CENTIVE
VOL. 4, NO. 1, PP.1173-1183, DEC 2024
ISBN: 978-602-53004-0-0

Conference on Electrical Engineering, Informatics, Industrial Technology, and Creative Media 2024

Uji Penetration Testing Web Server XYZ, Menggunakan Metode OWASP TOP 10 dan CVSS

Shelly Margareth[1], Bita Parga Zen*[2] , Abednego Indra Saputra[3], Yoachim Yeremia Simatupang[4], Clint Joy Perez Melody Mokosandi[5], Reymon Okto Christiaan[6], Anak Agung Ngurah Rai Ando Pradana[7], Ivan Lawrens Antonius Sundoro[8]

[1,2,3,4,5,6,7,8]Teknik Informatika, Universitas Ma Chung
[1,2,3,4,5,6,7,8]Villa Puncak Tidar Blok N No 1 Malang, Indonesia

[1] 312210024@student.machung.ac.id
[2] bita.parga@machung.ac.id
[3] 312210001@student.machung.ac.id
[4] 312210025@student.machung.ac.id
[5] 312210008@student.machung.ac.id
[6] 312210020@student.machung.ac.id
[7] 312210004@student.machung.ac.id
[8] 311910010@student.machung.ac.id

Semakin maraknya perang siber saat ini membuat website semakin rentan mengalami peretasan, hal yang paling sering terjadi peretasan yaitu webserver mengalami serangan Ransomware DDOS, Malware dan Trojan pada studi kasus ini melakukan penelitian dengan studi kasus webserver XYZ menggunakan metode OWASP TOP 10 dengan 10 pengujian yaitu dengan tahapan informatioan gathering, vulnerability testing, exploit dan post exploit..pada score hasil kerentanan CVSS dalam hal ini tahapan yang dilakukan melalui information gathering ditemukan port 80 port 21 yang terbuka,. Vulnerability Testing menggunakan OWASP dan hasil penetration testing ditermukan Kerentanan yang paling kritis adalah Cross-Site Scripting (XSS) dan Insecure Data Transmission, yang keduanya memiliki dampak signifikan terhadap keamanan data pengguna dan integritas aplikasi web. Selain itu, Content Security Policy Not Set dan Missing Anti-Clickjacking Header juga menunjukkan bahwa kebijakan keamanan dasar belum diterapkan, sehingga memperbesar risiko eksploitasi. untuk hasil uji CVSS v4.0 Score : Kerentanan masuk kategori nilai 4.8 sebagai kategori kerentanan medium kesimpulan hasil uji penetrasi diterasi tersebut diperlukan keamananan firewall, IDS dan IPS agar data pada webserver tersebut tergolong aman

Kata Kunci: Penetration Testing, OWASP, CVSS, Keamanan Siber

Penulis Koresponden:
Bita Parga Zen
Program Studi Sistem Informasi, Universitas Ma Chung, Villa Puncak Tidar Blok N no. 1, Doro, Karangwidoro, Kec. Dau, Kabupaten Malang, Jawa Timur 65151 Indonesia Email: bita.parga@machung.ac.id

I. PENDAHULUAN

Berbagai kemajuan ilmu pengetahuan teknologi informasi komunikasi dan sistem pertahanan saat ini berkembang begitu pesat dan luas, hal ini memberi dukungan besar terhadap kemajuan, keamanan dan ketahanan bagi perlindungan suatu negara, Perkembangan teknologi dan informasi juga menciptakan berbagai peperangan yang berbasis pada jaringan dan memanfaatkan informasi serta mampu melaksanakan

perang di ranah digital maupun perang *cyber*, hal ini tentu dapat berpengaruh terjadinya keretasan pada suatu sistem *server*. [1]

Serangan terhadap sistem informasi dan data yang dikelola oleh organisasi, baik itu pemerintah, perusahaan, atau individu, semakin sering terjadi. Berdasarkan laporan dari *Cyber Security* dan *Infrastructure Security Agency* (CISA), lebih dari 70% organisasi global mengalami setidaknya satu insiden keamanan *cyber* pada tahun 2023. Peretasan akun, serangan ransomware, dan pencurian data pribadi adalah beberapa bentuk ancaman yang kian meningkat, menimbulkan kerugian finansial dan reputasi yang buruk.[2]

Melihat dari banyaknya pengguna internet di Indonesia , tentu akan rentan terjadinya serangan *cyber*, serangan *cyber* adalah segala bentuk baik dalam perbuatan, perkataan, pemikiran baik yang dilakukan dengan sengaja maupun tidak sengaja oleh pihak manapun, yang ditujukan pada sistem elektronik yang berupa muatan informasi maupun peralatan yang sangat bergantung pada teknologi dan jaringan.[3] Bentuk ancaman dari serangan *cyber* saat ini diantaranya adalah Serangan *Advanced Persistent Threats* (APT), *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS), Serangan *Defacement*, Serangan *Phising*, Serangan *Malware, Trojan Horse*, *CrackingPassword*, dan *Spam*.[4][5]

