BHATARA: Jurnal Multidisiplin
Vol. 3, No.1, Januari 2026, pp. 24-31, ISSN: 2476-9843

Analisis Hasil Uji Penetrasi Menggunakan Metode *Information Systems Security Assessment Framework* (ISSAF) pada Website

Iyondiansyah Eka Cahyo[1], Hastari Utama[2]
[1]Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta
[2]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta

Jl. Ring Road Utara, Ngringin, Condongcatur, Kec. Depok, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55281

Coresponding e-mail: [1]iyondiansyahekacahyo@students.amikom.ac.id

Abstrak

Ancaman keamanan pada situs web sering kali disebabkan oleh adanya celah keamanan yang dapat dimanfaatkan pihak tidak berwenang untuk melakukan tindakan berbahaya. Penelitian ini bertujuan untuk menganalisis kerentanan keamanan pada website dummy dengan menerapkan metode Information Systems Security Assessment Framework (ISSAF) dalam pelaksanaan uji penetrasi. Pengujian dilakukan menggunakan pendekatan black box testing dengan fokus pada tiga jenis serangan umum: SQL Injection, Cross-Site Scripting (XSS), dan Cross-Site Request Forgery (CSRF). Hasil penelitian mengidentifikasi bahwa SQL Injection tergolong risiko sedang, sedangkan XSS dan CSRF termasuk dalam kategori risiko tinggi berdasarkan analisis faktor ancaman dan dampak teknis-bisnis. Rekomendasi mitigasi yang diusulkan meliputi penerapan prepared statements, Content Security Policy (CSP), dan CSRF token untuk meningkatkan keamanan sistem. Penelitian ini diharapkan dapat menjadi acuan dalam pengujian dan peningkatan keamanan aplikasi web berbasis kerangka kerja terstruktur.

***Kata Kunci**: Uji Penetrasi, ISSAF, SQL Injection, Cross-Site Scripting, CSRF, Keamanan Website.*

Abstract

Website security threats are often caused by vulnerabilities that can be exploited by unauthorized parties to perform harmful actions. This study aims to analyze security vulnerabilities in a dummy website by implementing the Information Systems Security Assessment Framework (ISSAF) method in penetration testing. The testing was conducted using a black box testing approach, focusing on three common attack types: SQL Injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF). The results identified that SQL Injection is classified as a medium risk, while XSS and CSRF fall into the high-risk category based on threat agent and technical-business impact analysis. Proposed mitigation recommendations include implementing prepared statements, Content Security Policy (CSP), and CSRF tokens to enhance system security. This study is expected to serve as a reference for testing and improving the security of web applications based on a structured framework.

***Keywords:** Penetration Testing, ISSAF, SQL Injection, Cross-Site Scripting, CSRF, Website Security*

1. Pendahuluan

Perkembangan teknologi internet di Indonesia menunjukkan peningkatan signifikan dari tahun ke tahun, di mana pengguna internet pada tahun 2024 diperkirakan mencapai lebih dari 221 juta orang (APJII, 2024 dalam [18]). Pertumbuhan ini tidak hanya membawa dampak positif dalam bidang pendidikan, bisnis, dan interaksi sosial, tetapi juga diikuti oleh meningkatnya ancaman keamanan siber. Data Badan Siber dan Sandi Negara (BSSN) mencatat bahwa dalam periode Januari hingga September 2022, Indonesia mengalami lebih dari 852 juta anomali lalu lintas siber, dengan infeksi malware mencapai 55,6%, kebocoran data 15,20%, dan serangan trojan sebesar 10,21% (BSSN, 2022 dalam [18]). Kondisi ini mengindikasikan bahwa kerentanan sistem informasi, terutama pada platform berbasis web, menjadi celah yang sering dimanfaatkan oleh pihak tidak berwenang untuk melakukan aksi kriminal.

