ANALISIS CELAH KEAMANAN PADA WEBSITE SMA NEGERI 3 BERAU DENGAN METODE PENETRATION TESTING

Nanda Hidayat [1] **, Muhammad Agung Nugroho** [2]
[1), 2)] *Informatika Universitas Teknologi Digital Indonesia*
email : nanda.hidayat@students.utdi.ac.id [1)], m.agung.n@utdi.ac.id [2)]

Abstraksi

Perkembangan informasi digital membuat website menjadi sangat berguna dan semkain mudah untuk diraih oleh semua khalayak. SMA Negeri 3 Berau adalah salah satu institusi Pendidikan di Talisayan yang menerapkan pengembangan website sebagai sistem informasi. Akan tetapi dengan beragamnya penggunaan website yang tersedia beragam juga penyimpangan internet akan terjadi. Untuk menghalau hal tersebut bisa dilakukan dengan metode penetration testing dengan tahap-tahap seperti footprinting dengan menggunakan DNSDumpster dan WPThemeDetector, Scanning fingerprinting dengan alat seperti OWASP ZAP, WPScan, dan Nikto untuk memindai titik-titik celah keamanan website SMAN 3 Berau. Hasil pemindaian keamanan website SMAN 3 Berau diperoleh 7 titik kerentanan dengan OWASP ZAP, 4 kerentanan diperoleh dengan WPScan, dan 9 Kerentanan yang diperoleh menggunakan Nikto. Sehingga output dari pemindaian berupa daftar celah keamanan dimanfaatkan sebagai pertimbangan pencegahan bagi pihak pengelola website.

***Kata Kunci*:**
cyber Security, keamanan sistem, *penetration testing*, *vulnerability*, *wordpress*

Abstract

The development of digital information has made websites very useful and accessible to all audiences. SMA Negeri 3 Berau is one of the educational institutions in Talisayan that implements website development as an information system. However, various internet deviations will also occur with the variety of website uses available. To dispel this can be done by penetration testing method with stages such as footprinting using DNSDumpster and WPThemeDetector, Scanning fingerprinting with tools such as OWASP ZAP, WPScan, and Nikto to scan the points of security holes on the website of SMAN 3 Berau. The security scan results of the SMAN 3 Berau website obtained 7 vulnerability points with OWASP ZAP, 4 vulnerabilities obtained with WPScan, and 9 vulnerabilities obtained using Nikto. So that the output of the scan in the form of a list of security holes is utilized as a preventive consideration for the website manager.

***Keywords*:**
cyber Security, keamanan sistem, *penetration testing*, *vulnerability*, *wordpress*

Pendahuluan

Situs website memiliki tugas yang berguna di era informasi digital ini. Semakin berkembangnya, situs web semakin mudah diraih oleh semua khalayak. [1] merupakan satu diantara *Content Manegement System* (CMS yang berarti platform gratis, meskipun ada juga yang berbayar. CMS ini juga memiliki kendali yang mudah dikuasai karena dibuat kedalam Bahasa sederhana dalam konteks mengembangkan situs web serta memelihara konten secara daring. sendiri dipisahkan jadi 2 jenis yang dapat digunakan sebagai blog, salah satunya digunakan di wordpress.com dan satu lagi untuk membuat website [2] apapun yang bisa ditinjau di wordpress.org. sementara itu memiliki versi yang menerapkan Bahasa Indonesia, tujuannya agar pengguna yang kesesakan dalam bahasa inggris, mampu mengaplikaasikannya kedalam Bahasa Indonesia. [3] Ada juga tujuan dari penelitian ini yakni untuk mengenali apa saja kerentanan [4] pada keamanan situs website pada salah satu sekolah yang ada di daerah berau yaitu, SMA Negeri 3 Berau. Penelitian ini pun memiliki ruang lingkup yang terbatas pada pengujian sisi website saja, tidak termasuk keterlibatan dengan aspel infrastruktur fisik atau jaringan internal. Fokus utamanya terletak pada identifikasi titik-titik [5] kerentanan umum situs sman3berau.com yang ditemukan pada situs *wordpress*. Penelitian ini pula akan dilakukan dengan metode *Penetration Testing* guna memperoleh celah keamanan pada situs web SMAN 3 Berau. Sehingga pihak pengelola website dapat melakukan Tindakan pencegahan berdasarkan data celah keamanan.

