

Analisis Sistem Keamanan Website XYZ Menggunakan Framework OWASP ZAP

Muhammad Ramdani Syam Al'Am'yubi^a, Danur Wijayanto, S.Kom., M.Cs^b.

^{a, b}Universitas Aisyiyah Yogyakarta, Jl. Siliwangi (Ring Road Barat) No. 63, Yogyakarta, Indonesia
Email: 2011501037@student.unisayogya.ac.id

ABSTRACT

Website services have become a platform that is most often used by almost all groups to get the information they need. Apart from that, website services can also become a media profile, such as the XYZ website, which is the website of Wahyu Arif Purnomo, a Security Analyst and Developer in one of the IT-related service provider companies. A website that can be accessed by all internet users requires an analysis of the security system to keep the website safe from the threat of hacker attacks. In testing website security system analysis using the Open Web Application Security Project (OWASP) method with software namely OWASP Zed Attack Proxy (ZAP) which is used to carry out security tests and recommendations for improvements that can be made on the website. on checking in progress to get 4 vulnerabilities. The results of 4 vulnerabilities get 2 low levels and 2 informational levels. With this analysis, you can find out the risk of a website's vulnerability and make it easier to take prevention based on the information you get.

Keywords: Website, OWASP ZAP, security system

ABSTRAK

Layanan *website* telah menjadi sebuah *platform* yang paling sering digunakan oleh hampir seluruh kalangan untuk mendapatkan informasi yang dibutuhkan. Selain itu layanan *website* juga bisa menjadi sebagai *media profile* seperti *website XYZ* yang merupakan *website* dari Wahyu Arif Purnomo seorang *Security Analyst* dan *Developer* disalah satu perusahaan Penyedia layanan berkaitan dengan IT. *Website* yang bisa diakses oleh semua pengguna internet diperlukan analisis sistem keamanan untuk menjaga *website* tetap aman dari ancaman serangan peretas. Dalam pengujian analisis sistem keamanan *website* menggunakan metode *Open Web Application Security Project (OWASP)* dengan perangkat lunak yaitu *OWASP Zed Attack Proxy (ZAP)* yang digunakan untuk melakukan pengujian keamanan dan rekomendasi perbaikan yang dapat dilakukan pada *website*. pada pengecekan berlangsung mendapatkan 4 kerentanan. Hasil 4 kerentanan mendapatkan 2 *level low* dan 2 *level informational*. Dengan adanya analisis ini, bisa mengetahui resiko kerentanan suatu *website* dan mempermudah melakukan pencegahan berdasarkan informasi yang di dapat.

Keywords: Website, OWASP ZAP, sistem keamanan

1. PENDAHULUAN

Perkembangan digital seperti *website* berkembang seiring berjalannya tahun. *Website* menjadi sumber informasi yang besar dan penggunaannya sudah banyak di terapkan di berbagai bidang[1]. Ini mempengaruhi keamanan *website* dimana ancaman siber tampak besar baik dari penjaga data pribadi pengguna dan peretas yang diluar untuk memanfaatkan celah yang ada untuk kepentingan pribadi[2]. Pengamanan sebuah *website* di perlukan sebab semakin banyak terbukanya pengetahuan tentang *hacking* dan *cracking*, didukung dengan *tools* yang bisa digunakan dengan gratis, dimana memudahkan terjadi serangan untuk mencari celah keamanan *website*[3]. Total serangan siber Indonesia mencapai angka 100 juta kasus hingga April 2022. Jenis serangan siber yang di sering di temukan Badan Siber dan Sandi Negara(BSSN) didominasi oleh serangan *ransomware* dan *malware*[4]. Kurangnya pemahaman terhadap keamanan *website* terutama pada sistem keamanan membuat masalah bagi pengembang.

Website merupakan kumpulan halaman yang menampilkan informasi, gambar, suara, video yang bersifat statis mau dinamis yang saling terkait yang dihubungkan dengan jaringan halaman[5]. *Website XYZ* merupakan *website profile* dari Wahyu Arif Purnomo yang merupakan *security analyst* dan *Developer* disalah satu perusahaan penyedia layanan berkaitan dengan IT.

