ANALISIS KERENTANAN WEBSITE DI LINGKUNGAN UNIVERSITAS MATARAM MENGGUNAKAN OWASP ZAP

(Vulnerability Assessment Of Websites In The Environment Of Mataram University Using OWASP ZAP)

Lalu Fathir Ayodya Rahman[1], Ahmad Zafrullah M. [1], Ariyan Zubaidi [1]
[1]Dept Informatics Engineering, Mataram University
Jl. Majapahit 62, Mataram, Lombok NTB, INDONESIA
Email: lalufathir10@gmail.com@gmail.com, [zaf, zubaidi13]@unram.ac.id

Currently, websites have become an integral component in various sectors of life, including business, entertainment, and education. Universitas Mataram (UNRAM), as one of the leading universities in the West Nusa Tenggara Province, utilizes a website as the main platform to convey information related to university programs and activities. However, with the rapid development of information technology, the vulnerability level to website security within the UNRAM environment has also increased. This research specifically focuses on vulnerability analysis on several subdomains within the UNRAM environment using the Open Web Application Security Project (OWASP) method. The analytical approach involves scanning subdomains using OWASP ZAP, identifying security vulnerabilities, and providing recommendations for corrective actions in accordance with the OWASP vulnerability list. The research results indicate that out of a total of 108 identified vulnerabilities across all tested subdomains, only 50,92% can be classified as valid vulnerabilities after the verification process. Each subdomain, such as SIA, SPI, FEB, FT, and PSTI, has different vulnerability levels, with verified vulnerability percentages of 71.43%, 45.45%, 75%, 77.78%, and 56.25%, respectively. Improvement recommendations include implementing Anti-CSRF tokens, SameSite attributes on cookies, proper server configuration, component updates such as Bootstrap, jQuery, and Chart.js, and enhancing cryptographic security measures.

***Keywords**: Website Security, Information Systems, Vulnerability Analysis, OWASP Zap, OWASP Top 10-2021, Universitas Mataram.*

1. PENDAHULUAN

Website atau web adalah kumpulan halaman web yang saling terhubung dan dapat diakses melalui browser saat terhubung dengan jaringan internet. Terdapat tiga kategori website, yaitu web statis, web dinamis, dan web interaktif. Web statis memiliki konten tetap, sementara web dinamis dapat berubah sesuai interaksi pengguna, dan web interaktif memungkinkan interaksi aktif antara pengguna dan website[1][2]. Website memiliki peran penting dalam berbagai bidang, seperti bisnis, pendidikan, dan hiburan. Dalam dunia bisnis, website dapat memungkinkan suatu perusahaan untuk memperluas jangkauan pasar. Dalam dunia pendidikan, website dapat digunakan sebagai platform pembelajaran online, di mana siswa dapat mengakses materi, mengumpulkan tugas, berinteraksi dengan guru, dan berpartisipasi dalam diskusi. Dan dalam bidang hiburan, user dapat dengan mudah mengakses dan menikmati berbagai jenis konten hiburan, seperti streaming film, mendengarkan musik secara online, bermain game online, dan informasi tentang acara hiburan yang sedang berlangsung[3]. Namun, seiring dengan perkembangan teknologi informasi yang pesat, kerentanan terhadap keamanan website dan sistem informasi juga mengalami peningkatan yang signifikan, yang dimana kerentanan tersebut dapat memberikan peluang kepada orang yang tidak bertanggung jawab untuk merusak sistem.

Kerentanan web adalah celah atau kelemahan dalam sistem atau aplikasi web yang dapat dimanfaatkan oleh seorang peretas untuk melakukan aksi yang merugikan seperti pencurian data penting, kerusakan sistem yang menghambat operasional, atau penyalahgunaan informasi yang berdampak pada reputasi dan kepercayaan publik[4]. Contoh kasus peretasan yang terjadi pada tahun 2022 oleh seorang hacker yang mengaku sebagai Bjorka, dimana ia berhasil melakukan peretasan terhadap web kementerian yang ada di Indonesia dan mendapatkan 1,3 miliar data *card* ponsel[5]. Dan kasus peretasan lain yang baru-baru ini terjadi adalah, kasus peretasan yang terjadi terhadap web layanan Bank BSI. Peretasan terhadap layanan bank syariah terbesar di Indonesia tersebut dilangsungkan menggunakan ransomware dan jumlah data yang dicuri pada sistem tersebut diklaim sebanyak 1,5 terabyte, termasuk 15 juta data pribadi nasabah dan karyawan[6]. Dengan adanya kejadian tersebut, keamanan web menjadi aspek yang sangat krusial karena serangan terhadap website dan sistem informasi dapat mengakibatkan kerugian. Melalui pemahaman yang mendalam tentang kerentanan web, suatu instansi dapat meningkatkan

keamanan sistem web mereka dan melindungi data serta sistem dari serangan yang berpotensi merugikan[7].

Universitas Mataram (UNRAM) merupakan salah satu perguruan tinggi di Indonesia yang telah mengembangkan website resmi untuk memberikan informasi terkait program dan kegiatan yang dilakukan oleh universitas. UNRAM memiliki subdomain yang berfungsi untuk mempermudah akses ke informasi yang lebih spesifik dan terkait dengan fakultas-fakultas atau unit-unit di dalam universitas. Namun, seperti halnya website pada umumnya, website di lingkungan UNRAM juga rentan terhadap celah keamanan. Hal ini terbukti melalui kasus peretasan yang terjadi pada web Manajemen Sistem Informasi Akademik (SIA) UNRAM pada bulan Februari 2018. Peretasan tersebut dilakukan oleh seseorang yang mengaku sebagai Hacker Loteng dan berhasil melakukan serangan Remote Code Execution (RCE) melalui unggahan berkas (file upload). Tindakan ini memungkinkan peretas untuk mengambil kendali server UNRAM dari jarak jauh[8]. Dalam kasus tersebut, Remote Code Execution (RCE) digunakan untuk menjalankan kode secara jarak jauh pada sistem atau server yang rentan. Peretas tersebut kemungkinan memanfaatkan kerentanan atau celah keamanan pada web SIA UNRAM untuk mengubah informasi, mencuri data, atau melancarkan serangan lainnya. Dan pada saat peretasan dilakukan, hanya ada dua petugas yang bertugas menjaga server. Kasus ini menunjukkan pentingnya menjaga keamanan web di lingkungan UNRAM agar terhindar dari akses yang tidak sah dan melindungi data serta sistem dari serangan peretas. Oleh karena itu, analisis kerentanan terhadap website dan sistem informasi di lingkungan UNRAM menjadi hal yang sangat penting untuk diberlakukan guna mengidentifikasi dan mengatasi potensi kelemahan keamanan.

Analisis kerentanan atau vulnerability assessment adalah sebuah proses yang sangat penting dalam pengelolaan keamanan informasi. Tujuannya adalah untuk mengidentifikasi serta melakukan evaluasi celah keamanan pada sistem atau jaringan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab[9]. Proses analisis kerentanan melibatkan penggunaan berbagai teknik dan alat untuk melakukan identifikasi celah keamanan yang ada, seperti kelemahan pada konfigurasi sistem, cacat pada perangkat lunak, serta kerentanan pada jaringan dan protokol yang digunakan. Proses ini juga dapat membantu mengevaluasi efektivitas dari tindakan mitigasi yang telah dilakukan untuk mengurangi resiko keamanan pada sistem atau jaringan. Dengan melakukan analisis celah pada suatu sistem atau jaringan, suatu organisasi dapat memastikan bahwa sistem atau jaringan yang digunakan tetap aman dari berbagai macam ancaman keamanan yang semakin beragam[10]. Salah satu metode yang dapat digunakan untuk melakukan analisis kerentanan adalah dengan memanfaatkan tool OWASP ZAP.

