Digital Transformation Technology (Digitech) | e-ISSN: 2807-9000
Volume 4, **Number** 1, Maret 2024
https://doi.org/10.47709/digitech.v4i1.4485

Analisis Tingkat Resiko Pada Website Xyz Menggunakan Metode Owasp

Danur Wijayanto[1*], Arizona Firdonsyah[2]
[1,2]Universitas `Aisyiyah Yogyakarta
[1]danurwijayanto@unisayogya.ac.id , [2]arizona@unisayogya.ac.id

open access
Histori Artikel:
Diajukan: 8 Agustus 2024
Disetujui: 10 Agustus 2024
Dipublikasi:14 Agustus 2024
Kata Kunci:
OWASP, Cyber, Security, Website, Vulnerabilites

Abstrak
Website adalah salah satu platform yang digunakan untuk menunjukkan beberapa jenis informasi. XYZ website adalah sebuah website *Company Profile* dari Studi Tari. Website XYZ masih menggunakan keamanan web standar yang digunakan untuk mengamankan data pribadi. Web tersebut pernah diserang menggunakan serangan XSS *(Cross-Site Scripting)*, namun kerentanannya masih belum diketahui. Pada penelitian ini, peneliti menggunakan metode OWASP *(Open Web Application Security Projects)* untuk memindai web tersebut. Untuk menentukan tingkat resiko, peneliti menggunakan *likelihood* dan *impact*. Pemindaian kerentanan keamanan menghasilkan 11 kerentanan dengan tingkat resiko yang berbeda – beda seperti 9 kerentanan mempunyai kategori sedang dan 2 kerentanan mempunyai kategori rendah. Tingkat kerentanan tersebut dihitung setelah mementukan tingkatan *likelihood* dan *impact* dari hasil pemindaian menggunakan OWASP ZAP.

PENDAHULUAN

Websi menjadi salah satu contoh dari perkembangan Teknologi Informasi. Website terdiri dari beberapa halaman yang kemudian dikombinasikan menjadi satu kesatuan dan dapat diakses secara luas melewati browser yang terhubung ke internet. Berdasarkan contributor (n.d.), website merukana keseluruhan halaman website yang ada pada suatu website yang terdapat informasi.Tim Berners-Lee (1980) adalah penemu website pertama, tujuannya adalah untuk membuat sebuah website yang memungkinkan pertukaran informasi sehingga memudahkan peneliti untuk bekerja. (Maharani, 2017). Konten dari website harus diperhatikan dengan baik dan jelas karena konten merupakan gambaran umum dari isi website yang akan ditampilkan kepada pembaca. Konten dapat disesuaikan dengan arah tujuan dibangunnya website tersebut, sehingga dapat bervariasi dalam menarik pembaca.

Website merupakan salah satu platform atau halaman yang digunakan untuk menampilkan berbagai macam informasi, XYZ merupakan website berupa *company profile* dari Studio Tari. Situs web ini menggunakan keamanan web dasar yang digunakan untuk mengamankan data pribadi. Pemantauan keamanan website sangat diperlukan apakah website tersebut aman atau terdapat celah keamanan untuk serangan keamanan (Maharani, 2017).

Sanggar Tari XYZ berdiri pada tanggal 2 Februari 1980 dan menjadi sebuah lembaga pendidikan yang bergerak dalam bidang pendidikan dan pelatihan. Sanggar Tari XYZ mempunyai pegawai diantaranya adalah pemilik sanggar yang berperan sebagai pimpinan dan kepala sanggar, selanjutnya terdapat admin , staf pemasaran, staf dokumentasi foto dan video, staf pengeditan video, dan staf foto, serta staf teknologi dan jaringan.

Pada tahun 2017 Studio Dance membangun website dengan nama xyz.com yang berisi profil dan aktivitas Studio Tari. Setelah itu website mendapatkan serangan XSS. Suspensi pun dilakukan pada website XYZ oleh penyedia layanan hosting dan akhirnya website/domain berhasil dikembalikan, namun celah keamanan yang diserang belum diketahui. Dalam penelitian ini, kami menggunakan metode OWASP untuk menentukan kerentanan situs xyz dan memberikan peringkat tingkat keparahan risiko.

