JURNAL LENTERA ICT **ISSN 2338-3143**
Volume 9 Nomor 2, November 2024 **E-ISSN 2986-9951**

VULNERABILITY SCANNING WEBSITE PMB MENGGUNAKAN *OPEN WEB APPLICATION SECURITY PROJECT* (OWASP)

Oleh:
Sari Prabandari

Program Studi Manajemen Informatika, Politeknik LP3I Jakarta
Gedung Sentra Kramat Jalan Kramat Raya No. 7-9 Jakarta Pusat 10450

Email: prabandari98@gmail.com

ABSTRACT

Information and communication technology has increased significantly over the past few decades. Websites are often the target of cyber attacks because there are vulnerabilities that can be exploited by attackers. This study aims to conduct a Vulnerability Assessment (VA) on the website of admission of new students by following the guidelines of the Open Web Application Security Project (OWASP). OWASP provides a list of the top ten vulnerabilities that are often found in web applications, such as SQL Injection, XSS (Cross-Site Scripting), and CSRF (Cross-Site Request Forgery). This study uses the Vulnerability Assessment and Penetration Testing (VAPT) method, which consists of several stages: information gathering, scanning to identify security holes, and generating reports. The tool that used include OWASPZAP to detect and test vulnerabilities. This study produces a report that identifies 33,3% medium risk level vulnerabilities (six flags), 38% low risk level vulnerabilities (seven flags), 27,7% Informational Risk Level (5 flags) and no high-level vulnerabilities. It is hoped that these results can help IT staff in improving the security and convenience of accessing their pmb websites.

Keywords: *Vulnerabilities, Security, PMB, Scanning, OWASP*

ABSTRAK

Teknologi informasi dan komunikasi mengalami peningkatan signifikan selama beberapa dekade terakhir. Website sering kali menjadi target serangan siber karena terdapat kerentanan yang bisa dimanfaatkan oleh penyerang. Penelitian ini bertujuan untuk melakukan *Vulnerability Assessment* (VA) pada website penerimaan mahasiswa baru, dengan mengikuti panduan dari *Open Web Application Security Project* (OWASP). OWASP menyediakan daftar sepuluh besar kerentanan yang sering ditemukan didalam aplikasi web, seperti SQL *Injection*, XSS (*Cross-Site Scripting*), dan CSRF(*Cross-Site Request Forgery*). Penelitian ini menggunakan metode *Vulnerability Assessment* dan *Penetration Testing* (VAPT), yang terdiri dari beberapa tahap: pengumpulan informasi, pemindaian untuk mengidentifikasi celah keamanan, serta pembuatan laporan. Tools yang digunakan adalah OWASPZAP untuk mendeteksi dan pengujian kerentanan. Studi ini menghasilkan laporan yang mengidentifikasi 33,3% kerentanan tingkat risiko sedang (enam tanda), 38% kerentanan tingkat risiko rendah (tujuh tanda), 27,7% tingkat risiko informasional (5 tanda) dan tidak ada kerentanan tingkat tinggi. Diharapkan hasil ini dapat membantu staf TI dalam meningkatkan keamanan dan kenyamanan mengakses situs web pmb nya.

Kata Kunci: Kerentanan, Keamanan, PMB, Pemindaian, OWASP

ISSN 2338-3143
E-ISSN 2986-9951

PENDAHULUAN

Teknologi informasi dan komunikasi mengalami peningkatan signifikan selama beberapa dekade terakhir, mempengaruhi berbagai aspek kehidupan, termasuk cara kita bekerja, berkomunikasi, serta mengakses informasi (Syarifuddin Syahab, 2023). Inovasi seperti internet, ponsel pintar, dan komputasi awan telah membawa dampak signifikan pada sektor bisnis dan sosial, memungkinkan konektivitas global serta akses informasi yang lebih cepat dan efisien (Rabbani, 2023). Dalam dunia pendidikan, sistem penerimaan mahasiswa baru merupakan sebuah sistem yang dirancang untuk mengelola dan memudahkan proses pendaftaran mahasiswa baru di sebuah perguruan tinggi. Sistem ini memanfaatkan teknologi informasi untuk mengotomatiskan berbagai tahapan dalam proses penerimaan mahasiswa, mulai dari pendaftaran online, pengumpulan berkas, seleksi, hingga pengumuman hasil. Namun, seiring dengan kemajuan teknologi, ancaman keamanan siber juga meningkat secara signifikan, menyebabkan risiko bagi individu maupun organisasi (Hapsari, Pambayun, 2023). Kebocoran data dan serangan siber kini menjadi masalah global yang berdampak serius, mulai dari pencurian data hingga gangguan operasional dan kerusakan reputasi (Pitt, Apinento, e.t.c, 2023).

