ANALISIS KEAMANAN PADA WEBSITE DENGAN MENGGUNAKAN METODE PENETRATION TESTING DAN FRAMEWORK OWASP PADA WEBSITE XYZ

1st Arvynanda Pamungkas
Sistem Informasi
Telkom University
Surabaya, Indonesia
arvynanda@student.telkomuniversity.ac.id

2nd Muhammad Nasrullah
Sistem Informasi
Telkom University
Surabaya, Indonesia
emnasrul@telkomuniversity.ac.id

3rd Muhammad Ilham Alhari
Sistem informasi
Telkom University
Surabaya, Indonesia
ilhamalhari@telkomuniversity.ac.id

***Abstrak* — Dengan bertambahnya jumlah pengguna internet, keamanan jaringan telah menjadi elemen kritis yang sangat penting, mengingat dampaknya yang mencakup dalam berbagai aspek kehidupan, termasuk dalam konteks pekerjaan. Xyz adalah lembaga yang mengelola dan memberdayakan dana zakat, infaq, dan sedekah dengan amanah dan profesional. Dalam era teknologi informasi yang semakin maju, penting bagi Xyz untuk meningkatkan keamanan dan melindungi infrastruktur serta data sensitif yang ada pada Website mereka. Untuk mendukung kualitas layanan tersebut, pada penelitian ini dengan dengan metode Penetration Testing dengan framework OWASP Manfaat dari Penetration Testing untuk Website Xyz dapat mengetahui apa saja kekurangan dari keamanan yang ada pada website Xyz. Pada penelitian kali ini menggunakan metode Penetration Testing dengan menggunakan framework Open Web Application Security Project (OWASP). Pengujian berhasil menemukan beberapa kerentanan penting seperti adanya potensi *Broken Access Control* melalui akses langsung ke endpoint administratif tanpa autentikasi yang memadai (A01), kelemahan pada konfigurasi cookie dan header keamanan yang belum optimal (A02), serta indikasi kerentanan *Cross-Site Scripting* (XSS) pada parameter input pengguna (A03). Selain itu, desain sistem belum menerapkan validasi input numerik secara logis (A04), dan terdapat konfigurasi server yang tidak sesuai dengan praktik keamanan standar (A05). Penggunaan komponen perangkat lunak yang usang dan rentan (A06), ketiadaan mekanisme perlindungan terhadap serangan *brute force* serta token anti-CSRF (A07), dan praktik pemuatan skrip eksternal tanpa pembatasan yang memadai (A08) turut memperbesar risiko keamanan. Sistem juga belum menerapkan pencatatan (*logging*) dan pemantauan (*monitoring*) aktivitas secara efektif (A09).**

Kata kunci*— *Penetration Testing, Keamanan Sistem Informasi, OWASP.

I. PENDAHULUAN

Pemanfaatan internet di Indonesia terus meningkat. Menurut APJII, pada 2021–2022 terdapat 210,03 juta pengguna internet, naik 3,32% dari tahun sebelumnya [1]. Pertumbuhan ini membuka akses luas terhadap informasi, namun juga meningkatkan risiko penyalahgunaan, termasuk serangan terhadap situs web. Kasus kebocoran data BPJS Kesehatan (2021) dan aksi peretasan oleh akun anonim Bjorka (2022) menjadi bukti nyata ancaman tersebut [2]. Dalam konteks ini, penetration testing atau uji penetrasi menjadi metode penting untuk mengidentifikasi celah keamanan sistem secara proaktif. OWASP Top 10 (2021) menjadi acuan utama dalam mengklasifikasikan risiko keamanan aplikasi web, termasuk kategori seperti Broken Access Control, Cryptographic Failures, hingga Server-Side Request Forgery. Lembaga XYZ, sebagai Lembaga Amil Zakat Nasional, mengelola situs xyz.org untuk kegiatan penghimpunan dan penyaluran dana secara digital. Namun, potensi risiko seperti penyimpanan data donatur, transaksi keuangan, dan insiden keamanan sebelumnya – termasuk keberadaan file berbahaya (sym.php, c99.php) dan iklan judi yang menyusup – menandakan perlunya pengujian keamanan lebih lanjut. Untuk itu, penelitian ini akan melakukan uji penetrasi pada situs xyz.org dengan mengacu pada OWASP Top 10 guna mengidentifikasi kerentanan yang ada dan memberikan rekomendasi penguatan sistem.

