Analisis Keamanan *Website* Sekolah Menengah Atas Negeri 1 Surade Dengan Pendekatan *Comprehensive Website Security Assessment*

Website Security Analysis for State Senior High School 1 Surade with a Comprehensive Website Security Assessment Approach

Salman Alhidamkara[1*], Ivana Lucia Kharisma[2], Kamdan[3]
[1,2,3]Program Studi Teknik Informatika, Fakultas Teknik, Komputer dan Desain
Universitas Nusa Putra Sukabumi
e-mail: [*1]**salmanalhidamkara008@gmail.com**

Abstrak *- Perkembangan media informasi yang sangat pesat dan seiring dengan penggunaan website sebagai sumber informasi menjadi sangat signifikan dan telah diterapkan dalam berbagai bidang. Namun, seiring dengan peningkatan penggunaan website, keamanan pada website menjadi perhatian yang penting. Analisis celah keamanan diperlukan untuk mendeteksi ancaman di masa mendatang dan memastikan kerahasiaan, konsistensi, akurasi, validitas data, serta ketersediaan informasi, yang dikenal sebagai CIA Triad, sebagai komponen dasar keamanan informasi. Penggunaan website yang berisi informasi umum dari Sekolah Menengah Atas Negeri 1 Surade, berisi juga data dan informasi sensitif berupa data sekolah dan data siswa. Situs web Sekolah Menengah Atas Negeri 1 Surade berisi informasi umum tentang sekolah dan data sensitif yang terkait dengan sekolah dan siswanya. Tujuan dari penelitian ini adalah untuk mengidentifikasi risiko keamanan yang dapat membahayakan data sensitif yang tersimpan dan untuk menganalisis hasil Penilaian Keamanan Situs Web Komprehensif dalam menilai keamanan situs web Sekolah Menengah Atas Negeri 1 Surade. Hasil dari penelitian ini akan berkontribusi untuk meningkatkan kesadaran akan keamanan situs web dan membantu lembaga pendidikan lainnya dan pemerintah dalam memperkuat keamanan situs web untuk mengurangi ancaman siber di Indonesia.*
Kata Kunci - Analisis, Penilaian, Sekolah, Website, Penilaian Keamanan Website

Abstract *- The rapid development of information media along with the use of websites as a source of information has become very significant and has been applied in various fields. However, along with the increasing use of the website, security on the website is an important concern. Analysis of security gaps is needed to detect future threats and ensure confidentiality, consistency, accuracy, data validity, and availability of information, known as the CIA Triad, as a basic component of information security. The use of a website that contains general information from State Senior High School 1 Surade, also contains sensitive data and information in the form of school data and student data. The website of SMA Negeri 1 Surade contains general information about the school and sensitive data related to the school and its students. The purpose of this study is to identify security risks that can harm sensitive stored data and to analyze the results of the Comprehensive Website Security Assessment in assessing the security of the Surade 1 State Senior High School website. The results of this research will contribute to increasing awareness of website security and assisting other educational institutions and the government in strengthening website security to reduce cyberthreats in Indonesia.*
Keywords - Analysis, Assessment, School, Website, Website Security Assessment

I. PENDAHULUAN

Dalam perkembangan media informasi yang pesat, penggunaan *website* sebagai sumber informasi menjadi sangat signifikan dan telah diterapkan dalam berbagai bidang [1]. Namun, seiring dengan peningkatan penggunaan *website*, keamanan menjadi perhatian yang penting. Analisis celah keamanan diperlukan untuk mendeteksi ancaman di masa mendatang dan memastikan kerahasiaan, konsistensi, akurasi, *validitas* data, serta ketersediaan informasi, yang dikenal sebagai *CIA Triad*, sebagai komponen dasar keamananinformasi [2]

Pengujian penetrasi adalah proses penting untuk mengevaluasi keamanan sistem komputerdengan mensimulasikan serangan dari sumber jahat dan tidak sah, seperti peretasan dan jailbreaking. [3]. Sistem keamanan komputer melibatkan aspek teknis, manajerial, legalitas, dan politis [4]. Aplikasi berbasis website sering menjadi target peretasan dan pembobolan sistem karena pertumbuhan penggunaan aplikasi tersebut yang pesat [5].

