HIJM
HORIZON: Indonesian Journal of Multidisciplinary

p-ISSN: 2987-7776
e-ISSN: 2987-7180
Vol. 4, No. 4, 2026

ANALISIS KERENTANAN KEAMANAN WEBSITE RUANGCOSPLAY DENGAN MENGGUNAKAN METODE PENETRATION TESTING BERBASIS OWASP TOP 10:2021

Valentino Eka Apritha Putra[1], Joko Iskandar[2], Agung Prasetya[3]
[1, 2, 3]Universitas Bhineka PGRI, Jl. Mayor Sujadi No. 7, Tulungagung, Jawa Timur, Indonesia
Email: valentino.student@ubhi.ac.id

Article History

Received: 26-06-2026

Revision: 22-07-2026

Accepted: 27-08-2026

Published: 30-07-2026

Abstract. The RuangCosplay website manages user data and transactions, requiring a security system capable of protecting against various cyber threats. However, a comprehensive evaluation of the website's security vulnerability level based on current security standards is not yet available. This study aims to identify and analyze the security vulnerabilities of the Ruang Cosplay website using penetration testing methods based on the OWASP Top 10:2021. Testing refers to the NIST SP 800-115 framework, which includes the planning, discovery, attacking, and reporting stages. Vulnerability identification was carried out through open-source intelligence and scanning using Nmap, OWASP ZAP, Dirsearch, and WhatWaf. The results showed that no vulnerabilities with a high or critical risk level were found, so the website's overall security level is considered good. However, 11 vulnerabilities were identified, consisting of 3 medium-risk vulnerabilities and 8 low-risk vulnerabilities. Medium-risk vulnerabilities include the use of an outdated TLS protocol, the absence of a Content Security Policy header, and the failure to implement the Subresource Integrity attribute in third-party scripts. Low-risk vulnerabilities were dominated by misconfigurations in cookies and security headers. This research recommends updating to TLS 1.2 or TLS 1.3, implementing the HttpOnly and Secure attributes on cookies, and implementing Subresource Integrity to improve website security and reduce the potential for future exploits.

Keywords: Website Security, Penetration Testing, OWASP Top 10, NIST SP 800-115, System Vulnerabilities

Abstrak. Website RuangCosplay mengelola data pengguna dan transaksi sehingga memerlukan sistem keamanan yang mampu melindungi dari berbagai ancaman siber. Namun, belum tersedia evaluasi komprehensif terhadap tingkat kerentanan keamanan website tersebut berdasarkan standar keamanan terkini. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan keamanan website Ruang Cosplay menggunakan metode *penetration testing* berdasarkan *OWASP Top 10:2021*. Pengujian mengacu pada kerangka kerja *NIST SP 800-115* yang meliputi tahap *planning*, *discovery*, *attacking*, dan *reporting*. Identifikasi kerentanan dilakukan melalui *open-source intelligence* serta pemindaian menggunakan Nmap, OWASP ZAP, Dirsearch, dan WhatWaf. Hasil penelitian menunjukkan bahwa tidak ditemukan kerentanan dengan tingkat risiko tinggi maupun kritis, sehingga secara umum tingkat keamanan website berada pada kategori cukup baik. Meskipun demikian, teridentifikasi 11 kerentanan, yang terdiri atas 3 kerentanan berisiko menengah dan 8 kerentanan berisiko rendah. Kerentanan berisiko menengah meliputi penggunaan protokol TLS versi lama, tidak adanya header *Content Security Policy*, dan tidak diterapkannya atribut *Subresource Integrity* pada skrip pihak ketiga. Adapun kerentanan berisiko rendah didominasi oleh *misconfiguration* pada *cookie* dan *security header*. Penelitian ini merekomendasikan pembaruan ke TLS 1.2 atau TLS 1.3, penerapan atribut *HttpOnly* dan *Secure* pada *cookie*, serta implementasi *Subresource Integrity* untuk meningkatkan keamanan website dan mengurangi potensi eksploitasi pada masa mendatang.

