e-ISSN: 2987-1891
Available online at
http://pcinformatika.org/index.php/pcif/index
Journal on Pustaka Cendekia Informatika
Volume 3 No. 1, Februari-Mei 2025, pp 125-132

Analisis Kerentanan Web Menggunakan ZAP oleh *Checkmarx* pada Situs Kuliah Daring LMS Universitas Kebangsaan Republik Indonesia

Mughni Al Muzaki[1*], Reksi Zender Perdian[2], Rohman Fajar[3], Saripah[4], Syifa Khofifah[5], Subhanjaya Angga Atmaja[6]

[1,2,3,4,5] Program Studi Teknik Informatika, Fakultas Ilmu Komputer dan Sistem Informasi, Universitas Kebangsaan Republik Indonesia, Jl. Terusan Halimun No.37, Lkr. Sel., Kec. Lengkong, Kota Bandung, Jawa Barat, Indonesia.
E-mail: Mughnialmuzaki74@gmail.com
* Corresponding Author

https://doi.org/10.70292/pctif.v3i1.63

ARTICLE INFO

Article history
Received: 27 June 2025
Revised: 03 July 2025
Accepted: 09 July 2025

Kata Kunci
Keamanan Aplikasi Web, ZAP, OWASP, Kerentanan Sistem, Pembelajaran Daring, Analisis Keamanan, Checkmarx.

Keywords
Web Application Security, ZAP, OWASP, System Vulnerabilities, Online Learning, Security Analysis, Checkmarx.

ABSTRACT

Penelitian ini bertujuan untuk melakukan analisis keamanan pada situs kuliah daring tersebut dengan menggunakan alat ZAP (Zed Attack Proxy) versi 2.16.1, yang dikembangkan oleh OWASP dan didistribusikan oleh Checkmarx. Metode yang digunakan adalah pengujian black-box dengan pendekatan pemindaian aktif untuk mengidentifikasi celah keamanan yang mungkin dimiliki oleh aplikasi. Proses pemindaian dilakukan pada seluruh halaman utama dan sumber daya situs dengan memperhatikan berbagai aspek seperti header HTTP, manajemen sesi, penggunaan pustaka JavaScript, hingga konfigurasi keamanan lainnya. Hasil dari proses pemindaian menunjukkan terdapat 14 potensi kerentanan yang diklasifikasikan ke dalam empat kategori tingkat risiko, yaitu tinggi (1 temuan), sedang (4 temuan), rendah (6 temuan), dan informasional (3 temuan). Temuan paling signifikan adalah penggunaan pustaka JavaScript yang rentan (usang), tidak adanya kebijakan keamanan konten (Content Security Policy), serta kekurangan dalam penerapan header HTTP yang penting seperti X-Frame-Options, Strict-Transport-Security, dan X-Content-Type-Options. Selain itu, ditemukan pula kelemahan dalam atribut cookie dan penggunaan file JavaScript eksternal tanpa kontrol sumber yang memadai. Berdasarkan hasil tersebut, disusun serangkaian rekomendasi yang mengacu pada standar OWASP, termasuk pembaruan pustaka perangkat lunak, konfigurasi ulang header keamanan, penguatan manajemen sesi, dan penerapan kebijakan cache yang lebih aman.

This study aims to conduct a security analysis on the online lecture site using the ZAP (Zed Attack Proxy) tool version 2.16.1, developed by OWASP and distributed by Checkmarx. The method used is black-box testing with an active scanning approach to identify security vulnerabilities that may exist in the application. The scanning process was carried out on all main pages and site resources, paying attention to various aspects such as HTTP headers, session management, JavaScript library usage, and other security configurations. The results of the scanning process showed 14 potential vulnerabilities classified into four risk levels: high (1 finding), medium (4 finding), low (6 finding), and informational (3 finding). The most significant findings were the use of a vulnerable (outdated) JavaScript library, the absence of a content security policy (CSP), and deficiencies in the implementation of important HTTP headers such as X-Frame-Options, Strict-Transport-Security, and X-Content-Type-Options. In addition, weaknesses in cookie attributes and the use of external JavaScript files without adequate source control were also found. Based on these results, a series of recommendations were developed that adhere to OWASP standards, including updating software libraries, reconfiguring security headers, strengthening session management, and implementing more secure cache policies.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong berbagai sektor untuk bertransformasi secara digital, termasuk bidang pendidikan. Platform kuliah daring menjadi salah satu inovasi utama yang memungkinkan proses belajar-mengajar berlangsung secara fleksibel dan efisien tanpa harus bergantung pada pertemuan fisik. Sistem ini tidak hanya memberikan kemudahan akses kepada peserta didik dan pengajar, tetapi juga menyimpan berbagai data penting seperti identitas pengguna, catatan kehadiran, nilai, hingga materi pembelajaran. Namun demikian, digitalisasi ini membawa risiko baru dalam bentuk ancaman keamanan siber yang dapat mengganggu keberlangsungan sistem dan mengancam kerahasiaan data pengguna.

