Analisis Keamanan Sistem Informasi PT. XYZ Dengan Framework Issaf

1st Ahmad Mukhlis Najahul Haqq
Program Studi S1 Sistem Informasi
Universitas Telkom Surabaya
Surabaya, Indonesia
ahmadmukhlis@student.telkomuniversity.ac.id

2nd Muhammad Nasrullah, S.Kom., M.Kom.
Program Studi S1 Sistem Informasi
Universitas Telkom Surabaya
Surabaya, Indonesia
emnasrul@telkomuniversity.ac.id

3rd Rosyid Abdillah, S.Si., M.Kom.
Program Studi S1 Sistem Informasi
Universitas Telkom Surabaya
Surabaya, Indonesia
rosyidabdillah@telkomuniversity.ac.id

Abstrak* — Perkembangan teknologi informasi membuat website menjadi bagian penting dalam kegiatan operasional perusahaan, termasuk PT. XYZ yang bergerak di bidang teknologi pendidikan. Website PT. XYZ digunakan untuk menyampaikan informasi layanan, mengelola data pengguna, serta mendukung proses transaksi. Karena website ini mengelola data penting, maka diperlukan pengujian keamanan untuk mengetahui seberapa baik sistem melindungi data serta untuk menemukan kemungkinan adanya celah keamanan. Penelitian ini bertujuan untuk menilai keamanan website PT. XYZ dengan menggunakan metode penetration testing berdasarkan framework Information Systems Security Assessment Framework (ISSAF). Tahapan pengujian meliputi perencanaan dan persiapan, pelaksanaan pengujian, serta pembersihan sisa aktivitas pengujian. Proses pengujian dilakukan dengan bantuan beberapa tools keamanan, seperti Nmap, Nessus, OWASP ZAP, SQLMap, Burp Suite, Dirsearch, Hydra, dan Metasploit Framework. Hasil pengujian menunjukkan bahwa website telah memiliki mekanisme keamanan dasar, salah satunya dengan penggunaan layanan Cloudflare. Namun, masih ditemukan beberapa kelemahan, seperti pengaturan hak akses yang belum optimal, desain sistem yang kurang aman, konfigurasi keamanan yang belum tepat, serta belum adanya perlindungan terhadap serangan CSRF. Walaupun tidak ditemukan celah keamanan yang bersifat kritis, kelemahan tersebut tetap dapat menimbulkan risiko keamanan. Oleh karena itu, disarankan agar perusahaan meningkatkan pengendalian akses, memperkuat proses autentikasi, memperbaiki desain sistem, serta melakukan pengujian keamanan secara berkala.

***Kata Kunci:* Keamanan Website, Penetration Testing, ISSAF, PT. XYZ**

I. PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat di era modern telah menjadi bagian penting dalam kehidupan masyarakat (Nikum & Karuna, 2022). Salah satu bentuk pemanfaatan teknologi tersebut adalah penggunaan website sebagai media penyedia informasi dan layanan digital. Seiring waktu, website mengalami perkembangan yang signifikan, dimulai dari web 1.0 yang bersifat satu arah, kemudian berkembang menjadi web 2.0 yang memungkinkan interaksi dua arah antara pengguna dan sistem, hingga web 3.0 yang mampu mengolah serta menyimpulkan informasi secara cerdas berbasis data daring (Bashori & Ahmad Hasan, 2023). Perkembangan ini terus berlanjut pada era web 4.0 yang terintegrasi dengan konsep revolusi industri, di mana website tidak hanya berfungsi sebagai media informasi, tetapi juga terhubung dengan teknologi keamanan siber, Internet of Things (IoT), komputasi awan, serta cognitive computing (Putra & Yananto Mihadi, 2019).

