Analisis Keamanan Sistem Informasi pada Website Dinas Perpustakaan dan Kearsipan Kota Surabaya Menggunakan Metode ISSAF

1st Steven Hephzibah Olin
Fakultas Rekayasa Industri
Universitas Telkom
Surabaya, Indonesia
stevenhephzibaholin@student.telkomuniversity.ac.id

2nd Kharisma Monika Dian Pertiwi
Fakultas Informatika
Universitas Telkom
Surabaya, Indonesia
kharismamonikadp@telkomuniversity.ac.id

3rd Muhammad Ilham Alhari
Fakultas Rekayasa Industri
Universitas Telkom
Surabaya, Indonesia
ilhamalhari@telkomuniversity.ac.id

***Abstrak* — Penelitian ini bertujuan untuk menganalisis celah keamanan serta ancaman terhadap integritas dan kerahasiaan informasi dalam sistem informasi website Dinas Perpustakaan dan Kearsipan Kota Surabaya menggunakan kerangka kerja ISSAF (Information Systems Security Assessment Framework). Latar belakang penelitian ini adalah pentingnya keamanan data dan informasi dalam memastikan keberlangsungan sistem, yang belum sepenuhnya disadari oleh Dinas Perpustakaan dan Kearsipan. Metode yang digunakan meliputi pengujian terhadap sistem keamanan, khususnya terkait dengan SSL dan versi PHP yang digunakan. Hasil penelitian menunjukkan bahwa meskipun sistem tergolong aman, terdapat celah keamanan yang perlu segera diperbaiki untuk mengurangi risiko eksploitasi kerentanan, seperti pada sistem keamanan SSL dan penggunaan versi PHP yang lama. Rekomendasi utama dari penelitian ini adalah untuk memperbarui protokol keamanan dan bahasa pemrograman ke versi terbaru guna meningkatkan tingkat keamanan sistem secara keseluruhan. Kesimpulan dari penelitian ini adalah bahwa peningkatan dan pengelolaan sistem keamanan website Dinas Perpustakaan dan Kearsipan Kota Surabaya dapat dilakukan dengan efektif melalui implementasi rekomendasi yang disarankan. Penelitian ini diharapkan dapat membantu pihak Dispusip dalam meningkatkan keamanan dan pengelolaan sistem informasi yang lebih baik.**

***Kata kunci*— keamanan data, sistem informasi, issaf, celah keamanan, rekomendasi keamanan, peningkatan sistem keamanan.**

I. PENDAHULUAN

Perkembangan teknologi yang semakin canggih menciptakan kemudahan dalam berbagai kegiatan manusia. Dengan berkembangnya teknologi dan ditemukannya jaringan internet, manusia menjadi lebih mudah dalam mengakses informasi dan membagikan data ke seluruh dunia. Kemudahan yang ditawarkan sepadan dengan risiko yang dapat muncul dari berbagai hal. Ancaman di dunia digital, terutama website, dapat mempengaruhi sistem secara keseluruhan. Ancaman ini dapat berasal dari berbagai sumber, seperti serangan peretas (hacker) yang berusaha merusak atau mencuri data sensitif, dan malware yang dapat merusak integritas sistem. Mengingat banyaknya informasi penting yang disimpan dan diakses melalui website, pengembang dan administrator website harus memastikan bahwa sistem keamanan yang kuat dan terkini diterapkan untuk melindungi data dan privasi pengguna[1].

Website adalah dokumen yang berisi banyak tautan untuk menghubungkan satu dokumen dengan dokumen lainnya. Dengan menggunakan browser pada smartphone atau komputer, pengguna dapat mengakses website dari mana saja dan kapan saja, menjadikannya pilihan terbaik untuk memudahkan pekerjaan manusia sehari-hari. Berdasarkan publikasi International Telecommunication Union (ITU), Global Cyber Security Index Indonesia pada tahun 2020 berada pada peringkat ke-24 dari 194 negara. Meskipun peringkat ini cukup baik, masih ada beberapa peristiwa kebocoran data, seperti data BPJS, Kementerian Kesehatan, E-KTP, dan situs Badan Intelijen Negara (BIN) yang diretas dan dijual di forum jual beli data. Kejadian ini menimbulkan pertanyaan tentang peran dan kemampuan negara dalam menjaga integritas dan kerahasiaan data pribadi[2].

