ANALISIS KERENTANAN DAN PENGUATAN KEAMANAN WEBSITE MENGGUNAKAN METODOLOGI OPEN WEB APPLICATION SECURITY PROJECT (OWASP) PADA WEBSITE SISTEM INFORMASI MANAJEMEN XYZ

1st Hariz Husain
Direktorat Universitas Telkom Purwokerto
Universitas Telkom Purwokerto
harizhusain@student.telkomuniversity.ac.id

2nd Sandy Fernandez
Direktorat Universitas Telkom Purwokerto
Universitas Telkom Purwokerto
sandhyf@telkomuniversity.ac.id

***Abstrak* — Ancaman terhadap keamanan website milik instansi pemerintah terus meningkat, terutama karena masyarakat kini sangat bergantung pada layanan digital.Website Sistem InformasiXYZ Kabupaten xyz termasuk salah satu yang berpotensi mengalami serangan, seperti penyisipan konten ilegal dan kebocoran data sensitif. Permasalahan ini menunjukkan bahwa masih terdapat celah keamanan yang perlu segera diidentifikasi dan diperbaiki. Website pemerintah sering menjadi sasaran serangan siber karena menyimpan data penting dan digunakan oleh masyarakat luas. Pengelolaan keamanannya belum sepenuhnya maksimal, yang dapat berdampak pada terganggunya pelayanan publik. Solusi yang dilakukan adalah dengan menganalisis keamanan website menggunakan pendekatan OWASP, yaitu metode yang digunakan untuk mengidentifikasi sepuluh jenis kerentanan umum. Proses dilakukan melalui tahapan pengumpulan data, pemindaian kerentanan untuk mengetahui sejauh mana celah keamanan dapat dieksploitasi. Selain itu, penelitian ini juga memberikan rekomendasi teknis untuk menutup celah keamanan yang ditemukan. Hasil pengujian menunjukkan adanya kerentanan serius dan ditemukannya tujuh celah keamanan dengan risiko sedang hingga tinggi pada sistem, mencakup kelemahan Broken Access Control, Cryptographic Failures, Injection, Security Misconfiguration, Vulnerable and Outdated Components, Software and Data Integrity Failures, serta Identification and Authentication Failures. Rekomendasi mitigasi disusun untuk setiap kerentanan, seperti pembatasan akses direktori, penerapan HTTPS, validasi input, pembaruan komponen usang, dan penggunaan 2FA. Evaluasi menunjukkan bahwa penerapan langkah perbaikan tersebut dapat meningkatkan keamanan secara signifikan. Penelitian ini menjadi acuan penguatan keamanan siber bagi pengelola website pemerintahan.**

***Kata kunci*— keamanan website, OWASP, kerentanan siber, mitigasi, Kabupaten Xyz.**

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mengubah pola interaksi antara pemerintah dan masyarakat, menjadikan website sebagai media utama pelayanan publik. Website instansi pemerintah kini tidak hanya digunakan untuk menyampaikan informasi, tetapi juga menyediakan sistem manajemen internal, seperti layanan kepegawaian mencakup pengajuan cuti, kenaikan pangkat, dan pensiun. Namun, semakin tingginya pemanfaatan teknologi ini turut meningkatkan risiko serangan siber. Tercatat pada tahun 2022 terdapat lebih dari 100 juta insiden siber yang mengancam kerahasiaan dan integritas data publik [1].

Di Kabupaten XYZ, sejumlah website pemerintah mengalami masalah serius terkait keamanan. Salah satu contoh nyata adalah penyisipan iklan tidak sah ke dalam situs resmi. Hal ini menandakan lemahnya kontrol akses dan kurangnya pembaruan sistem, yang menjadikan website rentan terhadap eksploitasi. Selain itu, minimnya edukasi keamanan siber bagi pengelola dan pengguna memperbesar risiko serangan dan menurunkan kepercayaan publik terhadap layanan digital pemerintah. Menjawab tantangan tersebut, pendekatan sistematis berbasis standar internasional dibutuhkan untuk memperkuat keamanan web. Penelitian ini menerapkan metodologi Open Web Application Security Project (OWASP) untuk menganalisis kerentanan pada website Sistem Informasi XYZ. OWASP dipilih karena fleksibilitas dan panduan praktisnya dalam menghadapi ancaman khusus aplikasi web modern [2]. Dibandingkan kerangka kerja lain seperti PTES, yang lebih cocok untuk pengujian tingkat organisasi [3], atau OSSTMM yang terlalu kompleks untuk mitigasi aplikasi web [4], OWASP dinilai lebih efisien dan relevan.