Salah satu institusi yang memiliki website adalah Sekolah Menengah Atas Negeri 1 Surade di Indonesia. Website tersebut digunakan untuk memberikan informasi kepada orang tua siswa, murid, dan staf sekolah. Keamanan website menjadi faktor krusial karena website tersebut digunakan untuk memberikan informasi kepada orang tua siswa, murid, dan staf sekolah. Informasi yang disimpan dalam website sekolah tersebut bisa mencakup data pribadi siswa, jadwal pelajaran, catatan akademik, dan informasi sensitif lainnya. Jika keamanan website tidak terjamin, hal ini dapat mengakibatkan pencurian data, penyebaran informasi palsu, atau gangguan pada operasional sekolah.

Penelitian menggunakan metode *Footprinting* dan *Vulnerability Scanning* pada *website* kampus dan menemukan beberapa celah keamanan dengan tingkat risiko medium hingga *low* [6] Sementara itu, pada tahun 2022 menggunakan *Acunetix Vulnerability Scanner* pada *website* ITP dan menemukan beberapa celah keamanan dengan tingkat ancaman pada level 3 atau tinggi. Ancaman keamanan tersebut meliputi SQL injection, cross-site scripting (XSS), file inclusion, dan serangan brute force pada halaman login [7]. Pada tahun 2018 penelitian menggunakan metode Penetration Testing (Pentest) pada website SMA Negeri 2 Sumbawa Besar dan menemukan beberapa celah keamanan dengan tingkat risiko low dan medium. Celah-celah tersebut mencakup 13 sub file vulnerability yang dapat dimanfaatkan oleh penyerang untuk melakukan serangan.[8]

Percobaan penetrasi dilakukan dengan cara menyusup ke akses pengguna terlebih dahulu, menggunakan metode enumeration. Enumeration adalah salah satu upaya penyerang untuk memperoleh akses dengan mencoba berbagai password yang mungkin dari generator hash. Enumeration dapat dilakukan dengan menggunakan beberapa alat open-source seperti hydra, medusa, dan John The Ripper.Penelitian ini menggunakan alat hydra untuk melakukan pengujian cracking password. Melakukan hacking pada komputer melibatkan pelanggaran privasi dan keamanan jaringan pada beberapa tingkat. Konsekuensi dari tindakan hacking tersebut bervariasi, mulai dari sekadar keingintahuan hingga kegiatan ilegal yang dapat merusak atau bahkan menghapus file, situs web, atau perangkat lunak. Meskipun begitu, banyak perusahaan besar yang menyewa tim hacker untuk mengeksplorasi celah keamanan jaringan pada instansi mereka. Teknik footprinting melibatkan pengumpulan data atau informasi yang berkaitan dengan target yang akan diteliti. Untuk tujuan ini, beberapa aplikasi dapat digunakan, termasuk CMD

(Command Prompt), Zenmap, dan who is domain. Vulnerability Scanning Vulnerability scanning merupakan suatu proses untuk mendapatkan informasi mengenai kerentanan pada jaringan [6] . *Penetration testing* merupakan suatu bentuk simulasi yang digunakan untuk menguji dan mengevaluasi tingkat keamanan suatu sistem [9]. *ISSAF (Information System Security Assessment Framework)*adalah suatu teknik evaluasi keamanan untuk jaringan, sistem, dan aplikasi [10]

II. METODE

Penelitian ini menggunakan metode *Comprehensive Website Security Assessment* untuk melakukan analisis keamanan pada *website* Sekolah Menengah Atas Negeri 1 Surade (sman1surade.sch.id). Metode *Comprehensive Website Security Assessment* digunakan untuk melakukan penilaian keamanan *website* dengan melakukan serangkaian pengujian untuk mengidentifikasi dan mengevaluasi kerentanan dan kelemahan keamanan yang ada pada website tersebut.

a. Analisa Kebutuhan

Penelitian ini menggunakan beberapa perangkat pendukung seperti yang tercantum pada Tabel 1

