JATIKOM: Jurnal Aplikasi dan Teori Ilmu Komputer
ISSN: 2615-577X (Online)

Analisis Kerentanan Website XYZ Menggunakan Metode Vulnerability Assessment Penetration Testing Dan OWASP WSTG (Studi Kasus: XYZ)

Fajar Cahya Islami[#1]

Universitas Muhammadiyah Malang, *Indonesia*

[1]fajaarcahya94@webmail.umm.ac.id

Abstract*— *The rapid development of digital technology in the current era allows everyone to access a particular technology service, where there is a lot of important data that is very valuable in the current era. With so many people who can access a service, we cannot know whether the person has good or bad intentions. That way, the stored data must be maintained, safe, and its authenticity can be ascertained, so that organizations, governments, and every technology service are required to ensure the security of their systems, so that important data cannot be stolen, changed, or damaged by irresponsible people.

Key Words*— *Penetration Testing, OWASP, ZAP, Nessus, Vulnerability Assessment, Web Security.

Abstrak— **Pesatnya perkembangan teknologi digital di-era sekarang memungkinkan semua orang dapat mengakses suatu layanan teknologi tertentu, dimana banyak data penting yang sangat berharga di-era sekarang. Dengan banyaknya orang yang dapat mengakses suatu layanan, kita tidak dapat mengetahui orang tersebut berniat baik atau buruk. Dengan begitu data yang tersimpan harusnya terjaga, aman, dan dapat dipastikan keasliannya, sehingga organisasi, pemerintah, maupun setiap layanan teknologi dituntut untuk memastikan keamanan pada sistem mereka, agar data-data yang penting tidak dapat dicuri, diubah, maupun dirusak oleh orang yang tidak bertanggung jawab.**

***Kata kunci*— Pengujian Penetrasi, OWASP, ZAP, Nessus, Penilaian Kerentanan, Keamanan Web.**

I. PENDAHULUAN

Keamanan sistem informasi di-era digital ini sangatlah penting, dimana banyak sekali kasus serangan siber pada suatu sistem informasi. Salah satunya pada kasus yang terjadi pada tahun 2022 yang lalu, yaitu bjorka seseorang ataupun organisasi yang dimana membuat Negara Indonesia mengalami kerugian berupa pencurian data, dengan begitu hal ini juga dapat dialami oleh individu, instansi, maupun organisasi yang tentu sangat merugikan.

Indonesia mendapatkan serangan siber 1,225 miliar disetiap harinya, data ini diperoleh dari Kementerian Komunikasi dan Informatika dan dibenarkan oleh beberapa Kementrian di Indonesia. Dari milyaran kasus serangan siber, perusahaan keamanan yang bernama Siber, Eset menyebutkan ransomware masih menjadi momok untuk perusahaan pada tahun 2018 [1]. Begitu pula yang terjadi pada tahun 2022 jenis serangan yang sering terjadi antara lain adalah malware 56,84%, bocornya data 14,75% dan malware berbentuk trojan sebanyak 10,90% dari keseluruhan serangan siber [2]. Serangan terhadap sistem informasi dan data yang dikelola oleh organisasi, baik itu pemerintah, perusahaan, atau individu, semakin sering terjadi. Berdasarkan laporan dari Cyber Security dan Infrastructure Security Agency (CISA), lebih dari 70% organisasi global mengalami setidaknya satu insiden keamanan cyber pada tahun 2023. Peretasan akun, serangan ransomware, dan pencurian data pribadi adalah beberapa bentuk ancaman yang kian meningkat, menimbulkan kerugian finansial dan reputasi yang buruk [3]. Menurut Hinsa Siburian, kepala Badan Siber dan Sandi Negara (BSSN), pada tahun 2021 terjadi 888.711.736 serangan siber. Oleh karena itu, untuk melindungi informasi pribadi pengguna dan mengurangi kejahatan siber yang dapat menerobos sistem keamanan saat ini, situs web penelitian harus menjalani uji penetrasi [4].

Dengan kasus tersebut, dapat disimpulkan keamanan sistem informasi sangatlah penting, dikhawatirkan ada sekelompok orang maupun individu yang tidak bertanggung jawab merusak sistem, maupun mencuri data pada sistem website ataupun sistem informasi. Dengan meningkatnya teknik serangan, maka mengakibatkan kerentanan baru yang dapat dieksploitasi dan dimanfaatkan oleh orang yang tidak beretika yang bertujuan mencuri data maupun menghancurkan sistem pada kompetitor ataupun organisasi.

