameSite Attribute None	*Medium*	1
Cross-Domain JavaScript Source File Inclusion	*Medium*	1228
X-Content Type-Option Header Missing	*Medium*	633
Modern Web Application	*Medium*	610
Session Management Response Identified	*Medium*	3
User Agent Fuzzer	*Medium*	828
Absence of anti CSRF Tokens	*Low*	178
Timestamp Disclosure - Unix	*Low*	1227
Information Disclosure - Suspicious Comment	*Low*	615
Re-examine Cache-control Directive	*Low*	610
User Controllable HTML Element Attribute (Potential XSS)	*Low*	487

Berdasarkan *scanning report* didapatkan hasil *risk level* bahwa *website e-learning* ILMU2 menunjukkan adanya 20 tanda bahaya (*alerts*) dengan tingkat ancaman dari yang terendah sampai dengan yang tertinggi. Hasil *risk level* ini meliputi celah keamanan, kategori, lokasi, metode, parameter dan juga solusi untuk menghadapi hal tersebut. Berdasarkan hasil

alert, ditemukan total 20 jenis kerentanan, yang terdiri dari 6 risiko tinggi (*high*), 8 risiko sedang (*medium*), dan 6 risiko rendah (*low*). Beberapa kerentanan memiliki jumlah *instance* yang sangat besar, seperti *Content Security Policy Header Not Set* dengan 615 *instance*, *Strict Transport Security Header Not Set* sebanyak 636 *instance*, serta *Server Leaks Version Information* yang mencapai 1236 *instance*. Adanya temuan ini menunjukkan terdapat kelemahan signifikan dalam penerapan praktik keamanan dasar pada *website e-learning* ILMU2 milik Universitas Pembangunan Nasional "Veteran" Jawa Timur.

Kerentanan dengan tingkat risiko tinggi sebagian besar berkaitan dengan pengelolaan *header* keamanan dan pengungkapan informasi *server*, yang dapat dimanfaatkan oleh penyerang untuk melancarkan serangan seperti XSS (*Cross-Site Scripting*), MITM (*Man-in-the-Middle*), dan f*ingerprinting* versi *server*. Selain itu, terdapat beberapa kelemahan pada aspek autentikasi dan manajemen sesi, seperti *Authentication Request Identified*, *Session Management Response Identified*, serta tidak ditemukannya token anti-CSRF pada banyak formulir. Hal ini menunjukkan bahwa sistem rentan terhadap serangan pemalsuan permintaan dan pengambilalihan sesi. Di sisi lain, kerentanan seperti *SQL Injection* dan *User Controllable HTML Element Attribute* menunjukkan bahwa *input* pengguna belum divalidasi dengan baik, yang dapat membuka peluang eksploitasi melalui injeksi atau manipulasi DOM. Oleh karena itu, diperlukan tindakan perbaikan segera terhadap celah-celah ini guna meningkatkan keamanan dan keandalan sistem *e-learning* ILMU2 secara keseluruhan.

Maka dari itu Tabel 2. menampilkan hasil *Alert Detail* yang berisi solusi dengan tujuan agar dapat digunakan untuk mengurangi risiko dari masing-masing ancaman yang terdeteksi oleh OWASP ZAP.

Tabel 2. *Alert Detail*

Alert Name	***Risk Level***	**Rekomendasi Solusi**
Content Security Policy (CSP) Header Not Set	*High*	Tambahkan header *Content-Security-Policy* untuk membatasi sumber konten dan mencegah serangan XSS
Hidden File Found	*High*	Hapus atau lindungi file tersembunyi dari akses publik dan batasi direktori dengan konfigurasi *server*
Server Leaks Version Information via "Server" HTTP Header	*High*	Hapus atau sembunyikan *header* versi *server* dari respons HTTP untuk menghindari *fingerprinting* oleh penyerang

