Analisis Vulnerability Scanning pada Alat Pemindaian Kerentanan Web: Studi Kasus Pemanfaatan Probely dalam Aplikasi Web

Ridwan Dwi Irawan[1*], Herin Dwibima Apriyanto[2], Ivan Rifky Hendrawan[3]
[1,2]Universitas Duta Bangsa Surakarta, [3]Universitas Amikom Yogyakarta
[12]Surakarta, Indonesia, [3]Yogyakarta, Indonesia
Email: [1]ridwan_dwiirawan@udb.ac.id, [2]herin_dwibima@udb.ac.id,
[3]ivanrifky0@gmail.com

Abstract

Vulnerability scanning is a process of identifying potential security weaknesses in web applications or networks using automated scanning tools. In this study, Probely was used to perform a risk assessment so that developers can detect vulnerabilities early and prepare appropriate preventive actions. The scan of the SMK Negeri 1 Nglipar website revealed 7 findings, all classified as low risk, including issues related to cipher suites, referrer policy, missing Content Security Policy (CSP) header, missing clickjacking protection, HSTS header not enforced, and the use of a deprecated TLS protocol. Although the risks are low, these findings still require follow-up based on Probely's recommendations to strengthen the website's security and support a more robust long-term information security strategy.

Keywords: *Vulnerability, Risk Assessment, Vulnerability, Probely.*

Abstraksi

Vulnerability Scanning adalah proses mengidentifikasi potensi kerentanan pada aplikasi/jaringan menggunakan alat pemindai otomatis. Pada penelitian ini digunakan Probely untuk melakukan risk assessment sehingga pengembang dapat mengetahui celah keamanan sejak dini dan menyiapkan langkah pencegahan. Hasil pemindaian pada website SMK Negeri 1 Nglipar menemukan 7 temuan kerentanan seluruhnya pada kategori low risk, yaitu pada cipher suites, referrer policy, missing content security policy header, missing clickjacking protection, HSTS header not enforced, dan deprecated TLS protocol. Meskipun berisiko rendah, temuan tersebut tetap perlu ditindaklanjuti sesuai rekomendasi Probely agar keamanan web meningkat dan dapat menjadi dasar penyusunan strategi keamanan informasi yang lebih kuat ke depan.

Kata Kunci: *Vulnerability, Risk Assessment, Kerentanan, Probely.*

1. PENDAHULUAN

Di era *World Wide Web* (WWW), aplikasi berbasis web telah menjadi tulang punggung berbagai layanan daring yang digunakan oleh masyarakat lintas sektor dan institusi. Aplikasi web modern memungkinkan pengguna untuk berbagi, memproses, dan memanipulasi informasi secara real time melalui berbagai platform digital [4]. Namun, kemudahan akses tersebut juga diiringi dengan meningkatnya risiko keamanan, terutama pada aspek kerahasiaan, integritas, dan ketersediaan data (*confidentiality, integrity, availability*) yang sangat bergantung pada keamanan aplikasi web itu sendiri [6]. Kerentanan seperti *Cross-Site Scripting* (XSS) dan SQL Injection menjadi ancaman utama yang dapat menyebabkan kebocoran data pengguna maupun pengambilalihan kendali

sistem [4], [8]. Oleh karena itu, diperlukan upaya sistematis dalam menganalisis dan menguji keamanan aplikasi berbasis web melalui pendekatan vulnerability scanning yang terstruktur. Penelitian Fanani, Mu'min, dan Tristanti [4] menegaskan bahwa pemanfaatan alat pemindaian seperti OWASP ZAP mampu mendeteksi kerentanan pada level aplikasi secara otomatis, terutama untuk serangan XSS dan injection.

Dalam konteks yang lebih luas, Isnaini et al. [6] mengombinasikan metode *Vulnerability Assessment* and *Penetration Testing* (VAPT) untuk menilai sistem layanan akademik perguruan tinggi. Hasilnya menunjukkan bahwa pemindaian kerentanan otomatis yang dilanjutkan dengan validasi manual dapat menghasilkan laporan yang lebih akurat dan komprehensif. Hal ini sejalan dengan temuan Madani [8], yang menegaskan efektivitas penggunaan standar OWASP Top 10–2021 dalam menguji keamanan website terhadap ancaman berbasis input pengguna dan manajemen sesi.