STUDI LITERATUR

OWASP adalah organisasi/perusahaan nirlaba yang fokus pada aplikasi keamanan data website. Metode OWASP juga digunakan oleh Yudiana et al (2021) untuk menguji kerentanan dan menghindari pihak yang tidak bertanggung jawab. Berdasarkan hasil OWASP ZAP, Sistem Informasi e-office STMIK ROSMA mempunyai 13 kerentanan. Hasil OWASP menunjukkan 10 kerentanan sehingga perlu dilakukan pemeliharaan website oleh pengembang *e-office* STMIK ROSMA. Penelitian yang dilakukan oleh Yunus (2019) menggunakan metode yang mirip dengan kombinasi *Security Tools Project* (STP) dengan tujuan menguji keamanan dan kerentanan data situs www.xyz.com. Dengan menggunakan metode OWASP, penelitian ini menentukan kerentanan yaitu pengujian otentikasi, pengujian otorisasi, pengujian manajemen sesi, dan penanganan kesalahan. Metode OWASP dapat dikombinasikan dengan metode lain, seperti penelitian yang dilakukan oleh Hariyadi & Nastiti (2021) yang mana

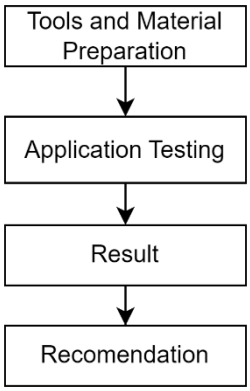
Metode *Sudomy* digunakan sebagai alat untuk membantu Pengumpulan Informasi dan Pemetaan Jaringan. Penelitian yang dilakukan oleh Ghozali et al. (2019) membahas tentang tingkat risiko pada sistem informasi harga komoditas utama dengan menggunakan Metode OWASP. Security gap testing digunakan untuk mendeteksi kerentanan website menggunakan Aplikasi Acunetix. Hasil keseluruhan yang diperoleh menunjukkan bahwa *Framework Codeigniter* dan PHP *Native* mempunyai tingkat kerentanan yang sama pada *likelihood* sedang, dampak pada tingkat rendah. Priyawati et al. (2022) juga melakukan pengujian dan analisis kerentanan situs web menggunakan OWASP. Hasil pengujian menunjukkan website aplikasi target memiliki 12 kerentanan dengan rincian 8,3% pada tingkat kerentanan tinggi atau 1 peringatan, 41,7% pada tingkat sedang, 33,3% pada tingkat rendah, dan 16,7 pada tingkat informasi. Kerentanan tersebut berkaitan dengan hal-hal yang berkaitan dengan *A01-Broken Access Control*, *A03-Injection*, *A05-Security Misconfiguration*, *A08-Software* dan Kesalahan Integritas Data.

Penelitian serupa dilakukan oleh Elanda & Buana (2020), The OWASP version 4 method: Systematic Review diterapkan pada proses pengujian keamanan sistem aplikasi ujian online yang mengakibatkan beberapa kategori kerentanan otentikasi dan manajemen sesi yang perlu diperbaiki. Kuncoro & Fayruz Rahma (2022) melakukan penelitian serupa dengan Metode OWASP: Scoping Review yang bertujuan untuk menganalisis penggunaan Framework OWASP dalam pengujian keamanan sistem komputer. Hasil pencarian keamanan dan pengujian celah keamanan ditemukan beberapa kelemahan dan kerentanan pada sistem. Penelitian lain yang dilakukan oleh Utoro et al (2020) melakukan analisa keamanan data menggunakan aplikasi OWASP ZAP pada website e-learning SMKN 1 Cibatu dengan Penetration Testing Execution Standard (PTES). Dari empat jenis serangan yang diketahui dari Langkah pasca eksploitasi, terdapat tiga serangan yang berhasil dieksploitasi yaitu Eavesdropping, cross-site Scripting, dan Cross-Site Request Forgery yang menggunakan aplikasi Wireshark, Pentest-tools.com dan OWASP ZAP.

Perbandingan antara metode OWASP dengan ISAF dilakukan oleh Guntoro et al (2020) di Universitas Lancang Kuning untuk menganalisis keamanan Open Journal System (OJS). Metode ISSAF menggunakan aplikasi Whois Domain sedangkan Metode OWASP menggunakan aplikasi OWASP ZAP, hasil yang didapat dari metode kedua adalah tidak ditemukan ancaman serangan yang mampu ditembus oleh hacker. Penelitian lain yang menggunakan OWASP dan ISAF dilakukan oleh Dirgahayu (2015) dengan menggunakan metode ini untuk menguji kerentanan keamanan data Web Server di IKIP PGRI Madiun. Hasil yang diperoleh menunjukkan bahwa Web Server masih mempunyai kerentanan.