Keamanan aplikasi web menjadi aspek krusial dalam menjamin kerahasiaan, integritas, dan ketersediaan data yang dikelola oleh platform pembelajaran daring. Tanpa pengamanan yang memadai, kerentanan dalam sistem dapat dieksploitasi oleh pihak tidak bertanggung jawab. Oleh karena itu, penting untuk melakukan pengujian keamanan secara berkala menggunakan alat yang andal. Salah satu tools yang umum digunakan dalam praktik pengujian keamanan aplikasi web adalah ZAP (Zed Attack Proxy) dari OWASP, yang juga tersedia dalam distribusi dari Checkmarx.

Penelitian ini bertujuan untuk menganalisis tingkat keamanan situs https://uk.kuliahdaring.id dengan menggunakan ZAP versi 2.16.1 dari Checkmarx. Dengan melakukan pemindaian terhadap berbagai potensi kerentanan — seperti penggunaan library usang, absennya header keamanan, serta konfigurasi cookie yang tidak sesuai standar — diharapkan temuan ini dapat menjadi dasar dalam perbaikan sistem. Langkah ini penting untuk meningkatkan ketahanan situs terhadap serangan dan menjamin perlindungan data pengguna dalam ekosistem pembelajaran daring.

Keamanan Aplikasi Web

Keamanan aplikasi web adalah sekumpulan praktik dan teknologi yang bertujuan untuk melindungi sistem berbasis web dari berbagai ancaman siber, seperti peretasan, injeksi kode, pencurian data, dan serangan lainnya. Dalam konteks pendidikan daring, pentingnya keamanan web semakin tinggi mengingat aplikasi sering kali menyimpan data pribadi pengguna seperti nama, alamat surel, nilai akademik, dan informasi login. Menurut OWASP (Open Web Application Security Project), sebuah aplikasi web yang tidak memiliki mekanisme keamanan yang memadai dapat menjadi sasaran empuk bagi penyerang yang ingin mengeksploitasi celah yang ada. Untuk itu, pengembangan aplikasi web yang aman harus dimulai sejak tahap perancangan sistem, dengan mempertimbangkan ancaman yang mungkin terjadi dan cara pencegahannya.

OWASP Top 10

OWASP adalah organisasi nirlaba yang berfokus pada peningkatan keamanan perangkat lunak dan memberikan panduan dalam membangun aplikasi yang aman. Salah satu produk paling berpengaruh dari OWASP adalah daftar "OWASP Top 10", yang merupakan kompilasi dari sepuluh risiko keamanan paling umum yang sering ditemukan pada aplikasi web. Versi terkini dari daftar ini (OWASP Top 10 Tahun 2021) mencakup beberapa jenis kerentanan utama seperti kegagalan kontrol akses, kesalahan dalam penggunaan kriptografi, serangan injeksi, desain yang tidak aman, serta komponen perangkat lunak yang rentan atau usang. Dalam konteks penelitian ini, perhatian utama diberikan pada kerentanan akibat penggunaan komponen atau library yang sudah usang (A06: Vulnerable and Outdated Components), karena hal ini sering ditemukan pada situs web yang belum memperbarui dependensi mereka secara berkala.

Zed Attack Proxy (ZAP)

ZAP (Zed Attack Proxy) adalah salah satu alat keamanan open-source yang dikembangkan oleh OWASP dan secara luas digunakan untuk menguji keamanan aplikasi web. Alat ini bekerja dengan cara bertindak sebagai proxy antara browser dan server, sehingga memungkinkan pengguna untuk menganalisis lalu lintas jaringan dan mendeteksi kerentanan secara pasif maupun aktif. ZAP memiliki berbagai fitur seperti pemindaian otomatis terhadap kerentanan (active scan), pemindaian pasif terhadap konten dan respons (passive scan), pemetaan struktur situs melalui spidering, serta pembuatan laporan hasil pemindaian dalam berbagai format seperti PDF atau HTML. Keunggulan utama dari ZAP terletak pada kemudahan penggunaannya, fleksibilitasnya untuk pemula maupun profesional, serta sifatnya yang gratis dan bersumber terbuka, sehingga dapat diakses secara luas oleh berbagai kalangan.

