Journal of Data Analytics, Information, and Computer Science (JDAICS)
Volume 1, No 4 – Oktober 2024
e-ISSN : 3032-4696

IMPLEMENTASI VULNERABILITY ASSESSMENT OWASP (OPEN WEB APPLICATION SECURITY PROJECT) PADA WEBSITE UNIVERSITAS TEKNOLOGI MATARAM

Dedi Supriadi[1]*, Emi Suryadi[2], Rudi Muslim[3], Lalu Delsi Samsumar[4]
[1,2,3,4]Universitas Teknologi Mataram, Indonesia
[1]dedisupriadi011002@gmail.com ,[2]emisuryadi@gmail.com
[3]rudimuslim93@gmai.com, [4] samsumarld@utmmataram.ac.id

Received: 08-10- 2024	Revised: 20-10-2024	Approved: 25-10-2024

ABSTRACT

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 Universitas Teknologi Mataram 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, eksploitasi celah, serta pembuatan laporan. Tools yang digunakan antara lain OWASPZAP dan Burp Suite untuk mendeteksi dan pengujian kerentanan. Penelitian ini menghasilkan laporan yang mengidentifikasi tiga kerentanan dengan level sedang, empat kerentanan dengan level rendah, serta tidak ada kerentanan dengan level tinggi. Setelah pemindaian, hasil pengujian menunjukkan bahwa serangan Clickjacking berhasil dieksploitasi, sementara serangan XSS tidak berhasil dilakukan, menunjukkan adanya mekanisme pertahanan yang baik terhadap XSS. Selain itu, ditemukan beberapa kelemahan dalam konfigurasi aplikasi. Solusi perbaikan yang direkomendasikan disesuaikan dengan standar keamanan OWASP. Dengan dilakukannya VAPT ini, diharapkan pengelola website Universitas Teknologi Mataram dapat meningkatkan keamanan dan mengurangi risiko serangan siber yang berpotensi merugikan. Implementasi OWASP sebagai panduan pengujian keamanan terbukti efisien dalam mendeteksi serta mengatasi celah keamanan dalam aplikasi web.

Kata kunci: Vulnerability Assessment, *Penetration Testing*, *OWASP*, *Website Application Security*, *Cybersecurity*.

PENDAHULUAN

Teknologi informasi dan komunikasi mengalami peningkatan signifikan selama beberapa dekade terakhir, mempengaruhi berbagai aspek kehidupan, termasuk cara kita bekerja, berkomunikasi, serta mengakses informasi [1]. 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 [2]. Di dunia pendidikan, sistem informasi akademik telah menjadi solusi penting dalam pengelolaan data mahasiswa dan administrasi, seperti yang diterapkan oleh Universitas Teknologi Mataram (UTM). Namun, seiring dengan kemajuan teknologi, ancaman keamanan siber juga meningkat secara signifikan, menyebabkan risiko bagi individu maupun organisasi [3]. Kebocoran data dan serangan siber kini menjadi masalah global yang berdampak serius, mulai dari pencurian data hingga gangguan operasional dan kerusakan reputasi [4].

Situs web Universitas Teknologi Mataram (UTM) pernah menjadi target serangan siber, di mana penyerang berhasil mengubah tampilan utama situs dengan menampilkan pesan yang tidak sesuai [5], sehingga mencoreng citra profesional universitas dan

merusak kepercayaan publik [6]. Celah keamanan yang dieksploitasi oleh penyerang ini sebagian besar disebabkan oleh kurangnya pemantauan serta perlindungan sistem yang memadai. Oleh karena itu, perlu dilakukan langkah konkret untuk meningkatkan keamanan website UTM dan melindunginya dari serangan dimasa depan.

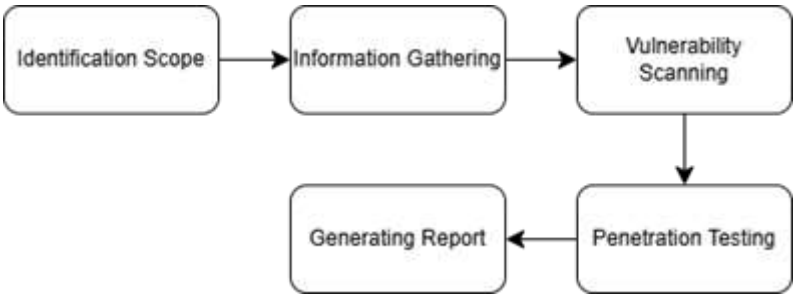
OWASP (Open Web Application Security Project) telah menjadi acuan utama dalam pengujian keamanan aplikasi web [7]. Salah satu metode yang paling sering digunakan dalam keamanan aplikasi web yaitu *Vulnerability Assessment* dan *Penetration Testing (VAPT),* terdiri dari dua metode utama: penilaian kerentanan *(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 [8].