Permasalahan yang dihadapi adalah masih banyak sistem yang belum menerapkan keamanan yang layak, seperti belum adanya menu login pada bagian registrasi tamu dan kurangnya enkripsi data. Selain itu, belum pernah dilakukan uji coba keamanan karena keterbatasan pengetahuan dan sumber daya, sehingga pihak Dinas Perpustakaan dan Kearsipan tidak mengetahui celah dan kerentanan yang ada pada website ini. Akhir-akhir ini, seorang hacker bernama Bjorka menjadi topik perbincangan di internet, termasuk di Indonesia. Dari akhir Agustus hingga awal September 2022, Bjorka diketahui telah menyebarkan sejumlah data sensitif, termasuk angka telepon, kartu identitas, dan kartu keluarga. Data ini diperoleh dari berbagai sumber asli, seperti operator internet Indihome, biaya pemilihan umum (KPU), dan prosedur pendaftaran kartu SIM. Menurut studi dan analisis yang dilakukan oleh DAKA Advisory, kerugian yang disebabkan oleh kejahatan siber di Indonesia diperkirakan sebesar $895 miliar, atau sekitar 1,20% dari total perkiraan

kerugian global akibat kejahatan siber sebesar $71,620 miliar[3].

Penelitian ini bertujuan untuk menganalisis keamanan website Dispusip guna mengetahui celah dan kerentanan yang ada. Pengujian akan dilakukan menggunakan metode Penetration Testing, yaitu simulasi serangan yang terkendali untuk mengidentifikasi kerentanan pada aplikasi, website, jaringan, dan sistem informasi. Jika ditemukan celah keamanan, maka akan dapat diidentifikasi dan ditangani lebih awal sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab. Framework yang digunakan dalam penelitian ini adalah The Information System Security Assessment Framework (ISSAF). ISSAF adalah kerangka terstruktur yang mengategorikan penilaian keamanan sistem informasi dalam berbagai domain dan kriteria. Pengujian dilakukan dengan lebih dari satu metode penyerangan untuk meminimalisir kemungkinan tidak ditemukannya kerentanan. Tujuan penelitian ini adalah menemukan aspek kerentanan pada website berdasarkan framework ISSAF dan memberikan rekomendasi perbaikan untuk meningkatkan keamanan website Dinas Perpustakaan dan Arsip Kota Surabaya.

II. KAJIAN TEORI

A. Keamanan Sistem Informasi

Keamanan sistem informasi adalah tindakan untuk mencegah atau mendeteksi penipuan dalam sistem berbasis informasi yang tidak memiliki bentuk fisik, dengan melindungi beberapa aspek utama yaitu kerahasiaan, integritas dan ketersediaan[4].

B. Serangan Keamanan Siber (Cyber Security Attack)

Serangan keamanan siber adalah serangan yang dilakukan oleh individu, kelompok, organisasi, atau negara terhadap sistem informasi komputer, jaringan, infrastruktur, atau perangkat pribadi yang biasanya bersumber anonim. Serangan siber dapat berupa berbagai jenis serangan, seperti kebocoran data, pencurian identitas, serangan malware, dan pengumpulan data informasi untuk mencari celah keamanan [5].

C. Information System Security Assessment Framework

Information System Security Assessment (ISSAF) adalah sebuah framework yang terstruktur dan membagi keamanan sistem informasi ke dalam berbagai kategori dan evaluasi yang spesifik. Tujuannya adalah untuk memberikan masukan dan rekomendasi untuk penilaian keamanan berbasis alur kerja yang nyata dan dapat digunakan sebagai dasar untuk memverifikasi keamanan sistem informasi[6].

D. Penetration Testing

Penetration Testing adalah metode untuk menguji kerentanan dalam sistem, mengidentifikasi bug, konfigurasi yang tidak sesuai, kesalahan perangkat keras dan perangkat lunak serta kelemahan teknis yang ada pada sistem informasi yang diujikan. Penetration Testing berguna untuk mengidentifikasi dan memperbaiki kerentanan infrastruktur jaringan, menunjukkan betapa rentannya serangan berbahaya dan ancaman pada jaringan tersebut[7].