Tabel 1. Kebutuhan Perangkat

No	Device	Spesifikasi
1	Laptop / PC	-Lenovo ideapad S145 - Ram 4 GB - SSD 120 GB
2	Sistem Operasi	Windows 10 Home Single Language
3	*Penetration Tool*	Hydra
4	*Vulnerabilities Tool*	Nmap
5	*Footprinting Tool*	Nmap
6	*Network*	Indihome Sukabumi 30 mbps

Dalam penelitian ini, terdapat perangkat dan alat yang akan digunakan sebagai dukungan. Detail kebutuhan perangkat yang diperlukan tercantum pada Tabel 3.1, yang meliputi penggunaan laptop dengan RAM 4 GB, SSD 120 GB, sistem operasi Windows 10, serta menggunakan koneksi internet dengan kecepatan 30 mbps.

Pemilihan sistem operasi Windows 10 sebagai sistem operasi yang digunakan dalam penelitian ini dapat memiliki beberapa alasan ilmiah yang mendasarinya:

1. Ketersediaan dan Popularitas : Windows 10 merupakan salah satu sistem operasi yang paling banyak digunakan di seluruh dunia. Hal ini berarti banyaknya sumber daya dan dukungan yang tersedia untuk pengguna Windows 10, termasuk dokumentasi, tutorial, forum, dan komunitas pengguna yang luas. Dengan popularitasnya, Windows 10 juga telah diuji dan digunakan secara luas dalam lingkungan komputasi, termasuk dalam konteks keamanan dan pengujian sistem.
2. Kompatibilitas Perangkat Lunak : Windows 10 mendukung berbagai perangkat lunak dan aplikasi, termasuk alat-alat yang akan digunakan dalam penelitian ini. Dengan menggunakan Windows 10, peneliti dapat memastikan bahwa alat-alat yang dibutuhkan dapat dijalankan dengan baik dan memiliki kompatibilitas yang baik

dengan sistem operasi yang digunakan.

3. Kemudahan Penggunaan : Windows 10 memiliki antarmuka pengguna yang intuitif dan mudah digunakan, dengan banyak fitur dan dukungan yang dirancang untuk pengguna dengan berbagai tingkat keahlian. Hal ini dapat mempermudah peneliti dalam mengoperasikan perangkat dan alat-alat yang digunakan dalam penelitian, sehingga fokus dapat diberikan pada tujuan utama penelitian.
4. Fleksibilitas : Windows 10 menawarkan fleksibilitas yang cukup baik dalam mengkonfigurasi sistem operasi sesuai dengan kebutuhan pengguna. Hal ini memungkinkan peneliti untuk menyesuaikan pengaturan dan konfigurasi sistem sesuai dengan keperluan penelitian, termasuk dalam hal pengaturan jaringan, keamanan, dan administrasi.

Meskipun terdapat sistem operasi khusus untuk tujuan keamanan dan pengujian seperti Kali Linux, Parrot OS, dan BlackArch, pemilihan Windows 10 dalam penelitian ini mungkin didasarkan pada faktor-faktor di atas yang mempengaruhi keputusan peneliti, seperti ketersediaan sumber daya, kompatibilitas perangkat lunak, kemudahan penggunaan, dan fleksibilitas. Selain itu, daftar alat yang akan digunakan juga tercantum pada **Tabel 2**

Tabel 2. *Tool* yang digunakan

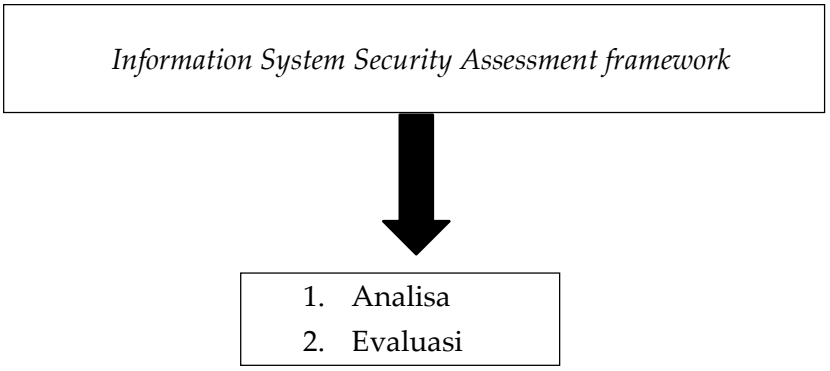
No	Step	Tool
1	*Phase 1 Assessment Planning*	*-Burp Suite* *-Who Is Domain*
2	*Phase 2 Assessment Execution*	*Hydra*
3	*Phase 3 Assessment Reporting*	*Manual*