Salah satu ancaman yang sering muncul adalah serangan melalui website yang terinfeksi, di mana pengguna tidak menyadari bahwa aktivitas penjelajahan mereka dapat menjadi pintu masuk bagi malware. Data menunjukkan bahwa 21,2% pengguna internet di Indonesia mengalami serangan melalui web, menempatkan Indonesia pada peringkat ke-96 secara global dalam hal risiko penjelajahan web (CNN Indonesia, 2024). Contoh konkret terjadi pada tahun 2024, di mana sebuah universitas menjadi target serangan yang menyamar sebagai tawaran pekerjaan freelance, namun sebenarnya berisi malware Remote Access Trojan (RAT) untuk mengintai aktivitas korban (Hackread, 2019). Fenomena ini menguatkan urgensi dilakukannya evaluasi keamanan website secara sistematis dan berkelanjutan.

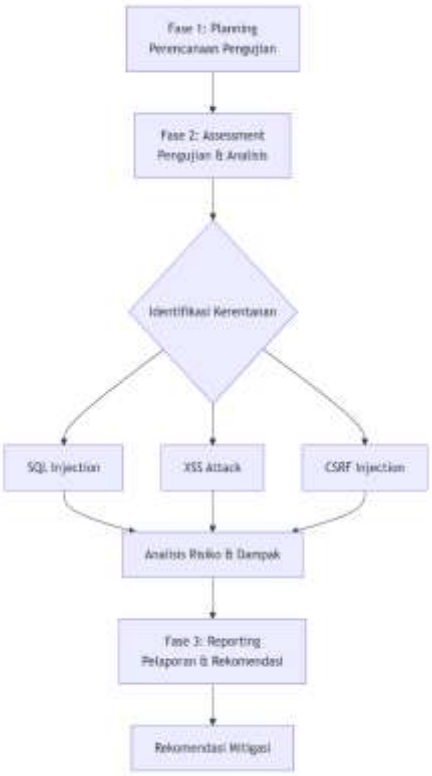
Untuk mendeteksi dan mengevaluasi kerentanan keamanan pada sistem informasi, salah satu pendekatan yang dapat digunakan adalah pengujian penetrasi (*penetration testing*). Metode ini mensimulasikan serangan yang mungkin dilakukan oleh penyerang untuk mengidentifikasi kelemahan sebelum dieksploitasi secara nyata. Dalam konteks ini, kerangka kerja Information Systems Security Assessment Framework (ISSAF) menjadi relevan karena menawarkan cakupan pengujian yang komprehensif, baik dari sisi eksternal maupun internal sistem, serta menyediakan tahapan terstruktur mulai dari perencanaan hingga pelaporan (Rochman dkk., 2021). ISSAF juga dinilai mampu mengungkap berbagai celah keamanan umum seperti SQL Injection dan Cross-Site Scripting (XSS) serta memberikan rekomendasi perbaikan yang terukur (F. Mario dkk., 202). Berdasarkan latar belakang tersebut, penelitian ini difokuskan untuk menganalisis hasil uji penetrasi pada website dummy menggunakan metode ISSAF. Rumusan masalah yang diangkat meliputi: (1) Bagaimana cara melakukan analisis uji penetrasi menggunakan framework ISSAF untuk mengidentifikasi celah keamanan pada website dummy? (2) Apa saja kerentanan yang terdeteksi? (3) Bagaimana strategi mitigasi yang dapat diterapkan untuk meningkatkan keamanan website? Penelitian ini dibatasi pada pengujian black box terhadap website dummy, dengan hanya menguji tiga jenis serangan utama berdasarkan ISSAF, yaitu SQL Injection, XSS, dan CSRF, tanpa melakukan eksploitasi lanjutan yang dapat merusak sistem.

Secara umum, penelitian ini diharapkan dapat memberikan kontribusi baik secara teoretis maupun praktis. Secara teoretis, hasil penelitian dapat menambah referensi mengenai penerapan ISSAF dalam pengujian keamanan website. Secara praktis, penelitian ini dapat menjadi panduan bagi pengelola website dalam melakukan evaluasi keamanan sebelum sistem diimplementasikan secara riil. Dengan demikian, upaya pencegahan dan mitigasi risiko siber dapat dilakukan lebih dini, sehingga integritas, kerahasiaan, dan ketersediaan data dapat tetap terjaga.