Header Keamanan Web

ISSN 2987-1891 (online)

Header HTTP merupakan bagian dari komunikasi antara klien (biasanya browser) dan server, yang dapat digunakan untuk mengatur berbagai aspek dari perilaku dan keamanan aplikasi web. Beberapa header keamanan penting meliputi Content-Security-Policy (CSP), Strict-Transport-Security (HSTS), X-Frame-Options, dan X-Content-Type-Options. CSP digunakan untuk mengatur sumber daya yang dapat dimuat oleh halaman web dan sangat efektif dalam mencegah serangan Cross-Site Scripting (XSS). HSTS memastikan bahwa semua koneksi ke server hanya dilakukan melalui protokol HTTPS, sehingga mencegah serangan downgrade atau penyadapan data. Sementara itu, X-Frame-Options mencegah halaman ditampilkan dalam bingkai (frame) yang dapat dimanfaatkan dalam serangan clickjacking. X-Content-Type-Options digunakan untuk mencegah browser menebak tipe konten yang salah, yang bisa membuka celah bagi serangan MIME-sniffing. Penerapan header-header ini dapat secara signifikan meningkatkan tingkat keamanan aplikasi web.

Library JavaScript dan Kerentanannya

Penggunaan pustaka JavaScript pihak ketiga seperti jQuery, Bootstrap, atau DataTables sangat umum dalam pengembangan aplikasi web modern karena dapat mempercepat proses pengembangan dan menyediakan fungsionalitas yang kompleks dengan mudah. Namun, pustaka-pustaka ini juga dapat menjadi sumber kerentanan apabila digunakan dalam versi yang sudah lama dan belum mendapatkan pembaruan keamanan. Library yang rentan dapat memungkinkan penyerang menyisipkan kode berbahaya, mencuri data, atau memanipulasi fungsi aplikasi. Oleh karena itu, pengembang harus secara berkala memeriksa daftar dependensi proyek mereka, memastikan semua pustaka berada pada versi terbaru, dan menghindari penggunaan pustaka dari sumber yang tidak terpercaya. Alat bantu seperti Retire.js dan Snyk dapat digunakan untuk mendeteksi library yang sudah usang dan memberikan informasi mengenai risiko keamanannya.

Cookie dan Pengelolaannya

Cookie adalah data kecil yang dikirim dari situs web dan disimpan di perangkat pengguna, biasanya untuk menyimpan sesi login atau preferensi pengguna. Namun, jika cookie tidak dikelola dengan aman, ia dapat menjadi pintu masuk bagi serangan seperti pencurian sesi (session hijacking) dan serangan lintas situs (CSRF). Beberapa atribut penting yang harus ditetapkan pada cookie untuk meningkatkan keamanannya adalah HttpOnly, Secure, dan SameSite. Atribut HttpOnly memastikan bahwa cookie tidak dapat diakses melalui skrip JavaScript, sehingga mengurangi risiko pencurian melalui XSS. Atribut Secure memastikan cookie hanya dikirimkan melalui koneksi HTTPS, sedangkan SameSite membatasi pengiriman cookie lintas domain yang sangat berguna dalam mencegah serangan CSRF. Konfigurasi cookie yang tidak tepat dapat mengakibatkan kebocoran informasi atau akses tidak sah ke akun pengguna.

Cache-Control dan Privasi Data

Cache-control adalah mekanisme pengaturan penyimpanan data di sisi klien, seperti di browser atau proxy. Dalam konteks aplikasi web yang menangani informasi sensitif, seperti aplikasi pembelajaran daring, pengaturan cache menjadi sangat penting agar data tidak disimpan dalam perangkat pengguna secara tidak aman. Header Cache-Control dapat digunakan untuk menentukan apakah konten boleh disimpan, berapa lama disimpan, dan oleh siapa. Untuk informasi yang bersifat rahasia atau pribadi, pengembang disarankan menggunakan pengaturan seperti "no-store" atau "no-cache" yang akan mencegah browser menyimpan salinan halaman secara lokal. Jika tidak diatur dengan benar, informasi yang seharusnya bersifat pribadi bisa tetap tersedia bahkan setelah pengguna keluar dari aplikasi, terutama ketika perangkat digunakan secara bersama.

