Analisis Keamanan Situs Web Perpustakaan SMAN 3 Tambun Selatan Menggunakan Metode *Vulnerability Assessment*

Fajar Prasetya

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Singaperbangsa Karawang
Jl. HS. Ronggo Waluyo, Telukjambe Timur, Karawang
fajar.prasetya19078@student.unsika.ac.id

Abstrak

Penggunaan *website* sudah banyak sekali digunakan sebagai media penyebaran informasi oleh berbagai instansi. Namun dengan semakin banyaknya penggunaan *website* muncul beragam kejahatan maya yang berusaha mencuri data dari sebuah *website*. Hal itu bisa saja terjadi pada website perpustakaan SMAN 3 Tambun Selatan yang dapat mengakibatkan pencurian data dan perubahan konten website. Untuk mencegah hal tersebut, sebuah penelitian dilakukan dengan tujuan untuk mencari celah kerentanan pada *website* perpustakaan SMAN 3 Tambun Selatan. Penelitian dilakukan dengan menggunakan metode *Vulnerability assessment* yang terdiri dari tiga tahapan, yaitu *network discovering, vulnerability scanning,* dan *vulnerability analysis*. Hasil dari pengujian dengan tool OWASP didapatkan beberapa celah kerentanan yang termasuk kedalam golongan resiko rendah. Rekomendasi utama dari analisis ini diharapkan agar pengelola *website* perpustakaan SMAN 3 Tambun Selatan untuk memperbaiki konfigurasi *website* nya.

Kata kunci: *OWASP, vulnerability assesment, website security*

Abstract

The use of the website has been widely used as a medium for disseminating information by various agencies. However, with the increasing use of websites, various cybercrimes appear that try to steal data from a website. This could happen to the library website at SMAN 3 Tambun Selatan which could result in data theft and changes to website content. To prevent this, a study was conducted with the aim of looking for vulnerabilities on the library website at SMAN 3 Tambun Selatan. The research was conducted using the Vulnerability Assessment method which consisted of three stages, including network discovery, vulnerability scanning, and vulnerability analysis. The results of testing with the OWASP tool found several vulnerability loopholes that belong to the low risk group. The main recommendation from this analysis is that the manager of the SMAN 3 Tambun Selatan library website can improve the website configuration.

Keywords: *OWASP, vulnerability assesment, website security*

1. PENDAHULUAN

Perkembangan teknologi sangatlah cepat di era digitalisasi seperti sekarang ini. Penggunaan *website* sebagai media informasi semakin berkembang dan banyak bidang-bidang yang sudah menerapkan pengggunaannya. Banyak sekali instansi atau badan menggunakan media elektronik seperti *website* sebagai media pelayanan ataupun sarana penyebaran informasi di beberapa sektor kehidupan, salah satunya adalah sektor pendidikan. SMAN 3 Tambun Selatan merupakan salah satu sekolah yang menggunakan *website* sebagai sarana pelayanan beberapa fasilitas sekolah seperti perpustakaan. Melalui perpustakaan *online* SMAN 3 Tambun Selatan tentu saja akan memudahkan para siswa siswi untuk mengakses buku-buku yang ada di perpustakaan sekolah secara jarak jauh.

DOI: 10.34128/jsi.v9i1.488 *Received: 28 September 2022*
Accepted: 27 Juni 2023

Sebuah *website* pasti menyimpan aset data yang penting berupa informasi dari sebuah organisasi. Seiring dengan kemajuan teknologi pentingnya keamanan terhadap suatu *website* menjadi hal utama karena apabila suatu keamanan diabaikan memungkinkan terjadinya pencurian data atau mengubah tampilan dari suatu *website* [2]. Hal itu bisa saja terjadi pada contoh kasus website perpustakaan SMAN 3 Tambun Selatan yang bisa menyebabkan hilangnya data-data buku ataupun merubah isi konten dari *website* perpustakaan. Untuk mengantisipasi dan mencegah terjadinya masalah pada *website* perpustakaan, maka dibutuhkan penerapan metode yang terstruktur dan komprehensif terhadap masalah keamanan ini untuk menjamin keamanan data *website* sebuah organisasi.