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)* [9]. Berdasarkan penelitian yang dilakukan oleh [10] 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 [11], 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 [12] menegaskan bahwa penilaian kerentanan merupakan langkah krusial dalam menjaga keamanan situs web. Hal tersebut terlihat dalam penelitian [13], 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 Universitas Teknologi Mataram (UTM) sasaran yang ingin dicapai dalam penelitian ini yaitu untuk mengidentifikasi kemungkinan adanya kerentanan di dalam sistem web universitas dan memberikan rekomendasi perbaikan yang sesuai, berdasarkan standar keamanan yang telah ditetapkan.

METODE PENELITIAN

Penelitian ini menerapkan metode *Vulnerability Assessment* dan *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 [14]. 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 [15], metode VAPT unggul dalam mendeteksi dan menganalisis kerentanan aplikasi web, serta memberikan langkah-langkah mitigasi yang efisien untuk memperkuat keamanan sistem.

Berikut tahapan *Vulnerability Assessment dan Penetration Testing (VAPT)* yang dilaksanakan dalam studi ini.



Gambar 1. Tahapan Penelitian

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* UTM. 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 UTM, termasuk server, platform, dan layanan pendukung. Alat yang digunakan dalam tahap ini meliputi *Whois* untuk memperoleh informasi domain, *TheHarvester* untuk pengumpulan data publik, *Nmap* untuk pemetaan jaringan, dan *Whatweb* untuk identifikasi teknologi web.
3. *Vulnerability Scanning*
   Proses pemindaian kerentanan memanfaatkan OWASPZAP guna mendeteksi kemungkinan adanya celah keamanan pada situs web UTM.
4. Eksploitasi
   Tahap ini bertujuan untuk memverifikasi apakah celah keamanan yang ditemukan dapat dieksploitasi oleh penyerang, serta untuk mengukur dampak potensial dari kerentanan tersebut.
5. *Generating Report*
   Laporan akhir disusun berdasarkan hasil temuan, mencakup tingkat risiko, serta rekomendasi langkah-langkah mitigasi yang diperlukan untuk meningkatkan keamanan website UTM.

HASIL DAN PEMBAHASAN

Di bagian hasil dan pembahasan ini, penulis akan mengimplementasikan tahapan *Vulnerability Assessment* dan *Penetration Testing* (VAPT) yang terdiri dari:

Information Gathering

Proses pengumpulan informasi dilaksanakan dengan menggunakan beberapa alat, yaitu *Nmap*, *TheHarvester*, *Whois*, dan *Whatweb*, untuk mengidentifikasi informasi penting terkait infrastruktur sistem yang diuji. Dari hasil pemindaian, diperoleh data yang mencakup alamat IP, *sub domain*, *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 di tahap selanjutnya.

Vulnerability Scanning

Pemindaian kerentanan dilaksanakan dengan tujuan untuk mengidentifikasi celah perlindungan pada situs web UTM. Alat yang digunakan dalam tahapan ini adalah OWASPZAP.

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (9.1%)	1 (9.1%)	1 (9.1%)	3 (27.3%)
	Low	0 (0.0%)	1 (9.1%)	2 (18.2%)	1 (9.1%)	4 (36.4%)
	Informational	0 (0.0%)	0 (0.0%)	2 (18.2%)	2 (18.2%)	4 (36.4%)
	Total	0 (0.0%)	2 (18.2%)	5 (45.5%)	4 (36.4%)	11 (100%)

Gambar 2. Hasil Scanning OWASPZAP berdasarkan Risiko dan Confidence

Berdasarkan Gambar 2 di atas, pemindaian kerentanan situs web Universitas Teknologi Mataram mengidentifikasi total 11 kerentanan. Dari sisi *risk*, terdapat 3 kerentanan dengan risiko menengah, 4 dengan risiko rendah, dan 4 kerentanan bersifat informatif. Berdasarkan *Confidence* level, 2 kerentanan dikategorikan dengan keyakinan tinggi, 5 dengan keyakinan menengah, dan 4 dengan keyakinan rendah. Daftar kerentanan tersebut ditunjukkan dalam tabel 1 dibawah ini.