Kemajuan teknologi website memberikan berbagai kemudahan bagi pengguna dan perusahaan, namun di sisi lain juga meningkatkan risiko keamanan informasi. Website yang mengelola data penting berpotensi memiliki celah keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Kerentanan tersebut dapat menimbulkan dampak serius, seperti kerugian finansial, kebocoran data, serta penurunan kepercayaan dan reputasi perusahaan (Vriano, 2023).

Beberapa kasus kebocoran data yang terjadi di Indonesia menunjukkan pentingnya perhatian terhadap aspek keamanan website. Kasus peretasan Tokopedia menyebabkan kebocoran data lebih dari 90 juta akun pengguna dan jutaan data merchant yang diperjualbelikan di dark web (Indonesia, 2024). Selain itu, Bank Syariah Indonesia (BSI) juga mengalami kebocoran data yang melibatkan jutaan informasi nasabah dan data internal perusahaan (Paramitha, 2023). Kasus lain terjadi pada Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementerian Dalam Negeri yang mengalami kebocoran ratusan juta data penduduk, mencakup berbagai informasi pribadi yang bersifat sensitif (Setiadi & Budi Arie, 2024). Tidak hanya itu, ribuan website berbasis WordPress juga dilaporkan terinfeksi malware akibat eksploitasi kerentanan pada plugin, yang dimanfaatkan untuk mengarahkan pengguna ke situs penipuan (Andhika, 2024).

Berdasarkan berbagai kasus tersebut, diperlukan upaya serius dari pemerintah dan perusahaan untuk meningkatkan keamanan aplikasi dan website yang digunakan. Salah satu metode yang umum digunakan untuk mengevaluasi keamanan sistem adalah pengujian penetrasi (penetration testing). Metode ini dilakukan dengan mensimulasikan serangan terhadap sistem secara terkontrol guna mengetahui sejauh mana sistem mampu bertahan serta mengidentifikasi potensi kerentanan yang masih ada (Zeebaree, 2020).

Pengujian penetrasi merupakan serangkaian aktivitas yang bertujuan untuk mengidentifikasi kelemahan dan celah keamanan pada sistem informasi melalui pendekatan eksploitasi yang terencana (Rabbani, 2020). Hasil dari pengujian ini dapat digunakan sebagai dasar dalam memberikan rekomendasi perbaikan keamanan. Dalam pelaksanaannya, pengujian penetrasi dapat mengacu pada berbagai framework, seperti Information Systems Security Assessment Framework (ISSAF), Penetration Testing Execution Standard (PTES), dan framework lainnya (Silmina, 2022).

PT. XYZ merupakan perusahaan yang bergerak di bidang konsultasi, pelatihan, riset, serta pendampingan berkelanjutan dalam mendukung transformasi teknologi informasi di sektor pendidikan (Mohamad Fauzi N. F., 2016). PT. XYZ menyediakan berbagai program pelatihan dan pengembangan sekolah, serta mengelola website sebagai media penyedia workshop, kursus, dan pelatihan. Dalam proses transaksi, website PT. XYZ mengelola data pribadi pengguna, termasuk data penagihan dan pembayaran, sehingga aspek keamanan website menjadi sangat penting. Hingga saat ini, website PT. XYZ belum pernah dilakukan pengujian penetrasi secara menyeluruh, sehingga diperlukan evaluasi keamanan untuk mendeteksi potensi kerentanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab (Prasetyo et al., 2020).

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk melakukan penilaian risiko keamanan website PT. XYZ melalui pengujian penetrasi menggunakan alat uji kerentanan sistem. Hasil penelitian diharapkan dapat menghasilkan rekomendasi perbaikan keamanan yang didukung oleh temuan kerentanan serta langkah mitigasi yang dapat diterapkan. Dengan demikian, penelitian ini diharapkan mampu membantu meningkatkan tingkat keamanan website PT. XYZ secara berkelanjutan serta meminimalkan risiko serangan siber di masa mendatang (Fahmi Fachri, 2021; Imperva, 2025).