Vulnerability Assessment termasuk kedalam salah satu metode untuk mengamankan sebuah perangkat jaringan, sistem operasi, maupun sistem informasi yang sangat berguna di masa sekarang. Tujuan Vulnerability Assessment adalah menemukan suatu kerentanan yang dapat dipindai, dengan begitu dapat meminimalisir serangan maupun eksploitasi yang dilakukan oleh orang atau individu maupun kelompok yang tidak bertanggung jawab.

Penetration Testing juga termasuk kedalam salah satu cara atau metode untuk mengamankan suatu sistem operasi, perangkat, infrastruktur jaringan, maupun software, akan tetapi

memiliki perbedaan dengan Vulnerability Assessment. Penetration Testing bertujuan untuk mengidentifikasi kerentanan pada sistem. sehingga hal ini dapat digunakan sebagai pengujian keamanan sistem pada perusahan maupun organisasi, sebagai langkah identifikasi dan penanganan jika masalah ini datang mengancam keamanan pada sistem [5].

Dan sebagai acuan keamanan website salah satu perusahaan atau organisasi yaitu OWASP atau (Open Web Application Security Project) memberikan panduan yang harus dilakukan pengetesan keamanan meliputi sebagai berikut, "Information Gathering, Configuration and Deployment Management Testing, Identity Management Testing, Authentication Testing, Authorization Testing, Session Management Testing, Input Validation Testing, Testing for Error Handling, Testing for Weak Cryptography, Business Logic Testing, Client-side Testing, API Testing dan Reporting" [6]. OWASP memiliki metode keamanan data terbesar untuk sistem, data yang dikumpulkan untuk mempersiapkan standar keamanan pada aplikasi. sehingga kerangka kerja ini banyak digunakan sebagai pengujian pada aplikasi dalam vulnerability assessment. menggunakan kerangka kerja ini mengurangi risiko keamanan pada aplikasi [7].

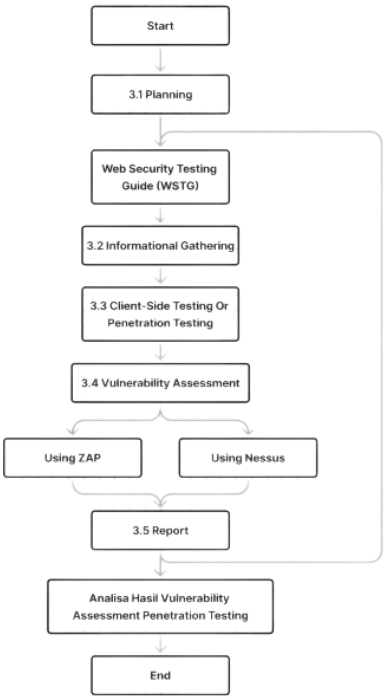
Dengan begitu metode OWASP (Open Web Application Security Project) dapat dipakai untuk menguji kerentanan keamanan pada sebuah website [8]. Namun pada penelitian ini penulis berfokus pada kerentanan Information Gathering untuk memfilter informasi awal yang biasanya banyak dimanfaatkan peretas, dan Client-side Testing untuk melakukan pengetesan yang bertujuan mencari kerentanan Cross-site Scripting atau XSS. Dengan begitu tujuan akhir dari penelitian ini berfokus untuk meningkatkan keamanan sistem informasi website XYZ, dari ancaman eksploitasi kerentanan yang didapatkan dengan menggunakan metode Vulnerability Assessment dan Penetration Testing dan berdasarkan OWASP Web Security Testing Guide (WSTG).

Pemerintahan Kota Malang merupakan suatu lembaga instansi pemerintahan Indonesia yang terletak di Kota Malang yang mempunyai halaman website yang berjalan secara operasional. Sistem pada Kota Malang tentunya memiliki banyak data maupun suatu informasi yang tentu sangat penting dan juga rahasia, dengan hal ini maka menjadi penting untuk mengamankan website tersebut, agar data yang ada tidak dicuri dan dimanfaatkan oleh orang yang tidak beretika.

Dari permasalahan yang terjadi pada pemerintahan maupun perusahaan, maka akan dilakukan sebuah pengujian pada web pemerintahan kota Malang menggunakan metode Vulnerability Assessment Penetration Testing dan OWASP WSTG.

II. METODE

Untuk dapat menyelesaikan penelitian ini, ada beberapa tahapan yang digunakan penulis dalam menyelesaikan penelitian ini yang tertera pada Gambar 1. meliputi Planning, Information Gathering, Vulnerability Assessment, Penetration Testing, dan Report.



