e-ISSN 2549-7472
Edumatic: Jurnal Pendidikan Informatika
Vol. 8 No. 1, Juni, 2024, **Hal. 272-281**
DOI: 10.29408/edumatic.v8i1.25834

Penerapan Metode *Vulnerability Assessment* untuk Identifikasi Keamanan Website berdasarkan OWASP ID Tahun 2021

Candra Darmawan [1,*], Julius Panda Putra Naibaho [1], Alex De Kweldju [1]

[1] Program Studi Teknik Informatika, Universitas Papua, Indonesia
[*] Correspondence: candradarmawan43@gmail.com

Received: 30 April 2024 | Revised: 4 Mei 2024 | Accepted: 10 Mei 2024 | Published: 20 Juni 2024

Abstrak
Universitas sebagai institusi pendidikan, berpotensi menjadi target serangan siber. Hal ini menjadi masalah yang tidak terelakan, salah satunya Universitas papua (UNIPA). Tujuan penelitian ini mengetahui celah keamanan website UNIPA berdasarkan OWASP ID tahun 2021 dan menerapkan mitigasi. Jenis penelitian ini adalah penelitian kuantitatif dengan metode *Vulnerability Assessment and Penetration Testing Life Cycle* (VAPT). Metode VAPT pada penelitian ini melalui lima tahapan yaitu *scope*, *information gathering*, *vulnerability assessment*, *risk assessment*, dan *reporting*. Objek penelitian ini yaitu website UNIPA. Pengumpulan data memakai data primer, hasil *scanning* aplikasi *Zed Attack Proxy* (ZAP). Diperoleh data *alerts ID*, *alerts*, *risk*, dan OWASP ID sebagai informasi kerentanan website UNIPA. Analisis data penelitian menggunakan OWASP ID. Hasil temuan kami, kerentanan website UNIPA dipengaruhi dua faktor, kelemahan keamanan website dan kelalaian pengguna. Kerentanan dengan *alerts ID* A1, A2, A3, A4 A5, dan A6 merupakan kelompok kelemahan keamanan website. Solusinya, kerentanan perlu memanfaatkan sistem khusus seperti anti-CSRF, CSP, CDN, *Strict-Transport-Security Header*, dan pengecekan *timestamp* agar website proporsional. Sedangkan kerentanan dengan *alerts ID* A7 adalah klasifikasi kelalaian pengguna. Solusinya, pengguna wajib menggunakan *browser* versi terbaru. *Browser* dengan versi terbaru memiliki mekanisme keamanan *X-Content-Type-Options: nosniff* untuk mencegah serangan *sniffing*.

Kata kunci: universitas papua; kerentanan website; vapt; mitigasi; owasp id tahun 2021

Abstrac
Universities, as educational institutions, are potential targets of cyber attacks. This is inevitable problem, one of which the University of Papua (UNIPA). The purpose this research is to find the security gaps the UNIPA website based on OWASP ID in 2021 and implement mitigation. Type of research is quantitative research with Vulnerability Assessment and Penetration Testing Life Cycle (VAPT) method. The VAPT method in research goes through five stages, namely scope, information gathering, vulnerability assessment, risk assessment, and reporting. The object of research is UNIPA website. Data collection uses primary data, the results of scanning the Zed Attack Proxy (ZAP) application. Data obtained from alerts ID, alerts, risk, and OWASP ID as information on vulnerability of UNIPA website. Research data analysis using OWASP ID. The results our findings, the vulnerability of UNIPA website is influenced by two factors, website security weaknesses and user negligence. Vulnerabilities with alerts ID A1, A2, A3, A4 A5, and A6 are a group website security weaknesses. The solution, vulnerabilities need utilize special systems such as anti-CSRF, CSP, CDN, Strict-Transport-Security Header, and timestamp checking so that the website is proportional. Meanwhile, the vulnerability with alerts ID A7 is a classification of user negligence. The solution is users must use the latest version of the browser. Browsers with latest version have X-Content-Type-Options: nosniff security mechanism to prevent sniffing attacks.

Keywords: *university of papua; website vulnerability; vapt; mitigation; owasp id in 2021*

PENDAHULUAN

Permasalahan serangan siber lambat laun mengalami peningkatan (Damayanti & Hikmah, 2022). Id-SIRTII/CC serta badan Siber dan Sandi Negara menyampaikan, 976.429.996 total trafik anomali yang terdeteksi pada tahun 2022 (Syafaat, 2024). Universitas sebagai institusi pendidikan, berpotensi menjadi target serangan siber (Kusumaningrum et al., 2022). Salah satu titik serangannya yaitu website resmi Universitas (Kestina & Widi Nurcahyo, 2023). Website adalah gabungan *page* yang tersusun bersama domain atau subdomain khusus, yang diakses lewat jaringan internet (Romadhon et al., 2021). Salah satu pemanfaatan website yaitu mengolah data informasi terbaru kepada masyarakat (Sansena & Samsudin, 2023). Dalam lingkup Universitas, website berfungsi menyajikan sumber informasi terbaik serta media utama bagi pihak yang ingin terhubung dengan Universitas terkait. Alhasil, website resmi Universitas sering menjadi salah satu target serangan siber.