2. Metode Penelitian

Penelitian ini menerapkan pendekatan kualitatif eksploratif dengan metode uji penetrasi (*penetration testing*) untuk menganalisis kerentanan keamanan pada sebuah website dummy. Kerangka kerja utama yang digunakan adalah Information Systems Security Assessment Framework (ISSAF), yang dipilih karena menyediakan tahapan sistematis dan terstruktur dalam mengevaluasi keamanan sistem informasi, mulai dari perencanaan, pengumpulan informasi, analisis kerentanan, hingga pelaporan hasil (Sarker dkk., 2023). Metode ini dianggap sesuai karena mampu mengidentifikasi celah keamanan secara komprehensif baik dari sisi eksternal maupun internal sistem, sekaligus memberikan rekomendasi mitigasi berbasis risiko. Penelitian

ini dirancang dengan pendekatan *grey box testing*, di mana sebagian informasi tentang struktur website telah diketahui sebelumnya, sehingga memungkinkan analisis yang lebih mendalam tanpa mengabaikan perspektif eksternal sebagaimana dalam black box testing. Adapun alur penelitian ini mengikuti tahapan sistematis berdasarkan framework ISSAF, yang dimulai dari perencanaan hingga pelaporan. Secara visual, alur penelitian dapat ditunjukkan pada Gambar 1.



Gambar 1. Tahapan Penelitian

2.1. Fase Planning

Fase *planning* atau perencanaan merupakan tahap awal yang krusial untuk menetapkan fondasi pengujian penetrasi. Pada fase ini, peneliti mendefinisikan ruang lingkup dan tujuan pengujian dengan jelas, termasuk penetapan target yaitu website dummy yang telah dikonfigurasi secara khusus untuk mensimulasikan kerentanan keamanan nyata. Pemilihan framework ISSAF didasarkan pada kemampuannya menyediakan struktur metodologis yang komprehensif dan sistematis, mencakup seluruh siklus pengujian dari persiapan hingga evaluasi akhir (Sarker dkk., 2023). Selain itu, pada fase ini juga ditetapkan pendekatan *grey box testing*, di mana peneliti memiliki pengetahuan terbatas tentang sistem target, sehingga dapat mensimulasikan ancaman eksternal sekaligus melakukan analisis internal yang terarah. Aspek etis dan legal juga dipertimbangkan dengan memastikan bahwa pengujian hanya dilakukan pada lingkungan terkontrol tanpa melanggar regulasi keamanan siber.

2.2. Fase Assessment

Fase *assessment* atau pengujian merupakan inti dari penelitian ini, di mana penerapan teknis metode ISSAF dilakukan secara bertahap. Tahap pertama adalah *information gathering*, yaitu pengumpulan data mengenai target menggunakan alat seperti Nmap untuk pemindaian jaringan dan WHOIS untuk identifikasi informasi domain. Selanjutnya, dilakukan *vulnerability analysis* dengan memanfaatkan OWASP ZAP dan SQLMap untuk mendeteksi celah keamanan potensial seperti SQL Injection, XSS, dan CSRF. Setelah kerentanan teridentifikasi, dilakukan simulasi eksploitasi terkendali untuk memverifikasi tingkat keparahan dan dampak masing-

masing celah tanpa menyebabkan kerusakan aktual pada sistem. Proses ini diikuti dengan analisis risiko kuantitatif menggunakan matriks faktor ancaman (*threat agent factors*) dan faktor kerentanan (*vulnerability factors*) sesuai panduan ISSAF, yang memungkinkan penilaian objektif terhadap tingkat kemungkinan (*likelihood*) dan dampak (*impact*) dari setiap kerentanan.

2.3. Fase Reporting (Pelaporan dan Rekomendasi)

Fase terakhir ini berfokus pada dokumentasi hasil dan formulasi rekomendasi perbaikan. Semua temuan kerentanan didokumentasikan secara sistematis dalam bentuk laporan teknis yang mencakup deskripsi celah, bukti eksploitasi, tingkat risiko (rendah, sedang, tinggi), serta dampak potensial terhadap aspek kerahasiaan, integritas, dan ketersediaan data. Berdasarkan analisis risiko yang telah dilakukan, dirumuskan **rekomendasi mitigasi spesifik** untuk setiap jenis serangan, seperti penerapan *prepared statements* untuk mencegah SQL Injection, *Content Security Policy (CSP)* untuk mengurangi risiko XSS, serta penggunaan *CSRF tokens* dan *SameSite cookie attributes* untuk menangkal serangan CSRF. Laporan ini tidak hanya berfungsi sebagai dokumen akademik, tetapi juga sebagai panduan praktis bagi pengembang dan administrator sistem dalam meningkatkan posture keamanan website sebelum diimplementasikan ke lingkungan produksi.