Penggunaan Aplikasi Web yang semakin tinggi meningkatkan perhatian pada keamanan Aplikasi Web (D. Yadav et al., 2018). Aplikasi Web sangat rentan terhadap serangan (S. Kumaret al., 2017). *Vulnerability Assessment* adalah langkah yang dapat dilakukan dalam menemukan kerentanan sebuah sistem termasuk Aplikasi Web. Vulnerability Assessment dapat dilakukan menggunakan sebuah *tool* berupa *Vulnerability Scanner* (E. I. Alwi & F. Umar, 2020) dan *Open Web Application Security Project Zed Attack Proxy* (OWASP ZAP) merupakan merupakan salah satunya.

Sebagai langkah antisipasi, perlu dilakukan langkah konkret untuk meningkatkan keamanan website PMB dan melindunginya dari serangan dimasa depan. OWASP (*Open Web Application Security Project*) telah menjadi acuan utama dalam pengujian keamanan aplikasi web (Riandhanu, 2022). Salah satu metode yang paling sering digunakan dalam keamanan aplikasi web yaitu *Vulnerability Assessment dan Penetration Testing* (VAPT), terdiri dari dua metode utama: penilaian kerentanan (VA) dan pengujian penetrasi (PT). VAPT memungkinkan identifikasi kerentanan keamanan secara komprehensif, yang kemudian diuji untuk mengeksploitasi kerentanan tersebut dan menilai seberapa rentan sistem terhadap serangan (Dwitawati, 2023). Panduan utama dalam VAPT adalah daftar OWASP Top 10, yang menyajikan rangkuman sepuluh vulnerabilitas paling umum yang kerap ditemukan pada aplikasi web. Kerentanan tersebut mencakup ancaman kritis seperti SQL *Injection*, XSS(*Cross-Site Scripting*) dan CSRF (*Cross- Site Request Forgery*) (Nurelasari, 2024).

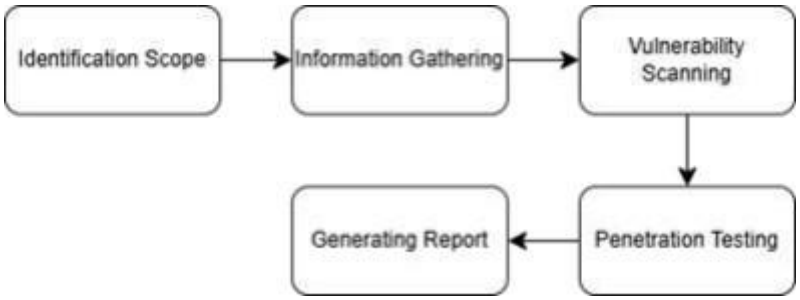
METODE PENELITIAN

Penelitian ini menerapkan metode *Vulnerability Assessmentdan Penetration Testing* (VAPT), yang berpedoman pada standar *Open Web Application Security Project*(OWASP). Metode VAPT adalah sebuah langkah evaluasi kerentanan pada sistem, jaringan, atau aplikasi serta pengujian kemampuan mereka untuk menghadapi potensi serangan dari pihak yang tidak berwenang (Andhika, 2024). Dengan penerapan VAPT, penelitian ini, berupaya untuk memberikan penilaian menyeluruh terkait tingkat keamanan sistem serta menyusun rekomendasi.

Perbaikan guna meningkatkan ketahanan terhadap ancaman siber. Menurut penelitian (Darmawan, 2021), metode VAPT unggul dalam mendeteksi dan menganalisis

ISSN 2338-3143
E-ISSN 2986-9951

kerentanan aplikasi web, serta memberikan langkah-langkah mitigasi yang efisien untuk memperkuat keamanan sistem. Berikut tahapan *Vulnerability Assessment* yang dilaksanakan dalam studi ini**.**



Gambar 1. Tahapan Penelitian

Metode Pengumpulan Data

Gambar 1 menunjukkan tahapan terstruktur dalam penerapan metode VAPT, mulai dari *Identification Scope* hingga *Generating Report* yang mencakup Rekomendasi keamanan. Setiap tahapan dirancang untuk memberikan pemahaman menyeluruh mengenai kondisi keamanan sistem yang diuji.