II. KAJIAN TEORI

Kajian teori merupakan landasan ilmiah yang memuat serangkaian asumsi, postulat, tesis, hipotesis, proposisi. Penyusunan dasar teori dilakukan secara sistematis dengan memperhatikan keterkaitan antar variabel yang relevan untuk mendukung analisis dan interpretasi dalam suatu penelitian.

A. Sistem Informasi

Sistem Informasi (SI) merupakan sistem terpadu yang menggabungkan aktivitas manusia dan teknologi untuk mendukung fungsi manajerial dan operasional suatu

organisasi. SI mencakup interaksi antara manusia, data, informasi, teknologi, dan algoritma dalam rangka mengelola informasi secara efektif (Adani, 2021). Beberapa ahli mendefinisikan SI sebagai kumpulan komponen yang saling terhubung dan berfungsi untuk mengumpulkan, mengolah, menyimpan, dan mendistribusikan informasi guna mendukung proses pengambilan keputusan dan pengendalian dalam organisasi. SI juga merepresentasikan informasi mengenai individu, lokasi, serta berbagai elemen organisasi dan lingkungannya[3].

B. Keamanan Sistem Informasi

Keamanan Sistem Informasi adalah upaya untuk mencegah atau mendeteksi penipuan dalam sistem berbasis informasi, di mana informasi tidak memiliki bentuk fisik. Informasi merupakan aset penting yang perlu dijaga, karena kebocoran atau kegagalan sistem dapat menimbulkan kerugian finansial dan menurunkan produktivitas perusahaan[4].

C. OWASP *(Open Worldwide Application Project)*

OWASP (Open Worldwide Application Security Project) adalah organisasi nirlaba yang fokus meningkatkan keamanan perangkat lunak. Didirikan pada 2001, OWASP menyediakan sumber daya gratis seperti proyek, alat, dan panduan keamanan aplikasi. Beberapa inisiatif utamanya meliputi OWASP Top 10, Web Security Testing Guide, dan Zed Attack Proxy. OWASP juga memberikan pelatihan dan edukasi bagi pengembang serta profesional keamanan untuk menerapkan praktik terbaik dalam mengamankan aplikasi web[5].

D. Uji Penetrasi

Uji Penetrasi adalah simulasi serangan siber terhadap sistem komputer untuk mengidentifikasi kerentanannya. Meskipun memerlukan waktu dan biaya, uji ini memberikan masukan berharga dari ahli keamanan dan membantu mencegah kerugian besar. Prosesnya melibatkan tahapan yang kompleks dan terstruktur[6].

E. Identfikasi Risk Level

Identifikasi tingkat risiko (risk level) dalam penetration testing adalah proses penting untuk menilai ancaman dari kerentanan yang ditemukan. Penilaian ini didasarkan pada dua indikator utama: likelihood (kemungkinan eksploitasi) dan impact (dampak terhadap sistem atau data). Likelihood dipengaruhi oleh ketersediaan exploit, tingkat kesulitan teknis, dan akses yang dibutuhkan, sedangkan impact mencerminkan potensi kerugian pada aspek kerahasiaan, integritas, ketersediaan, dan reputasi. Nilai risiko dihitung dengan rumus Risk Level = Likelihood × Impact dan diklasifikasikan ke dalam kategori seperti rendah hingga kritis. Proses ini membantu organisasi memprioritaskan mitigasi secara efektif untuk perlindungan sistem yang berkelanjutan[7].

F. Black Box Testing

Black-box testing adalah metode pengujian di mana penguji tidak memiliki akses ke struktur internal sistem, seperti algoritma atau data. Pengujian dilakukan hanya melalui antarmuka, tanpa mengetahui cara kerja internalnya. Salah satu jenisnya adalah functional testing, yang memverifikasi apakah fitur aplikasi memenuhi persyaratan fungsional. Misalnya, jika sistem diminta menampilkan nomor telepon klien berdasarkan nomor identifikasi, maka sistem harus menunjukkan data tersebut hanya jika input valid[8].