E. Blackbox Testing

Pada pendekatan ini penguji memiliki pengetahuan yang terbatas atau hanya memiliki sedikit informasi tentang target yang akan diuji. Penguji hanya mencari tahu dan memeriksa setiap celah keamanan sistem berdasarkan kemampuan, pengetahuan, pengalaman maupun keahlian. Tujuan penguji pada dasarnya adalah untuk mengaudit keamanan dari sumber luar dengan cara mensimulasikan atau menempatkan diri sebagai attacker[7].

III. METODE

A. Metode yang digunakan

Metode yang digunakan dalam penelitian ini berupa wawancara. Tujuan dari wawancara adalah mendapatkan sejumlah informasi, mendiskusikan serta menentukan rekomendasi perbaikan.

B. Alat dan Bahan Penelitian

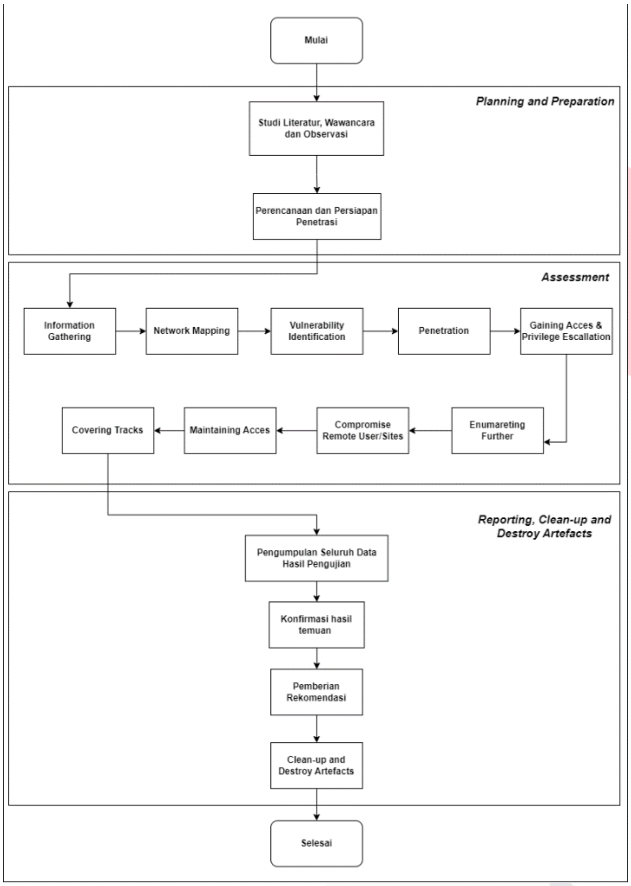
Tabel 1
Alat dan Bahan

No	Tahapan	Tools/Metode	Fungsi
1.	Sistem Operasi	*Oracle VM Virtualbox, Kali Linux*	*Tools* yang akan digunakan untuk menjalankan sistem operasi dan pengujian penetrasi (*Penetration Testing*)
2.	*Information Gathering*	*Whois, ping, nslookup*	Mengumpulkan informasi umum dan memperoleh domain lain yang terkait *website.*
3.	*Network Mapping*	*Nmap, traceroute*	Melakukan *Port Scanning*
4.	*Vulnerability Identification*	*Nessus* dan *Owaspzap*	Melakukan pemindaian *Vulnerability*
5.	*Penetration Testing*	*SQL map, XSS (Cross-Site Scripting)*	Melakukan serangan *SQL Injection* dan XSS
6.	*Gaining Acces and Privilege Escalation*	*Burp Suite, hydra* dan *Metasploit*	Memperoleh informasi akun pada *website* dan memperoleh halaman login page
7.	*Enumerating Further*	*Whireshark* dan *Cookie manager*	Memperoleh informasi *Password* dan informasi *cookies*
8.	*Compromise Remote User/Sites*	*Manual Test*	Memperoleh akses remote ke dalam *website*