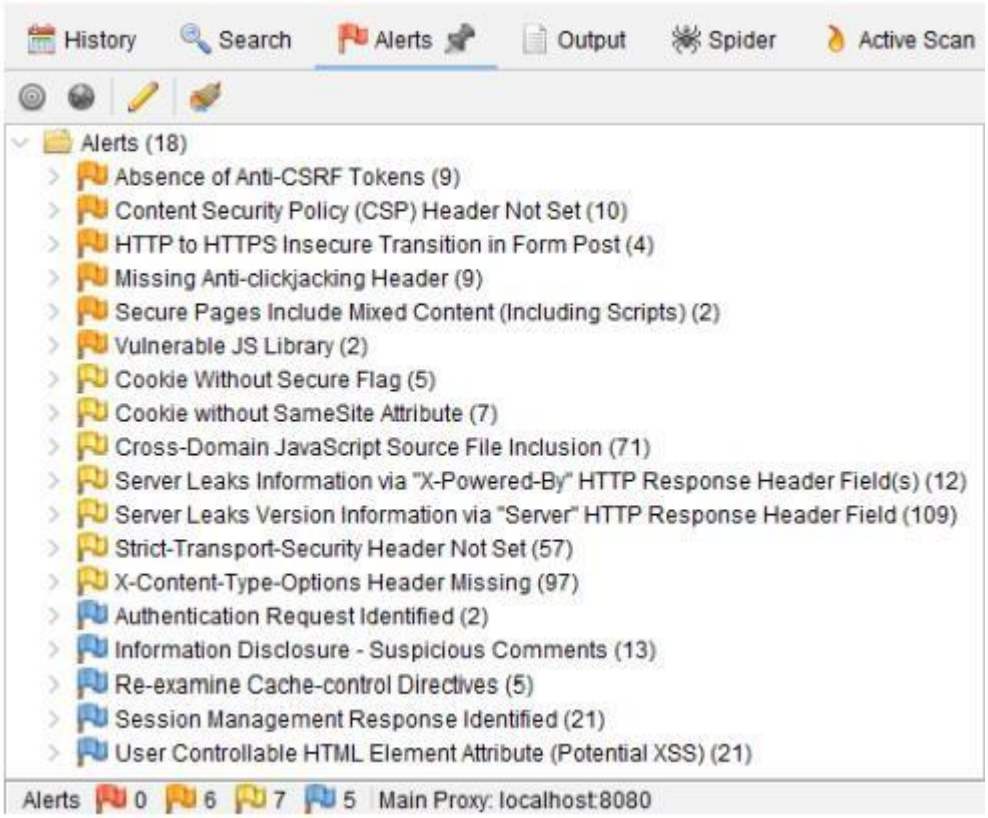
1. *Identification Scope*
   Pada tahap ini, ruang lingkup pengujian ditentukan dengan fokus pada halaman web utama website PMB. Batasan ini dilakukan untuk memastikan bahwa pengujian hanya mencakup area yang relevan dengan tujuan evaluasi keamanan situs web.
2. *Information Gathering*
   Tahap pengumpulan informasi bertujuan untuk mengidentifikasi teknologi yang digunakan oleh website PMB termasuk server, platform, dan layanan pendukung. Alat yang digunakan dalam tahap ini meliputi Whois untuk memperoleh informasi domain, Where is My IP untuk pengumpulan data publik dan Whatweb untuk identifikasi teknologi web.
3. *VulnerabilityScanning*
   Proses pemindaian kerentanan memanfaatkan OWASPZAP guna mendeteksi kemungkinan adanya celah keamanan pada situs web PMB.
4. *Penetration Testing (Eksploitasi)*
   Tahap ini bertujuan untuk memverifikasi apakah celah keamanan yang ditemukan dapat dieksploitasi oleh penyerang, serta untuk mengukur dampak potensial dari kerentanan tersebut. Peneliti tidak melakukan tahap ini karena alasan teknis
5. *GeneratingReport*
   Laporan akhir disusun berdasarkan hasil temuan, mencakup tingkatrisiko, serta rekomendasi langkah-langkah mitigasi yang diperlukan untuk meningkatkan keamanan website PMB.

ANALISI DAN PEMBAHASAN

Berdasarkan penelitian yang dilakukan oleh (Hasibuan, Handoko, 2023) menunjukkan bahwa penerapan *Vulnerability Assessment* (VA) dengan memanfaatkan panduan OWASP terbukti efektif dalam mengidentifikasi serta memitigasi risiko serangan siber pada aplikasi web. Panduan OWASP, seperti OWASP Top 10, memberikan kerangka yang jelas dan terstruktur untuk mengidentifikasi kerentanan utama yang sering

ditemukan pada aplikasi web. Penelitian ini selaras dengan temuan (Syarifudin, Setiyani, 2023), yang menekankan bahwa panduan OWASP, khususnya OWASP Top 10, harus dijadikan acuan utama dalam proses pengujian keamanan aplikasi web untuk memandu upaya mitigasi risiko secara efektif. Selain itu, dalam jurnal (Orisa, Ardita, 2021), menegaskan bahwa penilaian kerentanan merupakan langkah krusial dalam menjaga keamanan situs web. Hal tersebut terlihat dalam penelitian (Darojat, Setiyono, 2022) yang menekankan pentingnya penilaian kerentanan secara berkala guna melindungi informasi sensitif dan menjaga kepercayaan publik. Oleh sebab itu, penelitian ini menggunakan panduan OWASP sebagai acuan utama dalam mengevaluasi tingkat keamanan situs web PMB. Sasaran yang ingin dicapai dalam penelitian ini yaitu untuk mengidentifikasi kemungkinan adanya kerentanan di dalam sistem web PMB dan memberikan rekomendasi perbaikan yang sesuai, berdasarkan standar keamanan yang telah ditetapkanpembahasan ini, penulis akan mengimplementasikan tahapan *Vulnerability Assessmentdan Penetration Testing*(VAPT) yang terdiri dari:

1. ***InformationGathering***
   Proses pengumpulan informasi dilaksanakan dengan menggunakan beberapa *tools*, yaitu Whois, Whereis My IP dan Whatweb, untuk mengidentifikasi informasi penting terkait infrastruktur sistem yang diuji. Dari hasil pemindaian, diperoleh data yang mencakup alamat IP, subdomain, port yang terbuka, layanan yang berjalan, serta teknologi web yang digunakan oleh server. Selain itu, informasi mengenai registrasi domain, seperti domain, penyedia layanan, dan nama server juga berhasil diidentifikasi. Hasil pengumpulan informasi ini memberikan gambaran menyeluruh mengenai konfigurasi jaringan dan teknologi yang digunakan dalam sistem. Data ini menjadi landasan penting dalam analisis kerentanan lebih lanjut dan memudahkan dalam tahap pemindaian kerentanan ditahap selanjutnya.
2. ***Vulnerability Scanning***
   Pemindaian kerentanan dilaksanakan dengan tujuan untuk mengidentifikasi celah keretanan pada situs web PMB. Tools yang digunakan dalam tahapan ini adalah OWASPZAP.



Gambar 2. Hasil Scanning OWASPZAP berdasarkan Risiko dan Confidence

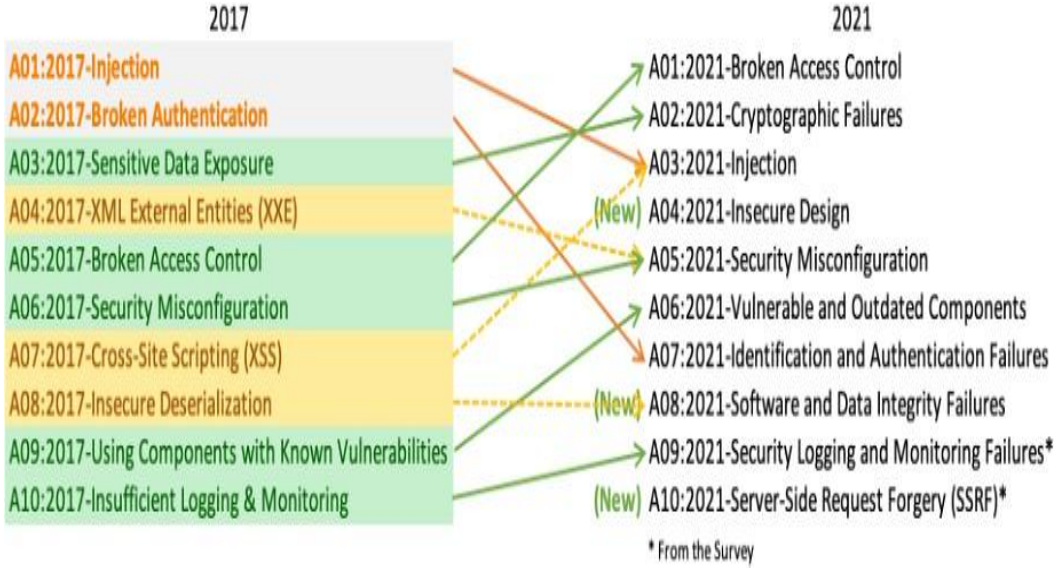
Berdasarkan Gambar 2 di atas, pemindaian kerentanan situs web PMB, mengidentifikasi total 18 kerentanan. Dari sisi risk, terdapat 6 kerentanan dengan risiko menengah (33%), 7 kerentanan dengan risiko rendah (38%), dan 5 kerentanan bersifat informatif (27%).

Tabel 1. Daftar Kerentanan dari hasil *Vulnerability Asseement*

No	Alert	Risk
1	Absence of Anti CSRF Token (9)	Medium
2	Content Security Policy (CSP) Header not Set (10)	Medium
3	HTTP to HTTPS Insecure Transition in Form Post (4)	Medium
4	Missing Anti-click jacking Header (9)	Medium
5	Secure Pages Include Mixed Content(Including Script) (2)	Medium
6	Vulnerable JS Library (2)	Medium
7	Cookie Without Secure Flag (5)	Low
8	Cookie Without SameSite Attribute (7)	Low
9	Cross-Domain JavaScript Source File Inclussion (71)	Low
10	Server Leaks Information via "X-Powered-By" HTTP Response Header Fileds (12)	Low
11	Server leaks version information via "server" HTTP Response Header Field (109)	Low
12	Strict- Transport- Security Header Not Set (57)	Low
13	X- Content- Type -Options Header Missing (97)	Low
14	Authentication Request Identified (2)	Informational
15	Information Disclosure - Suspicious Comment (13)	Informational

16	Re-examine Cache-control Directive (5)	Informational
17	Session Management Response Identified (21)	Informational
18	User Controllable HTML Element Attribute (Potential XSS) (21)	Informational

Kerentanan-kerentanan ini memiliki relevansi yang kuat dengan beberapa kategori yang diidentifikasi dalam OWASP Top 10 2021. OWASP Top 10 adalah proyek dari *Open Web Application Security Project* yang bertujuan mengidentifikasi dan mengklasifikasikan risiko keamanan aplikasi web yang paling umum. Daftar ini diperbarui secara berkala untuk mencerminkan tren terbaru dalam dunia keamanan siber.