Secara lebih spesifik, penelitian ini diarahkan untuk menilai kondisi keamanan aplikasi web pada studi kasus yang dipilih melalui tiga fokus utama, yaitu: (1) melakukan pemindaian kerentanan menggunakan Probely untuk memperoleh daftar temuan beserta tingkat risikonya, (2) memetakan dan menginterpretasikan temuan tersebut ke dalam kategori kerentanan OWASP Top 10–2021 guna mengetahui area keamanan yang paling rentan, serta (3) merumuskan rekomendasi teknis perbaikan yang realistis untuk diterapkan agar keamanan aplikasi dapat ditingkatkan secara bertahap dan berkelanjutan.

Penelitian-penelitian sebelumnya menunjukkan bahwa pengujian kerentanan menggunakan alat otomatis seperti OWASP ZAP [4], JDAICS [11], dan Edumatic [7] dapat mengidentifikasi kerentanan hingga tingkat risiko tinggi. Dengan demikian, pemanfaatan Probely sebagai studi kasus dalam penelitian ini diharapkan dapat memberikan kontribusi nyata terhadap peningkatan keamanan aplikasi web di lingkungan pendidikan, khususnya pada sistem layanan berbasis web di sekolah maupun universitas di Indonesia.

2. TINJAUAN PUSTAKA

Penelitian oleh Fanani, Mu'min, dan Tristanti [4] menyoroti pentingnya penerapan metode pemindaian otomatis dalam mendeteksi kerentanan keamanan aplikasi web menggunakan OWASP ZAP. Studi tersebut mengidentifikasi berbagai celah keamanan seperti Cross-Site Scripting (XSS) dan SQL Injection pada situs pendidikan berbasis web, serta menunjukkan efektivitas OWASP ZAP dalam mengungkap kerentanan tingkat menengah hingga tinggi. Hasilnya memperlihatkan bahwa pemindaian otomatis dapat menghasilkan laporan komprehensif yang menjadi dasar langkah mitigasi risiko. Pendekatan ini sangat relevan dengan penelitian yang memanfaatkan alat modern seperti Probely, yang mengimplementasikan prinsip serupa dalam mendeteksi kerentanan secara sistematis.

Studi yang dilakukan oleh Supriadi, Suryadi, Muslim, dan Samsumar [11] memperluas pemanfaatan kerangka OWASP (Open Web Application Security Project) untuk menilai tingkat keamanan website universitas. Peneliti menggunakan kombinasi alat seperti OWASP ZAP dan Burp Suite untuk mengidentifikasi kelemahan autentikasi dan

konGambarurasi server yang berpotensi dimanfaatkan oleh penyerang. Hasil penelitian mereka menunjukkan bahwa pengujian berbasis standar OWASP mampu meningkatkan keandalan sistem keamanan web melalui deteksi dini dan dokumentasi risiko.

Isnaini, Asyari, Amrillah, dan Suhartono [6] melalui penelitian pada ILKOM Jurnal Ilmiah menerapkan metode Vulnerability Assessment and Penetration Testing (VAPT) terhadap sistem layanan mahasiswa berbasis web. Pengujian dilakukan melalui dua pendekatan: pemindaian otomatis untuk identifikasi awal, dan pengujian manual guna memverifikasi hasil temuan.

Sementara itu, Madani [8] dalam JEITECH Journal UNRAM meneliti penerapan penetration testing berbasis OWASP Top 10 – 2021 untuk mengukur keamanan situs web institusi. Penelitian ini menyimpulkan bahwa pengujian berbasis standar OWASP dapat menjadi dasar penyusunan protokol keamanan adaptif bagi aplikasi web modern. Kajian ini memperkuat gagasan bahwa alat seperti Probely, yang mengadopsi standardized threat taxonomy serta otomasi deteksi dan remediasi kerentanan, berperan penting dalam meningkatkan ketahanan siber organisasi.