OWASP ZAP (Open Web Application Security Project Zed Attack Proxy) merupakan tool analisis keamanan web bersifat open-source yang dikembangkan oleh organisasi OWASP[11]. Salah satu alasan utama memanfaatkan alat ini adalah, pada penelitian yang dilakukan oleh Samir Kumar Paudel dengan jurnal penelitiannya yang berjudul "Vulnerable Web Applications and How to Audit Them" yang dimana ia melakukan pengujian efektivitas OWASP ZAP dalam menemukan kerentanan pada sebuah aplikasi web. Setelah melakukan pengujian dan mendapatkan hasilnya, ia menyimpulkan bahwa OWASP ZAP terbukti efektif dalam menemukan kerentanan pada aplikasi sampel[12]. Penggunaan alat ini dapat membantu mempercepat proses analisis dan dapat mengidentifikasi serangan pada website. Selain itu, alat ini mudah digunakan, sehingga pemula tidak akan menemukan banyak kendala saat melakukan pemindaian pada suatu website[13].

Penggunaan OWASP ZAP untuk melakukan analisis kerentanan pada subdomain di lingkungan Universitas Mataram dianggap penting dan diperlukan mengingat semakin kompleksnya ancaman keamanan yang dapat membahayakan sistem informasi universitas. Dalam konteks ini, penggunaan OWASP ZAP sebagai alat bantu dalam melakukan analisis kerentanan pada subdomain diharapkan dapat membantu meningkatkan keamanan sistem informasi universitas dan mengurangi potensi resiko keamanan yang mungkin terjadi. OWASP ZAP juga dipilih karena telah diakui sebagai salah satu tool yang cukup efektif dan dapat diandalkan dalam melakukan analisis kerentanan pada website, termasuk pada subdomain. Oleh karena itu, penggunaan OWASP ZAP di lingkungan Universitas Mataram dapat menjadi alternatif untuk mengidentifikasi celah keamanan pada subdomain website.

Berdasarkan hal tersebut, penelitian ini akan berfokus pada analisis kerentanan beberapa subdomain website di lingkungan Universitas Mataram menggunakan OWASP ZAP. Dalam penelitian ini, akan diidentifikasi subdomain website yang terdapat di lingkungan Universitas Mataram, dilakukan analisis kerentanan keamanan pada subdomain website menggunakan OWASP ZAP, dan memberikan rekomendasi tindakan untuk meminimalisir resiko keamanan pada subdomain website.

2. TINJAUAN PUSTAKA

Dalam penelitian [11] dengan judul "Security Audit for Vulnerability Detection and Mitigation of UPT Integrated Laboratory (ILab) ITERA Website Based on OWASP Zed Attack Proxy (ZAP)" oleh Ilham Firman Ashari dan rekan-rekannya, menjelaskan bahwa penggunaan OWASP ZAP sebagai alat pemindaian keamanan web membantu mendeteksi sejumlah besar kerentanan, termasuk

kerentanan pada situs web ILab ITERA. Hasil analisis menunjukkan bahwa situs web memiliki beberapa kerentanan yang memungkinkan serangan seperti SQL injection, cross-site scripting (XSS), dan serangan injeksi JavaScript. Setelah dilakukan tindakan perbaikan dan pengujian ulang, kerentanan berhasil diperbaiki. Oleh karena itu, penggunaan OWASP ZAP sangat direkomendasikan untuk menjaga keamanan situs web.

Pada penelitian selanjutnya yang dilakukan oleh Deepika Sagar serta rekan-rekannya, dalam artikel [13] yang berjudul "Studying Open Source Vulnerabilitir Scanners for Vulnerabilities in Web Applications" menyatakan bahwa setelah melakukan pengujian dan analisis alat pemindai w3af, ZAP, dan Skipfish pada parameter yang berbeda, mereka menyimpulkan bahwa OWASP ZAP memberikan hasil yang lebih baik dibandingkan dengan Skipfish dan w3af. Kesimpulan ini diperoleh dengan memeriksa dengan seksama fitur keseluruhan yang dimiliki oleh setiap pemindai dan kualitas hasil yang dihasilkan oleh masing-masing pemindai.

Dalam buku [14] yang berjudul "Mastering Modern Web Penetration Testing Master The Art Of Conducting Modern Pen Testing Attacks And Techniques On Your Web Application Before The Hacker Does!", Prakhar Prasad mengatakan bahwa keamanan web merupakan suatu proses yang berkelanjutan dan bukan hanya sekedar penerapan teknologi atau solusi tunggal. Ia mengatakan bahwa penting untuk memahami secara menyeluruh tentang ancaman-ancaman yang ada, teknik-teknik serangan yang biasa digunakan, dan metode-metode pengujian keamanan web untuk mengembangkan strategi keamanan yang efektif. Selain itu, Prakhar Prasad juga menekankan pentingnya penerapan tiga prinsip keamanan informasi, yaitu Confidentiality, Integrity, dan Availability (CIA) dalam konteks keamanan web. Ia juga membahas teknik-teknik pengamanan web, seperti penggunaan enkripsi, authentication, dan authorization untuk melindungi data sensitif dan mencegah akses yang tidak sah.

Pada penelitian [15] yang berjudul "Implementasi OWASP ZAP Untuk Pengujian Keamanan Sistem Informasi Akademik" oleh Gregorius Hendita Artha Kusuma, melakukan penelitian terkait penerapan OWASP ZAP sebagai alat pengujian keamanan pada sistem informasi akademik. Pada penelitian ini, Gregorius melakukan implementasi OWASP ZAP untuk menguji keamanan sistem informasi akademik dan mengidentifikasi kerentanan atau celah keamanan yang mungkin terdapat pada sistem. Hasil penelitian menunjukkan bahwa OWASP ZAP berhasil mengidentifikasi beberapa celah keamanan pada sistem informasi akademik yang diuji, seperti kerentanan Cross-Site Scripting (XSS), SQL Injection, dan lain-lain. Dengan demikian, penelitian ini membuktikan bahwa OWASP ZAP dapat menjadi alat yang efektif untuk melakukan pengujian keamanan pada sistem informasi akademik.

Pada penelitian [16] yang berjudul "Analisis Website Tapanuli Tengah Menggunakan Metode Open Web Application Security Project Zap (Owasp Zap)" yang dilakukan oleh Khairrun Nisa dan rekan-rekannya, dilakukan penelitian terhadap website Tapanuli Tengah menggunakan metode Owasp Zap. Hasil penelitian menunjukkan adanya beberapa kerentanan pada website yang dianalisis, termasuk kerentanan XSS dan SQL injection. Penelitian ini menekankan pentingnya penggunaan alat-alat keamanan web seperti Owasp Zap dalam memastikan keamanan website.

Relevansi antara penelitian yang akan dilakukan dengan penelitian terkait adalah memiliki fokus pada pengujian keamanan dan kerentanan web dengan menggunakan OWASP ZAP sebagai alat pemindaian dan fokus pada aspek celah keamanan web.

3. METODOLOGI PENELITIAN

3.1. Analisis Kebutuhan

Dalam penelitian ini, akan digunakan alat dan bahan yang diperlukan untuk melakukan analisis menggunakan OWASP ZAP. Berikut adalah spesifikasi alat dan bahan yang akan digunakan dalam penelitian ini:

a. Komputer/Laptop dengan spesifikasi yang tertera pada Tabel 1.

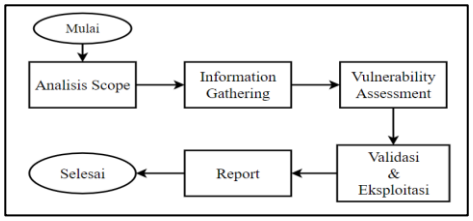
Tabel 1. Spesifikasi minimum perangkat keras penelitian

Komponen	Spesifikasi Minimum
Prosesor	Intel Core i3 atau AMD Ryzen 3
RAM	4 GB
Storage	128 GB HDD atau 64 GB SSD
Sistem Operasi	Linux, macOS, atau Windows

b. *Tool* OWASP ZAP versi 2.14.0.
c. Web *browser*: Google Chrome atau Mozilla Firefox.
d. *Tools* bantuan: Burp Suite, SQLMap, XSSer, dan alat bantuan lainnya.