Serangan terhadap website Universitas itu beragam, tergantung titik mana yang ingin diserang. Contoh, ketika seorang peretas ingin merubah tampilan website maka dilakukan teknik *web deface* (Nuroji, 2023). Peretas juga memakai teknik *Distributed Denial of Service* (DDoS) agar website tidak bisa diakses dengan membanjiri sistem menggunakan paket yang dikirim secara konstan (Ekawijana et al., 2024). Peluang terparahnya yaitu teknik *Cross-Site Scripting* (XSS), yang dibuat dengan menyisipkan *script* berbahaya ke sistem web target (Narhudin et al., 2024). Kerentanan sistem IT adalah titik yang sering dimanfaatkan pihak tidak bertanggung jawab untuk memperoleh keuntungan pribadi (Budiman et al., 2021). Hal ini menjadi masalah yang tidak terelakan, salah satunya Universitas papua (UNIPA). UNIPA memiliki website resmi yang bertujuan memberikan informasi terbaru seputar aktivitas kampus bagi Mahasiswa/i, Dosen, pihak internal kampus, dan masyarakat umum. Namun, terdapat keluhan pada website UNIPA seperti, website sering menolak respon pengguna saat ingin diakses dan fitur website yang lambat merespon permintaan pengguna. Walaupun permasalahan ini tidak secara terus menerus terjadi dan terkesan tidak mengancam keamanan pengguna, hal ini tetap meresahkan karena mengganggu kenyamanan pengguna. Disisi lain, banyaknya informasi yang disimpan dan dikelola sebuah website, meningkatkan risiko kehilangan, kerusakan, dan kebocoran data ke pihak – pihak yang tidak berwenang (Umar et al., 2023). Pernyataan ini menimbulkan keresahan tersendiri terhadap keamanan website UNIPA. Terlebih belum ada informasi yang jelas mengenai keamanan website resmi UNIPA. Dari permasalahan tersebut, kami mencoba menganalisis lebih lanjut, terkait keamanan website UNIPA dengan menggunakan teknik *vulnerability* assessment untuk memeriksa celah kerentanannya.

Secara umum, *vulnerability assessment* diterapkan untuk mendeteksi celah keamanan pada infrastruktur jaringan, sistem operasi, dan aplikasi yang berpotensi mendapat serangan (Muhyidin et al., 2020). Teknik ini berfungsi menjaga poin *confidentiality*, *integrity*, dan *availability* sistem (Zirwan, 2022). Informasi celah keamanan yang ditemukan pada website UNIPA akan dikelompokkan berdasarkan *Open Web Application Security Project* atau OWASP versi 2021. OWASP adalah komunitas yang menciptakan sebuah metode, berisi 10 daftar kerentanan website tertinggi yang mengancam keamanan suatu website (Yudiana et al., 2021). Metode ini sangat populer diterapkan, terkhusus dalam praktik *vulnerability assessment* pada keamanan website (Rohim & Setiyani, 2023). Daftar kerentanan beserta kodenya yaitu *Broken Access Control* (A01:2021), *Cryptographic Failures* (A02:2021), *Injection* (A03:2021), *Insecure Design* (A04:2021), *Security Misconfiguration* (A05:2021), *Vulnerable and Outdated Components* (A06:2021), *Identification and Authentication* (A07:2021), *Software and Data Integrity Failures* (A08:2021), *Security Logging and Monitoring Failures* (A09:2021), dan *Server-Side Request Forgery* (A10:2021). Standar OWASP ID mengalami pembaruan secara berkala yang dilakukan oleh para ahli di bidang keamanan website (Tinambunan et al., 2024). Sehingga, pihak yang menerapkan standar ini dijamin terhindar dari

pedoman yang kadaluarsa. Maka, dengan menggunakan OWASP ID tahun 2021 pada penelitian ini, hasil identifikasi celah kerentanan website UNIPA menjadi lebih mutakhir .

Penelitian tentang penerapan *vulnerability assessment* menggunakan OWASP pernah dilakukan sebelumnya. Penelitian yang dilakukan oleh Taryana & Heryana (2023) yang melakukan *vulnerability assessment* pada website BPJS kesehatan menggunakan OWASP. Lalu, penelitian yang dilakukan oleh Riandhanu (2022) yang memanfaatkan *vulnerability assessment* untuk menganalisis keamanan website absensi menggunakan OWASP. Kemudian, penelitian yang dilakukan oleh Darwis et al. (2022) yang menerapkan *vulnerability assessment* untuk menganalisis kerentanan website renovaction menggunakan OWASP. Ketiga penelitian ini memiliki tujuan yang sama untuk mendeteksi kerentanan pada website. Namun, proses menjelaskan celah kerentanan hingga proses penentuan mitigasi tidak rinci. Maka dari itu, penelitian ini akan dilakukan pengembangan menggunakan standar *Web Application Security Consortium* (WASC) ID, dan *Common Weakness Enumeration* (CWE) ID untuk mengatasi hal tersebut. WASC ID adalah standar menangani permasalahan khusus kerentanan website. Sedangkan CWE ID adalah standar untuk menilai kelemahan dasar perangkat lunak. Kedua standar ini digunakan kami sebagai informasi pendukung selain informasi utama dari OWASP ID.