Gambar 1. Metode penelitian

A. Planning

Pada tahapan ini, penulis melakukan perancangan yang akan dilakukan untuk mendukung penyelesaian tugas akhir. Ada dua tahapan pada Planning meliputi:

Identifikasi Alat dan Bahan Pengujian

Tahap ini melakukan identifikasi alat dan bahan yang digunakan untuk melakukan pengujian keamanan aplikasi website. Kebutuhan yang digunakan meliputi perangkat keras dan perangkat lunak seperti dibawah ini:

a. Perangkat Keras Perangkat keras atau device yang digunakan untuk melakukan pengujian keamanan website menggunakan laptop dengan virtualisasi Virtual Machine Kali Linux.
b. Perangkat Lunak atau aplikasi yang digunakan untuk melakukan pengujian keamanan website XYZ menggunakan software OWASP ZAP dan Nessus.

Untuk dapat menyelesaikan penelitian ini, ada beberapa tahapan yang digunakan penulis dalam menyelesaikan penelitian ini yang tertera pada Gambar 1. meliputi Planning, Information Gathering, Vulnerability Assessment, Penetration Testing, dan Report.

Skenario Pengujian

Pada tahapan ini menjelaskan skenario pengujian, berikut beberapa skenario pengujian yang dilakukan:

a. Tahapan pertama melakukan scanning menggunakan alat yang digunakan, yang bertujuan untuk mencari kerentanan.
b. Membuat tabel yang berisi berbagai macam serangan yang dapat dilakukan dari kerentanan yang didapatkan.
c. Melakukan analisis presentase kerentanan yaitu berupa Critical, High, Medium, dan Low berdasarkan alat yang digunakan.

d. Hasil dari kedua alat tersebut akan dibuat tabel priority yang berisi semua kerentanan yang didapatkan.
e. Memberikan rekomendasi perbaikan pada setiap kerentanan yang didapatkan, untuk mencegah dari serangan yang ada pada tabel berbagai macam serangan, yaitu pada point B.
f. Melakukan analisa hasil berdasarkan rekomendasi perbaikan yang telah diberikan.

B. Information Gathering

Pada tahapan ini menerapkan daftar pertama dari OWASP Web Security Testing Guide yang harus dilakukan pengetesan, yang berguna untuk mencari informasi target sebanyak-banyaknya yang bertujuan untuk mempermudah proses selanjutnya.

C. Vulnerability Assessment

Berikut tahapan pengujian menggunakan perangkat lunak OWASP Zed Attack Proxy (ZAP).

a. Yang harus dilakukan adalah mengunduh sertifikat perangkat lunak yang digenerate langsung dari ZAP dan menghubungkan sertifikat atau lisensi ke browser yang digunakan.
b. Inputkan IP Address yang digunakan pada website target atau alamat website yang ingin di scan kerentanannya.
c. Mulai melakukan scanning, dan elemen yang diuji seperti Injection, Information Disclosure, dan masih banyak lagi element lainnya.
d. Adalah hasil dari scanning yang nantinya akan dianalisis lebih lanjut.

Berikut tahapan pengujian menggunakan perangkat lunak Nessus.

a. Melakukan instalasi Nessus pada sistem operasi yang digunakan.
b. Melakukan registrasi dan aktivasi akun yang akan dikirim lewat email.
c. Inputkan IP Address atau Hostname website target.
d. Tools akan melakukan scanning dengan melakukan testing pada elemen- elemen yang ada pada website.
e. Hasil dari scanning akan dilakukan analisa lebih lanjut.

D. Penetration Testing

Tahap ini melakukan pengujian berdasarkan daftar OWASP WSTG yaitu pada point Client-side Testing yang bertujuan melakukan penetrasi untuk mendapatkan kerentanan Cross-site Scripting atau yang biasa disebut XSS. Cross-site Scripting atau serangan XSS adalah jenis serangan yang memanfaatkan celah keamanan pada sebuah sistem dengan melakukan sebuah penyuntikan script untuk mencuri beberapa data dan informasi yang bersifat rahasia [9].

E. Report

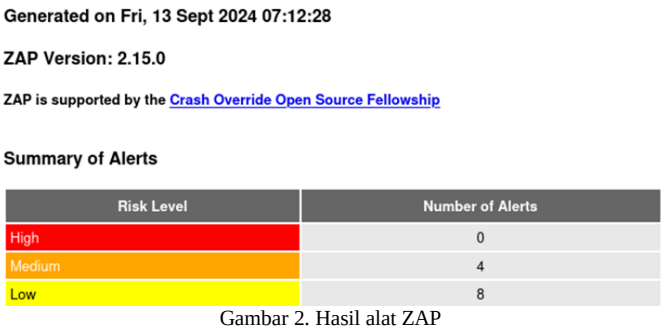
Pada tahap ini berisi penjelasan mengenai kerentanan apa saja yang didapatkan dari tools ZAP dan Nessus serta hasil dari Information Gathering dan Penetration Testing yang dilakukan pada sisi Client-side untuk mencari kerentanan XSS, serta memberikan rekomendasi perbaikan pada kerentanan yang didapatkan.