Tinjauan Pustaka

Penulisan penelitian ini dibangun berdasarkan temuan relevan dari penelitian-penelitian sebelumnya untuk memanfaatkan metode dan alat untuk menguji kerentanan situs website. Berdasarkan berberapa penelitian sebelumnya yang memanfaatkan beberapa alat *scanning* dan analisis

seperti OWASP ZAP, WPScan, dan Nikto serta beberapa sumber daya tambahan seperti DNSDumpster dan WPThemeDetector. Untuk meningkatkan penulisan pada penelitian ini, tinjauan Pustaka komparatif dilakukan dengan fokus pada penelitian-penelitian yang terkait dengan topik ini, termasuk:

Penelitian sebelumnya yang melakukan uji coba pada tingkat keamanan dan melakukan identifikasi kerentanan pada situs website salah satu sekolah yang ada di Sumbawa Besar. Pada penelitian ini dilakukan uji coba website sekolah menggunakan metode uji penetrasi. Proses ini terdiri dari beberapa langkah, yaitu *Footprinting*, *Scanning Fingerprinting*, eksploitasi, dan pelaporan. Dalam pengujian keamanan website tersebut diperoleh beberapa celah yang rentan dengan total yang terdeteksi ada 13 subfile berstatus rendah dan sedang. [6]

Penelitian yang dilakukan oleh Riandhanu berfokus pada analisis kerentanan aplikasi berbasis web menggunakan metode OWASP dan alat keamanan lainnya untuk menilai tingkat keamanan suatu aplikasi. Hasil pengujian menunjukkan kerentanan ancaman kritis dengan 1 hasil tingkat tinggi, 3 temuan tingkat sedang, 4 hasil dengan tingkat rendah, serta terdapat 7 keluaran risiko yang teridentifikasi menurut OWASP Top 10 berupa *Sensitive data Exposure*, *Security Misconfiguration*, dan *Using Components with know Vulnerabilities.* [7]

Penelitian dari Ramadhani membahas celah WordPress dengan penggunaan alat Analisa seperti WPScan serta pertimbangan teknik pengamanan yang ampuh untuk mengurangi risiko. Dari hasil penelitian Ramadhani didapatkan analisis berupa titik-titik kerentanan serius, termasuk kerentanan injeksi *SQL, XSS,* dan kerentanan otentikasi. [8]

Penelitian selanjutnya membahas tentang titik rentan pada sejumlah website FFTI di UNJAYA. Dengan memanfaatkan *IP Address* target dan alat Zenmap yang digunakan untuk memindai dan menunjukkan host aktif dalam jaringan. Dari penelitian ini dapat disimpulkan bahwa website ftti.unjaya.ac.id mempunyai tingkat kerentanan yang aman dibandingkan app.ftti.unjaya.ac.id dan elearning.ftti.unjaya.ac.id. situs website app.ftti.unjaya.ac.id mempunyai tingkat risiko kerentanan paling serius, yaitu *Critical*, sedangkan elearning.ftti.unjaya.ac.id menampilkan tingkat kerentanan tertinggi pada tingkat tinggi. [9]

Penelitian Rochman dkk mencoba untuk menemukan titk rentan, serta temuan pengujian celah keamanan dari rumah sakit Xyz telah dirangkum beberapa kelemahan seperti berikut:

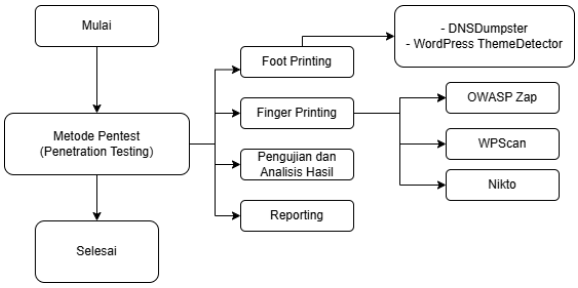
Situs web masih menyalakan pemberitahuan error pada saat ada kekeliruan dalam baris kode program, situs web target masih menampilkan halaman public html, web target menamai file autentikasi dengan nama yang mudah diduga dan umum. [10]