Keempat penelitian tersebut secara umum memperlihatkan benang merah bahwa pengujian keamanan aplikasi web yang mengacu pada kerangka OWASP dan didukung alat pemindaian otomatis maupun semiautomatis terbukti efektif sebagai deteksi dini celah keamanan. Fanani et al. [4] menegaskan kemampuan OWASP ZAP dalam menemukan kerentanan khas aplikasi web seperti XSS dan SQL Injection pada situs pendidikan hingga tingkat risiko menengah–tinggi, sedangkan Supriadi et al. [11] memperluas pendekatan dengan mengombinasikan OWASP ZAP dan Burp Suite untuk mengidentifikasi kelemahan autentikasi serta konGambarurasi server pada website universitas. Isnaini et al. [6] memperkuat akurasi temuan melalui integrasi VAPT, yakni pemindaian otomatis yang diverifikasi manual, sehingga hasil lebih komprehensif dan layak dijadikan dasar mitigasi. Madani [8] kemudian menempatkan pengujian tersebut pada taksonomi OWASP Top 10–2021 dan menyoroti bahwa kerentanan yang bersumber dari input pengguna, autentikasi, dan manajemen sesi merupakan vektor serangan dominan yang perlu diuji secara rutin. Secara keseluruhan, literatur menunjukkan bahwa standar OWASP beserta tool scanning memberikan kerangka yang kuat untuk pemetaan risiko dan penyusunan rekomendasi perbaikan keamanan aplikasi web, terutama pada ranah institusi pendidikan.

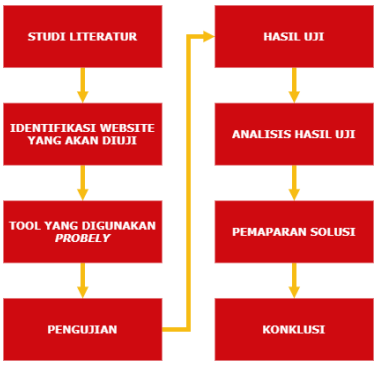
Namun, kajian-kajian tersebut masih menyisakan ruang pengembangan pada pemanfaatan platform vulnerability scanning modern yang berbasis continuous detection seperti Probely, yang tidak hanya melakukan pemindaian snapshot tetapi juga mendukung pemantauan berkelanjutan, pelaporan terintegrasi, dan rekomendasi remediasi yang lebih operasional. Sebagian penelitian terdahulu berfokus pada satu kali pemindaian atau kombinasi tools tanpa mengulas bagaimana pemindaian berkelanjutan dapat memengaruhi prioritas perbaikan dan peningkatan keamanan secara iteratif dari waktu ke waktu. Selain itu, konteks aplikasi web pendidikan di Indonesia dengan pemetaan temuan langsung ke klasifikasi OWASP Top 10–2021 serta penyusunan rekomendasi teknis yang realistis sesuai kondisi pengelolaan sistem lokal belum banyak

dieksplorasi secara spesifik. Karena itu, studi yang menerapkan Probely pada sistem layanan berbasis web di lingkungan pendidikan Indonesia diperlukan untuk melengkapi kekosongan tersebut dan memperluas bukti empiris mengenai efektivitas continuous vulnerability scanning dalam meningkatkan ketahanan keamanan aplikasi web secara berkelanjutan.

3. METODE PENELITIAN

Pada penelitian ini akan membahas hasil yang didapatkan dari pengujian menggunakan probely sebagai salah satu tool untuk menguji vulnerability testing.

3.1. Alur Penelitian



Gambar 1. Alur Penelitian

Dijelaskan pada Gambar 1. menggunakan metode studi pustaka dan dokumentasi untuk membangun landasan teoritis serta kerangka kerja pengujian keamanan aplikasi web, dengan sumber data berupa jurnal ilmiah, buku, standar OWASP, dokumentasi resmi Probely, serta referensi teknis lain yang relevan. Studi pustaka dihimpun melalui penelusuran basis data daring (misalnya Google Scholar, IEEE Xplore, ScienceDirect) dan kunjungan pustaka, lalu diseleksi berdasarkan kesesuaian topik, tahun publikasi, dan kontribusinya terhadap vulnerability scanning. Dokumentasi teknis yang dikaji mencakup arsitektur Probely, mekanisme crawling dan scanning, kategori kerentanan yang didukung, serta format pelaporan dan rekomendasi perbaikannya sebagaimana digambarkan pada Gambar. 1 sebagai alur penelitian.