Strict Transport Security Header Not Set	*High*	Tambahkan *header Strict-Transport-Security* untuk memaksa koneksi HTTPS dan mencegah serangan *downgrade*
Authentication Request Identified	*High*	Gunakan koneksi HTTPS untuk semua permintaan autentikasi dan lindungi data kredensial dari pengintaian
GET for POST	*High*	Gunakan metode HTTP yang sesuai (POST) untuk permintaan yang mengubah data, dan batasi akses melalui konfigurasi *server*
SQL Injection	*Medium*	Validasi semua *input* pengguna dan gunakan *prepared statements* atau ORM untuk mencegah injeksi SQL
SQL Injection - SQLite	*Medium*	Gunakan *parameterized queries* khusus SQLite dan sanitasi *input* pengguna sebelum diproses ke *database*
Big Redirect Detected	*Medium*	Periksa dan batasi penggunaan *redirect*, serta pastikan tidak mengarah ke *domain* luar yang tidak terpercaya
Cookie with SameSite Attribute None	*Medium*	Tambahkan atribut *SameSite=Strict* atau *Lax* pada *cookie* untuk mencegah pengiriman lintas situs
Cross-Domain JavaScript Source File Inclusion	*Medium*	Hindari memuat skrip dari *domain* yang tidak terpercaya dan gunakan CSP untuk mengontrol sumber eksternal
X-Content-Type-Options Header Missing	*Medium*	Tambahkan *header X-Content-Type-Options: nosniff* untuk mencegah *browser* menebak tipe konten
Modern Web Application	*Medium*	Informasi ini bersifat informatif pastikan *framework modern* yang digunakan dikonfigurasi dengan benar
Session Management Response Identified	*Medium*	Implementasikan pengelolaan sesi yang aman dengan *session* ID yang dienkripsi dan rotasi ID secara berkala
User Agent Fuzzer	*Medium*	Gunakan *firewall* aplikasi web (WAF) dan deteksi aktivitas *fuzzer* secara dini dengan *rate limiting* dan *logging*
Absence of Anti-CSRF Tokens	*Low*	Tambahkan token CSRF pada semua *form* dan validasi token tersebut di sisi *server* untuk mencegah serangan pemalsuan permintaan

Timestamp Disclosure - Unix	*Low*	Hindari menampilkan *timestamp* Unix secara langsung dalam respon, terutama jika berkaitan dengan sistem internal
Information Disclosure - Suspicious Comment	*Low*	Hapus komentar HTML atau kode yang bersifat sensitif atau mengandung informasi *internal* dari *output* halaman
Re-examine Cache-control Directive	*Low*	Pastikan penggunaan *header cache* tidak menyebabkan penyimpanan data sensitif di *browser* pengguna atau *proxy* publik
User Controllable HTML Element Attribute (Potential XSS)	*Low*	Validasi dan sanitasi *input* pengguna untuk mencegah manipulasi elemen HTML dan potensi XSS.

Dari pengujian yang dilakukan pada *website e-learning* ILMU2, diperoleh sejumlah rekomendasi solusi yang dapat diterapkan untuk mencegah berbagai kerentanan yang terdeteksi. Seperti yang ditampilkan pada Tabel 2. solusi tersebut mencakup langkah-langkah teknis yang merujuk pada praktik keamanan *website*. Diharapkan nantinya hasil pengujian terhadap efektivitas solusi dapat dilakukan oleh *administrator* sistem yang memiliki akses penuh terhadap konfigurasi dan kode sumber *website* untuk meningkatkan keamanan dan kenyamanan pengguna dalam menggunakan *website* secara aman.

Beberapa solusi penting yang direkomendasikan antara lain adalah penambahan *header* keamanan seperti *Content-Security-Policy, Strict-Transport-Security,* dan *X-Content-Type-Options* untuk mengurangi risiko serangan XSS, *man-in-the-middle*, serta *content sniffing*. Selain itu, sistem disarankan untuk menyembunyikan informasi versi *server* guna mencegah *fingerprinting* oleh penyerang. Dalam hal pengelolaan *input* dan sesi pengguna, penggunaan *prepared statements* untuk mencegah *SQL injection*, validasi *input* secara ketat, serta implementasi token anti-CSRF merupakan langkah penting dalam memperkuat keamanan pada bagian autentikasi dan data pengguna. Dengan menerapkan solusi-solusi tersebut, diharapkan sistem *e-learning* ILMU2 dapat lebih terlindungi dari potensi eksploitasi yang bersumber dari kerentanan aplikasi *website*. Maka dari itu, kolaborasi antara pihak penguji dan *administrator* sistem sangat diperlukan agar mitigasi risiko dapat diimplementasikan secara optimal dan berkelanjutan.

5. KESIMPULAN DAN SARAN

Pengujian *e-learning* ILMU2 milik UPN "Veteran" Jawa Timur dilakukan untuk melakukan analisis keamanan terhadap *website* ILMU2 UPN "Veteran" Jawa Timur dengan menggunakan metode pengujian OWASP ZAP. Hasil pengujian keamanan terhadap *website e-learning* ILMU2 menunjukkan bahwa sistem masih memiliki sejumlah kerentanan yang signifikan. Berdasarkan laporan hasil scanning OWASP ZAP, terdeteksi sebanyak 20 jenis *alert* dengan rincian 6 risiko tinggi (*high*), 8 risiko sedang (*medium*), dan 6 risiko rendah (*low*). Jumlah *instance* yang tinggi seperti *Strict Transport Security Header Not Set* (636) dan *Server Leaks Version Information* (1236) menunjukkan lemahnya penerapan standar keamanan dasar. Temuan ini menandakan perlunya perbaikan menyeluruh untuk melindungi sistem dari potensi serangan seperti XSS, MITM, dan SQL injection.

