**Repeater : Publikasi Teknik Informatika dan Jaringan**
**Volume. 4 Nomor. 3 Juli 2026**
e-ISSN : 3046-7276, p-ISSN : 3046-7284, Hal 75-88
DOI: https://doi.org/10.62951/repeater.v4i3.962
*Tersedia*: https://journal.aptii.or.id/index.php/Repeater

# Evaluasi Keamanan *Website* Unm.ac.id Menggunakan Metodologi *Penetration Testing* Berdasarkan Framework OWASP Top 10

**Muhammad Fadlu Rahman[1*], Satria Gunawan Zain[2], Abdul Rahman Patta[3]**
[1-3] Program Studi Teknik Komputer, Jurusan Teknik Informatika Dan Komputer, Fakultas Teknik, Universitas Negeri Makassar, Indonesia
*Email: mfadlurahmama@gmail.com [1*], satria.gunawan.zain@unm.ac.id [2], abd.rahman.patta@unm.ac.id [3]*

**Penulis Korespondensi: mfadlurahmama@gmail.com*

***Abstract****. The high incidence of cyberattacks across various sectors reported by the National Cyber and Crypto Agency (BSSN) poses a serious threat to data and service security in application systems, including at Makassar State University, which relies on web-based information technology for many of its activities, thereby creating potential risks to its website security. This study aims to evaluate the security of the domain unm.ac.id and its subdomains using penetration testing methods, identify security vulnerabilities based on the OWASP Top 10, and develop relevant mitigation strategies. The method used is penetration testing through several stages: information gathering, enumeration, vulnerability scanning, exploitation, OWASP Top 10–based security classification, risk assessment using CVSS 3.1, and formulation of mitigation strategies. The results identified 9 validated vulnerability types, with the majority of OWASP Top 10 classifications falling under security misconfiguration, cryptographic failures, and the use of vulnerable or outdated components. Most vulnerabilities were at medium, low, and informational levels. It can therefore be concluded that security mechanisms on the website have been implemented, but periodic evaluation and reinforcement of security are still required to minimize potential risks and prevent future attacks.*

***Keywords****: CVSS 3.1; OWASP Top 10; Penetration Testing; Unm.ac.id; Website Security.*

**Abstrak**. Tingginya insiden serangan siber menurut Badan Siber dan Sandi Negara (BSSN) di berbagai sektor dapat mengancam keamanan data dan layanan pada sistem aplikasi, termasuk pada Universitas Negeri Makassar, yang menggunakan teknologi informasi berbasis website dalam melakukan berbagai aktivitas. Hal ini menyebabkan terjadinya potensi pada keamanan website. Penelitian ini bertujuan untuk mengevaluasi keamanan domain unm.ac.id dan subdomain menggunakan metode penetration testing, mengidentifikasi celah keamanan berdasarkan OWASP Top 10, serta menyusun strategi mitigasi yang relevan. Metode yang digunakan adalah penetration testing melalui tahapan information gathering, enumeration, vulnerability scanning, exploitation, klasifikasi keamanan berbasi OWASP Top 10, penilaian risiko berdasarkan CVSS 3.1, dan menyusun strategi mitigasi. Hasil penelitian menemukan 9 jenis kerentanan tervalidasi dengan mayoritas klasifikasi berdasakan OWASP Top 10 adalah kesalahan konfigurasi, kegagalan kriptografi, dan penggunaan komponen yang memiliki kerentanan atau versi lama. Sebagian besar kerentanan berada pada tingkat medium, low, dan informational. Dengan demikian dapat disimpulkan bahwa mekanisme keamanan pada website telah diterapkan, namun masih diperlukan evaluasi dan penguatan keamanan secara berkala untuk meminimalkan potensi risiko dan mencegah serangan lanjutan di masa mendatang.

**Kata kunci**: CVSS 3.1; Keamanan Website; OWASP Top 10; Penetration Testing; Unm.ac.id.

## 1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi pada berbagai bidang melalui peningkatan kecepatan pertukaran informasi, efisiensi layanan, dan keterhubungan antarsistem. Di sisi lain, peningkatan ketergantungan terhadap teknologi juga memperluas permukaan serangan dan meningkatkan risiko penyalahgunaan sistem informasi. Ancaman tersebut dapat memengaruhi kerahasiaan, integritas, dan ketersediaan data, baik pada tingkat individu maupun organisasi. Daeng et al. (2023) menjelaskan bahwa perkembangan teknologi tidak hanya memberikan manfaat, tetapi juga membuka peluang terjadinya berbagai

*Naskah Masuk: 23 Mei 2026; Revisi: 20 Juni 2026; Diterima: 25 Juli 2026; Terbit: 27 Juli 2026*

bentuk kejahatan siber. Kondisi tersebut menempatkan keamanan siber sebagai komponen yang harus diintegrasikan dalam pengembangan dan pengelolaan sistem informasi.