METODE

Jenis dan Pendekata Penelitian

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan tujuan utama menggambarkan dan menganalisis kondisi keamanan dari situs web kuliah daring yang menjadi objek studi. Pendekatan deskriptif kualitatif dipilih karena memungkinkan peneliti untuk memperoleh pemahaman mendalam terkait berbagai jenis kerentanan yang ditemukan melalui pemindaian keamanan, serta mampu memberikan gambaran komprehensif tentang tingkat risiko dan dampak potensialnya. Selain itu, metode ini memberikan ruang bagi interpretasi hasil yang relevan dengan konteks keamanan siber saat ini. Penelitian ini juga digolongkan sebagai studi kasus, di mana analisis fokus pada satu objek

spesifik yaitu situs kuliah daring milik institusi pendidikan, sehingga hasilnya dapat memberikan insight khusus yang aplikatif bagi pengelola situs tersebut.

Objek Penelitian

Objek penelitian yang menjadi fokus adalah situs web pembelajaran daring dengan alamat domain https://uk.kuliahdaring.id. Situs ini merupakan platform utama yang digunakan dalam proses pembelajaran digital yang melibatkan mahasiswa, dosen, dan staf administrasi. Keberadaan situs ini sangat strategis karena menyimpan data-data sensitif seperti informasi identitas mahasiswa, nilai akademik, materi kuliah, serta riwayat aktivitas pengguna. Mengingat pentingnya fungsi dan data yang diolah, keamanan situs ini harus dipastikan agar tidak terjadi kebocoran data atau penyalahgunaan oleh pihak-pihak yang tidak bertanggung jawab. Oleh karena itu, analisis keamanan secara menyeluruh terhadap situs ini menjadi hal yang krusial untuk menjaga integritas, kerahasiaan, dan ketersediaan layanan pembelajaran daring.

Analisis Sistem

Analisis sistem dalam penelitian ini dilakukan untuk memahami secara menyeluruh tahapan pengujian keamanan terhadap situs web, dengan mengacu pada metode standard dalam penetration testing. Pendekatan ini mencakup empat tahap utama, yaitu footprinting, scanning dan enumeration, exploit, serta reporting. Tahapan ini dipilih karena memberikan alur yang sistematis dalam menemukan dan mengevaluasi kerentanan sistem. Footprinting digunakan untuk mengumpulkan informasi awal tentang sistem target, seperti IP dan port aktif, dengan tools seperti Nmap atau Angry IP Scanner. Selanjutnya, scanning dan enumeration dilakukan menggunakan ZAP atau OpenVAS untuk mendeteksi kelemahan spesifik. Tahap exploit menguji apakah celah yang ditemukan dapat dimanfaatkan, sementara reporting berfungsi menyusun hasil temuan secara rinci baik melalui laporan otomatis dari ZAP maupun pencatatan manual. Pendekatan ini memungkinkan peneliti untuk tidak hanya mengidentifikasi risiko, tetapi juga memberikan rekomendasi perbaikan yang relevan.

Tabel 1. Tahapan yang digunakan dalam penelitian

NO	STEP (METODE)	TOOLS
1.	Footprinting	Nmap atau Angry IP Scanner
2.	Scanning Fingerprinting And Enumeration	OpenVas atau ZAP
3.	Exploit	Bypass
4.	Reporting	ZAP & Manual

Alat dan Bahan Penelitian

Untuk mendukung proses pemindaian keamanan, penelitian ini menggunakan perangkat lunak ZAP (Zed Attack Proxy) versi 2.16.1 yang merupakan produk open-source dari OWASP. ZAP dipilih karena kemampuannya yang lengkap dalam melakukan pemindaian keamanan baik secara pasif (passive scan) maupun aktif (active scan), serta mudah diintegrasikan dengan browser untuk memonitor dan mengintervensi lalu lintas data. Selain itu, browser Mozilla Firefox digunakan sebagai media pengakses situs secara manual selama pengujian, untuk memastikan interaksi yang real-time dan pengambilan data lengkap. Seluruh aktivitas dilakukan pada lingkungan sistem operasi Windows 11, yang menjadi platform utama dalam penelitian ini, menjamin kestabilan dan kompatibilitas alat yang digunakan.