Evaluasi keamanan perlu dilakukan untuk mencari celah kerentanan pada sebuah *website*. Evaluasi dilakukan untuk mencegah adanya resiko kehiilangan data-data penting jika *website* mengalami kerusakan atau *crash* [4]. Sebuah metode diterapkan untuk mencari celah keamanan sebuah website yaitu dengan metode Vulnerability Assessment. Tujuan utama dari metode ini adalah untuk mengidentifikasi titik-titik lemah yang dapat dieksploitasi oleh ancaman atau serangan yang bertujuan untuk mengakses, merusak, atau mengambil alih sistem atau sumber daya yang terkait. Sebuah penelitian [2] [4] telah melakukan analisis keamanan sebuah website dengan metode vulnerability assessment untuk mencari beberapa kerentanan website dan memberikan rekomendasi perbaikannya.

Maka dari pemaparan diatas penulis menawarkan solusi yaitu dengan menganalisa keamanan *website* perpustakaan SMAN 3 Tambun Selatan menggunakan metode Vulnerability Assessment. Dalam analisa tersebut akan diperoleh berbagai macam kerentanan yang memungkinkan penyerang masuk dalam *website* perpustakaan SMAN 3 Tambun Selatan. Kemudian peneliti akan memberikan rekomendasi dari hasil analisa keamanan *website* tersebut. Dengan adanya analisa keamanan *website* perpustakaan SMAN 3 Tambun Selatan, diharapkan mampu menjadi solusi bagi SMAN 3 Tambun Selatan agar dapat meningkatkan keamanan *website*.

2. TINJAUAN PUSTAKA

2.1 Analisis

Panjang Kata analisis diadaptasi dari bahasa Inggris "*analysis*" yang secara etimologis berasal dari bahasa Yunani kuno yaitu "*Analusis*". Kata 'analusis' memiliki arti menguraikan kembali. Berdasarkan Kamus Besar Bahasa Indonesia (KBBI), analisis merupakan penyelidikan terhadap suatu peristiwa (karangan, perbuatan, dan sebagainya) untuk mengetahui keadaan yang sebenarnya (sebab-musabab, duduk perkaranya, dan sebagainya). Analisis juga bisa diartikan sebagai penjabaran sesudah dikaji sebaik-baiknya, ataupun pemecahan persoalan yang dimulai dengan dugaan akan kebenarannya [10].

Kata analisis sering sekali ditemukan dalam berbagai bidang ilmu, salah satunya adalah analisis pada sistem informasi. Dalam bidang sistem informasi, analisis diperlukan sebelum dirancangnya sebuah sistem. Analisis pada sistem dilakukan untuk mengidentifikasi permasalahan pada rancangan sistem agar dapat ditemukan solusi untuk membangun sistem yang lebih efektif dan efisien. Langkah-langkah yang harus dilakukan dalam melakukan analisis sistem informasi yaitu mengidentifikasi permasalahan, menentukan dan memahami pola kerja sistem, dan menganalisis kesalahan yang terjadi.

2.2 *Website*

Website atau Situs web adalah kumpulan halaman web yang dapat diakses publik dan saling terkait yang dikelompokkan bersama dalam satu nama domain yang unik. Situs web dapat dibuat dan dikelola oleh individu, kelompok, bisnis, atau organisasi untuk melayani berbagai tujuan [7]. Menurut [1] website merupakan kumpulan halaman informasi yang tersedia melalui internet sehingga bisa diakses seluruh dunia selama memiliki koneksi internet tanpa batas ruang dan waktu. Organisasi dan bisnis melalui situs web mereka, bertujuan untuk memberikan informasi dan layanan kepada anggota dan pelanggan mereka. *Website* juga sudah menjadi media hiburan seperti bermain game online, menonton film, mendengarkan musik, dan lain sebagainya. Situs web ada berbagai macam jenisnya, diantaranya situs blog, situs media sosial, situs portal berita, situs web hiburan, situs web pendidikan, situs web pemerintah, situs web keanggotaan, dan juga situs mesin telusur.

Secara sederhana, sebuah situs web dibangun dengan beberapa perangkat lunak atau kumpulan kode. Itu adalah teknologi yang membuat konten yang dibuat di beberapa komputer jarak jauh dapat diakses oleh orang-orang di seluruh dunia. Landasan terbentuknya sebuah *website* adalah adanya internet dan sistem world wide web. Internet merupakan teknologi atau infrastruktur yang menghubungkan komputer di seluruh dunia dan memungkinkan berbagi informasi. World Wide Web (atau Web) merupakan sistem yang memungkinkan berbagi informasi menggunakan internet. Dengan kata lain, web adalah kumpulan besar dokumen digital, situs web, halaman web, media, dan lain-lain.