Gambar 3. Perbandingan OWASP Top 10 2017 dan 2021

Tabel 2. Kerentanan yang ditemukan pada Web PMB yang masuk dalam list OWASP Top 10 2021

No	Alert	Risk
1	Broken Access Control	Medium
2	Cryptographic Failures	Medium dan Informational
3	Injection	Tidak ditemukan
4	Insecure Design	Medium
5	Security Misconfiguration	Medium dan Informational
6	Vulnerable and Outdated Component	Tidak ditemukan
7	Identification and Authentication Failures	Low
8	Software and Data Integrity Failures	Tidak ditemukan
9	Security Logging and Monitoring Failures	Medium
10	Server-Side Request Forgery	Medium

Berdasarkan Tabel 2 diatas, kerentanan-kerentanan yang ditemukan memiliki relevansi yang kuat dengan beberapa kategori yang diidentifikasi dalam OWASP Top 10 2021. Kerentanan tersebut mencakup:

1. *Absence of Anti-CSRF Tokens*
   Situs web PMB belum mengimplementasikan mekanisme token anti-CSRF, yang merupakan langkah penting dalam mencegah serangan *Cross-Site Request Forgery* (CSRF). Serangan ini memungkinkan penyerang memanfaatkan sesi autentikasi pengguna untuk melakukan tindakan yang tidak sah. Kerentanan ini dikaitkan dengan A01:*Broken Access Control* dan memiliki tingkat risiko sedang.
2. *Content Security Policy (CSP) Header Not Set*
   Situs web PMB belum menerapkan Content Security Policy (CSP), yang merupakan mekanisme esensial dalam melindungi aplikasi web dari serangan Cross-Site Scripting (XSS). Kerentanan tersebut terkait dengan A05: *Security Misconfiguration* dan dinilai memiliki tingkat risiko sedang.
3. *HTTP to HTTPS Insecure Transition in Form Post*
   Merupakan sebuah kerentanan keamanan web yang terjadi ketika sebuah halaman web yang tidak aman (HTTP) mengirimkan data ke halaman web yang aman (HTTPS). Hal ini dapat menyebabkan data yang dikirimkan melalui formulir tersebut dapat diintersep oleh penyerang melalui serangan *Man-in-the-Middle* (MITM). Kerentanan ini dapat terjadi karena browser tidak secara otomatis mengalihkan koneksi ke HTTPS ketika pengguna mengklik tombol submit pada formulir. Hal ini dapat menyebabkan data yang dikirimkan melalui formulir tersebut dapat diintersep oleh penyerang yang berada di antara pengguna dan server web.
4. *Missing Anti-Clickjacking Header*
   Situs web PMB belum menerapkan header anti Clickjacking, yang berfungsi melindungi aplikasi dari serangan Clickjacking dengan mencegah pemuatan halaman dalam iframe oleh situs lain. Kerentanan ini dikaitkan dengan A05: Security Misconfiguration dan memiliki tingkat risiko sedang.
5. *Secure Pages Include Mixed Content(Including Script)*
   Berarti sebuah halaman web yang diakses melalui protokol HTTPS (secure) memuat konten yang diakses melalui protokol HTTP (*non-secure*). Konten ini bisa berupa gambar, skrip, atau *stylesheet*. Ancaman keamanan yang mungkin muncul adalah *Man-in-the-middle* (MitM) *attacks* (Penyerang dapat mengintersep dan memodifikasi data yang dikirimkan melalui koneksi HTTP yang tidak aman) dan adanya serangan *data interception* (data yang dikirimkan melalui koneksi HTTP dapat dengan mudah diintersep oleh pihak ketiga yang tidak berwenang).