Melalui kombinasi *scanning* aplikasi ZAP yang mengikuti standar OWASP ID, informasi CWE ID, dan WASC ID membuat hasil yang diteliti lebih komprehensif. Hal ini dikarenakan, kompleksitas data yang diperoleh dalam melakukan penelitian, membuat gambaran celah kerentanan yang ditemukan semakin lebih luas. Tujuan penelitian ini mengetahui celah keamanan website UNIPA berdasarkan OWASP ID tahun 2021 dan menerapkan mitigasi. Dari tujuan tersebut, kami ingin informasi kondisi keamanan website UNIPA bisa diketahui, serta setiap titik kerentanan yang berpotensi mengancam keamanan website bisa diperbaiki secara tepat. Sehingga, pengguna dapat dengan nyaman mengakses website UNIPA.

METODE

Jenis penelitian ini adalah penelitian kuantitatif dengan metode *Vulnerability Assessment and Penetration Testing Life Cycle* (VAPT). VAPT adalah metodologi yang khusus menguji keamanan jaringan atau sistem aplikasi (Budiman et al., 2021). Tujuan metode penelitian ini agar proses identifikasi celah keamanan sampai proses perbaikan mendapatkan hasil yang maksimal dan terstruktur (Hafitzhah et al., 2023). VAPT terbentuk oleh *vulnerability assessment* sebagai tahap pengecekan celah kerentanan sistem dan *penetration testing* untuk percobaan menguji sistem (Ibrahim et al., 2022).

Metode VAPT pada penelitian ini melalui lima tahapan yaitu *scope*, *information gathering*, *vulnerability assessment*, *risk assessment*, dan *reporting*. Tahap *scope* dilakukan untuk menentukan objek penelitian. Objek penelitian ini yaitu website UNIPA. Selanjutnya, tahap *information gathering* untuk mencari informasi tentang objek penelitian yang sudah ditentukan pada tahap *scope*. Pengumpulan data memakai data primer, hasil *scanning* aplikasi *Zed Attack Proxy* (ZAP). Diperoleh data alerts ID, alerts, risk, dan OWASP ID sebagai informasi kerentanan website UNIPA. Lalu, dilanjutkan pada tahap *vulnerability assessment* untuk menentukan celah kerentanan objek penelitian. kemudian, celah kerentanan akan dianalisis pada tahap *risk assessment* untuk memahami potensi dampak yang ditimbulkan berdasarkan hasil informasi WASC ID, CWE ID, dan OWASP ID. Analisis data penelitian menggunakan OWASP ID. Terakhir tahap *reporting*, kami mendokumentasikan setiap temuan yang diperoleh pada tahap sebelumnya, untuk menentukan solusi pada setiap kerentanan dengan baik.

HASIL DAN PEMBAHASAN

Hasil

Terdapat tujuh kerentanan yang diberikan ID A1 – A7. Kerentanan dengan ID A1 merupakan kelemahan sistem autentikasi yang membuat akses pengguna mudah diambil alih. selanjutnya, kerentanan dengan ID A2 merupakan Kelemahan pada *Control Security Policy* (CSP) membuat website rentan dimasukkan *script* berbahaya. Kemudian, kerentanan dengan ID A3 adalah Kelemahan pada konfigurasi *header X-Frame-Options* sehingga website utama mudah disematkan iframe berbahaya. Berikutnya, kerentanan dengan ID A4 adalah kelemahan pada sistem yang tidak bisa memvalidasi file *JavaScript* domain lain. Lalu, kerentanan dengan ID A5 adalah kelemahan pada *Strict-Transport-Security Header* sehingga koneksi pengguna dan website mudah terkena penyadapan. Kemudian, kerentanan dengan ID A6 merupakan kelemahan website atau server web yang menyebarkan informasi sensitif pengguna seperti waktu login, pola aktivitas, dan waktu pembuatan akun. Terakhir, kerentanan dengan ID A7 merupakan kelemahan saat browser melakukan MIME sniffing atau menebak jenis format file dari server web yang dapat dilihat hasilnya pada tabel 1.