Risiko keamanan siber di Indonesia masih menunjukkan tingkat yang perlu mendapat perhatian. Berdasarkan *National Cyber Security Index*, Indonesia memperoleh skor keamanan siber sebesar 63,64 dari 100 pada tahun 2023, menempati peringkat ke-12 di antara negara anggota G20 dan peringkat ke-49 dari 176 negara secara global (National Cyber Security Index, 2023). Badan Siber dan Sandi Negara (BSSN, 2024) mencatat 330.527.636 anomali lalu lintas siber sepanjang tahun 2024, termasuk 5.780 insiden yang menargetkan domain tertentu. Kegiatan *IT Security Assessment* pada tahun yang sama juga menemukan 1.931 kerentanan dengan tingkat risiko yang bervariasi. Jenis kerentanan yang dominan mencakup *information disclosure*, *insecure direct object reference* (IDOR), *cross-site scripting* (XSS), *weak password policy*, dan *broken access control*. Selain itu, sebanyak 2.362 domain dilaporkan terdampak insiden keamanan, yang menunjukkan luasnya paparan sistem berbasis web terhadap ancaman siber (BSSN, 2024).

Risiko tersebut juga relevan bagi perguruan tinggi yang menggunakan aplikasi web untuk mendukung layanan akademik, administrasi, pembelajaran, penelitian, dan penyebaran informasi. Sistem informasi akademik, *learning management system*, repositori institusi, perpustakaan digital, dan layanan registrasi mengelola data mahasiswa, dosen, serta aktivitas akademik yang bersifat sensitif. Pemanfaatan teknologi informasi dalam pendidikan tinggi memang meningkatkan aksesibilitas dan efisiensi layanan, tetapi juga menimbulkan kebutuhan perlindungan terhadap data dan keberlangsungan sistem (Handayani et al., 2019). Darmawan et al. (2024) menegaskan bahwa aplikasi web institusi pendidikan dapat menjadi sasaran serangan seperti XSS, kebocoran informasi, kesalahan konfigurasi, dan gangguan ketersediaan layanan. Keamanan aplikasi web perguruan tinggi harus mencakup perlindungan terhadap aspek *confidentiality*, *integrity*, dan *availability* sebagai elemen utama *CIA triad*.

Universitas Negeri Makassar (UNM) memanfaatkan domain utama dan berbagai subdomain untuk menyediakan sistem informasi akademik, layanan pembelajaran, publikasi ilmiah, perpustakaan, registrasi, serta layanan administratif lainnya. Berdasarkan observasi awal dan wawancara dengan pengelola infrastruktur teknologi informasi, lingkungan aplikasi web UNM pernah mengalami serangan *distributed denial-of-service* (DDoS), *bypass* administrator pada WordPress, perubahan tampilan situs atau *web defacement*, serta IDOR. Penggunaan komponen dan teknologi yang belum diperbarui secara konsisten juga dapat menciptakan celah yang tetap dapat dimanfaatkan meskipun sistem telah dilindungi oleh *web application firewall*. Kondisi tersebut menunjukkan bahwa keberadaan perangkat perlindungan

tidak menggantikan kebutuhan terhadap pembaruan komponen, penguatan konfigurasi, pengendalian akses, dan evaluasi keamanan secara berkala (Darmawan et al., 2024).

Salah satu metode yang dapat digunakan untuk mengevaluasi keamanan aplikasi web adalah *penetration testing*. Metode ini dilakukan dengan menyimulasikan teknik serangan secara terkendali dan berizin untuk mengidentifikasi kerentanan yang berpotensi dieksploitasi oleh pihak tidak berwenang. Berbeda dari pemindaian kerentanan yang hanya menghasilkan daftar indikasi kelemahan, *penetration testing* mencakup pengumpulan informasi, enumerasi, analisis kerentanan, validasi, eksploitasi terbatas, dan pelaporan hasil pengujian (Adam et al., 2023). Lazarov et al. (2025) menjelaskan bahwa proses pengujian penetrasi yang sistematis diperlukan agar ruang lingkup, bukti teknis, tingkat risiko, dan rekomendasi perbaikan dapat didokumentasikan secara konsisten.

Kerentanan yang ditemukan melalui proses tersebut perlu diklasifikasikan menggunakan kerangka yang terstandar. OWASP Top 10 menyediakan kategori risiko utama aplikasi web yang dapat digunakan untuk mengidentifikasi pola kelemahan, seperti *broken access control*, *cryptographic failures*, *injection*, *security misconfiguration*, serta penggunaan komponen yang rentan atau tidak diperbarui. Penggunaan OWASP Top 10 membantu mengubah temuan teknis menjadi kategori risiko yang lebih sistematis dan dapat dipahami oleh pengembang maupun pengelola sistem (Darmawan et al., 2024; Supriyatna et al., 2024). Tingkat keparahan setiap temuan selanjutnya dapat dinilai menggunakan *Common Vulnerability Scoring System* (CVSS) berdasarkan karakteristik serangan dan dampaknya terhadap kerahasiaan, integritas, serta ketersediaan sistem (Dharmawangsa et al., 2023).

Meskipun pemindai otomatis dapat mempercepat identifikasi awal, hasil pemindaian tidak seluruhnya menunjukkan kerentanan yang benar-benar dapat dieksploitasi. Alat otomatis dapat menghasilkan *false positive* akibat perbedaan konfigurasi server, mekanisme perlindungan, respons aplikasi, dan kondisi lingkungan pengujian. Karena itu, setiap indikasi kerentanan perlu diverifikasi melalui pengujian manual dan analisis respons sistem sebelum ditetapkan sebagai temuan valid. Zahra et al. (2023) menyatakan bahwa evaluasi keamanan tidak hanya memerlukan identifikasi celah, tetapi juga penilaian dampak dan penyusunan rekomendasi teknis yang dapat dipahami oleh pengelola sistem. Validasi manual juga diperlukan untuk mencegah penetapan tingkat risiko yang terlalu tinggi terhadap temuan yang tidak memiliki dampak nyata.