Objek uji pada penelitian ini adalah website smkn1nglipar.sch.id yang dipilih karena indikasi kerentanan operasional, ditandai oleh munculnya komentar berbahasa asing yang bersifat spam sehingga menimbulkan kekhawatiran pengelola terkait potensi compromise pada sisi aplikasi maupun server. Pengujian dilakukan dalam ruang lingkup black-box vulnerability scanning (tanpa akses kode sumber) untuk menilai potensi kesalahan aplikasi sebelum dilakukan perubahan langsung pada lingkungan produksi. Batasan pengujian ditetapkan agar aktivitas scanning tidak mengganggu layanan, misalnya dengan membatasi laju request (rate limit), kedalaman crawling (crawl depth), dan pengecualian pada endpoint sensitif seperti halaman administrasi, upload besar, atau fungsi transaksi bila ada.

Tahapan teknis dimulai dari konGambarurasi target pada Probely dengan parameter utama: domain/URL target, metode crawling (spider otomatis), cakupan halaman (include/exclude rules), serta profil pemindaian (scan profile) yang menentukan jenis uji yang dijalankan. Probely kemudian melakukan discovery untuk memetakan attack surface melalui crawling, pengumpulan parameter input (query string, form fields, headers), serta identifikasi teknologi (server, framework, CMS, library). Setiap temuan diberi level risiko menggunakan skema penilaian Probely (umumnya mengacu pada CVSS atau severity internal) dengan kategori seperti Low, Medium, High, atau Critical, disertai bukti temuan (request/response), endpoint terdampak, parameter yang memicu, serta deskripsi dampak.

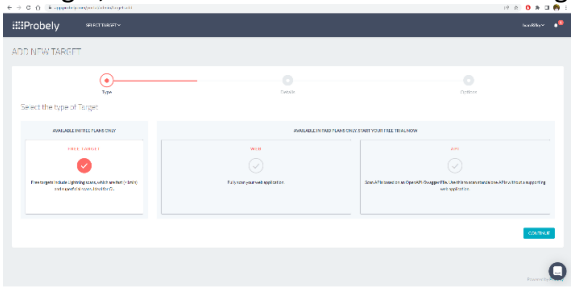
Hasil pemindaian kemudian dianalisis untuk menginterpretasikan tingkat risiko dan prioritas perbaikan dengan mengelompokkan temuan ke dalam kategori OWASP Top 10–2021, menilai kemungkinan eksploitasi (likelihood), besaran dampak (impact), dan konteks implementasi website pendidikan. Output utama penelitian berupa rekapitulasi temuan kerentanan, peta kategorisasi risiko, serta rekomendasi mitigasi teknis dari Probely yang diperkaya dengan penjelasan implementatif, misalnya sanitasi dan validasi input, penerapan prepared statements, penguatan konGambarurasi header keamanan, hardening TLS, serta perbaikan manajemen sesi. Rekomendasi ini disusun agar dapat langsung ditindaklanjuti oleh pengelola website sesuai prioritas severity, kemudian menjadi dasar penarikan kesimpulan mengenai kondisi keamanan smkn1nglipar.sch.id dan efektivitas penggunaan Probely sebagai alat vulnerability scanning pada lingkungan pendidikan.

3.2. Probely

Probely melakukan pemeriksaan security headers, cookie flags, dan SSL/TLS. Bagian paling menarik adalah para pengguna dapat menjadwalkan pemeriksaan secara berkala. Sehingga pemeriksaan dapat dilakukan secara rutin untuk mendeteksi virus. Dimana menggunakan *Site Address* https://app.probely.com/ pada smkn1nglipar.sch.id. Analisis yang akan dilakukan adalah menggunakan Probely sebagai *tools* untuk menguji permasalahan keamanan yang bersinggungan dengan keamanan *website*.

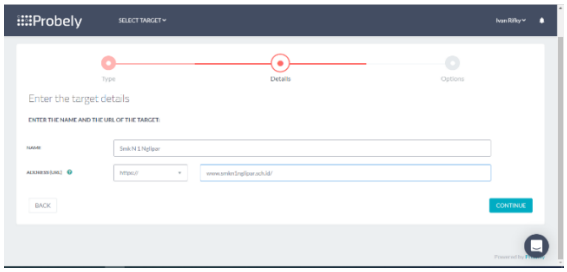
3.3. Pengujian

Langkah pertama terlihat pada Gambar. 2. yaitu register atau daftar akun Probely, kemudian add menu target, kemudian dilakukan aktifitas Free Target.