3.2. Metode Penelitian

Pada penelitian ini, dilakukan pengujian untuk menguji seberapa efektif penggunaan tool OWASP ZAP dalam menganalisis kerentanan web di lingkungan Universitas Mataram. Metode yang dilakukan pada penelitian ini mencakup beberapa langkah dan dapat dilihat pada Gambar 1.



Gambar 1. Langkah-langkah alur penelitian

3.2.1. Analisis *scope*

Tahap *analisis scope* adalah tahap awal yang dimana bertujuan untuk menentukan ruang lingkup dan tujuan

dari penelitian[26]. Pada tahapan ini akan dilakukan penentuan ruang lingkup yang akan dianalisis, seperti subdomain dari website unram.ac.id yang akan menjadi fokus penelitian, OWASP ZAP yang digunakan sebagai *tool* untuk melakukan analisis, dan menentukan metode untuk melakukan penelitian. *Analisis scope* ini penting untuk memfokuskan upaya penelitian pada aspek-aspek yang relevan dan relevan dengan keamanan web di lingkungan Universitas Mataram.

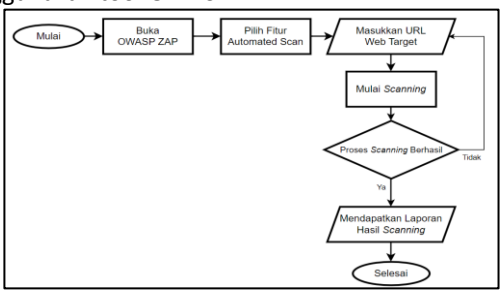
3.2.2. *Information* gathering

Setelah melakukan *analisis scope*, tahap selanjutnya yang akan dilakukan yaitu tahap *information gathering*. Pada tahap ini, fokus utamanya adalah mengumpulkan informasi yang relevan yang terdapat di lingkungan Universitas Mataram. Informasi yang berhasil dikumpulkan akan digunakan sebagai dasar atau acuan untuk tahap berikutnya[27]. Beberapa informasi yang dikumpulkan antara lain adalah:

a. Informasi sistem web: Informasi yang mencakup detail teknis mengenai platform, *framework*, atau CMS (*Content Management System*) yang digunakan untuk mengembangkan dan menjalankan website tersebut.
b. Daftar *subdomain*: Informasi mengenai daftar subdomain yang ada di lingkungan Universitas Mataram juga akan dikumpulkan.
c. Kebijakan keamanan: Informasi terkait kebijakan dan standar keamanan yang diterapkan untuk melindungi sistem dan data.

3.2.3. *Vulnerability assessment*

Setelah selesai dengan proses pengumpulan informasi, tahap selanjutnya adalah *vulnerability assessment*. Tahap ini menjadi fokus utama dari penelitian, karena pada tahap ini akan dilakukan identifikasi dan evaluasi terhadap potensi celah keamanan yang ada dalam sistem menggunakan tool OWASP ZAP.



Gambar 2. Diagram alir Vulnerability Assessment menggunakan OWASP ZAP.

Untuk melakukan melaksanakan pemindaian, fitur automated scan yang tersedia pada OWASP ZAP akan digunakan untuk melakukan pemindaian terhadap setiap subdomain yang telah ditentukan untuk dianalisis.

Sebelum menggunakan fitur tersebut, terdapat beberapa persyaratan yang harus dipenuhi. Beberapa persyaratan tersebut meliputi:

a. Sistem yang akan dianalisis dan komputer atau laptop yang digunatakan harus terhubung dengan jaringan internet, karena pemindaian akan dilakukan secara online.
b. Memastikan subdomain yang akan dianalisis dapat diakses melalui jaringan internet agar fitur automated scan dapat memindai potensi kerentanan keamanan yang mungkin ada pada setiap subdomain.

Dengan memenuhi beberapa persyaratan tersebut, maka pemindaian akan dapat dilakukan.

Setelah memperoleh laporan hasil dari proses scanning, beberapa informasi yang signifikan dapat diidentifikasi untuk setiap jenis kerentanan yang ditemukan dan dimasukkan ke dalam tabel yang telah ditentukan. Tabel 3 memuat rincian lengkap mengenai hasil scanning menggunakan OWASP ZAP, termasuk jenis kerentanan, URL terkait, resiko, tingkat keyakinan, dan deskripsi dari celah keamanan yang telah ditemukan.

3.2.4. Validasi & eksploitasi

Setelah tahap *vulnerability assessment* selesai, langkah berikutnya adalah melakukan validasi dan eksploitasi. Tujuan dari tahap ini adalah untuk melakukan validasi terhadap hasil analisis yang telah dilakukan menggunakan *tool* OWASP ZAP, dan kemudian dilakukan eksploitasi terhadap kerentanan yang ditemukan tersebut. Fokus utama dari tahap ini adalah untuk memastikan bahwa kerentanan yang teridentifikasi benar-benar valid dan dapat dimanfaatkan untuk memperoleh akses yang tidak sah ke dalam sistem.

3.2.5. *Report*

Setelah semua tahap penelitian selesai dilakukan, langkah terakhir adalah tahap Report. Pada tahap ini dilakukan penyusunan terkait laporan hasil akhir web yang dianalisis, menghitung jumlah persentase kerentanan yang valid pada setiap web, dan memberikan solusi untuk kerentanan yang telah divalidasi. Penyusunan laporan tersebut melibatkan proses identifikasi dan evaluasi kerentanan berdasarkan daftar OWASP Top 10-2021.

Adapun hasil dari proses yang telah dilakukan akan digunakan tabel hasil laporan akhir sesuai web yang diuji dan akan digunakan perhitungan jumlah total persentase validasi kerentanan dengan rincian sebagai berikut:

a. Tabel hasil laporan akhir sesuai web yang diuji

Tabel 2. Tabel laporan hasil akhir

No	Jenis Kerentanan (OWASP Top 10)	Kerentanan	Risk	Status	Keterangan

Laporan tersebut akan berisi rangkuman lengkap mengenai klasifikasi jenis kerentanan dalam daftar list “OWASP Top 10 - 2021”, kerentanan yang ditemukan, tingkat resiko, status validasi, serta keterangan dari kerentanan yang teridentifikasi.

b. Perhitungan Jumlah Total Persentase Kerentanan Valid

Adapun perhitungan persentase jumlah kerentanan yang valid pada masing-masing web dan

total persentase kerentanan yang valid pada seluruh web yang diuji:

a. Perhitungan persentase jumlah kerentanan yang valid pada masing-masing web

$$X = \frac{Kerentanan\ valid\ pada\ web}{\text{Total kerentanan yang teridentifikasi pada web}} \times 100\% \quad (1)$$

b. Perhitungan total persentase kerentanan yang valid pada seluruh web\

$$y = \frac{Total\ kerentanan\ valid\ pada\ seluruh\ web}{\text{Total kerentanan yang teridentifikasi pada seluruh web}} \times 100\% \quad (2)$$

4. HASIL DAN PEMBAHASAN

Pada bab ini, akan dijelaskan temuan-temuan yang dihasilkan sebagai hasil dari penelitian yang telah dieksekusi. Temuan-temuan tersebut diperoleh dengan merujuk kepada metode penelitian yang telah dijelaskan secara detail pada bab sebelumnya, khususnya dalam konteks analisis kerentanan yang menggunakan OWASP ZAP sebagai alat analisis keamanan di lingkungan UNRAM.

4.1 Hasil Information Gathering

Informasi yang diperoleh pada tahap ini akan menjadi dasar penting untuk menganalisis kerentanan pada web yang akan dianalisis. Dibawah ini merupakan tabel yang berisikan data hasil dari beberapa temuan informasi dasar yang diperoleh selama tahap *information gathering*.