Di era digital ini, aplikasi web telah menjadi komponen penting dalam hampir semua aspek kehidupan, baik itu *e-commerce*, layanan perbankan online, atau sistem pemerintahan digital. Namun, seiring dengan meningkatnya ketergantungan pada aplikasi web, ancaman terhadap keamanan juga semakin tinggi.[6] Seringkali kita melihat bahwa aplikasi web yang rentan terhadap serangan dapat mengekspos data sensitif dan merusak integritas sistem. untuk itu, berbagai inisiatif dan standar keamanan[7], seperti OWASP Top 10 - 2021, OWASP Top 10 mencakup 10 jenis kerentanan yaitu, *Broken Access Control, Cryptographic Failures, Injection, Insecure Design, Security Misconfiguration, Vulnerable and Authentication Failures, Software and Data Integrity Failures*, *Security Logging and Monitoring Failures*, dan *Server-Side Request Forgery*. [8] OWASP ZAP atau biasa disebut ZAP yaitu *Zed Attack Proxy*. ZAP adalah aplikasi yang berguna untuk melakukan *penetration test* mencari *vulnerabilities* dalam suatu *web applications* dengan cara mudah. Dengan adanya fitur *scanner* otomatis sebaik sebagaimana kita menggunakan tool untuk menemukan *vulnerabilities* secara manual.[9] Di dalam *web server* biasanya terdapat serangan serangan salah satunya adalah CSRF yaitu *Cross Site Request Forgery*, merupakan serangan dengan menggunakan sistem *request*, atau kata lain serangan *cyber* yang mengeksploitasi *website* dengan membuat pengguna tanpa sadar mengirim permintaan.[10] Dan beberapa ancaman lainnya seperti SQL *Injection*, DoS, XSS, dan lain lainnya.

Keamanan aplikasi web tidak hanya penting untuk melindungi data pribadi pengguna, namun juga untuk menjaga integritas operasional organisasi. Oleh sebab itu diperlukan untuk melakukan *penetration* untuk mengidentifikasi kerentanan dan menilai seberapa tingkat resikonya. Dengan sistem *Common Vulnerability Scoring System* (CVSS), *Common Vulnerability Scoring System* (CVSS) adalah sebuah standar terbuka yang digunakan untuk menilai tingkat keparahan kerentanan keamanan perangkat lunak dan sistem komputer. CVSS membantu organisasi memprioritaskan respon mereka terhadap kerentanan berdasarkan risiko yang dinilai. CVSS menggunakan tiga kelompok metrik utama untuk menghitung skor kerentanan dari skala 0 (tidak ada risiko) hingga 10 (risiko kritis).[11]

Tingkat *Common Vulnerability Scoring System* (CVSS) sering dikategorikan dalam tiga tingkat utama berdasarkan skor yang diberikan.

Tabel 1 CVSS

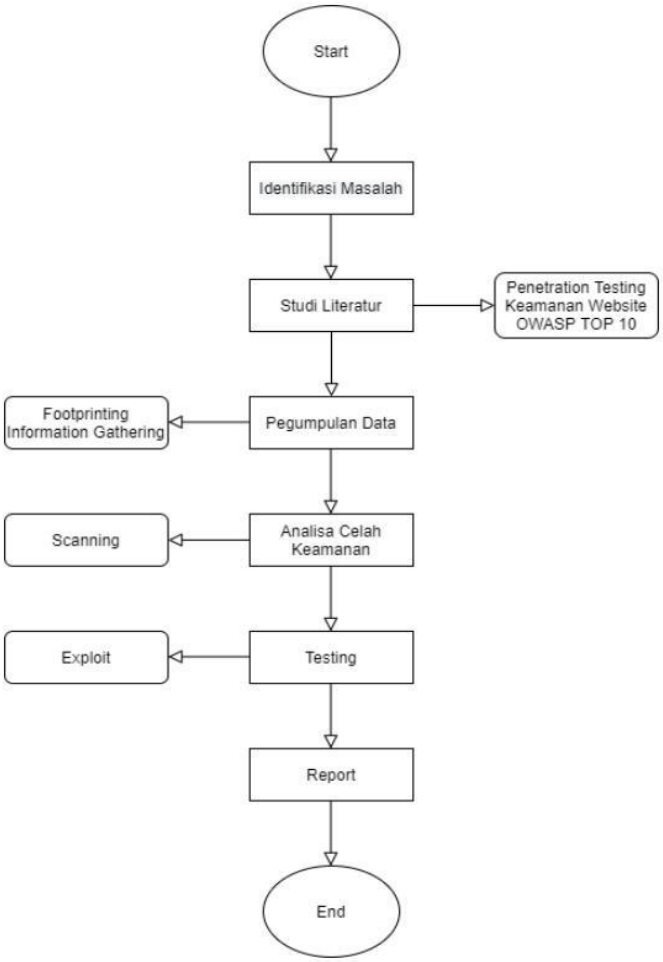
Tingkat CVSS	Skor	Deskripsi
Low	0.1 - 3.9	Kerentanan yang berdampak kecil pada sistem. Biasanya dapat diatasi tanpa mendesak, karena dampaknya terhadap kerahasiaan, integritas, dan ketersediaan (*CIA Triad*) cenderung rendah.
Medium	4.0 - 6.9	Kerentanan dengan resiko menengah. Masalah ini dapat berdampak signifikan jika dibiarkan terlalu lama, meskipun mungkin memerlukan eksploitasi lanjutan oleh penyerang.
High	7.0 - 8.9	Kerentanan yang memerlukan perhatian segera karena memiliki