Adapun hasil penelitian yang dilakukan oleh Nisa dkk berupa penilaian keamanan situs web Tapanuli Tengah dengan metode *OWASP ZAP* demi mengidentifikasi hal-hal yang diperlukan untuk menyurutkan kerentanan yang berpotensi membahayakan. Berbagai tahapan *OWASP* dilakukan, seperti pengumpulan informasi, pengujian manajemen sesi, pengujian validasi data, dan pengujian layanan web. Dari temuan penelitian ekstensif yang terdeteksi di situs web 192.187.99.170 didapat hasil berupa 22079 ancaman *Timestamp Disclosure – Unix* dengan level ancaman berada di tingkatan rendah. [11]

Keamanan haruslah dipertimbangkan saat merancang suatu website untuk menanggulangi ancaman serius pemilik website dan pengguna yang mengaksesnya karena rentan terhadap serangan siber seperti peretasan, pencurian data sensitif, atau bahkan dibajak pihak lain. [12], [13] Pengamanan pada website adalah aspek yang tidak bisa diabaikan. Dalam era digital sekarang website merupakan media yang menyampaikan informasi termasuk dari sekolah, maka dibutuhkan sebuah keamanan untuk menghalau serangan yang berpotensi merusak, merebut informasi berharga dan merusak penampilan situs website di sebuah organisasi, instansi ataupun sekolah. [6] diantaranya alat yang dapat dipakai untuk pemindaian ialah OWASP ZAP, yang dirancang untuk melakukan uji penetrasi guna untuk mengidentifikasi kerentanan. [11], [14] alat seperti WPScan digunakan untuk pemindaian titik-titik kerentanan pada website, seperti *plugins* dan tema. sendiri merupakan *CMS* yang menyediakan lebih dari 40% pada situs website di internet. [8] Nikto, berguna untuk pemindaian website wordpress dan memungkinkan untuk mendapatkan file yang terlupakan, skrip yang terbuka, atau konfigurasi server yang rentan [15].

Metode Penelitian

Setiap website memiliki titik-titik celah kerentanan yang tentunya berpotensi terkena serangan oleh orang tak berkomitmen. Hal ini merupakan ancaman serius, selain itu dengan kompleksitas dan kerentanan situs website yang terus berkembang juga menjadi tantangan tersendiri dalam mengidentifikasi dan mengatasi masalah keamanan tersebut. Dalam analisa keamanan situs web di SMAN 3 Berau dengan gaya *penetration testing (pentest)* sesuai langkah-langkah yang ditentukan untuk meperloeh data yang dibutuhkan untuk penyelesaian masalah. Adapun alur penelitian yang bisa dilihat dari bagan penelitian dibawah adalah:



Gambar 1 Diagram Penelitian

1. Tahapan ini dilakukan dengan menggunakan alat yang bisa ditemukan pada peramban internet yaitu, DNSDumpster dan WPThemeDetector. Alat ini memperoleh *IP Address, Hosting Provider, Server Hostname, Domain,* dan bahkan tema utama yang digunakan oleh situs website target. Proses ini bertahap dengan memasukkan url dan domain website target kedalam pencaharian kedual alat tersebut.

Tabel 1 Hasil Footprinting

Temuan	Informasi
Ip Address	185.229.118.84
Domain Name	sman3berau.com
Hosting Provider	AS-HOSTINGER, CY (ASN:47583
Server Hostname	srv159.niagahoster.com
Theme	Atua 1.0.68

2. Scanning Fingerprinting

   Pada fase ini dilakukan scanning untuk mengetahui bagian-bagian rentan pada website target dengan beberapa alat yang digunakan sebagai berikut:

   a. OWASP ZAP

      Penerapan pemindaian dilakukan dengan melibatkan url [16] dari website target kemudian gunakan mode serangan dan pemindaian otomatis dan tunggu beberapa saat untuk mendapatkan hasil kerentanannya.

   b. WPScan

      WPScan ialah *tools* yang dikembankan guna mengidentifikasi titik rentan pada situs website [8] dengan berbekal domain dan *Ip Address* yang didapatkan dari DNSDumpster yang kemudian dilanjutkan dengan mengidentifikasi kerentanan dari website SMA Negeri 3 Berau.

   c. Nikto

      Tahapan ini mencoba menggali potensi kerentanan pada website target secara mendalam. Serupa dengan WPScan, informasi yang dikeluarkan oleh Nikto terdapat sebagian celah yang rentan dengan risiko yang tingkat tinggi, medium, dan rendah.