II. METODE

A. Alur Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode penetration testing untuk menganalisis tingkat keamanan website PT. XYZ. Pengujian dilakukan berdasarkan kerangka kerja *Information Systems Security Assessment Framework* (ISSAF) yang menyediakan tahapan pengujian keamanan secara sistematis dan terstruktur. Pendekatan ini dipilih karena mampu mengevaluasi keamanan sistem dari sudut pandang pihak eksternal (*black-box testing*) serta menghasilkan temuan yang dapat dianalisis secara teknis dan akademik.

Pengumpulan data dilakukan melalui wawancara terstruktur dengan Divisi Sistem Informasi PT. XYZ. Wawancara ini bertujuan untuk memperoleh izin resmi pelaksanaan pengujian, memahami kondisi sistem yang diuji, serta menentukan ruang lingkup dan batasan pengujian. Selain itu, hasil wawancara digunakan sebagai dasar penyusunan rekomendasi perbaikan keamanan sistem informasi.

Pengujian keamanan dilakukan dengan memanfaatkan berbagai tools yang disesuaikan dengan tahapan ISSAF, meliputi *information gathering*, *network mapping*, *vulnerability identification*, *penetration testing*, hingga *reporting*. Tools yang digunakan antara lain Whois, Nslookup, Dig, Wappalyzer, Nmap, Nessus, OWASP ZAP, SQLMap, Burp Suite, Dirsearch, Hydra, Metasploit Framework, serta Cookie Manager. Penggunaan tools tersebut bertujuan untuk mengidentifikasi konfigurasi sistem, layanan aktif, potensi kerentanan, serta mekanisme keamanan yang diterapkan pada website PT. XYZ.

Metodologi penelitian mengikuti alur ISSAF yang diawali dengan tahap *planning and preparation*, yaitu penentuan tujuan, ruang lingkup, dan batasan pengujian agar proses berjalan aman dan terkontrol. Selanjutnya dilakukan tahap *assessment* yang mencakup pengumpulan informasi, pemetaan jaringan, identifikasi kerentanan, eksploitasi terbatas, peningkatan hak akses, enumerasi lanjutan, hingga evaluasi kemungkinan kompromi sistem. Tahap akhir adalah *clean-up and destroy artefacts* untuk memastikan tidak ada jejak pengujian yang tertinggal pada sistem target.

Hasil pengujian dianalisis dengan mengelompokkan temuan berdasarkan jenis kerentanan, dampak keamanan, dan tingkat risiko. Seluruh temuan disusun dalam bentuk laporan terstruktur yang mencakup rekomendasi perbaikan keamanan sistem. Laporan ini menjadi dasar evaluasi bagi PT. XYZ dalam meningkatkan kontrol akses, konfigurasi keamanan, serta mekanisme perlindungan sistem.

Pelaksanaan penetration testing dilakukan dengan memperhatikan aspek etika dan hukum. Seluruh pengujian dilakukan setelah memperoleh *informed consent* dari pihak PT. XYZ dan dibatasi sesuai ruang lingkup yang disepakati. Penelitian ini tidak melakukan eksploitasi berlebihan, menjaga kerahasiaan data, serta mematuhi peraturan perundang-undangan yang berlaku, termasuk UU ITE dan kode etik penelitian akademik.

III. HASIL DAN PEMBAHASAN

A. Hasil Penetration Testing

Tahap *penetration testing* dilakukan sebagai kelanjutan dari proses identifikasi kerentanan untuk memvalidasi sejauh mana potensi celah keamanan dapat direalisasikan serta dampaknya terhadap sistem website XYZ.id. Simulasi serangan dilakukan secara terbatas dan terkendali, hanya untuk pembuktian teknis, tanpa menyebabkan gangguan operasional maupun perubahan data pada sistem.