3. Hasil dan Pembahasan

Bab ini menyajikan temuan utama dari pelaksanaan uji penetrasi pada website dummy menggunakan kerangka kerja Information Systems Security Assessment Framework (ISSAF). Hasil pengujian diklasifikasikan berdasarkan tiga jenis serangan yang menjadi fokus penelitian, yaitu SQL Injection, Cross-Site Scripting (XSS) Attack, dan Cross-Site Request Forgery (CSRF) Injection. Setiap kerentanan yang teridentifikasi dianalisis secara mendalam dengan mempertimbangkan faktor teknis, mekanisme eksploitasi, serta dampak potensial terhadap aspek kerahasiaan, integritas, dan ketersediaan sistem. Selain itu, bab ini membahas evaluasi risiko kuantitatif menggunakan metodologi penilaian risiko berbasis ISSAF, yang menggabungkan analisis threat agent factors dan vulnerability factors untuk menentukan tingkat keparahan (severity) masing-masing celah keamanan. Pembahasan lebih lanjut juga menyoroti efektivitas implementasi ISSAF dalam konteks pengujian website dummy, serta menyajikan rekomendasi mitigasi yang dapat diterapkan untuk memperkuat pertahanan sistem sebelum diimplementasikan pada lingkungan produksi.

3.1. SQL Injection

Pengujian SQL Injection berhasil mengidentifikasi kerentanan pada form login dan parameter URL yang tidak melakukan validasi dan sanitasi input dengan memadai. Eksploitasi menggunakan payload dasar seperti ' OR '1'='1 pada kolom username terbukti dapat melewati mekanisme autentikasi dan memberikan akses tidak sah ke database. Hasil pemindaian dengan SQLMap juga mengungkapkan bahwa website dummy rentan terhadap Union-based SQL Injection, yang memungkinkan penyerang menggabungkan hasil query dari tabel berbeda untuk mengekstrak informasi sensitif. Menurut penelitian Ferdianto (2023), kerentanan SQL Injection sering muncul akibat penggunaan query dinamis tanpa parameterized statements atau prepared statements pada lapisan aplikasi [28]. Temuan ini mengonfirmasi bahwa meskipun teknik tersebut sudah dikenal luas, implementasi keamanan yang lemah masih menjadi masalah umum pada pengembangan website.

3.2. Cross-Site Scripting (XSS) Attack

Uji XSS pada kolom komentar dan formulir umpan balik website dummy berhasil mendemonstrasikan dua jenis serangan: Reflected XSS melalui parameter URL dan Stored XSS melalui input yang disimpan di database. Skrip berbahaya <script>alert('XSS')</script> yang dimasukkan dapat dieksekusi di browser pengguna lain ketika halaman yang terkait diakses. Kerentanan ini terjadi karena aplikasi tidak menerapkan output encoding atau input sanitization secara konsisten. Studi oleh Arrysatrya dkk. (2024) menyatakan bahwa XSS masih menjadi ancaman utama pada aplikasi web modern karena kompleksitas konteks output (HTML, JavaScript, CSS) yang sering tidak sepenuhnya dipertimbangkan dalam proses penyaringan [31]. Hasil pengujian ini menunjukkan bahwa

meskipun mitigasi seperti Content Security Policy (CSP) telah tersedia, penerapannya sering diabaikan pada tahap pengembangan.

3.3. Cross-Site Request Forgery (CSRF) Injection

Pengujian CSRF mengungkapkan bahwa website dummy tidak menerapkan mekanisme pertahanan seperti CSRF token atau validasi Referer header. Dengan memanfaatkan sesi aktif pengguna, penyerang dapat membuat halaman jahat yang secara otomatis mengirimkan permintaan (request) untuk mengubah email atau kata sandi pengguna tanpa persetujuan. Eksperimen dengan teknik clickjacking juga berhasil menunjukkan bagaimana elemen halaman dapat dibajak untuk menipu pengguna melakukan tindakan berbahaya. Menurut Ashari dkk. (2022), CSRF merupakan ancaman yang sering diremehkan karena eksploitasinya tidak langsung mencuri data, namun mampu memicu perubahan status sistem yang kritis [32]. Temuan ini memperkuat pentingnya perlindungan proaktif pada setiap permintaan yang mengubah status (state-changing requests).