3. Pelaporan

   Setelah berurusan dengan *scanning fingerprinting*, akan mengambil langkah selanjutnya berupa pembuatan laporan dari hasil temuan celah celah keamanan dari pengujian. Laporan ini akan mencakup kerentanan yang ditemukan, berserta saran dan rekomendasi yang dapat diterapkan untuk meningkatkan keamanan website. Dalam pelaporan ini juga dapat dilakukan *benchmark* keamanan menggunakan standar *CIS* [18]. Pelaporan juga dapat menjadi dasar untuk melakukan proses forensik [19] atau identifikasi celah keamanan dengan melakukan analisis dari beberapa file seperti log.

Hasil dan Pembahasan

Dari proses *penetration testing* terhadap website SMA Negeri 3 Berau dengan menggunakan tools seperti OWASP ZAP, WPScan, dan Nikto. Hasil pengujian celah-celah keamanan ditemukan dapat dilihat sebagai berikut:

Tabel 2 Hasil Temuan *OWASP ZAP*

Peringatan	Risiko
Cloud Metadata Potentially Exposed	Tinggi
Content Security Policy (CSP) Header Not Set	Sedang
Missing Anti-clickjacking Header	Sedang
Cookie No HttpOnly Flag	Rendah
Cookie without SameSite Attribute	Rendah
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Rendah
Timestamp Disclosure - Unix	Rendah

Hasil tampilan dari keluaran scanning OWASP ZAP menunjukkan 1 risiko dengan dampak yang tinggi, 2 risiko dengan dampak sedang dan 4 yang berdampak rendah. Risiko tersebut akan dijabarkan ssebagai berikut:

Tabel 3 Deskripsi dan Solusi Oleh Tools *OWASP ZAP*

NO	Peringatan	Deskripsi	Solusi
1	*Cloud Metadata Potentially Exposed*	Serangan ini memanfaatkan server NGINX yang salah untuk mengakses metadata instan dari fasilitas cloud semacam AWS, GCP, dan Azure. Hal tersebut tersedia pada internal 169.254.169.254, yang bisa diekspos jika NGINX tidak dikonfigurasi secara benar dan diakses melalui header Host.	Apapun konfigurasi NGINX, jangan percaya pada data pengguna. Pada kasus ini kemungkinan besar pada factor $host yang ditetapkan oleh header host kemudian bisa dikendalikan oleh pihak penyerang.
2	*Content Security Policy (CSP) Header Not Set*	Peringatan berikut dimanfaatkan untuk hal-hal dari pencurian hingga vandalisme situs bahkan	Cek kembali server dari web, aplikasi, penyeimbang beban, dll. Anda dikonfigurasi untuk mengatur

		penyebaran malware.	header Content-Security-Policy
3	*Missing Anti-clickjacking Header*	Respons tersebut tidak merawat dari serangan 'ClickJacking'. Respons tersebut seharusnya mengikutkan Content-Security-Policy dengan arahan 'frame-ancestors' atau X-Frame-Options.	Penelusuran web membantu header HTTP Content-Security-Policy dan X-Frame-Options. periksa salah satunya ditetapkan pada setiap halaman web yang ditampilkan.
4	*Cookie No HttpOnly Flag*	Ini bisa menggunakan cookie yang dapat diakses melalui JavaScript. apabila skrip berbahaya berjalan di halaman ini, skrip tersebut dapat mengakses cookie dan meneruskannya ke situs web lain. dalam sesi cookie, pembajakan sesi bisa terjadi	Yakinkan bahwa tanda HttpOnly ditetapkan untuk semua cookie.
5	*Cookie without SameSite Attribute*	Menyetel cookie tanpa menentukan atribut SameSite memungkinkan cookie dibagikan sebagai hasil permohonan "lintas situs". Atribut SameSite adalah tindakan penanggulangan yang efektif terhadap pemalsuan permintaan lintas situs, penyertaan skrip lintas situs, serta serangan pengaturan waktu.	Pada bagian server web, aplikasi, penyeimbang beban, dll. Kemudian lakukan konfigurasi agar menghilangkan header “X-Powered-By”
6	*Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)*	Pada server web bisa memberikan informasi melalui beberapa header respons HTTP X-Powered-By. Akses ini melancarkan penyerang untuk melakukan identifikasi komponen pada aplikasi web, serta celah yang rentanberpotensi didapatkan komponen tersebut.	Selalu periksa server dari web, aplikasi, penyeimbang beban dan lainnya. Lakukan konfigurasi untuk menghapus header X-Powered-By
7	*Timestamp Disclosure - Unix*	Stempel waktu dinyatakan oleh aplikasi/server web. - Unix	pengecekan secara manual untuk faktor data stempel waktu kurang
			sensitif, dan data tidak mungkin digabungkan untuk untukmenunjukkan pola yang bisa dieksploitasi.

