ANALISIS KEAMANAN WEBSITE SEKOLAH SMAN 1 TEMPULING DENGAN MENGGUNAKAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP)

[1]Nurjannah, [2]Abdul Muni
[12]Sistem Informasi, Fakultas Teknik dan Ilmu Komputer, Universitas Islam Indragiri
Tembilahan Kota, Indragiri Hilir, Riau, Indonesia
Email: *jannahheaven82@gmail.com*, *abdulmuni@live.com*

ABSTRAK

Keamanan website merupakan satu hal penting dalam perancangan sebuah website, namun masih banyak pengembang website yang kurang berhati-hati dalam meningkatkan keamanan website nya. Pengembang situs web harus menerapkan keamanan situs web yang baik di awal perancangan situs web, karena mungkin suatu saat situs web yang telah dibangun akan menjadi target kerusakan oleh peretas. Selain itu, pengembang situs web harus sering mengikuti tren serangan terbaru agar dapat menjaga dan meningkatkan situs web dari hal-hal yang tidak diinginkan. *Vulnerability assessment* merupakan sebuah keretanan, kekurangan atau celah pada sistem, yang dapat dimanfaatkan oleh satu atau lebih penyerang untuk melakukan serangan yang dapat membahayakan kerahasiaan, integritas, atau ketersediaan suatu sistem. Oleh karena itu peneliti akan melakukan pengujian mengenai keamanan website yang ada pada salah satu sekolah yaitu SMAN 1 Tempuling, SMAN 1 Tempuling merupakan Sekolah Menengah Atas Negeri yang ada di Provinsi Riau Kabupaten Indragiri Hilir Kecamatan Tempuling Kelurahan Sungai Salak yang beralamat di Jalan 21 Maret RT 006 RW 003 Sungai Salak, menggunakan aplikasi OWASP-ZAP, sebagai bahan percobaan untuk menguji bagaimana kerentanan website tersebut tehadap serangan-serangan yang dilakukan melalui aplikasi OWASP-ZAP.

Kata Kunci : Keamanan, website, *vulnerability assessment,* OWASP-ZAP

1 PENDAHULUAN

Perkembangan website di Indonesia sekarang ini sangat pesat, hal ini terjadi karena semakin bertambahnya jumlah pengguna layanan internet dari tahun ke tahun Beberapa website yang sering diakses oleh pengguna diantaranya search engine, ecommerce, sosial media, portal berita dan lain–lain, akan tetapi dibalik kemudahan layanan yang disediakan oleh setiap website, ternyata terdapat beberapa masalah pada celah keamanan, dengan memanfaatkan celah kemanan ini seseorang dapat melakukan serangan pada website tersebut.

Keamanan website merupakan satu hal penting dalam perancangan sebuah website. Namun, masih banyak pengembang website yang kurang berhati-hati dalam meningkatkan keamanan website nya. Pengembang situs web harus menerapkan keamanan situs web yang baik di awal perancangan situs web, karena mungkin suatu saat situs web yang telah dibangun akan menjadi target kerusakan oleh peretas. Selain itu, pengembang situs web harus sering mengikuti tren serangan terbaru agar dapat menjaga dan meningkatkan situs web dari hal-hal yang tidak diinginkan. *Vulnerability assessment* merupakan sebuah keretanan, kekurangan atau celah pada sistem, yang dapat dimanfaatkan oleh satu atau lebih penyerang untuk melakukan serangan yang dapat membahayakan kerahasiaan, integritas, atau ketersediaan suatu sistem.[1]

Sebuah sistem pada umumnya memliki mekanisme keamanan yang diterapkan oleh pihak pengembang, namun pada kenyataannya terdapat banyak informasi penting dan *critical* yang dapat diakses tanpa izin akibat dari celah keamanan oleh sistem tersebut. OWASP merupakan aplikasi yang dirancang untuk menguji developer maupun pentester dalam *cyber security* tentang kerentanannya yang umum terjadi pada aplikasi web.[2]

Oleh karena itu peneliti akan melakukan pengujian mengenai keamanan website yang ada pada salah satu sekolah yaitu SMAN 1 Tempuling, SMAN 1 Tempuling merupakan Sekolah

Menengah Atas Negeri yang ada di Provinsi Riau Kabupaten Indragiri Hilir Kecamatan Tempuling Kelurahan Sungai Salak yang beralamat di Jalan 21 Maret RT 006 RW 003 Sungai Salak, dengan Nomor Pokok Sekolah Nasional: 10402069. Adapun visi dari SMAN 1 Tempuling yaitu menjadikan warga sekolah yang edukatif, kreatif, kompetitif berdasarkan iman dan takwa (era kompak), dan misi nya melaksanakan pelayanan pendidikan sesuai Standar Nasional Pendidikan (SNP), mewujudkan pendidikan yang menghasilkan lulusan cerdas spritual, emosional, kinestetis dan intelektual, serta melaksanakan pembelajaran aktif, inovatif, kreatif, efektif, menyenangkan, dan melaksanakan kepemimpinan pembelajaran.