3.4. Analisis Faktor Ancaman dan Kerentanan

Berdasarkan metodologi penilaian risiko ISSAF, dilakukan kuantifikasi faktor ancaman (threat agent factors) dan faktor kerentanan (vulnerability factors) untuk menentukan tingkat kemungkinan (likelihood) eksploitasi. Hasil perhitungan dirangkum dalam Tabel 1.

Tabel 1. Nilai *Threat Agent Factors* dan *Vulnerability Factors*

No	Jenis Serangan	Skill Level	Motive	Opportunity	Size	Ease of Discovery	Ease of Exploit	Awareness	Intrusion Detection	Overall Likelihood
1	SQL Injection	5	9	4	5	3	5	6	6	5.37 (Medium)
2	XSS Attack	3	4	7	9	1	5	6	8	5.37 (Medium)
3	CSRF Injection	9	9	9	6	7	5	6	8	**7.37** High)

SQL Injection memiliki *skill level* menengah (5) namun *motive* tinggi (9) karena potensi keuntungan besar bagi penyerang. Namun, *ease of discovery* rendah (3) mengindikasikan bahwa kerentanan ini tidak selalu mudah ditemukan secara otomatis. XSS Attack memiliki *size* ancaman tertinggi (9) karena dapat menargetkan pengguna anonim secara luas, namun *ease of discovery* sangat rendah (1) karena membutuhkan pengujian manual yang mendalam. CSRF Injection mencatat nilai tertinggi pada sebagian besar faktor ancaman (*skill level*, *motive*, *opportunity*), menunjukkan bahwa serangan ini memerlukan keahlian tinggi namun memberikan peluang eksploitasi yang luas dengan sumber daya minimal. Perhitungan *overall likelihood* menggunakan rumus ISSAF (1).

$$Likelihood = (Threat\ Agent\ Factors + Vulnerability\ Factors) / 2 \quad (1)$$

di mana masing-masing faktor dihitung berdasarkan rata-rata komponennya. Hasil ini sejalan dengan penelitian Ghozali dkk. (2019) yang menyatakan bahwa CSRF sering memiliki tingkat kemungkinan tinggi karena kurangnya kesadaran pengembang dan mudahnya eksploitasi dengan alat otomatis.

3.5. Dampak Teknis dan Bisnis

Analisis dampak teknis dan bisnis dilakukan untuk menilai tingkat keparahan (severity) masing-masing kerentanan. Hasil evaluasi disajikan dalam Tabel 2.

Tabel 2. Nilai *Technical Impact* dan *Business Impact*

No	Jenis Serangan	Loss of Confidentiality	Loss of Integrity	Loss of Availability	Loss of Accountability	Financial Damage	Reputation Damage	Non-Compliance	Privacy Violation	Overall Impact
1	SQL Injection	6	5	9	7	3	5	7	5	5.87 (Medium)
2	XSS Attack	9	7	7	1	9	9	5	7	6.75 (High)
3	CSRF Injection	2	5	5	9	3	5	7	9	5.62 (Medium)

SQL Injection memiliki dampak ketersediaan (availability) tertinggi (9) karena dapat mengakibatkan gangguan total layanan melalui penghapusan atau korupsi data. XSS Attack mencatat dampak kerahasiaan (confidentiality) tertinggi (9) karena mampu mencuri sesi pengguna dan data sensitif, serta menyebabkan kerusakan reputasi signifikan (9). CSRF Injection memiliki dampak akuntabilitas (accountability) tertinggi (9) karena serangan sulit dilacak, serta pelanggaran privasi tertinggi (9) jika mengakibatkan kebocoran data skala besar.