METODE

Tahapan yang dilakukan dalam penelitian ini adalah Persiapan Alat dan Bahan, Pengujian Aplikasi, Hasil, Perhitungan Rating Risiko OWASP, dan Rekomendasi. yang ditunjukkan pada Gambar 1.



Gambar 1. Metode Penelitian

Persiapan Alat dan Bahan

Peneliti menggunakan Sistem Operasi Windows 10 64 bit dan OWASP ZAP versi 2.11.1 untuk pengujian keamanan website.

Pengujian Aplikasi

OWASP ZAP merupakan aplikasi *open source* yang berguna untuk melakukan uji penetrasi pada prinsip OWASP untuk mendeteksi keamanan aplikasi berbasis web. OWASP ZAP berfokus untuk mendeteksi kerentanan website dengan metode manual dan otomatis. ZAP akan menghasilkan laporan atau hasil darinya dalam bentuk format HTML dan XML. *Penetration test* atau biasa disebut dengan proses pemeriksaan keamanan website dan menghasilkan laporan kerentanan (*OWASP Zed Attack Proxy Project*, 2023).

Hasil

Terdapat 11 tes panduan yang ada di OWASP terdiri dari :

1. Pendahuluan dan Tujuan, informasi yang diberikan berkaitan dengan bahasa pemrograman untuk website aplikasi dan tentang metafile aplikasi.
2. *Configuration* dan *Deployment Management Testing,* jaringan konfigurasi yang digunakan untuk melakukan pengujian dengan ekstensi file serta untuk mencari backup yang berisi informasi penting dan pengujian dengan metode HTTPS.
3. Pengujian Manajemen Identitas, Pengujian Manajemen akun mencakup akses aplikasi dan aturan untuk proses pendaftaran akun dan peningkatan akun.
4. Pengujian Otentikasi, menguji akses yang benar seperti kerentanan transversal direktori, lupa kata sandi dan fitur pintu belakang.
5. Pengujian Otorisasi, aktivitas login sebagai pemilik akun dan login menggunakan aktivitas ilegal.
6. *Session Management Testing*, menguji sesi dari *cookies* yang digunakan pemilik untuk mengakses tanpa *login*.
7. Pengujian Validasi Input, pengujian SQL *Injection*, XML *Injection*, dan CSS digunakan untuk pengujian validasi dengan *script* yang dapat dieksekusi.
8. Pengujian Penanganan Kesalahan, pengujian dilakukan untuk menguji kesalahan yang terjadi, informasi yang muncul adalah kredensial, misalnya database, *bug*, atau komponen yang terkait dengan aplikasi yang dijelaskan pada
9. Pengujian Kriptografi lemah, pengujian kriptografi aplikasi untuk mengenkripsi informasi rahasia dan internal
10. *Business Logic Testing*, pengujian dilakukan terhadap kerentanan keamanan pada aplikasi yang terfokus pada proses bisnis.
11. *Client-side Testing*, pengujian kerentanan memanfaatkan *script* yang dijalankan, celah-celah yang dapat muncul dari klien dan hal ini dapat membahayakan klien.

Ada metode OWASP Untuk menentukan dan menggabungkan risiko kuantitas (*OWASP Risk Rating Methodology*, n.d.) :

1. *Likelihood*

Tahapan ini mempunyai 2 komponen yang mendukung kemungkinan-kemungkinan yang ada, yaitu faktor agen ancaman dan faktor kerentanan.

Threat Agent Factors

Terdapat 4 atribut pada faktor ini yaitu *Skill Level*, *Motive*, *Opportunity*, dan *Size*. *Skill Level* mencakup seberapa terampil suatu ancaman. *Motive* mencakup bagaimana penyerang termotivasi untuk menentukan dan mengeksploitasi kerentanan. *Opportunity* mencakup sumber daya yang dibutuhkan untuk menentukan dan mengeksploitasi kerentanan. *Size* mencakup seberapa besar ancamannya. Rumus yang digunakan untuk mendapatkan *Threat Agent* dengan Metode OWASP *Risk Rating* menggunakan Persamaan 1.