1. ***Broken Access Control***

GAMBAR 1
)Hasil Broken Access Control (Vulnerability Identification → Exploitation))

Pengujian terhadap aspek *Broken Access Control* menunjukkan bahwa server merespons permintaan HTTP yang dimodifikasi tanpa pembatasan khusus terhadap nilai *User-Agent*. Kondisi ini mengindikasikan bahwa mekanisme validasi klien belum diterapkan secara optimal dan berpotensi dimanfaatkan apabila dikombinasikan dengan teknik serangan lain.

2. Analisis Menggunakan *OpenSSL*

GAMBAR 2
(HASIL OPENSSL PADA XYZ.ID)

Berdasarkan gambar 2 ditunjukkan hasil pengujian terhadap aspek kriptografi pada website XYZ.id yang bertujuan untuk mengevaluasi penerapan mekanisme pengamanan komunikasi data. Pengujian dilakukan untuk memastikan bahwa layanan web telah menggunakan saluran komunikasi yang terenkripsi dengan baik. Hasil pengamatan menunjukkan bahwa proses komunikasi antara klien dan server dapat berlangsung secara normal tanpa ditemukan kendala yang mengindikasikan kesalahan konfigurasi. Selain itu, sistem menggunakan sertifikat keamanan digital yang diterbitkan oleh pihak penyedia terpercaya dengan status valid dan masih dalam masa berlaku. Berdasarkan temuan tersebut, dapat disimpulkan bahwa mekanisme enkripsi data pada proses transmisi telah diterapkan secara tepat dan secara umum berada pada kategori aman.

3. Pengujian *Injection* menggunakan SQLMap

GAMBAR 3
(HASIL INJECTION SQLMAP PADA XYZ.ID)

Pengujian *Injection* menggunakan SQLMap tidak menemukan parameter yang dapat dieksploitasi. Endpoint yang diuji menunjukkan penerapan validasi input dan kemungkinan penggunaan *prepared statement*, sehingga risiko *SQL Injection* tergolong rendah. Hal ini diperkuat dengan tidak ditemukannya database atau eksekusi perintah lanjutan selama pengujian.

4. Insecure Design

GAMBAR 4
(HASIL *BURPSUITE WORDPRESS LOGIN* YANG GAGAL PADA XYZ.ID)

Berdasarkan gambar 4 di atas menunjukkan proses awal ketika pengguna mencoba masuk ke website. Browser mengirimkan data login ke server, termasuk informasi akun dan identitas perangkat. Semua data tersebut digunakan oleh sistem untuk memastikan apakah pengguna yang mencoba masuk memiliki hak akses atau tidak.

5. Security Misconfiguration

GAMBAR 5
(HASIL ANALISIS HEADER HTTP MENGGUNAKAN CURL)

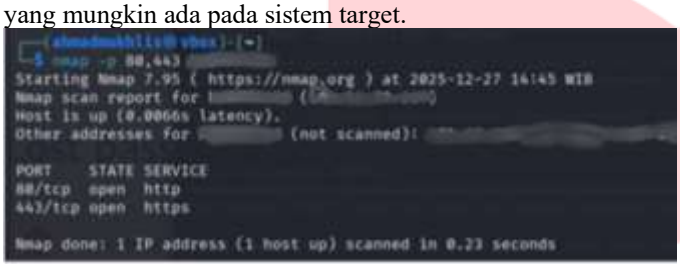
Berdasarakn gambar 5 memperlihatkan hasil pemeriksaan *HTTP response header* menggunakan perintah *curl*. Dari hasil tersebut diketahui bahwa *website* XYZ.id berada di balik layanan *Cloudflare*, menggunakan *PHP* versi 8.1, serta memanfaatkan sistem *caching* seperti *LiteSpeed*, selain itu, penerapan kebijakan keamanan seperti *Content Security Policy* juga teridentifikasi. Namun demikian, masih

terdapat informasi teknologi *backend* yang dapat dibaca secara terbuka, yang berpotensi menyebabkan information *disclosure* apabila tidak dikonfigurasi dengan pembatasan yang lebih ketat.

