Seminar Nasional Sosial, Ekonomi, Pendidikan, Penelitian, Pengabdian, dan Kesehatan (Snsep3k) **e ISSN: 2774-9754**
Volume 6 Nomor 1, November 2025- April 2026
https://conferences.citradharma.org/snsep3k/

Pemindaian Kerentanan Website RPH Surabaya Berdasarkan OWASP Top 10

Farrel Tiuraka Vierino[1]*, Henni Endah Wahanani[2] , Achmad Junaidi[3]
[1,2,3] UPN "Veteran" Jawa Timur, Jawa Timur, Indonesia
*Korespondensi Penulis. E-mail: 21081010222@student.upnjatim.ac.id , henniendah@upnjatim.ac.id , achmadjunaidi.if@upnjatim.ac.id

DOI: https://doi.org/10.56480/snsep3k.v6i1.12

Abstract

This study aims to identify security vulnerabilities on the official website of Rumah Potong Hewan (RPH) Surabaya using the OWASP Top 10 2021 standard and to provide recommendations for improving website security. The research method applies a vulnerability assessment approach through three main stages: planning, information gathering, and vulnerability scanning. The information gathering process was carried out using Nslookup, Whois, Nmap, Dirsearch, and Wappalyzer to obtain data related to IP addresses, domain information, open ports, accessible directories, and web technologies used. Vulnerability scanning was conducted using OWASP ZAP with manual explore and automated scan methods. The results show that a total of 33 security alerts were identified, comprising 1 high-risk, 11 medium-risk, 11 low-risk, and 10 informational vulnerabilities. Of these findings, 22 alerts (67%) fall into the OWASP Top 10 2021 categories, with the most dominant category being A05:2021 – Security Misconfiguration at 45.5%. Other identified categories include A06:2021 – Vulnerable and Outdated Components, A01:2021 – Broken Access Control, A02:2021 – Cryptographic Failures, and A03:2021 – Injection. These findings indicate that the website still has significant weaknesses in security configuration, access control mechanisms, cryptographic implementation, and input validation. Therefore, it can be concluded that the RPH Surabaya website requires comprehensive security improvements, particularly in server configuration, component updates, access control enforcement, encryption mechanisms, and input validation, in order to minimize the risk of cyberattacks on public service websites.

Kata kunci– Vulnerability Scanning, OWASP Top 10 2021, Website Security

A. PENDAHULUAN

Perkembangan teknologi digital mendorong peningkatan pemanfaatan website sebagai sarana utama penyediaan layanan informasi publik. Namun, peningkatan tersebut juga menyebabkan lonjakan ancaman serangan siber. Berdasarkan laporan Badan Siber dan Sandi Negara, sepanjang tahun 2022 tercatat lebih dari 370 juta aktivitas serangan siber di Indonesia, mengalami peningkatan signifikan dibandingkan tahun sebelumnya (BSSN, 2022). Bahkan, Indonesia menempati peringkat ketiga sebagai negara yang paling sering menjadi target serangan siber di dunia (Widyanuratikah, 2025). Kondisi ini menunjukkan bahwa ancaman terhadap sistem web semakin banyak terjadi.

Tingkat kesiapan keamanan siber Indonesia secara global menunjukkan adanya tantangan yang masih perlu diperkuat. Berdasarkan Global Cybersecurity Index 2020, Indonesia berada pada peringkat 24 dan mengalami peningkatan dibandingkan tahun sebelumnya, namun masih menghadapi berbagai risiko serangan siber (ITU, 2020). Selain itu, laporan Lanskap Keamanan Siber Indonesia 2023 menunjukkan sektor pemerintahan menjadi salah satu target utama serangan dengan insiden yang meliputi kebocoran data, defacement website, ransomware, hingga potensi serangan DDoS (BSSN, 2023). Hal ini menggambarkan sistem instansi memiliki tingkat kerentanan yang tinggi jika tidak didukung keamanan yang optimal.

Website sebagai pintu utama pertukaran informasi memiliki berbagai potensi celah keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Oleh karena itu, diperlukan proses pengujian keamanan untuk mengidentifikasi kelemahan sistem secara sistematis. Penetration testing dengan pemindaian kerentanan keamanan merupakan salah satu pendekatan untuk menemukan celah keamanan pada web sebelum dieksploitasi oleh penyerang (McGraw et al., 2005). Standar yang paling banyak digunakan dalam pengujian keamanan adalah OWASP Top 10 yang

merangkum sepuluh kategori kerentanan paling kritis dan berisiko tinggi pada aplikasi web (OWASP, n.d.).