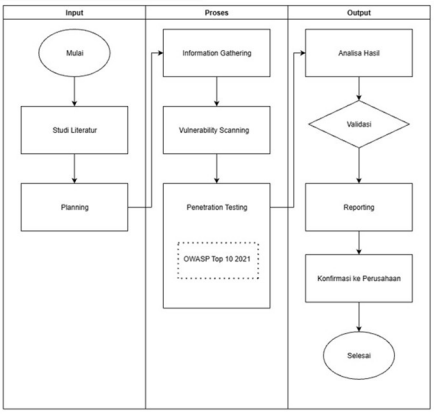
G. Fuzzing

Fuzzing adalah teknik dalam penetration testing yang menguji sistem dengan input acak, tidak valid, atau tak terduga untuk menemukan celah keamanan, seperti buffer overflow dan kesalahan validasi. Teknik ini dapat dilakukan secara black-box, white-box, atau grey-box, tergantung informasi yang dimiliki penguji. Fuzzing efektif untuk menguji ketahanan aplikasi web, protokol, dan API terhadap input berbahaya, serta mendukung pendekatan pengujian yang proaktif dalam menghadapi ancaman siber yang terus berkembang[9].

III. METODE

Peneliti menggunakan framework OWASP Top – 102021 pada pengujian penetrasi ini, sebagai pedoman utama untuk mengidentifikasi dan mengevaluasi kerentanan keamanan pada sistem, guna memastikan pengujian dilakukan sesuai dengan standar terbaik yang relevan dengan konteks penelitian.

A. Alur Penelitian



GAMBAR 1
Alur Penelitian

Pada tahapan Input, dilakukan pengumpulan studi literatur sebagai referensi. Tahap Planning mencakup analisis fitur website dan wawancara dengan pihak perusahaan untuk memperoleh informasi terkait. Selanjutnya, pada tahap Proses, dilakukan information gathering (seperti domain ID, IP, dll), vulnerability scanning, dan penetration testing. Tahap Metode menggunakan standar OWASP Top 10 2021 sebagai acuan pengujian. Terakhir, tahap Output meliputi analisis hasil pengujian, validasi terhadap standar OWASP, penyusunan laporan, dan konfirmasi ke perusahaan.

IV. HASIL DAN PEMBAHASAN

A. Planning

Pada tahapan planning ini merupakan langkah awal untukmemastikan bahwa tujuan pengujian telah sesuai, adapunwebsite yang diuji beralamat di xx1y.id. *Website* inimerupakan platform yang digunakan oleh XYZ untuk mendukung layanan konsultasi pendidikan. Pengujian

penetrasi dilakukan pada situs ini untuk mengidentifikasi celah kerentanan keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Pada tahapan ini juga dilakukan wawancara untuk mendapatkan informasi yang mendalam terkait tujuan, fungsi, dan layanan yang ditawarkan pada *website* objek.

B. Information Gathering

TABEL 1

Hasil *Information Gathering*

Tools	Hasil
Whois	Domain ID: xxxxx-xxxxxxxx, Nama Domain: xxxxxx.xx, Nama Server, alamat registrar, dan informasi lainnya yang terkait dengan web.
Nslookup	IP Address: 103.xx.xx.xxx dan 118.xx.xx.xxx, Mail Exchanger, Informasi SOA (Start of Authority) record.
Dig	IP Address: 103.xx.xx.xxx dan 118.xx.xxx.xxx)
Nmap	Port 80/HTTP, Port 443/SSL HTTP,Port 8080/HTTP, Port 8443/SSLHTTP

C. Vulnerability Scanning

Pada tahap vulnerability scanning ini dilakukan pemindaian kerentanan pada website XYZ, peneliti menggunakan sebuah aplikasi open-source yang bernama OWASP ZAP (*Zed Attack Proxy*) untuk membantu dalam proses pengidentifikasian kerentanan keamanan yang terdapat pada situs web XYZ.

D. Penetration Testing

Pada tahapan penetration testing ini peneliti melakukan serangkaian uji penetrasi dengan berbagai skenario untuk menemukan celah keamanan yang sesuai dengan OWASP Top – 10 2021.