Sebuah *website* dibuat dari sekumpulan kode atau bahasa pemrograman. Bahasa pemrograman yang paling umum adalah HTML (HyperText Markup Language), CSS (Cascading Style Sheets), PHP (Hypertext Preprocessor), Javascript, dan masih banyak lagi. Sebuah *website* akan berfungsi ketika dua hal ini berkerja sama, yaitu *domain name* dan *web hosting*. *Domain name* merupakan nama dari sebuah situs web sebagai sebuah alamat agar *website* tersebut dapat diakses oleh semua orang. Saat sebuah alamat *website* dimasukkan pada *web browser, browser* akan menavigasikan melalui web untuk menemukan lokasi halaman dan kemudian menampilkan informasi konten *website* tersebut. Sedangkan *web hosting* atau *server* merupakan sebuah penyimpanan untuk *website*. *Server* iniliah yang digunakan untuk menyimpan seluruh file dan isi konten dari sebuah *website* yang dijalankan. Sebuah *server* biasanya dimiliki oleh perusahaan penyedia *server* yang mempunyai penyimpanan yang sangat besar [8].

2.3 Keamanan *Website*

Keamanan *Website* atau Web Security merupakan cara atau langkah-langkah untuk mengatasi berbagai jenis serangan atau *attack* dalam teknologi internet atau *website*. Dalam hal ini, keamanan situs web adalah proses yang berkelanjutan dan bagian penting dari pengelolaan situs web. Keamanan situs web penting karena siapapun pasti tidak ingin *website* miliknya diretas atau dibobol. Jika sebuah *website* diretas atau bahkan diblokir, hampir tidak mungkin *website* miliknya akan kembali dikarenakan data traffic nya sudah hilang. Memiliki *website* yang tidak aman akan berakibat sangat buruk, misalnya organisasi pemilik *website* tersebut dapat dituntut hukum karena pelanggaran data kliennya [5].

Ada banyak jenis dari serangan yang dilakukan oleh penjahat dunia maya seperti *Cross-site scripting, SQL Injection, DOS Attack, Path Disclosure, Memory Corruption, Cross-site request forgery,* dan masih banyak lagi yang termasuk injeksi pada kode PHP atau Javascript. Ancaman terhadap sebuah *website* sulit terhindarkan. Banyak cara bagi *hacker* untuk membobol *website* tanpa disadari oleh para pemilik dan juga para penggunanya. Beberapa langkah agar sebuah *website* terlindungi dari serangan *hacker* diantaranya adalah membuat *password* admin yang kuat dan tidak mudah ditebak, melakukan *backup* data secara rutin, selalu *update* perangkat lunak dan *tools,* menggunakan *firewall,* dan memilih layanan *hosting* yang terpercaya [9].

2.4 *Vulnerability assessment*

Vulnerability Asessment merupakan tinjauan sistematis terhadap kelemahan keamanan dari sebuah sistem informasi. Kegiatan ini akan mengevaluasi apakah sistem rentan terhadap sebuah serangan, kemudian menetapkan tingkat keparahan kerentanan tersebut dan merekomendasikan remediasi atau mitigasi [6]. *Vulnerability assessment* tidak melakukan pembobolan pada celah keamanan suatu sistem. *Vulnerability assessment* lebih fokus pada penemuan berbagai *vulnerability* pada sebuah sistem komputer dalam jaringan target. Beberapa ancaman yang dapat dicegah pada *Vulnerability assessment* diantaranya *SQL Injection, XSS,* mekanisme otentikasi yang salah, ataupun perangkat lunak yang dikirimkan dengan pengaturan tidak aman seperti kata sandi admin yang dapat ditebak.