Tabel 3. Hasil pencarian informasi

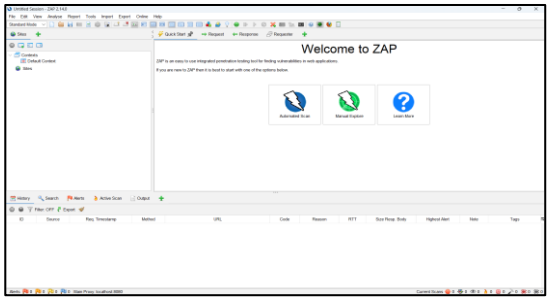
No	Daftar Web Target	Web Address	IP Address	CMS	Firewall
1	SIA UNRAM	sia.unram.ac.id	103.133.160.103	-	Apache Generic
2	SPI UNRAM	spi.unram.ac.id	103.133.160.246	Word Press 6.2.3	360 WAF (360)
3	Fakultas Ekonomi & Bisnis	feb.unram.ac.id	103.133.160.83	Word Press 6.2.3	FortiWeb WAF (Fortinet) / Open Source WAF (Modsecurity)
4	Fakultas Teknik	ft.unram.ac.id	103.133.160.74	Word Press 6.2.3	Fortiweb WAF (Fortinet) / Nginx Generic Protection
5	Program Studi Teknik Informatika	if.unram.ac.id	103.133.160.197	Word Press 6.1.1	AnYu WAF (Anyu Technologies) / Apache Generic

Informasi yang telah diperoleh pada tahap ini akan menjadi landasan utama dalam pemahaman karakteristik teknis dari setiap entitas web yang akan dianalisis kerentanannya.

4.2 Aplikasi Proses Scanning Menggunakan OWASP ZAP

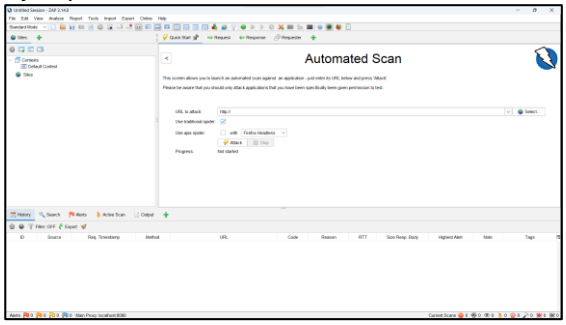
Tahap berikutnya adalah tahap *vulnerability assessment*. Tahap ini merupakan tahap yang bertujuan untuk menilai keamanan web dengan melakukan identifikasi dan menganalisis potensi kerentanan dan resiko yang mungkin terjadi. Pada tahap ini, proses *scanning* diterapkan dengan menggunakan *framework* OWASP ZAP, dimana proses *scanning* disesuaikan dengan skema yang telah diuraikan pada bab sebelumnya. Berikut adalah tahapan-tahapan dalam skema *vulnerability assessment* menggunakan OWASP ZAP:

Langkah pertama yang dilakukan oleh *user*, yaitu membuka *framework* OWASP ZAP yang telah terinstalasi pada perangkat yang digunakan. Ketika membuka *framework* OWASP ZAP, *user* akan langsung dialihkan menuju *landing page* atau halaman awal sesuai pada Gambar 3.



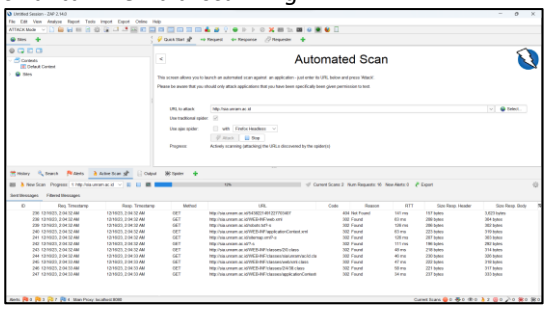
Gambar 3. Landing Page OWASP ZAP

Setelah *landing page* atau halaman awal pada OWASP ZAP berhasil ditampilkan seperti Gambar 3, langkah selanjutnya adalah memilih menu *automated scan*.



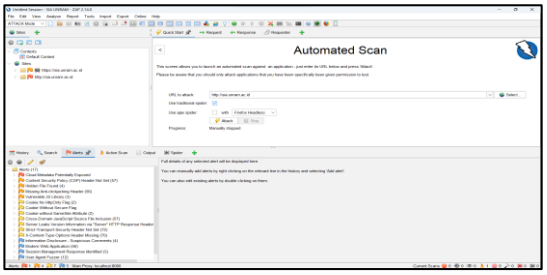
Gambar 4. Menu Automated Scan OWASP ZAP

Setelah menu *automated scan* ditampilkan seperti pada Gambar 4, *user* meng-*input URL* web target yang akan di *scanning* pada *URL field* dan menekan tombol *attack* untuk memulai *scanning*.



Gambar 5. Proses Scanning OWASP ZAP

Pada Gambar 5 merupakan tampilan pada saat proses *scanning* menggunakan OWASP ZAP defang berlanglung.



Gambar 6. *Alerts Report* pada OWASP ZAP

Pada Gambar 6 merupakan tampilan setelah proses scanning berhasil dilakukan. Pada tahap ini, *user* akan memperoleh data *alerts report* atau laporan peringatan yang menyajikan hasil temuan keamanan. Laporan ini memberikan informasi rinci tentang potensi kerentanan yang ditemukan selama proses *scan*.

4.3 Analisis Hasil Vulnerability Assessment

Berikut ini adalah rangkuman data hasil temuan dari proses *vulnerability assessment* yang dilakukan menggunakan framework OWASP ZAP pada setiap situs web yang dianalisis.

Tabel 4. Data hasil scanning web SIA UNRAM

No	Jenis Kerentanan	URL	*Risk*	*Confidence*	Deskripsi
1	Content Security Policy (CSP) Header Not Set	https://sia.unram.ac.id/robots.txt	*Medium*	*High*	Header CSP tidak diatur
2	Hidden File Found	http://sia.unram.ac.id/.hg	*Medium*	*Low*	Ditemukan file tersembunyi
3	Missing Anti-clickjacking Header	http://sia.unram.ac.id	*Medium*	*Medium*	Header Anti-clickjacking tidak diatur

Pada Tabel 4 berisikan beberapa data hasil scanning terhadap web SIA UNRAM menggunakan OWASP ZAP, terdapat sebanyak 17 kerentanan yang berhasil teridentifikasi.

Tabel 5. Data hasil scanning web SPI UNRAM

No	Jenis Kerentanan	URL	*Risk*	*Confidence*	Deskripsi
1	SQL Injection - MySQL	http://spi.unram.ac.id/?p=209	*High*	*Medium*	Ditemukan kerentanan SQL Injection tipe MySQL
2	Absence of Anti-CSRF Tokens	http://spi.unram.ac.id	*Medium*	*Low*	Tidak terdapat konfigurasi Anti-CSRF Tokens
3	Missing Anti-clickjacking Header	http://spi.unram.ac.id	*Medium*	*Medium*	Header Anti-clickjacking tidak diatur

Pada Tabel berisikan beberapa data hasil *scanning* terhadap web SPI UNRAM menggunakan OWASP ZAP, terdapat sebanyak 26 kerentanan yang berhasil teridentifikasi.

Tabel 6. Data hasil scanning web FEB UNRAM

No	Jenis Kerentanan	URL	*Risk*	*Confidence*	Deskripsi
1	PII Disclosure	https://feb.unram.ac.id/wp-content/plugins/elementor-pro/assets/js/elements-handlers.min.js?ver=3.6.5	*High*	*Medium*	Terdapat pengungkapan informasi PII (Personally Identifiable Information)
2	Absence of Anti-CSRF Tokens	http://feb.unram.ac.id	*Medium*	*Low*	Tidak terdapat Konfigurasi Anti-CSRF Tokens
3	Content Security Policy (CSP) Header Not Set	http://feb.unram.ac.id	*Medium*	*High*	Header Content Security Policy (CSP) tidak diatur

Pada Tabel 6 berisikan beberapa data hasil scanning terhadap web FEB UNRAM menggunakan OWASP ZAP, terdapat sebanyak 20 kerentanan yang berhasil teridentifikasi.