2 TINJAUAN PUSTAKA

Berikut ini adalah penelitian yang telah dilakukan dan memiliki korelasi yang searah dengan penelitian yang akan dibahas dalam jurnal ini. Dalam upaya menyempurnakan penelitian maka perlu dilakukan kajian literature, diantaranya yaitu:

Tabel 1. Penelitian Terdahulu

No.	Peneliti	Judul	Kesimpulan
1.	Muhammad Ramdani Syam Al'Am'yubi a ,DanurWijayanto , S.Kom., M.Cs	Analisis sistem keamanan website xyz menggunakan framework owasp-zap	Berdasarkan pengujian yang dilakukan mengunakan OWASP ZAP 2.10.0 mendapatkan 4 kerentanan yaitu Incomplete or No Cache-control Header Set, Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s), Information Disclosure - Suspicious Comments, dan Timestamp Disclosure – Unix. Pada ke 4 kerentanan yang didapat memiliki 2 tingkat risiko low dan 2 tingkat risiko informational. Pada CWE memiliki 3 ID yang sama yaitu CWE ID 200 dan 1 CWE ID 525 Sedangkan WASC memilki ID yang sama yaitu WASC ID 13.[3]
2.	I Wayan Sriyasa, Victor Ilyas Sugara	Analisis keamanan website menggunakan *open web application security web (owasp)*	Rekomendasi perbaikan terhadap temuan sudah diberikan, dan diantaranya bersifat perbaikan didalam source code dan konfigurasi pada application server/web server yang digunakan pada aplikasi tersebut. Perbaikan diprioritaskan kepada temuan yang bersifat High, Medium dan Low, terhadap temuan celah keamanan yang bersifat Informational, tidak menjadi keharusan untuk dilakukan perbaikan.[4]
3.	Ahmad Zaini1, Rony Wijanarko2	Analisis Keamanan Website Menggunakan standar keamanan *open web application security project (owasp)* studi kasus website penerimaan mahasiswa baru universitas wahid hasyim semarang	Berdasarkan hasil analisis mengunakn OWASP-ZAP ditemukan beberapa celah dan kerentan pada website, penulis sudah menyampaikan kepada pihak terkait untuk ditindaklnjuti agar website diperbaiki maupun ditingkatkan untuk memperbaiki website dalam meminimalisir celah yang bisa diexploitasi oleh hacker. Berdasarkan

No.	Peneliti	Judul	Kesimpulan
			hasil analisis, kerentanan yang ditemukan hanya dari konfigurasi yang kurang tepat. Dan tidak ditemukan kerentanan lain karena sistem telah berhasil menerapkan beberapa fitur keamanan.[5]
4.	Ela Nurelasari, Difa Gumilang Al Farabi	Analisis keamanan sistem website menggunakan metode *open web application security project (owasp)* pada simantep.id	Dalam melakukan vulnerability assessment atau penilaian kerentanan celah keamanan pada website simantep.id menggunakan metode OWASP Top 10 tahun 2021 yang bertujuan untuk menguji tingkat keamanan. menunjukkan grafik hasil scanning menggunakan aplikasi OWASPZap yang seberapa mungkin ada celah keamanan pada website target berdasarkan tingkat ancaman disini terbagi menjadi beberapa kategori berdasarkan dampak yang ditimbulkan dari celah keamanan tersebut yaitu , Medium 3, Low 3, Informational 4. Metode OWASP Top 10 tahun 2021.[6]
5.	Nabila Athifah Zahra1*, Farras Hafish Zidane1, Nur Racana Kuslaila1	Analisis keamanan sistem informasi pada website pt sentra vidya utama (sevima) menggunakan metode owasp	Dari penelitian yang telah dilakukan dapat disimpulkan bahwa keamanan sistem informasi pada website PT Sentra Vidya Utama (SEVIMA) menggunakan metode OWASP (Open Web Application Security Project) terdapat beberapa kerentanan yang perlu ditangani. Ditemukan ada empat resiko yang tergolong pada tingkat medium dengan skor secara keseluruhan sebesar 5.75.[7]
6.	Verseveranda Setyo Nugroho 1), Febrian Wahyu Christanto 2)*	Analisis keamanan website dengan information system *security assessment framework (issaf) and open web application security project (owasp)*	Berdasarkan hasil pengujian penetrasi pada website diaundangkamu.com, maka dapat mengambil kesimpulan berdasarkan pengujian menggunakan metode ISSAF dan OWASP bahwa website diaundangkamu.com tergolong sangat aman karena tidak mampu untuk ditembus dengan beberapa serangan cyber. Fitur Cyber Defense yang disediakan penyedia layanan hosting memberikan proteksi keamanan cyber seperti serangan virus, malware, ransomware, dan berbagai bentuk ancaman baru.[8]
7.	Muhammad Arifai Nurrizki1, Erik Iman Heri Ujianto2,Rianto3	Analisis keamanan website desa budaya DIY dengan metode	Pengujian dan analisis keamanan website Desa Budaya telah berhasil. Tahapan yang dilalui dalam analisis keamanan website ini yaitu menguji