Tabel 4 Temuan Kerentanan WPScan

NO	Kerentanan	Status	Risiko
1	XML-RPC Aktif	Aktif	Tinggi
2	WordPress Versi Outdated (6.5.5)	Aktif	Tinggi
3	WP-Cron Aktif	6.5.5 (Kadaluwarsa)	Sedang
4	File Sensitif	Terekspos	Rendah

Tabel 5 Temuan Plugins WPScan

NO	Plugins	Versi	Status
1	Google-site-kit	1.1250	Kadaluwarsa
2	Image-optimization	1.5.3	Kadaluwarsa
3	Litespeed-cache	6.5.02	Kadaluwarsa
4	Post-views-counter	1.4.6	Kadaluwarsa
5	Wordpress-seo	22.6	Kadaluwarsa

Dari hasil *plugins* yang diperoleh, ternyata berstatus kadaluwarsa. Mungkin terlihat sepele, akan tetapi dapat menimbulkan risiko keamanan pada situs website. *Plugins* dengan status kadaluwarsa dapat digunakan oleh penyerang untuk melangsungkan serangan seperti *Cross-Site Scripting (XSS)* yang dilakukan dengan memasukkan script yang dapat mengancam privasi dari pengguna, atau *SQL Injection* yang berpotensi memperoleh akses ilegal ke database, dan bahkan *Remote Code Execution (RCE)* yang memberikan penyerang kendali penuh untuk menjalankan perintah pada server. Selain memberikan dampak pada keamanan, *plugins* yang kadaluwarsa bisa mempengaruhi kinerja website seperti menyebabkan *eror*, *malfungsi* atau bahkan *downtime.* Oleh karena itu diberikan rekomendasi solusi terhadap *plugins* yang kadaluwarsa, yang ditampilkan pada table 7.

Berikut adalah rekomendasi solusi dari mengatasi kerentanan yang ditemukan oleh WPScan dalam pemindaian kerentanan dan juga *plugins* dapat dilihat berikut:

Tabel 6 Dampak dan rekomendasi solusi dari kerentanan yang ditemukan WPScan

NO	Kerentanan	Dampak	Rekomendasi Solusi
1	*XML-RPC Aktif*	Serangan Brute Force, Serangan DDoS, Upaya Login Tanpa Izin.	Nonaktifkan jika tidak digunakan, Batasi akses IP, Implementasi aturan WAF.
2	*WordPress Versi Outdated (6.5.5)*	Kerentanan yang diketahui, Patch keamanan hilang, Masalah Kompatibitas	Update ke versi terbaru, Backup sebelum update, Atur auto-update
3	*WP-Cron Aktif*	Potensi DDoS, Pengurasan Sumber Daya Server.	Gunakan system cron, atur interval yang tepat, pantau eksekusi cron

4	*File Sensitif*	Pengungkapan informasi,	Hapus atau sembunyikan readme.html

Tabel 7 Dampak keamanan dan rekomendasi solusi pada plugins yang ditemukan

NO	*Plugins*	Potensi serangan	Rekomendasi Solusi
1	*Google-site-kit*	Rentan terhadap eksploitasi kerentanan lama seperti kebocoran data konfigurasi.	Perbarui ke versi terbaru (1.138.0) untuk memastikan semua patch keamanan diterapkan.
2	*Image-optimization*	Berpotensi rentan terhadap penyalahgunaan file upload atau injeksi kode.	Perbarui ke versi terbaru (1.5.4) untuk menutup potensi kerentanan.
3	*Litespeed-cache*	Kemungkinan rentan terhadap serangan cache poisoning atau kebocoran data cache.	Perbarui ke versi terbaru (6.5.2) dan periksa pengaturan keamanan cache untuk mencegah penyalahgunaan.
4	*Post-views-counter*	Rentan terhadap serangan XSS jika validasi input tidak memadai.	Perbarui ke versi terbaru (1.4.7) dan pastikan validasi input dilakukan dengan benar.
5	*Wordpress-seo*	Rentan terhadap manipulasi data meta SEO atau kebocoran informasi sensitif.	Perbarui ke versi terbaru (23.7) dan pastikan pengaturan akses pengguna dibatasi untuk mencegah perubahan yang tidak sah.