Sejumlah penelitian terdahulu telah menggunakan OWASP ZAP dan kerangka OWASP untuk menilai keamanan aplikasi web akademik maupun pemerintahan (Darul Fata, 2023; Herawati et al., 2023; Muhammad Fauzi et al., 2024). Namun, sebagian penelitian masih

berfokus pada hasil pemindaian otomatis tanpa memberikan validasi manual yang memadai terhadap setiap indikasi kerentanan. Pendekatan tersebut dapat menyebabkan hasil pemindai diperlakukan sebagai temuan akhir meskipun belum dibuktikan melalui *proof of concept*. Prasetiyo et al. (2024) telah mengombinasikan pemindaian dan validasi menggunakan beberapa perangkat pengujian, tetapi penelitian yang mengintegrasikan pemetaan aset dalam satu ekosistem domain perguruan tinggi, penggunaan beberapa perangkat pemindai, validasi manual, klasifikasi OWASP Top 10, penilaian CVSS 3.1, dan strategi mitigasi masih terbatas.

Berdasarkan kesenjangan tersebut, penelitian ini bertujuan mengevaluasi keamanan domain dan subdomain Universitas Negeri Makassar melalui *penetration testing* non-destruktif yang mengombinasikan pengujian otomatis dan manual. Pengujian dilakukan melalui tahapan *information gathering*, *enumeration*, *vulnerability scanning*, validasi dan eksploitasi terkendali, klasifikasi temuan berdasarkan OWASP Top 10 tahun 2021, serta penilaian risiko menggunakan CVSS 3.1. Setiap temuan yang tervalidasi didokumentasikan dalam bentuk bukti teknis terbatas dan dilengkapi dengan strategi mitigasi berdasarkan karakteristik kerentanan. Kontribusi penelitian ini terletak pada penerapan proses evaluasi yang tidak hanya mengandalkan keluaran perangkat pemindai, tetapi juga menekankan validasi *false positive*, penilaian dampak aktual, dan penyusunan rekomendasi perbaikan yang dapat digunakan dalam pengelolaan keamanan aplikasi web perguruan tinggi.

## 2. KAJIAN TEORITIS

### Keamanan Aplikasi Web

Website merupakan kumpulan halaman yang saling terhubung dan diakses melalui protokol HTTP atau HTTPS menggunakan peramban. Selain menyajikan informasi, website modern juga menjalankan berbagai layanan yang melibatkan penyimpanan, pemrosesan, dan pertukaran data pengguna (Wirawan et al., 2024). Kondisi tersebut menyebabkan aplikasi web rentan terhadap pencurian data, perubahan informasi, akses tidak sah, dan gangguan layanan apabila tidak dilengkapi dengan pengamanan yang memadai.

Keamanan aplikasi web bertujuan menjaga aspek *confidentiality*, *integrity*, dan *availability* melalui perlindungan terhadap aplikasi, server, jaringan, serta data yang dikelola. Kerentanan dapat muncul akibat kesalahan konfigurasi, kelemahan autentikasi, penggunaan komponen usang, atau pengelolaan informasi sensitif yang tidak tepat (Nurelasari et al., 2024). *Web application firewall* (WAF) dapat memberikan perlindungan tambahan dengan memantau dan menyaring lalu lintas HTTP/HTTPS yang berbahaya, tetapi efektivitasnya tetap

bergantung pada konfigurasi, pembaruan aturan, dan mekanisme keamanan pada aplikasi itu sendiri (Dawadi et al., 2023).

**Penetration Testing**

*Penetration testing* merupakan pengujian keamanan yang dilakukan dengan menyimulasikan serangan secara terkendali dan berizin untuk mengidentifikasi serta memvalidasi kerentanan yang dapat dieksploitasi. Pengujian ini tidak hanya mendeteksi indikasi kelemahan, tetapi juga menilai kemungkinan eksploitasi dan dampaknya terhadap sistem (Adam et al., 2023).

Tahapan umum *penetration testing* meliputi perencanaan, pengumpulan informasi, enumerasi, pemindaian kerentanan, eksploitasi terkendali, analisis risiko, dan pelaporan (Lazarov et al., 2025). Pengujian dapat mengombinasikan perangkat otomatis untuk memperluas cakupan pemindaian dengan pemeriksaan manual untuk memvalidasi hasil dan mengurangi *false positive* (Kongara & Krishnama, 2023).

Berdasarkan tingkat informasi yang diberikan kepada penguji, *penetration testing* dapat dilakukan melalui pendekatan *black-box, grey-box*, dan *white-box*. Pendekatan *black-box* menempatkan penguji sebagai penyerang eksternal tanpa informasi internal sistem. *Grey-box* memberikan sebagian informasi atau hak akses pengguna biasa, sedangkan *white-box* memberikan akses terhadap kode sumber, arsitektur, dan konfigurasi sistem. Penelitian ini menggunakan pendekatan *black-box* untuk menggambarkan risiko serangan dari pihak eksternal.