Tabel 1. Daftar Kerentanan

No.	***Alert***	***Risk***
1	*Absence of Anti-CSRF Tokens*	*Medium*
2	*Content Security Policy (CSP) Header Not Set*	*Medium*
3	*Missing Anti-Clickjacking Header*	*Medium*
4	*Server Leaks Information via X-Powered-By HTTP respons Header Field*	*Low*
5	*Strict-Transport-Security Header Not Set*	*Low*
6	*Timestamp Disclosure – Unix*	*Low*
7	*X-Content-Type-Options Header Missing*	*Low*
8	*Information Disclosure – Suspicious Comment*	*Informational*
9	*Modern Web Application*	*Informational*
10	*Re-examine Cache-control Directives*	*Informational*
11	*User Agent Fuzzer*	*Informational*

Kerentanan-kerentanan ini 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 Universitas Teknologi Mataram 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 Universitas Teknologi Mataram 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. ***Missing Anti-Clickjacking Header***
   Situs web Universitas Teknologi Mataram 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
4. ***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.
5. ***Strict-Transport-Security Header Not Set***
   Ketiadaan *Header Strict Transport Security (HSTS)* pada situs web Universitas Teknologi Mataram 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.
6. ***Timestamp Disclosure – Unix***
   Berdasarkan analisis terhadap sistem di Universitas Teknologi Mataram (UTM), pengungkapan *Timestamp – Unix* dalam aplikasi dapat mengungkapkan informasi waktu, pada sistem server, yang berpotensi dimanfaatkan oleh penyerang untuk melancarkan serangan atau mengidentifikasi versi perangkat lunak yang digunakan. Kerentanan ini dikategorikan dalam *A01: Broken Access Control* dan dinilai memiliki tingkat risiko rendah.
7. ***X-Content-Type-Options Header Missing***
   Ketiadaan *header X-Content-Type-Options* pada situs web Universitas Teknologi Mataram (UTM) 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.

8. ***Information Disclosure – Suspicious Comment***
   Komentar dalam kode sumber situs web Universitas Teknologi Mataram (UTM) 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.
9. ***Modern Web Application***
   Kerentanan dalam praktik pengembangan web modern , termasuk pada situs web Universitas Teknologi Mataram (UTM), sering kali berkaitan dengan aspek keamanan dan manajemen konfigurasi yang memerlukan evaluasi ulang untuk memastikan integritas sistem.
10. ***Re-examine Cache-control Directives***
    Kesalahan dalam pengaturan kontrol *cache* pada situs web Universitas Teknologi Mataram (UTM) dapat menyebabkan penyimpanan data sensitif di dalam *cache*, yang jika tidak dikelola dengan baik dapat memungkinkan akses tidak sah oleh pihak ketiga.
11. ***User Agent Fuzzer***
    Penggunaan alat *fuzzing* yang tidak efektif pada *Header User-Agent* di situs web Universitas Teknologi Mataram (UTM) dapat memungkinkan penyerang mengidentifikasi kerentanan atau menguji keandalan mekanisme pertahanan aplikasi melalui manipulasi *Header User-Agent.*

Eksploitasi

1. ***Clickjacking***

Berdasarkan hasil analisis yang dilakukan pada website Universitas Teknologi Mataram (UTM), ditemukan adanya kerentanan berjenis *Missing Anti Clickjacking Header*. Kerentanan ini disebabkan oleh tidak adanya konfigurasi *X-Frame-Options* dalam respons server, yang berfungsi untuk melindungi situs web dari serangan *Clickjacking*. *Clickjacking* merupakan metode penyerangan yang memungkinkan penyerang untuk menipu pengguna agar melakukan klik pada elemen halaman web tanpa disadari, umumnya dengan memanfaatkan *frame* transparan untuk menyembunyikan konten asli.