$$Threat\ Agent = \frac{Skill\ level+Motive+Opportunity+Size}{4} \quad (1)$$

Vulnerability Factors

Vulnerability factor mencakup atribut termasuk *ease of discovery*, *ease of exploit*, *awareness* dan *intrusion detection*. *Ease of discovery* mencakup seberapa mudah bagi agen ancaman untuk menemukan kerentanannya, *ease of exploit* mencakup seberapa mudah bagi agen ancaman untuk mengeksploitasi kerentanan dengan benar, *awareness* mencakup seberapa terkenal kerentanan tersebut bagi agen ancaman dan *intrusion detection*. termasuk seberapa besar eksploitasi yang dapat dideteksi. Rumus yang digunakan untuk memperoleh *Vulnerability* dengan Metode OWASP *Risk Rating* menggunakan Persamaan 2.

$$Vulnerability = \frac{Discovery+Exploity+Awareness+\ Inst.Detection}{4} \quad (2)$$

2. *Impact Score*

Terdapat dua komponen dari *Impact Score* : *Technical Impact Factors* dan *Business Impact Factors*.

Technical Impact Factors

Ada beberapa atribut termasuk hilangnya kerahasiaan, hilangnya integritas, hilangnya ketersediaan, dan hilangnya akuntabilitas. Hilangnya kerahasiaan mencakup seberapa banyak data yang dapat diungkapkan dan seberapa sensitif data tersebut, hilangnya integritas mencakup seberapa banyak data yang dapat rusak dan

seberapa rusaknya, hilangnya ketersediaan mencakup berapa banyak layanan yang dapat hilang dan betapa pentingnya layanan tersebut, dan hilangnya akuntabilitas mencakup apakah akan mengambil tindakan agen ancaman dapat ditelusuri ke individu. Rumus yang digunakan untuk memperoleh Technical Impact Factors menggunakan Persamaan 3.

$$Technical\ Impact = \frac{confidentiality+integrity+availabillity+\ accountabillity}{4} \quad (3)$$

Business Impact Factors

Business Impact Factor memiliki beberapa atribut, termasuk *financial damage*, *reputation damage*, *non-compliance*, dan *privacy violation*. *Financial damage* mencakup seberapa besar kerugian finansial akibat eksploitasi, *reputation damage* mencakup apakah hasil eksploitasi akan merusak reputasi yang akan merugikan bisnis, *non-compliance* mencakup seberapa banyak paparan yang tidak diketahui, dan *privacy violation* mencakup seberapa banyak informasi identitas pribadi dapat diungkapkan, Rumus yang digunakan untuk memperoleh Faktor Dampak Bisnis menggunakan Persamaan 4.

$$Business\ Impact = \frac{financial\ damage+repulation\ damage+\ non-compliance+p.violation}{4} \quad (4)$$

HASIL

Pemindaian OWASP ZAP menghasilkan 11 kerentanan yaitu: *Directory Browsing, Vulnerable JS Library, X-Frame-Options Header Not Set, Absence of Anti-CSRF Tokens, Application Error Disclosure, Cross-Domain JavaScript Source File Inclusion, Incomplete or No Cache-control Header Set, Secure Pages Include Mixed Content, Timestamp Disclosure – Unix, X-Content-Type-Options Header Missing, and Information Disclosure Suspicious Comments*. Pengujian ini mendapatkan hasil uji dari Metode GET dan POST yang dilakukan ke website tujuan.

Hasil diperoleh berdasarkan pembobotan skor *Likelihood* dan *Impact* untuk menentukan skor risiko keseluruhan yang dihitung berdasarkan tingkat keparahannya dengan menggunakan *risk rating calkulator*. Hasil yang diperoleh adalah 9 kerentanan keamanan yang memiliki peringkat risiko keparahan dengan kategori sedang dan 2 kerentanan keamanan yang memiliki peringkat risiko keparahan kategori rendah. Hasil keseluruhan ditunjukkan pada Tabel 1.