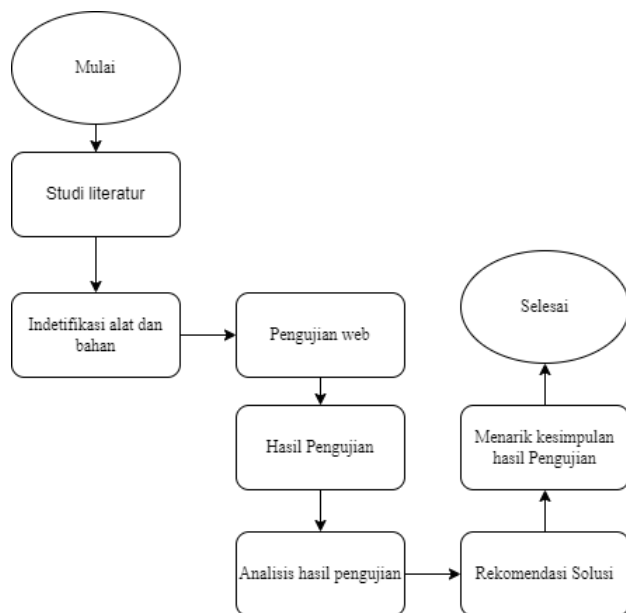
Dalam menjaga keamanan data dan informasi, terdapat metode yang dapat dilakukan yaitu metode *penetration testing*. *Penetration testing* merupakan proses yang melibatkan proses analisis kepada sebuah *website* untuk mencari potensi celah keamanan seperti kesalahan konfigurasi, kesalahan pengembangan *software* maupun *hardware*, dan kelemahan dalam logika proses[6]. Salah satu metode yang bisa dilakukan adalah *penetration testing* menggunakan *Open Web Application Security Project (OWASP)*[7].

Open Web Application Security Project (OWASP) merupakan aplikasi berbasis web pengujian keamanan *non profit* amal dari Amerika Serikat yang digunakan sebagai *framework* pengujian keamanan[8]. OWASP keanggotaan yang berasal dari para ilmuwan, peneliti, dan sektor swasta yang menerbitkan laporan artikel, alat atau peralatan, dan dokumen bersifat *open source*[9]. Penggunaan *framework OWASP* melakukan pendekatan sederhana untuk menghitung dan menilai risiko pada web. Dengan mengetahui risiko yang akan terjadi memudahkan untuk mengetahui kerentanan web dan mengurangi risiko yang terjadi[10].

2. METODOLOGI

Metodologi penelitian yang dilakukan untuk menyelesaikan penelitian ini menggunakan metode studi literatur, indentifikasi alat dan bahan, pengujian *website*, hasil pengujian, analisa hasil

pengujian, kesimpulan hasil Analisa, dan solusi yang diberikan. Langkah atau rancangan penelitian ditunjukkan pada Gambar 1.



Gambar 1. Alur Penelitian

2.1. Studi literatur

Tahap studi literatur ini mempelajari buku-buku, e-book, jurnal dan artikel tentang website, jaringan komputer, sistem keamanan dan materi-materi pendukung yang berkaitan dengan jurnal penelitian yang dibuat, sehingga membantu penulis menyelesaikan penelitian.

2.2. Identifikasi alat dan bahan

Pada tahap identifikasi alat dan bahan digunakan untuk mengetahui alat dan bahan yang di gunakan untuk pengujian analisis keamanan *website*. kebutuhan meliputi perangkat keras dan perangkat lunak.

- Perangkat keras
Perangkat keras yang digunakan adalah laptop dengan Sistem Operasi Windows 10 dengan *processor* Intel Core i5 gen 10 RAM 8GB dengan sistem operasi 64-bit.
- Perangkat lunak
Perangkat lunak yang digunakan adalah *Open Web Application Security Project*(OWASP) versi 2.10.0 dengan kategori pengunduhan Windows(64).

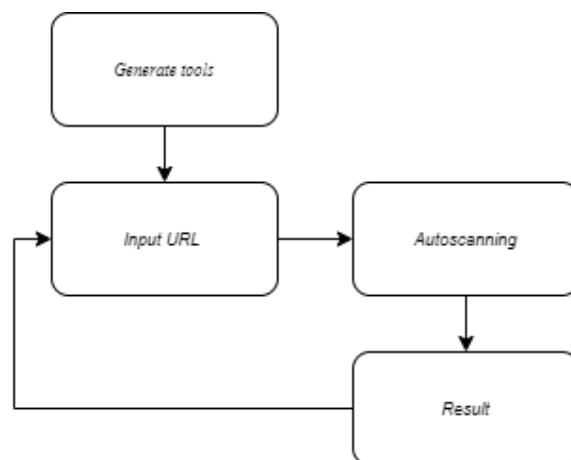
2.3. Pengujian Website

Tahap pengujian website menggunakan perangkat lunak *Open Web Application Security Project*(OWASP) dan *OWASP Zed Attack Proxy*(ZAP) yang ditunjukkan pada Gambar 2.