No.	Peneliti	Judul	Kesimpulan
		penetration testing (pentest) dan owasp zap.	sistem dengan menggunakan cara Footprinting, Scanning Fingerprinting, Exploit serta Report. Pengujian di keamanan website Desa Budaya dilakukan dengan menggunakan beberapa tools yaitu Who.is, NSlookup, Nmaps dan OWASP (Open Web Application Security Project) ZAP.[9]
8.	Naikson Fandier Saragih,Reinhard Tamalawe, Indra M Sarkis.	Analisis dan implementasi secure code pada pengembangan sistem keamanan website fikom-methodist.com menggunakan penetration testing dan owasp zap.	Aassessment menggunakan Tools Owasp Zap untuk mendeteksi kerentanan CSRF berhasil dilakukan.pada web dengan menemukan celah kerentanan CSRF 14 celah (absence of Anti-CSRF Token) dan pada Method GET terdeteksi sebanyak 11 serta Method POST sebanyak 3 dengan risiko rrendah (Low). Ujicoba serangan secara manual menggunakan rekayasa social media(phising). pada elemen URL website melalui form Register dengan Method POST. Serangan CSRF one-click, berhasil masuk ke dalam.[10]
9.	M. Wahidin1*, Dhian Nur Rahayu2, R. Mega Yulianto3	Analisis kerentanan situs web kopkar syariah PT BSIN menggunakan owasp zed attack proxy	Penelitian ini menghasilkan analisis kerentanan pada website Koperasi Karyawan Syariah PT BSIN. Kerentanan yang ditemukan adalah X-Frame-Options Header Not Set, Absence of Anti-CSRF Tokens, Cookie No HttpOnly Flag, Cookie without SameSite Attribute, Incomplete or No Cache-control Header Set, Secure Pages Include Mixed Content, Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s), X-ContentType-Options Header Missing, Charset Mismatch, Information Disclosure - Suspicious Comments, Timestamp Disclosure – Unix.[11]
10.	Dewi Aryanti, Nurholis dan Joy Nashar Utamajaya	Analisis kerentanan keamanan website menggunakan metode owasp (open web application security project) pada dinas tenaga kerja.	aplikasi berbasis website yang memiliki karakter aplikasi web yang berbeda maka dapat disimpulkan Perlu adanya penilaian risiko kerentanan keamanan terhadap aplikasi berbasis website agar bisa terlihat potensi risiko keamanan untuk mencegah dan mengatasi risiko keamanan sebelum aplikasi berbasis website di upload ke server dan terdapat 7 risiko dengan 3 risiko memiliki risk severity high, 2 risiko memiliki risk severity medium, 2 risiko memiliki risk severity low.[12]

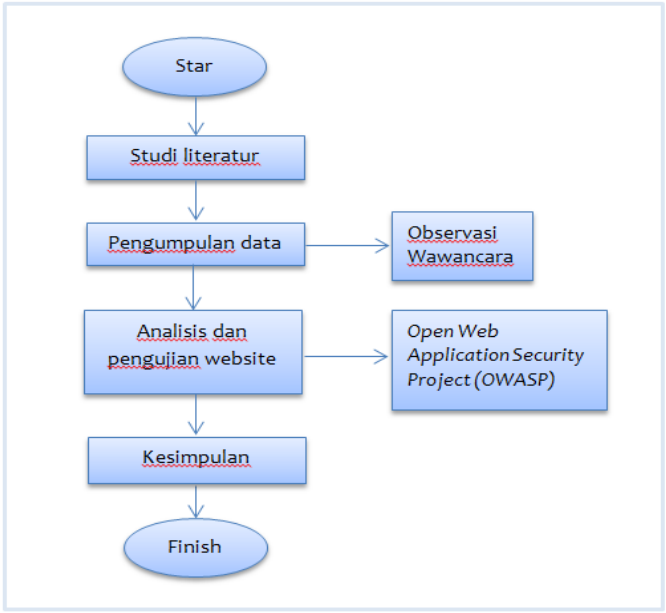
Analisis adalah sebuah kegiatan untuk mencari pola ataupun metode berasumsi yang berhubungan dengan pengetesan dengan cara analitis kepada suatu buat memastikan bagian, jalinan antar bagian, dan ikatan dengan totalitas. Analisa merupakan sesuatu upaya buat menguraikan sesuatu permasalahan jadi bagian-bagian *(decomposition)* hasil lapisan wujud sesuatu yang dijabarkan itu nampak dengan nyata, asli dan dapat dimengerti permasalahannya.[13]

Website adalah kumpulan dari halaman web yang sudah dipublikasikan di jaringan internet dan memiliki domain/URL *(Uniform Resource Locator)* yang dapat diakses semua pengguna internet dengan cara mengetikan alamatnya. Hal ini dimungkinkan dengan adanya teknologi *World Wide Web* (WWW) halaman website biasanya berupa dokumen yang ditulis dalam format *Hyper Text Markup Language* (HTML), yang bisa diakses melalui HTTP, HTTPS adalah suatu protokol yang menyampaikan berbagai informasi dari server website untuk ditampilkan kepada para user atau pemakai melalui web browser.[14]

Open Web Application Security Project (OWASP) merupakan organisasi non profit berfokus pada peningkatan keamanan perangkat lunak, OWASP menjadi framework yang digunakan oleh pengembang dan ahli teknologi untuk mengamankan website. OWASP memberikan platform bagi pengembang untuk meningkatkan keamanan sistem melalui proyek yang *open-source* bersama dengan *tools* dari OWASP sebagai pendukung dalam pengujian sistem.[15]