Tabel 1 *Hasil skor resiko keseluruhan*

Vulnerability ID	**Nama Celah**	***Likelihood***	***Impact***	***Overall Risk Rating***
(OTG-CONFIG-004)	***Directory Browsing*** - *Review Old, Backup and Unreferenced Files for Sensitive Information*	Medium	Medium	Medium
(OTG-CONFIG-006)	***Secure Pages Include Mixed Content*** - *Test HTTP Methods*	Medium	Medium	Medium
(OTGINPVAL-015)	***Vulnerable JS Library*** - *Testing for incubated vulnerabilities*	Medium	Medium	Medium
(OTG-INPVAL001)	***Cross-Domain JavaScript Source File Inclusion*** - *Testing for Reflected Cross Site Scripting*	Medium	Medium	Medium
(OTGSESS-004)	***X-Frame-Options Header Not Set*** - *Testing for Exposed Session Variables*	Medium	Low	Low
(OTGSESS-005)	***Absence of Anti-CSRF Tokens*** - *Testing for Cross Site Request Forgery (CSRF)*	Medium	Medium	Medium
(OTG-CRYPST-003)	***Application Error Disclosure*** - *Testing for Sensitive information sent via unencrypted channels*	Medium	Low	Low

Vulnerability ID	**Nama Celah**	***Likelihood***	***Impact***	***Overall Risk Rating***
(OTGAUTHN-006)	***Incomplete or No Cache-control Header Set*** - *Testing for Reflected Cross Site Scripting*	Medium	Medium	Medium
(OTG-BUSLOGIC004)	***Timestamp Disclosure – Unix*** - *Test for Process Timing*	Medium	Medium	Medium
(OTG-CLIENT-011)	***X-Content-Type-Options Header Missing*** - *Test Web Messaging*	Medium	Medium	Medium
(OTG-INFO-005)	***Information Disclosure – Suspicious Comments*** – *Review Webpage Comments and Metadata for Information Leakage*	Medium	Medium	Medium

PEMBAHASAN

Tahapan ini berisi analisis terhadap hasil yang diperoleh dari perhitungan risiko dengan metode rating risiko OWASP. Metode ini telah digunakan sebelumnya oleh Hardiani et al. (2022) namun tidak menjelaskan secara rinci hasil dari tingkat keparahan risiko. Tingkatan pada *likelihood* dan *Impact* mempunyai 3 kategori batas nilai yang telah ditentukan seperti terlihat pada Tabel 1.

Tabel 2 *Likelihood* dan *Impact Level*

Likelihood and *Impact*	
0 to < 3	LOW
3 to < 6	MEDIUM
6 to 9	HIGH

Berdasarkan Tabel 2, dilakukan pembobotan faktor *likelihood* terhadap 11 kerentanan yang didapatkan. Tabel hasil analisa *likelihood* ditunjukkan pada Tabel 3. Pada Tabel 3, menunjukkan terdapat 11 kerentanan yang mempunyai level *likelihood* sedang.

Tabel 3 Tabel Hasil Pembobotan *Likelihood*

No	Vuln ID	Nama Celah	*Threat Agent Factors*				*Vulnerability Factors*					
			Skill Level	*Motive*	*Opportunity*	*Size*	*Ease of discovery*	*Ease of exploit*	*Awareness*	*Intrusion Detection*	TOTAL	*Likelihood*
1	(OTG-CONFIG-004)	***Directory Browsing*** - *Review Old, Backup and Unreferenced Files for Sensitive Information*	3	4	7	9	9	3	6	3	5,500	Medium
2	(OTG-CONFIG-006)	***Secure Pages Include Mixed Content*** - *Test HTTP Methods*	6	4	7	2	9	5	9	1	5,375	Medium
3	(OTGINPVAL-015)	***Vulnerable JS Library*** - *Testing for incubated vulnerabilities*	3	9	7	2	9	3	9	3	5,625	Medium
4	(OTG-INPVAL001)	***Cross-Domain JavaScript Source File Inclusion*** - *Testing for Reflected Cross Site Scripting*	6	4	4	2	9	3	6	8	5,250	Medium
5	(OTGSESS-004)	***X-Frame-Options Header Not Set*** - *Testing for Exposed Session Variables*	1	4	7	6	1	1	6	8	4,250	Medium
6	(OTGSESS-005)	***Absence of Anti-CSRF Tokens*** - *Testing for Cross Site Request Forgery (CSRF)*	6	9	4	2	9	5	4	1	5,000	Medium
7	(OTG-CRYPST-003)	***Application Error Disclosure*** - *Testing for Sensitive information sent via unencrypted channels*	6	4	4	2	9	5	6	1	4,625	Medium
8	(OTGAUTHN-006)	***Incomplete or No Cache-control Header Set*** - *Testing for Reflected Cross Site Scripting*	6	4	4	2	9	1	6	1	4,125	Medium