Berdasarkan penelitian Sarker dkk. (2023), pendekatan kuantitatif dalam penilaian dampak memungkinkan prioritisasi mitigasi yang lebih objektif, terutama ketika sumber daya keamanan terbatas. Hasil analisis ini menunjukkan bahwa meskipun CSRF memiliki likelihood tinggi, dampak keseluruhan berada pada kategori medium, sementara XSS justru memiliki dampak tinggi meskipun kemungkinannya medium.

3.6. Tingkat Risiko Keseluruhan (Overall Risk Severity)

Dengan menggabungkan nilai likelihood pada Tabel 3 dan impact pada Tabel 4 diperoleh tingkat risiko keseluruhan berdasarkan matriks risiko ISSAF.

Tabel 3. Overall Risk Severity

No	Jenis Serangan	Likelihood	Impact	Overall Risk Rating
1	SQL Injection	Medium	Medium	Medium
2	XSS Attack	Medium	High	High
3	CSRF Injection	High	Medium	High

Tabel 3 menjelaskan bahwa SQL Injection dikategorikan risiko medium karena meskipun dampaknya signifikan, kemungkinan eksploitasi membutuhkan tingkat keahlian tertentu dan tidak semua kerentanan mudah ditemukan. XSS Attack dan CSRF Injection sama-sama mendapatkan risiko tinggi, namun dengan alasan berbeda: XSS karena dampak kerahasiaan dan reputasi yang sangat berat, sementara CSRF karena kemudahan eksploitasi dan potensi pelanggaran privasi skala luas. Temuan ini konsisten dengan studi oleh Anggraeni dkk. (2022) yang juga mengidentifikasi XSS dan CSRF sebagai kerentanan berisiko tinggi dalam konteks website pendidikan, terutama karena sering diabaikan dalam fase pengembangan [9]. Hasil analisis risiko ini akan menjadi dasar formulasi rekomendasi mitigasi pada bagian selanjutnya.

Hasil penelitian mengonfirmasi bahwa website dummy yang diuji mengandung tiga kerentanan kritis yang umum ditemukan dalam aplikasi web modern, yaitu SQL Injection, XSS Attack, dan CSRF Injection. Temuan ini konsisten dengan penelitian sebelumnya oleh Anggraeni dkk. (2022) yang juga mengidentifikasi kerentanan serupa pada website institusi pendidikan menggunakan metodologi ISSAF, meskipun dengan variasi tingkat keparahan yang berbeda. Perbedaan ini dapat disebabkan oleh konfigurasi keamanan spesifik pada website dummy yang sengaja dibuat rentan untuk tujuan pengujian. Secara metodologis, penerapan kerangka kerja ISSAF terbukti efektif dalam memberikan struktur sistematis untuk identifikasi, eksploitasi

terkendali, dan analisis risiko kerentanan. Tahapan yang terdefinisi dengan jelas, mulai dari planning hingga reporting, memungkinkan pengujian dilakukan secara komprehensif tanpa mengabaikan aspek etis dan keamanan sistem.

Analisis mendalam terhadap faktor ancaman (threat agent factors) mengungkapkan dinamika yang menarik antara tingkat keahlian penyerang, motivasi, dan kemudahan akses. SQL Injection, meskipun memerlukan keahlian teknis menengah (*skill level=5*), memiliki motivasi sangat tinggi (*motive=9*) karena potensi ganjaran finansial langsung dari pencurian data. Sementara itu, CSRF Injection mencatat nilai tertinggi pada hampir semua faktor ancaman, termasuk *opportunity=9* yang menunjukkan bahwa serangan ini dapat dilakukan dengan sumber daya minimal. Fenomena ini didukung oleh penelitian Sarker dkk. (2023) yang menyatakan bahwa ancaman dengan opportunity tinggi cenderung lebih sering terjadi di lingkungan dengan kesadaran keamanan rendah, karena penyerang tidak memerlukan akses khusus atau alat canggih [12]. Di sisi lain, XSS Attack memiliki *size=9* karena dapat menargetkan pengguna anonim dalam jumlah besar, namun ease of discovery yang sangat rendah (1) mengindikasikan bahwa kerentanan ini sering terlewat dalam pengujian otomatis.