Tabel 7. Data hasil scanning web Fakultas Teknik UNRAM

No	Jenis Kerentanan	URL	*Risk*	*Confidence*	Deskripsi
1	HTTP to HTTPS Insecure Transition in Form Post	http://ft.unram.ac.id	*Medium*	*Medium*	Terdapat transisi tidak aman dari HTTP ke HTTPS pada pengiriman formulir
2	Hidden File Found	http://ft.unram.ac.id/.hg	*Medium*	*Low*	Ditemukan file tersembunyi
3	Cookie Without Secure Flag	https://ft.unram.ac.id/sitemap.xml	*Low*	*Medium*	Cookie tidak memiliki flag Secure

Pada Tabel 7 berisikan *beberapa* data hasil scanning terhadap web Fakultas Teknik UNRAM menggunakan OWASP ZAP, terdapat sebanyak *20* kerentanan yang berhasil teridentifikasi.

Tabel 8. Data hasil scanning web Prodi Teknik Informatika UNRAM

No	Jenis Kerentanan	URL	*Risk*	*Confidence*	Deskripsi
1	Absence of Anti-CSRF Tokens	https://if.unram.ac.id/hello-world/	*Medium*	*Low*	Tidak terdapat konfigurasi Anti-CSRF Tokens

2	Missing Anti-clickjacking Header	http://if.unram.ac.id	*Medium*	*Medium*	Header Anti-clickjacking tidak diatur
3	Timestamp Disclosure - Unix	http://if.unram.ac.id	*Low*	*Low*	Terdapat pengungkapan timestamp dalam format Unix

Pada Tabel 8 berisikan *beberapa* data hasil scanning terhadap web Prodi Teknik Informatika UNRAM menggunakan OWASP ZAP, terdapat sebanyak 22 kerentanan yang berhasil teridentifikasi.

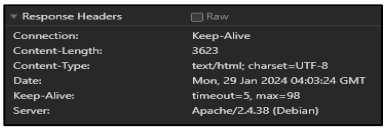
4.4 Validasi & Eksploitasi

Setelah semua data pada tahap *vulnerability assessment* berhasil diperoleh, langkah selanjutnya adalah tahap eksploitasi. Tujuan utama pada tahap ini adalah untuk melakukan validasi terhadap temuan yang telah diperoleh pada tahap sebelumnya, serta melakukan eksploitasi apakah kerentanan yang telah teridentifikasi oleh *tool* OWASP ZAP merupakan kerentanan yang benar-benar dapat dimanfaatkan sebagai celah keamanan pada sistem.

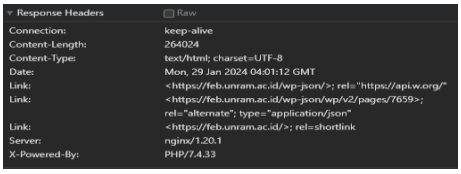
Berikut adalah beberapa hasil dari proses validasi yang telah dilakukan terhadap beberapa kerentanan yang telah diidentifikasi pada setiap situs web:

a. *Content Security Policy (CSP) Header Not Set*

Untuk melakukan validasi terhadap CSP header yang tidak diatur, dilakukan pengecekan secara manual melalui browser menggunakan fungsi *inspect*. Setelah dilakukan pengecekan, terbukti bahwa CSP *header* dengan format "Content-Security-Policy" tidak diterapkan pada website.



Gambar 7. Validasi CSP Header not set pada web SIA UNRAM

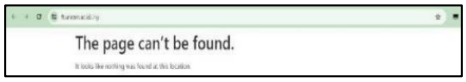


Gambar 8. Validasi Content Security Policy (CSP) Header Not Set pada web FEB

b. *Hidden File Found*

File tersembunyi yang ditemukan adalah *file* dengan ekstensi ".hg", yang dimana file tersebut biasanya terkait dengan sistem kontrol yang digunakan untuk melacak perubahan dalam kode sumber selama pengembangan perangkat lunak. Pada saat pengecekan manual menggunakan *browser*, respon yang didapat pada saat mengakases alamat "http://sia.unram.ac.id/.hg" pada web SIA UNRAM adalah status 404 (tidak ditemukan).

Gambar 9. Validasi hidden file yang ditemukan pada web SIA UNRAM

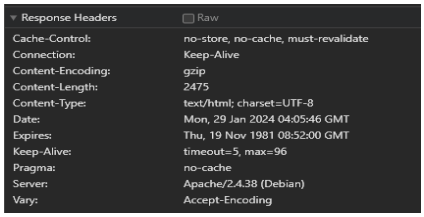


Gambar 10. Validasi Hidden File Found pada web FT

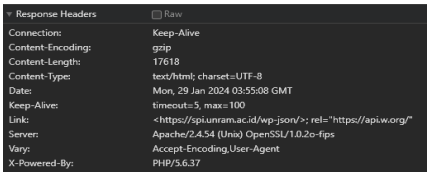
Pada Gambar 10, menunjukkan respon yang didapat pada saat mengakases URL "http://ft.unram.ac.id/.hg" pada web FT. Dimana tampilan halaman web tersebut menampilkan status "The page can't be found".

c. *Missing Anti-clickjacking Header*

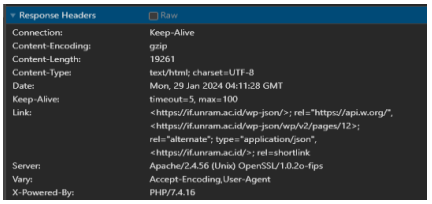
Dilakukan pembuktian terhadap kerentanan *Missing Anti-clickjacking Header* menggunakan fungsi *inspect* melalui *browser*, dan terbukti bahwa konfigurasi *anti-clickjacking header* dengan format "X-Frame-Options" pada web SIA, SPI, dan Prodi Teknik Informatika UNRAM tidak tersedia.



Gambar 11. Validasi Missing Anti-clickjacking Header pada web SIA UNRAM



Gambar 12. Validasi Missing Anti-clickjacking Header pada web SPI UNRAM

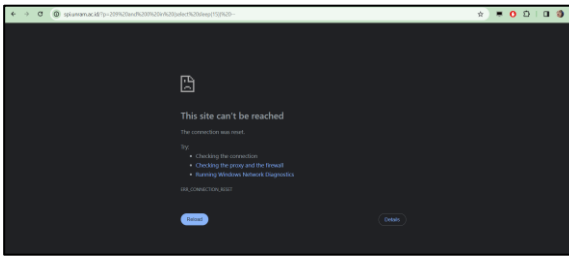


Gambar 13. Validasi Missing Anti-clickjacking Header pada web Teknik Informatika UNRAM

d. *SQL Injection – MySQL*

Validasi kerentanan ini dilakukan secara manual melalui browser dengan cara menyisipkan *payload* "and 0 in (select sleep(15)) --" pada *URL* "http://spi.unram.ac.id/?p=209". Payload yang disisipkan tersebut merupakan perintah untuk

membuat kondisi *false* dan memaksa *database* untuk tidur selama 15 detik. Setelah melakukan eksekusi *payload* dan menunggu selama 15 detik, server pada web SPI tidak memberikan respon apapun.



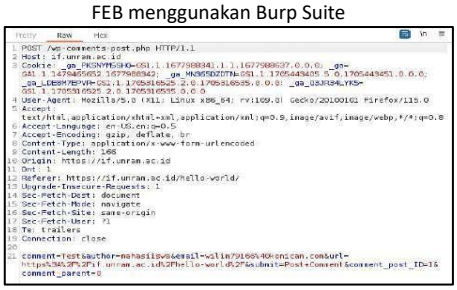
Gambar 14. Validasi SQL Injection – MySQL pada web SPI UNRAM

e. *Absence of Anti-CSRF Tokens*

Dengan tidak adanya *Anti-CSRF Token* yang diterapkan pada web SPI, FEB, FT, dan PSTI dapat meningkatkan resiko terhadap serangan *Cross-Site Request Forgery* (*CSRF*), yang dimana serangan tersebut dapat mempengaruhi integritas data pada sistem. *Script* yang terdeteksi sebagai kerentanan *Absence of Anti-CSRF Tokens* merupakan *script search form* dengan *method GET*.