3 METODOLOGI

Berikut kerangka kerja penelitian yang dilakukan dalam melakukan analisis kerentanan suatu website menggunakan aplikasi OWASP, dalam penelitian ini akan menggunakan website sebagai bahan percobaan untuk menguji bagaimana kerentanan website tersebut tehadap serangan-serangan yang dilakukan melalui aplikasi OWASP. Berdasarkan Gambar 1, tahapan yang pertama yaitu melakukan studi literatur dari beberapa sumber jurnal dalam rangka mencari informasi mengenai penyerangan dan kerentanan website, lalu mengumpulkan data untuk memperoleh informasi yang dibutuhkan dalam rangka mencapai tujuan penelitian, selanjutnya menganalisis dan melakukan pengujian kerentanan website menggunakan aplikasi OWASP dan mencari solusinya, langkah terakhir menarik kesimpulan dari hasil penelitian yang telah dilakukan.



Gambar 1. Kerangka kerja penelitian

Observasi dilakukan peneliti pada Selasa 28 Mei 2024 di Jalan 21 Maret RT 006 RW 003 Sungai Salak untuk memperoleh data dan informasi yang akurat tentang penelitian yang dilakukan dengan cara melakuan penelitian dan percobaan secara langsung pada website yang akan digunakan, berikut merupakan gambar pada saat peneliti melakukan observasi di SMAN 1 Tempuling

Gambar 2. Observasi di SMAN 1 Tempuling

Berdasarkan hasil wawancara yang dilakukan bersama jurnalistik di sekolah SMAN 1 Tempuling yakni ibu Rosdiana Halim, M.Pd. didapati hasil sebagai berikut : Website ini di operasikan sekitar 9 tahun yang lalu, pada website https://sman1tempuling.sch.id/ menggunakan software rumah web dan wordpres, keamanan yang digunakan ialah Anti CSRF yakni keamanan bawaan framework pada website tersebut. Dalam pengelolaannya website ini memiliki beberapa fungsi yakni dapat melihat berbagai macam informasi yang ada pada SMAN 1 Tempuling website ini juga dapat diakses oleh semua orang, berikut merupakan gambar pada saat peneliti melakukan wawancara dengan jurnalistik di sekolah tersebut.

Gambar. 3 Wawancara bersama jurnalistik SMAN 1 Tempuling

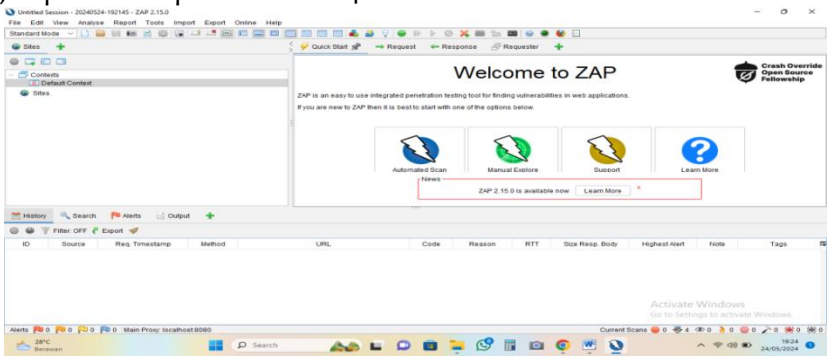
4 HASIL DAN PEMBAHASAN

Internet adalah komunikasi global yang menghubungkan seluruh komputer di dunia meskipun berbeda sistem operasi dan mesin. Internet adalah jaringan komputer yang menghubungkan antar jaringan secara global, internet dapat juga dapat disebut jaringan alam suatu jaringan yang luas. Seperti halnya jarigan komputer lokal maupun jaringan komputer area, internet juga menggunakan protokol komunikasi yang sama yaitu TCP/IP (Tranmission Control Protocol / Internet Protocol).

Keamanan yang suatu website merupakan salah satu prioritas yang sangat utama bagi seorang pengololah atau pengguna situs. Kebanyakan pengguna hanya mengutamakan design tampilan dan konten apa supaya menarik pengunjung sebanyak banyaknya. Jika seorang pengolah atau pengguna mengabaikan keamanan suatu website maka yang dirugikan adalah pengguna itu sendiri karena seseorang dapat mengambil data-data penting pada suatu website dan bahkan pula dapat dapat mengacak-acak tampilan website tersebut. Paling utama keamanan sebuah situs adalah melindungi komputer, aplikasi dan jaringannya dengan tujuan mengamankan informasi yang berada didalamnya.[16]