**OWASP Top 10**

Open Worldwide Application Security Project (OWASP) merupakan organisasi terbuka yang menyediakan standar, dokumentasi, dan perangkat untuk meningkatkan keamanan aplikasi web (Herawati et al., 2023). Salah satu pedoman utamanya adalah OWASP Top 10, yaitu klasifikasi risiko keamanan aplikasi web yang digunakan untuk membantu proses identifikasi, evaluasi, dan mitigasi kerentanan (Supriyatna et al., 2024).

OWASP Top 10 tahun 2021 terdiri atas *broken access control*, *cryptographic failures*, *injection*, *insecure design*, *security misconfiguration*, *vulnerable and outdated components*, *identification and authentication failures*, *software and data integrity failures*, *security logging and monitoring failures*, serta *server-side request forgery*. Dalam penelitian ini, OWASP Top 10 digunakan untuk mengelompokkan kerentanan yang telah melalui proses validasi, bukan untuk menetapkan kerentanan hanya berdasarkan keluaran perangkat pemindai.

**Perangkat Pengujian Keamanan**

Pengujian menggunakan beberapa perangkat dengan fungsi yang berbeda pada setiap tahap. OWASP ZAP digunakan untuk pemindaian otomatis dan analisis lalu lintas HTTP/HTTPS melalui fitur *passive scanner*, *active scanner*, dan *intercepting proxy* (Herawati et al., 2023). Burp Suite digunakan untuk menangkap, memodifikasi, dan menguji permintaan maupun respons aplikasi melalui fitur *Proxy*, *Repeater*, dan *Intruder* (Dwi Agustina et al., 2025).

Perangkat lain digunakan sesuai kebutuhan pengujian, seperti Subfinder untuk enumerasi subdomain, HTTPX untuk memverifikasi subdomain aktif, Nuclei untuk mendeteksi pola kerentanan, SQLMap untuk validasi *SQL injection*, serta Wappalyzer untuk mengidentifikasi teknologi dan komponen aplikasi. Hasil pemindaian perangkat tersebut tetap diperiksa secara manual sebelum dinyatakan sebagai temuan yang valid.

**Common Vulnerability Scoring System**

*Common Vulnerability Scoring System* (CVSS) merupakan kerangka penilaian yang digunakan untuk mengukur tingkat keparahan kerentanan secara kuantitatif. CVSS versi 3.1 menilai karakteristik kerentanan berdasarkan *attack vector*, *attack complexity*, *privileges required*, *user interaction*, *scope*, serta dampaknya terhadap *confidentiality*, *integrity*, dan *availability* (Dharmawangsa et al., 2023).

Skor CVSS diklasifikasikan menjadi rendah pada skor 0,1–3,9, sedang pada skor 4,0–6,9, tinggi pada skor 7,0–8,9, dan kritis pada skor 9,0–10,0. Dalam penelitian ini, CVSS 3.1 digunakan untuk menentukan tingkat keparahan dan prioritas mitigasi pada setiap kerentanan yang telah divalidasi. Temuan yang tidak menunjukkan dampak keamanan yang dapat dihitung ditempatkan sebagai informasi tambahan dan tidak dinilai sebagai kategori resmi CVSS.

## 3. METODE PENELITIAN

Penelitian ini merupakan penelitian evaluatif deskriptif menggunakan *authorized black-box penetration testing* untuk menilai keamanan aplikasi web pada domain dan subdomain Universitas Negeri Makassar. Pengujian dilaksanakan selama Oktober 2025–Januari 2026 secara daring dan luring di Laboratorium Jaringan dan *Security*, Fakultas Teknik, Universitas Negeri Makassar. Penelitian telah memperoleh izin resmi dari Direktur UPT TIK Universitas Negeri Makassar dan difokuskan pada 11 subdomain utama yang telah disepakati. Seluruh pengujian dilakukan secara non-destruktif tanpa serangan *denial-of-service*, rekayasa sosial, pengambilan data, eskalasi hak akses, atau tindakan lain yang berpotensi mengganggu layanan dan privasi pengguna.

Pengujian meliputi tahapan *information gathering*, *enumeration*, *vulnerability scanning*, validasi dan eksploitasi terkendali, klasifikasi kerentanan, serta pelaporan. Perangkat yang digunakan meliputi Subfinder, HTTPX, Wappalyzer, OWASP ZAP, Nuclei, Burp Suite, SQLMap, dan perangkat pendukung lainnya. Setiap indikasi kerentanan diverifikasi secara manual untuk membedakan temuan valid dari *false positive*, kemudian diklasifikasikan berdasarkan OWASP Top 10 tahun 2021. Tingkat keparahan temuan dinilai menggunakan CVSS 3.1 berdasarkan karakteristik serangan dan dampaknya terhadap kerahasiaan, integritas, serta ketersediaan sistem. Hasil analisis didokumentasikan dalam bentuk *proof of concept* terbatas dan dilengkapi dengan rekomendasi mitigasi sesuai karakteristik setiap kerentanan.

## 4. HASIL DAN PEMBAHASAN

### Hasil

Tahap *information gathering* dilakukan melalui enumerasi subdomain, identifikasi teknologi, dan pengumpulan informasi terbuka. Subfinder mengidentifikasi 847 subdomain, crt.sh menemukan 546 subdomain, dan layanan enumerasi berbasis web menemukan 386 subdomain. Setelah proses deduplikasi dan pemeriksaan konektivitas, diperoleh 209 subdomain aktif yang digunakan dalam tahapan berikutnya. Teknologi yang teridentifikasi mencakup Cloudflare, BIG-IP, PHP, Laravel, WordPress, dan beberapa versi jQuery. Pada tahap enumerasi sisi klien, sebanyak 19.193 berkas JavaScript dikumpulkan dan 757 berkas dapat diakses secara publik. Pemeriksaan lanjutan tidak menemukan *application programming interface key*, token, kredensial, atau konfigurasi sensitif pada berkas tersebut.