Teknik Pengumpulan Data

Pengumpulan data dilakukan dengan metode pemindaian keamanan berbasis alat (tool-based security scanning), yang terbagi menjadi dua jenis utama:

1. Passive Scan: Pada tahap ini, ZAP hanya mengamati lalu lintas HTTP/HTTPS yang terjadi antara browser dan server tanpa melakukan perubahan atau injeksi data apapun. Tujuannya adalah untuk mengidentifikasi masalah keamanan yang muncul secara inheren seperti tidak adanya header keamanan, penggunaan cookie tanpa atribut proteksi, atau kebocoran informasi dalam respon server. Pendekatan ini minim risiko dan memberikan gambaran awal mengenai kondisi keamanan situs.
2. Active Scan: Setelah pemindaian pasif, dilakukan pemindaian aktif yang bersifat lebih agresif dengan mengirimkan permintaan-permintaan manipulatif (payload testing) kepada server. Teknik ini bertujuan mengidentifikasi kerentanan yang lebih kompleks seperti Cross-Site Scripting (XSS), SQL Injection, dan kelemahan pada otentikasi atau otorisasi yang mungkin tidak terlihat dalam

ISSN 2987-1891 (online)

pemindaian pasif. Active scan memberikan gambaran mendalam tentang potensi eksploitasi yang dapat dilakukan oleh penyerang.

Seluruh hasil pemindaian kemudian disimpan dalam bentuk laporan oleh ZAP, yang akan dianalisis lebih lanjut dengan klasifikasi tingkat risiko (tinggi, sedang, rendah, dan informasional) dan tingkat kepercayaan, serta merujuk pada standar keamanan OWASP Top 10.

Prosedur Penelitian

Langkah-langkah pelaksanaan penelitian ini dirancang secara sistematis sebagai berikut:

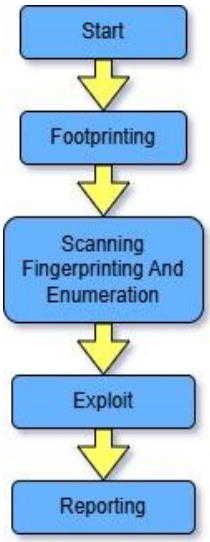
1. Menetapkan objek penelitian yakni situs https://uk.kuliahdaring.id sebagai target pengujian keamanan.
2. Mengunduh, menginstal, dan mengonfigurasi perangkat lunak ZAP versi 2.16.1 pada lingkungan Windows 11.
3. Mengintegrasikan ZAP sebagai proxy pada browser Mozilla Firefox untuk dapat memonitor dan mengontrol lalu lintas data antara browser dan server.
4. Melakukan pengamatan awal dengan melakukan navigasi manual pada situs untuk memastikan semua fitur dapat diakses dan terdeteksi oleh ZAP.
5. Melaksanakan Passive Scan dengan membiarkan ZAP merekam seluruh komunikasi data tanpa intervensi aktif.
6. Melakukan Active Scan dengan menggunakan fitur otomatis pada ZAP untuk mengirimkan payload uji ke berbagai titik input pada situs.
7. Mengekspor hasil pemindaian ke dalam laporan dan melakukan analisis terhadap temuan berdasarkan tingkat risiko dan referensi OWASP.
8. Mengklasifikasikan dan mengelompokkan kerentanan berdasarkan jenis dan dampaknya terhadap keamanan aplikasi.
9. Menyusun rekomendasi perbaikan yang relevan untuk meningkatkan ketahanan situs terhadap ancaman siber.
10. Menyusun laporan akhir penelitian berisi ringkasan hasil, pembahasan, rekomendasi, dan kesimpulan.

Validasi Data

Untuk memastikan validitas dan keakuratan data yang diperoleh, setiap temuan kerentanan yang dihasilkan oleh ZAP diverifikasi melalui beberapa cara:

1. Membandingkan hasil dengan dokumentasi resmi OWASP serta literatur keamanan terkini yang diakui secara internasional.
2. Melakukan pengecekan manual secara langsung pada elemen situs, seperti header HTTP, versi pustaka JavaScript, dan atribut cookie menggunakan developer tools pada browser.
3. Mengulangi pengujian pada beberapa waktu berbeda untuk memastikan konsistensi hasil.