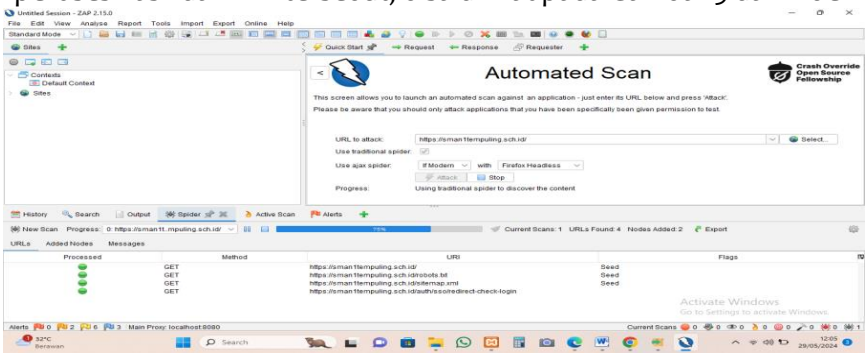
Implementasi sistem dilakukan dengan menyerang website dvdaily.store dengan menggunakan aplikasi owasp-zap yang nanti akan diuji coba untuk mengetahui kerentanan atau celah yang terdapat di website https://sman1tempuling.sch.id/, self test dapat dilakukan dengan menggunakan aplikasi OWASP dengan automated scanner atau manual expore yang bertujuan untuk mendapatkan hasil kerentanan terhadap website agar dapat menghindari serangan yang tidak diinginkan terjadi pada website tersebut. Maka dari itu diperlukan pengujian terhadap suatu website guna untuk menjaga keamanan data dari pihak yang tidak bertanggung jawab. Hal yang dibutuhkan untuk scanning vulnerability adalah sebuah link website yang sudah dipublikasikan ke

internet dan sudah mendapaatkan ijin untuk dapat melakukan scanning vulnerability website. Berikut adalah langkah-langkah dalam mencari celah keamanan dengan menggunakan OWASP melalui automated scanner dan manual expore: Pertama silahkan buka apliaksi OWASP, jika sudah terbuka maka akan ada 2 pilihan yang disediakan oleh aplikasi OWASP yaitu Automated scan dan Manual expore, dapat dilihat pada Gambar 4 dibawah ini.

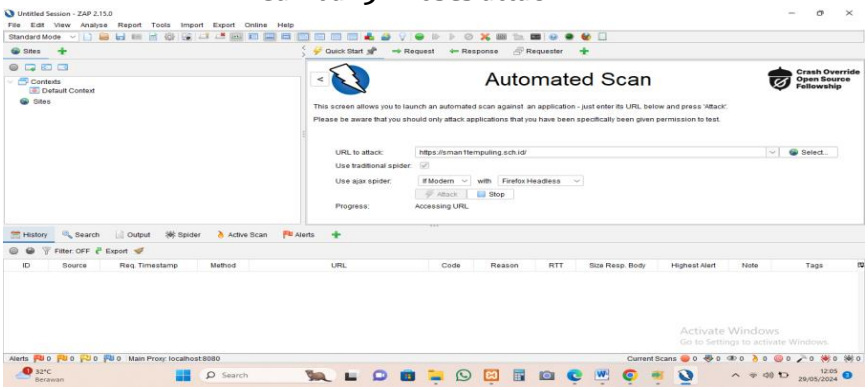


Gambar 4. Tampilan awal OWASP-ZAP

Jiika ingin menggunakan automated scan maka langsung saja klik automated scan, lalu masukan link *https://sman1tempuling.sch.id/* kemudian klik attack maka aplikasi OWASP-ZAP akan langsung memperoses hasil dari link tersebut, bisa dilihat pada Gambar 5 dan 6 berikut ini:

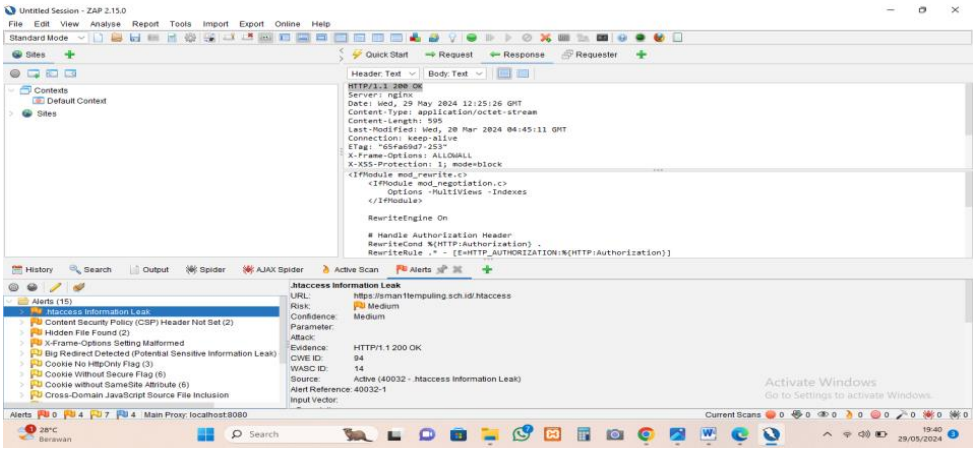


Gambar 5. Proses attack link



Gambar 6. Proses automated scan

Dalam proses pengujian atau validasi OWASP-ZAP menggunakan pemindaian aktif, aturan pemindaian aktif, peringatan, pengujian pada kontrol akses, aturan kontrol akses dan aturan kontrol pasif, sehingga hasil dari pemindaian ini menemukan kerentanan sedang, dangkal hingga informatif. Pada hal ini peneliti akan melakukan pengujian kerentanan secara menyeluruh pada website SMAN 1 Tempuling setelah proses *scanning* sudah selesai maka akan terlihat beberapa kerentanan menurut OWASP-ZAP berdasarkan hasil yang diperoleh, total kerentanan website tersebut berkisar 15 macam berdasarkan hasil level yang dapat dilihat pada Gambar 7 dan tabel 2 berikut.