Proses OWASP meliputi perencanaan, analisis kebutuhan, identifikasi kerentanan melalui information gathering dan eksploitasi, serta penyusunan rekomendasi dan penguatan sistem. Studi sebelumnya membuktikan efektivitas OWASP dalam mengidentifikasi celah keamanan pada situs Dinas Tenaga Kerja dan memberikan rekomendasi mitigasi. Kombinasi OWASP dengan metode PTES juga terbukti memperkuat keamanan secara menyeluruh pada website pemerintah Kabupaten XYZ [5].

Melalui penelitian ini, kelemahan seperti injeksi, autentikasi lemah, dan konfigurasi salah dapat diidentifikasi dan ditangani. Rekomendasi teknis seperti penggunaan

firewall aplikasi web, patching sistem, dan pembaruan reguler disampaikan guna meningkatkan integritas dan kerahasiaan data. Harapannya, penelitian ini mendorong kesadaran akan pentingnya keamanan web dan menjadi referensi penguatan sistem informasi pemerintahan daerah.

II. KAJIAN TEORI

A. Keamanan Website

Keamanan website adalah upaya untuk melindungi sistem, data, dan pengguna dari berbagai ancaman siber yang memanfaatkan celah atau kerentanan pada aplikasi web. Dalam konteks ini, keamanan tidak hanya mencakup perlindungan terhadap serangan langsung, tetapi juga mencakup penerapan standar, prosedur, dan teknologi untuk mencegah akses tidak sah, manipulasi data, atau kerusakan sistem. Salah satu pendekatan yang umum digunakan adalah OWASP (Open Web Application Security Project), yang menyediakan panduan terhadap sepuluh jenis kerentanan paling umum pada aplikasi web, seperti Injection dan Cross-Site Scripting (XSS), sehingga organisasi dapat mengidentifikasi, mengevaluasi, dan memperbaiki kelemahan sistem secara sistematis.

B. Konsep Dasar Kerentanan Website

Kerentanan website adalah kelemahan atau celah dalam desain, implementasi, atau konfigurasi sistem web yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan tindakan merugikan seperti pencurian data, perusakan sistem, atau gangguan layanan. Kerentanan ini dapat muncul dari berbagai aspek, seperti input pengguna yang tidak divalidasi, skrip berbahaya yang dapat disisipkan ke dalam halaman web, atau pengaturan keamanan server yang tidak tepat. Pentingnya memahami dan mengatasi kerentanan website terletak pada upaya melindungi integritas sistem dan data pengguna dari ancaman siber yang semakin kompleks. Dengan mengenali potensi celah sejak dini dan menerapkan langkah mitigasi yang tepat, organisasi tidak hanya dapat mengurangi risiko serangan, tetapi juga membangun kepercayaan pengguna terhadap keamanan dan keandalan sistem digital yang mereka kelola.

C. Pengembangan Website

Pengembangan website adalah proses merancang, membangun, dan memelihara situs web agar dapat berjalan sesuai fungsinya. Dalam konteks keamanan, pengembangan website mencakup penerapan praktik-praktik terbaik untuk mencegah kerentanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Pentingnya pengembangan website yang aman terletak pada perlindungan terhadap data pengguna, menjaga kestabilan layanan digital, dan membangun kepercayaan publik. Dengan meningkatnya serangan siber yang menyasar aplikasi web, pengembang dituntut untuk menerapkan standar keamanan seperti OWASP dan pendekatan Secure Software Development Lifecycle (S-SDLC) guna memastikan bahwa keamanan telah dipertimbangkan sejak tahap awal pengembangan. Hal ini menjadi krusial dalam menciptakan sistem yang tangguh terhadap ancaman serta mendukung keberlanjutan layanan digital yang andal dan terpercaya.

