ANALISIS KEAMANAN SISTEM INFORMASI WEBSITE MENGGUNAKAN METODE PENETRATION TESTING DENGAN OWASP TOP 10 2021 (STUDI KASUS PT. XYZ)

Achmad Fajar Royyan Wachid
Fakultas Rekayasa Industri
Sistem Informasi
Surabaya, Indonesia
royyan@student.telkomuniversity.ac.id

Muhammad Nasrullah, S.kom., M.Kom.
Fakultas Rekayasa Industri
Sistem Informasi
Surabaya, Indonesia
emnasrul@telkomuniversity.ac.id

Rizky Fenaldo Maulana, S.kom., M.Kom.
Fakultas Informatika
Informatika
Surabaya, Indonesia
rizkyfenaldo@telkomuniversity.ac.id

***Abstrak* —** Meningkatnya risiko serangan terhadap keamanan data berbasis website menjadi perhatian berbagai pihak, termasuk PT XYZ, perusahaan pengembang software untuk apotek dan klinik yang telah digunakan oleh lebih dari 2.500 apotek dan klinik di lebih dari 400 kota di Indonesia. Data yang disimpan mencakup informasi sensitif yang harus dijaga agar tidak jatuh ke pihak yang tidak berwenang. Penelitian ini bertujuan mengidentifikasi kerentanan dalam sistem informasi PT XYZ dan memberikan rekomendasi peningkatan keamanan. Pengujian dilakukan dengan metode penetration testing menggunakan OWASP Top 10 2021. Hasil pengujian menemukan beberapa kerentanan signifikan, termasuk kelemahan kontrol akses, kegagalan kriptografi, SQL Injection, XSS, serta masalah konfigurasi keamanan seperti kurangnya header CSP dan X-Frame-Options. Beberapa komponen sistem juga rentan akibat penggunaan versi jQuery yang usang dan CVE yang belum diperbarui. Selain itu, ditemukan masalah validasi otentikasi serta kelemahan dalam logging dan monitoring. Rekomendasi perbaikan mencakup penguatan kontrol akses, penerapan parameterized queries, konfigurasi header keamanan yang lebih ketat, pembaruan komponen sistem, serta peningkatan sistem otentikasi dan monitoring. Dengan implementasi perbaikan ini, PT XYZ dapat meningkatkan keamanan sistem dan melindungi data pelanggan secara lebih efektif.

I. PENDAHULUAN

PT XYZ adalah perusahaan yang mengembangkan aplikasi apotek dan klinik berbasis website untuk membantu manajemen data obat, pasien, rekam medis, keuangan, dan analisis data. Seiring dengan meningkatnya ketergantungan pada teknologi digital, keamanan informasi menjadi isu krusial bagi perusahaan yang mengelola data sensitif. Serangan siber seperti malware, eksploitasi, injeksi database, dan serangan denial-of-service (DoS) semakin sering terjadi dan mengancam keamanan sistem[1]. Di Indonesia, ancaman siber meningkat sebesar 6,15% dari tahun 2020 hingga 2021, dengan berbagai serangan seperti SQL Injection, phishing, dan pencurian data pribadi[2]. Salah satu kasus besar terjadi pada tahun 2020, ketika 279 juta data warga Indonesia diretas dan dijual di forum daring, yang diduga berasal dari BPJS Kesehatan.[3] PT XYZ sendiri pernah mengalami insiden peretasan melalui serangan injeksi, yang menunjukkan adanya potensi kerentanan dalam sistem mereka. Dengan adanya ancaman tersebut, perusahaan perlu melakukan evaluasi keamanan sistem informasi berbasis website untuk mencegah kebocoran data yang dapat merugikan bisnis dan pelanggan[4]. Salah satu metode yang umum digunakan dalam pengujian keamanan adalah penetration testing (pentesting), yang merupakan simulasi serangan nyata untuk mengidentifikasi potensi kerentanan dalam sistem[5]. Penelitian ini menggunakan standar OWASP Top 10 2021, sebuah daftar yang disusun oleh komunitas keamanan siber global untuk mengidentifikasi sepuluh risiko keamanan aplikasi web yang paling kritis[6]. Beberapa penelitian sebelumnya telah menggunakan OWASP Top 10 versi 2017 dan OWASP versi 4 dalam pengujian keamanan website[7] Namun, dalam penelitian ini, digunakan OWASP Top 10 2021 karena mencerminkan ancaman terbaru dalam dunia keamanan siber. Dengan menerapkan penetration testing berdasarkan OWASP Top 10 2021[8], penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan dalam sistem informasi website PT XYZ serta memberikan rekomendasi perbaikan guna meningkatkan keamanan. Hasil penelitian ini diharapkan dapat membantu PT XYZ dalam memperkuat sistem keamanan mereka, melindungi data pelanggan, serta meningkatkan kepercayaan pengguna terhadap layanan yang disediakan[9].