6. *Vulnerable JS Library*
   Kerentanan yang ada pada JS Library memungkinkan terjadinya serangan XSS (*Cross-Site Scripting*) yang memungkinkan penyerang menyuntikkan kode berbahaya ke dalam halaman web. Selain itu juga berpotensi terjadinya Bug pada sistem (Kode yang tidak sempurna dapat menyebabkan perilaku yang tidak terduga atau bahkan membuat aplikasi *crash*). Serangan lain yang mungkin terjadi karena kerentana pada JS Library adalah *backdoor* (beberapa JS Library ada yang mengandung kode yang sengaja dibuat untuk memberikan akses tidak sah kepada pihak ketiga).
7. *Cookie Without Secure Flag*
   Merupakan sebuah cookie yang tidak memiliki atribut *Secure* yang ditetapkan. Atribut *Secure* adalah sebuah mekanisme keamanan yang digunakan untuk membatasi pengiriman cookie hanya melalui koneksi HTTPS yang terenkripsi. Jika sebuah cookie tidak memiliki atribut *Secure*, maka cookie tersebut dapat dikirimkan melalui koneksi HTTP, bahkan jika pengguna sedang mengakses situs web melalui koneksi HTTPS. Hal ini membuat cookie rentan terhadap serangan man-in-the-middle (MitM) di mana penyerang dapat mengintersep dan memodifikasi data yang dikirimkan antara browser dan server.
8. *Cookie Without SameSite Attribute*
   Merupakan kerentanan karena cookie yang tidak memiliki atribut SameSite yang ditetapkan. Atribut SameSite adalah sebuah mekanisme keamanan yang digunakan untuk membatasi pengiriman cookie lintas situs, sehingga dapat membantu mencegah serangan CSRF *(Cross-Site Request Forgery*). Sebelum adanya atribut SameSite, cookie secara default akan dikirim dalam semua permintaan, termasuk permintaan lintas situs. Hal ini membuat cookie rentan terhadap serangan CSRF.
9. *Cross-Domain JavaScript Source File Inclussion*
   Merupakan sebuah kerentanan keamanan dalam aplikasi web yang memungkinkan penyerang menyuntikkan kode JavaScript berbahaya dari domain lain ke dalam aplikasi Anda. Dampak kerentanan jika di biarkan Penyerang dapat menjalankan kode JavaScript berbahaya di browser pengguna, yang dapat menyebabkan berbagai masalah seperti: Pencurian data sensitif (seperti cookie, token autentikasi); Perubahan tampilan dan perilaku situs web; Pengalihan pengguna ke situs web berbahaya; dan penyebaran malware.
   Escalation Privilege: Dalam beberapa kasus, penyerang dapat mengeksploitasi kerentanan ini untuk mendapatkan akses yang lebih tinggi ke sistem atau jaringan.
10. *Server Leaks Information via X-Powered-By HTTP respons Header Field*
    Header X-Powered-By secara eksplisit mengungkapkan teknologi serta versi server yang digunakan, seperti PHP atau framework web tertentu. Keterbukaan informasi ini dapat memberikan peluang bagi pihak yang tidak bertanggung jawab untuk mengeksploitasi potensi kerentanan pada server. Kerentanan ini terkait dengan A01: Broken Access Control dan dinilai memiliki tingkat risiko rendah.
11. *Server leaks version information via "server" HTTP Response Header Field*
    Kerentana yang terjadi saat seorang pengguna internet mengunjungi sebuah website dan server akan mengirimkan informasi tentang dirinya, termasuk jenis dan versi software yang digunakan. Informasi ini disebut sebagai "header HTTP". Kerentanan ini dapat mengundang serangan, jika seorang hacker mengetahui jenis dan versi server yang digunakan, mereka bisa mencari tahu celah keamanan yang spesifik untuk mengeksploitasi server tersebut. Dan kerentanan ini juga memudahkan serangan, karena Informasi versi server bisa membantu hacker memilih metode serangan yang paling efektif.

12. *Strict-Transport-Security Header Not Set*
    Ketiadaan Header Strict Transport Security (HSTS) pada situs web PMB menunjukkan bahwa situs tersebut belum memastikan penggunaan protokol HTTPS secara konsisten dalam komunikasi. Ketiadaan HSTS membuat situs ini rentan terhadap serangan downgrade dan sniffing. Kerentanan ini terkait dengan A05: Security Misconfiguration dan dikategorikan memiliki tingkat risiko rendah.
13. *X- Content- Type -Options Header Missing*
    Ketiadaan header X-Content-Type-Options pada situs web PMB memungkinkan peramban untuk melakukan penyelidikan tipe MIME, yang berpotensi dieksploitasi dalam serangan akibat kesalahan penanganan konten. Kerentanan ini terkait dengan kategori A05:Security Misconfiguration dan memiliki tingkat risiko rendah.
14. *Authentication Request Identified*
    Kerentanan tersebut berarti adanya kelemahan dalam sistem keamanan yang memungkinkan seseorang untuk mengidentifikasi adanya permintaan autentikasi. Ini seperti seseorang mengintip kunci rumah Anda ketika Anda mencoba membukanya.
15. *Information Disclosure – Suspicious Comment*
    Komentar dalam kode sumber situs web PMB yang mencurigakan dapat mengungkapkan informasi tambahan terkait aplikasi yang berpotensi memberikan keuntungan bagi penyerang. Kerentanan ini terkait dengan kategori A01: Broken Access Control dan dianggap sebagai kerentanan dengan tingkat risiko informasi.
16. *Re-examine Cache-control Directive*
    Kesalahan dalam pengaturan kontrol cache pada situs web PMB dapat menyebabkan penyimpanan data sensitif di dalam cache, yang jika tidak dikelola dengan baik dapat memungkinkan akses tidak sah oleh pihak ketiga.
17. *Session Management Response Identified*
    Kerentanan ini menunjukkan adanya kelemahan dalam sistem pengelolaan sesi yang memungkinkan penyerang mengidentifikasi atau memanfaatkan informasi terkait sesi pengguna. Serangan yang mungkin terjadi adalah hijacking Sesi: Penyerang bisa mencuri informasi sesi dan kemudian menyamar menjadi untuk melakukan tindakan- tindakan yang tidak sah, seperti mengakses data sensitif atau melakukan transaksi. Serangan kedua yang mungkin terjadi adalah fixation sesi: Penyerang bisa memaksa Anda untuk menggunakan sesi yang telah dibuat sebelumnya, sehingga mereka bisa melacak aktivitas Anda atau bahkan mengambil alih akun pengguna.
18. *User Controllable HTML Element Attribute (Potential XSS)*
    Kerentanan tersebut berartti adanya kelemahan dalam sebuah aplikasi web yang memungkinkan pengguna memasukkan data yang kemudian secara langsung dimasukkan ke dalam kode HTML tanpa melalui proses pembersihan atau pengamanan yang cukup. Hal ini bisa dimanfaatkan oleh penyerang untuk menyuntikkan kode jahat (misalnya, JavaScript) ke dalam halaman web. Serangan XSS bisa digunakan untuk mencuri informasi pribadi (penyerang bisa mencuri cookie sesi, token autentikasi, atau informasi sensitif lainnya dari pengguna, mengalihkan pengguna ke situs web berbahaya), penyerang bisa mengarahkan pengguna ke situs web yang berisi malware atau phishing; merusak tampilan websit (penyerang bisa mengubah tampilan website sehingga menjadi tidak berfungsi atau menampilkan konten yang tidak pantas).