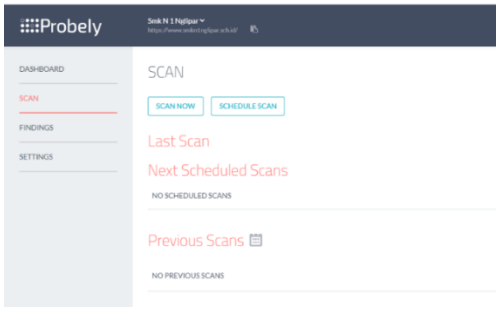
Gambar 2. Tampilan Registrasi Akun Probely

Masukan nama dan alamat link yang akan dijadikan target penetration test seperti pada Gambar. 3. Kemudian klik tombol “Continue” untuk menyimpan alamat target.



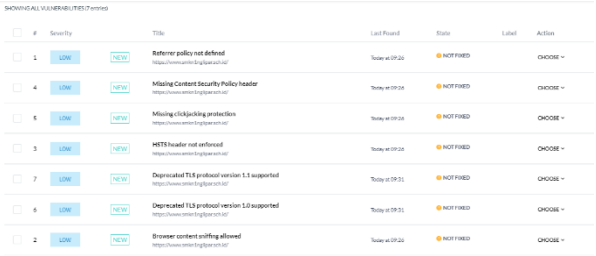
Gambar 3. Pemilihan Tujuan Website yang akan diuji

Lalu pilih scan now makan akan otomatis web akan mengecek untuk tingkat keamanan seperti pada Gambar. 4.



Gambar 4. Proses Scanning sedang berjalan

Web Probely akan secara otomatis mengecek tingkat keamanan dan menampilkan hasil selama kurang lebih 5 menit terlihat seperti Gambar. 5.



Gambar 5. Result dari proses Scanning menggunakan Probely

4. HASIL DAN PEMBAHASAN

Pada section ini, penelitian ini akan berfokus terhadap hasil yang dimunculkan sebagai permasalahan pada web smkn1nglipar.sch.id.

4.1. Pembahasan Hasil Pengujian

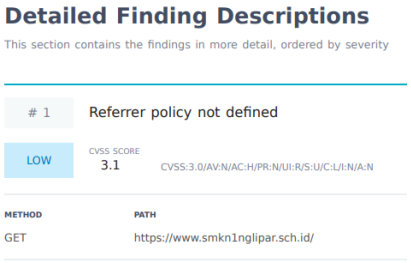
Pada bagian ini diberikan hasil penelitian yang dilakukan sekaligus dibahas secara komprehensip berupa gambar, grafik, tabel dan lain-lain yang mempermudah pembaca paham dan diacu di naskah.

Gambar 6. Hasil dari Pen Test

Detailed Finding Descriptions (Deskripsi Temuan Detil)

Pada Gambar. 7. menjelaskan beberapa proses untuk cara kerja kerja tau temuan dari permasalahan web Smkn1nglipar.sch.id, disini kita mengambil contoh untuk problem.

Referrer policy not difined



Gambar 8. Hasil menampilkan Referrer Policy not defined

Aplikasi tidak mencegah browser mengirimkan informasi sensitif ke situs pihak ketiga di header rujukan. URL tersebut mungkin berisi informasi sensitif, seperti token pemulihan sandi atau informasi pribadi, dan akan terlihat asal lainnya.

Solusi :

Aplikasi harus menetapkan kebijakan perujuk aman yang mencegah data sensitif dikirim ke situs pihak ketiga yang dibuktikan pada Gambar. 9 dan lebih detail pada Gambar. 10.

Bukti

Gambar 9. Evidence

Missing Content Security Policy header

Gambar 10. Evidence

Content Security Policy (CSP) adalah header HTTP yang digunakan pemilik situs untuk menentukan seperangkat aturan keamanan yang harus dimiliki browserikuti saat merender situs mereka.

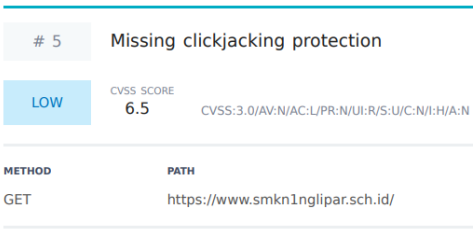
Solusi :

CSP cukup fleksibel untuk menentukan dari mana browser dapat memuat JavaScript, Stylesheet, gambar, atau font, di antara operasi lainnya.

Bukti

Gambar 11. Evidence

Missing clickjacking protection



Gambar 12. Evidence

Respons yang dapat dibingkai terjadi ketika satu atau beberapa halaman dapat digunakan pada iframe di situs web mana pun.