2.5 Open Web Application Security Project (OWASP)

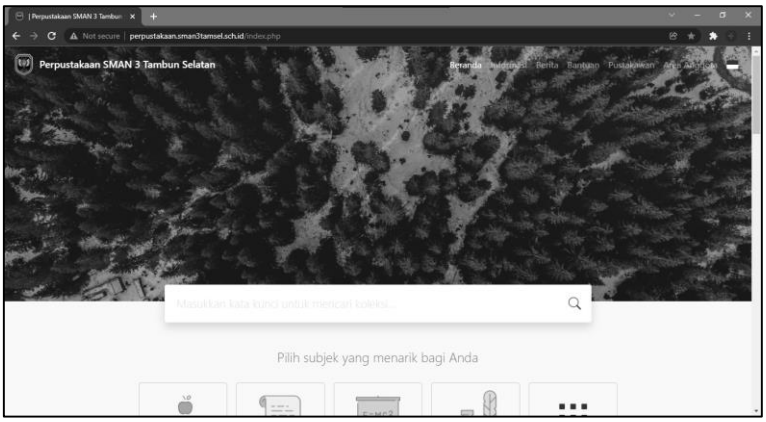
OWASP (*Open Web Application Security Project*) merupakan organisasi nirlaba di Amerika Serikat yang resmi secara daring pada bulan Desember 2001. OWASP adalah komunitas terbuka yang didedikasikan untuk memungkinkan organisasi memahami, mengembangkan, memperoleh, mengoperasikan, dan memelihara aplikasi yang dapat dipercaya dari aspek keamanan [11]. OWASP termasuk organisasi nirlaba global yang fokus pada peningkatan keamanan aplikasi web.

p-ISSN: 2460-173X
e-ISSN: 2598-5841

Tujuan utama OWASP adalah untuk menyediakan sumber daya, alat, pedoman, dan pengetahuan tentang keamanan aplikasi web secara terbuka dan bebas. Mereka berkomitmen untuk mempromosikan kesadaran, pemahaman, dan adopsi praktik keamanan yang baik dalam pengembangan perangkat lunak.

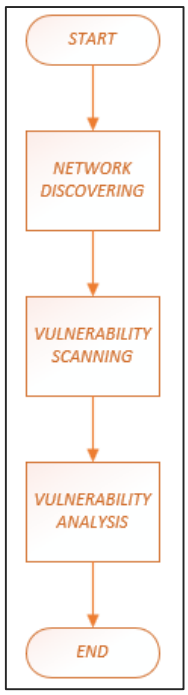
3. METODE PENELITIAN

Penelitian ini dilakukan dengan menggunakan metode *Vulnerability assessment*. Adapun objek dari penelitian ini adalah *website* perpustakaan SMAN 3 Tambun Selatan dengan alamat domain http://perpustakaan.sman3tamsel.sch.id.



Gambar 1. Tampilan *Website* Perpustakaan SMAN 3 Tambun Selatan.

Penelitian ini dibagi menjadi 3 tahapan yaitu *Network Discovering*, *Vulnerability Scanning*, dan *Vulnerability Analysis*. Sebelum melakukan tahapan-tahapan penelitian, penulis terlebih dahulu melakukan studi pustaka untuk mempelajari konsep, teknik, dan tahapan yang berkaitan dengan penelitian ini. Tahapan studi pustaka bersumber dari internet, buku, jurnal, maupun artikel ilmiah [2]. Adapun alur tahapan penelitian ini adalah sebagai berikut.



Gambar 2. Tahapan Penelitian.

p-ISSN: 2460-173X
e-ISSN: 2598-5841

3.1 *Network Discovering*

Tahapan *Network Discovering* bertujuan untuk menemukan informasi struktur rancang bangun dari keamanan jaringan dengan target sasaran halaman *website* yang dituju. Tahapan ini melibatkan pengumpulan data dan informasi tentang sistem yang akan dievaluasi. *Tools* yang digunakan pada tahapan ini adalah Whois, Nslookup, dan Nmap. Whois merupakan suatu alat atau protokol yang memungkinkan kita untuk mengakses *database domain* untuk mendapatkan informasi mengenai alamat, *email*, nomor telepon, tanggal daftar *domain*, serta tanggal kadaluarsa *domain*. Nslookup merupakan sebuah alat yang digunakan untuk mencari informasi jaringan, IP, *server*, serta dapat melakukan diagnosa pada masalah jaringan DNS. Nmap merupakan sebuah aplikasi yang digunakan untuk melakukan *scanning* pada jaringan untuk mengidentifikasi adanya *host port* atau *server* yang terbuka.

3.2 *Vulnerability Scanning*

Tahapan *Vulnerability* Scanning bertujuan untuk mencari celah keamanan pada *website*. Target dari scanning ini adalah SQL *Injection*, *Cross Site Scripting* (XSS), *Remote OS Command*, *Path Transversal*, dan *Private IP Disclosure*. *Tools* yang digunakan pada tahapan ini adalah aplikasi *Open Web Application Security Project* (OWASP) [3]. OWASP merupakan sebuah aplikasi yang dikembangkan untuk menjamin keamanan pada aplikasi yang dikembangkan oleh suatu organisasi.