III. HASIL DAN PEMBAHASAN

A. Hasil Pemindaian Alat Owasp ZAP

Hasil dari pemindaian kerentanan atau Vulnerability Assessment pada alat ini mendapatkan kerentanan medium dan low seperti yang tertera pada gambar 2 yang dimana hasil dari kerentanan yang didapatkan mempunyai risikonya masing-masing.

Pemindaian kerentanan menggunakan alat ini juga membutuhkan waktu kurang lebih satu jam yang dimana alat ini lebih cepat daripada Nessus. Untuk rincian kerentanan tertera pada gambar 3 dan tabel 1.



Generated on Fri, 13 Sept 2024 07:12:28

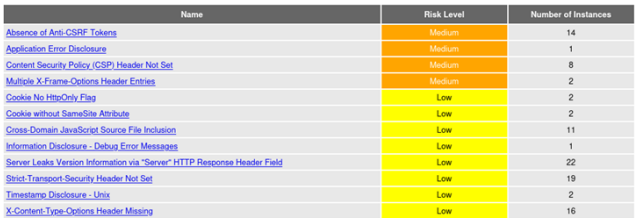
ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	8

Gambar 2. Hasil alat ZAP



Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	14
Application Error Disclosure	Medium	1
Content Security Policy (CSP) Header Not Set	Medium	8
Multiple X-Frame-Options Header Entries	Medium	2
Cookie No HttpOnly Flag	Low	2
Cookie without SameSite Attribute	Low	2
Cross-Domain JavaScript Source File Inclusion	Low	11
Information Disclosure - Debug Error Messages	Low	1
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	22
Strict-Transport-Security Header Not Set	Low	19
Timestamp Disclosure - Unix	Low	2
X-Content-Type-Options Header Missing	Low	16

Gambar 3. Detail kerentanan ZAP

TABEL 1. DETAIL KERENTANAN ZAP

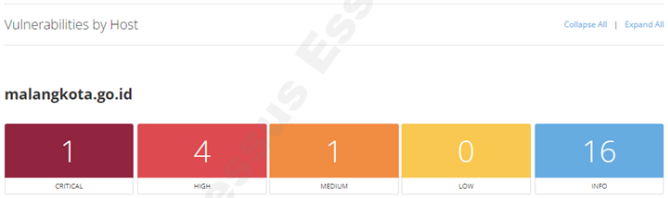
No	Nama Kerentanan	Mitigasi	Risiko
1	Absence of Anti-CSRF Tokens	Melakukan pemeriksaan terhadap header HTTP guna menentukan permintaan ini bersumber pada halaman yang diinginkan. sebab akan berdampak terhadap fungsionalitas, pengguna maupun proxy telah mematikan pengiriman kolom referer untuk alasan perlindungan pada data.	Medium
2	Application Error Disclosure	Melakukan pemeriksaan kode sumber di bagian ini. Gunakan halaman kesalahan khusus jika path atau input tidak sesuai.	Medium

No	Nama Kerentanan	Mitigasi	Risiko
		Pertimbangkan untuk menggunakan mekanisme untuk memberikan referensi serta identifikasi kesalahan yang jelas untuk pengguna.	
3	CSP Header Not Set	Memastikan server, maupun aplikasi hingga beban kerja dan semacamnya dilakukan konfigurasi. Kebanyakan pada web umumnya tidak mengatur header ini, dan sebaiknya melaukan konfigurasi pada CSP.	CSP Header Not Set
4	Multiple X-Frame-Options Header Entries	Pastikan hanya satu Header X-Frame-Options yang ada dalam respons.	Medium
5	Cookie No HttpOnly Flag	Pastikan HttpOnly dikonfigurasi ke seluruh cookie.	Low
6	Cookie without SameSite Attribute	Pastikan karakter SameSite dikonfigurasikan 'lax' atau yang sering digunakan yaitu 'strict' pada seluruh cookie.	Low
7	Cross-Domain JavaScript Source File Inclusion	memastikan data asal yaitu JavaScript memuat data dari tempat yang terpercaya, dan sumbernya asalnya tidak bisa dikendalikan oleh pengguna akhir.	Low
8	Information Disclosure - Debug Error Messages	Nonaktifkan pesan debugging sebelum mengirim ke produksi.	Low
9	Server Leaks Version Information via "Server" HTTP Response Header Field	“Pastikan server web dan aplikasi, load balancer dan semacamnya, untuk menghilang hal yang berkait dengan server, atau memberikan detail yang umum.	Low
10	Strict-Transport-Security Header Not Set	Pastikan server web, dan aplikasi, load balancer dan semacamnya, menerapkan konfigurasi Strict-Transport-Security.	Low
11	Timestamp Disclosure – Unix	Tegaskan bahwa data time stamp tidak sensitif, dan memberitahukan data tidak dapat digabung untuk melakukan kombinasi pola yang mungkin dapat dieksploitasi.	Low
12	X-Content-Type-Options Header Missing	Memastikan aplikasi maupun server menetapkan Header Content-Type, memastikan Header X-Content-Type-Options ke pengaturan 'nosniff' pada seluruh halaman. Apabila mungkin, dipastikan pengguna mengikuti browser web standar dan tidak menggunakan MIME-Sniffing, dan memungkinkan bisa mengarahkan pada web maupun server agar tidak menggunakan MIME-Sniffing.	Low