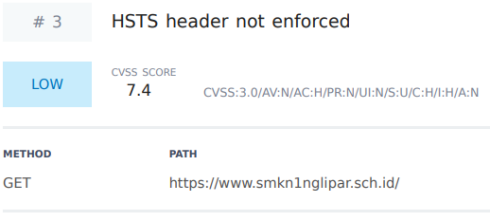
Solusi :

Kombinasi style sheet, iframe, dan teks yang dibuat dengan hati-hati dapat menipu pengguna agar percaya bahwa mereka memasukkan kata sandi untuk email atau rekening bank mereka alih-alih mengetiknya ke dalam bingkai yang terlihat yang dikendalikan oleh penyerang.

Bukti :

Gambar 13. Evidence

HSTS header not enforced



Gambar 14. Evidence

Aplikasi tidak memaksa pengguna untuk terhubung melalui saluran terenkripsi, yaitu melalui HTTPS.

Solusi :

Dengan cara ini, penyerang dapat menguping semua komunikasi antara korban dan server, termasuk kredensial korban, cookie sesi, dan informasi sensitif lainnya..

Bukti :

Gambar 15. Evidence

Deprecated TLS protocol version 1.1 supported

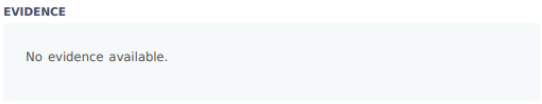
Gambar 16. Evidence

Protokol TLS versi 1.1 sudah usang dan tidak digunakan lagi oleh standar keamanan seperti NIST, PCI-DSS, dan sejenisnya.

Solusi :

Penyerang masih harus mampu menguping dan mencegat koneksi sebelum dapat mengirimkan serangan, tetapi mengingat ketersediaan hotspot Wi Fi terbuka yang tersebar luas, risikonya tidak dapat diabaikan.

Bukti :



Gambar 17. Evidence

Deprecated TLS protocol version 1.0 supported

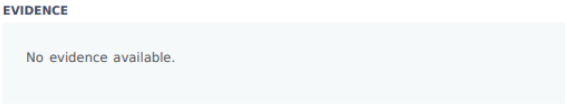
Gambar 18. Evidence

Protokol TLS versi 1.0 tidak digunakan lagi dan sekarang dianggap tidak aman oleh peneliti keamanan dan organisasi standar. Sebagai contoh, Dewan Standar Keamanan PCI (Industri Kartu Pembayaran) mewajibkan TLS 1.0 dinonaktifkan mulai pertengahan 2018.

Solusi :

Perhatikan bahwa TLS 1.0 bukan immedi sangat tidak aman, terutama karena BEAST pada dasarnya merupakan serangan sisi klien, jadi jika browser mutakhir, koneksi harus dapat menguping dan mencegat koneksi sebelum dapat mengirimkan serangan.

Bukti :



Gambar 19. Evidence

Browser content sniffing allowed

Gambar 20. Evidence

Aplikasi ini memungkinkan browser untuk mencoba meniru jenis konten dari respons. Ini berarti browser mungkin mencoba menebak tipe konten dengan melihat konten respons, dan merendernya dengan cara yang tidak dimaksudkan.

Solusi :

Menonaktifkan pengendapan pantomim harus dilihat sebagai lapisan pertahanan ekstra terhadap XSS, dan bukan sebagai pengganti XSS yang direkomendasikanteknik pencegahan.

Bukti :

Gambar 21. Evidence

Selanjutnya adalah secara menyeluruh pentest yang dilakukan menggunakan tool probely ditampilkan pada table I.