3.3 *Vulnerability Analysis*

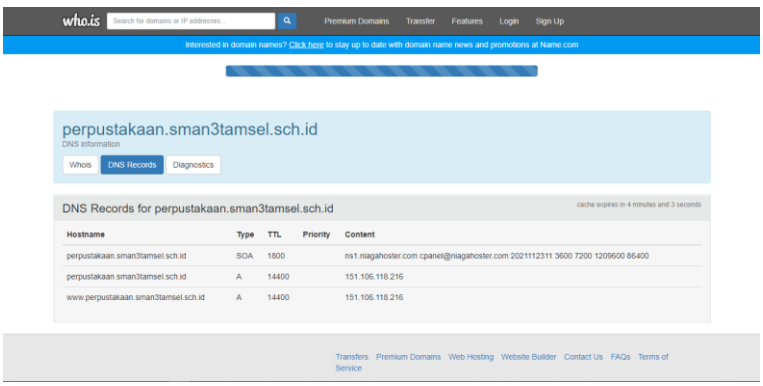
Pada tahapan *Vulnerability Analysis* penulis akan melakukan analisis berdasarkan informasi *vulnerability* yang ditemukan dari hasil *Vulnerability Scanning*. Analisis yang dilakukan di tahap ini berasal dari hasil laporan pengujian kerentanan dengan tool OWASP. Laporan analisis berisi rekomendasi langkah-langkah untuk mengurangi resiko kerentanan pada *website* tersebut.

4. PEMBAHASAN

4.1 Tahapan Network Discovery

Pada Pada tahapan ini dilakukan pengujian terhadap *website* perpustakaan SMAN 3 Tambun Selatan untuk mendapatkan informasi struktur rancang bangun keamanan jaringan *website*. Pada tahap ini digunakan 3 *tool*s yaitu Whois, Nslookup, dan Nmap.

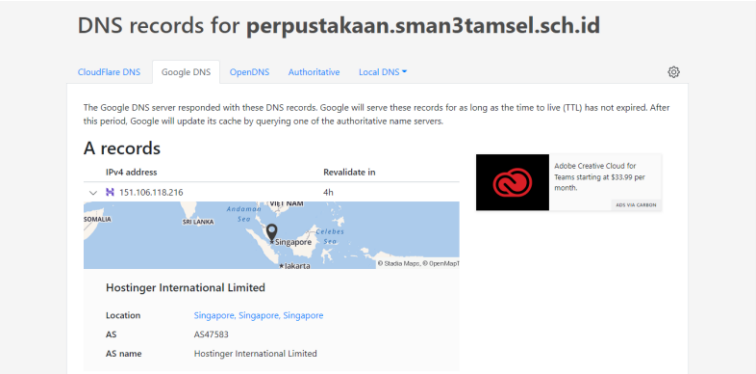
Pada pengujian dengan menggunakan *tool* Whois dilakukan untuk mengambil informasi alamat *domain* pada *website* SMAN 3 Tambun Selatan. Berdasarkan hasil pengujian didapatkan informasi berkaitan dengan daftar *hostname* tipe host, dan nama *server hosting* yang digunakan pada *website* perpustakaan SMAN 3 Tambun Selatan. *Website* perpustakaan ini menggunakan nama *domain* http://perpustakaan.sman3tamsel.sch.id, dengan tipe host SQA, dan menggunakan *server hosting* niagahoster.com. Hasil pengujian tertera pada Gambar 3.



Gambar 3. Hasil Pengujian dengan *tool* Whois.