Untuk memvalidasi kerentanan ini, dilakukan pengujian serangan Clickjacking menggunakan Burp Suite. Langkah pengujian dimulai dengan mengaktifkan mode *intercept* dan menkonfigurasi peramban agar menggunakan HTTP Proxy dengan IP 127.0.0.1 port 8080. Setelah proses *intercept* berhasil dilakukan, *plugin* Burp *Clickbandit* digunakan untuk menghasilkan skrip serangan *Clickjacking*. Skrip ini kemudian diimplementasikan pada situs web target melalui fitur *Developer Tool* pada peramban, khususnya menggunakan konsol. Hasil dari pengujian menunjukkan bahwa situs web UTM rentan terhadap serangan *Clickjacking*, dimana penyerang dapat memanipulasi tindakan pengguna tanpa sepengetahuan mereka. Seperti Gambar 3.

Temuan ini menunjukkan bahwa tidak adanya *X-Frame-Options* dalam konfigurasi server situs web UTM meningkatkan risiko terjadinya serangan *Clickjacking*, yang memungkinkan penyerang untuk mengeksploitasi kerentanan ini guna memanipulasi interaksi pengguna di situs web tersebut.

Oleh karena itu, untuk memitigasi risiko ini, disarankan agar server web UTM segera menerapkan X-Frame-Options yang sesuai. Selain itu, penggunaan kebijakan tambahan seperti *Content Security Policy (CSP)* dapat memberikan lapisan perlindungan lebih lanjut untuk mencegah eksploitasi lebih lanjut dari kerentanan serupa dan melindungi situs web UTM dari ancaman lainnya yang bersifat dinamis dan berbahaya.

2. ***Cross-Site Scripting (XSS)***

Pada pengujian keamanan yang dilakukan terhadap situs web Universitas Teknologi Mataram (UTM), ditemukan bahwa *Content Security Policy (CSP)* tidak diimplementasikan. Ketiadaan CSP berpotensi membuka celah keamanan bagi serangan *XSS (Cross-Site Scripting),* dimana pihak yang tidak bertanggung jawab dapat menyuntikkan skrip berisiko ke dalam situs web melalui input user atau manipulasi URL, guna menguji potensi kerentanan ini, dilakukan simulasi serangan XSS menggunakan *Burp Suite.* Pengujian dilakukan dengan menggunakan fitur *Intruder attack* pada Burp Suite, dimana *payload* yang digunakan adalah *"innerHTML=location.hash>#<script>alert(1)</script>". Payload* ini rancang untuk menyisipkan skrip XSS ke dalam halaman web target melalui manipulasi elemen HTML. URL yang digunakan dalam pengujian adalah *"http://burpsuite/show/2/9hkw2ng0hob0cjbqdv2sfhj5rjznrgv"* , dan hasil pengujian menunjukkan bahwa serangan tersebut tidak berhasil.

Kegagalan serangan XSS ini di sebabkan oleh mekanisme validasi *input* yang kuat pada sisi server. Setiap kali *intruder* mencoba memasukkan *payload* tertentu, server merespons dengan menghasilkan kesalahan (*error*), yang menandakan adanya lapisan perlindungan terhadap input yang tidak sah. Hasil ini mengidentifikasikan bahwa, meskipun CSP belum diterapkan, situs web UTM telah memiliki mekanisme validasi input yang memadai untuk menangkal serangan berbasis XSS pada level ini seperti pada gambar 4 berikut

Meskipun demikian, ketiadaan CSP menjadi kekurangan penting yang perlu diperbaiki. CSP berfungsi sebagai lapisan perlindungan tambahan yang secara efektif mencegah serangan XSS dengan membatasi sumber konte eksternal yang dapat dijalankan oleh situs web. Oleh karena itu, selain validasi input yang sudah diterapkan, penerapan CSP pada server UTM sangan di sarankan untuk mengurangi risiko serangan XSS yang lebih kompleks atau *baypass* yang mungkin dilakukan oleh penyerang.

Generating Report

Berdasarkan hasil pemindaian dan pengujian kerentanan situs web Universitas Teknologi Mataram menggunakan OWASPZAP mengidentifikasi sejumlah kerentanan yang memerlukan perbaikan. Tabel 2 berikut merangkum kerentanan, tingkat risiko, dan rekomendasi mitigasi yang relevan.