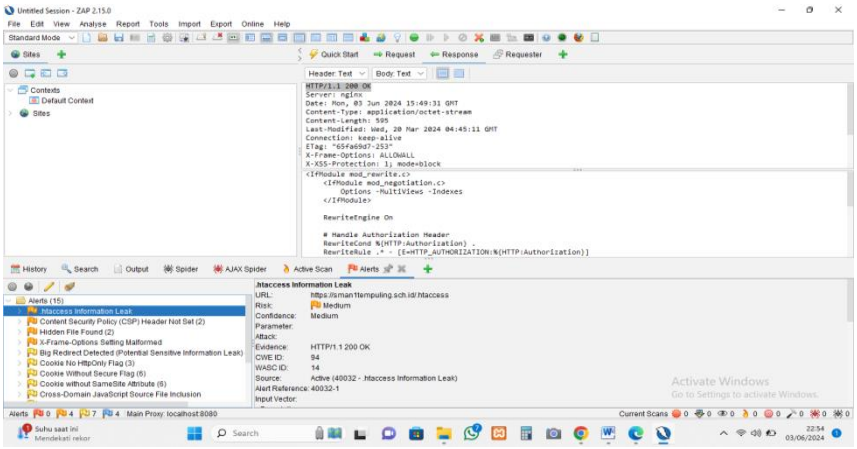


Gambar 7. Tampilan hasil kerentanan

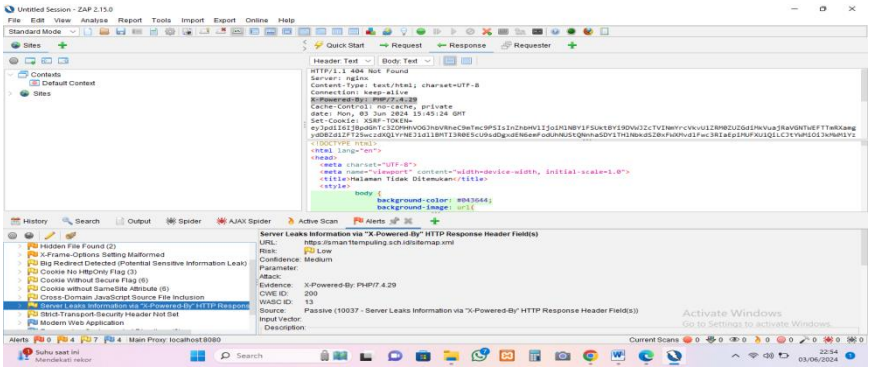
Tabel 2. Kerentanan berdasarkan hasil level menggunakan owasp-zap

No	Kerentanan website SMAN 1 Tempuling	Risk	Confidence
1	Htacces information leak	Medium	Medium
2	Content security policy (CSP) header not set	Medium	High
3	Hidden file founf	Medium	High
4	X-frame-options setting malformed	Medium	Medium
5	Big Redirect Detected (Potential Sensitive Information Leak)	Low	Medium
6	Cookie No HttpOnly Flag	Low	Medium
7	Cookie Without Secure Flag	Low	Medium
8	Cookie without SameSite Attribute	Low	Medium
9	Cross-Domain JavaScript Source File Inclusion	Low	Medium
10	Server Leaks Information via "X-Powered-By" HTTP Respons	Low	Medium
11	Strict-Transport-Security Header Not Set	Low	High
12	Modern Web Application	Informational	Medium
13	Re-examine Cache-control Directives	Informational	Low
14	Session Management Response Identified	Informational	Medium
15	User Agent Fuzzer	Informational	Medium

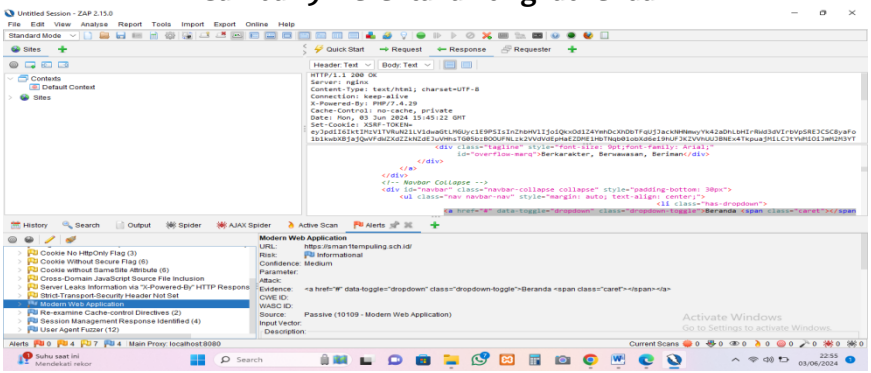
Setelah dilakukannya tahap scanning secara menyeluruh selanjutnya peneliti melanjutkannya ke tahap evaluasi, dimana peneliti melakukan evaluasi terhadap hasil dari penelitian, dengan melakukan pengujian pada website https://sman1tempuling.sch.id/. Berikut beberapa hasil pengujian kerentanan website secara menyeluruh dari berbagai tingkatan kerentanan mulai dari medium, low dan informational.