D. Open Web Application Security Project(OWASP)

OWASP (Open Web Application Security Project) adalah organisasi nirlaba global yang bertujuan meningkatkan keamanan perangkat lunak, khususnya aplikasi web, melalui penyediaan panduan, alat, dan sumber daya terbuka bagi pengembang, penguji, dan organisasi. Salah satu kontribusi utamanya adalah OWASP Top 10, yaitu daftar sepuluh jenis kerentanan paling kritis pada aplikasi web yang menjadi standar acuan internasional dalam praktik pengembangan aman. Pentingnya OWASP terletak pada perannya dalam membantu organisasi memahami, mengidentifikasi, dan mengurangi risiko keamanan siber melalui pendekatan yang sistematis dan terbuka. Dengan menerapkan prinsip-prinsip OWASP, seperti validasi input, penggunaan parameterized queries, dan pengujian otomatis menggunakan alat seperti OWASP ZAP, pengembang dapat membangun sistem yang lebih aman, menjaga kepercayaan pengguna, dan meminimalkan potensi kerugian akibat serangan siber.

III. METODE

Penelitian ini menyoroti keamanan website Sistem InformasiXYZ milik Pemerintah Kabupaten XYZ, yang berfungsi sebagai platform penyedia informasi dan layanan publik. Objek penelitian ini adalah sistem web itu sendiri, sementara subjeknya mencakup pengelola situs dan masyarakat sebagai pengguna. Pendekatan yang digunakan adalah metodologi Open Web Application Security Project (OWASP) untuk mendeteksi dan menilai celah keamanan. Melalui wawancara dan pengumpulan data dari para pengelola serta pengguna situs, penelitian ini bertujuan menggali pemahaman mengenai kebutuhan, kendala, dan pengalaman mereka dalam menggunakan serta mengelola website, khususnya dalam aspek perlindungan data dan keamanan sistem.

Pada tahap analisis kebutuhan, peneliti melakukan studi literatur sebagai dasar perumusan masalah, dengan menelaah teori, pendekatan, dan temuan dari berbagai sumber seperti buku, jurnal, dan laporan penelitian terdahulu. Langkah ini bertujuan untuk memahami konteks permasalahan secara luas serta menemukan celah pengetahuan yang belum banyak dikaji. Setelah pemetaan awal, peneliti merumuskan masalah dan menentukan pertanyaan penelitian yang spesifik, lalu menetapkan tujuan yang SMART—spesifik, terukur, relevan, dan berbatas waktu. Selain itu, ruang lingkup penelitian juga ditentukan untuk memastikan fokus dan efisiensi dalam proses penelitian.

Tahap selanjutnya adalah information gathering, yaitu proses pengumpulan data teknis sebanyak mungkin terkait sistem website, mulai dari informasi domain, alamat IP, struktur server, teknologi web, hingga konfigurasi CMS dan framework yang digunakan. Proses ini dilakukan melalui dua pendekatan: pasif (tanpa interaksi langsung) dan aktif (dengan teknik seperti pemindaian port dan deteksi teknologi). Data yang dikumpulkan digunakan untuk mengidentifikasi potensi kerentanan sistem seperti penggunaan versi perangkat lunak usang atau parameter input rentan terhadap serangan.

Setelah informasi teknis terkumpul, peneliti melanjutkan ke tahap eksploitasi, yaitu menguji kerentanan yang ditemukan dengan metode penetration testing untuk menilai dampaknya. Eksploitasi ini mengacu pada OWASP Top 10, termasuk isu seperti Injection, Broken Access Control, dan Security Misconfiguration. Hasil dari uji ini menjadi dasar dalam menyusun rekomendasi perbaikan sistem, dengan tujuan memperkuat pertahanan website terhadap potensi ancaman siber. Rekomendasi difokuskan pada pembaruan sistem, penerapan kontrol keamanan, dan peningkatan

monitoring untuk memastikan keamanan website secara menyeluruh dan berkelanjutan sesuai standar OWASP.