ISSN 2338-3143
E-ISSN 2986-9951

3. Generating Report

Berdasarkan hasil pemindaian dan pengujian kerentanan situs web PMB menggunakan OWASPZAP mengidentifikasi sejumlah kerentanan yang memerlukan perbaikan. Tabel 3 berikut merangkum kerentanan, tingkat risiko, dan rekomendasi mitigasi yang relevan.

Tabel 3. Rekomendasi Keamanan

No	Kerentanan	Tingkat Resiko	Rekomendasi Perbaikan
1	Absence of Anti CSRF Token	Medium	Menggunakan framework yang sudah terverifikasi dalam mengatasi serangan *Cross-Site Request Forgery* (CSRF).
2	Content Security Policy (CSP) Header not Set	Medium	Konfigurasi CSP (Content Security Policy) untuk membatasi sumber daya yang diizinkan untuk dimuat oleh browser.
3	HTTP to HTTPS Insecure Transition in Form Post	Medium	Semua halaman web yang mengandung formulir harus diakses melalui HTTPS
4	Missing Anti-click jacking Header	Medium	Tambahkan X-Frame-Options atau Content Security-Policy untuk mencegah serangan *Clickjacking.*
5	Secure Pages Include Mixed Content(Including Script)	Medium	Ganti semua URL yang menggunakan HTTP menjadi HTTPS untuk semua sumber daya, termasuk gambar, skrip, dan stylesheet.
6	Vulnerable JS Library	Medium	Selalu gunakan versi terbaru; Lakukan audit keamanan secara berkala, Gunakan alat analisis keamanan untuk melakukan pengecekan kerentanan
7	Cookie Without Secure Flag	Low	Selalu Tetapkan Atribut Secure; Gunakan HTTPS
8	Cookie Without SameSite Attribute	Low	Selalu tetapkan atribut SameSite; Gunakan nilai SameSite yang sesuai
9	Cross-Domain JavaScript Source File Inclussion	Low	Hindari Pemuatan Skrip Dinamis; Validasi Input; Gunakan Content Security Policy (CSP); Perbarui Perangkat Lunak
10	Server Leaks Information via "X-Powered-By" HTTP Response Header Fileds	Low	Hapus atau sembunyikan Header XPowered-By untuk menghindari pengungkapan informasi server kepada penyerang
11	Server leaks version information via "server" HTTP Response Header Field	Low	Sembunyikan Informasi Versi; Perbarui Server; Gunakan Firewall:
12	Strict- Transport- Security Header Not Set	Low	Terapkan Header Strict-Transport-Security untuk memastikan semua komunikasi menggunakan HTTPS.
13	X- Content- Type -Options Header Missing	Low	Tambahkan Header X-Content-TypeOptions digunakan guna mencegah serangan MIME Sniffing

14	Authentication Request Identified	Informational	Sembunyikan Informasi; Gunakan CAPTCHA; Batasi Percobaan Login: Gunakan Protokol Autentikasi yang Kuat; Pantau Aktivitas Login
15	Information Disclosure - Suspicious Comment	Informational	Hapus komentar kode yang mencurigakan atau yang mengandung informasi sensitif pada aplikasi
16	Re-examine Cache-control Directive	Informational	Optimalkan direktif cache-control untuk mencegah penyimpanan data sensitif pada klien.
17	Session Management Response Identified	Informational	Gunakan Cookie yang Aman; Gunakan Token Sesi yang Kuat; Lindungi dari XSS: Gunakan HTTPS:.Implementasikan Session Timeouts.
18	User Controllable HTML Element Attribute (Potential XSS)	Informational	Validasi input; Encoding; Gunakan library atau framework yang aman: Perbarui aplikasi web secara teratur