No	Tahapan	Tools/Metode	Fungsi
9.	*Maintaining Access*	*Manual Test*	Melakukan penanaman *backdoor*
10.	*Covering Tracks*	*Manual Test*	Menghapus log serangan

C. Alur Penelitian

Pada penelitian ini menggunakan kerangka kerja ISSAF. Alur pada penelitian ini dapat dilihat pada gambar berikut



Gambar 1
Alur Penelitian

IV. HASIL DAN PEMBAHASAN

A. Information Gathering

Penggunaan alat seperti Ping, Whois, dan Nslookup dapat mengungkap informasi sensitif seperti alamat IP, email, nomor telepon, serta server DNS dan email administrator. Misalnya, alat Ping dapat memaparkan sistem pada risiko serangan DDoS, yang dapat diatasi dengan menerapkan sistem keamanan CDN dan WAF. Sementara itu, Whois dan Nslookup dapat mengekspos informasi yang dapat dimanfaatkan untuk serangan phishing atau eksploitasi DNS, yang direkomendasikan untuk dilindungi melalui otentikasi dua faktor (2FA) dan DNSSEC.

B. Network Mapping

Penggunaan Nmap menunjukkan bahwa banyak port yang terbuka seperti port 21, 80, 443, 554, dan 1723. Port-port ini dapat menjadi pintu masuk bagi akses tidak sah, sehingga penting untuk menutup port yang tidak diperlukan. Alat lain seperti Traceroute digunakan untuk melacak dan mengidentifikasi jalur jaringan, namun tidak memberikan dampak negatif yang signifikan.

C. Vulnerability Identification

Penggunaan Nessus dan OWASP ZAP berhasil mengidentifikasi berbagai kerentanan, seperti penggunaan protokol SSL versi 2 dan 3 yang rentan, versi PHP yang tidak didukung, serta konfigurasi server Apache dan NGINX yang kurang aman. Rekomendasi yang diberikan termasuk menonaktifkan protokol SSL yang lama, memperbarui versi PHP dan server Apache, serta mengkonfigurasi server NGINX untuk membatasi akses ke metadata instance dan menutup potensi eksploitasi.

D. Penetration Testing

Alat seperti Sqlmap dan Metasploit digunakan untuk menguji kelemahan SQL Injection dan serangan brute force. Namun, tes ini gagal karena server telah dilengkapi dengan WAF dan mekanisme keamanan seperti rate limiting dan firewall yang efektif. Rekomendasi untuk meningkatkan keamanan termasuk memastikan WAF dikonfigurasi dengan benar, memperbarui rate limiting, dan menerapkan CAPTCHA.

E. Gaining Access and Privilege Escalation

Penggunaan alat seperti Hydra dan Burp Suite menguji keamanan login, namun gagal karena mekanisme rate limiting dan firewall yang ada. Ini menunjukkan pentingnya mempertahankan dan memperbarui konfigurasi keamanan seperti firewall dan Intrusion Detection/Prevention Systems (IDS/IPS).

F. Enumerating Further

Alat seperti Wireshark dan Cookie Manager digunakan untuk merekam dan mengelola data sensitif. Namun, sistem keamanan website telah menggunakan protokol TLS 1.2 dan 1.3, yang berhasil mengenkripsi data antara klien dan server. Selain itu, cookie yang ditemukan, seperti _csrf, phpsessid, dan ci_session, dilindungi dengan baik menggunakan flag HttpOnly dan isSession. Rekomendasi termasuk mempertahankan konfigurasi TLS terbaru dan melanjutkan penggunaan flag keamanan pada cookie untuk melindungi data sensitif dan meningkatkan manajemen sesi pengguna..

G. Compromising Remote Users/Sites

Tahap ini gagal karena sistem keamanan telah menerapkan pembatasan jumlah percobaan login yang dapat mencegah upaya serangan. Kegagalan ini juga disebabkan oleh kegagalan pada tahap sebelumnya (gaining access and privilege escalation).

H. Maintaining Access

Tahap ini tidak dapat tercapai karena kegagalan pada tahap sebelumnya. Penanaman backdoor sangat tidak dianjurkan karena dampaknya serius, seperti perusakan sistem dan kebocoran data sensitif secara permanen.