II. KAJIAN TEORI

A. Keamanan Sistem Informasi

Keamanan sistem informasi adalah serangkaian upaya untuk melindungi data, sistem, dan jaringan dari ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan informasi. Langkah-langkah keamanan mencakup enkripsi data, pengendalian akses, serta pemantauan dan deteksi ancaman untuk mencegah serangan siber[10]

B. OWASP

OWASP (Open Web Application Security Project) adalah komunitas global yang berfokus pada peningkatan keamanan aplikasi web. Salah satu proyek utama OWASP adalah OWASP Top 10, yaitu daftar sepuluh ancaman keamanan aplikasi web yang paling umum, seperti injeksi SQL, kesalahan autentikasi, dan serangan terhadap API[11].

C. Penetration Testing

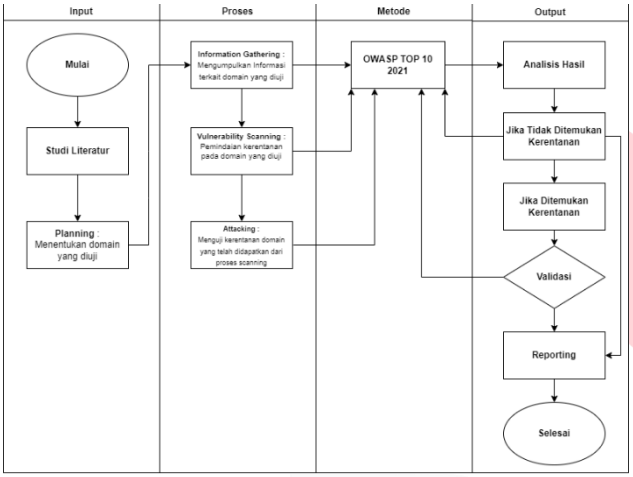
Penetration testing adalah metode pengujian keamanan sistem dengan mensimulasikan serangan siber untuk mengidentifikasi dan mengevaluasi potensi kerentanan. Metode ini membantu organisasi dalam merancang strategi perlindungan yang lebih efektif sebelum serangan nyata terjadi[12].

III. METODE

Penelitian ini menggunakan kerangka kerja OWASP Top 10 2021 sebagai pedoman utama dalam melakukan pengujian keamanan pada aplikasi web. Metode yang digunakan adalah penetration testing, yang bertujuan untuk mengidentifikasi, mengevaluasi, dan memberikan rekomendasi atas kerentanan yang ditemukan dalam sistem.

A. Tahapan Penelitian

Berikut tahapan penelitian ini:



GAMBAR 1
Tahapan penelitian

IV. HASIL DAN PEMBAHASAN

A. Information Gathering

Pada tahapan ini dilakukan pengumpulan informasi-informasi yang dibutuhkan seputar *webiste* xyz.com Informasi yang dibutuhkan merupakan informasi yang mendalam pada *website[13]*. Hasil *information gathering* bisa dilihat pada tabel dibawah ini.

TABEL 1
Hasil *Information Gathering*

Perintah	Hasil
dig	Informasi terkait domain yang meliputi nama domain dan alamat IP.
nslookup	Mengetahui Alamat IP dari nama domain, informasi nameserver dan email exchanger.