Website yang di uji adalah *website XYZ* yang merupakan *website profile* Wahyu Arif Purnomo. Hasil yang diperlukan di sesuaikan dengan keperluan yang menunjukkan jenis ancaman, peringkat risiko, jumlah skript, *CWE ID*, dan *WASC ID*.

Common Weakness Enumeration(CWE) merupakan daftar yang berisi jenis celah keamanan dan kerentanan yang di kategorikan untuk mengidentifikasi, memperbaiki, dan mencegah kerentanan[11].

Web Application Security Consortium(WASC) merupakan organisasi nirlaba yang berisi pedoman keamanan, informasi teknis, dan strategi penyerangan yang didasarkan kategori celah keamanan[12].



Gambar 2. Alur Pengujian

Hasil Pengujian diperoleh dari hasil uji yang dilakukan, hasil uji yang didapat inilah merupakan kerentanan-kerentanan yang ada pada *website XYZ*.

2.4. Hasil pengujian

Tahap hasil pengujian adalah tahap berisi penjelasan hasil yang didapatkan dari pengujian keamanan *website XYZ*.

2.5. Analisa hasil pengujian yang didapat

Tahap Analisa hasil pengujian yang di dapat dilakukan setelah hasil pengujian telah di peroleh dimana tahapan ini melalui beberapa tahapan yaitu identifikasi masalah, dampak dan keparahan resiko pada *website*, dan menyesuaikan peringkat resiko[13]. Risiko terdapat 5 level kategori risiko yang di tunjukkan pada Tabel 1.

Tabel 1. Level kategori risiko

Risk
High
Medium
Low
Informational

2.6. Solusi yang di berikan

Tahap Solusi yang diberikan melalui analisa pengujian untuk pencegahan kerentanan yang ada pada *website* terdeteksi oleh OWASP ZAP dan berdasarkan modul *Common Weakness Unumeration*(CWE).

2.7. Kesimpulan hasil Analisa

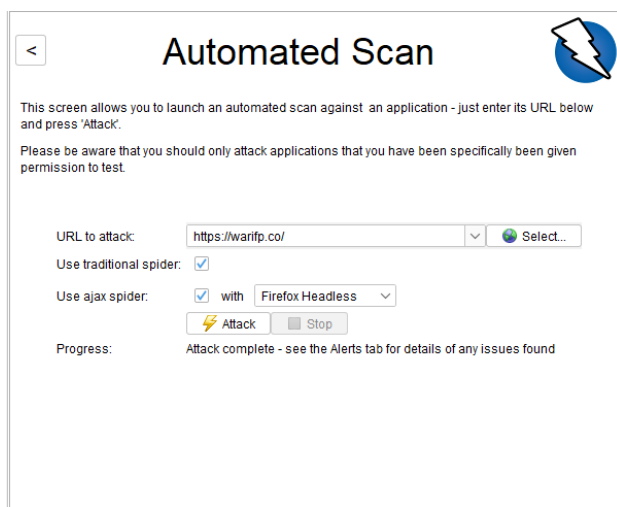
Tahap kesimpulan hasil analisa adalah tahap kesimpulan yang didapat dari Analisa hasil pengujian yang didapat yang sudah dilakukan menggunakan OWASP ZAP.

3. HASIL DAN PEMBAHASAN

Hasil pengujian yang dilakukan menggunakan OWASP ZAP 2.10.0 mendapatkan 4 kerentanan. Pengujian dilakukan menggunakan metode *autoscanning* untuk mendapatkan hasil yaitu jenis ancaman, peringkat risiko, *CWE ID*, *WASC ID*, dan memberikan solusi upaya pencegahan melalui *Common Weakness Enumeration(CWE)*.

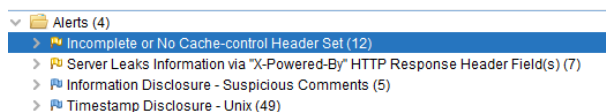
3.1. Pengujian website

Pengujian dilakukan menggunakan metode *penetration test* menggunakan *OWASP zed Attack Proxy(ZAP)*. Langkah yang dilakukan yakni melakukan *generate OWASP ZAP* dengan cara menghubungkan *OWASP* yang digunakan yaitu *Mozilla Firefox*, selanjutnya *input URL* yang ingin di *scan* untuk mendeteksi atau mencari celah kerentanannya yang di tunjukkan pada Gambar 3.