WPScan ialah alat yang ampuh [8] dalam menemukan celah keamanan untuk situs web wordpress seperti 2 celah dengan risiko yang tinggi seperti *XML-RPC* Aktif dan *Wordpress* Versi Outdate. Kedua celah ini berpotensi terkena serangan seperti *Brute Force*, Serangan *DDoS* hingga hilangnya *Patch* keamanan. Selain 3 temuan tersebut, ada juga beberapa *plugins* yang didapatkan dengan versi yang lama sehingga berpotensi mengandung kerentanan dan bisa menjadi target serangan.

Tabel 8 Temuan Scan Nikto

No	Keren-tanan	Tingkat Risiko	Risiko	Rekomendasi Solusi
1	*Breach Attack*	Tinggi	Kerentanan yang memanfaatkan kompresi HTTP (Content-Encoding: deflate) dan Memungkinkan penyerang mendapatkan informasi sensitif melalui teknik kompresi adaptif. Ini berdampak pada Pencurian data sensitif seperti CSRF tokens, Kebocoran informasi session, Sesi informasi kebocoran.	Nonaktifkan HTTP compression untuk data sensitive, implementasikan CSRF tokens
2	*Missing CSP*	Sedang	Header keamanan yang tidak ada untuk mengontrol sumber daya yang dapat dimuat oleh browser, dan memberikan kemungkinan serangan berbasis injeksi seperti XSS.	Implementasikan header Content-Security-Policy (CSP).
3	*Missing Permission-Policy*	Sedang	Header yang tidak ada untuk membatasi akses ke fitur browser sensitive.	Implementasikan header Permissions-Policy.
4	*Missing Referrer-Policy*	Sedang	Header tidak ada untuk mengontrol informasi referrer yang dikirim. Berpotensi terjadi kebocoran informasi sensitif melalui perujuk.	Implementasikan header Referrer-Policy.
5	*File /LJY9eG3P.php terdeteksi*	Sedang	File mencurigakan yang dapat menjadi kemungkinan file backup atau sementara.	Hapus atau amankan file backup/temporary.
6	*PHP Version Exposed*	Rendah	Informasi teknologi yang dapat dimanfaatkan untuk eksploitasi	Sembunyikan versi PHP agar tidak dapat diakses oleh pengguna.
7	*WP API Exposed*	Rendah	API yang dapat memberikan informasi struktur website	Batasi akses ke /wp-json/.
8	*HTTP Methods*	Rendah	Metode HTTP tidak standar yang dapat memberikan informasi server dan potensi penyalahgunaan metode HTTP.	Batasi metode HTTP hanya yang diperlukan, seperti GET dan POST.
9	*SSL/TLS Config*	Rendah	Penggunaan sertifikat wildcard kurang optimal untuk keamanan	Gunakan sertifikat spesifik untuk setiap subdomain jika memungkinkan.

Berdasarkan data dan hasil setelah menggunakan nikto, diidentifikasi beberapa celah yang dimiliki website SMA Negeri 3 Berau seperti, Kerentanan utama yang ditemukan adalah potensi *BREACH Attack* melalui *Content-Encoding header* yang diset

ke "*deflate*", ini merupakan risiko tinggi yang perlu segera ditangani karena dapat menjadikan website target diakses dengan mudah oleh penyerang dengan memakai Teknik adaptif, serangan ini bisa dengan mudah merekonstruksi data sensitif, seperti token *CSRF*, yang berpotensi penyerang melakukan tindakan ilegal, seperti kebocoran data dan bahkan bisa mengambil alih akun pengguna. *BREACH Attack* ini juga berisiko tinggi karena susahnya mendeteksi serangan dikarenakan menggunakan fitur *HTTP* normal, yang memberikan peluang bagi aktivitas berbahaya untuk lolos dari pemantauan standar keamanan. Sistem menggunakan server *LiteSpeed* dengan PHP versi 8.1.29 dan dihosting di platform Hostinger. Website menggunakan *CMS* WordPress yang teridentifikasi melalui *endpoint API* yang terekspos. Terdapat beberapa *security header* yang belum diimplementasikan. Hasil dengan menggunakan nikto dalam melakukan pemindaian lebih fokus pada kerentanan umum dan konfigurasi server, tanpa melakukan pemeriksaan mendalam terhadap file-file spesifik.