Alur Pengujian

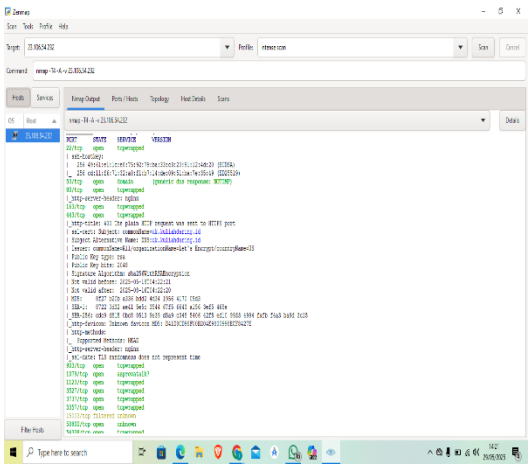


Gambar 1. Alur Pengujian

Alur pengujian keamanan sistem dilakukan secara sistematis dan berurutan untuk memastikan setiap potensi kerentanan dapat diidentifikasi dan dianalisis secara menyeluruh. Pengujian dimulai dari tahap awal pengumpulan informasi hingga penyusunan laporan akhir yang komprehensif. Setiap tahapan memiliki peran penting dalam membentuk pemahaman terhadap kondisi keamanan sistem secara keseluruhan. Proses ini bertujuan tidak hanya untuk menemukan kelemahan, tetapi juga untuk memberikan gambaran mengenai risiko yang mungkin ditimbulkan serta rekomendasi mitigasi yang tepat. Dengan mengikuti alur yang terstruktur, pengujian menjadi lebih terarah dan hasilnya dapat dijadikan acuan dalam perbaikan dan penguatan sistem keamanan.

HASIL DAN PEMBAHASAN

Footprinting



Gambar 2. *Footprinting*

Footprinting merupakan salah satu tahapan awal atau langkah pertama melakukan Penetration and Vulnerability Testing, dalam tahapan ini dimana penulis menggali informasi sebanyak mungkin mengenai target yang telah ditentukan. Seperti Whois, NSLookup, Mapping Network dan informasi lainnya yang dibutuhkan. Dalam tahapan ini penulis di bantu oleh berbagai macam tool software maupun tool online scanner untuk dapat melakukannya seperti tools NMAP dan Angry IP Scanner dan lain-lain.

Scanning Fingerprinting and Enumeration

Scanning Fingerprinting

Langkah scanning fingerprinting ini akan menggunakan tool ZAP dimana tool ini dapat digunakan pada sistem operasi windows, tool ini dapat menampilan dari suatu range IP Address, sebagai administrator tool ini akan membantu dalam menemukan vulnerability dalam jaringan (IP Address atau hostname). Selain menampilan kelemahan dari suatu source, tool ini akan menampilkan level tingkat kelemahan dari alerts (vulnerability) yang ditemukan

Enumeration

Langkah enumeration ini akan menggunakan NMAP Scanner di mana tool ini dapat menampilan detail dari suatu range IP Address, seperti port apa saja yang terbuka, terfilter atau tertutup dari suatu IP Address. Jadi, sebagai seorang tester, akan mendapatkan dan mengevaluasi port yang terbuka apakah port tersebut cocok dengan IP Address yang terkait. Dengan hasil enumeration juga langsung dilanjutkan ke arah scanning web vulnerability untuk mendapatkan seluruh informasi mengenai celah atau kerentanan apa saja yang didapat dari hasil scanning tersebut.

Langkah scaning yang akan dilakukan pada tahapan enumeration yakni dengan menggunakan Nmap Scanner yang dilakukan pada Operating System Kali Linux v.2- 2017, mengenai target yang akan discaning yakni dengan IP Address 23.106.54.232 alamat IP https://uk.kuliahdaring.id yang diberikan dari penyedia hosting dan 192.168.10.100 alamat IP Address server utama di Universitas Kebangsaan Republik Indonesia mengenai penjelasan hasil scaning dapat dilihat pada gambar 4.2 diatas. Nmap sendiri akan melakukan pemindaian untuk membedakan port yang terbuka dengan port yang disaring (filtered) dari Ip Addres 23.106.54.232 dapat disimpulkan bahwa IP tersebut ialah IP Server yang digunakan oleh Universitas Kebangsaan Republik Indonesia, dan jenis OS (Operating System) yang digunakan ialah operating system windows 11, DBMS (Database Management System) yang digunakan

ISSN 2987-1891 (online)

MySQL, server Apache versi.2.2.6 disistem operating windows 32bit dan menggunakan SSL OpenSLL versi.0.9.8, dengan kondisi port dan service yang semuanya terbuka (open) seperti port 80, 135, 443, 445, 1688, 3306, 8082, hingga 49157 tanpa diterapkan pengamanan dengan cara memfilter.