IV. HASIL DAN PEMBAHASAN

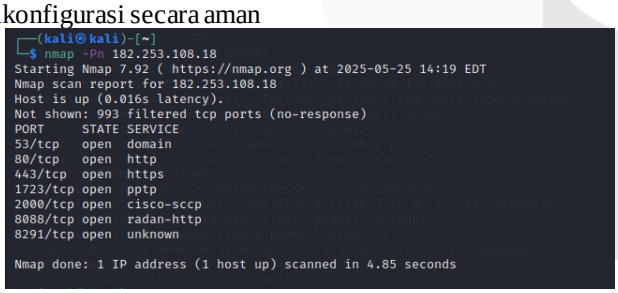
A. Information Gathering (Pengumpulan Informasi)

Tahapan awal dalam pengujian keamanan dilakukan dengan metode information gathering atau pengumpulan informasi, yang bertujuan untuk mengidentifikasi aset-aset digital, arsitektur layanan dari sistem informasi yang diuji, yaitu Sistem Informasi XYZ milik Sistem Informasi Manajemen XYZ.

Tahap awal pengujian keamanan dilakukan melalui analisis HTTP response header menggunakan WhatWeb pada subdomain utama Sistem Informasi Manajemen XYZ. Hasil analisis menunjukkan penggunaan Nginx/1.16.1 dan PHP/7.3.33 yang telah mencapai status End-of-Life sejak Desember 2021, serta konfigurasi cookie HttpOnly tanpa Secure yang berpotensi memungkinkan transmisi melalui HTTP. Meskipun beberapa pengaturan seperti cache-control telah sesuai standar keamanan, keberadaan komponen usang tetap menjadi potensi kerentanan.

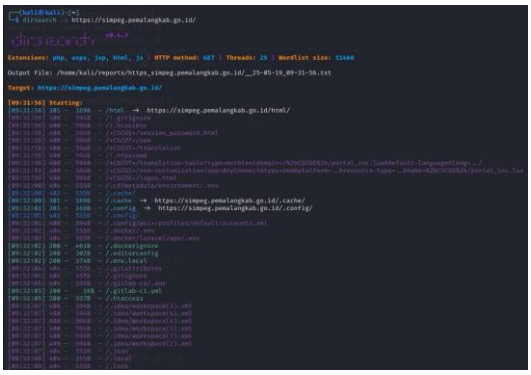
GAMBAR 1. Analisis header HTTP menggunakan WhatWeb

Selanjutnya, pemindaian port menggunakan Nmap mengidentifikasi beberapa port terbuka, antara lain 53 (DNS), 80 (HTTP), 443 (HTTPS), 1723 (PPTP VPN), 2000 (Cisco SCCP), 8000 (HTTP alternatif), dan 8291 (MikroTik Winbox). Port-port tersebut, khususnya yang bersifat administratif atau tidak digunakan secara publik, berisiko dimanfaatkan oleh pihak yang tidak berwenang jika tidak dikonfigurasi secara aman



GAMBAR 2. Pemindaian menggunakan Nmap

Tahap berikutnya adalah enumerasi direktori menggunakan Dirsearch untuk mengidentifikasi jalur dan file sensitif yang dapat diakses publik. Ditemukan beberapa file penting seperti .env.local, config.xml, .htaccess, serta direktori /docker dan /storage/ yang dapat diakses tanpa autentikasi. Temuan ini menunjukkan lemahnya pengendalian akses dan pengelolaan direktori, sehingga berpotensi membuka celah terhadap kebocoran informasi atau penyalahgunaan sistem.



GAMBAR 3. Proses pemindaian direktori

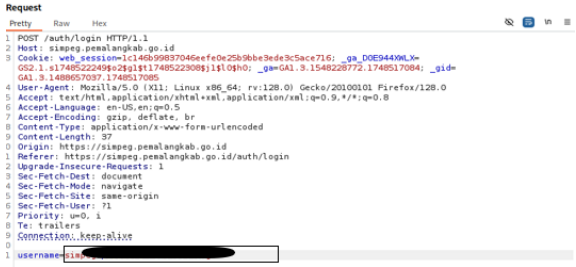
B. Eksploitasi Website Asli

Pendekatan OWASP diterapkan untuk mengidentifikasi celah umum dan berdampak pada website Sistem Informasi Manajemen XYZ. Pengujian menggunakan alat seperti OWASP ZAP, Dirsearch, dan Nmap, serta metode manual untuk validasi hasil.sssssssssss Pengujian keamanan pada Sistem Informasi Manajemen XYZ dilakukan dengan mengacu pada kerangka kerja OWASP Top 10.