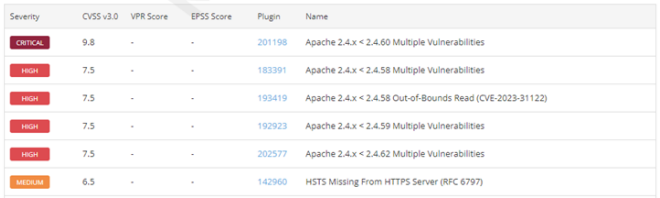
Nessus

Hasil dari pemindaian kerentanan atau Vulnerability Assessment pada alat ini mendapatkan kerentanan critical, high, dan medium seperti yang tertera pada gambar 4. Yang dimana hasil dari kerentanan yang didapatkan mempunyai risiko nya masing-masing.

Pemindaian kerentanan menggunakan alat ini juga membutuh kan waktu yang sangat lama, kurang lebih proses pemindaian membutuhkan waktu kurang lebih empat jam. Dan untuk rincian kerentanan dapat dilihat pada gambar 5 dan tabel 2.



Gambar 4. Hasil alat Nessus



Gambar 5. Detail kerentanan Nessus

TABEL 2. DETAIL KERENTANAN NESSUS

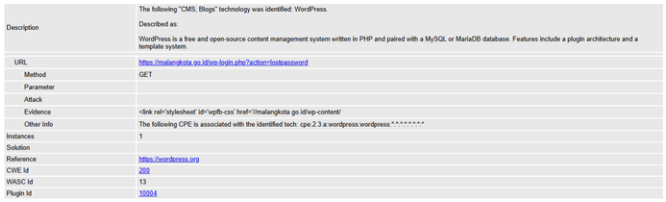
No	Nama Kerentanan	Mitigasi	Risiko
1	Apache 2.4.x Beberapa kerentanan	Tingkatkan ke Apache versi 2.4.60 atau yang lebih baru.	Critical
2	Apache 2.4.x Beberapa kerentanan	Tingkatkan ke Apache versi 2.4.58 atau yang lebih baru.	High
3	Apache 2.4.x Out-of-Bounds Read (CVE-2023-31122)	Tingkatkan ke Apache versi 2.4.58 atau yang lebih baru.	High
4	Apache 2.4.x Beberapa kerentanan	Tingkatkan ke Apache versi 2.4.59 atau yang lebih baru.	High
5	Apache 2.4.x Beberapa kerentanan	Tingkatkan ke Apache versi 2.4.62 atau yang lebih baru.	High
6	HSTS Missing From HTTPS Server (RFC 6797)	Konfigurasikan server web jarak jauh untuk menggunakan HSTS.	Medium

B. Hasil Web Security Testing Guide (WSTG)

Information Gathering

Hasil dari Information Gathering ini merupakan perpaduan penggunaan teknik otomatis dan teknik manual. Dan berikut ini hasil yang didapatkan:

a. Terdapat content management sistem atau cms wordpress yang tertera yaitu Gambar 6