Kata Kunci: Keamanan Website, Penetration Testing, OWASP Top 10, NIST SP 800-115, Kerentanan Sistem

How to Cite: Putra, V. E. A., Iskandar, J., Prasetya, A. (2026). Analisis Kerentanan Keamanan *Website Ruangcosplay* dengan Menggunakan Metode *Penetration Testing* Berbasis Owasp TOP 10:2021. (2026). *HORIZON: Indonesian Journal of Multidisciplinary*, 4 (4), 4783-4795. http://doi.org/10.54373/hijm.v4i4.6748

PENDAHULUAN

Perkembangan layanan berbasis web telah mendorong berbagai organisasi, termasuk komunitas digital, memanfaatkan website sebagai media penyedia informasi, interaksi pengguna, dan transaksi daring. Keandalan layanan tersebut tidak hanya ditentukan oleh aspek fungsionalitas, tetapi juga oleh tingkat keamanan sistem yang mampu melindungi data pengguna dari berbagai ancaman siber. Oleh karena itu, keamanan aplikasi web menjadi bagian yang tidak terpisahkan dari kualitas layanan digital, terutama pada platform yang mengelola data pribadi dan aktivitas pengguna (Salaam & Iskandar, 2024).

Meningkatnya penggunaan website diikuti oleh peningkatan jumlah dan kompleksitas serangan siber yang menargetkan aplikasi web. Berbagai jenis serangan, seperti *SQL Injection*, *Cross-Site Scripting* (XSS), *Cross-Site Request Forgery* (CSRF), dan *Broken Access Control*, masih menjadi penyebab utama kebocoran data serta gangguan layanan (Suhendar et al., 2022). Untuk meminimalkan risiko tersebut, *Open Worldwide Application Security Project* (OWASP) merumuskan *OWASP Top 10:2021* sebagai standar internasional yang mengelompokkan sepuluh kategori kerentanan paling kritis pada aplikasi web, mulai dari *Broken Access Control* hingga *Server-Side Request Forgery* (OWASP, 2021). Standar ini banyak digunakan sebagai acuan dalam proses *vulnerability assessment* maupun *penetration testing* karena mampu memberikan gambaran sistematis mengenai tingkat keamanan suatu aplikasi.

Website RuangCosplay merupakan platform komunitas dan penyewaan kostum yang menyediakan berbagai fitur, seperti registrasi pengguna, autentikasi, pengelolaan profil, serta layanan yang berpotensi berkembang menjadi transaksi elektronik. Karakteristik tersebut menyebabkan website mengelola data pengguna yang perlu memperoleh perlindungan memadai. Hasil observasi awal menunjukkan bahwa hingga penelitian ini dilakukan belum pernah dilaksanakan pengujian keamanan secara komprehensif terhadap website Ruang Cosplay berdasarkan standar *OWASP Top 10:2021*. Akibatnya, kondisi keamanan sistem, jenis kerentanan yang mungkin dimiliki, serta tingkat risikonya belum diketahui secara objektif. Kondisi ini berpotensi membuka peluang eksploitasi terhadap kelemahan konfigurasi server, mekanisme autentikasi, maupun komponen aplikasi yang dapat mengancam kerahasiaan, integritas, dan ketersediaan data pengguna (Rizkayanti, 2023).

Sejumlah penelitian terdahulu telah menerapkan *penetration testing* maupun *vulnerability assessment* menggunakan OWASP ZAP, Burp Suite, Acunetix, dan berbagai *web vulnerability scanner* pada website institusi pendidikan, pemerintahan, dan organisasi bisnis. Hasil penelitian menunjukkan bahwa berbagai aplikasi web masih memiliki kerentanan pada kategori *Broken Access Control*, *Security Misconfiguration*, *Injection*, *Vulnerable and*

Outdated Components, serta kategori lain dalam *OWASP Top 10* (Margareth et al., 2024; Amirul Mu'min et al., 2025; Firnanda et al., 2025a). Meskipun demikian, penelitian tersebut umumnya berfokus pada website institusional yang memiliki infrastruktur dan tata kelola keamanan yang relatif lebih matang. Penelitian mengenai website komunitas lokal, seperti RuangCosplay, masih sangat terbatas, padahal karakteristik pengguna, pola interaksi, dan pengelolaan sistemnya memiliki tantangan keamanan yang berbeda. Dengan demikian, masih terdapat *research gap* mengenai evaluasi keamanan website komunitas menggunakan pendekatan *penetration testing* yang mengacu pada standar internasional.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk (1) mengidentifikasi kerentanan keamanan pada website RuangCosplay melalui metode *penetration testing,* (2) mengklasifikasikan setiap temuan berdasarkan kategori *OWASP Top 10:2021,* (3) menentukan tingkat risiko setiap kerentanan menggunakan *Common Vulnerability Scoring System* (CVSS), dan (4) merumuskan rekomendasi mitigasi yang sesuai untuk meningkatkan keamanan website. Hasil penelitian diharapkan memberikan kontribusi praktis bagi pengelola RuangCosplay dalam memperkuat sistem keamanan, sekaligus menjadi referensi bagi pengembangan keamanan website komunitas digital yang memiliki karakteristik serupa.