No	Vuln ID	Nama Celah	*Threat Agent Factors*				*Vulnerability Factors*					
			Skill Level	*Motive*	*Opportunity*	*Size*	*Ease of discovery*	*Ease of exploit*	*Awareness*	*Intrusion Detection*	TOTAL	*Likelihood*
9	(OTG-BUSLOGIC 004)	***Timestamp Disclosure – Unix*** *- Test for Process Timing*	1	4	9	9	1	1	6	8	4,8 75	Medium
10	(OTG-CLIENT-011)	***X-Content-Type-Options Header Missing*** *- Test Web Messaging*	3	1	9	4	1	9	4	8	4,8 75	Medium
11	*(OTG-INFO-005)*	***Information Disclosure – Suspicious Comments*** *– Review Webpage Comments and Metadata for Information Leakage*	1	4	7	9	1	9	4	3	4,7 50	Medium

Selain melakukan pembobotan *likelihood*, dilakukan juga pembobotan pada faktor *impact* terhadap 11 kerentanan yang telah ditemukan. Hasil pembobotan faktor *impact* ditunjukkan pada Tabel 4. Pada tabel tersebut menunjukkan terdapat 9 kerentanan yang mempunyai level *impact* sedang dan 2 kerentanan mempunyai level *impact* rendah.

Tabel 4 Tabel Hasil Pembobotan *Impact*

No	Vuln ID	Nama Celah	*Technical Impact Factors*				*Businesses Impact Factors*					
			Loss of Confidentiality	*Loss of integrity*	*Loss of availability*	*Loss of accountability*	*Financial damage*	*Reputation damage*	*Non-compliance*	*Privacy violation*	TOTAL	*Impact*
1	(OTG-CONFIG-004)	***Directory Browsing*** *- Review Old, Backup and Unreferenced Files for Sensitive Information*	6	1	7	7	1	1	2	3	3.5 00	Medium
2	(OTG-CONFIG-006)	***Secure Pages Include Mixed Content*** *- Test HTTP Methods*	7	3	5	7	3	5	5	3	4.7 50	Medium
3	(OTGINPVAL-015)	***Vulnerable JS Library*** *- Testing for incubated vulnerabilities*	2	3	5	7	3	5	7	3	4.3 75	Medium
4	(OTG-INPVAL001)	***Cross-Domain JavaScript Source File Inclusion*** *- Testing for Reflected Cross Site Scripting*	2	3	5	7	1	1	2	3	3.0 00	Medium
5	(OTGSESS-004)	***X-Frame-Options Header Not Set*** *- Testing for Exposed Session Variables*	7	1	1	1	1	1	2	3	2.1 25	LOW
6	(OTGSESS-005)	***Absence of Anti-CSRF Tokens*** *- Testing for Cross Site Request Forgery (CSRF)*	7	7	5	7	7	5	5	3	5.7 50	Medium
7	(OTG-CRYPST-003)	***Application Error Disclosure*** *- Testing for Sensitive information sent via unencrypted channels*	2	3	5	1	3	1	5	3	2.8 75	Low
8	(OTGAUTHN-006)	***Incomplete or No Cache-control Header Set*** *- Testing for Reflected Cross Site Scripting*	6	5	5	1	1	1	2	3	3.0 00	Medium
9	(OTG-BUSLOGIC004)	***Timestamp Disclosure – Unix*** *- Test for Process Timing*	6	1	5	7	1	5	2	3	3.7 50	Medium
10	(OTG-CLIENT-011)	***X-Content-Type-Options Header Missing*** *- Test Web Messaging*	6	1	5	7	1	1	5	3	3.6 25	Medium
11	*(OTG-INFO-005)*	***Information Disclosure – Suspicious Comments*** *– Review*	6	3	1	1	3	5	5	3	3.3 75	Medium

No	Vuln ID	Nama Celah	*Technical Impact Factors*				*Businesses Impact Factors*					
			Loss of Confidentiality	*Loss of integrity*	*Loss of availability*	*Loss of accountability*	*Financial damage*	*Reputation damage*	*Non-compliance*	*Privacy violation*	TOTAL	*Impact*
		Webpage Comments and Metadata for Information Leakage										

Setelah mendapatkan *likelihood* dan *Impact Risk*, selanjutnya menentukan nilai tingkat risiko secara keseluruhan yang dapat diperoleh dari Tabel 5 yang kemudian didapatkan hasil 9 kerentanan keamanan yang memiliki peringkat risiko keparahan dengan kategori sedang dan 2 kerentanan keamanan yang memiliki peringkat risiko keparahan kategori rendah