Penelitian ini melakukan pengujian penetrasi sesuai dengan Information System Security Assessment framework, yang mencakup tiga fase seperti yang ditunjukkan pada **Tabel 3**.

Tabel 3. Tabel Pengujian

No	*Phase*	Objective
1	*Assessment Planning*	Mempersiapkan dan merencanakan penilaian keamanan
2	*Assessment Execution*	Lakukan penilaian keamanan
3	*Assessment Reporting*	Mendokumentasikan dan melaporkan temuan penilaian

b. Skenario pengujian



Gambar 1. Alur Pengujian

3 Phase Information *System Security Assessment* adalah sebagai berikut :

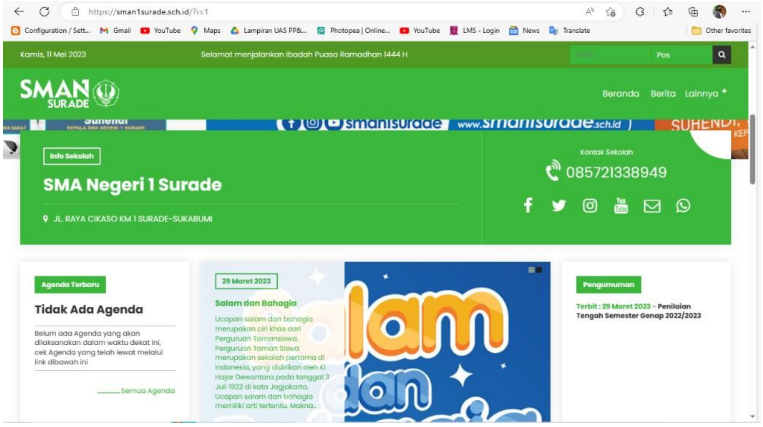
a) Phase 1 terdiri dari information gathering dan network mapping.

1) *Information Gathering*

Dalam tahap ini peneliti menggunakan internet untuk mendapatkan informasi sebanyak-banyaknya dari *website* dengan menggunakan metode teknikal (DNS/WHOIS) dan non-teknikal (*Search Engine*, list E-mail, dan lain-lain). Informasi bisa didapatkan melalui sumber-sumber publik seperti internet, dan organisasi-organisasi yang mempunyai informasi publik, seperti perpustakaan dan lain-lain. Beberapa tindakan yang dilakukan pada fase ini antara lain:

1. Mencari informasi tentang *website* dari berbagai sumber.
2. Menemukan host yang digunakan oleh *website* dan mencari tahu sistem operasi, aplikasi *web server*, dan bahasa pemrograman yang digunakan.
3. Melakukan pemetaan jaringan untuk mengetahui port yang terbuka dan layanan yang berjalan pada setiap host.

Untuk *website* Sekolah Menengah Negeri 1 Surade, informasi dapat diperoleh dengan mengunjungi *website* resmi sekolah di https://sman1surade.sch.id/. Berikut adalah screenshot tampilan website tersebut ditunjukkan pada **Gambar 2** berikut:



Gambar 2. Tampilan Website

Dari website tersebut, informasi yang dapat dikumpulkan antara lain adalah profil sekolah, struktur organisasi, jadwal kegiatan, galeri foto, dan berita terbaru. Selain itu, terdapat juga informasi kontak sekolah seperti alamat, nomor telepon, dan email.