METODE

Penelitian ini merupakan studi penerapan (*applied research*) dengan pendekatan kualitatif melalui metode *penetration testing* untuk mengidentifikasi dan mengevaluasi kerentanan keamanan pada website RuangCosplay. Proses pengujian mengacu pada kerangka kerja NIST SP 800-115 yang terdiri atas empat tahapan, yaitu *planning*, *discovery*, *attacking*, dan *reporting*, serta mengacu pada standar OWASP Web Security Testing Guide (WSTG) dan klasifikasi OWASP Top 10:2021.

Perencanaan (*Planning*)

Tahap ini bertujuan menentukan ruang lingkup pengujian, target, serta perangkat yang digunakan. Target penelitian difokuskan pada domain utama ruangcosplay.com karena hasil penelusuran awal tidak menunjukkan adanya subdomain yang menjadi objek pengujian. Pada tahap ini juga dilakukan identifikasi kebutuhan perangkat keras, perangkat lunak, dan *security tools* yang digunakan selama proses *penetration testing*, serta penentuan skenario pengujian yang sesuai dengan ketentuan NIST SP 800-115.

Tahapan *Discovery*

Tahap *discovery* merupakan proses *information gathering* untuk memperoleh informasi teknis mengenai website target. Aktivitas yang dilakukan meliputi identifikasi struktur website, sistem operasi, layanan (*services*), port yang terbuka, teknologi web yang digunakan, struktur direktori, serta potensi kerentanan awal. Pengumpulan data dilakukan menggunakan Google Dorking, Nmap, Dirsearch, WhatWaf, Nikto, WPScan, dan OWASP ZAP.

Tahap Penyerangan (*Attacking*)

Tahap *attacking* dilakukan untuk memvalidasi kerentanan yang ditemukan pada tahap sebelumnya melalui eksploitasi secara terkendali (*controlled exploitation*). Pengujian difokuskan pada kerentanan yang termasuk dalam kategori OWASP Top 10:2021, seperti *Broken Access Control*, *Cross-Site Scripting (XSS)*, *SQL Injection*, dan *Security Misconfiguration*. Pengujian dilakukan menggunakan OWASP ZAP, Burp Suite, dan sqlmap untuk memastikan apakah kerentanan benar-benar dapat dieksploitasi serta menilai dampaknya terhadap keamanan website.

Tahap Pelaporan (*Reporting*)

Tahap terakhir adalah penyusunan laporan hasil pengujian. Seluruh temuan diklasifikasikan berdasarkan kategori OWASP Top 10:2021 dan tingkat risikonya menggunakan Common Vulnerability Scoring System (CVSS). Setiap kerentanan disajikan dalam bentuk deskripsi, bukti teknis (*proof of concept*), tingkat risiko, serta rekomendasi mitigasi sebagai dasar bagi pengelola website dalam menentukan prioritas perbaikan keamanan.

Subjek dan Lokasi Penelitian

Subjek dalam penelitian ini adalah website RuangCosplay yang dapat diakses melalui alamat https://ruangcosplay.com/, yaitu aplikasi web yang menyediakan layanan sewa kostum cosplay, katalog cosrent, dan forum komunitas bagi pengguna di berbagai daerah di Indonesia. Lokasi penelitian bersifat remote karena seluruh proses pengujian dilakukan dari lingkungan kerja peneliti menggunakan laptop MacBook Air M2 dengan sistem operasi macOS dan koneksi internet untuk mengakses server RuangCosplay yang berada pada layanan hosting/cloud pihak ketiga.

Teknik Pengumpulan Data

- Studi literatur; studi literatur dilakukan dengan mempelajari jurnal ilmiah, buku, tugas akhir, serta dokumentasi resmi OWASP dan NIST yang berkaitan dengan keamanan aplikasi web, OWASP Top 10:2021, dan metodologi penetration testing.
- Observasi langsung *website* RuangCosplay; observasi dilakukan dengan mengakses langsung website RuangCosplay guna memahami struktur halaman, fitur utama, alur interaksi pengguna, serta jenis input yang tersedia, seperti halaman Home, Cari Kostum, List Cosrent, Forum, Jadwal Event, dan Buat Akun.
- Pengumpulan data teknis hasil pengujian; data teknis dikumpulkan dari output tools seperti Nmap, dirsearch, OWASP ZAP, sqlmap, WhatWaf, Nikto, dan WPScan berupa log pemindaian, daftar kerentanan, bukti request–response, serta hasil eksploitasi terkontrol. Selain itu, catatan manual dan screenshot selama eksploitasi menggunakan Burp Suite dan ZAP juga dikumpulkan untuk memperkuat bukti temuan.