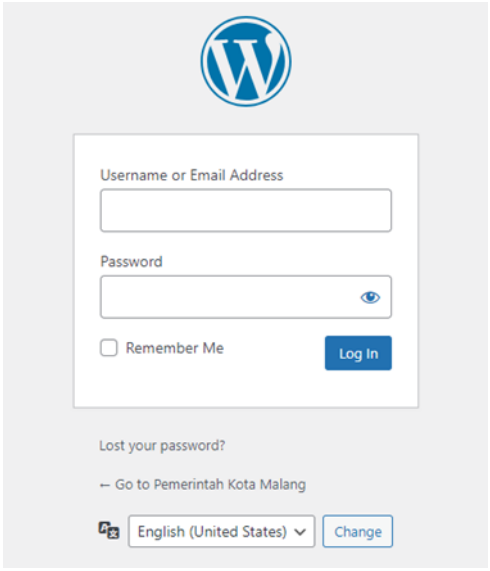


Gambar 6. CMS Wordpress

b. Terdeteksi menggunakan Wordpress versi 6.1.3 gambar 7

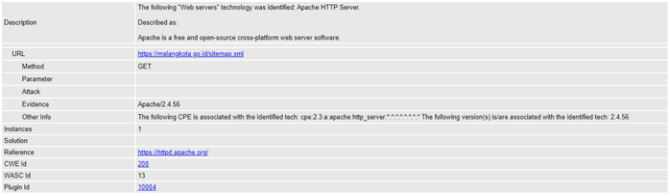
Gambar 7. Versi Wordpress

c. Terdapat link yang mengarah ke halaman login admin pada gambar 8, https://malangkota.go.id/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmalangkota.go.id%2Fwp-admin%2F



Gambar 8. Login page admin

d. Terdeteksi menggunakan web server apache versi ke Apache/2.4.56 gambar 9

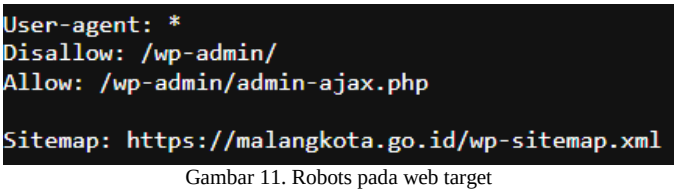


Gambar 9. Versi web server apache

e. Terdeteksi menggunakan sistem operasi Debian yang tertera, yaitu gambar 10

Gambar 10. Sistem operasi Debian

f. Halaman robots yang tertera pada web target seperti tertera, yaitu gambar 11



Gambar 11. Robots pada web target

g. Subdomain pada web target seperti yang tertera, yaitu gambar 12

Gambar 12. Subdomain pada web target

Clint-side Testing

Berikut ini merupakan hasil dari pengujian Client-side Testing pada web yang dituju, dengan menggunakan teknik manual dan teknik otomatis. Dan berikut hasil yang didapatkan:

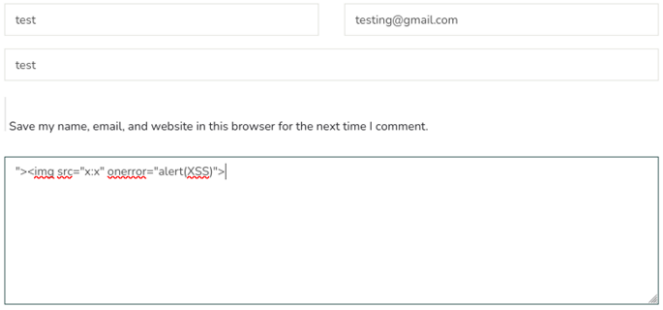
a. Percobaan XSS Pertama

Gambar 13. XSS testing pertama

Pada halaman search gambar 13 telah dilakukan pengetesan script XSS. XSS akan memberikan beberapa peringatan menggunakan kode “string” berformat “alert(1)” yang akan dikirim ke HTTP, sehingga XSS dapat memberikan suatu observasi dalam proses penetration testing untuk menggunakan payload “<script>alert(1);< /script> atau pada error =”alert(1);” (Zaidan, Noeraini, Sari, & Akbi, 2023). Akan tetapi tidak berhasil dikarenakan web target sudah melakukan sanitasi dengan tepat. Berikut jika dilihat dari respon alat BrupSuite pada gambar 14.