Gambar 8. Kerentanan Tingkat Sedang



Gambar 9. Kerentanan tingkat rendah



Gambar 10. Kerentanan tingkat infomartional

Terakhir peneliti melakukan uji coba terhadap hasil penelitian dan pemahaman kembali terkait penggunaan dari hasil penelitian. Pada tahap ini juga, pengujian dilakukan secara menyeluruh dan hasil dari pengujian tersebut dikelompokkan secara bertahap sesuai dengan tipe kerentanan, level kerentanan, dan rekomendasi yang disarankan guna mempermudah pihak administrator dapat mengetahui kerentanan dan berusaha memperbaiki kesalahan pada system.

Tabel 3. Hasil pengujian kerentanan secara menyeluruh

Vulnerability Type	*Level*	*Recommendation*
Htacces information leak	Medium	Pastikan file .htaccess tidak dapat diakses.
X-frame-options setting malformed	Medium	Pastikan pengaturan yang valid digunakan pada semua halaman web yang dikembalikan oleh situs Anda (jika Anda mengharapkan halaman tersebut hanya dibingkai oleh halaman di server Anda (misalnya, itu bagian dari FRAMESET) maka Anda sebaiknya menggunakan SAMEORIGIN, sebaliknya jika Anda tidak pernah mengharapkan halaman tersebut dibingkai, Anda harus menggunakan DENY. Sebagai alternatif, pertimbangkan untuk menerapkan arahan "frame-ancestors" dari Kebijakan Keamanan Konten.
Big Redirect Detected (Potential Sensitive Information Leak)	Medium	Pastikan tidak ada informasi sensitif yang bocor melalui respons pengalihan. Respons pengalihan seharusnya hampir tidak memiliki konten.
Cookie No HttpOnly Flag	Medium	Pastikan tanda HttpOnly disetel untuk semua cookie.
Cookie Without Secure Flag	Medium	Setiap kali cookie berisi informasi sensitif atau merupakan token sesi, maka cookie tersebut harus selalu diteruskan menggunakan saluran terenkripsi. Pastikan tanda aman disetel untuk cookie yang berisi informasi sensitif tersebut.
Cookie without SameSite Attribute	Medium	Pastikan atribut SameSite disetel ke 'longgar' atau idealnya 'ketat' untuk semua cookie.

Vulnerability Type	*Level*	*Recommendation*
Cross-Domain JavaScript Source File Inclusion	Medium	Pastikan file sumber JavaScript dimuat hanya dari sumber tepercaya, dan sumber tersebut tidak dapat dikontrol oleh pengguna akhir aplikasi.
Server Leaks Information via "X-Powered-By" HTTP Respons	Medium	Pastikan server web, server aplikasi, penyeimbang beban, dll. Anda dikonfigurasi untuk menyembunyikan header "X-Powered-By".
Modern Web Application	Medium	ni adalah peringatan informasional sehingga tidak diperlukan perubahan
Session Management Response Identified	Medium	Ini adalah peringatan informasional dan bukan kerentanan sehingga tidak ada yang perlu diperbaiki.
User Agent Fuzzer	Medium	Perlu peringatan
Content security policy (CSP) header not set	High	Pastikan server web, server aplikasi, penyeimbang beban, dll. Anda dikonfigurasi untuk menyetel header Kebijakan Keamanan Konten.
Hidden file founf	High	Pertimbangkan apakah komponen tersebut benar-benar diperlukan dalam produksi atau tidak, jika tidak maka nonaktifkan. Jika ya, pastikan akses ke sana memerlukan autentikasi dan otorisasi yang sesuai, atau batasi paparan ke sistem internal atau IP sumber tertentu, dll.
Strict-Transport-Security Header Not Set	High	Pastikan server web, server aplikasi, penyeimbang beban, dll. Anda dikonfigurasi untuk menerapkan Keamanan Transportasi Ketat
Re-examine Cache-control Directives	Low	Untuk konten yang aman, pastikan header HTTP kontrol cache disetel dengan "tanpa cache, tanpa penyimpanan, harus divalidasi ulang". Jika suatu aset harus di-cache, pertimbangkan untuk menyetel arahan "publik, usia maksimal, tidak dapat diubah"

5 KESIMPULAN

Berdasarkan hasil pengujian menggunakan OWASP-ZAP, website SMAN 1 Tempuling ditemukan memiliki total 15 kerentanan yang tersebar dalam berbagai tingkat risiko dan kepercayaan. Kerentanan-ketentanan tersebut bervariasi dari risiko tinggi hingga informasional. Beberapa kerentanan utama yang ditemukan termasuk kebocoran informasi melalui file .htaccess, header *Content Security Policy* (CSP) yang tidak diatur, dan atribut keamanan pada cookie yang tidak diterapkan dengan benar. Kerentanan ini menunjukkan adanya celah keamanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab jika tidak segera ditangani. Adapun tingkat keamanan website SMAN 1 Tempuling saat ini dapat dikategorikan sebagai **medium,** beberapa kerentanan berisiko tinggi dan menengah perlu segera diperbaiki untuk meningkatkan tingkat keamanan secara keseluruhan. Dengan mengimplementasikan rekomendasi di atas, diharapkan tingkat keamanan website sekolah dapat ditingkatkan menjadi lebih aman dan tahan terhadap serangan siber.