Tingkat CVSS	Skor	Deskripsi
		dampak serius pada sistem atau data. Dapat menyebabkan kebocoran data atau kerusakan sistem.
Critical	9.0 - 10.0	Kerentanan dengan resiko yang sangat tinggi dan dampak besar terhadap kerahasiaan, integritas, serta ketersediaan. Biasanya memerlukan tindakan segera untuk mitigasi.

Dalam hal ini peneliti melakukan identifikasi keamanan web server XYZ terhadap ancaman cyber serta mengeksplorasi solusi teknis dan kebijakan yang dapat diterapkan untuk memperkuat sistem keamanan informasi dari *web server* XYZ tersebut dengan menggunakan metode yang telah disebutkan, yaitu OWASP Top 10 untuk melakukan *penetration test* dan melakukan skoring berdasarkan CVSS. Penelitian ini juga meninjau pentingnya metode penetration untuk mengetahui dan bertujuan meminimalisir resiko kebocoran data dari *web server* XYZ.

II. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah menggunakan metode kuantitatif berupa uji penetrasi (*penetration test*) melalui OWASP TOP 10 dan CVSS. Dengan melalui metode penelitian uji penetrasi (*penetration test*) kita dapat mengetahui apabila terdapat orang-orang yang tidak bertanggung jawab seperti *hacker* yang ingin meretas atau meng-*crack webserver* yang dituju.



Gambar 1. Tahapan Uji Penetration Testing [13]

Dengan metode yang sama, peneliti memperoleh informasi dan data terkait kerentanan (*vurnerability*) yang terdapat pada *webserver* yang dituju. Dimana dalam hal ini, peneliti menggunakan standarisasi OWASP dan *Scoring System* dan melakukan uji penetrasi dengan standarisasi *SQL Injection*.[14]

Saat dilakukan, penelitian dapat menentukan langkah dari proses persiapan yaitu berdasarkan latar belakang tentang kebutuhan keamanan yang efektif untuk melindungi data dari serangan siber, ancaman *cyber attack*. Melakukan tahapan Security Assessment mulai dari *Scanning Vulnerability assessment* yang mengikuti standar OWASP TOP 10 lalu melakukan *penetration testing* sehingga penelitian akan lebih efektif. [15]

Tabel 2 List OWASP Top 10 [16]

No	Nama	Deskripsi
1	*Broken Access Control*	Pengaturan kontrol akses yang buruk dapat menyebabkan user mengakses data atau fitur yang seharusnya tidak dapat di akses.
2	*Cryptographic Failures*	Gagal melindungi data sensitif, seperti kata sandi atau informasi pribadi, dengan teknik *enkripsi* yang kuat.
3	*Injection*	Penyerang menyisipkan kode berbahaya, seperti SQL atau *script*, yang dapat dieksekusi oleh aplikasi dan merusak sistem.
4	*Insecure Design*	Aplikasi dirancang tanpa mempertimbangkan potensi ancaman atau kerentanannya, sehingga rentan terhadap serangan.
5	*Security Misconfiguration*	Pengaturan yang salah atau default yang tidak diubah membuka celah yang dimanfaatkan oleh penyerang untuk mengeksploitasi sistem.
6	*Vulnerable & Outdated Components*	Penggunaan komponen software yang tidak diperbarui dapat meningkatkan risiko serangan.
7	*Identification & Authentication Failures*	Sistem gagal mengidentifikasi atau memverifikasi pengguna dengan baik, seperti penggunaan kata sandi yang lemah.
8	*Software & Data Integrity Failures*	Data dan perangkat lunak yang digunakan oleh tidak diverifikasi atau tidak dapat dipercaya, membuka celah untuk manipulasi.
9	*Security Logging & Monitoring Failures*	Tidak mencatat aktivitas mencurigakan atau memantau potensi ancaman, menghambat respons terhadap serangan.
10	*Server-side Request Forgery*	Penyerang memanipulasi untuk membuat permintaan ke *server internal* yang seharusnya tidak dapat diakses dari luar, membuka kemungkinan pencurian data.

Penilaian dengan CVSS dilakukan dengan memberi skor 0 hingga 10, kemudian digolongkan menjadi 3 kategori yaitu *Low*, *Medium*, dan *High*. Setiap kategori menggambarkan tingkat ancaman yang ditimbulkan oleh kerentanan. Jika skor CVSS berada diantara 0.1-3.9 maka dampak pada sistem/ data kecil, skor CVSS berada diantara 4.0-6.9 menyebabkan masalah yang lebih besar meski belum sepenuhnya dapat membahayakan sistem/data sedangkan jika skor CVSS berada di 7.0-8.9 maka dapat menyebabkan masalah yang serius dan dapat menyebabkan kerusakan besar pada sistem dan data, dan jika skor CVSS berada di 9-10 maka dapat dikatakan menyebabkan masalah yang sangat serius dan dapat menyebabkan dampak besar terhadap kerahasiaan, integritas, serta ketersediaan..