Gambar 3. Autoscanning OWASP

Autoscanning dilakukan untuk mendapatkan kerentanan yang ada pada *Website XYZ* yang ditunjukkan pada Gambar 4.



Gambar 4. Hasil autoscanning

Hasil pengujian kerentanan *website Warifp.co* menggunakan *OWASP ZAP* dengan proses *autoscanning* mendapatkan 4 kerentanan.

3.2. Hasil pengujian OWASP ZAP ZAP

Pengujian yang dilakukan menggunakan *OWASP ZAP* mendapatkan hasil yang di sudah disesuaikan keperluan yang menunjukkan jenis ancaman, peringkat risiko, jumlah skript *CWE ID*, dan *WASC ID*. proses pengujian mendapatkan 4 kerentanan yang di tunjukkan pada Tabel 2.

Tabel 2. Celah kerentanan

Alert	Risk level	Skript	CWE ID	WASC ID
Incomplete or No Cache-control Header Set	Low	12	525	13
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	7	200	13
Information Disclosure - Suspicious Comments	Informational	5	200	13
Timestamp Disclosure - Unix	Informational	49	200	13

Kerentanan yang didapat memiliki *risk level low* dan *informational*. Pada *risk level low* terdiri dari ancaman *Incomplete or No Cache-control Header Set* dan *Server Leaks Information via "X-Powered-By" HTTP*. Sedangkan pada *risk level informational* ancaman yang diperoleh adalah *Information Disclosure - Suspicious Comments* dan *Timestamp Disclosure - Unix*. *CWE ID* pada tiap kerentanan memiliki hasil yang sama yaitu *CWE ID 200* kecuali ancaman *Incomplete or No Cache-control Header Set* yang memiliki *CWE ID 525*.dimana *CWE ID 200* artinya pemaparan informasi sensitif yang tidak valid sedangkan *CWE IDE 525* Penggunaan *cache web browser* mengandung informasi sensitif[11]. Untuk *WASC ID* tiap kerentanan memiliki hasil yang sama yaitu *WASC ID 13* yaitu kebocoran informasi[12].

3.3. Solusi yang di berikan

Solusi yang diberikan untuk pencegahan kerentanan yang ada pada *website* terdeteksi oleh *OWASP ZAP* dan berdasarkan modul *CWE(Common Weakness Unumeration)*, bertujuan untuk mengurangi risiko kerentanan dan meningkatkan keamanan *website*.

Tabel 3. Kerentanan *website* dan solusi OWASP ZAP

Alert	Risk Level	Solusi
Incomplete or No Cache-control Header Set	Low	pastikan header HTTP kontrol-cache disetel dengan no-cache, no-store, must-revalidate.
Server Leaks Information via "X-Powered-By" HTTP	Low	Pastikan server web, server aplikasi, penyeimbang beban, dll. Anda dikonfigurasi untuk menekan header "X-Powered-By".

Response Header Field(s)		
Information Disclosure - Suspicious Comments	Information al	Hapus semua komentar yang mengembalikan informasi yang dapat membantu penyerang dan perbaiki masalah mendasar yang mereka rujuk.
Timestamp Disclosure - Unix	information al	Konfirmasikan secara manual bahwa data stempel waktu tidak sensitif, dan bahwa data tidak dapat digabungkan untuk mengungkapkan pola yang dapat dieksploitasi.

Pengujian dilakukan mendapatkan jenis kerentanan dan solusi. Hasil solusi yang didapat untuk tahapan pencegahan kerentanan yang ditampilkan pada Tabel 3. Menampilkan kerentanan, tingkat risiko, dan solusi yang didapat dari pengujian OWASP ZAP.

Terdapat 2 solusi yang untuk meningkatkan keamanan website yang diperoleh berdasarkan modul CWE yang di tunjukkan pada Tabel 4.

CWE ID	Celah Keamanan	Potential Mitigations
525	Use of Web Browser Cache Containing Sensitive Information	Fase: Arsitektur dan Desain Fase: Arsitektur dan Desain; Penerapan Lindungi informasi yang disimpan dalam cache. Gunakan kebijakan caching terbatas untuk formulir dan halaman web yang berpotensi memiliki informasi sensitif
200	Exposure of Sensitive Information to an Unauthorized Actor	Fase: Arsitektur dan Desain Strategi = Pemisahan Hak Istimewa Diperlukan sistem area yang aman dimana data sensitif tidak keluar dari sistem tidak di percaya dan jangan membiarkan data sensitif melakukan konfigurasi dengan situs yang tidak dipercaya. Untuk melakukan konfigurasi berikan kepada orang kepercayaan untuk mengelola hak istimewa dan mengakses informasi.