A01 – Broken Access Control, di mana hasil enumerasi direktori menggunakan Dirsearch menunjukkan keberadaan file sensitif seperti .env yang dapat diakses publik tanpa autentikasi. Validasi melalui Burp Suite mengonfirmasi file tersebut berisi informasi kredensial basis data, kunci enkripsi aplikasi, serta secret key layanan eksternal. Kondisi ini membuktikan lemahnya pembatasan akses terhadap sumber daya internal, yang dapat dimanfaatkan untuk eskalasi serangan.

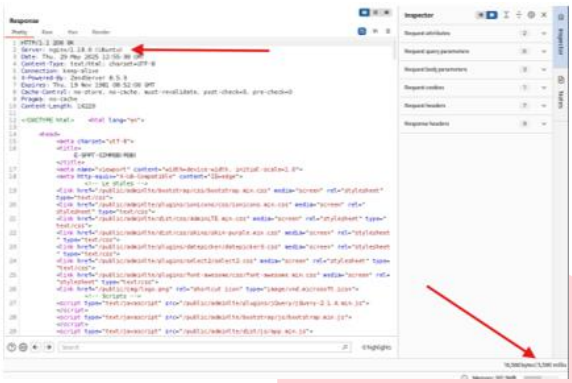
GAMBAR 4. Request proxy menggunakan Burpsuite.

A02 – Cryptographic Failures teridentifikasi dari analisis HTTP header dan konfigurasi cookie menggunakan WhatWeb dan Burp Suite. Ditemukan bahwa parameter kredensial dikirim dalam bentuk clear text melalui koneksi tidak terenkripsi (HTTP). Situasi ini memungkinkan terjadinya serangan Man-in-the-Middle maupun packet sniffing, sehingga pihak ketiga yang berada dalam jaringan yang sama dapat membaca data sensitif secara langsung.



Gambar 5. Hasil percobaan cryptographic failures.

A03 – Injection, pengujian blind SQL injection berbasis waktu dilakukan dengan menyisipkan payload pada parameter username. Respon server menunjukkan penundaan selama lima detik, menandakan perintah SQL dijalankan tanpa validasi input. Kerentanan ini memungkinkan penyerang membaca, memodifikasi, atau menghapus data dalam basis data secara tidak terdeteksi.

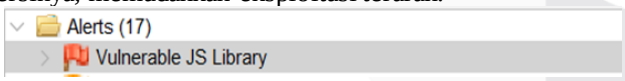


Gambar 6. Hasil serangan Blind SQL.

A04 – Security Misconfiguration diidentifikasi melalui pemindaian Nuclei yang menemukan absennya beberapa HTTP Security Headers penting, seperti Content-Security-Policy dan X-Frame-Options. Kekosongan ini memperbesar risiko terhadap Cross-Site Scripting (XSS), Clickjacking, serta data leakage.

Gambar 7. Deteksi konfigurasi header tidak aman menggunakan Nuclei

A05 – Vulnerable and Outdated Components, kombinasi pengujian OWASP ZAP, Nuclei, dan analisis manual terhadap file composer.lock mengungkap penggunaan pustaka usang seperti bacon/bacon-qr-code versi 2.0.8, yang memiliki riwayat kerentanan. Akses publik ke composer.lock memungkinkan penyerang mengetahui daftar pustaka dan versinya, memudahkan eksploitasi terarah.

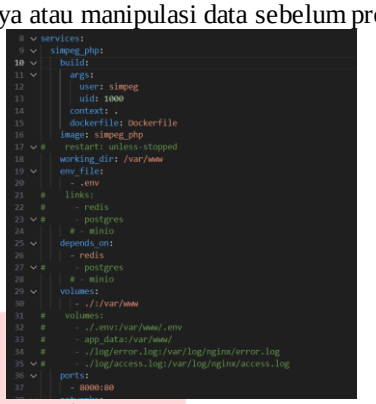


Gambar 8. Hasil pengujian vulnerable menggunakan OWASP ZAP.