Tabel 1. Hasil scanning website unipa

Alerts ID	***Alerts***	***Risk***	**OWASP ID**
A1	*Absence of Anti-CSRF Tokens*	*Medium*	A01:2021
A2	*Content Security Policy* (CSP) *Header Not Set*	*Medium*	A05:2021
A3	*Missing Anti-clickjacking Header*	*Medium*	A05:2021
A4	*Cross-Domain JavaScript Source File Inclusion*	*Low*	A08:2021
A5	*Strict-Transport-Security Header Not Set*	*Low*	A05:2021
A6	*Timestamp Disclosure – Unix*	*Low*	A01:2021
A7	*X-Content-Type-Options Header Missing*	*Low*	A05:2021

Tabel 2. Informasi cwe id pada website unipa

Alerts ID	**CWE ID**	**Informasi CWE ID**
A1	352	kerentanan yang dimanfaatkan penyerang untuk membohongi pengguna dengan memanfaatkan cookie sesi.
A2	693	Kerentanan yang terjadi saat perlindungan autentikasi, otorisasi, dan enkripsi tidak dibuat dengan benar.
A3	1021	Kerentanan yang dimanfaatkan penyerang untuk menipu pengguna di aplikasi website dengan mekanisme yang lebih banyak, salah satunya serangan *clickjacking*.
A4	829	Kerentanan yang terjadi ketika aplikasi website mengakses kode dari sumber yang tidak terpercaya.
A5	319	Kerentanan yang terjadi saat aplikasi website tidak bisa memvalidasi input pengguna dengan baik dan benar.
A6	200	Kerentanan yang terjadi ketika informasi sensitif pengguna diketahui dengan leluasa oleh pihak lain secara ilegal.
A7	693	Kerentanan yang terjadi saat perlindungan autentikasi, otorisasi, dan enkripsi tidak dibuat dengan benar.

Hasil selanjutnya mencari informasi CWE ID dan WASC ID pada kerentanan. Keterkaitan antara informasi CWE ID dan WASC ID adalah melakukan identifikasi kerentanan keamanan.

Informasi celah kerentanan CWE ID dapat dilihat pada tabel 2 dan informasi celah kerentanan WASC ID yang dapat dilihat pada tabel 3.

Tabel 3. Informasi wasc id pada website unipa

Alerts ID	WASC ID	Informasi WASC ID
A1	9	Celah kerentanan yang timbul karena aplikasi website tidak mampu memvalidasi inputan dengan baik dan benar.
A2	15	Celah kerentanan yang terjadi ketika aplikasi website tidak bisa mentransmisikan data sensitif pengguna dengan enkripsi yang baik
A3	15	Celah kerentanan yang terjadi ketika aplikasi website tidak bisa mentransmisikan data sensitif pengguna dengan enkripsi yang baik
A4	15	Celah kerentanan yang terjadi ketika aplikasi website tidak bisa mentransmisikan data sensitif pengguna dengan enkripsi yang baik
A5	15	Celah kerentanan yang terjadi ketika aplikasi website tidak bisa mentransmisikan data sensitif pengguna dengan enkripsi yang baik
A6	13	Celah kerentanan yang muncul saat aplikasi website tidak menerapkan kontrol akses yang baik.
A7	15	Celah kerentanan yang terjadi ketika aplikasi website tidak bisa mentransmisikan data sensitif pengguna dengan enkripsi yang baik

Berdasarkan hasil tabel 2, terdapat titik kerentanan yang beragam. Kerentanan tersebut menginformasikan, jika website UNIPA rentan terhadap serangan XSS, injeksi data, dan kebocoran data sensitif menurut sudut pandang kelemahan perangkat lunak. Untuk tabel 3, kerentanan diklasifikasi menjadi tiga titik kerentanan. kerentanan memberi informasi kalau, website UNIPA rawan terhadap serangan yang mengincar sistem autentikasi, injeksi XML, dan kebocoran data sensitif pengguna ketika diperhatikan melalui sudut pandang kelemahan website secara spesifik. Setelah memperoleh informasi CWE ID dan WASC ID, dilakukan tahap mendefinisikan celah kerentanan pada website UNIPA yang disajikan pada tabel 4. Poin tahap ini yaitu, mendeskripsikan celah kerentanan dan kemungkinan serangan – serangan yang terjadi. Hasil pada tahap ini merupakan kombinasi dari informasi OWASP ID, CWE ID, dan WASC ID melalui proses *scanning* aplikasi ZAP.

Tabel 4 menjelaskan, kerentanan timbul dari dua titik yaitu kelemahan konfigurasi keamanan website UNIPA dan kekeliruan pengguna saat memanfaatkan *browser* yang sesuai. Sehingga, perlu dilakukan penanganan lebih lanjut. Untuk itu, dilakukan tahap terakhir yaitu mitigasi. Proses ini bertujuan melindungi website dan pengguna, dari segala bentuk risiko ancaman keamanan berdasarkan informasi celah kerentanan yang diperoleh pada tahap sebelumnya yaitu tabel 4.

Sementara itu, hasil pada tabel 5 menunjukkan, perlindungan terhadap website UNIPA perlu dilakukan perbaikan konfigurasi keamanan website dan pengguna wajib memastikan *browser* yang digunakan sesuai. Ketika website diperbaiki dan pengguna memanfaatkan *browser* yang tepat sesuai rekomendasi yang disajikan pada tabel 5, diharapkan keamanan website dan pengguna bisa terjaga dengan baik.