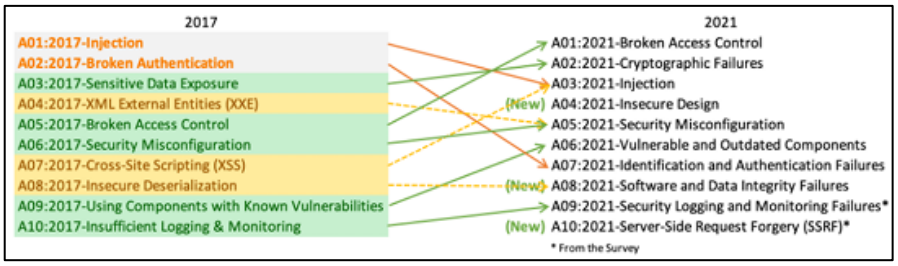
Rumah Potong Hewan (RPH) Surabaya merupakan salah satu instansi yang memanfaatkan website sebagai media penyampaian informasi kepada masyarakat dan memiliki potensi untuk diserang oleh orang yang tidak bertanggung jawab. Berdasarkan informasi yang diperoleh dari pihak pengelola, website RPH Surabaya pernah mengalami peretasan dengan munculnya konten yang tidak relevan.

Sejumlah penelitian sebelumnya telah membahas pengujian keamanan website menggunakan standar OWASP Top 10, salah satunya pada website XYZ yang berhasil mengidentifikasi kerentanan berdasarkan penilaian risiko OWASP (Priambodo et al., 2023). Penelitian yang membahas pemindaian kerentanan website instansi pada sektor pengelolaan sistem yang masih terbatas. Inilah yang menjadi dasar dilakukannya penelitian pada RPH Surabaya sebagai objek kajian.

Unsur baru penelitian ini dengan menerapkan pemindaian kerentanan berbasis OWASP Top 10 2021 pada website instansi pelayanan publik yang masih jarang menjadi fokus penelitian sebelumnya. Tujuan dari penelitian ini untuk mengidentifikasi kerentanan keamanan berdasarkan standar OWASP Top 10 2021 serta memberikan rekomendasi perbaikan untuk memperkuat sistem . Dengan demikian, hasil penelitian ini diharapkan mampu memberikan kontribusi dalam mendukung penerapan keamanan siber pada layanan berbasis web.

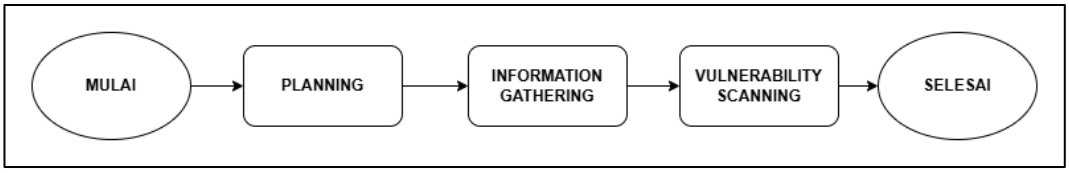
B. METODE

Penelitian ini memetakan kerentanan keamanan berdasarkan standar OWASP Top 10 2021 dengan menggunakan Kali Linux sebagai OS dan mozila firefox sebagai browser melalui tiga tahapan utama, yaitu *planning*, *information gathering*, dan *vulnerability scanning*.



Gambar 1. Daftar OWASP Top 10

Gambar 1. menunjukkan perbandingan OWASP Top 10 tahun 2017 dan 2021 yang disusun dengan pendekatan berbasis data dari organisasi keamanan global serta survei dari OWASP. OWASP Top 10 merupakan dokumen standar keamanan aplikasi web yang berisi sepuluh kategori risiko keamanan aplikasi web yang kritis dan sering. sehingga menjadi rujukan utama bagi pengembang dan praktisi keamanan dalam mengidentifikasi serta memitigasi kerentanan paling signifikan pada aplikasi web (OWASP, 2021).



Gambar 2. Tahapan penelitian

Gambar 2. Merupakan alur tahapan penelitian dimana tahap *planning* merupakan tahap awal dalam pengujian keamanan yang berfungsi untuk menentukan sasaran serta ruang lingkup. Pada tahap ini ditetapkan sistem yang menjadi objek pengujian dan izin yang harus dipenuhi.. Tahap planning menjadi fondasi utama dalam pengujian keamanan karena menentukan arah dan keberhasilan seluruh tahapan berikutnya (Kissel, 2013).