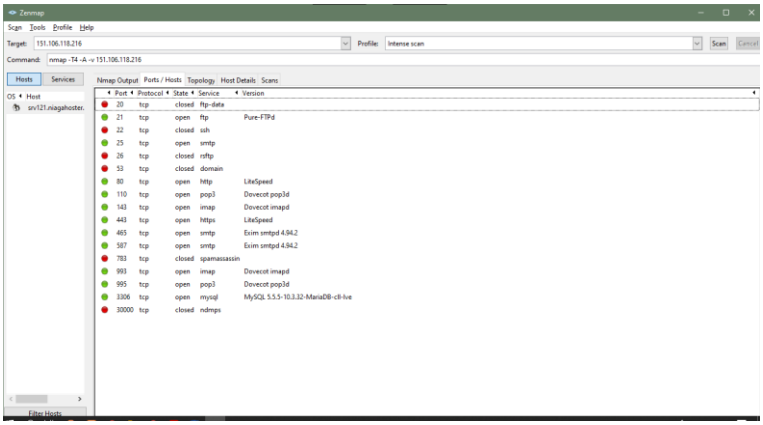
p-ISSN: 2460-173X
e-ISSN: 2598-5841

Pada pengujian dengan menggunakan *tool* Nslookup dilakukan untuk mengetahui IP dari domain pada *website* SMAN 3 Tambun Selatan. Berdasarkan hasil pengujian didapatkan informasi alamat IP *website* perpustakaan SMAN 3 Tambun Selatan yaitu "151.106.118.216", serta alamat *server* yang berada di Singapura dengan nama *server* yaitu Hostinger. Hasil pengujian tertera pada Gambar 4.



Gambar 4. Hasil Pengujian dengan *tool* Nslookup.

Pada pengujian dengan menggunakan *tool* NMap dilakukan untuk mengetahui *port* atau *server* yang terbuka pada *website* SMAN 3 Tambun Selatan. Berdasarkan hasil pengujian didapatkan *port* yang terbuka berjumlah 11 *port*. *Port* yang terbuka tersebut diantaranya ftp, smtp, http, pop3, imap, mysql, dan https. Hasil pengujian tertera pada Gambar 5.

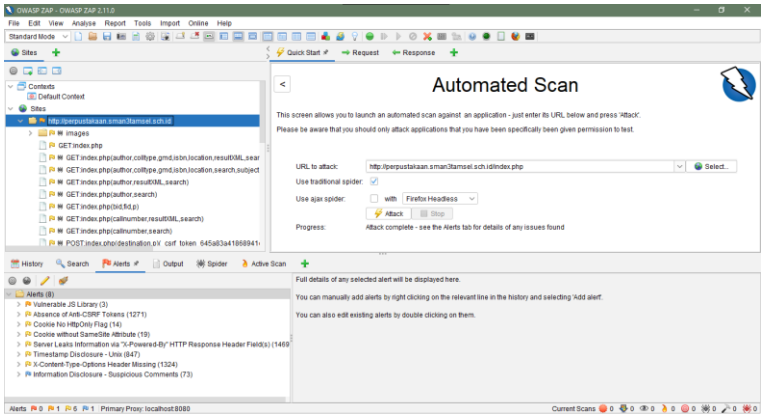


Gambar 5. Hasil Pengujian dengan *tool* NMap

4.2 Tahapan Vulnerability Scanning

Pada tahapan *vulnerability* scanning dilakukan untuk menguji keamanan *website* dan mengidentifikasi kerentanan keamanan pada *website* perpustakaan SMAN 3 Tambun Selatan. Berdasarkan hasil pengujian yang dilakukan dengan menggunakan *tool* OWASP ZAP ditemukan 8 alert diantaranya *Vulnerable JS Library*, *Absence of anti-CSRF tokens*, *Cookie No HttpOnly Flag*, *Cookie Without Samesite Attribute*, *Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)*, *Timestamp Disclosure – Unix*, *X-Content-Type-Options Header Missing*, dan *Information Disclosure - Suspicious Comments*.

p-ISSN: 2460-173X
e-ISSN: 2598-5841



Gambar 6. Hasil Pengujian dengan *tool* OWASP ZAP.

4.3 Tahapan Vulnerability Analysis

Pada tahapan *vulnerability analysis* dilakukan analisis berdasarkan hasil pengujian kerentanan *website* perpustakaan SMAN 3 Tambun Selatan yang dilakukan menggunakan *tool* OWASP ZAP. Analisis yang dilakukan akan membagi *alert* berdasarkan tingkat kerentanannya. Hasil analisis akan disajikan pada Tabel 1 berikut.