B. Network Mapping

Network Mapping merupakan tahapan pemetaan dan pemindaian yang berguna untuk mengumpulkan informasi terkait perangkat yang tersedia atau port yang terbuka pada infrastruktur jaringan *website* dengan menggunakan perintah *nmap* pada *tools kali linux[14]*. Hasil *Network Mapping* bisa dilihat pada tabel dibawah ini.

TABEL 2
Hasil *Network Mapping*

Perintah	Hasil
nmap -sS -sV	Ditemukan dua port yang bersifat open pada website, yaitu port 80/tcp dan 443/tcp.

C. Wapplyzer

Pada tahap ini peneliti menggunakan extension *Wappalyzer* yang memberikan jabaran tentang komponen yang membentuk infrastruktur situs web.

TABEL 3
Hasil Wapplyzer

Teknologi	Keterangan
Analistik	Google Analytics Facebook Pixel
Bahasa Pemrograman	PHP
Kerangka Kerja Mobile	jQuery-pjax
Kerangka Kerja Web	Yii
Pengelola Tag	Google Tag Manager
Sistem Operasi	Ubuntu
Pemutar Video	YouTube
Security	reCAPTCHA HSTS
Font Script	Font Awesome Google Font API
JavaScript Libraries	jQuery UI Spin.js Select2 Core-js jQuery
JavaScript Graphics	Chart.js
Customer data platform	Segment
UI Frameworks	Bootstrap
Server Website	Apache HTTP Server

D. Penetration Testing

Pada tahap ini, peneliti melakukan pengujian terhadap celah keamanan pada sebuah website. Informasi yang telah dikumpulkan dari tahap sebelumnya digunakan sebagai referensi dalam proses pengujian ini. Pengujian kerentanan dilakukan melalui dua metode, yaitu: pemindaian menggunakan alat OWASP ZAP serta uji penetrasi[15]. Hasil eksploitasi dari kedua metode tersebut dapat dilihat dalam tabel berikut.

TABEL 4
Hasil *Penetration Testing*

Daftar Kerentanan	Temuan Kerentanan
A01: Broken Access Control	Percobaan akses admin tanpa login dan akses fitur admin dari user kasir tidak berhasil, namun terdapat indikasi kontrol akses yang lemah, memungkinkan

Daftar Kerentanan	Temuan Kerentanan
	penggunaan metode HTTP yang tidak seharusnya.
A02: Cryptographic Failures	Ditemukan beberapa masalah keamanan, termasuk cookie yang dapat dikirim melalui koneksi tidak aman dan permintaan lintas situs, header cache-control yang tidakdikonfigurasi dengan tepat, serta pengungkapan Unix Timestamp oleh aplikasi/server web yang dapat dimanfaatkan oleh penyerang untuk menganalisis sistem. Selain itu, terdapat kelemahan dalam konfigurasi SSL/TLS, seperti penggunaan protokol lama dan cipher suites yang tidak aman.
A03: Injection	Ditemukan kerentanan keamanan, yaitu parameter id pada endpoint rentan terhadap SQL injection, serta potensi serangan XSS melalui manipulasi header Referer
A04: Insecure Design	Sistem memiliki validasi yang baik untuk mencegah upload file berbahaya
A05: Security Misconfiguration	Ditemukan beberapa masalah keamanan, termasuk ketiadaan Content Security Policy (CSP), risiko Clickjacking, informasi versi server yang terekspos, serta risiko MIME-sniffing. Selain itu, tidak ada HTTP Strict Transport Security (HSTS), header Content-Type kosong atau tidak ada, masalah validasi User-Agent, dan potensi risiko dari konten yang diambil dari cache.
A06: Vulnerable Components	Ditemukan beberapa kerentanan keamanan, termasuk penggunaan versi jQuery yang rentan (CVE-2020-7656) serta adanya beberapa CVE
	yang terdeteksi di komponen sistem.
A07: Auth Failures	reCAPTCHA berhasil mencegah brute force dan Respons yang diberikan telah diidentifikasi mengandung token manajemen sesi.
A08: Software Integrity Failures	Ditemukan potensi masalah keamanan, yaitu halaman memuat satu atau lebih file skrip dari domain pihak ketiga, yang dapat meningkatkan risiko serangan, serta potensi open redirect melalui parameter URL tid.
A09: Logging/Monitoring Failures	Deteksi aktivitas serangan terbatas.
A10: SSRF	Aplikasi tidak rentan terhadap SSRF.