Pengecekan Keabsahan Data

- Trigulasi Tools dan Sumber Data; Kerentanan yang ditemukan oleh satu *tools* OWASP ZAP diverifikasi menggunakan tools lain seperti *sqlmap, Burp Suite, Nikto*, atau pengujian manual untuk memastikan bahwa temuan bukan *false positive*. Data teknis juga dibandingkan dengan hasil observasi langsung dan informasi dari owner RuangCosplay agar interpretasi kerentanan sesuai dengan kondisi operasional sistem.
- Reproduksibilitas Pengujian; Setiap langkah pengujian dicatat secara rinci seperti waktu, parameter, payload, hasil. Sehingga dapat diulang dan menghasilkan temuan yang konsisten, sesuai prinsip dokumentasi pengujian pada NIST SP 800-115.
- Validasi Temuan Kritis dengan Pemilik Sistem; Untuk kerentanan yang berdampak tinggi, peneliti melakukan konfirmasi kepada pemilik atau administrator RuangCosplay dengan menyertakan deskripsi dan bukti minimal, serta meminta klarifikasi apakah perilaku tersebut memang tidak diinginkan atau merupakan fitur yang dikontrol.
- Penggunaan Standar OWASP Top 10:2021; Pengkategorian kerentanan mengikuti definisi resmi OWASP Top 10:2021, sehingga mengurangi subjektivitas peneliti dalam mengklasifikasikan jenis kelemahan pada aplikasi *web*.

Teknik Analisis Data

Analisis data dilakukan secara bertahap berdasarkan hasil *penetration testing* untuk memperoleh gambaran tingkat keamanan website RuangCosplay. Tahapan analisis meliputi sebagai berikut.

- Identifikasi Kerentanan; Seluruh hasil pengujian dari proses *discovery* dan *attacking* dikompilasi untuk mengidentifikasi kerentanan yang ditemukan pada website. Setiap temuan diverifikasi berdasarkan bukti teknis (*proof of concept*) guna memastikan bahwa kerentanan benar-benar terdapat pada sistem dan bukan merupakan *false positive*.
- Klasifikasi Kerentanan berdasarkan *OWASP Top 10:2021;* Kerentanan yang telah terverifikasi selanjutnya dikelompokkan ke dalam kategori risiko *OWASP Top 10:2021* (A01–A10), seperti *Broken Access Control*, *Cryptographic Failures*, *Security Misconfiguration*, dan kategori lainnya. Tahap ini bertujuan untuk mengetahui distribusi jenis kerentanan serta aspek keamanan yang paling membutuhkan perhatian.
- Penilaian Tingkat Risiko; Setiap kerentanan dianalisis menggunakan Common Vulnerability Scoring System (CVSS) dengan mempertimbangkan tingkat kemudahan eksploitasi (*exploitability*) dan dampaknya terhadap aspek kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) sistem. Berdasarkan nilai CVSS, setiap temuan diklasifikasikan ke dalam tingkat risiko Low, Medium, High, atau Critical, sehingga diperoleh prioritas penanganan yang objektif.
- Analisis dan Penyusunan Rekomendasi Mitigasi; Hasil klasifikasi dan penilaian risiko dianalisis untuk menentukan strategi mitigasi yang sesuai. Rekomendasi disusun dengan mengacu pada *OWASP Web Security Testing Guide*, *OWASP Top 10:2021*, serta praktik terbaik keamanan aplikasi web. Rekomendasi meliputi perbaikan konfigurasi server, pembaruan protokol keamanan, penguatan mekanisme autentikasi, penerapan *security headers*, pembaruan komponen perangkat lunak, dan peningkatan proses pemantauan keamanan.
- Penarikan Kesimpulan; Tahap akhir dilakukan dengan menyintesiskan seluruh hasil analisis untuk menggambarkan tingkat keamanan website RuangCosplay, mengidentifikasi kerentanan yang paling berisiko, serta menyimpulkan prioritas mitigasi yang perlu diterapkan guna meningkatkan keamanan sistem secara menyeluruh.