Kesimpulan dan Saran

Berbekal dari penelitian terdahulu, hasil *penetration testing* yang dilakukan terkait analisis keamanan website menggunakan metode *penetration testing* dengan berbagai alat seperti OWASP ZAP, WPScan dan Nikto mampu menemukan berbagai jenis kerentanan keamanan pada situs web. Berdasarkan penggunaan OWASP ZAP menemukan 7 celah yang berpotensi untuk terkena serangan dari pihak-pihak tak bertanggung jawab guna mengeksploitasi situs web.Adapun temuan dari WPScan berupa beberapa kerentanan yang perlu segera ditangani. Fitur *XML-RPC* yang aktif meningkatkan risiko serangan *brute force*, *DDoS*, dan sistem enumerasi, ditemukan juga penggunaan versi *WordPress* yang usang dan berpeluang terhadap berbagai ancaman, termasuk eksekusi kode jarak jauh, injeksi *SQL*, dan *XSS*. Selain itu, aktivasi *WP-Cron* dapat dimanfaatkan untuk serangan *DDoS*, dan file sensitif yang berpotensi membahayakan data internal. Pemindaian menggunakan Nikto menemukan kerentanan yang perlu segera ditangani untuk meningkatkan keamanan. Potensi serangan *BREACH* akibat penggunaan *Content-Encoding: deflate*, kurangnya *header* keamanan seperti *Content-Security-Policy* dan *Referrer-Policy*, serta adanya file cadangan yang tidak aman merupakan perhatian utama. Selain itu, mengungkap informasi server, seperti versi *PHP* dan titik akhir *API WordPress*, meningkatkan risiko eksploitasi, sementara penggunaan sertifikat *SSL wildcard* menambah kerentanan pada subdomain.

Berdasarkan output penelitian ini, memberikan saran berguna untuk meningkatkan keamanan aplikasi web sesuai dengan tujuan utamanya mengidentifikasi kelemahan dari keamanan situs web serta menawarkan Langkah-langkah perbaikan untuk menaikkan perlindungan data dan integritas. Maka untuk itu, peningkatan keamanan dilakukan dengan memperbaiki celah dengan risiko tinggi seperti *XML-RPC* yang tidak selalu harus di aktifkan, kemudian versi *wordpress* yang usang dan memerlukan permaruan. Terdapat juga *WP-Cron* yang lebih baik di aktifkan atau membatasi akses, kemudian hapus atau berikan perlindungan terhadap file sensitif. Mengaktifkan *conten-encoding*, serta penerapan *content-security-policy*, *referrer-policy*, dan *permission-policy*.

Daftar Pustaka

[1] A. S. Riyadi, E. Retnadi, and A. D. Supriatna, "Perancangan Sistem Informasi Berbasis Website Subsistem Guru Di Sekolah Pesantren Persatuan Islam 99 Rancabango | Jurnal Algoritma", Accessed: Nov. 26, 2024. [Online]. Available: https://jurnal.itg.ac.id/index.php/algoritma/article/view/49

[2] M. A. Nugroho, *Seni Literasi Digital: Mozaik Ulasan Transformasi Digital untuk Kesehatan Mental - Jejak Pustaka*. Jejak Pustaka, 2023.

[3] A. A. A. Ushud, I. Novita, and N. Juliasari, "Pelatihan Pemanfaatan CMS Untuk Pembuatan Website Bagi OrangTua Siswa Sekolah Alam Tangerang," *J. Pengabdi. Masy. TEKNO*, vol. 2, no. 1, Art. no. 1, Jun. 2021.

[4] D. Dwi Cahyani, L. P. Windy Puspita Dewi, K. D. Rama Suryadi, and I. M. Edy Listartha, "Analisis Kerentanan Website SMP Negeri 3 Semarapura Menggunakan Metode Pengujian Rate Limiting dan OWASP," *INSERT Inf. Syst. Emerg. Technol. J.*, vol. 2, no. 2, pp. 106–112, Jan. 2022, doi: 10.23887/insert.v2i2.42936.