Berdasarkan perspektif dampak teknis, ketiga kerentanan menunjukkan profil yang berbeda-beda. SQL Injection memiliki dampak ketersediaan (availability) tertinggi (9), yang sejalan dengan penelitian Ferdianto (2023) yang menyatakan bahwa serangan ini dapat menyebabkan gangguan layanan parah melalui penghapusan atau korupsi data [28]. Sementara itu, XSS Attack berdampak paling signifikan pada aspek kerahasiaan (*confidentiality=9*) karena kemampuannya mencuri token sesi dan kredensial pengguna. Hasil ini memperkuat temuan Arrysatrya dkk. (2024) yang menekankan bahwa XSS modern semakin canggih dalam mengekstrak data sensitif tanpa meninggalkan jejak yang mudah dideteksi [31]. CSRF Injection, meskipun memiliki dampak kerahasiaan rendah (2), justru paling berbahaya dalam hal akuntabilitas (*accountability=9*) dan privasi (*privacy violation=9*), karena eksploitasinya yang terselubung dan potensial membocorkan data pribadi dalam skala masif.

Tingkat risiko keseluruhan (overall risk severity) yang dihasilkan dari matriks ISSAF memberikan perspektif prioritisasi yang jelas untuk tindakan mitigasi. Fakta bahwa XSS Attack dan CSRF Injection sama-sama dikategorikan high risk meskipun dengan kombinasi likelihood-impact yang berbeda, menggarisbawahi kompleksitas manajemen risiko keamanan siber. XSS cenderung memiliki dampak jangka panjang terhadap reputasi organisasi, sementara CSRF lebih berisiko dalam konteks kepatuhan regulasi dan privasi data. Temuan ini selaras dengan penelitian Ghozali dkk. (2019) yang menekankan bahwa penilaian risiko tidak boleh hanya melihat kemungkinan eksploitasi, tetapi juga memperhitungkan konteks bisnis dan regulasi yang melingkupi sistem [36]. Oleh karena itu, pendekatan mitigasi yang diusulkan perlu bersifat holistik, menggabungkan perbaikan teknis dengan peningkatan kesadaran (security awareness) dan penegakan kebijakan keamanan.

Secara keseluruhan, penelitian ini menguatkan relevansi penggunaan kerangka kerja terstruktur seperti ISSAF dalam konteks pengujian penetrasi website. Metodologi yang sistematis tidak hanya membantu mengidentifikasi kerentanan, tetapi juga memberikan dasar kuantitatif untuk pengambilan keputusan terkait alokasi sumber daya keamanan. Namun, perlu diakui bahwa implementasi ISSAF memerlukan waktu dan keahlian teknis yang memadai, yang mungkin menjadi kendala bagi organisasi dengan sumber daya terbatas. Ke depan, penelitian lanjutan dapat mengembangkan adaptasi ISSAF yang lebih ringkas tanpa mengorbankan kedalaman analisis, atau mengintegrasikannya dengan framework lain seperti OWASP Testing Guide untuk cakupan pengujian yang lebih luas.

4. Kesimpulan

Penelitian ini berhasil mengimplementasikan Information Systems Security Assessment Framework (ISSAF) sebagai metodologi terstruktur dalam melakukan uji penetrasi terhadap website dummy. Hasil pengujian mengidentifikasi tiga kerentanan utama, yaitu SQL Injection (risiko medium), Cross-Site Scripting-XSS Attack (risiko tinggi), dan Cross-Site Request Forgery CSRF Injection (risiko tinggi), yang menunjukkan bahwa website dummy

memiliki celah keamanan kritis yang umum ditemukan pada aplikasi web. Analisis kuantitatif berdasarkan faktor ancaman dan kerentanan ISSAF membuktikan bahwa meskipun SQL Injection memiliki dampak teknis yang signifikan terhadap ketersediaan sistem, XSS dan CSRF justru lebih berisiko secara keseluruhan karena kombinasi antara kemudahan eksploitasi, dampak reputasi yang parah, dan potensi pelanggaran privasi skala luas.Secara metodologis, kerangka kerja ISSAF terbukti efektif dalam menyediakan pendekatan sistematis mulai dari perencanaan, assessment, hingga pelaporan, sehingga memungkinkan identifikasi kerentanan secara komprehensif dan terukur. Penelitian ini juga mengonfirmasi bahwa integrasi antara analisis teknis dan penilaian risiko bisnis sebagaimana diatur dalam tahapan ISSAF dapat menghasilkan prioritisasi mitigasi yang lebih objektif dan kontekstual. Dengan demikian, penelitian ini tidak hanya menyoroti kerentanan spesifik pada website dummy, tetapi juga memperkuat nilai praktis penerapan framework terstandarisasi dalam pengujian keamanan aplikasi web, khususnya sebagai langkah preventif sebelum implementasi sistem ke lingkungan produksi.