Tabel 2. Rekomendasi Keamanan

No.	Kerentanan	Tingkat Risiko	Rekomendasi Perbaikan
1	*Absence of Anti-CSRF Tokens*	*Medium*	Menggunakan *framework* yang sudah ter verifikasi dalam mengatasi serangan *Cross-Site Request Forgery (CSRF).*
2	*Content Security Policy*	*Medium*	Konfigurasi *CSP (Content Security Policy)*

No.	Kerentanan	Tingkat Risiko	Rekomendasi Perbaikan
	(CSP) Header Not Set		untuk membatasi sumber daya yang diizinkan untuk dimuat oleh *browser*.
3	*Missing Anti-Clickjacking Header*	*Medium*	Tambahkan *X-Frame-Options* atau *Content-Security-Policy* untuk mencegah serangan *Clickjacking*.
4	*Server Leaks Information via X-Powered-By HTTP respons Header Field*	*Low*	Hapus atau sembunyikan *Header X-Powered-By* untuk menghindari pengungkapan informasi server kepada penyerang.
5	*Strict-Transport-Security Header Not Set*	*Low*	Terapkan *Header Strict-Transport-Security* untuk memastikan semua komunikasi menggunakan HTTPS.
6	*Timestamp Disclosure – Unix*	*Low*	Menyembunyikan atau meminimalisir informasi terkait *Timestamp* untuk mengurangi potensi eksploitasi.
7	*X-Content-Type-Options Header Missing*	*Low*	Tambahkan *Header X-Content-Type-Options* digunakan guna mencegah serangan MIME *Sniffing*
8	*Information Disclosure – Suspicious Comment*	*Low*	Hapus komentar kode yang mencurigakan atau yang mengandung informasi sensitif pada aplikasi.
9	*Modern Web Application*	*Informatif*	Pastikan aplikasi web modern sesuai dengan standar keamanan terbaru.
10	*Re-examine Cache-control Directives*	*Informatif*	Optimalkan direktif *cache-control* untuk mencegah penyimpanan data sensitif pada klien.
11	*User Agent Fuzzer*	*Informatif*	Periksa kembali autentikasi pengguna dan proses identifikasi untuk mencegah eksploitasi melalui *fuzzing*.

KESIMPULAN

Berdasarkan hasil *Vulnerability Assessment* pada situs web Universitas Teknologi Mataram, ditemukan total 11 kerentanan yang terdiri dari 3 vulnerabilitas yang memiliki risiko menengah, 4 vulnerabilitas yang memiliki risiko rendah, serta 4 vulnerabilitas informatif. Kerentanan berisiko menengah memerlukan perhatian prioritas dalam upaya perbaikan. Selain itu, serangan seperti *Clickjacking* berhasil dilakukan, menandakan kebutuhan akan peningkatan perlindungan terhadap manipulasi antarmuka pengguna. Disisi lain, mekanisme keamanan yang diterapkan telah berhasil mencegah serangan *Cross-Site Scripting (XSS),* menunjukkan efektivitas validasi *input*. 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

[1] 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.

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

[3] 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.

[4] F. B. Pitt, J. Apinento, M. K. Abdan, and J. Riel, "Meningkatkan Keamanan Siber: Analisis Komprehensif terhadap Ancaman Saat Ini dan Penanggulangan yang Efektif," Nov. 2023. [Online]. Available: https://www.researchgate.net/publication/375711952

[5] J. Desmon, S. Hidayatulloh, and Y. Jumaryadi, "SYSTEMATIC LITERATURE REVIEW: SERANGAN DEFACE WEBSITE SEBAGAI BENTUK KEJAHATAN SIBER," 2024. [Online]. Available: https://jurnal.umj.ac.id/index.php/just-it/index

[6] D. Nur Diana, M. Amin, and M. Zeinudin, "ANALISIS KRIMINOLOGIS DEFACING DALAM BENTUK CYBER CRIME," 2023.

[7] 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.

[8] I. M. Raazi, I. Dwitawati, and P. Nabila, "UJI VULNERABILITY ASSESSMENT DALAM MENGETAHUI TINGKAT," *JINTECH: Journal of Information Technology*, vol. 4, no. 1, 2023, [Online]. Available: https://journal.ar-raniry.ac.id/index.php/jintech

[9] E. Nurelasari, D. Gumilang, and A. Farabi, "ANALISIS KEAMANAN SISTEM WEBSITE MENGGUNAKAN METODE OPEN WEB APPLICATION SECURITY PROJECT (OWASP) PADA SIMANTEP.ID," 2024.

[10] 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.unity-academy.sch.id/index.php/jirsi/article/view/51

[11] 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.

[12] 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.

[13] E. Z. Darojat, E. Sediyono, and I. Sembiring, "Vulnerability Assessment Website E-Government 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.

[14] 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/

[15] 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.