Pada tahap ini, peneliti melakukan pengumpulan informasi mengenai website Sekolah Menengah Atas Negeri 1 Surade melalui berbagai sumber yang tersedia di internet. Informasi yang dikumpulkan dimasukan kedalam table berikut :

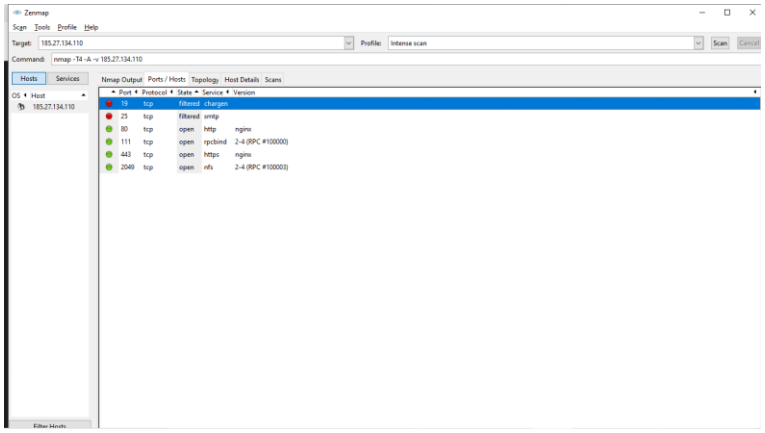
Tabel 4. Informasi *Website*

Informasi Website	**Detail**
URL website	http://sman1surade.sch.id/
Tanggal pembuatan *website*	Tidak diketahui
Bahasa pemrograman yang digunakan	PHP, JavaScript, HTML
Sistem operasi server	Linux
Server web	Apache

Versi CMS yang digunakan	Joomla! 3.9.26
Daftar halaman *website*	Beranda, Profil, Berita, Guru, Siswa, Fasilitas, Kontak Kami
Daftar *plugin* yang digunakan	Akeeba Backup Core, JCE Editor, JCH Optimize, Joomla! Update Notification, RSFirewall!, Widgetkit

2) *Network Mapping*

Setelah informasi berhasil didapatkan dari tahap *information gathering*, langkah selanjutnya adalah melakukan *network mapping*. *Network mapping* dilakukan dengan tujuan untuk mengetahui struktur dan konfigurasi jaringan yang terhubung dengan target. Peneliti menggunakan tools seperti Nmap untuk melakukan *scanning port* pada jaringan yang terhubung dengan target.

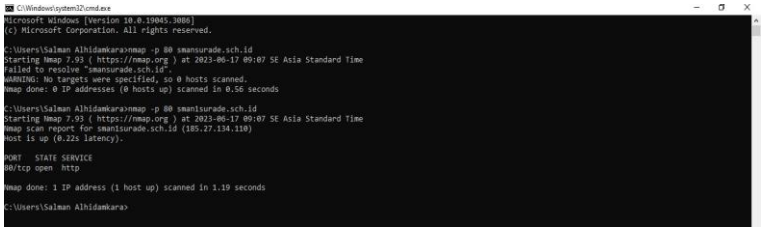


Gambar 3. Hasil Scanning Menggunakan Nmap

b) Phase 2 (*assessment*) terdiri *vulnerability scanning* dan *penetration dan enumerate further*

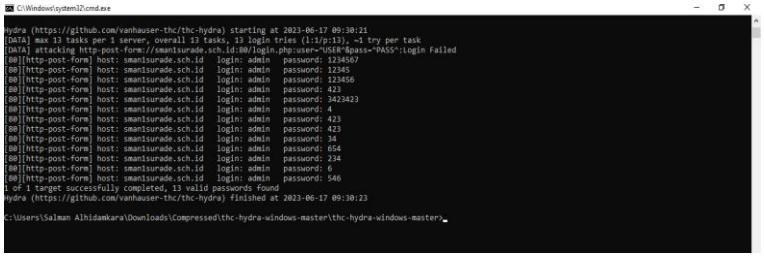
Berikut Langkah- Langkah yang dilakukan pada phase 2 (*assessment*)

1. Melakukan pemindaian kerentanan (vulnerability scanning) pada website menggunakan tools Nmap. Pemindaian ini akan mengidentifikasi kerentanan keamanan yang mungkin ada pada website.



Gambar 4. Hasil Scanning Menggunakan CMD

2. Melakukan *penetrasi* (*penetration testing*) dan *enumerate further* pada *website* untuk menguji kekuatan sistem keamanan *website* dan untuk menemukan username dan paswword.