Pemindaian otomatis menggunakan OWASP ZAP menghasilkan 4 indikasi risiko tinggi, 27 sedang, 32 rendah, dan 29 informasional. Nuclei menghasilkan 10 indikasi sedang, 195 rendah, dan 3.307 informasional. Seluruh hasil tidak langsung ditetapkan sebagai kerentanan, tetapi diverifikasi melalui pengujian manual. Indikasi *SQL injection*, *path traversal*, *server-side request forgery*, enumerasi pengguna WordPress, dan *subdomain takeover* tidak dapat dibuktikan secara teknis sehingga diklasifikasikan sebagai *false positive*. Hasil ini menunjukkan bahwa keluaran pemindai otomatis memerlukan validasi sebelum digunakan untuk menentukan kondisi keamanan aplikasi.

**Tabel 1.** Temuan Kerentanan yang Tervalidasi.

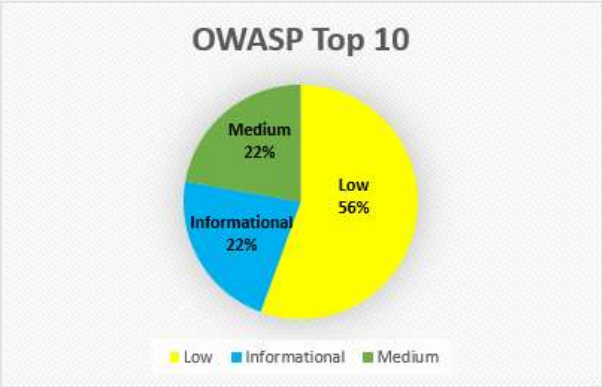
| No. | Kerentanan tervalidasi | Aset terdampak | Kategori OWASP Top 10 | CVSS 3.1 | Tingkat risiko |
|---|---|---|---|---|---|
| 1 | *Apache Server Status Page Exposure* | 2 subdomain | A05:2021–*Security Misconfiguration* | 5,3 | Sedang |
| 2 | *Sensitive Information Disclosure* | 1 subdomain | A02:2021–*Cryptographic Failures* | 5,3 | Sedang |
| 3 | *Verbose Database Error Disclosure* | 1 subdomain | A05:2021–*Security Misconfiguration* | 3,7 | Rendah |
| 4 | Berkas ZIP aplikasi dapat diakses publik | 4 subdomain | A05:2021–*Security Misconfiguration* | 3,7 | Rendah |
| 5 | *Clickjacking* | 24 subdomain | A05:2021–*Security Misconfiguration* | 3,7 | Rendah |
| 6 | *Origin IP Exposure* akibat kesalahan konfigurasi TLS | 1 subdomain | A05:2021–*Security Misconfiguration* | 3,7 | Rendah |
| 7 | Halaman phpinfo() dapat diakses publik | 5 subdomain | A05:2021–*Security Misconfiguration* | 3,7 | Rendah |
| 8 | Penggunaan pustaka JavaScript usang | 3 subdomain | A06:2021–*Vulnerable and Outdated Components* | Tidak dinilai | Informasional |
| 9 | Metode HTTP OPTIONS diaktifkan | 1 subdomain | A05:2021–*Security Misconfiguration* | Tidak dinilai | Informasional |

Sebagian besar temuan berada dalam kategori A05:2021–*Security Misconfiguration*. Kerentanan tersebut meliputi halaman status Apache dan phpinfo() yang terbuka, pesan kesalahan basis data yang terlalu rinci, berkas cadangan aplikasi yang dapat diakses publik, tidak adanya perlindungan terhadap *clickjacking*, paparan alamat IP server asal, dan aktivasi metode HTTP yang tidak diperlukan. Temuan terbanyak adalah *clickjacking* pada 24 subdomain akibat tidak diterapkannya X-Frame-Options atau direktif frame-ancestors pada *Content Security Policy*. Walaupun tergolong berisiko rendah, cakupan aset yang luas menunjukkan perlunya penerapan konfigurasi keamanan secara terpusat dan konsisten.

Dua temuan dengan tingkat risiko sedang adalah akses publik terhadap halaman status Apache dan dokumen yang memuat kredensial dalam bentuk teks biasa. Halaman status Apache mengungkapkan informasi aktivitas server, versi perangkat lunak, jaringan internal, dan permintaan yang sedang diproses. Sementara itu, dokumen publik yang memuat nama pengguna dan kata sandi dapat meningkatkan risiko pengambilalihan akun apabila kredensial masih aktif atau digunakan kembali pada layanan lain. Validasi kredensial tidak dilakukan untuk menjaga etika penelitian dan mencegah akses tidak sah.

Lima temuan memperoleh skor CVSS 3.1 sebesar 3,7 dan dikategorikan berisiko rendah. Pesan kesalahan basis data mengungkapkan struktur kueri, nama tabel atau kolom, jalur berkas, dan kode kesalahan, tetapi pengujian lanjutan tidak membuktikan adanya *SQL injection*. Berkas ZIP yang dapat diakses publik mengungkapkan struktur aplikasi dan aset kode sumber.