Tabel 4. Informasi celah kerentanan pada website unipa

Alerts ID	**Informasi Celah Kerentanan**
A1	Sistem anti-CSRF pada website UNIPA belum difungsikan dengan optimal, sehingga rentan mengalami serangan CSRF atau *Cross-Site Request Forgery*. Serangan ini memanfaatkan kepercayaan pengguna terhadap website untuk melakukan tindakan-tindakan yang tanpa disadari, mengancam keamanan pribadinya. Inti dari penyerang memanfaatkan celah keamanan ini untuk mengambil akses penuh pengguna untuk tujuan tertentu. Website UNIPA diidentifikasi memiliki celah ini, sehingga potensi hak akses pengguna untuk dieksploitasi itu ada.
A2	Penerapan CSP atau *Content Security Policy* website UNIPA belum baik membuat peluang website dimasukkan *script* berbahaya oleh penyerang semakin besar. Serangan keamanan yang berpotensi pada website UNIPA berdasarkan celah kerentanan ini, yaitu *Cross Site Scripting* (XSS), *malware*, dan injeksi data.
A3	Sistem *header X-Frame-Options* pada website UNIPA belum difungsikan dengan benar. Alhasil, muncul iframe atau *in-line-frame* elemen HTML yang menyisipkan konten website eksternal ke halaman website utama yang tidak bisa tervalidasi keamanannya. kerugian bagi penguna apabila mengakses iframe yang salah dan mengakibatkan kerugian seperti pencurian data dan pengambilan hak akses penuh pengguna.
A4	Website UNIPA belum mampu menjamin keamanan akses file *JavaScript* dari domain lain. Informasi pada website UNIPA tidak dihosting servernya sendiri, melainkan ada juga dari domain lain. Namun, informasi dari domain tersebut yang tampil di halaman website utama, keamanannya belum terjamin karena belum adanya sistem yang cocok untuk mengatasinya. Sehingga, keamanan dari pengguna yang mengakses website bisa terancam seperti pelacakan pengguna sampai pengambilan hak akses akun.
A5	Website UNIPA belum mengaktifkan *Strict-Transport-Security Header* sebagai mekanisme keamanan server website, untuk mendorong *browser* menggunakan koneksi HTTPS yang aman. Komunikasi antara pengguna dan website terdapat celah yang dimanfaatkan penyerang untuk penyadapan. Celah pada website UNIPA ini berpotensi terkena serangan MITM atau *Man-in-the-Middle*.
A6	Website UNIPA memiliki peluang terkena serangan *timming attack* dan *replay attack*. *Timming attack* dimanfaakan penyerang untuk menghitung waktu yang dilakukan website untuk mengoperasikan perintah tertentu. Setelah itu, dilanjutkan dengan *reply attack* untuk mengganggu interaksi antara pengguna dan website melalui serangan MITM atau XSS.
A7	kerentanan ini timbul saat pengguna memakai perantara *browser* yang versinya lama. *Browser* dengan versi terbaru umumnya dilengkapi fitur *X-Content-Type-Options: nosniff* yang tidak dimiliki *browser* versi lama. Kerentanan ini sangat jarang terjadi sebab, umumnya dari kesalahan pengguna karena ketidakpahaman penguna terhadap versi *browser*.

Tabel 5. Informasi mitigasi celah kerentanan pada website unipa

Alerts ID	**Informasi Mitigasi Celah Kerentanan**
A1	Website UNIPA perlu menjalankan fitur anti-CSRF dengan penerapan kontrol ESAPI. Kontrol ini bertujuan memvalidasi setiap inputan pengguna saat mengakses website secara *real time*. Dengan begitu, diharapkan fitur – fitur website UNIPA yang dimanfaatkan pengguna, bebas dari ancaman dan kepercayaan pengguna pada website turut meningkat dan stabil.
A2	Menerapkan CSP, agar membatasi izin sumber daya berupa *script*, gambar, font, dan lainnya untuk ditampilkan pada halaman website UNIPA. proteksi ini diharapkan mampu meminimalisir serangan XSS, *malware*, dan injeksi data. Hasilnya, pengguna bisa mengakses seluruh informasi baik itu informasi utama maupun tambahan yang ditampilkan pada website UNIPA dengan aman dan nyaman.
A3	Website UNIPA perlu menjalankan fitur *header X-Frame-Options* dengan benar. Karena, fitur tersebut membantu website UNIPA untuk memfilter iframe yang layak tampil di halaman website utama. Jika terdapat intensi mencurigakan dari iframe, maka sistem *header X-Frame-Options secara* otomatis akan menolak iframe tersebut untuk ditampilkan. Fitur ini juga berfungsi melindungi pengguna dari serangan *clickjacking*.
A4	Website UNIPA perlu memperhatikan konfigurasi *Content Security Policy* (CSP), *Content Delivery Network* (CDN), dan *Strict Transport Security Header*. CSP bertugas melindungi informasi baik itu *script*, gambar, video, iframe dan sejenisnya untuk ditampilkan pada halaman web. Kontrol CDN memastikan server website UNIPA berjalan dengan aman. Dan *Strict Transport Security Header* mengupayakan website selalu memakai koneksi HTTPS. Tiga kontrol ini menjamin peningkatan performa dan keamanan website UNIPA sekaligus pengguna dapat merasa aman saat mengaksesnya.
A5	Menerapkan *Strict-Transport-Security Header* pada website UNIPA dengan benar. Kontrol ini penting agar mendorong koneksi website selalu menggunakan HTTPS. Dengan begitu, komunikasi antara pengguna dan website, dalam hal ini website UNIPA itu terenksripsi dengan sempurna. Sehingga, mencegah upaya penyadapan atau kebocoran data, sebab segala informasi yang terjadi berada dalam bentuk yang tidak bisa dibaca manusia (enkripsi).
A6	Dilakukan tahap pengecekan *timestamp* pada website UNIPA secara manual oleh pengelola website. Hal ini untuk memastikan akurasi dan keabsahan data *timestamp* pada sistem website sekaligus mencegah serangan *reply attack* pada website UNIPA. manfaat dari proses ini, kepercayaan penggun untuk mengadopsi website UNIPA semakin meningkat.
A7	Bisa diberikan notifikasi khusus diawal akses, berupa panduan penggunaan website UNIPA. Panduan menginformasikan spesifikasi pemilihan *browser* yang wajib digunakan ketika mengakses website UNIPA. Detail yang bisa dijelaskan terkait versi *browser,* lengkap dengan contoh versi *browser* yang kompatibel dan tidak. Dengan begitu, pengguna bisa mengakses website UNIPA dengan aman dan nyaman.