6. Security Logging and Monitoring Failures

Hasil pemetaan jaringan menunjukkan bahwa server website XYZ.id hanya menyediakan akses ke layanan utama yang dibutuhkan untuk operasional web. Tidak ditemukan layanan tambahan atau port yang terbuka secara tidak semestinya, temuan ini mengindikasikan bahwa konfigurasi jaringan server tergolong baik, karena hanya layanan yang diperlukan yang terekspos ke publik.

Tahapan ini merupakan bagian dari proses *Network Mapping*, yang bertujuan untuk memahami permukaan serangan (*attack surface*) dan mengevaluasi potensi risiko yang mungkin ada pada sistem target.



GAMBAR 6
(HASIL PEMINDAIAN *NMAP* PADA XYZ.ID)

7. Vulnerable and Outdated Components

GAMBAR 7
(HASIL WPSCAN PADA XYZ.ID)

Berdasarkan gambar 7 di atas menghasilkan pemindaian menggunakan *WPScan*, dapat diketahui bahwa situs XYZ.id menggunakan *Content Management System (CMS) WordPress*. *Tools* ini berhasil mengidentifikasi beberapa informasi sistem secara pasif, seperti versi *WordPress*, keberadaan file *robots.txt*, serta *endpoint API WordPress* (wp-json). Informasi diperoleh tanpa proses gangguan, sehingga menunjukkan bahwa *website* masih membuka sebagian detail teknis kepada publik. Kondisi ini berpotensi dimanfaatkan pada tahap *information gathering*, sesuai dengan tahapan awal dalam *framework* ISSAF, meskipun tidak secara langsung menunjukkan adanya eksploitasi aktif.

B. Reporting

TABLE 1
(HASIL REPORTING PADA XYZ.ID)

No	Tahap ISSAF	Tools	Hasil Pengujian	Status
1	*Information Gathering*	*Whois, Nsloockup, Dig*	Informasi domain & DNS teridentifikasi	Berhasil
2	*Technology Identification*	*Wappalyzer*	CMS & teknologi terdeteksi	Berhasil
3	*Network Mapping*	*Nmap*	*Port* xxx & xxx terbuka	Berhasil
4	*Vulnerability Identification*	*Nessus*	Temuan informasional & konfigurasi	Ditemukan
5	*Web Vulnerability Scan*	*OWASP ZAP*	*Absence of Anti-CSRF* Token	Ditemukan
6	*Exploitation*	*SQL Map*	*SQL Injection* tidak berhasil	Aman
7	*Authentication Testing*	*Hydra*	*Brute force* failed	Aman

IV. KESIMPULAN

Berdasarkan hasil evaluasi keamanan sistem informasi menggunakan kerangka kerja *Information Systems Security Assessment Framework* (ISSAF), dapat dinyatakan bahwa tingkat keamanan website yang menjadi objek penelitian berada pada kondisi relatif memadai. Walaupun demikian, masih ditemukan beberapa kelemahan yang tergolong signifikan, terutama pada tahapan identifikasi kerentanan, proses eksploitasi, dan pengujian akses, yang berpotensi menimbulkan risiko apabila tidak segera ditangani. Penerapan ISSAF dinilai efektif karena mampu menyajikan alur pengujian yang sistematis dan terstruktur, sehingga memberikan pemahaman yang komprehensif mengenai kondisi keamanan sistem secara menyeluruh. Hasil pengujian penetrasi menunjukkan adanya sejumlah celah teknis, seperti desain parameter input yang belum optimal dan berpotensi terhadap serangan injeksi, penerapan kontrol akses serta mekanisme otorisasi yang masih kurang ketat, keberadaan halaman login tersembunyi yang dapat memperluas permukaan serangan, serta konfigurasi keamanan pada tingkat server dan aplikasi yang belum sepenuhnya sesuai dengan standar praktik terbaik. Dari sisi ketahanan sistem, mekanisme autentikasi telah menunjukkan kemampuan yang cukup baik dalam menghadapi serangan otomatis, namun tetap diperlukan peningkatan pengamanan untuk mengantisipasi bentuk serangan yang lebih kompleks dan berkelanjutan di masa mendatang demi menjaga keamanan dan kerahasiaan data pengguna.