HASIL DAN PEMBAHASAN

Tahapan *Discovery*

Pada tahap discovery, dilakukan pemetaan sistem dan identifikasi kerentanan awal menggunakan OWASP ZAP, Nmap, Dirsearch, dan WhatWAF. seltelah melakukan tahap *scanning* menggunakan *tools* tersebut bahwa *website* ruangcosplay.com ini menggunakan cloudflare untuk keamanan *firewall*. Untuk hasil keseluruhan *vulnerability scanner* yang telah dilakukan pada *website* target disajikan pada table berikut:

Tabel 4. 1 Hasil Identifikasi Kerentanan *Website* Ruangcosplay

URL Target	Jenis Celah Keamanan	Tingkat Ancaman
ruangcosplay.com	Content Security Policy (CSP) Header Not Set	Medium
	HTTP to HTTPS Insecure Transition in Form Post	Medium
	Sub Resource Integrity Attribute Missing	Medium
	Big Redirect Detected (Potential Sensitive Information Leak)	Low
	Cookie No HttpOnly Flag	Low
	Cookie Without Secure Flag	Low
	Cross-Domain JavaScript Source File Inclusion	Low
	In Page Banner Information Leak	Low
	Strict-Transport-Security Header Not Set	Low
	Timestamp Disclosure - Unix	Low
	X-Content-Type-Options Header Missing	Low

Tahapan *Attacking*

Pada tahapan ini dilakukan proses pengujian terhadap kemungkinanan celah keamanan yang telah ditemukan pada perangkat lunak OWASP ZAP dari tahap *scanning* yang selanjutnya kita dapat melakukan pengujian difokuskan pada skenario eksploitasi berdasarkan alert tinggi yang berpotensi membahayakan *website* ruangcosplay.com.

Pengujian Cross-Site Scripting (A03:2021-Injection)

Pada tahap ini penulis melakukan pengujian terhadap *website* ruangcosplay.com dengan memasukkan *script* <script>alert(‘XSS Berhasil’)</script> kedalam kolom pencarian. Hasil menunjukkan bahwa *script* tidak dapat di eksekusi oleh *browser*, melainkan telah di render sebagai teks biasa (*string*). Hal ini telah membuktikan bahwa aplikasi telah menerapkan mekanisme *Data Escaping/Sanitization* yang baik pada parameter tersebut, sehingga celah XSS berhasil dicegah oleh system dan peringatan dari *scanner* dapat diklasifikasikan sebagai *False Positive* pada endpoint ini.

Pengujian Security Misconfiguration (A05:2021-Security Misconfiguration)

Berdasarkan peringatan sebelumnya berkat temuan dari OWASP ZAP terkait *Cookie No HttpOnly Flag,* harus dilakukan pengujian manual menggunakan fitur *Developer Tools* pada *browser.* Disini penulis melakukan pengujian dengan megeksekusi perintah *JavaScript* document.cookie pada *console* untuk memulai penyerangan *Cross-Site Scripting* (XSS). Dalam pengujian yang telah di lakukan pada gambar di atas menunjukkan ketiadaan *Flag HttpOnly* pada *Cookie,* hasil eksekusi menunjukkan bahwa *cookie sensitive* aplikasi yaitu *XSRF-TOKEN,* dapat diakses dan dibaca secara langsung oleh *JavaScript* dalam bentuk *plaintext.* Hal ini memberi tahu bahwa memvalidasi kerentanan keamanan miskonfigurasi, di mana ketidak adaan atribut *HttpOnly* membuat *token* pengguna rentan di curi oleh penyerang jikalau penyerang berhasil mencuri dia dapat menginject *script* berbahaya kedalam halaman *website.*

Pengujian Cryptographic Failures (A02:2021- Cryptographic Failures)

Pengujian dilakukan menggunakan *tools* Nmap dengan *script* nmap –script ssl-enum-ciphers -p 443 <target>. Tujuannya untuk mengidentifikasi versi protocol enkripsi dan *cipher suites* apa saja yang masih di dukung dan diizinkan oleh server. Berdasarkan pengujian yang telah di lakukan, ditemukan kerentanan *Cryptographic Failures* berupa dukungan server terhadap protocol yang sudah lama, yaitu TLSv1.0 dan TLSv1.1. Kondisi ini memungkinkan penyerang dalam jaringan (*Man-in-the-Middle*) untuk melakukan *Downgrade Attack,* yaitu memaksa pengguna turun ke protokol lama TLS 1.0 atau 1.1 yang akibatnya, sistem menjadi rentan terhadap eksploitasi kriptografi (seperti serangan BEAST atau POODLE) yang memungkinkan penyerang untuk mendekripsi lalu lintas jaringan dan mencuri data sensitif pengguna, seperti *cookie* sesi admin.