Reporting

Berdasarkan hasil pemindaian menggunakan ZAP (Zed Attack Proxy) terhadap sistem informasi akademik Universitas Kebangsaan Republik Indonesia, ditemukan sebanyak 14 kerentanan dengan tingkat risiko yang bervariasi, mulai dari tingkat informasional, rendah, sedang, hingga tinggi. Kerentanan tersebut meliputi penggunaan pustaka JavaScript yang telah usang dan rentan, absennya header keamanan seperti Content Security Policy (CSP) dan Strict-Transport-Security (HSTS), serta pengaturan atribut cookie yang belum optimal. Selain itu, hasil pengujian menunjukkan bahwa tidak ditemukan adanya celah SQL Injection, yang menandakan bahwa sistem telah memiliki validasi input dasar yang cukup baik pada sisi aplikasi. Meskipun demikian, selama proses pemindaian, teridentifikasi beberapa port terbuka dan endpoint yang dapat diakses dari luar, yang berpotensi dimanfaatkan oleh pihak tidak bertanggung jawab jika tidak dikonfigurasi dengan benar. Oleh karena itu, diperlukan langkah mitigasi lanjutan untuk memperkuat konfigurasi server dan menutup celah-celah yang teridentifikasi.

SIMPULAN

Berdasarkan hasil pengujian keamanan terhadap situs https://uk.kuliahdaring.id menggunakan alat bantu ZAP (Zed Attack Proxy) versi 2.16.1, ditemukan sejumlah kerentanan keamanan yang tersebar dalam beberapa tingkat risiko. Dari total 14 temuan, kerentanan diklasifikasikan menjadi 1 risiko tinggi, 4 risiko sedang, 6 risiko rendah, dan 3 temuan informasional. Temuan ini mengindikasikan bahwa meskipun situs sudah memiliki beberapa mekanisme keamanan, masih terdapat celah yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab jika tidak segera ditangani.

Salah satu kerentanan dengan tingkat risiko tinggi adalah penggunaan pustaka JavaScript yang sudah usang, yaitu jquery.dataTables.js. Penggunaan pustaka yang rentan dapat menjadi pintu masuk eksploitasi apabila tidak diperbarui ke versi terbaru. Selain itu, beberapa kelemahan lainnya termasuk tidak diterapkannya header keamanan penting seperti Content Security Policy (CSP), X-Frame-Options, Strict-Transport-Security (HSTS), dan X-Content-Type-Options. Header-header ini merupakan bagian penting dari praktik pengamanan modern karena mampu mencegah serangan seperti clickjacking, downgrade attack, dan MIME sniffing.

Adapun kerentanan tingkat rendah juga menunjukkan bahwa cookie yang digunakan belum disertai dengan atribut keamanan seperti HttpOnly, Secure, dan SameSite, yang seharusnya diimplementasikan untuk melindungi sesi pengguna dari serangan pencurian atau manipulasi. Temuan informasional seperti adanya komentar mencurigakan dalam kode, cache-control yang lemah, dan pengelolaan sesi yang teridentifikasi juga merupakan hal penting yang patut menjadi perhatian demi menjaga integritas sistem secara menyeluruh.

Secara keseluruhan, pengujian ini berhasil mengungkap aspek-aspek penting yang perlu diperbaiki dan ditingkatkan guna mencegah risiko kebocoran data dan meningkatkan ketahanan aplikasi terhadap serangan siber.