A06 – Identification and Authentication Failures ditemukan pada modul login admin. Sistem tidak membatasi jumlah percobaan login dan tidak menerapkan CAPTCHA, sehingga rentan terhadap brute force attack. Selain itu, perilaku case-sensitive pada username, meskipun tidak langsung menyebabkan user enumeration, tetap dapat dijadikan indikator validitas akun.

Gambar 9. Hasil respon yang dikirim server.

A07 – Software and Data Integrity Failures, analisis konfigurasi Docker Compose menunjukkan file .env dimuat langsung ke dalam container, serta seluruh direktori proyek di-mount tanpa mekanisme verifikasi integritas seperti hash atau digital signature. Kondisi ini membuka peluang injeksi kode berbahaya atau manipulasi data sebelum proses build.



Gambar 10. Konfigurasi Nuclei menggunakan VSCode

C. Exploitasi Website Cloning

A01- Broken Access Control

Gambar 11. Hasil request proxy menggunakan Burpsuite.

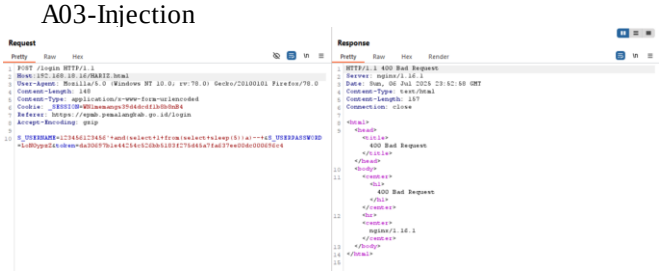
Hasil pengujian pada gambar ini merupakan upaya validasi kembali setelah dilakukan tindakan pengamanan terhadap sistem yang sebelumnya rentan. Pengujian dilakukan dengan mengaktifkan request proxy di Burp Suite untuk mengakses endpoint sensitif seperti .env.local namun tidak di temukan kembali informasi kridensial.

A02-Cryptographic Failures

Gambar 12. Hasil percobaan cryptographic failures dengan Burpsuite.

Hasil pengujian menunjukkan bahwa kerentanan terkait nilai parameter username=XYZ dan password=Pem%40!s4ong yang sebelumnya terbaca secara langsung dalam payload permintaan, telah berhasil diperbaiki. Saat ini, informasi kredensial telah dienkripsi dengan baik selama transmisi, sehingga tidak lagi terlihat dalam bentuk clear text. Dengan perbaikan ini, pihak ketiga yang berada dalam satu jaringan, termasuk pada koneksi Wi-Fi publik, tidak dapat membaca informasi sensitif meskipun melakukan penyadapan lalu lintas jaringan menggunakan tools seperti Wireshark atau tcpdump. Risiko serangan Man-in-the-Middle (MitM) maupun packet sniffing pun telah diminimalkan.

A03-Injection



Gambar 13. Hasil serangan Blind SQL.

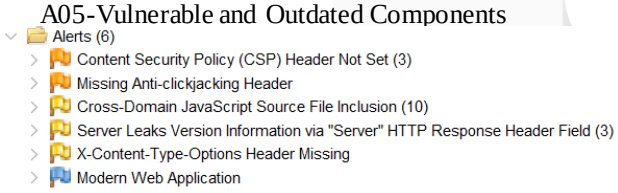
Berdasarkan hasil pengujian sebelumnya, ditemukan kerentanan Blind SQL Injection pada parameter S_USERNAME yang memungkinkan eksekusi perintah sleep(5) untuk menguji respon server. Namun, setelah dilakukan pengujian ulang dengan payload yang sama, server memberikan respon HTTP/1.1 400 Bad Request, sebagaimana ditunjukkan pada Gambar 4.16 Hal ini menandakan bahwa celah tersebut telah diperbaiki melalui validasi input atau mekanisme proteksi tambahan, sehingga server tidak lagi mengeksekusi perintah injeksi yang berbahaya.

A04-Security Misconfiguration

Gambar 14. Deteksi konfigurasi header tidak aman menggunakan Nuclei.