Selanjutnya proses pelaksanaan penelitian dilakukan dengan melakukan tinjauan lokasi yang akan diuji, pengumpulan, pengolahan data dan hasil penelitian yang siap untuk dianalisis berdasarkan metode yang dilakukan. Hasil analisis terdapat pada kesimpulan penelitian berupa identifikasi seluruh serangan siber sehingga keamanan sistem IT dapat diketahui. Populasi pada penelitian ini adalah website dengan internet

protocol 103.5*.14*.16* yang akan dilakukan uji keamanannya. Sistem yang dirancang ditujukan untuk mendeteksi kerentanan pada sebuah website melalui tahap uji penetrasi secara menyeluruh terhadap kerentanan yang terjadi pada *server* dan bagaimana cara mengatasinya.

III. HASIL DAN PEMBAHASAN

Pada bagian hasil dan pembahasan ini, dilakukan pengujian keamanan terhadap website xyz.ac.id menggunakan beberapa metode, yaitu ZAP (*Zed Attack Proxy*), OWASP, CVSS (*Common Vulnerability Scoring System*), dan *Kali Linux*. Metode ini diterapkan untuk mengidentifikasi dan menganalisis potensi kerentanannya yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Penjelasan berikut menguraikan tahapan pengujian yang dilakukan dengan masing-masing metode.

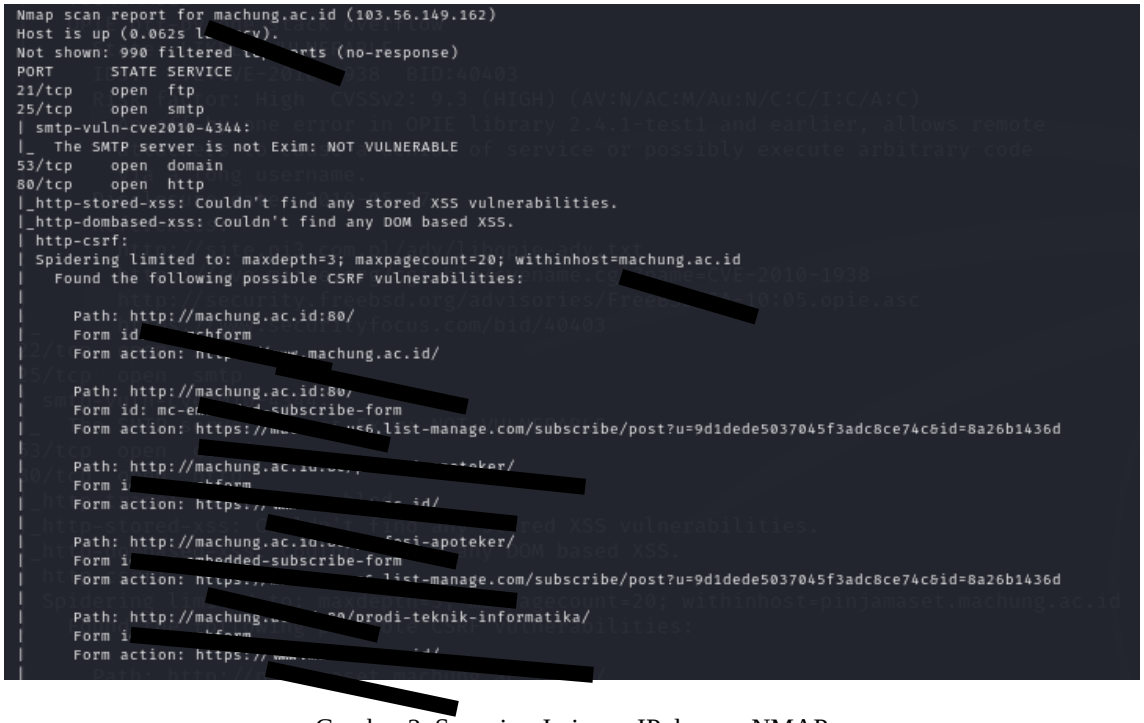
Pengujian pertama dilakukan dengan menggunakan ZAP (*Zed Attack Proxy)*, sebuah alat otomatis yang digunakan untuk memindai aplikasi web dan mendeteksi kerentanannya. ZAP memetakan struktur aplikasi web dan menganalisis potensi titik lemah yang bisa dieksploitasi. Pengujian ini bertujuan untuk menemukan celah-celah keamanan yang umum terjadi, seperti injeksi SQL atau masalah dalam pengelolaan sesi.