REFERENSI

[1] M. D. Al Vriano, "Pengujian Keamanan Web Juice Shop dengan MetodePentesting Berbasis Owasp Top 10," *J. Multidisiplin Saintek*, vol. 1, no. 6, pp. 81–90, 2023.

[2] P. R. Silalahi *et al.*, "Analisis Keamanan Transaksi E-Commerce dalam mencegah penipuan online," *J. Manajemen, Bisnis dan Akunt.*, vol. 1, no. 4, pp. 224–235, 2022.

[3] M. R. S. . Al'am'yubi and D. . Wijayanto, "Analisis Sistem Keamanan Website XYZ menggunakan Framework OWASP ZAP," *J. Ilmu Komput.*, vol. 3, no. 1, pp. 1–5, 2023, [Online]. Available: https://journal.umgo.ac.id/index.php/juik/index

[4] N. M. Farhan and B. Setiaji, "Indonesian Journal of Computer Science," *Indones. J. Comput. Sci.*, vol. 12, no. 2, pp. 284–301, 2023, [Online]. Available: http://ijcs.stmikindonesia.ac.id/ijcs/index.php/ijcs/article/view/3135

[5] J. Informatika *et al.*, "Analisis Keamanan Website menggunakan Standar Keamanan Open Web Application Security Project (OWASP) Studi Kasus Website penerimaan mahasiswa Baru Universitas Wahid Hasyim Semarang," vol. 5, no. 2, 2023.

[6] B. P. Sembiring, M. F. Sidiq, and W. A. Prabowo, "Analisis Keamanan Sistem Informasi menggunakan Metode Open Web Application Security Project (Owasp)," vol. 8, no. 3, pp. 3049–3054, 2024.

[7] N. A. Zahra, F. H. Zidane, and N. R. Kuslaila, "Analisis Keamanan Sistem Informasi pada Website Pt Sentra Vidya Utama (Sevima) menggunakan metode Owasp," *Pros. Semin. Nas. Teknol. dan Sist. Inf.*, vol. 3, no. 1, pp. 384–393, 2023, doi: 10.33005/sitasi.v3i1.564.

[8] 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, 2021, doi: 10.36418/jist.v2i4.124.

[9] M. A. Nurrizki *et al.*, "Analisis Keamanan Website Desa Budaya DIY dengan metode Penetration Testing (Pentest) dan OWASP ZAP," pp. 1–7, 2024.

[10] Naikson Fandier Saragih, Reinhard Tamalawe, and Indra M Sarkis, "Analisis dan Implementasi Secure Code pada Pengembangan Sistem Keamanan Website Fikom-Methodist.Com menggunakan Penetration Testing dan Owasp Zap," *J. TIMES*, vol. XII, no. 1, pp. 28–39, 2023.

[11] M. Wahidin, D. N. Rahayu, and R. M. Yulianto, "Analisis Kerentanan Situs Web KopKar Syariah PT BSIN menggunakan OWASP Zed Attack Proxy," *J. Interkom J. Publ. Ilm. Bid. Teknol. Inf. dan Komun.*, vol. 18, no. 4, pp. 25–31, 2024, doi: 10.35969/interkom.v18i4.321.

[12] A. Penilaian, K. Keuangan, D. I. Bursa, and E. Indonesia, "Berikut ini adalah versi HTML dari file http://jurnal.uinsu.ac.id/index.php/tawassuth/article/view/1710. Google membuat versi HTML dari dokumen tersebut secara otomatis pada saat menelusuri web. Kata kunci yang dipakai untuk penelusuran sudah distabilo an," vol. 1, no. December 2021, pp. 1–7, 2022.

[13] P. M. Purba, A. C. Amandha, R. H. Purnama, A. Ikhwan, P. S. Informasi, and S. D. Teknologi, "Page 1," vol. 4, no. 4, pp. 1–6, 2022.

[14] M. H. Wibowo, F. Ulum, N. Penulis, K. : Muhammad, and H. Wibowo, "Sistem Informasi Koperasi Simpan Pinjam Berbasis Website pada PRIMKOPPABRI Bandar Lampung," *J. Teknol. dan Sist. Inf.*, vol. 4, no. 1, pp. 22–27, 2023, [Online]. Available: https://jim.teknokrat.ac.id/index.php/sisteminformasi/article/view/2434

[15] S. Review, O. Web, A. Security, W. Security, and T. Guide, "(OWASP) pada Pengujian Keamanan Website : Literature Review".

[16] A. F. Hasibuan and D. Handoko, "Analisis Keretanan Website dengan Aplikasi Owasp Zap," *J. Ilmu Komput. dan Sist. Inf.*, vol. 2, no. 2, pp. 257–270, 2023, [Online]. Available: https://jurnal.unity-academy.sch.id/index.php/jirsi/article/view/51