Gambar 15. Validasi Absence of Anti-CSRF pada web SPI UNRAM menggunakan Burp Suite

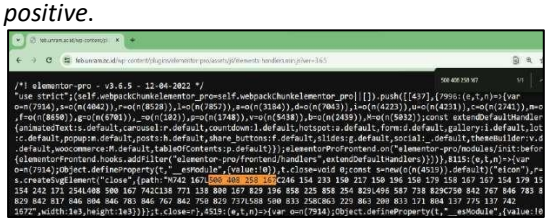
Gambar 16. Validasi Absence of Anti-CSRF Tokens pada web FEB menggunakan Burp Suite



Gambar 17. Validasi Absence of Anti-CSRF Tokens pada web Prodi Teknik Informatika UNRAM menggunakan Burp Suite

f. *PII Disclosure*

PII Disclosure adalah kerentanan yang memiliki resiko terhadap bocornya informasi pribadi user. Celah kerentanan ini dapat divalidasi secara manual dengan cara melakukan pengecekan terhadap link yang diberikan oleh tool OWASP ZAP, apakah informasi yang teridentifikasi adalah informasi sensitif atau merupakan *false positive*. Setelah melakukan validasi terhadap data *evidence* "500 408 258 167" yang dianggap temuan kerentanan *PII Disclosure* pada web FEB UNRAM, data tersebut adalah hanya koordinat dalam format path SVG dan tidak ada informasi pribadi apapun yang ditemukan. Oleh karena itu, kerentanan *PII Disclosure* yang teridentifikasi dapat dikategorikasn sebagai kerentanan *false positive*.



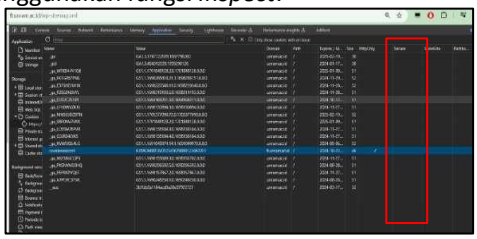
Gambar 18. Validasi PII Disclosure pada web FEB

g. *HTTP to HTTPS Insecure Transition in Form Post*

HTTP to HTTPS Insecure Transition in Form Post menyebabkan potensi resiko keamanan yang tinggi, karena data yang dikirimkan melalui formulir menjadi rentan terhadap serangan peretas. Validasi celah kerentanan ini dapat dilakukan dengan cara mengamati URL pada saat mengirim formulir untuk mengakses laman "http://ft.unram.ac.id".

h. *Cookie Without Secure Flag*

Celah kerentanan ini teridentifikasi karena pada sistem tidak menerapkan konfigurasi secure flag pada cookie. Jika konfigurasi tersebut tidak diterapkan pada cookie, ada kemungkinan informasi sensitif yang dikirimkan melalui koneksi *HTTP* rentan terhadap serangan Man-in-the-Middle (MITM). Validasi celah kerentanan ini dilakukan secara manual melalui browser dengan menggunakan fungsi *inspect*.



Gambar 19. Validasi Cookie Without Secure Flag pada web FT

i. *Timestamp Disclosure* – Unix

Timestamp Disclosure berformat Unix teridentifikasi sebagai kerentanan karena mengungkapkan atau memberikan informasi

timestamp dalam format Unix kepada user. Validasi pada celah kerentanan ini dilakukan dengan cara manual melalui browser menggunakan fitur inspect element.

Gambar 20. Validasi Timestamp Disclosure - Unix pada web Teknik Informatika UNRAM

Pada web Prodi Teknik Informatika UNRAM, tepatnya pada source HTML teridentifikasi adanya beberapa timestamp dengan format unix, yaitu "1673341464", "1673341465", dan "1704174277". Apabila timestamp tersebut dikonversi secara urut, maka hasilnya akan menjadi "2023/01/10 17:04:24", "2023/01/10 17:04:25", dan "2024/01/02 13:44:37".

4.5 Report dan Pembahasan

Tahap ini adalah tahap terakhir pada penelitian yang dilakukan. Pada tahap ini hasil yang telah diperoleh dilakukan pengklasifikasian sesuai daftar kerentanan OWASP Top 10-2021, dan kemudian dilakukan pembahasan berdasarkan standar keamanan OWASP.

a. Web SIA UNRAM

Pada situs web SIA UNRAM, ditemukan 14 dari 17 celah keamanan yang dapat diklasifikasikan berdasarkan daftar OWASP Top 10-2021. Setelah proses validasi terhadap celah keamanan yang telah diklasifikasikan, ditemukan bahwa hanya tersisa 10 celah keamanan yang valid atau sebesar 58,82%, dengan perhitungan persentase:

$$\text{Persentase kerentanan yang valid pada web SIA} = \frac{10}{17} \times 100\% = 58{,}82\% \quad (3)$$

Dari total kerentanan yang telah divalidasi dan diklasifikasikan dalam OWASP Top 10-2021, kerentanan-kerentanan yang ditemukan meliputi:

1. Broken Access Control (A01:2021) – 5,88%
2. Security Misconfiguration (A05:2021) – 47,05%
3. Vulnerable and Outdated Components (A06:2021) – 5,88%

b. Web SPI UNRAM

Pada situs web SPI UNRAM, ditemukan 22 dari 26 celah keamanan yang dapat diklasifikasikan berdasarkan daftar OWASP Top 10-2021. Setelah proses validasi terhadap celah keamanan yang telah diklasifikasikan, ditemukan bahwa hanya tersisa 10 celah keamanan yang valid atau sebesar 38,46%, dengan perhitungan persentase:

$$\text{Persentase kerentanan yang valid pada web SPI} = \frac{10}{26} \times 100\% = 38{,}46\% \quad (4)$$

Dari total kerentanan yang telah divalidasi dan diklasifikasikan dalam OWASP Top 10-2021, kerentanan-kerentanan yang ditemukan meliputi:

1. *Broken Access Control* (A01:2021) - 15,38%
2. *Security Misconfiguration* (A05:2021) - 19,32%
3. Vulnerable and Outdated Components (A06:2021) - 3,84%

c. Web FEB UNRAM

Pada situs web FEB UNRAM, ditemukan 16 dari 20 celah keamanan yang dapat diklasifikasikan berdasarkan daftar OWASP Top 10-2021. Setelah proses validasi terhadap celah keamanan yang telah diklasifikasikan, ditemukan bahwa hanya tersisa 12 celah keamanan yang valid atau sebesar 60%, dengan perhitungan persentase:

$$\text{Persentase kerentanan yang valid pada web FEB} = \frac{12}{20} \times 100\% = 60\% \quad (5)$$

Dari total kerentanan yang telah divalidasi dan diklasifikasikan dalam OWASP Top 10-2021, kerentanan-kerentanan yang ditemukan meliputi:

1. *Broken Access Control* (A01:2021) - 20%
2. *Cryptographic Failures* (A02:2021) - 5%
3. *Security Misconfiguration* (A05:2021) - 35%

d. Web FT UNRAM

Pada situs web FT UNRAM, ditemukan 18 dari 23 celah keamanan yang dapat diklasifikasikan berdasarkan daftar OWASP Top 10-2021. Setelah proses validasi terhadap celah keamanan yang telah diklasifikasikan, ditemukan bahwa hanya tersisa 14 celah keamanan yang valid atau sebesar 60,87%, dengan perhitungan persentase:

$$\text{Persentase kerentanan yang valid pada web FT} = \frac{14}{23} \times 100\% = 60{,}87\% \quad (6)$$

Dari total kerentanan yang telah divalidasi dan diklasifikasikan dalam OWASP Top 10-2021, kerentanan-kerentanan yang ditemukan meliputi:

1. *Broken Access Control* (A01:2021) - 17,39%
2. *Cryptographic Failures* (A02:2021) - 4,34%
3. *Security Misconfiguration* (A05:2021) - 34,78%
4. Vulnerable and Outdated Components (A06:2021) - 4,34%

e. Web Prodi Teknik Informatika UNRAM

Pada situs web Prodi Teknik Informatika UNRAM, ditemukan 16 dari 22 celah keamanan yang dapat diklasifikasikan berdasarkan daftar OWASP Top 10-2021. Setelah proses validasi terhadap celah keamanan yang telah

diklasifikasikan, ditemukan bahwa hanya tersisa 9 celah keamanan yang valid atau sebesar 40,91%, dengan perhitungan persentase:

$$\text{Persentase kerentanan yang valid pada web Prodi Teknik Informatika} = \frac{9}{22} \times 100\% = 40{,}91\% \quad (7)$$