Pembahasan

Hasil temuan kami adalah terdapat tujuh kerentanan pada website resmi UNIPA. Tujuh kerentanan ini memiliki identitas khusus atau ID berupa A1 – A7. Setiap kerentanan memiliki tingkat risiko dan titik kerentanan yang berbeda. Berdasarkan tingkat risiko sesuai informasi

tabel 1, kerentanan dengan ID A1 – A3 memiliki risiko dengan level *medium* atau sedang, sedangkan ID A4 – A7 memiliki risiko dengan level *low* atau rendah. Untuk titik kerentanan, patokan penilainnya melalui OWASP ID. Jika dilihat berdasarkan informasi tabel 1, tujuh kerentanan ini bila disesuaikan menurut standar OWASP ID, terdiri dari tiga kelompok. Pertama, kerentanan dengan ID A1 dan A6 masuk dalam kategori OWASP ID A01:2021 atau *Broken Access Control*. Artinya, kerentanan yang masuk dalam kelompok ini, memiliki titik kerentanan terhadap rusaknya penerapan kontrol akses antara pengguna dan sumber daya. Kedua, kerentanan dengan ID A2, A3, A5, dan A7 tergolong kategori OWASP ID A05:2021 atau *Security Misconfiguration*. Artinya, kerentanan untuk kelompok ini memiliki titik kerentanan pada lemahnya pengaturan keamanan dari sisi konfigurasi perangkat lunak, sistem, dan jaringan. Ketiga, kerentanan dengan ID A4 untuk kategori OWASP ID A08:2021 yaitu *Software and Data Integrity Failures*. Artinya, kerentanan pada kategori ini mempunyai titik kerentanan terhadap integritas perangkat lunak beserta pengembangannya yang tidak terjaga membuat potensi untuk disalahgunakannya data penting pengguna oleh pihak tidak bertanggung jawab semakin tinggi. Kami juga mencari informasi CWE ID dan WASC ID. Hasil secara lengkap bisa dilihat pada tabel 2 untuk informasi CWE ID dan tabel 3 untuk informasi WASC ID. Dari sisi CWE ID, setiap celah kerentanan memiliki kode CWE ID yang berbeda, kecuali kerentanan A2 dan A7. Berarti dari sudut pandang kelemahan perangkat lunak secara umum, hampir semua celah kerentanan memiliki titik serangan yang berbeda kecuali kerentanan dengan ID A2 dan A7. Sedangkan untuk WASC ID, semua celah kerentanan terbagi dalam tiga kode WASC ID yang berlainan. Maka dari sudut pandang kelemahan website, celah kerentanan yang ditemukan hanya memiliki tiga titik serangan yang beragam. Solusi yang cocok untuk kerentanan CWE ID dan WASC ID relatif sama, yaitu melakukan konfirmasi identitas pengguna yang sesuai, membangun kontrol akses yang baik untuk pengguna, menciptakan enkripsi sistem yang kuat, dan memvalidasi input pengguna dengan baik.