E. *Reporting*

TABEL 5
Hasil *Reporting*

Daftar Kerentanan	Rekomendasi Perbaikan
A01: Broken Access Control	atasi endpoint hanya menerima metode HTTP yang sesuai.
A02: Cryptographic Failures	Untuk meningkatkan keamanan, sebaiknya konfigurasi flag Secure pada cookie agar hanya dikirim melalui HTTPS, atur atribut SameSite ke Strict atau Lax untuk mencegah serangan CSRF, serta tambahkan header Cache-Control dan Pragma untuk mencegah caching informasi sensitif. Selain itu, pastikan untuk secara manual memverifikasi bahwa data timestamp tidak mengandung informasi sensitif, menggunakan konfigurasi SSL/TLS yang kuat dan terbaru, serta menonaktifkan protokol lemah. Pastikan hanya versi protokol yang aman (misalnya TLS 1.2/1.3) yang diaktifkan dan hapus cipher lemah sambil mengaktifkan

Daftar Kerentanan	Rekomendasi Perbaikan
	algoritma enkripsi yang kuat..
A03: Injection	Gunakan kueri parameter atau pustaka ORM untuk menghindari kerentanan SQL Injection. Dan bersihkan validasi semua input pengguna, termasuk header HTTP.
A04: Insecure Design	Sistem memiliki validasi yang baik untuk mencegah upload file berbahaya
A05: Security Misconfiguration	Untuk meningkatkan keamanan, sebaiknya tambahkan header Content Security Policy (CSP) untuk mencegah serangan XSS dan injeksi data, serta header X-Frame-Options untuk mengurangi risiko serangan clickjacking. Sembunyikan informasi versi server dari header HTTP dan pesan kesalahan, dan gunakan header X-Content-Type-Options: nosniff untuk mencegah sniffing tipe MIME. Selain itu, tambahkan header Strict-Transport-Security (HSTS) untuk memaksa koneksi HTTPS, serta sertakan header Content-Type dalam respons HTTP untuk menentukan format data. Pastikan untuk memvalidasi dan membersihkan header User-Agent sebelum diproses, dan memastikan bahwa respons tidak berisi informasi sensitif, pribadi, atau khusus pengguna.
A06: Vulnerable Components	Perbarui ke versi jQuery atau pustaka lainnya yang terbaru dan aman. Secara rutin perbarui dan tambal komponen pihak ketiga untuk mengatasi kerentanan yang diketahui.
A07: Auth Failures	reCAPTCHA berhasil mencegah brute force dan Respons yang diberikan telah diidentifikasi
	mengandung token manajemen sesi.
A08: Software Integrity Failures	Pastikan file sumber JavaScript hanya dimuat dari sumber tepercaya yang tidak dapat dikendalikan oleh pengguna akhir aplikasi. Selain itu, lakukan validasi dan pembatasan URL pengalihan hanya ke domain yang terpercaya untuk mengurangi potensi risiko dari sumber yang tidak sah.
A09: Logging/Monitoring Failures	Aktifkan logging yang menyeluruh dan pastikan data sensitif dikecualikan dari log.
A10: SSRF	Aplikasi tidak rentan terhadap SSRF.

V. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa sistem informasi website PT XYZ memiliki tingkat kerentanan yang dapat dianalisis menggunakan standar OWASP TOP 10 tahun 2021 melalui metode penetration testing. Hasil pengujian menunjukkan berbagai jenis kerentanan yang berpotensi dimanfaatkan oleh penyerang untuk mengeksploitasi sistem. Oleh karena itu, rekomendasi perbaikan yang diberikan diharapkan dapat meningkatkan keamanan sistem, memperkuat perlindungan terhadap ancaman siber, serta menjaga keamanan data pengguna.