Berdasarkan hasil pengujian dan analisis risiko, disarankan agar pihak pengelola sistem *e-learning* ILMU2 segera melakukan penanganan terhadap kerentanan yang ditemukan, dimulai dari risiko tinggi sebagai prioritas utama. Penerapan solusi yang telah dirinci dalam Tabel 2, seperti penambahan header keamanan (*Content-Security-Policy*, *Strict-Transport-Security*, dan *X-Content-Type-Options*), penyembunyian informasi versi server, serta penggunaan *prepared statements*, validasi *input*, dan token anti-CSRF, sangat penting untuk dilakukan. Langkah ini diharapkan dapat meningkatkan keamanan dan keandalan sistem *e-learning* ILMU2 secara berkelanjutan.

DAFTAR REFERENSI

Alshamrani, A., Alwan, M., & Shafie, A. (2020). Security threats and countermeasures in e-learning systems. Journal of Information Security Research, 12(2), 103–112.

Bator, R. J., Bryan, A. D., & Schultz, P. W. (2011). Who gives a hoot?: Intercept surveys of litterers and disposers. Environment and Behavior, 43(3), 295–315. https://doi.org/10.1177/0013916509356884

Hasan, H. H., & Nasihin, H. (2023). Efektivitas pemanfaatan media e-learning dalam pembelajaran fiqih kelas VIII di SMP IT Nur Hidayah Surakarta. Attractive: Innovative Education Journal, 5(2), 505–513.

Hidayati, S. N. (2016). Pengaruh pendekatan keras dan lunak pemimpin organisasi terhadap kepuasan kerja dan potensi mogok kerja karyawan. Jurnal Maksipreneur: Manajemen, Koperasi, dan Entrepreneurship, 5(2), 57–66. http://dx.doi.org/10.30588/SOSHUMDIK.v5i2.164

Kaur, J., & Kaur, A. (2021). OWASP ZAP based vulnerability detection of web applications. Journal of Web Engineering and Technology, 18(4), 245–254.

Kuncoro, A. W. (2022). Analisis metode Open Web Application Security Project (OWASP) pada pengujian keamanan website: Literature review. AUTOMATA, 3(1), 1–5.

Kusuma, G. (2022). Implementasi OWASP ZAP untuk pengujian keamanan sistem informasi akademik. Jurnal Teknologi Informasi: Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika, 16(2), 178–186.

Mohammed, A. A., Al-Khafaji, A. J., & Mahdi, D. S. (2022). Cybersecurity vulnerabilities in educational web applications: A case study. International Journal of Computer Applications, 184(3), 15–22.

Nasihin, H., Efendi, R., & Salmiyatun, S. (2020). Pemanfaatan Facebook sebagai media pembelajaran Pendidikan Agama Islam pada masa pandemi COVID-19. At-Turots: Jurnal Pendidikan Islam, 2(1), 23–37.

Nurdin, Salman, & Kadang, O. M. (2024). Pengujian kelemahan keamanan aplikasi web menggunakan peretasan etis. Prosiding Seminar Ilmiah Sistem Informasi dan Teknologi Informasi, 13(2), 234–243.

Nurlaili, I., & Hasanah, L. (2022). Analisis celah keamanan sistem informasi berbasis web menggunakan OWASP ZAP. Jurnal Ilmu Komputer dan Aplikasi, 14(3), 145–153.

Retnoningsih, E. (2017). Perbandingan Learning Management System Edmodo dan Moodle dalam pembelajaran online. Information System for Educators and Professionals, 1(2), 221–230.

Risdwiyanto, A., & Kurniyati, Y. (2015). Strategi pemasaran perguruan tinggi swasta di Kabupaten Sleman Yogyakarta berbasis rangsangan pemasaran. Jurnal Maksipreneur: Manajemen, Koperasi, dan Entrepreneurship, 5(1), 1–23. http://dx.doi.org/10.30588/SOSHUMDIK.v5i1.142

Sari, M. D., & Prasetyo, R. B. (2021). Evaluasi keamanan sistem informasi akademik menggunakan OWASP. Jurnal Teknologi Informasi dan Ilmu Komputer, 8(2), 220–228.

Sugara, V. I., & Sriyasa, I. W. (2024). Analisis keamanan website e-learning menggunakan OWASP ZAP. Jurnal Teknologi dan Keamanan Siber, 9(1), 25–34.

Yulianto, R., & Hidayat, R. (2020). Implementasi penetration testing pada website akademik berbasis OWASP ZAP. Prosiding SNATIF, 7(1), 98–103.