Selanjutnya, pengujian dilakukan dengan pendekatan OWASP (*Open Web Application Security Project*), yang berfokus pada 10 kerentanannya yang paling umum, seperti *Cross-Site Scripting* (XSS), *Insecure Deserialization*, dan *Broken Authentication*. Metode ini memberikan pedoman untuk mengevaluasi aplikasi web secara menyeluruh berdasarkan standar keamanan yang telah ditetapkan oleh OWASP, untuk mengidentifikasi risiko yang dapat dihadapi aplikasi web.

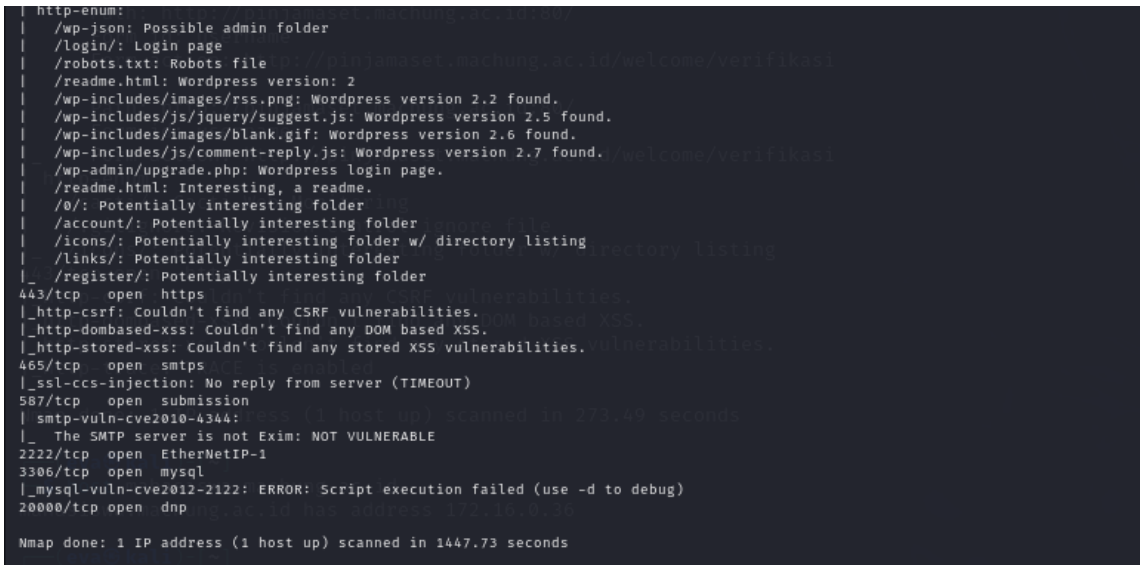
CVSS (*Common Vulnerability Scoring System*) digunakan untuk menilai tingkat keparahan kerentanannya. Sistem penilaian ini memberikan skor berdasarkan dampak dan kemungkinan eksploitasi dari setiap kerentanan yang ditemukan. Pengujian ini penting untuk menentukan prioritas penanganan, sehingga tim pengembang dapat fokus pada kerentanannya yang paling kritis dan perlu segera ditangani.

Metode terakhir yang digunakan adalah *Kali Linux*, sebuah sistem operasi berbasis Linux yang dilengkapi dengan berbagai alat untuk pengujian penetrasi dan audit keamanan. Dengan menggunakan alat-alat dari Kali Linux, pengujian dilakukan untuk mengeksploitasi celah keamanan yang ada dan menguji apakah celah tersebut dapat dimanfaatkan untuk memperoleh akses tidak sah ke sistem atau data.

Keempat metode ini memberikan hasil yang saling melengkapi dan dapat diterapkan pada website lain untuk mengidentifikasi dan mengevaluasi tingkat keamanan. Dengan melakukan pengujian secara komprehensif, website dapat diperiksa untuk kerentanannya, sehingga dapat diambil tindakan perbaikan untuk meningkatkan sistem keamanannya. Waktu Dalam Tahapan *Penetration testing* dilakukan setelah peneliti melakukan *scanning vulnerability.*