Dari total kerentanan yang telah divalidasi dan diklasifikasikan dalam OWASP Top 10-2021, kerentanan-kerentanan yang ditemukan meliputi:

1. *Broken Access Control* (A01:2021) - 13,64%
2. *Security Misconfiguration* (A05:2021) - 27,27%
3. Vulnerable and Outdated Components (A06:2021) - 4,34%

Berdasarkan total jumlah kerentanan yang telah divalidasi pada seluruh web yang diuji, yaitu berjumlah 55 kerentanan valid dari jumlah total 108 kerentanan yang teridentifikasi oleh OWASP ZAP maka didapatkan perhitungan:

$$\text{Persentase total kerentanan valid pada seluruh web} = \frac{55}{108} \times 100\% = 50{,}92\% \quad (8)$$

4.6 Analisis

Berdasarkan data yang diperoleh, hasil analisis keamanan terhadap situs web Sistem Informasi Akademik (SIA) UNRAM, Satuan Pengawas Internal (SPI) UNRAM, Fakultas Ekonomi dan Bisnis (FEB), Fakultas Teknik (FT), dan Program Studi Teknik Informatika (PSTI) UNRAM menunjukkan bahwa dari total 108 celah kerentanan yang diidentifikasi di seluruh subdomain yang diuji, , hanya terdapat 86 (79,63%) kerentanan yang dapat diklasifikasikan ke dalam daftar kerentanan OWASP Top 10-2021, dan hanya ada sebanyak 55 (50,92%) kerentanan valid dari total keseluruhan kerentanan yang teridentifikasi oleh OWASP ZAP.

Pada situs web SIA UNRAM, dari 17 celah keamanan yang diidentifikasi, ada sebanyak 71,43% kerentanan yang dianggap valid setelah proses verifikasi. Kerentanan terkait *Broken Access Control* (A01:2021) sebanyak 7,14%, dengan solusi penerapan atribut *SameSite* pada *cookie*. Sedangkan *Security Misconfiguration* (A05:2021) mencapai 57,14%, dengan solusi melibatkan perlindungan terhadap *cloud metadata*, penerapan *Content Security Policy* (CSP) *Header*, *anti-clickjacking header*, dan lainnya. Kerentanan *Vulnerable and Outdated Components* (A06:2021) sebanyak 7,14%, dengan rekomendasi untuk memperbarui Bootstrap.

Pada situs web SPI UNRAM, dari 26 celah keamanan yang diidentifikasi, hanya 45,45% kerentanan yang dianggap valid setelah proses verifikasi. *Broken Access Control* (A01:2021) sebanyak 18,18%, dengan solusi penerapan token *Anti-CSRF*, konfigurasi kontrol akses *Cross-Domain*, dan lainnya. *Security Misconfiguration* (A05:2021) mencapai 22,73%, dengan solusi serupa seperti pada SIA UNRAM. Kerentanan *Vulnerable and Outdated Components* (A06:2021) sebanyak 4,54%, dengan rekomendasi untuk memperbarui jQuery.

Pada situs web Fakultas Ekonomi dan Bisnis UNRAM, dari 20 celah keamanan yang diidentifikasi, ada sebanyak 75% kerentanan yang dianggap valid setelah proses verifikasi. *Broken Access Control* (A01:2021) sebanyak 25%, dengan solusi penerapan token *Anti-CSRF* dan pengaturan pesan *debug*. *Cryptographic Failures* (A02:2021) mencapai 6,25%, dengan solusi konfigurasi protokol. *Security Misconfiguration* (A05:2021) sebanyak 43,75%, dengan solusi seperti pada SIA UNRAM.

Pada situs web Fakultas Teknik UNRAM, dari 23 celah keamanan yang diidentifikasi, ada sebanyak 77,78% yang dianggap valid setelah proses verifikasi. *Broken Access Control* (A01:2021) sebanyak 22,22%, dengan solusi penerapan token *Anti-CSRF* dan atribut *SameSite* pada *cookie*. *Cryptographic Failures* (A02:2021) mencapai 5,55%, dengan solusi konfigurasi protokol. *Security Misconfiguration* (A05:2021) sebanyak 44,44%, dengan solusi serupa seperti pada Fakultas Ekonomi dan Bisnis.

Pada situs web Program Studi Teknik Informatika UNRAM, dari 22 celah keamanan yang diidentifikasi, hanya 56,25% yang dianggap valid setelah proses verifikasi. *Broken Access Control* (A01:2021) sebanyak 18,75%, dengan solusi penerapan token *Anti-CSRF* dan atribut *SameSite* pada *cookie*. *Security Misconfiguration* (A05:2021) sebanyak 37,5%, dengan solusi seperti pada Fakultas Teknik.

Dari hasil analisis tersebut, terdapat dua aspek kerentanan yang menonjol, yaitu *Broken Access Control* (A01:2021) dan *Security Misconfiguration* (A05:2021), terutama memengaruhi subdomain SIA UNRAM, SPI UNRAM, FEB, FT, dan Prodi Teknik Informatika.

Dengan ditemukannya 50,92% kerentanan valid pada hasil analisis yang telah dilakukan, hal tersebut menunjukkan bahwa tingkat kerentanan pada web dilingkungan Universitas Mataram dapat dianggap tinggi, karena lebih dari setengah dari kerentanan yang diidentifikasi dapat dianggap sebagai kerentanan yang signifikan dan memerlukan perhatian serius untuk diperbaiki demi meningkatkan keamanan sistem. Oleh karena itu, sangat penting untuk segera mengambil langkah-langkah untuk memperbaiki dan mengurangi risiko keamanan dengan memberikan beberapa tindakan pencegahan seperti penerapan token *Anti-CSRF* dan konfigurasi *Content Security Policy* (CSP) *Header* menjadi sangat krusial dalam melindungi informasi penting dan mencegah potensi serangan yang dapat merugikan.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah melakukan proses analisis kerentanan dengan memanfaatkan OWASP ZAP untuk mengidentifikasi potensi celah keamanan pada beberapa sistem web di

lingkungan Universitas Mataram, dapat ditarik kesimpulan bahwa:

a. Dalam penelitian ini, metode OWASP ZAP telah terbukti efektif dalam menganalisis dan mengevaluasi keamanan website di lingkungan Universitas Mataram. Dengan menggunakan metode ini, peneliti berhasil mengidentifikasi total 108 celah keamanan, di mana 79,63% di antaranya dapat diklasifikasikan ke dalam daftar OWASP Top 10-2021. Hasil ini menunjukkan bahwa metode OWASP ZAP dapat digunakan secara efektif untuk mendeteksi dan memetakan kerentanan pada website, sehingga memungkinkan penanganan yang tepat dan efisien terhadap kerentanan tersebut.
b. Ditemukan beberapa kerentanan dengan tingkat *risk medium* seperti *Absence of Anti-CSRF Tokens*, *Content Security Policy* (CSP) *Header Not Set*, *Vulnerable JS Library*, dan beberapa kerentanan lainnya yang memerlukan langkah-langkah pengamanan. Rekomendasi termasuk penerapan token *Anti-CSRF* dan atribut *SameSite* pada *cookie* untuk mencegah *CSRF*, penyesuaian konfigurasi server untuk menghindari *Security Misconfigurations*, dan integrasi *Content Security Policy* (*CSP*) *Header*. Pembaruan berkala terhadap komponen seperti Bootstrap dan jQuery diperlukan untuk menanggulangi *Vulnerable* and *Outdated Components*. Upaya pencegahan terhadap *Cryptographic Failures* dapat dilakukan melalui konfigurasi protokol yang memastikan pengiriman data terenkripsi secara optimal. Temuan-temuan tersebut menegaskan perlunya implementasi tindakan pencegahan dan perbaikan untuk mengurangi tingkat kerentanan, meningkatkan keamanan, dan mengurangi resiko serangan potensial pada *website* di lingkungan Universitas Mataram.