4. KESIMPULAN

Berdasarkan pengujian yang dilakukan menggunakan 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 memiliki ID yang sama yaitu WASC ID 13. Pengujian OWASP ZAP dan melalui modul *Common Weakness Unenumeration(CWE)* memberikan solusi untuk melakukan

pencegahan pada tiap kerentanan untuk mencegah kerentanan yang di terima. Pada OWASP memberikan solusi sesuai dengan jenis ancaman yang didapat sedangkan pada CWE memberikan solusi sesuai dengan CWE ID tiap kerentanan yang didapat pada OWASP ZAP.

DAFTAR PUSTAKA

- [1] K. Nisa, M. A. Putra, R. A. Siregar, and M. D. Irawan, "Analisis Website Tapanuli Tengah Menggunakan Metode Open Web Application Security Project Zap (Owasp Zap)," vol. 3, no. 4, pp. 308–316, 2022.
- [2] R. Ashar, "Jurnal Informasi dan Teknologi Analisis Keamanan Open Website Menggunakan Metode OWASP dan ISSAF," vol. 4, no. 4, 2022, doi: 10.37034/jsisfotek.v4i4.233.
- [3] Neng Ita Sopia Fazriani, Banta Cut, and Sanusi, "Uji Keamanan Website Terhadap Serangan Path Traversal Pada Website Pendaftaran Warga," *J. Ris. dan Inov. Pendidik.*, vol. 1, no. 1, pp. 15–20, 2019.
- [4] E. Andriya, "Antisipasi Bersama Tingkatkan Sistem dan Cegah Serangan Siber," *Ditjen Apl. Inform.*, pp. 1–3, 2022, [Online]. Available: <https://aptika.kominfo.go.id/2022/09/antisipasi-bersama-tingkatkan-sistem-dan-cegah-serangan-siber/>
- [5] W. Andriyan, S. S. Septiawan, and A. Aulya, "Perancangan Website sebagai Media Informasi dan Peningkatan Citra Pada SMK Dewi Sartika Tangerang," *J. Teknol. Terpadu*, vol. 6, no. 2, pp. 79–88, 2020, doi: 10.54914/jtt.v6i2.289.
- [6] A. Dharmawan, "Penetration Testing Menggunakan Owasp Top 10 Pada Domain Xyz. Ac. Id," *Electro Luceat*, vol. 8, no. 1, 2022, [Online]. Available: <https://jurnal.poltekstpaul.ac.id/index.php/jelekn/article/view/455%0Ahttps://jurnal.poltekstpaul.ac.id/index.php/jelekn/article/download/455/328>
- [7] G. Hendita, A. Kusuma, P. T. Informatika, F. Teknik, U. Pancasila, and J. Selatan, "7.+Jurnal+Teknologi+Informasi+-+Gregorius+-+OWASP-perbaikan," vol. 16, no. 2, pp. 178–186, 2022.
- [8] A. Elanda and R. Lintang Buana, "ANALISIS KEAMANAN SISTEM INFORMASI BERBASIS WEBSITE DENGAN METODE OPEN WEB APPLICATION SECURITY PROJECT (OWASP) VERSI 4: SYSTEMATIC REVIEW," 2020. [Online]. Available: www.xyz.com

- [9] A. Kurniawan, "Penerapan Framework OWASP dan Network Forensics untuk Analisis, Deteksi, dan Pencegahan Serangan Injeksi di Sisi Host-Based," *J. Telemat.*, vol. 14, no. 1, pp. 9–18, 2019, [Online]. Available: <https://journal.ithb.ac.id/telematika/article/view/267%0Ahttps://journal.ithb.ac.id/telematika/article/download/267/281>
- [10] B. Ghozali, K. Kusrini, and S. Sudarmawan, "Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating," *Creat. Inf. Technol. J.*, vol. 4, no. 4, p. 264, 2019, doi: 10.24076/citec.2017v4i4.119.
- [11] C. W. E. Version, "CWE Version 4.6".
- [12] W. S. C. (WASC) Application, "WASC Threat Classification," *Response*, pp. 1–172, 2010.
- [13] T. Hardiani, "Data Security Analysis with Framework OWASP on Website XYZ," 2017.