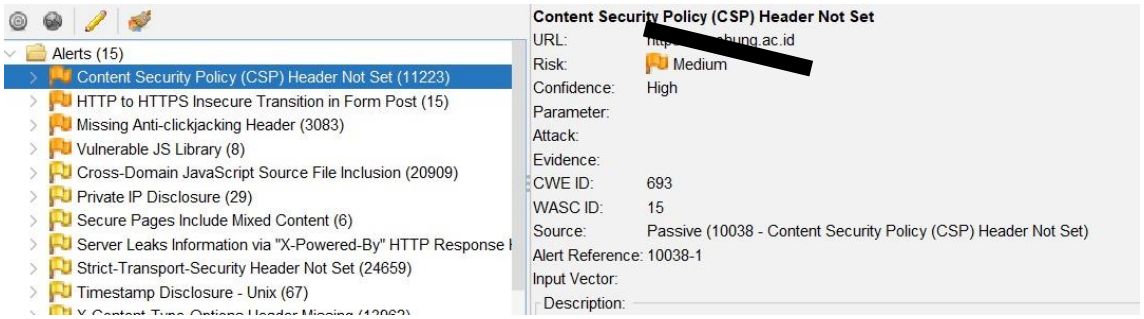


Gambar 2. Scanning Jaringan IP dengan NMAP



Gambar 3. Scanning Jaringan IP dengan NMAP

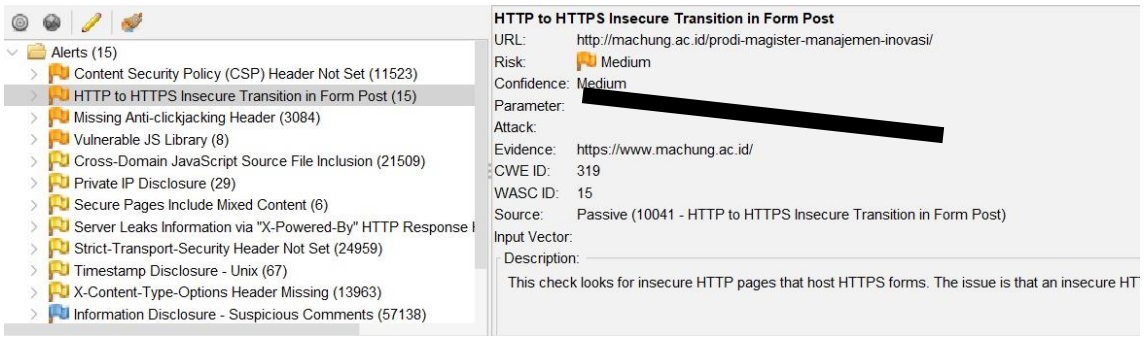
Hasil Scan IP pada Gambar 2 dan Gambar 3 tersebut menampilkan beberapa situs dan port seperti port 21 untuk FTP, Port 80 alamat website (HTTP) dan Port 3306 sebagai port MYSQL dan menggunakan *Script Vuln* yang tersedia di Nmap untuk scan kerentanan *website*, dari hasil scan terdapat celah untuk dilakukan tahapan uji kerentanan seperti kerentanan terhadap CSRF pada port 80, CSRF adalah serangan keamanan web yang memaksa pengguna yang sudah teridentifikasi untuk mengirimkan permintaan tanpa disadari, selanjutnya dari IP tersebut akan dilakukan tahapan untuk pembuktian sistem keamanan dengan standar *Open Web Application Security Project* (OWASP) dan tahapan *Common Vulnerability Scoring System* (CVSS)



Gambar 4. Scanning Jaringan IP menggunakan ZAP

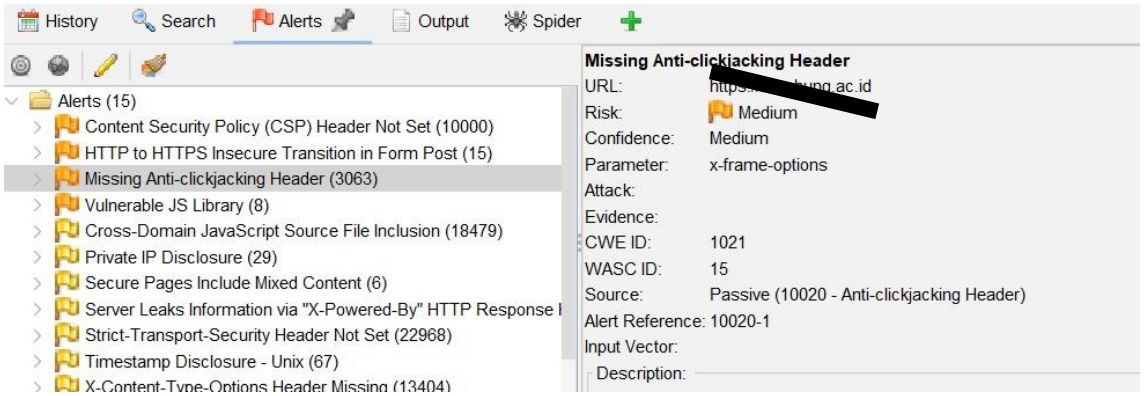
Seiring dengan semakin berkembangnya sistem keamanan informasi, terutama pada server web, para peneliti memutuskan untuk menguji secara mendalam sebuah sistem dengan alamat IP 172.5*14*.16*. Pengujian ini bertujuan untuk mengidentifikasi segala kelemahan keamanan yang mungkin ada pada sistem tersebut. Proses pengujian yang dilakukan mengikuti tahapan yang umum dikenal dalam dunia keamanan siber, yaitu *vulnerability assessment* atau penilaian kerentanan. Pada tahap ini, sistem akan 'diperiksa secara menyeluruh' untuk mencari celah keamanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab.

Untuk melakukan pemeriksaan yang komprehensif, para peneliti menggunakan standar keamanan web yang diakui secara global, yaitu OWASP Top 10. Standar ini merangkum 10 jenis serangan web paling umum dan berbahaya. Hasil dari pemindaian ini menunjukkan adanya beberapa kelemahan keamanan pada sistem yang diuji, diantaranya: Content Security Policy(CSP) not Set.