Tahap *information gathering* merupakan proses pengumpulan informasi dengan tujuan memahami sistem sebelum dilakukan pemindaian kerentanan. Informasi yang dikumpulkan mencakup domain, IP, layanan, port, serta teknologi yang digunakan untuk menjadi dasar penting dalam menentukan strategi dan fokus pada tahap vulnerability scanning berikutnya (Scarfone & Mell, 2012). Tools yang digunakan pada terminal kali linux tahap ini yaitu, whois untuk mengetahui domain dan pemilik IP, nslookup untuk mengetahui

informasi DNS dan IP, nmap untk menemukan port yang terbuka, dirsearch untuk menemukan direktori yang tersembunyi yang dapat diakses, dan wappalyzer yang dijalankan pada browser untuk mengetahui teknologi yang digunakan.

Tahap terakhir *vulnerability scanning* untuk mengidentifikasi celah keamanan pada website. Tujuan utama dari *vulnerability scanning* adalah untuk memperoleh daftar kerentanan yang dapat dianalisis tingkat risikonya sebagai dasar tindakan perbaikan keamanan (Scarfone, Souppaya, Cody, & Orebaugh, 2008). Dalam tahap ini menggunakan tools OWASP ZAP dengan dua metode, yaitu *manual explore* dan *automated scan*. Manual explore dilakukan dengan menelusuri fitur website melalui browser yang terintegrasi dengan OWASP ZAP sehingga pemindaian secara pasif, *automated scan* dilakukan dengan menjalankan pemindaian aktif secara otomatis. Hasil pemindaian yang dihasilkan OWASP ZAP diklasifikasikan ke dalam beberapa tingkat risiko, yaitu *High, Medium, Low*, dan *Informational* yang menunjukkan tingkat keparahan setiap kerentanan yang ditemukan (OWASP, 2023)

C. HASIL DAN PEMBAHASAN

Pada tahap *planning* dilakukan untuk memperoleh perizinan, objek yang akan diuji, informasi riwayat keamanan, metode yang akan digunakan. Beberapa aspek penting pada tahap *planning* ada pada tabel 1. Berikut:

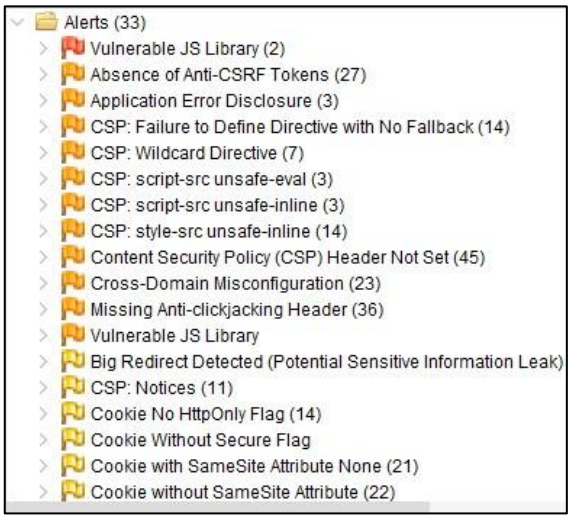
Tabel 1. Hasil tahap *planning*

No.	Aspek	Keterangan
1.	Objek Pengujian	Website resmi RPH Surabaya (https://www.rphsurabaya.co.id/)
2.	Riwayat Keamanan	Pernah diretas muncul konten tidak relevan
3.	Perizinan	Telah mendapat izin dari pihak RPH Surabaya dan dilaksanakan secara legal
4.	Metode Yang Digunakan	OWASP Top 10 2021 (klasifikasi kerentanan)

Pada tahap *information gathering* dilakukan untuk informasi dari sistem seperti informasi IP, Domain, teknologi yang digunakan, direktori yang dapat diakses, dan informasi port aktif sebagai informasi awal untuk tahap selanjutnya dan dapat sebagai kerentanan yang dapat diperbaiki. Beberapa hasil informasi dari pada tahap *information gathering* ada pada tabel 2. Berikut:

Tabel 2. Hasil tahap *information gathering*

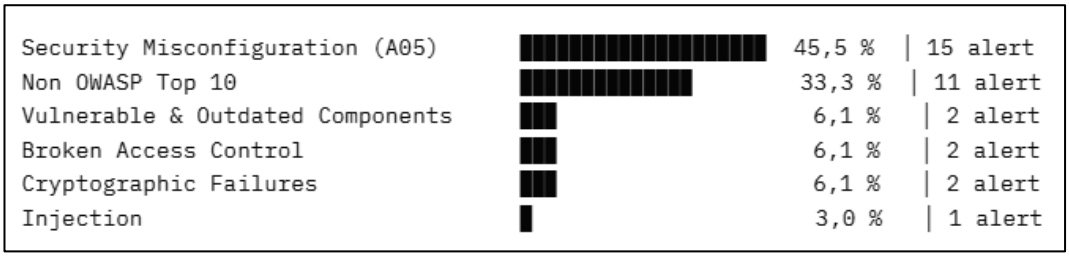
No.	Tools	Hasil
1.	Nslookup	IP website adalah 203.xxx.xxx.xxx
2.	whois	Domain RPH SURABAYA terdaftar pada PT Digital Registra Indonesia yang berlaku hingga Januari 2026. Status domain clientTransferProhibited dan serverTransferProhibited. Website dikelola penyedia hosting RUMAHWEB.
3.	nmap	Ditemukan port aktif FTP (21), HTTP (80), HTTPS (443), POP3 (110), IMAP (143), SMTPS (465), Submission (587), IMAPS (993), POP3S (995), RTSP (554), dan PPTP (1723).
4.	Dirsearch	Direktori yang dapat diakses seperti /administrator, /login, /index.php, /cpanel, /webmail, dan /download.
5.	Wappalyzer	Teknologi yang digunakan meliputi framework CodeIgniter, bahasa pemrograman PHP, web server LiteSpeed, pustaka jQuery versi 3.4.1, Bootstrap versi 4.4.1, Font Awesome, RSS, dan protokol HTTP/3.



Gambar 3. Hasil *vulnerability scanning* dengan OWASP ZAP

Gambar 3 merupakan hasil pemindaian kerentanan dengan OWASP ZAP yang menghasilkan ada 33 alert atau ada 33 kerentanan. Dari 33 kerentanan

yang didapatkan terbagi menjadi 1 kerentanan dengan level resiko tinggi, 11 kerentanan dengan level resiko medium, 11 kerentanan dengan level resiko rendah, dan 10 kerentanan dengan level resiko informational atau hanya bersifat informatif.



Gambar 4. Hasil dengan persentase chart

Pada gambar 4 merupakan hasil persentase yang menunjukkan 67% atau 22 alert kerentanan yang terdeteksi termasuk kedalam OWASP Top 10 2021 dan 33,3% atau 11 alert kerentanan yang tidak termasuk OWASP TOP 10 2021. 67% yang termasuk OWASP Top 10 2021 diantaranya adalah 45,5% A05 *Security Misconfiguration* dengan 15 alert kerentanan, 6,1% A06 *Vulnerable Components* dengan 2 alert kerentanan, 6,1% *A01 Broken Access Control* dengan 2 alert kerentanan, 6,1% *A02 Cryptographic Failures* dengan 2 alert kerentanan, dan 3,0% A03 *Injection* dengan 1 alert kerentanan.

Rekomendasi perbaikan untuk A05 *Security Misconfiguration* dengan memastikan seluruh header keamanan seperti Content-Security-Policy (CSP), X-Content-Type-Options, X-Frame-Options, dan Strict-Transport-Security (HSTS) diterapkan. Informasi versi server pada header HTTP harus disembunyikan, serta konfigurasi cookie perlu diperbaiki dengan mengaktifkan atribut Secure, HttpOnly, dan SameSite. Akses terhadap direktori dan file konfigurasi sensitif yang tidak diperlukan harus dibatasi.

Untuk A06 Vulnerable and Outdated Components dilakukan dengan memperbarui seluruh library, framework, dan komponen pihak ketiga yang digunakan, khususnya pustaka JavaScript yang terdeteksi memiliki kerentanan. Penggunaan dependency management seperti Composer atau NPM harus disertai dengan pemantauan kerentanan secara berkala melalui

database vulnerability resmi, serta mengganti komponen yang sudah tidak didukung.

A01 Broken Access Control dengan memperketat autentikasi dan otorisasi di sisi server untuk setiap halaman dan fitur penting. Implementasi Anti-CSRF Token wajib diterapkan pada seluruh form sensitif, serta penerapan role-based access control harus dilakukan secara konsisten agar pengguna tidak dapat mengakses fitur di luar haknya.