Tahapan *Reporting*

Tabel 4. Rekapitulasi Hasil Pengujian Keamanan OWASP Top 10:2021

NO	Daftar OWASP TOP 10:2021	Celah kerentanan	Hasil pengujian
1.	A01:2021-Broken Access Control	Tidak ditemukan	-
2.	A02:2021-Cryptographic Failures	Ditemukan celah kerentanan berjenis *HTTP to HTTPS Insecure Transition* dan dukungan TLS usang.	Berhasil mendeteksi kerentanan transisi *form post* yang tidak aman melalui *scanner* ZAP. Selain itu, pemindaian Nmap memvalidasi bahwa *server edge* masih mengizinkan protokol usang (TLS 1.0/1.1).

3.	A03:2021-Injection	Ditemukan peringatan potensi kerentanan berjenis *Cross-Site Scripting* (XSS).	Tidak berhasil dieksploitasi. Berdasarkan verifikasi manual, aplikasi telah menerapkan mekanisme *Data Escaping/Sanitization* yang baik, sehingga *payload* dirender sebagai teks biasa dan celah diklasifikasikan sebagai *False Positive* yang telah dimitigasi.
4.	A04:2021-Insecure Design	Tidak ditemukan	-
5.	A05:2021-Security Misconfiguration	Ditemukan celah kerentanan berjenis *Security Header Missing* dan *Insecure Cookie*.	Berhasil diverifikasi secara manual. Pembuktian (PoC) melalui *console browser* menunjukkan *cookie* sesi dapat dibaca oleh JavaScript akibat ketiadaan *flag HttpOnly*. Ketiadaan *header* penting (CSP, HSTS) juga terkonfirmasi.
6.	A06:2021-Vulnerable and Outdated Component	Tidak ditemukan	-
7.	A07:2021-Identification and Authentication Failures	Tidak ditemukan	-
8.	A08:2021-Software and Data Integrity Failures	Ditemukan celah kerentanan berjenis *Sub Resource Integrity Attribute Missing.*	Berhasil menemukan bahwa *website* target memuat *resource/script* pihak ketiga tanpa atribut validasi integritas data (SRI).
9.	A09:2021-Security Logging and Monitoring Failures	Tidak ditemukan	-
10.	A10:2021-Server-Side Request Forgery (SSRF)	Tidak ditemukan	-

Rekomendasi Perbaikan (Mitigasi)

Meskipun hasil pengujian menunjukkan tidak ditemukan kerentanan dengan tingkat risiko tinggi maupun kritis, keberadaan tiga kerentanan kategori menengah dan delapan kerentanan kategori rendah tetap menunjukkan bahwa website RuangCosplay memerlukan perbaikan konfigurasi keamanan. Sebagian besar temuan berasal dari aspek *Security Misconfiguration*, *Cryptographic Failures*, dan *Software and Data Integrity Failures*, yang umumnya disebabkan oleh konfigurasi server yang belum mengikuti praktik keamanan modern. Kondisi ini menunjukkan bahwa keamanan aplikasi web tidak hanya ditentukan oleh tidak adanya serangan yang berhasil, tetapi juga oleh kemampuan sistem dalam mencegah peluang eksploitasi sejak tahap konfigurasi. Menurut Saragih et al. (2023), kesalahan konfigurasi keamanan merupakan salah satu penyebab utama munculnya celah keamanan pada aplikasi web dan perlu ditangani melalui penerapan *secure coding* serta konfigurasi server yang sesuai

standar. Temuan serupa juga dilaporkan oleh Arief et al. (2025) yang menunjukkan bahwa *Security Misconfiguration* menjadi kerentanan yang paling sering ditemukan pada pengujian *penetration testing* berbasis OWASP Top 10.

Keunggulan penelitian ini terletak pada penggunaan kombinasi kerangka kerja NIST SP 800-115, OWASP Top 10:2021, dan penilaian risiko berbasis CVSS, sehingga setiap kerentanan tidak hanya berhasil diidentifikasi, tetapi juga diklasifikasikan berdasarkan tingkat risikonya. Pendekatan tersebut memungkinkan penentuan prioritas mitigasi yang lebih objektif dibandingkan sekadar melakukan *vulnerability scanning*. Hasil penelitian juga memperlihatkan bahwa sebagian besar kerentanan yang ditemukan berkaitan dengan konfigurasi keamanan (*configuration-based vulnerabilities*), bukan kelemahan logika aplikasi. Temuan ini sejalan dengan penelitian Putri et al. (2025) yang menyatakan bahwa kombinasi *penetration testing* dan analisis berbasis OWASP mampu memberikan gambaran menyeluruh mengenai tingkat keamanan aplikasi web serta membantu menentukan prioritas perbaikan secara sistematis. Demikian pula, Dewi et al. (2025) menunjukkan bahwa proses validasi hasil pemindaian sangat penting untuk membedakan kerentanan yang benar-benar dapat dieksploitasi dari *false positive*, sehingga rekomendasi keamanan menjadi lebih akurat.