Tabel 1. Ringkasan Pen Test Result

Problem	Deskripsi	Solusi
Weak cipher suites enabled	Suite cipher ini saat ini dianggap rusak dan, tergantung pada cipher suite tertentu, menawarkan keamanan yang buruk atau tidak ada sama sekali.	Weak cipher suites enabled
Referrer policy not defined	Aplikasi tidak mencegah browser mengirimkan informasi sensitif ke situs pihak ketiga di header rujukan.Aplikasi harus menetapkan kebijakan perujuk aman yang mencegah data sensitif dikirim ke situs pihak ketiga	Masalah ini dapat diperbaiki dengan mengirimkan header Referrer-Policy dengan nilai yang aman dan valid
Missing Content Security Policy header	Kebijakan Keamanan Konten (CSP) adalah header HTTP di mana pemilik situs menentukan seperangkat aturan keamanan yang harus diikuti oleh browser saat merender situs	Dapat menentukan Kebijakan Keamanan Konten dengan menyetel header di aplikasi. Contoh menetapkan kebijakan yang lebih spesifik untuk skrip, melalui script-src, membatasi pembuatan script ke subdomain mana pun dari example.com.
Missing clickjacking protection	Respons yang dapat dibingkai terjadi ketika satu atau beberapa halaman dapat digunakan pada iframe di situs web mana pun	Mengirim header yang menginstruksikan browser untuk tidak mengizinkan pembingkaian sewenang-wenang,
HSTS header not enforced	Aplikasi tidak memaksa pengguna untuk terhubung melalui saluran terenkripsi, yaitu melalui HTTPS. Penyerang mampu mencegat lalu lintas antara korban dan situs atau memalsukan alamat situs dapat mencegah pengguna terhubung ke sana melalui saluran terenkripsi	Aktifkan HTTP Strict Transport Security (HST).

Deprecated TLS protocol version 1.1 supported	Protokol TLS versi 1.1 sudah usang dan tidak digunakan lagi oleh standar keamanan seperti NIST, PCI-DSS, dan sejenisnya. Versi ini memiliki berbagai kekurangan desain yang dapat merusak keamanan komunikasi.	Menonaktifkan TLS 1.0. Disarankan agar versi protokol TLS yang lebih tinggi diaktifkan, idealnya versi 1.2 dan yang lebih baru.
Deprecated TLS protocol version 1.0 supported	Protokol TLS versi 1.0 tidak digunakan lagi dan sekarang dianggap tidak aman oleh peneliti keamanan dan organisasi standar	Menonaktifkan TLS 1.0. Disarankan agar versi protokol TLS yang lebih tinggi diaktifkan, idealnya versi 1.2 dan yang lebih baru.

5. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa proses Vulnerability Scanning menggunakan alat Probely terbukti efektif dalam mengidentifikasi berbagai potensi kerentanan pada website SMK Negeri 1 Nglipar. Hasil pemindaian menunjukkan adanya kelemahan pada beberapa aspek keamanan, antara lain konGambarurasi Cipher Suites, Referrer Policy, Missing Content Security Policy Header, Missing Clickjacking Protection, HSTS Header Not Enforced, serta penggunaan Deprecated TLS Protocol. Seluruh temuan tersebut dikategorikan dalam tingkat risiko rendah (low risk), namun tetap memerlukan tindak lanjut perbaikan sesuai rekomendasi yang dihasilkan oleh sistem. Temuan ini mengindikasikan bahwa walaupun tingkat kerentanan tidak bersifat kritis, penerapan kebijakan keamanan web secara menyeluruh tetap diperlukan untuk mencegah potensi eksploitasi di masa depan.

Sebagai saran tindak lanjut, pengelola website perlu segera melakukan hardening konGambarurasi keamanan dengan (1) menonaktifkan Deprecated TLS Protocol dan hanya mengaktifkan TLS versi terbaru (minimal TLS 1.2/1.3) serta memperbarui Cipher Suites ke konGambarurasi yang direkomendasikan agar koneksi terenkripsi lebih kuat, (2) menerapkan security headers secara lengkap seperti Content-Security-Policy (CSP), HSTS, X-Frame-Options/Frame-ancestors, dan Referrer-Policy untuk menekan risiko serangan berbasis browser seperti clickjacking dan data leakage. Dengan penerapan saran tersebut, keamanan website diharapkan meningkat secara bertahap dan berkelanjutan, sekaligus mengurangi peluang penyalahgunaan seperti spam atau aktivitas mencurigakan lainnya.

DAFTAR PUSTAKA

[1] "Analisis Kerentanan Aplikasi Web E-commerce Kopi Lampung Nusantara," Jurnal Expert (UBL), Des. 2024. [Online]. Tersedia: https://jurnal.ubl.ac.id/index.php/expert/article/download/4034/2863.