Gambar 5. Hasil Penetrasi Menggunakan Hydra

c) Phase 3 *reporting*

1. *Reporting*, Setelah menemukan ancaman atau serangan pada *website*, langkah berikutnya adalah melaporkan dan merekomendasikan tindakan pengamanan untuk *website* tersebut sebagai hasil dari analisis.[13]

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	5 (71.4%)
Missing Anti-clickjacking Header	Medium	5 (71.4%)
Strict-Transport-Security Header Not Set	Low	2 (28.6%)
X-Content-Type-Options Header Missing	Low	8 (114.3%)
Information Disclosure - Suspicious Comments	Informational	4 (57.1%)
Modern Web Application	Informational	5 (71.4%)
Re-examine Cache-control Directives	Informational	1 (14.3%)
Total		7

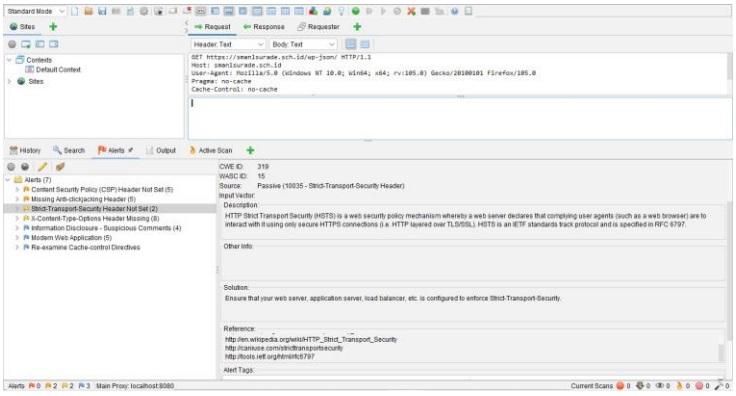
Gambar 6. Hasil Report menggunakan OWASP ZAP

2. Analisis *Sistem,* Analisis sistem pada penelitian ini dilakukan dengan mengidentifikasi risiko keamananpada website Sekolah Menengah Atas Negeri 1 Surade dan menganalisis kemungkinanterjadinya serangan *cyber* terhadap *website* tersebut. Setelah risiko diidentifikasi, peneliti akanmemberikan rekomendasi dan solusi untuk mengatasi risiko tersebut dan meningkatkan keamanan *website.*

   Analisis sistem dilakukan dengan tahapan sebagai berikut:

   a. Identifikasi risiko keamanan
   b. Evaluasi risiko: Menilai risiko keamanan yang diidentifikasi dan menentukan tingkat urgensi untuk mengatasi risiko tersebut.
   c. Mitigasi risiko: Memberikan rekomendasi dan solusi untuk mengatasi risiko keamanan yang diidentifikasi dan meningkatkan keamanan website.
   d. Implementasi solusi: Melaksanakan solusi yang direkomendasikan untuk mengatasi risiko keamanan dan meningkatkan keamanan website.
   e. Pengujian ulang: Melakukan pengujian ulang setelah implementasi solusi untuk memastikan bahwa risiko keamanan telah berhasil diatasi dan *website* sudah aman dariserangan *cyber.*

Dalam melakukan analisis sistem, peneliti menggunakan standar keamanan *web* OWASP (*Open Web Application Security Project*) sebagai acuan. OWASP adalah komunitas global yang berfokus pada meningkatkan keamanan perangkat lunak aplikasi *web.* OWASP menyediakan panduan, alat, dan sumber daya lain untuk membantu para profesional keamanan dalam mengatasi risiko keamanan pada aplikasi *web.*



Gambar 7. Hasil Analisis menggunakan OWASP ZAP

IV. KESIMPULAN

Berdasarkan hasil pengujian yang dilakukan, ditemukan beberapa peringatan keamanan dan informasi terkait dengan penilaian. Berikut adalah rincian mengenai peringatan tersebut:

1. Risiko tingkat menengah terkait dengan Kebijakan Keamanan Konten (CSP) yang tidak ada. CSP adalah mekanisme yang membantu melindungi situs web dari serangan cross- site scripting (XSS) dan serangan injeksi skrip. Kekurangan kebijakan ini dapat meningkatkan risiko keamanan.
2. Risiko tingkat menengah juga terkait dengan header Anti-clickjacking yang tidak ada. Header Anti-clickjacking membantu melindungi pengguna dari serangan clickjacking, di mana penyerang dapat memanipulasi tampilan situs web dan mengelabui pengguna agar melakukan tindakan yang tidak diinginkan. Kehilangan header ini meningkatkan risiko serangan clickjacking.
3. Risiko tingkat rendah terkait dengan header Strict-Transport-Security (HSTS) dan X-Content-Type-Options yang hilang. Header HSTS membantu melindungi situs web dari serangan pengalihan HTTPS, sementara header X-Content-Type-Options membantu mencegah serangan skrip lintas situs. Kehilangan header ini dapat mengurangi lapisan keamanan yang diterapkan pada situs web.

Berdasarkan temuan-temuan di atas, disarankan untuk mengatasi kerentanan tersebut dan meninjau konfigurasi keamanan secara keseluruhan untuk meningkatkan postur keamanan situs web. Tindakan perbaikan yang mungkin termasuk penerapan kebijakan keamanan konten (CSP), header Anti-clickjacking, Strict-Transport-Security (HSTS), dan X-Content- Type-Options yang sesuai, serta peninjauan terhadap komentar yang mencurigakan dan konfigurasi cache. Dengan melakukan tindakan-tindakan ini, keamanan situs web secara keseluruhan dapat ditingkatkan.

DAFTAR PUSTAKA

[1] A. M. Tania *et al.*, "Copyright@2018. P2M STMIK BINA INSANI Keamanan Website Menggunakan Vulnerability Assessment," *INFORMATICS FOR EDUCATORS ANDPROFESSIONALS*, vol. 2, no. 2, pp. 171–180, 2018.

[2] B. Tasya Kumala Dewi and M. Andri Setiawan, "Kajian Literatur: Metode dan Tools Pengujian Celah Keamanan Aplikasi Berbasis Web."

[3] A. W. Kuncoro, J. Informatika, F. Rahma, and M. E. Jurusan Informatika, "Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review." [Online]. Available: https://www.sciencedirect.com

[4] A. Rochman, R. Rohian Salam, dan Sandi Agus Maulana Sekolah Tinggi Manajemen Ilmu Komputer, and S. Likmi, "DI RUMAH SAKIT XYZ," ANALISIS KEAMANAN WEBSITE DENGAN INFORMATION SYSTEM SECURITY ASSESSMENT

[5] FRAMEWORK (ISSAF) DAN OPEN WEB APPLICATION SECURITY PROJECT, vol. 2, no. 4, 2021.

[6] A. Zirwan, "Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner," Jurnal Informasi dan Teknologi, pp. 70–75, Mar. 2022, doi: 10.37034/jidt.v4i1.190.

[7] M. Fatkhurozzi, "Seminar Nasional Informatika Bela Negara (SANTIKA) Analisa Keamanan Website Menggunakan Metode Footprinting dan Vulnerability Scanning pada Website Kampus".

[8] A. Zirwan, "Pengujian dan Analisis Kemanan Website Menggunakan Acunetix Vulnerability Scanner," Jurnal Informasi dan Teknologi, pp. 70–75, Mar. 2022, doi: 10.37034/jidt.v4i1.190.

[9] Y. Mulyanto, M. Taufan Asri Zaen, and S. Sihab, "Analisis Keamanan Website SMA Negeri 2 Sumbawa Besar Menggunakan Metode Penetration Testing (Pentest)," Journal of Information System Research,

vol. 4, no. 1, pp. 202–209, 2022, doi: 10.47065/josh.v4i1.2335.

[10] Y. Thurfah Afifa Rosaliah and B. Hananto, Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM

[11] xxx. 2021.

[12] B. Tasya Kumala Dewi and M. Andri Setiawan, "Kajian Literatur: Metode dan Tools Pengujian Celah Keamanan Aplikasi Berbasis Web."