Rekomendasi mitigasi yang dihasilkan dalam penelitian ini difokuskan pada pembaruan protokol enkripsi ke TLS 1.2 atau TLS 1.3, penerapan atribut HttpOnly dan Secure pada *cookie*, implementasi Content Security Policy (CSP), serta penggunaan Subresource Integrity (SRI) pada sumber daya eksternal. Implementasi rekomendasi tersebut tidak hanya berfungsi menutup kerentanan yang ditemukan, tetapi juga meningkatkan ketahanan sistem terhadap serangan seperti *cross-site scripting* (XSS), *session hijacking*, *man-in-the-middle attack*, dan manipulasi skrip pihak ketiga. Hasil ini sejalan dengan penelitian Madya et al. (2025) yang menyatakan bahwa penerapan standar keamanan OWASP secara konsisten mampu menurunkan risiko eksploitasi pada aplikasi web, terutama pada aspek konfigurasi server dan pengelolaan komunikasi terenkripsi. Selain itu, Lestari et al. (2025) menegaskan bahwa perbaikan konfigurasi keamanan secara berkala merupakan langkah preventif yang efektif untuk menjaga kerahasiaan, integritas, dan ketersediaan layanan web. Dengan demikian, penelitian ini tidak hanya menghasilkan identifikasi kerentanan, tetapi juga memberikan rekomendasi teknis yang dapat diterapkan sebagai acuan peningkatan keamanan website komunitas maupun aplikasi web dengan karakteristik serupa.

KESIMPULAN

Berdasarkan hasil pengujian kerentanan keamanan yang telah dilakukan sebelumnya pada website ruangcosplay.com menggunakan metode penetration testing berbasis OWASP Top 10:2021, dapat ditarik beberapa Kesimpulan guna menjawab tujuan penelitian ini sebelumnya. Secara keseluruhan, pengujian ini berhasil mendapatkan celah keamanan website target dengan menemukan beberapa celah keamanan yang didominasi oleh Tingkat ancaman menengah dan rendah.

- Pertama, pada pengujian kategori Cryptographic Failures (A02:2021), ditemukan bahwa layanan server masih memberikan dukungan terhadap protocol TLS versi lama (1.0 dan 1.1) serta membiarkan transisi formular yang tidak aman dari HTTP ke HTTPS. Kelemahan ini berpotensi membuka jalur bagi intersepsi data di jaringan public.
- Kedua, terkait peringatan potensi Injection atau skrip lintas situs (A03:2021), proses pembuktian manual berhasil memvalidasi bahwa system telah menerapkan mekanisme sanitasi data yang sangat baik. Oleh karena itu, temuan dari pemindaian otomatis ini secara definitive diklasifikasikan sebagai positive false yang berarti fitur pencarian aman dari injeksi.
- Ketiga, pada kategori Security Misconfiguration (A05:2021), teridentifikasi adanya ketidakadaan keamanan header penting bagi server
- seperti Content Security Policy dan HTTP Strict Transport Security. Selain itu, session cookie pengguna juga tidak dilengkapi dengan atribut perlindungan seperti HttpOnly dan Secure, yang mempermudah scenario pembajakan session.
- Keempat, pada kategori Software and Data Integrity Failures (A08:2021), pengujian menemukan bahwa penemuan pada resource skrip dari pihak eksternal tidak dilengkapi atribut Sub Resource Integrity, sehingga system rentan terhadap modifikasi kode pihak ketiga yang tidak disadari.
- Secara garis besar, tujuan untuk mengetahui Tingkat keamanan website ruangcosplay.com telah tercapai. Meskipun tidak ditemukan celah berisiko tinggi yang dapat langsung mengambil alih system secara penuh atau broken acces control, akumulasi dari ketentanan Tingkat menengah dan rendah ini tetap memerlukan Tindakan mitigrasi agar keamanan data pengguna dan operasional layanan dapat terjamin dengan baik kedepannya.

REKOMENDASI

Berdasarkan Kesimpulan dari hasil pengujian yang telah dipaparkan, berikut adalah beberapa saran yang diharapkan penulis dapat memberikan manfaat secara teoritis maupun praktis bagi pihak yang terkait dengan penelitian ini kedepannya. Bagi pihak pengembang atau pengelola Perusahaan ruangcosplay.com, disarankan untuk segera menerapkan rekomendasi perbaikan teknis yang telah disusun dalam laporan ini. Langkah perbaikan seperti penonaktifan protocol TLS lama, penambahan atribut *HTTPOnly* pada *cookie*, serta penyematan nilai hash *cryptographic* untuk *resource* eksternal sangat penting dilakukan. Perbaikan ini akan menjadi dasar utama dalam meningkatkan keamanan system guna meminimalkan potensi kebocoran data pengguna serta menjaga reputasi *website*, dan kepercayaan komunitas terhadap *platform* tersebut.