TABEL 2

Hasil *Penetration Testing*

ID	Temuan
A01:2021 – Broken Access Control	Ditemukan celah keamanan berupa 2 file *webshell* yang perlu segera ditangani
A02:2021 – Cryptographic Failures	Ditemukan empat kerentanan terkait konfigurasi cookie dan header keamanan, seperti tidak adanya flag HttpOnly, Secure, SameSite, dan Strict-Transport-Security Header
A03:2021 – Injection	Ditemukan kerentanan minor, dan tidak ada eksploitasi serius yang terdeteksi selama pengujian ini
A04:2021 – Insecure Design	Ditemukan dua parameter yang mengandung kerentanan terkait Modern *Web Application* dan pengaturan *Cache-Control*
A05:2021 – Security Misconfiguration	Ditemukan tiga parameter yang mengandung kerentanan, seperti tidak tersedianya *header Content Security Policy* (CSP), kebocoran versi server melalui *header* "Server", dan tidak adanya X-*Content-Type-Options Header*
A06:2021 – Vulnerable and Outdated Component	Ditemukan satu parameter rentan pada file *jquery-plugin-collection.js*, yang termasuk dalam kategori *Vulnerable JS Library*. Selain itu, hasil dari Wappalyzer mengidentifikasi beberapa komponen yang telah usang dan rentan, seperti *jQuery 2.2.0, jQuery UI 1.11.4, Moment.js 2.11.0, Modernizr 2.7.1,* dan *Bootstrap 3.3.6.*
A07:2021 – Identification and Authentication Failures	Ditemukan kerentanan Absence of Anti-CSRF Tokens serta tidak adanya mekanisme pembatasan percobaan login seperti CAPTCHA
A08:2021 – Software and Data Integity Failures	Ditemukan kerentanan Cross-Domain JavaScript Source File Inclusion, yang menunjukkan bahwa situs memuat skrip dari domain eksternal tanpa kontrol yang memadai.
A09:2021 – Security Logging and Monitoring	Ditemukan server selalu merespons permintaan login dengan kode status HTTP 200, meskipun permintaan tersebut tidak valid
A10:2021 – Server-Side Request Forgery	Tidak ditemukan indikasi kerentanan SSRF pada seluruh endpoint yang diuji

E. Reporting

Pada tahapan reporting ini dilakukan penyusunan daftar temuan hasil pengujian dan pemberian rekomendasi perbaikan.

TABEL 3

Hasil *Reporting*

ID	Temuan	Rekomendasi Perbaikan
A01	*Access Control Weakness*	Terapkan RBAC(*Role Base Access Control*) dan sembunyikan struktur direktori sensitif.
	Webshell Detection	Terapkan kontrol akses berbasis peran yang ketat dan validasi parameter.
	Sensitive File Disclosure	Nonaktifkan direktori yang tidak perlu, atur permission dan lakukan hardening terhadap direktori sensitif
A02	*Cookie Without Secure Flag*	Terapkan atribut cookie HttpOnly, Secure, SameSite dan header Strict-Transport-Security