Hasil pemindaian menggunakan Nuclei, sebagaimana ditunjukkan pada Gambar 4.17, menunjukkan bahwa sebelumnya server tidak menyertakan sejumlah HTTP Security Headers penting dalam setiap responsnya dan terdapat Composer.json. Namun, setelah dilakukan perbaikan, seluruh header keamanan yang direkomendasikan telah diterapkan dengan benar. Dengan adanya perbaikan ini, server kini mampu mencegah berbagai serangan seperti Cross-Site Scripting (XSS), Clickjacking, kebocoran data antar origin, serta sniffing data pada koneksi tidak terenkripsi.

A05-Vulnerable and Outdated Components



Gambar 15 Hasil pengujian vulnerable menggunakan OWASP ZAP.

Hasil pengujian menggunakan OWASP ZAP sebelumnya mendeteksi bahwa website menggunakan file JavaScript dari pustaka versi lama yang berpotensi memiliki celah keamanan. Namun, setelah dilakukan pembaruan, seluruh pustaka JavaScript telah diperbarui ke versi terbaru dan lebih aman. Dengan perbaikan ini, potensi penyusupan script berbahaya atau serangan jarak jauh melalui komponen frontend telah berhasil diatasi, sehingga kerentanan tersebut tidak lagi ditemukan.

A06-Identification and Authentication Failures

Gambar 16. Hasil respon yang dikirim server.

Pada pengujian kerentanan kategori Identification and Authentication Failures, peneliti melakukan login kembali ke halaman admin dengan memasukkan username DIMAS menggunakan huruf kapital. Berdasarkan hasil intersepsi melalui tools Burp Suite, sistem sudah tidak menerima input tersebut dan mengembalikannya dalam bentuk yang sama tanpa perubahan bahkan sudah tidak ,uncul sama sekali, yang mengindikasikan bahwa sistem sudah di perbaiki.

A07-Software and Data Integrity Failures

Gambar 17. Konfigurasi Nuclei menggunakan VSCode

Berdasarkan gambar konfigurasi pada Gambar 4.21, sebelumnya file .env disertakan secara langsung melalui entri env_file: - .env, dan seluruh direktori proyek di-mount ke dalam container dengan volumes: - ./:/var/www. Namun, setelah dilakukan perbaikan, konfigurasi tersebut telah diubah sehingga file .env tidak lagi dimasukkan secara langsung ke dalam container. Dengan perbaikan ini, informasi sensitif seperti kredensial database dan API key yang sebelumnya berisiko terekspos kini telah diamankan dan tidak dapat diakses secara langsung, baik dari dalam container maupun dari sisi host.

D. Pembahasan

Berdasarkan pengujian subdomain Sistem Informasi Manajemen XYZ dengan pendekatan OWASP, ditemukan kerentanan pada aspek kontrol akses, kriptografi, injeksi, konfigurasi, dan integritas sistem. Temuan ini menunjukkan adanya titik lemah yang berpotensi dieksploitasi jika tidak segera diperbaiki. Tabel berikut memuat ringkasan jenis kerentanan, status, tingkat risiko, dan rekomendasi mitigasi.

Tabel 1.

Kode	Jenis Kerentanan	Status Temuan	Level Risiko
A01	*Broken Access Control*	Teridentifikasi	Tinggi
A02	*Cryptographic Failures*	Teridentifikasi	Tinggi
A03	*Injection (SQL Injection)*	Teridentifikasi	Tinggi
A04	*Security Misconfiguration*	Teridentifikasi	Sedang
A05	*Vulnerable and Outdated Components*	Teridentifikasi	Tinggi
A06	*Software and Data Integrity Failures*	Teridentifikasi	Sedang–Tinggi
A07	*Identification and Authentication Failures*	Teridentifikasi	Sedang–Tinggi