Bagi kalangan akademis dan institusi Universitas, hasil dari penelitian ini disarankan untuk dijadikan sebagai salah satu referensi studi kasus nyata dalam mata kuliah keamanan informasi. Laporan ini dapat dimanfaatkan sebagai wawasan tambahan bagi siswa untuk memahami bagaimana standar internasional OWASP Top 10:2021 diimplementasikan secara langsung dalam mengaudit *aplikasi web*. Bagi peneliti selanjutnya, disarankan untuk memperluas cakupan ruanglingkup pengujian. Karena penelitian ini terbatas pada pengujian dari sudut pandang eksternal tanpa akseske struktur dalam *server*, peneliti berikutnya dapat mencoba pengujian *white-box testing* guna untuk menganalisis kerentanan langsung dari sisi kode sumber. Selain perangkat lunak pemindai keamanan lainnya guna mengeksplorasi penggunaan perangkat lunak pemindai keamanan lainnya agar dapat memperkaya tingkat akurasi perbandingan deteksi kerentanan keamanan yang telah ditemukan pada system yang lebih kompleks.

REFERENSI

Amirul, M., Tristanti, N., Pramuja, G., & Fanani, I. (2025). Analisis dan pengujian kerentanan website menggunakan OWASP ZAP. *Jurnal Riset Sistem dan Teknologi Informasi (RESTIA), 3*(1), 36–50. https://doi.org/10.30787/restia.v3i1.1886

Darmayuda, I. P. G. A. M., Sasmita, G. M. A., & Putri, G. A. A. P. (2024). OWASP framework and OCTAVE method for penetration testing web apps of College X. *Jurnal Ilmiah Merpati*, *12*(2), 105–113. https://doi.org/10.24843/JIM.2024.v12.i02.p03

Fadhli, M. (2024). Comprehensive analysis of penetration testing frameworks and tools: Trends, challenges, and opportunities. *Indonesian Journal of Electrical Engineering and Renewable Energy (IJEERE), 4*(1), 15–22.

Firnanda, M. Y., Wahanani, H. E., & Junaidi, A. (2025). Website security testing using PTES method and OWASP Top 10 approach. *Bit-Tech*, *8*(1), 404–415. https://doi.org/10.32877/bt.v8i1.2564

Margareth, S., Zen, B. P., Saputra, A. I., Simatupang, Y. Y., Mokosandi, C. J. P. M., Christiaan, R. O., Pradana, A. A. N. R., & Sundoro, I. L. A. (2024). Uji penetration testing web server XYZ menggunakan metode OWASP Top 10 dan CVSS. *Proceedings of the National Conference on Electrical Engineering, Informatics, Industrial Technology, and Creative Media*, *4*(1), 1173–1183. https://doi.org/10.20895/centive.v4i1.400

Open Worldwide Application Security Project. (2021). *OWASP Top 10: 2021*. https://owasp.org/Top10/2021/

Open Worldwide Application Security Project. (2025). *OWASP ZAP: Getting started*. https://www.zaproxy.org/getting-started/

Rizkayanti, T. (2023). Analisis keamanan website menggunakan metode *vulnerability assessment*. *JURTIKom (Jurnal Teknologi Informatika dan Komputer)*, *1*(1), 1–9. https://doi.org/10.51401/jurtikom.v1i1.3172

Salaam, P. A., & Iskandar, J. (2024). Pengembangan sistem informasi digital berbasis website menggunakan pendekatan ADDIE di Desa Cikalong Sukahaji, Majalengka. *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, *9*(2), 1022–1030. https://doi.org/10.29100/jipi.v9i2.5535

Sholawati, A., Setyadi, H. J., & Masa, A. P. A. (2024). Implementasi penetration testing pada sistem informasi terpadu layanan prodi menggunakan framework ISSAF. *Techno, 25*(2). https://doi.org/10.30595/techno.v25i2.21140

Suhendar, H., Iskandar, J., Kurniadi, D., & Septiana, Y. (2022). Asset management system design of village based on geographic information system. *Jurnal Teknik Informatika (JUTIF)*, *3*(4), 815–819. https://doi.org/10.20884/1.jutif.2022.3.4.299