REFERENSI

A. M. Rabbani, A. B. (2020). e-Proceeding of Engineering. *Implementasi Dan Analisis Security Auditing Menggunakan Open Source Software Dengan Framework Mitre Attack, 7*(2), 7080-7087.

andhika. (2024, September 23). *Terdapat Lebih dari 17.000 Situs WordPress Diserang Balada Injector*. Dipetik Desember 22, 2023, dari Linked In: https://id.linkedin.com/pulse/terdapat-lebih-dari-17000-situs-wordpress-diserang-balada-injector-7hzdc

Bashori, Ahmad Hasan. (2023). *Pendidikan Transformatif Menjawab Tantangan "The 5.0 Era"*. Surabaya: XYZ Indonesia.

Esi Putri Silmina, A. F. (2022). Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test Dan ISSAF. *Transmisi : Jurnal Ilmiah Teknik Elektro, 24*(3), 83-91.

Fahmi Fachri, A. F. (2021). Analisis Keamanan Webserver Menggunakan Penetration Test. *Journal Informatika, 8*(2), 183-190. Diambil kembali dari https://www.researchgate.net/publication/354277125_Analisis_Keamanan_Webserver_menggunakan_Penetration_Test

Imperva. (2025, Agustus 20). *Penetration Testing*. (penetration-testing) Dipetik January 5, 2024, dari Thales Cybersecurity: https://www.imperva.com/learn/application-security/penetration-testing/

Indonesia, C. (2024, juni 12). *Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan dijual*. (https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual/) Dipetik November 20, 2023, dari https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual/

Mohamad Fauzi N. F. (2016). website XYZ. *https://XYZ.id/*, 3.

Nikum, Karuna. (2022). Answers to the Societal Demands with Education 5.0: Indian Higher Education System. *Journal of Engineering Education Transformations, 36*(36), 115-127.

Paramitha, D. D. (2023, November 27). *15 Juta Data Nasabah BSI Diduga Bocor, Pakar Siber: Hati-hati Serangan Phishing ke Pemilik Rekening*. Dipetik November 20, 2023, dari Tempo: https://bisnis.tempo.co/read/1726521/15-juta-data-nasabah-bsi-diduga-bocor-pakar-siber-hati-hati-serangan-phising-ke-pemilik-rekening

Prasetyo, S. Eko, N. Hassanah. (2020). Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode Issaf. *Jurnal Ilmiah Informatika*, 45-55.

Putra, Yananto Mihadi. (2019). Analysis of Factors Affecting the Interests of SMEs Using Accounting Applications. *Analysis of Factors Affecting the Interests of SMEs Using Accounting Applications. Journal of Economics and Business*, 818-826.

Setiadi, Budi Arie. (2024, November 1). *iData Pribadi 337 Juta Penduduk Indonesia Diduga Bocor, Kominfo Bakal Lakukan Pemeriksaan*. Dipetik January 29, 2024, dari Liputan6: https://www.liputan6.com/tekno/read/5346772/data-pribadi-337-juta-penduduk-indonesia-diduga-bocor-kominfo-bakal-lakukan-pemeriksaan

Subhi R. M. Zeebaree, K. J. (2020). Indonesian Journal of Electrical Engineering and Computer Science. *Impact analysis of SYN flood DDoS attack on HAProxy and NLB cluster-based web servers, 19*(1), 510-517.

Vriano. (2023). Pengujian Keamanan Web Juice Shop Dengan Metode Pentesting Berbasis OWASP Top 10. *Jurnal Sains dan Teknologi, 1*(6), 91-100.