Tabel 1. Tabel Hasil Pengujian Kerentanan

No	Alert	Risk				Ket.
		High	Medium	Low	Informational	
1	Vulnerable JS Library		3			Untuk level risk medium berada pada tahap yang mengkhawatirkan, harus segera diperbaiki oleh admin, berjumlah 3.
2	Absence of anti-CSRF tokens			1271		Untuk level risk low masih berada pada keadaan kerusakan ringan, namun akan lebih baik untuk diperbaiki oleh admin karena jumlahnya yang cukup banyak yaitu 4944.
3	Cookie No HttpOnly Flag			14		
4	Cookie Without Samesite Attribute			19		
5	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)			1469		
6	Timestamp Disclosure – Unix			847		

7	X-Content-Type-Options Header Missing	1324		
8	Information Disclosure - Suspicious Comments.		73	Untuk level risk informational ini masih berada pada keadaan kerusakan ringan, berjumlah 73.

Berdasarkan hasil analisis yang dilakukan menggunakan *tool*s OWASP didapatkan hampir semua kerentanan dikategorikan sebagai *low risk*, yang tergolong *medium risk* berjumlah satu dan *informational ris*k berjumlah satu. Meskipun hampir semua kerentanannya tergolong *low risk*, namun jumlah *vulnerability* nya bisa dikatakan cukup banyak yaitu berjumlah 5020. Maka dari itu diperlukan langkah antisipasi untuk memperkaiki celah-celah kerentanan yang ada supaya tidak semakin memburuk. Berikut ini adalah beberapa rekomendasi perbaikan dari *tool*s OWASP yang disajikan pada Tabel 2.

Tabel 2. Tabel Rekomendasi Perbaikan dari OWASP

No	*Vulnerability*	Jumlah *Vulnerability*	Rekomendasi
1	Vulnerable JS Library	3	Lakukanlah upgrade pada jquery ke versi yang terbaru
2	Absence of anti-CSRF tokens	1271	Fase: Arsitektur dan Desain Gunakan perpustakaan atau kerangka kerja yang diperiksa yang tidak memungkinkan kelemahan ini terjadi atau menyediakan konstruksi yang membuat kelemahan ini lebih mudah untuk dihindari. Misalnya, gunakan paket anti CSRF seperti OWASP CSRFGuard. Fase: Implementasi Pastikan aplikasi Anda bebas dari masalah skrip lintas situs, karena sebagian besar pertahanan CSRF dapat dilewati menggunakan skrip yang dikendalikan penyerang. Fase: Arsitektur dan Desain Hasilkan nonce unik untuk setiap formulir, tempatkan nonce ke dalam formulir, dan verifikasi nonce setelah menerima formulir. Pastikan nonce tidak dapat diprediksi (CWE-330). Perhatikan bahwa ini dapat dilewati menggunakan XSS. Identifikasi operasi yang sangat berbahaya. Saat pengguna melakukan operasi berbahaya, kirim permintaan konfirmasi

			terpisah untuk memastikan bahwa pengguna bermaksud melakukan operasi itu. Perhatikan bahwa ini dapat dilewati menggunakan XSS. Gunakan kontrol Manajemen Sesi ESAPI. Kontrol ini mencakup komponen untuk CSRF. Jangan gunakan metode GET untuk permintaan apa pun yang memicu perubahan status. Fase: Implementasi Periksa header HTTP Referer untuk melihat apakah permintaan berasal dari halaman yang diharapkan. Ini dapat merusak fungsionalitas yang sah, karena pengguna atau proxy mungkin telah menonaktifkan pengiriman Perujuk karena alasan privasi.
3	Cookie No HttpOnly Flag	14	Pastikan bahwa flag HttpOnly disetel untuk semua cookie.
4	Cookie Without Samesite Attribute	19	Pastikan atribut SameSite diatur ke 'lax' atau idealnya 'strict' untuk semua cookie.
5	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	1469	Pastikan server web Anda, server aplikasi, penyeimbang beban, dll. dikonfigurasi untuk menekan header "X-Powered-By".
6	Timestamp Disclosure – Unix	847	Konfirmasikan secara manual bahwa data stempel waktu tidak sensitif, dan bahwa data tidak dapat digabungkan untuk mengungkapkan pola yang dapat dieksploitasi.
7	X-Content-Type-Options Header Missing	1324	Pastikan aplikasi/server web menyetel header Content-Type dengan tepat, dan menyetel header X-Content-Type-Options ke 'nosniff' untuk semua halaman web. Jika memungkinkan, pastikan bahwa pengguna akhir menggunakan browser web yang sesuai standar dan modern yang tidak melakukan sniffing MIME sama sekali, atau yang dapat diarahkan oleh aplikasi web/server web untuk tidak melakukan sniffing MIME.
8	Information Disclosure - Suspicious Comments.	73	Hapus semua komentar yang mengembalikan informasi yang dapat membantu penyerang dan perbaiki masalah mendasar yang mereka rujuk.