Sebagai tindak lanjut dari hasil identifikasi kerentanan berdasarkan kerangka kerja OWASP, disusun strategi penguatan keamanan yang bersifat menyeluruh dan berkelanjutan. Strategi ini mencakup perbaikan teknis, penguatan manajerial, dan pembaruan kebijakan untuk

mencegah, mendeteksi, dan merespons ancaman siber secara efektif. Pada tahap awal, langkah yang dilakukan meliputi pembatasan akses ke direktori dan file sensitif, pembaruan komponen perangkat lunak yang rentan, penerapan protokol HTTPS dengan sertifikat SSL/TLS yang sah, serta konfigurasi header keamanan. Secara lebih spesifik, mitigasi difokuskan pada tujuh kategori kerentanan OWASP, yaitu: **(**A01**)** pembatasan akses dan penerapan kontrol berbasis peran; **(**A02**)** penerapan enkripsi kuat dan konfigurasi cookie aman; **(**A03**)** validasi dan sanitasi input untuk mencegah injeksi; **(**A04**)** konfigurasi sistem sesuai standar keamanan; **(**A05**)** pembaruan rutin komponen usang; **(**A06**)** penguatan autentikasi dengan password kompleks, 2FA, dan proteksi sesi; serta **(**A07**)** perlindungan integritas perangkat lunak melalui verifikasi hash dan proses deployment aman. Penerapan strategi ini diharapkan dapat meningkatkan ketahanan aplikasi terhadap berbagai jenis serangan siber, sekaligus menjaga kerahasiaan, integritas, dan ketersediaan data publik.

V. KESIMPULAN

Hasil pengujian keamanan pada subdomain Sistem Informasi Manajemen XYZ menggunakan pendekatan OWASP menunjukkan beberapa kerentanan serius yang berpotensi dimanfaatkan pihak tidak berwenang untuk mengakses, memodifikasi, atau merusak sistem. Temuan meliputi lemahnya kontrol akses, kurangnya enkripsi data, input yang tidak difilter dengan baik, konfigurasi sistem yang kurang aman, penggunaan komponen usang, serta tidak adanya validasi integritas saat proses build dan deployment. Selain itu, sistem belum memiliki mekanisme perlindungan brute force maupun fitur keamanan tambahan seperti CAPTCHA atau autentikasi dua faktor (2FA). Untuk mengatasi hal tersebut, disarankan penerapan pembatasan akses pada direktori sensitif, penggunaan protokol HTTPS, validasi input yang ketat, pembaruan rutin komponen perangkat lunak, serta penambahan 2FA. Implementasi langkah-langkah ini diharapkan mampu meningkatkan ketahanan sistem terhadap serangan siber sekaligus memastikan keamanan data dan layanan publik yang diberikan.

REFERENSI

[1] Ridho et al., "PENINGKATAN LITERASI KEAMANAN DIGITAL UNTUK MENCEGAH CYBER CRIME DI SMK BINA BANGSA KOTA TANGERANG," Jurnal Pengabdian kepada Masyarakat, vol. 2, no. 5, 2025, [Online]. Available: https://jurnalmahasiswa.com/index.php/appa

[2] N. K. D. S. A. P. Yustika Citra Mahendra, "STRATEGI PENANGANAN KEAMANAN SIBER (CYBER SECURITY) DI INDONESIA," Jurnal Review Pendidikan dan Pengajaran, 2023, Accessed: Jan. 31, 2025. [Online]. Available: https://journal.universitaspahlawan.ac.id/index.php/jrpp/article/download/20659/15250/68759

[3] G. P. A. A. F. P. C. B. A. P. D. N. Rahmat Setiawan, "PENTINGNYA PENDIDIKAN DIGITAL DALAM MENINGKATKAN KESADARAN DAN KETERAMPILAN ANAK DALAM MENGHINDARI CYBERCRIME," Jurnal Ilmiah Pendidikan Dasar, 2024, Accessed: Jan. 31, 2025. [Online]. Available: https://journal.unpas.ac.id/index.php/pendas/article/view/20558/10143

[4] S. M. G. A. I. Okky Prasetia, "Sosialiasi Pengenalan Pentingnya Cyber Security Guna Menjaga Keamanan Data di Era Digital Pada Siswa/i SMK Bakti Idhata Jakarta," Jurnal Inovasi Pengabdian Masyarakat, pp. 16–20, 2024.

[5] I. A. Ain, A. Ambarwati, and L. Junaedi, "Analisis Manajemen Risiko Teknologi Informasi dan Keamanan Aset Dengan Menggunakan Nist Sp 800-30 Revisi 1," Jurnal Ilmu Komputer dan Bisnis, vol. 13, no. 2a, pp. 155–165, Dec. 2022, doi: 10.47927/jikb.v13i2a.403.