Gambar 5. Scanning HTTP to HTTPS Incescure menggunakan ZAP

Selanjutnya dilakukan pemindaian untuk mengidentifikasi transmisi data yang tidak aman antara HTTP dan HTTPS pada saat pengiriman formulir (form post) menggunakan ZAP. Alat ini memeriksa apakah data sensitif yang dikirimkan melalui formulir web diproteksi dengan HTTPS (protokol yang aman) atau masih menggunakan HTTP yang rentan terhadap penyadapan dan manipulasi oleh pihak ketiga. Pemindaian ini bertujuan untuk memastikan bahwa informasi yang dikirimkan melalui formulir, seperti kata sandi atau data pribadi, dilindungi dengan enkripsi yang tepat, menghindari risiko kebocoran data akibat transmisi yang tidak aman.

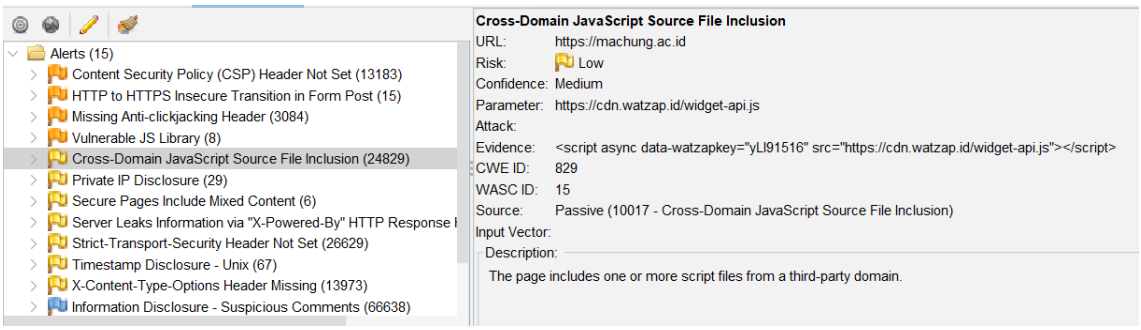


Gambar 6. Anti-clickjacking Scanner menggunakan ZAP

Pada Tahapan Scanning melalui aplikasi OWASP ZAP terdapat kerentanan yang terdeteksi bisa masuk dengan tingkat resiko medium, terdapat pada "Missing Anti-clickjacking Header" yang dapat menyerang web melalui clickjacking. Alat ini memeriksa apakah situs web telah mengimplementasikan perlindungan yang tepat terhadap clickjacking, yaitu serangan di mana pengguna diarahkan untuk mengklik elemen tersembunyi atau tidak terlihat pada halaman web yang dapat mengekspos mereka pada tindakan berbahaya. Scanner ini memastikan bahwa header **X-Frame-Options** atau **Content Security Policy (CSP)** telah diterapkan dengan benar untuk mencegah halaman web dimuat dalam iframe yang dapat dimanipulasi oleh penyerang.

Gambar 7. Vulnerable Scanner Java Script(JS) Library menggunakan ZAP

Selanjutnya melakukan pemindaian otomatis terhadap aplikasi untuk mengidentifikasi celah-celah keamanan yang umum, seperti SQL Injection, Cross-Site Scripting (XSS), Broken Authentication, dan Misconfigurations. Scanner ini menganalisis struktur aplikasi, menguji input/output, dan memeriksa potensi risiko yang dapat dieksploitasi oleh peretas. Setelah melakukan pemindaian ditemukan kerentan pada JS Library dengan tingkat resiko medium, salah satu penyebabnya karena versi yang digunakan adalah versi lama sehingga diharapkan untuk memperbaharui versi jquery ke versi lebih baru.



Gambar 8. Cross Domain Script Inclusion menggunakan ZAP

Cross Domain Script Inclusion Dari hasil scanning dengan alamat URL : https://ma*****.ac.id menggunakan OWASP terdapat pemberitahuan CrossDomain JavaScript Source File Inclusion yang berarti adalah terdapat kerentanan pada javascript seperti padah HTML pada web dan CSS pada layout keselarasan website bahwa kelemahan yang akan dihadapi ini merupakan sebagai sistem keamanan yang perlu ditingkatkan karena harus memperbarui referensi Javascript secara manual setiap kali versi baru dirilis. Dampak dari Cross Site Scripting (XSS) adalah dapat dengan mengeksekusi jarak jauh kode pada browser webserver, seperti mencuri kredensial, sesi, atau memberikan malware kepada pengguna, bukti kelemahan pada Cross Site Scripting. H

Tabel 3. Hasil Uji Coba Melalui CVSS

No	Base Matrics	Exploitability Metrics	Vulnerable System Impact Metrics	Subsequent System Impact Metrics
1	Attack Vector	Local	Low	Non
2	Confidentiality	Low	Low	Low
3	Integrity	Low	High	Non
4	Availability	None	High	Non

Dari hasil uji CVSS v4.0 Score : Kerentanan masuk kategori nilai 4.8 sebagai kategori kerentanan medium