Tabel 5 Keseluruhan Level kerentanan berdasrkan *Likelihood* dan *Impact*

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
Likelihood				

KESIMPULAN

Pemindaian kerentanan keamanan dari website xyz menghasilkan 11 kerentanan yaitu: *Directory Browsing, Vulnerable JS Library, X-Frame-Options Header Not Set, Absence of Anti-CSR tokens, Application Error Disclosure, Cross-Domain JavaScript Source File Inclusion, Incomplete or No Cache-control Header Set, Secure Pages Include Mixed Content, Timestamp Disclosure – Unix, X- Content-Type-Options header missing, and Information Disclosure Suspicious Comments* Kerentanan-kerentanan tersebut mempunyai tingkat keparahan risiko yang berbeda-beda sebagai berikut: 9 kerentanan keamanan memiliki peringkat risiko dengan kategori sedang dan 2 kerentanan keamanan dengan tingkat dengan kategori rendah yang dihitung setelah ditentukan Tingkat *Likelihood* dan *Impact* berdasarkan hasil pemindaian menggunakan OWASP ZAP.

REFERENSI

Contributor, M. (n.d.). *What is the difference between webpage, website, web server, and search engine?* What Is the Difference between Webpage, Website, Web Server, and Search Engine? Retrieved October 9, 2023, fromhttps://developer.mozilla.org/enUS/docs/Learn/Common_questions/Web_mechanics/Pages_sites_servers_and_search_engines

Dirgahayu, D. R. T. (2015). Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server. *Networking Engineering Research Operation (NERO)*, *1*(3).

Elanda, A., & Buana, R. L. (2020). Analisis Keamanan Sistem Informasi Berbasis Website Dengan Metode Open Web Application Security Project (OWASP) Versi 4: Systematic Review. *CESS (Journal of Computer Engineering, System and Science)*, *5*(2), 185. https://doi.org/10.24114/cess.v5i2.17149

Ghozali, B., Kusrini, K., & Sudarmawan, S. (2019). Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating. *Creative Information Technology Journal*, *4*(4), Article 4. https://doi.org/10.24076/citec.2017v4i4.119

Guntoro, G., Costaner, L., & Musfawati, M. (2020). Analisis Keamanan Web Server Open Journal System (OJS) menggunakan Metode ISSAF dan OWASP (Studi Kasus OJS Universitas Lancang Kuning). *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, *5*(1), 45. https://doi.org/10.29100/jipi.v5i1.1565

Hardiani, T., Wijayanto, D., & Latifah, N. (2022). Data Security Analysis with OWASP Framework on Website XYZ. *CYBERNETICS*, *6*(01).

Hariyadi, D., & Nastiti, F. E. (2021). Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta. *Jurnal Komtika (Komputasi dan Informatika)*, *5*(1), 35–42. https://doi.org/10.31603/komtika.v5i1.5134

Kuncoro, A. W., & Fayruz Rahma, S. T. (2022). Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review. *AUTOMATA*, *3*(1), Article 1. https://journal.uii.ac.id/AUTOMATA/article/view/21893

Maharani, M. Z. (2017). Analisis Keamanan Website Menggunakan Metode Scanning dan Perhitungan Security Metriks. *e-Proceeding of Applied Science*, *3*(3), 1775.

OWASP Risk Rating Methodology. (n.d.). OWASP Risk Rating Methodology. https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

OWASP Zed Attack Proxy Project. (2023, January 15). OWASP Zed Attack Proxy Project. https://wiki.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Priyawati, D., Rokhmah, S., & Utomo, I. C. (2022). Website Vulnerability Testing and Analysis of Internet Management Information System Using OWASP. *International Journal of Computer and Information System (IJCIS)*, *03*(03).

Utoro, S., Nugroho, B. A., Meinawati, M., & Widianto, S. R. (2020). Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard. *MULTINETICS*, *6*(2), 169–178. https://doi.org/10.32722/multinetics.v6i2.3432

Yudiana, Y., Elanda, A., & Buana, R. L. (2021). Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP Top 10. *CESS (Journal of Computer Engineering, System and Science)*, *6*(2), 185. https://doi.org/10.24114/cess.v6i2.24777

Yunus, M. (2019). Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework OWASP Versi 4. *Jurnal Ilmiah Informatika Komputer*, *24*(1), 37–48. https://doi.org/10.35760/ik.2019.v24i1.1988