ID	Temuan	Rekomendasi Perbaikan
	Sensitive URL Exposure	Batasi akses publik ke file sensitif, konfigurasi ulang robots.txt
A03	*URL Parameter Enumeration*	Lakukan validasi dan sanitasi input, batasi parameter terbuka di URL
	Reflected XSS Test	Gunakan filter input/output untuk mencegah XSS dan pastikan parameter tidak diekspos.
	SQL Injection Detection	Tidak perlu tindakan saat ini, namun tetap lakukan update library dan audit parameter input secara berkala
	Information Disclosure – Suspicious Comments	Komentar pada kode sumber yang memuat informasi sensitif, seperti path file atau catatan debugging, harus dihapus dari tampilan publik. Jika komentar tersebut menunjukkan adanya kerentanan, masalah tersebut harus diperbaiki sebelum kode dipublikasikan.
A04	*Modern Web Application*	Tidak perlu tindakan, hanya sebagai indikator struktur aplikasi modern
	Business Logic Vulnerability	Tambahkan validasi nilai di sisi server dan batas logis atas/bawah nominal donasi
A05	*Missing Content-Security-Policy (CSP) Header*	Setel header keamanan seperti CSP, X-Content-Type-Options, dan Server header.
	Server Leaks Version via "Server" HTTP Header	Pastikan bahwa server web, server aplikasi, load balancer, dan komponen lainnya dikonfigurasi untuk menyembunyikan header "Server" atau menyediakan informasi yang bersifat umum.
	X-Content-Type-Options Header Missing	Tambahkan X-Content-Type-Options: nosniff pada semua respons web
A06	*Vulnerable JavaScript Library*	Perbarui komponen pihak ketiga ke versi terbaru dan aman.
	Outdated Frontend Component Usage	Memperbarui library dan framework lama seperti jQuery, Bootstrap, dan Moment.js demi keamanan dan performa.
A07	*Lack of Login Rate Limiting & CAPTCHA*	Tambahkan CAPTCHA dan limit login attempts (rate limiting) berdasarkan IP dan user-agent
	Brute Force Vulnerability	Terapkan proteksi brute force: lockout sementara, delay, dan pemantauan log percobaan login
	Absence of Anti-CSRF Tokens	Implementasikan anti-CSRF token unik pada setiap request login
A08	*Cross-Domain JavaScript Source File Inclusion*	Pastikan hanya memuat JS dari sumber terpercaya, dan hindari input eksternal yang bisa dikontrol pengguna
	Cross-Domain JS Inclusion – Response Headers	Audit dan pastikan respon eksternal memiliki header keamanan, atau proxy-kan konten dari trusted source
A09	*Improper Authentication Feedback*	Tambahkan penanganan yang membedakan hasil login gagal dan sukses secara aman tanpa membocorkan informasi
A10	-	-

V. KESIMPULAN

Berdasarkan hasil penelitian terhadap keamanan website XYZ menggunakan metode penetration testing dengan acuan OWASP Top 10:2021, ditemukan sejumlah kerentanan signifikan seperti Broken Access Control, Cryptographic Failures, Injection, dan Security Misconfiguration. Pengujian dilakukan dengan pendekatan black-box menggunakan alat seperti OWASP ZAP, Burp Suite, dan SQLMap. Framework OWASP Top 10 terbukti efektif sebagai panduan sistematis dalam mengidentifikasi dan mengevaluasi risiko keamanan aplikasi web. Temuan menunjukkan adanya potensi ancaman terhadap integritas, kerahasiaan, dan ketersediaan sistem, yang dapat berdampak pada kebocoran data, gangguan layanan, serta penurunan kepercayaan publik. Oleh karena itu, diperlukan tindak lanjut melalui perbaikan kerentanan berdasarkan rekomendasi teknis yang telah disusun.

REFERENSI

[1] R. Pahlevi, "APJII: Penetrasi Internet Indonesia Capai 77,02% pada 2022," databoks.

[2] CNN Indonesia, "10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-ramai Bantah Baca artikel CNN Indonesia "10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-ramai Bantah," *CNN Indonesia*, Dec. 30, 2022.

[3] R. M. Adani, "Pengertian Sistem Informasi dan Cara Penerapannya," Sekawan Media. Accessed: Nov. 23, 2023. [Online]. Available: https://www.sekawanmedia.co.id/blog/apa-itu-sistem-informasi/

[4] Erfina, E. Utami, and A. Sunyoto, "Evaluasi Tingkat Kematangan Keamanan Informasi pada Sistem Informasi Manajemen Universitas Cokroaminoto Palopo," *Jurnal Ilmiah d'Computare*, Jan. 2018.

[5] Owasp, "About The Owasp Foundation," owasp.org. Accessed: Aug. 03, 2025. [Online]. Available: owasp.org

[6] CISCO, "What Is Penetration Testing?," CISCO.

[7] OWASP, "OWASP Risk Rating Methodology," OWASP Foundation.

[8] M. T. Dashti and D. Basin, "A Theory of Black-Box Tests," Jun. 2020.

[9] H. Xie, Z. Tan, and X. Liu, "Application of Artificial Intelligence in Financial Risk Management in a

Company," in *Proceedings of the 2024 8th International Conference on Big Data and Internet of Things*, New York, NY, USA: ACM, Sep. 2024, pp. 349–354. doi: 10.1145/3697355.3697412.