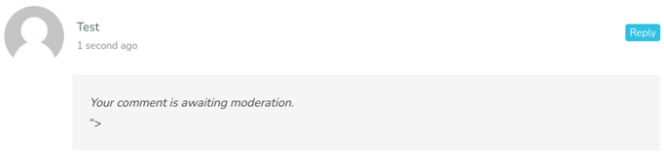
Gambar 14. Hasil XSS dari BrupSuite

b. Percobaan XSS Kedua



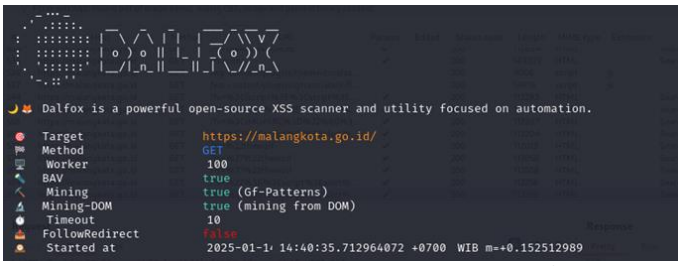
Gambar 15. XSS testing kedua

Pada halaman blog komentar gambar 15 telah dilakukan pengetesan script XSS, akan tetapi tidak berhasil dikarenakan web target sudah melakukan antisipasi XSS dengan tepat. Berikut hasil dari pengetesan yaitu pada gambar 16.



Gambar 16. Hasil testing kedua

c. Percobaan XSS dengan alat Dalfox



Gambar 17. Menggunakan alat otomatis dengan Dalfox

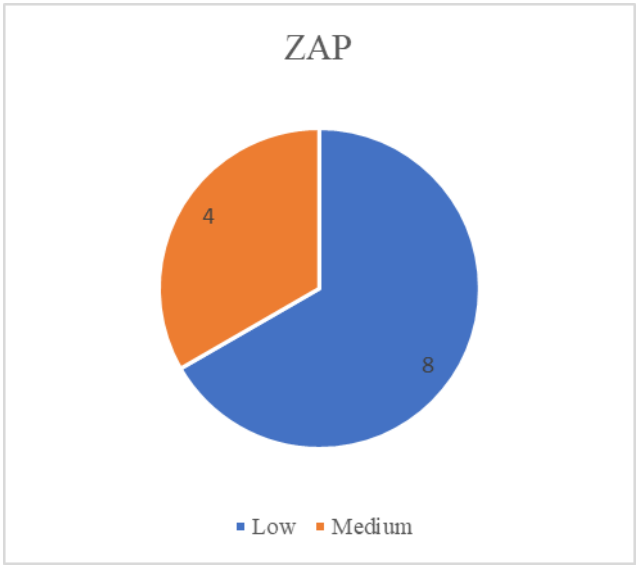
Berikut adalah percobaan menggunakan alat otomatis gambar 17 untuk mencari kerentanan XSS menggunakan alat Dalfox. Dengan hasil tidak mendapatkan kerentanan XSS apapun pada web target gambar 18

Gambar 18. Hasil dari alat Dafox

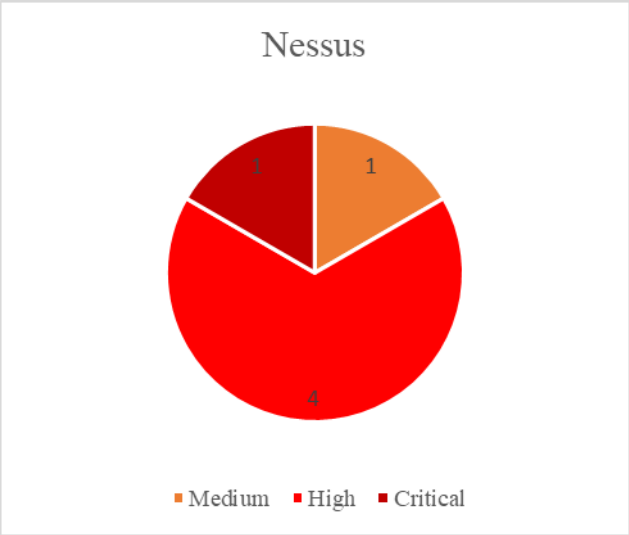
C. Report

Jumlah Kerentanan

Pada jumlah kerentanan ini adalah hasil pengujian menggunakan dua alat yaitu ZAP dan Nessus, dan dapat dilihat jumlah kerentanan yang didapatkan pada alat ZAP yaitu pada gambar 19, Sedangkan hasil kerentanan yang didapatkan dari alat Nessus yaitu pada gambar 20.



Gambar 19 Jumlah kerentanan dari alat ZAP



Gambar 20 Jumlah kerentanan dari alat Nessus

Pengujian Kerentanan XSS

Hasil dari pengujian Penetration Testing yang ditunjukkan pada web ini tidak menemukan kerentanan Cross-site Scripting apapun, dikarenakan pada web ini sudah melakukan pencegangan terhadap serangan XSS.

IV. KESIMPULAN

Tujuan penelitian ini menerapkan metode Vulnerability Assessment, Penetration Testing, dan OWASP Web Security Testing Guide untuk meningkatkan keamanan website xyz. Objek ini dipilih karena belum ada penelitian yang menerapkan metode Vulnerability Assessment, Penetration Testing dan OWASP WSTG terhadap website xyz.