[5] F. Prasetya, "Analisis Keamanan Situs Web Perpustakaan SMAN 3 Tambun Selatan Menggunakan Metode Vulnerability Assessment," *J. Sains Dan Inform.*, pp. 67–76, Aug. 2023, doi: 10.34128/jsi.v9i1.488.

[6] Y. Mulyanto, M. T. A. Zaen, Y. Yuliadi, and S. Sihab, "Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode Penetration Testing (Pentest)," *J. Inf. Syst. Res. JOSH*, vol. 4, no. 1, pp. 202–209, Oct. 2022, doi: 10.47065/josh.v4i1.2335.

[7] I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," *J. Inf. Dan Teknol.*, Oct. 2022, doi: 10.37034/jidt.v4i3.236.

[8] G. T. A. Ramadhani, M. R. R. Steyer, M. H. Maulidan, and A. Setiawan, "Analisis Kerentanan WordPress dengan WPScan dan Teknik Mitigasi," *J. Internet Softw. Eng.*, vol. 1, no. 4, p. 15, Jun. 2024, doi: 10.47134/pjise.v1i4.2613.

[9] D. Prihanto, A. Sholeh, C. B. Setiawan, and M. A. A. Al Badawi, "Analisis Kerentanan Menggunakan Vulnerability Assessment pada Situs Web Perguruan Tinggi," *Teknomatika J. Inform. Dan Komput.*, vol. 16, no. 2, pp. 66–72, Dec. 2023, doi: 10.30989/teknomatika.v16i2.1248.

[10] A. Rochman, R. Rohian Salam, and S. Agus Maulana, "Analisis Keamanan Website dengan Information System Security Assessment Framework (Issaf) dan Open Web Application Security Project (Owasp) di Rumah Sakit Xyz," *J. Indones. Sos. Teknol.*, vol. 2, no. 4, pp. 506–519, Apr. 2021, doi: 10.36418/jist.v2i4.124.

[11] K. Nisa, M. A. Putra, R. A. Siregar, and M. Dedi Irawan, "Analisis Website Tapanuli Tengah Menggunakan Metode Open Web Application Security Project Zap (*Owasp Zap*)," *Bull. Inf. Technol. BIT*, vol. 3, no. 4, pp. 308–216, Dec. 2022, doi: 10.47065/bit.v3i4.389.
[12] N. Hayaty and M. Cs, "Buku Ajar: Sistem Keamanan".
[13] F. Septian, M. H. Arfian, J. S. Asri, and B. Tjahjono, "Pengujian Keamanan Website dengan Metode Penetration Testing (Studi Kasus: Universitas Esa Unggul)," *Innov. J. Soc. Sci. Res.*, vol. 4, no. 5, Art. no. 5, Sep. 2024, doi: 10.31004/innovative.v4i5.15197.
[14] Y. Yudiana, A. Elanda, and R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP Top 10," *CESS J. Comput. Eng. Syst. Sci.*, vol. 6, no. 2, p. 185, Jul. 2021, doi: 10.24114/cess.v6i2.24777.
[15] R. Laipaka and A. Della, "Pengujian Keamanan Website Menggunakan Kali linux dan Nikto Untuk Mengetahui Kerentanan," 2023.
[16] 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, Aug. 2022, doi: 10.47111/jti.v16i2.3995.
[18] M. Najib, B. Purnomosidi D.P, and M. A. Nugroho, "IMPLEMENTASI SECURITY AUDITOR UNTUK STANDARDISASI INSTALASI SERVER PADA LAYANAN SAAS MENGGUNAKAN CIS BENCHMARK," *Cyber Secur. Dan Forensik Digit.*, vol. 5, no. 2, pp. 83–88, Jan. 2023, doi: 10.14421/csecurity.2022.5.2.3929.
[19] D. Hariyadi, M. A. Nugroho, C. B. Setiawan, and A. I. Wicaksono, "Hybrid Acquisition pada Forensik Digital Berbasis ISO/IEC 27037: 2012 Menggunakan Port Mirroring dan Single Board Computer," *J. Inf. Syst. Manag. JOISM*, vol. 5, no. 1, pp. 8–13, 2023.