REFERENSI

[1] K. Nisa, A. Putra, R. A. Siregar, and M. Dedi Irawan, “Bulletin of Information Technology (BIT) Analisis Website Tapanuli Tengah Menggunakan Metode Open Web Application Security Project Zap (Owasp Zap),” vol. 3, no. 4, pp. 308–316, 2022, doi: 10.47065/bit.v3i1.

[2] H. Azis and F. Fattah, “ANALISIS LAYANAN KEAMANAN SISTEM KARTU TRANSAKSI ELEKTRONIK MENGGUNAKAN METODE PENETRATION TESTING,” *ILKOM Jurnal Ilmiah*, vol. 11, no. 2, pp. 167–174, Aug. 2019, doi: 10.33096/ilkom.v11i2.447.167-174.

[3] Agus Wibowo, *Keamanan Sistem Jaringan Komputer*. Semarang: Yayasan Prima Agus Teknik, 2021. Accessed: Nov. 21, 2023. [Online]. Available: https://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/300

[4] I. Dermawan, A. Baidawi, Iksan, and S. Mellyana Dewi, “Serangan Cyber dan Kesiapan Keamanan Cyber Terhadap Bank Indonesia,” *Jurnal Informasi dan Teknologi*, vol. 5, no. 3, pp. 20–25, Aug. 2023, doi: 10.60083/jidt.v5i3.364.

[5] E. Z. Darojat, E. Sediyono, and I. Sembiring, “Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner,” *JURNAL SISTEM INFORMASI BISNIS*, vol. 12, no. 1, pp. 36–44, Sep. 2022, doi: 10.21456/vol12iss1pp36-44.

[6] M. Yunus, “ANALISIS KERENTANAN APLIKASI BERBASIS WEB MENGGUNAKAN KOMBINASI SECURITY TOOLS PROJECT BERDASARKAN FRAMEWORK OWASP VERSI 4,” *Jurnal Ilmiah Informatika Komputer*, vol. 24, no. 1, pp. 37–48, 2019, doi: 10.35760/ik.2019.v24i1.1988.

[7] D. F. Priambodo, A. D. Rifansyah, and M. Hasbi, “Penetration Testing Web XYZ Berdasarkan OWASP Risk Rating,” *Teknika*, vol. 12, no. 1, pp. 33–46, Feb. 2023, doi: 10.34148/teknika.v12i1.571.

[8] A. Elanda and R. Lintang Buana, “ANALISIS KUALITAS KEAMANAN SISTEM INFORMASI E-OFFICE BERBASIS WEBSITE PADA STMIK ROSMA DENGAN MENGGUNAKAN OWASP TOP 10,” 2021.

[9] B. Ghozali, “Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) untuk Penilaian Risk Rating Detect Web Application Security Flaws Using the Owasp (Open Web Application Security Project) Method for Risk Assessment,” *Dikirim: 09 Februari*, 2018.

[10] M. Awad, M. Ali, M. Takruri, and S. Ismail, “Security vulnerabilities related to web-based data,” *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 17, no. 2, pp. 852–856, 2019, doi: 10.12928/TELKOMNIKA.v17i2.10484.

[11] “OWASP Top 10 - 2021.” Accessed: Nov. 23, 2023. [Online]. Available: https://owasp.org/Top10/id/

[12] B. S. Rawal, G. Manogaran, and A. Peter, “The Basics of Hacking and Penetration Testing,” in *Cybersecurity and Identity Access Management*, Singapore: Springer Nature Singapore, 2023, pp. 21–46. doi: 10.1007/978-981-19-2658-7_2.

[13] A. Kurniawan, “Penerapan Framework OWASP dan Network Forensics untuk Analisis, Deteksi, dan Pencegahan Serangan Injeksi di Sisi Host-Based,” *Jurnal Telematika*, vol. 14, no. 1.

[14] Muchammad Zakaria, “Pengertian NMAP Adalah : Fungsi, Cara Kerja & Penggunaannya.” Accessed: Nov. 27, 2023. [Online]. Available: https://www.nesabamedia.com/pengertian-nmap/

[15] S. Hidayatulloh and D. Saptadiaji, “Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP).” [Online]. Available: http://jurnal.itg.ac.id/