Proses selanjutnya yang dilakukan kami yaitu menetapkan definisi setiap celah kerentanan sekaligus menentukan mitigasi kerentanan. Hasil lengkapnya tertera pada tabel 4 untuk definisi celah kerentanan dan tabel 5 untuk tahap mitigasi kerentanan. Kami menemukan, kerentanan website UNIPA dipengaruhi dua faktor, kelemahan keamanan website dan kelalaian pengguna. Kerentanan dengan *alerts ID* A1, A2, A3, A4, A5, dan A6 merupakan kelompok kelemahan keamanan website. Solusinya, kerentanan perlu memanfaatkan sistem khusus seperti anti-CSRF, CSP, CDN, *Strict-Transport-Security Header*, dan pengecekan *timestamp* agar website proporsional. sedangkan kerentanan dengan *alerts ID* A7 adalah klasifikasi kelalaian pengguna. Solusinya, pengguna wajib menggunakan *browser* versi terbaru. *Browser* dengan versi terbaru memiliki mekanisme keamanan *X-Content-Type-Options: nosniff* untuk mencegah serangan *sniffing*. Sistem ini bekerja dengan mengatur *browser* untuk menggunakan jenis file yang sesuai dengan *header content-type. Header content-type* difungsikan memberikan tanda untuk informasi pada *browser* mengenai jenis file yang dikirimkan dari server. Jika menggunakan *browser* versi lama yang tidak menerapkan sistem *X-Content-Type-Options: nosniff*, pengguna rentan terhadap serangan *sniffing* yang mengancam keamanan informasi pribadi pengguna. Masalah kerentanan ini tidak muncul dari sisi kelemahan website, melainkan kesalahan pengguna dalam pemilihan *browser.*

Hasil temuan kami menciptakan jawaban komprehensif dari kolaborasi informasi OWASP ID, WASC ID, dan CWE ID. Berbeda dengan penelitian yang dilakukan oleh (Taryana & Heryana, 2023) yang melakukan tahap analisis pada website BPJS kesehatan menggunakan OWASP ID, penelitian oleh (Riandhanu, 2022) yang menerapkan *vulnerability assessment* untuk analisis keamanan website absensi memakai OWASP ID, dan penelitian oleh Darwis et al. (2022) yang memanfaatkan *vulnerability assessment* dalam analisis website renovation menggunakan OWASP ID. Tiga penelitian ini hanya berlandaskan pada satu informasi utama yaitu OWASP ID. Sehingga hasil kurang komprehensif. Masalah lainnya

adalah kesulitan memahami hasil analisisnya, karena hanya menggunakan satu sudut pandang. Berbeda dengan temuan pada penelitian ini, yang mendeskripsikan setiap celah kerentanan website UNIPA melalui lebih dari satu perspektif. Metode yang digunakan pada penelitian ini juga lebih unggul karena, proses identifikasi hingga perbaikan kerentanan disusun secara bertahap dan teratur. Poin yang tidak kalah penting juga, sudut pandang yang digunakan melalui standar resmi komunitas keamanan siber. Maka, hasil penelitian menjadi informasi untuk menggambarkan kondisi keamanan website UNIPA sekaligus menerapkan mitigasi yang sesuai. Solusi bagi pihak Universitas Papua, perlu melakukan pemeliharaan website secara rutin, melakukan simulasi serangan terhadap website, dan menyewa jasa konsultan keamanan siber. Diharapkan membantu meningkatkan kualitas keamanan website dan meminimalisir timbulnya kerentanan pada website.

SIMPULAN

Hasil temuan kami menggunakan metode *vulnerability assessment* menunjukkan, berdasarkan OWASP ID tahun 2021, mayoritas celah kerentanan adalah A05:2021 yaitu *Security Misconfiguration* serta paling sedikit A01:2021 yaitu *Broken Access Control* dan A08:2021 yaitu *Software and Data Integrity Failures*. Hasil membuktikan, konfigurasi sistem dan pengaturan keamanan website UNIPA masih belum baik. Perlu dilakukan penanganan serius pada titik ini. Disisi lain, penerapan kontrol akses serta sistem integritas data dan perangkat lunak website UNIPA dinilai cukup baik. sehingga ancaman pada titik ini lebih sedikit namun, perlu ditangani lebih lanjut. Intensi kerentanan tidak hanya diakibatkan dari sisi kerentanan website, melainkan dari sisi pengguna saat menggunakan *browser* yang tidak layak. Parameter kelayakan website, ditentukan oleh kebaruan versi *browser* yang dimanfaatkan pengguna, sehingga pemilihan *browser* menjadi hal yang penting.

REFERENSI

Budiman, A., Ahdan, S., & Aziz, M. (2021). Analisis Celah Keamanan Aplikasi Web E-Learning Universitas Abc Dengan Vulnerability Assesment. *Jurnal Komputasi*, *9*(2), 1–10.

Damayanti, T. H., & Hikmah, I. R. (2022). Network Forensic Serangan DoS pada Jaringan Cloud berdasarkan Generic Framework for Network Forensics (GFNF). *Edumatic: Jurnal Pendidikan Informatika*, *6*(2), 334–343. https://doi.org/10.29408/edumatic.v6i2.6466

Darwis, E., Junaedy, & Musdar, I. A. (2022). Analisis Kerentanan Website Renovaction Menggunakan Rangkaian Security Tools Project Berdasarkan Framework Owasp. *KHARISMA Tech*, *17*(1), 1–15. https://doi.org/10.55645/kharismatech.v17i1.170

Ekawijana, A., Bakhrun, A., & Kurniawan, M. . (2024). Deteksi Serangan DDOS Pada Jaringan SDN dengan Metode Random. *Jurnal Media Informatika Budidarma*, *8*, 685–694.