I. Covering Tracks

Tahap ini tidak berhasil karena kegagalan dalam tahap-tahap sebelumnya. Sistem keamanan yang baik mencegah akses lebih lanjut, sehingga upaya untuk menghapus jejak serangan tidak diperlukan.

V. KESIMPULAN

Penelitian ini menggunakan framework ISSAF yang sangat membantu karena tahapan-tahapannya terstruktur dan sistematis. Framework ISSAF terdiri dari sembilan tahap yang terbagi menjadi beberapa bagian, seperti pencarian informasi (Information Gathering dan Network Mapping), pencarian kerentanan (Vulnerability Identification), pengujian dan serangan (Penetration Testing, Gaining Access and Privilege Escalation), serta pencarian data sensitif seperti cookie (Enumerating Further). Tahap lanjutan dari framework ini mencakup Compromise Remote User/Sites, Maintaining Access, dan Covering Tracks yang berfokus pada memperoleh, mengendalikan, dan mempertahankan akses istimewa.

Dalam penerapan langkah-langkah penetration testing pada website Dinas Perpustakaan dan Kearsipan Kota Surabaya, ditemukan beberapa celah keamanan yang signifikan. Celah ini meliputi data informasi penting seperti alamat IP, email, nomor telepon, dan server number, serta beberapa port yang terbuka seperti port 21, 80, 443, 554, dan 1723. Selain itu, terdapat dua celah keamanan dengan kategori critical, yaitu deteksi protokol SSL versi 2 dan 3 yang rentan, serta versi PHP yang belum diperbarui. Celah keamanan lain yang ditemukan mencakup konfigurasi server NGINX yang memungkinkan akses ke metadata instance (high severity) dan beberapa masalah yang teridentifikasi pada PHP, Apache HTTP Server, dan Apache HTTPS (kategori mixed). Selain itu, ada juga beberapa kerentanan dengan tingkat medium dan low yang harus diperhatikan.

Berdasarkan analisis yang dilakukan, penelitian ini memberikan lima rekomendasi utama untuk meningkatkan keamanan. Pertama, menggunakan Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) untuk memantau dan memblokir akses mencurigakan. Kedua, memblokir lalu lintas yang mencurigakan, termasuk pemindaian port dan upaya pemetaan jaringan, melalui firewall IDS atau IPS. Ketiga, memfilter dan membatasi port yang terbuka hanya untuk layanan yang benar-benar diperlukan serta membatasi akses ke port tertentu. Keempat, menonaktifkan layanan port yang tidak diperlukan dan memastikan semua perangkat lunak, termasuk sistem operasi, server web, dan aplikasi diperbarui secara rutin dengan patch keamanan terbaru. Kelima, menggunakan Web Application Firewall (WAF) untuk mencegah serangan dari luar atau pihak ketiga, sehingga meningkatkan keamanan website secara keseluruhan. Penelitian ini menekankan pentingnya penerapan langkah-langkah keamanan yang tepat untuk melindungi website dari potensi ancaman dan serangan yang beragam.

REFERENSI

[1] A. W. Wardhana and H. B. Seta, “Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada Website Universitas XYZ,” vol. 3, p. 2021.

[2] M. P. Aji, “Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective],” *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, vol. 13, no. 2, pp. 222–238, Jan. 2023, doi: 10.22212/jp.v13i2.3299.

[3] F. Indah *et al.*, “Jurnal Bidang Penelitian Informatika Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka),” 2022. [Online]. Available: https://ejournal.kreatifcemerlang.id/index.php/jbpi

[4] “Keamanan sistem Informasi”.

[5] L. Kestina and G. Widi Nurcahyo, “Penanganan Celah Keamanan Website dengan Ethical Hacking dan Issaf Menggunakan Acunetix Vulnerability (Studi Kasus di Bkpsdmd Kabupaten Kerinci)”.

[6] R. Umar, I. Riadi, M. Ihya, and A. Elfatiha, “Analisis Keamanan Sistem Informasi Akademik Berbasis Web Menggunakan Framework ISSAF”.

[7] G. Ary, S. Sanjaya, G. Made, A. Sasmita, D. Made, and S. Arsa, “Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF.”