Paparan alamat IP server asal memungkinkan akses langsung tanpa melalui lapisan perlindungan, sedangkan halaman phpinfo() mengungkapkan konfigurasi PHP, sistem operasi, modul, alamat internal, dan variabel lingkungan. Dua temuan lain, yaitu penggunaan jQuery versi usang dan aktivasi metode OPTIONS, ditempatkan sebagai informasi tambahan karena belum menunjukkan dampak keamanan yang dapat dinilai menggunakan CVSS.




**Gambar 1.** Distribusi Tingkat Risiko Temuan Tervalidasi.

Gambar distribusi tingkat risiko menampilkan dua temuan sedang, lima temuan rendah, dan dua temuan informasional. Tidak ditemukan kerentanan tervalidasi dengan tingkat risiko tinggi atau kritis. Distribusi tersebut menunjukkan bahwa kelemahan keamanan lebih banyak disebabkan oleh konfigurasi sistem, pengelolaan berkas, dan pemeliharaan komponen dibandingkan kerentanan yang memungkinkan eksploitasi langsung atau eskalasi hak akses.

Strategi mitigasi diprioritaskan pada penonaktifan halaman status dan phpinfo() pada lingkungan produksi, penghapusan dokumen sensitif serta berkas cadangan dari direktori publik, penerapan *custom error handling*, dan pemasangan X-Frame-Options atau Content-Security-Policy: frame-ancestors. Akses langsung ke server asal perlu dibatasi menggunakan *firewall* atau daftar IP yang diizinkan, sedangkan pustaka JavaScript harus diperbarui dan metode HTTP dibatasi hanya pada fungsi yang diperlukan. Seluruh nama subdomain, alamat IP, dan informasi teknis sensitif perlu tetap disamarkan pada artikel publikasi.

**Pembahasan**

*Penetration testing* digunakan untuk mengevaluasi keamanan aplikasi web melalui identifikasi, verifikasi, dan penilaian kerentanan yang berpotensi dieksploitasi. Pengujian pada domain Universitas Negeri Makassar dilakukan melalui tahapan *information gathering*, *enumeration*, *vulnerability scanning*, eksploitasi terkendali, dan pelaporan. Temuan yang telah divalidasi kemudian diklasifikasikan berdasarkan OWASP Top 10 dan dinilai menggunakan CVSS 3.1 untuk menentukan prioritas mitigasi.

Tahap pengumpulan informasi menghasilkan 209 subdomain aktif beserta informasi teknologi dan sumber daya yang tersedia secara publik. Enumerasi terhadap parameter, *endpoint*, direktori, dan berkas JavaScript menemukan sejumlah lokasi yang memerlukan pemeriksaan lanjutan. Meskipun terdapat 757 berkas JavaScript yang dapat diakses, tidak ditemukan *application programming interface key*, token, kredensial, atau konfigurasi sensitif. Temuan ini menunjukkan bahwa risiko kebocoran informasi melalui berkas JavaScript relatif rendah pada saat pengujian.

Pemindaian menggunakan OWASP ZAP, Nuclei, dan Subzy menghasilkan sejumlah indikasi kerentanan, tetapi tidak seluruhnya dapat dibuktikan. Indikasi *SQL injection*, *path traversal*, *server-side request forgery*, enumerasi pengguna WordPress, dan *subdomain takeover* tidak menunjukkan dampak teknis setelah validasi sehingga diklasifikasikan sebagai *false positive*. Pada pengujian *time-based SQL injection*, waktu respons tidak mengalami penundaan sesuai skenario serangan, sedangkan modifikasi parameter *path traversal* tidak menghasilkan informasi sensitif. Temuan SSRF menghasilkan respons 404, dan indikasi *subdomain takeover* tidak disertai bukti bahwa layanan dapat diambil alih. Hasil tersebut menegaskan bahwa keluaran perangkat otomatis harus diverifikasi sebelum dinyatakan sebagai kerentanan.

Pengujian mengidentifikasi sembilan jenis kerentanan valid, yaitu halaman status Apache yang dapat diakses publik, dokumen berisi kredensial dalam teks biasa, *verbose database error disclosure*, berkas ZIP aplikasi yang terbuka, *clickjacking*, paparan alamat IP server asal, halaman phpinfo() yang terbuka, penggunaan pustaka JavaScript usang, dan aktivasi metode HTTP OPTIONS. Pada temuan *verbose error handling*, pesan kesalahan mengungkapkan struktur kueri dan informasi internal sistem. Namun, pengujian menggunakan SQLMap tidak menemukan parameter yang dapat dieksploitasi sehingga kelemahan terbatas pada pengungkapan informasi dan belum berkembang menjadi *SQL injection*.

*Clickjacking* merupakan temuan dengan cakupan terluas, yaitu pada 24 subdomain. Kerentanan terjadi karena tidak diterapkannya X-Frame-Options atau kebijakan frame-ancestors, sehingga halaman dapat dimuat melalui elemen iframe pada situs lain. Kondisi tersebut dapat dimanfaatkan untuk *user interface redressing*, yaitu mengarahkan pengguna melakukan tindakan yang berbeda dari tampilan yang dipersepsikan. Walaupun tingkat risikonya rendah, jumlah aset terdampak menunjukkan belum konsistennya penerapan *security header* pada seluruh subdomain.