5.2 Saran

Berdasarkan penelitian yang sudah dilakukan, beberapa saran muncul sebagai panduan untuk penelitian selanjutnya dan untuk meningkatkan sistem web di Universitas Mataram yang menjadi fokus utama penelitian ini. Temuan ini juga mengungkapkan beberapa kelemahan dalam pengembangan otomatisasi OWASP ZAP yang dapat menjadi fokus pengembangan lebih lanjut pada penelitian mendatang, antara lain:

a. Diperlukan adanya pemeriksaan dan perawatan berkala pada seluruh sistem keamanan web di lingkungan Universitas Mataram. Hal ini bertujuan agar setiap celah keamanan dapat teridentifikasi lebih awal, dan mitigasi dapat segera diterapkan jika terdeteksi adanya kerentanan pada keamanan sistem.
b. Meberikan fasilitasi kolaborasi antara peneliti dengan pihak lain di dalam atau di luar universitas, mencakup kolaborasi dengan institusi lain, perusahaan, atau organisasi pemerintah.
c. Untuk peneliti selanjutnya, pastikan untuk menggunakan data terkini dan memperbarui metode penelitian jika diperlukan. Peningkatan data dan metode dapat menghasilkan temuan yang lebih akurat dan relevan.
d. Perluas kajian pustaka dengan mencakup literatur terbaru dan relevan. Hal ini dapat membantu mengidentifikasi tren, perubahan, atau perkembangan baru dalam domain penelitian yang bersangkutan.

DAFTAR PUSTAKA

[1] A. O. Sari, A. Abdilah, and Sunarti, *Web Programming*, 1st ed. Jakarta: Graha Ilmu, 2019.
[2] S. Muhammad Ibnu, *Otodidak Web Programming: Membuat Website Edutainment*. Elex Media Komputindo, 2020. [Online]. Available: https://books.google.co.id/books?id=I73NDwAAQBAJ&lpg=PP1&dq=Otodidak
[3] I. G. I. Sudipa *et al.*, *Penerapan Sistem Informasi di Berbagai Bidang*. PT. Sonpedia Publishing Indonesia, 2023.
[4] S. Farizy and E. S. Eriana, *Keamanan Sistem Informasi*. Pamulang: Unpam Press, 2022.
[5] L. Septiani, "Sebut Kominfo Bodoh, Hacker Pencuri Data di Indonesia Diduga Remaja," *katadata.co.id*, 2022. https://katadata.co.id/desysetyowati/digital/6319b5aa5be4e/sebut-kominfo-bodoh-hacker-pencuri-data-di-indonesia-diduga-remaja
[6] C. Saskia, "Hacker Spesialis Ransomware Klaim Jadi Dalang BSI Down Ancam Sebar Data Nasabah," *Kompas.com*, 2023. https://tekno.kompas.com/read/2023/05/13/10101957/hacker-spesialis-ransomware-klaim-jadi-dalang-bsi-down-dan-ancam-sebar-data?page=all
[7] A. Ramadhani, "Keamanan Informasi," *Nusant. - J. Inf. Libr. Stud.*, vol. 1, no. 1, p. 39, 2018, doi: 10.30999/n-jils.v1i1.249.
[8] SUARANTB.COM, "Situs Manajemen SIA Unram Diretas," 2018. https://www.suarantb.com/2018/02/13/situs-manajemen-sia-unram-diretas/
[9] A. Tiwari, P. J. Patel, and D. P. Sharma, "Vulnerability Assessment and Penetration Testing Approach Towards Cloud-Based Application and Related Services," *Int. J. Sci. Res. Sci. Eng. Technol.*, vol. 4099, pp. 395–403, 2021, doi: 10.32628/ijsrset218346.

[10] M. Yunus, "Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework Owasp Versi 4," *J. Ilm. Inform. Komput.*, vol. 24, no. 1, pp. 37–48, 2019, doi: 10.35760/ik.2019.v24i1.1988.

[11] I. F. Ashari, M. Affandi, H. T. Putra, and M. T. Nur, "Security Audit for Vulnerability Detection and Mitigation of UPT Integrated Laboratory (ILab) ITERA Website Based on OWASP Zed Attack Proxy (ZAP)," *J. Teknol. Inf. dan Komunikasi*, vol. 7, no. 1, p. 2023, 2023, [Online]. Available: https://doi.org/10.35870/jti

[12] S. K. Paudel, "Vulnerable Web Applications and How To Audit Them," *Bachelor Thesis*, p. 59, 2016, [Online]. Available: https://www.theseus.fi/bitstream/handle/10024/113581/my_thesis_final_v3.pdf?sequence=1

[13] S. Tyagi, D. Sagar, S. Kukreja, J. Brahma, and P. Jain, "Studying Open Source Vulnerability Scanners for Vulnerabilities in Web Applications," *Iioab*, vol. 9, pp. 43-49 Tyagi, Shobha et al. 2018, [Online]. Available: www.iioab.org

[14] P. Prasad, *Mastering Modern Web Penetration Testing*. Birmingham: Packt, 2016.

[15] G. Kusuma, "Implementasi Owasp Zap Untuk Pengujian Keamanan Sistem Informasi Akademik," *J. Teknol. Inf. J. Keilmuan dan Apl. Bid. Tek. Inform.*, vol. 16, no. 2, pp. 178–186, 2022, doi: 10.47111/jti.v16i2.3995.

[16] K. Nisa, M. A. Putra, R. A. Siregar, and M. D. Irawan, "Analisis Website Tapanuli Tengah Menggunakan Metode Open Web Application Security Project Zap (Owasp Zap)," *Bull. Inf. Technol.*, vol. 3, no. 4, pp. 308–316, 2022, doi: 10.47065/ bit.v3i1. 389.

[17] E. Darwis, Junaedy, and I. A. Musdar, "Analisis Kerentanan Website Renovaction Menggunakan Rangkaian Security Tools Project Berdasarkan Framework Owasp," *KHARISMA Tech*, vol. 17, no. 1, pp. 1–15, 2022, doi: 10.55645/kharismatech.v17i1.170.

[18] M. Pappada, "CouchDB Injection Active Scan Rules for OWASP ZAP," no. December, 2021, [Online]. Available: https://webthesis.biblio.polito.it/21248/1/tesi.pdf

[19] I. Dwinanto and H. Setiyani, "Implementasi Keamanan Komputer pada Aspek Confidentiality, Integrity, Availibility (CIA) Menggunakan Tools Lynis Audit System," *J. Maklumatika*, vol. 8, no. 1, pp. 35–46, 2021.

[20] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," *J. Algoritm.*, vol. 18, no. 1, pp. 77–86, 2021, doi: 10.33364/algoritma/v.18-1.827.

[21] OWASP, "OWASP Top 10:2021," *OWASP Top 10-2021*, 2021. https://owasp.org/Top10/#welcome-to-the-owasp-top-10-2021

[22] I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," *J. Inf. dan Teknol.*, vol. 4, no. 3, pp. 160–165, 2022, doi: 10.37034/jidt.v4i3.236.

[23] The Owasp Foundation, "OWASP Secure Coding Practices Checklist - OWASP," 2016. https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_Checklist

[24] OWASP, "Who is the OWASP® Foundation?," *OWASP® web page*, 2023. https://owasp.org/

[25] OWASP, "OWASP ZAP – Features," *zaproxy.org*, 2023. https://www.zaproxy.org/docs/desktop/start/features/

[26] E. I. Alwi, H. Herdianti, and F. Umar, "Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning," *INFORMAL Informatics J.*, vol. 5, no. 2, p. 43, 2020, doi: 10.19184/isj.v5i2.18941.

[27] F. Hardiansyah, I. G. N. Mantra, and M. Kom, "Vulnerability Assesment Dan Kajian Aspek Application Security Pada Aplikasi Skripsi Online (Sipso) Fti Perbanas," *SENAMIKA*, pp. 1–9, 2020.