[2] F. Widianto, E. S. Wijaya, H. Harjono, dan A. P. Wicaksono, "Analisis Kerentanan Pada Aplikasi Web Menggunakan Metode PTES," JPTI (Jurnal Pendidikan dan Teknologi Indonesia), vol. 5, no. 1, pp. 1–9, Jan. 2025. [Online]. Tersedia: https://jpti.journals.id/index.php/jpti/article/view/609

[3] R. Efendi, "Uji Kerentanan Keamanan pada Aplikasi Berbasis Web," AITI, Universitas Kanjuruhan Malang, 2024. [Online]. Tersedia: https://ejournal.uksw.edu/aiti/article/view/11372

[4] G. P. I. Fanani, M. A. Mu'min, dan N. Tristanti, "Analisis dan Pengujian Kerentanan Website Menggunakan OWASP ZAP," Jurnal Riset Sistem dan Teknologi Informasi (RESTIA), vol. 3, no. 1, 2025. [Online]. Tersedia: https://journal.aiska-university.ac.id/index.php/restia/article/view/1886

[5] N. T. Hartanti dan R. D. Irawan, "A Informasi Penentuan Tempat Magang Siswa SMK dengan Metode Simple Additive Weighting (SAW)," Jurnal Nasional Teknologi Komputer (JNASTEK), vol. 3, no. 3, pp. 45–52, Jul. 2023. [Online]. Tersedia: https://publikasi.hawari.id/index.php/jnastek/article/view/86

[6] K. Isnaini, M. H. Asyari, S. F. Amrillah, dan D. Suhartono, "Vulnerability Assessment and Penetration Testing on Student Service Center System," ILKOM Jurnal Ilmiah, vol. 16, no. 2, pp. 161–171, 2024. [Online]. Tersedia: https://jurnal.fikom.umi.ac.id/index.php/ILKOM/article/view/1969

[7] A. Jazuli, I. Salamah, dan S. Soim, "Deteksi Tingkat Kerentanan Keamanan Website dengan Metode Manual Pentest dan Tools Xspear," Edumatic: Jurnal Pendidikan Informatika, vol. 8, no. 2, Des. 2024. [Online]. Tersedia: https://e-journal.hamzanwadi.ac.id/index.php/edumatic/article/view/27109

[8] M. A. Madani, "Penetration Testing untuk Menguji Sistem Keamanan pada Website," JEITECH (Journal of Electrical Engineering, Information Technology, Control Engineering, and Robotic), vol. 2, no. 1, pp. 33–45, 2024. [Online]. Tersedia: https://journal.unram.ac.id/index.php/jeitech/en/article/view/3961

[9] D. A. Pratama, N. Nurmalitasari, dan R. D. Irawan, "Sistem Rekomendasi Pemilihan Paket Pembuatan Website Menggunakan Metode Multi-Attribute Utility Theory (MAUT)," Jurnal Teknologi Informasi dan Komunikasi (JTIK), vol. 8, no. 4, pp. 1121–1131, 2024. [Online]. Tersedia: https://lembagakita.org/journal/index.php/jtik/article/download/2577/2204/9954

[10] L. F. A. Rahman, "Analisis Kerentanan Website di Lingkungan ...," JTIKA, Universitas Mataram, 2025. [Online]. Tersedia: https://jtika.if.unram.ac.id/index.php/JTIKA/article/download/369/191

[11] D. Supriadi, E. Suryadi, R. Muslim, dan L. D. Samsumar, "Implementasi Vulnerability Assessment OWASP (Open Web Application Security Project) pada Website Universitas Teknologi Mataram," Journal of Data Analytics, Information, and Computer Science (JDAICS), vol. 1, no. 4, Okt. 2024. [Online]. Tersedia: https://journal.ppmi.web.id/index.php/jdaics/article/download/1368/974

[12] D. A. Utama, "Analisis Keamanan Website Menggunakan Metode PTES, ISSAF dan OWASP di Dinas Komunikasi dan Informasi Kota …," Jurnal Manajemen Informatika (JMI), 2024. [Online]. Tersedia: https://jurnal.unived.ac.id/index.php/jmi/article/view/5367

[13] H. Pahlawansah, M. F. Basmar, dan M. Yusuf, "Analisis Kerentanan Website SMK Muhammadiyah 2 Bontoala Makassar Menggunakan Metode OWASP (Open Web Application Security Project)," BIOS: Jurnal Teknologi Informasi dan Rekayasa Komputer, vol. 6, no. 2, pp. 92–100, Sep. 2025. [Online]. Tersedia: https://bios.sinergis.org/bios/article/view/180.