Berdasarkan OWASP Top 10 tahun 2021, temuan didominasi kategori A05:2021–*Security Misconfiguration*. Kategori ini mencakup halaman status server, phpinfo(), berkas

cadangan, *clickjacking*, paparan alamat IP asal, metode OPTIONS, dan penanganan pesan kesalahan. *Sensitive information disclosure* diklasifikasikan sebagai A02:2021–*Cryptographic Failures* karena kredensial ditampilkan dalam teks biasa, sedangkan penggunaan jQuery usang termasuk A06:2021–*Vulnerable and Outdated Components*. Dominasi kesalahan konfigurasi menunjukkan bahwa kelemahan lebih banyak disebabkan oleh pengelolaan server, berkas, dan komponen yang belum konsisten daripada kerentanan yang memungkinkan eskalasi hak akses secara langsung.

Penilaian risiko menghasilkan dua temuan tingkat sedang, lima tingkat rendah, dan dua temuan informasional. Temuan tingkat sedang berkaitan dengan pengungkapan status server dan kredensial, sedangkan temuan tingkat rendah terutama berupa kesalahan konfigurasi yang dapat membantu proses *reconnaissance* atau serangan lanjutan. Penilaian akhir mempertimbangkan skor CVSS 3.1, dampak aktual, dan hasil evaluasi bersama pengelola server. Tidak ditemukan kerentanan tervalidasi dengan tingkat risiko tinggi atau kritis.

Hasil penelitian ini memperlihatkan perbedaan antara pemindaian otomatis dan pengujian yang disertai validasi manual. Darul Fata (2023) menggunakan OWASP ZAP untuk mengidentifikasi kerentanan pada aplikasi akademik, tetapi tidak seluruh temuannya disertai validasi teknis. Muhammad Fauzi et al. (2024) juga menggunakan hasil perangkat pemindai sebagai dasar analisis, sehingga kemungkinan *false positive* belum sepenuhnya dieliminasi. Sebaliknya, Prasetiyo et al. (2024) mengombinasikan OWASP ZAP dan Burp Suite untuk memverifikasi kerentanan. Penelitian ini menerapkan pendekatan serupa dengan memperluas pemindaian pada ekosistem subdomain dan memvalidasi setiap indikasi sebelum dilakukan klasifikasi risiko.

Observasi awal menunjukkan bahwa lingkungan web UNM sebelumnya pernah mengalami DDoS, *web defacement*, *bypass* administrator WordPress, dan IDOR. Kerentanan *bypass* administrator dan IDOR tidak ditemukan kembali selama pengujian, yang mengindikasikan adanya perbaikan terhadap kelemahan sebelumnya. Keberadaan BIG-IP dan Cloudflare juga diduga membantu menyaring lalu lintas berbahaya. Namun, perlindungan WAF belum menggantikan kebutuhan untuk melakukan *hardening*, pembaruan komponen, pembatasan akses, serta evaluasi keamanan secara berkala.

Rekomendasi mitigasi difokuskan pada penonaktifan halaman status Apache dan phpinfo() pada lingkungan produksi, penghapusan dokumen serta berkas cadangan dari direktori publik, penerapan *custom error handling*, pemasangan X-Frame-Options atau *Content Security Policy*, pembatasan akses langsung ke server asal, pembaruan pustaka JavaScript, dan pembatasan metode HTTP. Rekomendasi tersebut disusun berdasarkan

karakteristik temuan dan mengacu pada praktik mitigasi yang digunakan dalam penelitian Darul Fata (2023) dan Prasetiyo et al. (2024). Pengujian ulang setelah perbaikan diperlukan untuk memastikan bahwa mitigasi telah diterapkan tanpa mengganggu fungsi layanan.

## 5. KESIMPULAN DAN SARAN

Penerapan *penetration testing* pada domain dan subdomain Universitas Negeri Makassar melalui tahapan *information gathering*, *enumeration*, *vulnerability scanning*, validasi, dan eksploitasi terkendali berhasil mengidentifikasi kerentanan yang didominasi oleh kategori A05:2021–*Security Misconfiguration*, disertai A02:2021–*Cryptographic Failures* dan A06:2021–*Vulnerable and Outdated Components*. Penilaian menggunakan CVSS 3.1 menunjukkan bahwa temuan berada pada tingkat sedang, rendah, dan informasional, sehingga perbaikan perlu diprioritaskan pada penguatan konfigurasi server, pembatasan akses terhadap informasi sensitif, pembaruan komponen, serta penerapan kontrol keamanan tambahan. Pengelola sistem disarankan segera menerapkan mitigasi dan melakukan *re-testing*, *hardening*, audit, serta pemantauan keamanan secara berkala. Penelitian berikutnya dapat memperluas ruang lingkup melalui pendekatan *grey-box* atau *white-box testing*, pengujian keamanan jaringan, evaluasi WAF dan SIEM, serta analisis terhadap layanan internal untuk memperoleh gambaran keamanan yang lebih menyeluruh.

## DAFTAR REFERENSI

Adam, H. M., Widyawan, & Putra, G. D. (2023). A review of penetration testing frameworks, tools, and application areas. *2023 IEEE 7th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, 319–324. IEEE. https://doi.org/10.1109/ICITISEE58992.2023.10404397

Badan Siber dan Sandi Negara. (2024). *Lanskap keamanan siber Indonesia 2024*. Direktorat Operasi Keamanan Siber.