Daftar Pustaka

1. Anggraeni, D. P., Zen, B. P., & Pranata, M. (2022). Security analysis on websites using the Information System Assessment Framework (ISSAF) and Open Web Application Security version 4 (OWASPv4) using the penetration testing method. *Jurnal Pertahanan: Media Informasi tentang Kajian Strategi Pertahanan yang Mengedepankan Identity, Nasionalisme, dan Integritas*, 8(3), 497–510. https://doi.org/10.33172/jp.v8i3.1777
2. Arrysatrya, M., Putranda, Y., Ari, I. K., Ngurah, I. G., & Cahyadi, A. (2024). Analisis serangan Cross Site Scripting (XSS) pada website OASE menggunakan metode OWASP. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 13(1), 159–166.
3. Ashari, I. F., Oktarina, V., Sadewo, R. G., & Damanhuri, S. (2022). Analysis of Cross Site Request Forgery (CSRF) attacks on West Lampung Regency websites using OWASP ZAP tools. *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, 11(2), 276–281. https://doi.org/10.32736/sisfokom.v11i2.1393
4. CNN Indonesia. (2024, 3 Juni). *Indonesia digempur 6 juta ancaman siber di awal 2024*. Diakses dari https://www.cnnindonesia.com/teknologi/20240603103200-185-1105033/indonesia-digempur-6-juta-ancaman-siber-di-awal-2024-cek-modusnya
5. Ferdianto, Y. (2023). Penerapan keamanan login admin dan filterisasi input untuk mencegah SQL Injection. *Jurnal Informatika dan Rekayasa Perangkat Lunak*, 4(3), 349–356. https://doi.org/10.33365/jatika.v4i3.3306
6. Ghozali, B., Kusrini, K., & Sudarmawan, S. (2019). Mendeteksi kerentanan keamanan aplikasi website menggunakan metode OWASP (Open Web Application Security Project) untuk penilaian risk rating. *Creative Information Technology Journal*, 4(4), 264–279. https://doi.org/10.24076/citec.2017v4i4.119
7. Hackread. (2019, 24 September). *Malware hits freelancers at Fiverr and Freelancer.com*. Diakses dari https://hackread.com/malware-hits-freelancers-at-fiverr-and-freelancer-com/
8. Leszczyna, R. (2022). Choosing the right cybersecurity solution: A review of selection and evaluation criteria. *Proceedings of ETHICOMP 2022*, 435–452.
9. Rochman, A., Salam, R. R., & Maulana, S. A. (2021). Analisis keamanan website dengan Information System Security Assessment Framework (ISSAF) dan Open Web Application Security Project (OWASP) di rumah sakit XYZ. *Pharmacognosy Magazine*, 75(17), 399–405.
10. Sarker, K. U., Yunus, F., & Deraman, A. (2023). Penetration taxonomy: A systematic review on the penetration process, framework, standards, tools, and scoring methods. *Sustainability*, 15(13), Article 10471. https://doi.org/10.3390/su151310471
11. Wijaya, I. G. A. S. P., Sasmita, G. M. A., & Pratama, I. P. A. E. (2024). Web application penetration testing on Udayana University's OASE e-learning platform using Information System Security Assessment Framework (ISSAF) and Open Source Security Testing Methodology Manual (OSSTMM). *International Journal of Information Technology and Computer Science*, 16(2), 45–56. https://doi.org/10.5815/ijitcs.2024.02.04
12. Yudiana, Y., Elanda, A., & Buana, R. L. (2021). Analisis kualitas keamanan sistem informasi e-office berbasis website pada STMIK Rosma dengan menggunakan OWASP Top 10. *CESS (Journal of Computer Engineering, System, and Science)*, 6(2), 185–194. https://doi.org/10.24114/cess.v6i2.24777