Berdasarkan kesimpulan tersebut, penulis memberikan beberapa saran untuk pengelola sistem maupun tim pengembang situs agar dapat meningkatkan keamanan aplikasi secara menyeluruh:

1. Segera perbarui seluruh pustaka eksternal JavaScript yang digunakan, khususnya pustaka yang diketahui memiliki kerentanan seperti jQuery DataTables, agar tidak menjadi titik masuk bagi eksploitasi.
2. Terapkan header keamanan penting seperti Content Security Policy (CSP), X-Frame-Options, Strict-Transport-Security (HSTS), dan X-Content-Type-Options untuk memperkuat kontrol terhadap konten dan melindungi pengguna dari berbagai jenis serangan.
3. Tambahkan atribut keamanan pada seluruh cookie, seperti Secure, HttpOnly, dan SameSite, untuk mencegah pencurian sesi dan menjaga kerahasiaan informasi pengguna.
4. Lakukan audit berkala terhadap file JavaScript eksternal yang dimuat dari domain pihak ketiga agar memastikan file tersebut tidak mengalami manipulasi atau perubahan berbahaya.
5. Bersihkan kode sumber dari komentar-komentar yang mengandung informasi teknis sensitif dan sesuaikan kebijakan cache-control agar data penting tidak tersimpan di sisi klien.

6. Lakukan pengujian penetrasi (penetration testing) secara rutin menggunakan berbagai alat bantu seperti ZAP, Acunetix, atau Burp Suite sebagai upaya pencegahan terhadap kerentanan baru yang mungkin muncul seiring waktu.

Dengan memperhatikan dan menindaklanjuti saran-saran tersebut, diharapkan sistem informasi yang digunakan dalam situs kuliah daring dapat lebih terlindungi dari ancaman keamanan siber yang terus berkembang.

UCAPAN TERIMA KASIH

Peneliti menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan dan kontribusi dalam pelaksanaan penelitian serta penyusunan artikel ini.

REFERENSI

13.+Abdul+Fattah+Hasibuan+141-154. (n.d.).

Ariyadi, T., Langgeng Widodo, T., Apriyanti, N., & Sasti Kirana, F. (n.d.). *Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP Analysis of Bina Darma University Academic Information System Security Vulnerabilities Using the OWASP* (Vol. 22, Issue 2).

Cahyani, D. D., Putu, L., Dewi, W. P., Dika, K., Suryadi, R., Made, I., & Listartha, E. (2021). Analisis Kerentanan Website Smp Negeri 3 Semarapura Menggunakan Metode Pengujian Rate Limiting Dan Owasp. *INSERT: Information System and Emerging Technology Journal*, *2*(2).

Dewangkara, I. B. I., Santi, K. S., Putri, V. A., & Listartha, I. M. E. (2022). Penerapan Analisis Kerentanan XSS dan Rate Limiting pada Situs Web MTsN 3 Negara Menggunakan OWASP ZAP. In *JURNAL INFORMATIKA UPGRIS* (Vol. 8, Issue 1). https://www.zaproxy.org/download/.

Edy Listartha, I. M., Premana Mitha, I. M. A., Aditya Arta, M. W., & Yuda Arimika, I. Km. W. (2022). Analisis Kerentanan Website SMA Negeri 2 Amlapura Menggunakan Metode OWASP (Open Web Application Security Project). *SIMKOM*, *7*(1), 23–27. https://doi.org/10.51717/simkom.v7i1.63

Kristianto, F., Rahman, S., Bahri, S., Studi Informatika, P., & KHARISMA Makassar, S. (2022). Analisis Kerentanan Pada Website Servio Menggunakan Acunetix Web Vulnerability. *JTRISTE*, *9*(1), 46–55. http://servio.store.

Kuncoro, A. W., Informatika, J., Rahma, F., & Jurusan Informatika, M. E. (n.d.). *Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review*. https://www.sciencedirect.com

Singasatia, D., Kom, M., Totohendarto, ; M Hafid, Si, S. M. M., Saputro, J., & Kom, S. (n.d.). *Penetration Testing Untuk Menguji Kerentanan Pada Sistem Informasi Akademik Di Sekolah Tinggi Teknologi Xyz*. http://www.IANA.org,

Wahidin, M., Rahayu, D. N., & Yulianto, R. M. (2024). Analisis Kerentanan Situs Web KopKar Syariah PT BSIN menggunakan OWASP Zed Attack Proxy. *Jurnal Interkom: Jurnal Publikasi Ilmiah Bidang Teknologi Informasi Dan Komunikasi*, *18*(4), 25–31. https://doi.org/10.35969/interkom.v18i4.321

Yunus, M. (2019). Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework Owasp Versi 4. *Jurnal Ilmiah Informatika Komputer*, *24*(1), 37–48. https://doi.org/10.35760/ik.2019.v24i1.1988

ISSN 2987-1891 (online)