Daeng, Y., Levin, J., Prayudha, M. R., Ramadhani, N. P., & Imanuel, S. (2023). Analisis penerapan sistem keamanan siber terhadap kejahatan siber di Indonesia. *Innovative: Journal of Social Science Research, 3*(6), 1135–1145.

Darmawan, C., Naibaho, J. P. P., & Kweldju, A. D. (2024). Penerapan metode vulnerability assessment untuk identifikasi keamanan website berdasarkan OWASP ID tahun 2021. *Edumatic: Jurnal Pendidikan Informatika, 8*(1), 272–281. https://doi.org/10.29408/edumatic.v8i1.25834

Darul Fata. (2023). *Evaluasi risiko celah keamanan menggunakan metodologi Open Web Application Security Project (OWASP) pada aplikasi web Sistem Informasi Akademik (SIAKAD) UIN Ar-Raniry* [Tugas akhir, Universitas Islam Negeri Ar-Raniry].

Dawadi, B. R., Adhikari, B., & Srivastava, D. K. (2023). Deep learning technique-enabled web application firewall for the detection of web attacks. *Sensors, 23*(4), 2073. https://doi.org/10.3390/s23042073

Dharmawangsa, I., Sasmita, G., & Pratama, I. P. A. E. (2023). Penetration testing berbasis OWASP Testing Guide versi 4.2: Studi kasus X website. *JITTER: Jurnal Ilmiah Teknologi dan Komputer, 4*(1), 1613. https://doi.org/10.24843/JTRTI.2023.v04.i01.p06

Dwi Agustina, V., Ariyadi, T., Syah Putra, T., & Lega, A. (2025). Teknik pengujian penetrasi HTTP menggunakan tools Burp Suite pada Kali Linux. *STORAGE: Jurnal Ilmiah Teknik dan Ilmu Komputer, 4*(1), 16–21. https://doi.org/10.55123/storage.v4i1.4770

Handayani, I., Febriyanto, E., & Kristanti, C. Y. (2019). Peran perkembangan teknologi informasi dan komunikasi dalam pembelajaran iLearning Plus di Universitas Raharja. *Jurnal Pendidikan Teknologi dan Kejuruan, 16*(2), 181. https://doi.org/10.23887/jptk-undiksha.v16i2.17859

Herawati, N., Budiyanto, V., & Uminingsih. (2023). Analisis keamanan sebuah domain menggunakan Open Web Application Security Project (OWASP) ZAP. *Jurnal Teknologi Technoscientia, 15*(2), 27–36. https://doi.org/10.34151/technoscientia.v15i2.4013

Kongara, D., & Krishnama, S. (2023). A process of penetration testing using various tools. *Mesopotamian Journal of CyberSecurity, 2023*, 93–103. https://doi.org/10.58496/MJCS/2023/014

Lazarov, W., Seda, P., Martinasek, Z., & Kummel, R. (2025). Penterep: Comprehensive penetration testing with adaptable interactive checklists. *Computers & Security, 154*, 104399. https://doi.org/10.1016/j.cose.2025.104399

Muhammad Fauzi, R., Hermawan, R., Rosian Adhy, D., & Maesaroh, S. (2024). Analisis kerentanan keamanan web menggunakan metode OWASP dan PTES di web pemerintahan Desa XYZ. *Jurnal Orang Elektro, 13*(2), 225–231. https://doi.org/10.30591/polektro.v13i2.6711

National Cyber Security Index. (2023). *Laporan National Cyber Security Index Indonesia 2023*.

Nurelasari, E., Gumilang, D., & Farabi, A. (2024). Analisis keamanan sistem website menggunakan metode Open Web Application Security Project (OWASP) pada simantep.id. *JATI: Jurnal Mahasiswa Teknik Informatika, 8*(3), 3049–3054. https://doi.org/10.36040/jati.v8i3.9314

Prasetiyo, N. A., Huwae, R. B., & Jatmika, A. H. (2024). Audit dan analisis website pemerintah menggunakan pengujian penetrasi SQL injection dan cross-site scripting (XSS). *Jurnal Teknologi Informasi, Komputer, dan Aplikasinya, 6*(2), 525–533. https://doi.org/10.29303/jtika.v6i2.425

Supriyatna, A. R., Asrowardi, I., Putra, S. D., & Subyantoro, E. (2024). Analisis kerentanan aplikasi web e-commerce berdasarkan standar OWASP Top 10: Studi kasus pada situs Kopi Lampung Nusantara. *EXPERT: Jurnal Manajemen Sistem Informasi dan Teknologi, 14*(2), 95. https://doi.org/10.36448/expert.v14i2.4034

Wirawan, I. K., Srirahayu, A., & Sopingi, S. (2024). Rancang bangun sistem informasi keuangan sekolah berbasis website. *Jurnal Teknologi dan Sistem Informasi Bisnis, 6*(4), 639–648. https://doi.org/10.47233/jteksis.v6i4.1455

Zahra, N. A., Zidane, F. H., & Kuslaila, N. R. (2023). Analisis keamanan sistem informasi pada sistem website PT Sentra Vidya Utama (SEVIMA) menggunakan metode OWASP. *Prosiding Seminar Nasional Teknologi dan Sistem Informasi*, *3*(1), 384–393. https://doi.org/10.33005/sitasi.v3i1.564