IV. KESIMPULAN

Penelitian menggunakan pendekatan OWASP TOP 10, CVSS, ZAP, dan Kali Linux untuk mengidentifikasi dan menganalisis kerentanan keamanan web secara komprehensif. Temuan utama adalah kerentanan kritis seperti Cross-Site Scripting (XSS) dan Insecure Data Transmission, serta kelemahan pada Content Security Policy dan Anti-Clickjacking Header. dan analisis menunjukkan skor CVSS v4.0 sebesar 4.8 (kategori medium), menandakan perlunya perbaikan keamanan lebih lanjut. Pendekatan ini menegaskan pentingnya pengujian penetrasi terstruktur dan mendalam dalam menjaga keamanan web. Penelitian ini memberikan kontribusi ilmiah dengan mengintegrasikan berbagai metode untuk identifikasi dan mitigasi kerentanan secara efektif.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada Universitas Ma Chung dan Fakultas Teknologi dan Desain Universitas Ma Chung yang mendukung penuh kegiatan nasional conferen ini

DAFTAR PUSTAKA

[1] S. Nurul, S. Anggrainy and S. Aprelyani, "Faktor Faktor yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi dan Network (Literature Review SIM)," *Jurnal Ekonomi Manajemen Sistem Informasi,* vol. 3, no. 5, pp. 564-566, 2022.

[2] B. Stackpole, "*MIT report details new cybersecurity risks*," *MIT Management Sloan School*, 30 April 2024.

[3] N. I. Bilondatu and V. Susanti, "Fenomena *Internet Trolling*, Sebuah Bentuk Kejahatan Siber," *Journal of Education, Humaniora and Social Sciences,* vol. 4, no. 3, pp. 2-3, 2022.

[4] B. P. Zen, R. A. Gultom dan A. H. Reksoprodjo, "Analisis *Security Assessment* Menggunakan Metode *Penetration Testing* Dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara,"J*urnal Teknologi Penginderaan,* vol. 2, no. Keamanan Teknologi Pertahanan Negara, pp. 106-108, 2020.

[5] A. D. Wiratama, "*Cyber Security In* 2023: *The Latest Challenges And Solutions*," *Jurnal Komputer Indonesia*, vol. 2, no. 1, pp. 47-49, 2023.

[6] Sujono, "Penerapan Aplikasi Sistem Informasi Kependudukan Berbasis Web Pada Kantor Kepala Desa Puput Kec.Simpangkatis," *Jurnal SIMETRIS*, vol. 9, no. 1, pp. 707-708, 2018.

[7] Satria Galang Saputra, Parga Zen, B., & Abdurahman. (2023). Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing Execution Standard (PTES). *Jurnal Sistem Informasi Galuh*, *1*(2), 43–51. https://doi.org/10.25157/jsig.v1i2.3152

[8] M. Aljabri *et al*., "*Testing and Exploiting Tools to Improve OWASP Top Ten Security Vulnerabilities Detection*," *2022 14th International Conference on Computational Intelligence and Communication Networks (CICN)*, Al-Khobar, Saudi Arabia, 2022, pp. 797-803.

[9] Alfidzar, H., & Zen, B. (2022). Implementasi HoneyPy Dengan Malicious Traffic Detection System (Maltrail) Menggunakan Analisis Deskriptif Guna Untuk Mendeteksi Serangan DDOS Pada Server. *Journal of Informatics Information System Software Engineering and Applications (INISTA)*, *4*(2), 32-45. https://doi.org/10.20895/inista.v4i2.534

[10] G. H. A. Kusuma, "Implementasi OWASP ZAP Untuk Pengujian Keamanan Sistem Informasi Akademik," *Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika*, vol. 16, no. 2, pp. 178-180, 2022.

[11] "CRF(*Cross Site Request Forgery*): Pengertian, Jenis dan Cara Mencegahnya," *Coding Studio*, 19 November 2023.

[12] P. Mell, H. Spring, D. Dugal, T. Fridley, A. Kundu, P. Nordwall, V. Pushpanathan, M. Tesauro and C. Turner, "*Measuring the Common Vulnerability Scoring System Base Score Equation*," *the NIST Editorial Review Board*, Gaithersburg, 2022.

[13] Y. T. A. Rosaliah, J. and B. Hananto, "Pengujian Celah Keamanan *Website* Menggunakan Teknik *Penetration Testing* dan Metode OWASP TOP 10 pada Website SIM xxx," *Jurnal Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya*, pp. 752-755, 2021.

[14] M. Adhari, Panduan Meretas Bagi Pemula (*Metasploitable Versus Kali*), Indramayu: CV. Adanu Abimata, 2022.

[15] Mochammad Dzaki Al Vriano, "Pengujian Keamanan Web Juice Shop Dengan Metode *Pentesting* Berbasis Owasp Top 10", *Kohesi*, vol. 1, no. 6, pp. 91–100, Oct. 2023.

[16] I. O. Riandhanu, "Analisis Metode *Open Web Application Security Project* Menggunakan Penetration Testing pada Keamanan *Website* Absensi," *Jurnal Informasi dan Teknologi*, vol. 4, no. 3, pp. 160-165, 2022.