Perbaikan untuk A02 Cryptographic Failures dilakukan dengan memastikan seluruh komunikasi data sensitif menggunakan protokol HTTPS dengan konfigurasi SSL/TLS yang kuat dan sertifikat yang valid. Header HSTS harus diaktifkan untuk memaksa koneksi terenkripsi, serta pengiriman data sensitif melalui URL harus dihindari dan digantikan dengan mekanisme yang lebih aman.

Perbaikan untuk A03 Injection dilakukan dengan menerapkan validasi dan sanitasi terhadap seluruh input pengguna sebelum diproses oleh sistem. Penggunaan prepared statement atau parameterized query wajib diterapkan untuk mencegah SQL Injection, serta output encoding perlu digunakan untuk mencegah terjadinya serangan *Cross-Site Scripting* (XSS).

D. SIMPULAN

Berdasarkan hasil penelitian terhadap website RPH Surabaya menggunakan standar OWASP Top 10 2021 dapat disimpulkan bahwa masih terdapat sejumlah kerentanan keamanan yang perlu mendapatkan perhatian. Pengujian yang dilakukan melalui tahapan planning, information gathering, dan vulnerability scanning berhasil mengidentifikasi sebanyak 33 alert kerentanan dengan tingkat risiko yang bervariasi, mulai dari tinggi, sedang, rendah, hingga informasional. Dari keseluruhan temuan tersebut, sebanyak 22 kerentanan atau sebesar 67% termasuk dalam kategori OWASP Top 10 2021, dengan dominasi terbesar pada kategori A05:2021 – Security Misconfiguration.

Kerentanan yang ditemukan menunjukkan masih adanya kelemahan pada aspek konfigurasi keamanan, penggunaan komponen yang rentan, kontrol akses, mekanisme kriptografi, serta potensi serangan injection. Oleh karena itu, rekomendasi perbaikan yang diberikan diharapkan dapat menjadi acuan dalam meningkatkan keamanan website melalui perbaikan konfigurasi server, pembaruan komponen, penguatan kontrol akses, penerapan enkripsi yang kuat, serta pada validasi input. Hasil penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan kesadaran pentingnya pengujian keamanan website untuk mengurangi risiko serangan siber di masa mendatang.

DAFTAR PUSTAKA

Badan Siber dan Sandi Negara. (2022). Laporan Tahunan Honeynet Project Tahun 2022. BSSN. https://www.scribd.com/document/958694116/Laporan-Tahunan-Honeynet-Project-Tahun-2022-BSSN

Badan Siber dan Sandi Negara. (2023). Lanskap Keamanan Siber Indonesia 2023. BSSN. https://educsirt.kemendikdasmen.go.id/portal/berita/197

International Telecommunication Union. (2020). Global Cybersecurity Index 2020. ITU. https://www.itu.int

McGraw, G., Arkin, B., & Stender, S. (2005). Building Security In: Software Penetration Testing. Addison-Wesley Professional. https://dl.acm.org/doi/10.1109/MSP.2005.23

OWASP. (n.d.). OWASP Top Ten. https://owasp.org/www-project-top-ten/

Priambodo, D. F., Rifansyah, A. D., & Hasbi, M. (2023). Penetration testing Web XYZ berdasarkan OWASP risk rating. Teknika, 12(1), 33–46. https://doi.org/10.34148/teknika.v12i1.571

Widyanuratikah, I. (2025). Indonesia negara ketiga paling sering terkena serangan siber. Republika. https://news.republika.co.id/berita/pg9slu354/indonesia-negara-ketiga-paling-sering-terkena-serangan-siber

OWASP. (2021). OWASP Top 10: The Ten Most Critical Web Application Security Risks. https://owasp.org/Top10/

Kissel, R. (2013). Glossary of Key Information Security Terms. National Institute of Standards and Technology.

https://www.nist.gov/publications/glossary-key-information-security-terms-1

carfone, K., & Mell, P. (2012). Guide to Intrusion Detection and Prevention Systems. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/94/final

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical Guide to Information Security Testing and Assessment. National Institute of Standards and Technology. https://csrc.nist.rip/library/NIST%20SB%202008-12%20Guide%20To%20Information%20Security%20Testing%20And%20Assessment.pdf

OWASP. (2023). OWASP Zed Attack Proxy (ZAP) User Guide. The Open Web Application Security Project. https://www.zaproxy.org