PENUTUP

Kesimpulan

Berdasarkan hasil Vulnerability Assessment pada situs web PMB, ditemukan total 18 kerentanan yang terdiri dari 6 vulnerabilitas yangmemiliki risiko menengah, 7 vulnerabilitas yang memiliki risiko rendah, serta 5 vulnerabilitas informatif. Kerentanan berisiko menengah memerlukan perhatian prioritas dalam upaya perbaikan. Secara keseluruhan, meskipun aspek keamanan sudah cukup terjaga, perbaikan lebih lanjut tetap diperlukan, terutama untuk menangani kerentanan dengan risiko menengah dan meningkatkan perlindungan terhadap serangan Clickjacking.

DAFTAR PUSTAKA

Andhika, “Mengenal Vulnerability Assessment and Penetration Testing (VAPT): Apa itu dan Mengapa Penting?,” Fourtrezz, 2023. Accessed: Aug. 03, 2024. [Online]. Available: https://fourtrezz.co.id/mengenal-vulnerability-assessment-and-penetration-testing-vapt- apa-itu-dan-mengapa-penting/

A. F. Hasibuan and D. Handoko, “Analisis Keretanan Website Dengan Aplikasi Owasp Zap,” Jurnal Ilmu Komputer dan Sistem Informasi, vol. 2, no. 2, pp. 257–270,2023, [Online]. Available: https://jurnal.unityacademy.sch.id/index.php/jirsi/article/view/51

A. Syarifuddin Syahab, “Analisis Audit Keamanan Informasi Website Dari Drown Attack Menggunakan Network Mapper Dan Qualys Ssl,” Jurnal Manajemen Informatika & Sistem Informasi (MISI), vol. 6, no. 1, 2023, doi: 10.36595/misi.v5i2.

C. Darmawan, J. P. P. Naibaho, and A. De Kweldju, “Penerapan Metode Vulnerability Assessment untuk Identifikasi Keamanan Website berdasarkan OWASP ID Tahun 2021,” Edumatic: Jurnal Pendidikan Informatika, vol. 8, no. 1, pp. 272–281, Jun. 2024, doi: 10.29408/edumatic.v8i1.25834.

D. A. Rabbani, "Pengaruh Perkembangan Teknologi terhadap Kehidupan dan Interaksi Sosial Masyarakat Indonesia," 2023. [Online]. Available: https://www.researchgate.net/publication/375525102

Dedi Supriadi1*,Emi Suryadi2, Rudi Muslim3, Lalu DelsiSamsumar41,2,3,4Universitas Teknologi Mataram, Indonesia Journal of Data Analytics, Information, and Computer Science (JDAICS)Volume 1, No 4–Oktober 2024e-ISSN : 3032-4696 Hal. 232 Implementasi Vulnerability Assessment Owasp (Open Web Application Security Project) Pada Websiteuniversitas Teknologi Mataram

D. Yadav, D. Gupta & D. Singh (2018). Vulnerabilities and Security of Web Applications.

E. Nurelasari, D. Gumilang, and A. Farabi, "Analisis Keamanan Sistem Website Menggunakan Metode Open Web Application Security Project (Owasp)Pada Simantep.Id," 2024.

E. Irawadi Alwi & F. Umar (2020). Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning.

E. Z. Darojat, E. Sediyono, and I. Sembiring, "Vulnerability Assessment Website EGovernment dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner," JURNAL SISTEM INFORMASI BISNIS, vol. 12, no. 1, pp. 36– 44, Sep. 2022, doi: 10.21456/vol12iss1pp36-44

I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," Jurnal Informasi dan Teknologi, Oct. 2022, doi: 10.37034/jidt.v4i3.236

Mira Orisa and M. Ardita, "Vulnerability Assesment Untuk Meningkatkan Kualitas Kemanan Web," Jurnal Mnemonic, vol. 4, no. 1, pp. 16–19, 2021, doi: 10.36040/mnemonic.v4i1.3213.

N. A. Syarifudin and L. Setiyani, "Analysis of Higher Education SIAKAD Website Security Gaps Using the Vulnerability Assessment Method," International Journal of Multidisciplinary Approach Research and Science, vol. 1, no. 03, pp. 332–344, Aug. 2023, doi: 10.59653/ijmars.v1i03.177

R. D. Hapsari and K. G. Pambayun, "ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis," Jurnal Konstituen, vol. 5, no. 1, pp. 1–17, Oct. 2023, doi: 10.33701/jk.v5i1.3208.

S. Kumar, et al. (2017). A Study on Web Application Security and Detecting Security Vulnerabilities

.