5. KESIMPULAN

Kesimpulan Berdasarkan hasil analisis dan pengujian yang telah dilakukan pada *website* perpustakaan SMAN 3 Tambun Selatan didapatkan kesimpulan bahwa *website* perpustakaan SMAN 3 Tambun Selatan masih terdapat beberapa celah kerentanan. Ini dibuktikan dari banyaknya jumlah kerentanan yang dihasilkan dari pengujian menggunakan *tool* OWASP. Namun bisa dikatakan dari beberapa kerentanan ini tergolong sebagai risiko yang rendah. Adapun masalah yang mengakibatkan munculnya celah-celah kerentanan hampir semua berasal dari server web. Adapun rekomendasi utama dari analisis ini diharapkan agar pengelola *website* perpustakaan SMAN 3 Tambun Selatan untuk memperbaiki konfigurasi pada *server website* nya. Untuk bagian hosting web diharapkan agar pengelola *website* bisa memilih layanan hosting yang lebih terpercaya lagi agar keamanan dari *website* perpustakaan ini dapat lebih terjamin lagi.

Penelitian ini masih memiliki sejumlah kekurangan dari sisi analisis yang kurang lengkap, dikarenakan penggunaan jumlah *analysis tool* yang terbatas. Harapan dari penulis untuk kedepannya agar penelitian ini bisa lebih dikembangkan dengan menggunakan metode yang lain untuk mendapatkan hasil analisis yang lebih akurat.

DAFTAR PUSTAKA

[1] Herdianti, H., & Umar, F, "Analisis Keamanan *Website* Menggunakan Teknik Footprinting dan *Vulnerability* Scanning," *INFORMAL: Informatics Journal*, vol. *5*, no. 2, pp. 43-48, 2020.

[2] Mulyanto, Y., Haryanti, E., & Jumirah, J, "ANALISIS KEAMANAN *WEBSITE* SMAN 1 SUMBAWA MENGGUNAKAN METODE *VULNERABILITY* ASESEMENT," *Jurnal Informatika Teknologi dan Sains*, vol. *3*, no. 3, pp. 394-400, 2021.

[3] Riadi, I., Yudhana, A., & Yunanri, W, "Analisis Keamanan *Website* Open Journal System Menggunakan Metode *Vulnerability assessment*," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. *7*, no. 4, pp. 853-860, 2020.

[4] Tania, A. M., Setiyadi, D., & Khasanah, F. N, "Keamanan *Website* Menggunakan *Vulnerability assessment*," *INFORMATICS FOR EDUCATORS AND PROFESSIONAL: Journal of Informatics*, vol. *2*, no. 2, pp. 171-180, 2018.

[5] Sucuri, "*Website* Security: How to Secure & Protect Your *Website*," sucuri.net, 2019. [Online]. Available: https://sucuri.net/guides/*website*-security/. [Accessed 2021].

[6] Imperva, "*Vulnerability assessment*," imperva.com, 2020. [Online]. Available: https://www.imperva.com/learn/application-security/*vulnerability*-assessment/. [Accessed 2021].

[7] Techopedia, "*Website*," techopedia.com, 2020. [Online]. Available: https://www.techopedia.com/definition/5411/*website*. [Accessed 2021].

[8] SiteSaga, "What is a *Website* & How Does it Work? (Easy Beginner's Guide)," sitesaga.com, 2021. [Online]. Available: https://www.sitesaga.com/what-is-a-*website*/. [Accessed 2021].

[9] Shella, "Apa Itu Web Security? Tips Untuk Melindungi *Website* dari Serangan Hacker," IDS Digital College, 2020. [Online]. Available: https://ids.ac.id/apa-itu-web-security-tips-untuk-melindungi-*website*-dari-serangan-hacker/. [Accessed 2021].

[10] Syafnidawaty, "ANALISIS," 2020. [Online]. Available: https://raharja.ac.id/2020/11/14/analisis/. [Accessed 2021].

[11] Sumarwanto, "Penggunaan OWASP 4 Sebagai Standar Pengujian Kerentanan Keamanan Aplikasi Berbasis Web", [Online]. Available: http://solmet.kemdikbud.go.id/?p=3098.