Hafitzhah, Y., Yunan, U., Septo, K., & Fathinuddin, M. (2023). Strategi Security Mitigation Dengan VAPT Pada Website Rekruitasi Asisten Praktikum. *Jurnal Riset Sistem Informasi Dan Teknik Informatika*, *8*, 627–639.

Ibrahim, A. M., Defisa, T., & Seta, H. B. (2022, October). Analisis Keamanan Sistem pada Website Perusahaan CV. Kazar Teknologi Indonesia dengan Metode Vulnerability Assesment and Penetration Testing (VAPT). *Prosiding Seminar Nasional Mahasiswa Bidang Ilmu Komputer dan Aplikasinya*, *3*(1), 312-325.

Kestina, L., & Widi Nurcahyo, G. (2023). Penanganan Celah Keamanan Website dengan Ethical Hacking dan Issaf Menggunakan Acunetix Vulnerability (Studi Kasus di Bkpsdmd Kabupaten Kerinci). *INNOVATIVE: Journal Of Social Science Research*, *3*(4), 9192–9203.

Kusumaningrum, A., Wijayanto, H., & Raharja, B. D. (2022). Pengukuran Tingkat Kesadaran Keamanan Siber di Kalangan Mahasiswa saat Study From Home dengan Multiple Criteria Decision Analysis (MCDA). *Jurnal Ilmiah SINUS*, *20*(1), 69. https://doi.org/10.30646/sinus.v20i1.586

Muhyidin, Y., Hafid Totohendarto, M., Undamayanti, E., & Tinggi Teknologi Wastukancana, S. (2020). Perbandingan Tingkat Keamanan Website Menggunakan Nmap Dan Nikto Dengan Metode Ethical Hacking. *Jurnal Teknologika*, 1–10.

Narhudin, D. E., Irawan, B., & Bahtiar, A. (2024). Evaluasi Keamanan Website Menggunakan Metode OWASP : Penilaian Terhadap Serangan Injeksi SQL dan Cross-Site Scripting (XSS). *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(1), 675–680. https://doi.org/10.36040/jati.v8i1.8700

Nuroji. (2023). Penerapan Intrusion Detection and Prevention System (IDPS) pada Jaringan komputer sebagai pencegahan serangan Port-Scanning. *Journal of Data Science and Information System (DIMIS)*, *1*(2), 41–49.

Riandhanu, I. O. (2022). Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi. *Jurnal Informasi Dan Teknologi*, *4*(3), 160–165. https://doi.org/10.37034/jidt.v4i3.236

Rohim, A., & Setiyani, L. (2023). Analisis Celah Keamanan E-LearningPerguruan Tinggi Menggunakan Vulnerability Assessment. *Jipakif*, *1*(1), 1–10. https://doi.org/10.24014/rmsi.v9i1.21823

Romadhon, M. H., Yudhistira, Y., & Mukrodin, M. (2021). Sistem Informasi Rental Mobil Berbsasis Android Dan Website Menggunakan Framework Codeigniter 3 Studi Kasus : CV Kopja Mandiri. *Jurnal Sistem Informasi Dan Teknologi Peradaban (JSITP)*, *2*(1), 30–36.

Sansena, Y., & Samsudin, S. (2023). Aplikasi Perhitungan Penyusutan Inventaris Barang menggunakan Decreasing Charge Method Berbasis Website. *Edumatic: Jurnal Pendidikan Informatika*, *7*(1), 169–177. https://doi.org/10.29408/edumatic.v7i1.17572

Syafaat, A. (2024). Identifikasi Kerentanan Keamanan pada Website Fakultas Ilmu Komputer Universitas SUBANG Menggunakan Metodologi OWASP. *Jurnal Ilmiah Fakultas Ilmu Komputer Universitas Subang*, *11*(1), 84–99.

Taryana, Y., & Heryana, N. (2023). Analisis Keamanan Website BPJS Kesehatan Menggunakan Metode Vulnerability Asesement. *Joutica*, *8*(1), 31–37. https://doi.org/10.24014/rmsi.v9i1.21823

Tinambunan, F., Junaidi, A., & Mustika Rizki, A. (2024). Pengujian Sistem Informasi Akademik Universitas X Melalui Pendekatan Penetration Testing Berdasarkan Owasp Top 10. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(1), 1062–1069. https://doi.org/10.36040/jati.v8i1.8920

Umar, R., Riadi, I., Ihya, M., & Elfatiha, A. (2023). Analisis Keamanan Sistem Informasi Akademik Berbasis Web Menggunakan Framework ISSAF. *Jutisi: Jurnal Ilmiah Teknik Informatika Dan Sistem Informasi*, *12*(1), 280–292.

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), 37-43. https://doi.org/10.24114/cess.v6i2.24777

Zirwan, A. (2022). Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner. *Jurnal Informasi Dan Teknologi*, *4*(1), 70–75. https://doi.org/10.37034/jidt.v4i1.190