Fase penelitian ini terdapat beberapa tahapan yang dilakukan, yaitu Planning untuk mempersiapkan alat dan bahan pendukung lainnya dalam penelitian ini, melakukan Information Gathering berdasarkan daftar OWASP WSTG yang harus dilakukan pengetesan untuk mendapatkan informasi sebanyak-banyaknya dari target yang dituju, setelah itu melakukan Vulnerability Assessment menggunakan alat ZAP dan Nessus untuk mendapatkan data kerentanan, selanjutnya melakukan pengetesan berdasarkan daftar OWASP WSTG yang mana dilakukan pada sisi Client-side Testing yang bertujuan untuk mencari kerentanan Cross Site Scripting atau XSS, serta melakukan Report yang nantinya akan dianalisis sebagai dasar keamanan pada sistem yang diuji serta memberikan rekomendasi perbaikan.

Luaran dari penelitian ini diharapkan dapat meningkatkan keamanan dari website xyz yang dituju, selain itu agar website xyz dapat terhindar dari serangan siber maupun eksploitasi kerentanan yang dapat merugikan website yang dituju.

Dari hasil pengujian alat ZAP dan Nessus mendapatkan kerentanan yang memiliki risiko yang berbeda, diantaranya Low, Medium, High hingga Critical. Dimana kerentanan yang didapatkan pada alat ZAP berupa kondisi Low berjumlah 8, dan kondisi Medium berjumlah 4. Dan pada alat Nessus mendapatkan kondisi Medium berjumlah 1, kondisi High berjumlah 4, dan kondisi Critical berjumlah 1. Sedangkan hasil dari pengujian Client-side Testing yang bertujuan mencari kerentanan pada XSS tidak ditemukan pada web xyz ini.

Berdasarkan hasil dari alat pengujian pada penelitian ini Nessus lebih unggul dalam mencari kerentanan pada server atau service yang berjalan, sedangkan pada ZAP unggul pada setiap rincian kerentanan yang ditemukan.

V. REFERENSI

[1] Andarista, K. (2023). Analisis tingkat keamanan website STIE Jambatan Bulan Timika menggunakan metode vulnerability assessment. Retrieved from https://eprints.umm.ac.id/id/eprint/1290/

[2] Andriyani, S., Sidiq, M. F., & Zen, B. P. (2023). Analisis celah keamanan pada website dengan menggunakan metode penetration testing dan framework issaf pada website SMK Al-Kautsar. Journal Informatic and Information Technology, 8798, 1–13. Retrieved from https://journal.ittelkom-pwt.ac.id/index.php/ledger/article/view/996

[3] Erlangga Chandra. (2023, January 4). BSSN: Hampir 1 miliar serangan siber hantam RI di 2022. Retrieved May 14, 2024, from https://www.cnnindonesia.com/teknologi/20230119144028-192-902537/bssn-hampir-1-miliar-serangan-siber-hantam-ri-di-2022

[4] Fandy, A. I. (2024). Pengujian celah keamanan website menggunakan teknik penetration testing dengan metode OWASP (Studi kasus: Website rapor online SMP Muhammadiyah 1 Malang). Retrieved from https://eprints.umm.ac.id/id/eprint/11704/2/BAB I.pdf

[5] Margareth, S., Zen, B. P., Saputra, A. I., Simatupang, Y. Y., Joy, C., Melody, P., … Sundoro, A. (2024). Uji penetration testing web server xyz, menggunakan metode OWASP top 10 dan CVSS, 1173–1182. Retrieved from https://scholar.google.co.id/citations?view_op=view_citation&hl=en&user=LHgcshQAAAAJ&sortby=pubdate&citation_for_view=LHgcshQAAAAJ:bEWYMUwI8FkC

[6] OWASP. (2020). WSTG - 4.2. Retrieved May 13, 2024, from https://owasp.org/www-project-web-security-testing-guide/v42/

[7] Rajasa M Agung. (2018). Indonesia diserang hacker miliaran kali tiap hari. Retrieved May 15, 2024, from https://www.kominfo.go.id/content/detail/11956/indonesia-diserang-hacker-miliaran-kali-tiap-hari/0/sorotan_media

[8] Ramadhani, R. F. (2023). Deteksi kerentanan keamanan website menggunakan metode OWASP (Studi kasus: Website satu data kabupaten Malang). Retrieved from https://eprints.umm.ac.id/id/eprint/1155/

[9] Zaidan, M., Noeraini, F., Sari, Z., & Akbi, R. (2023). Website vulnerability analysis of ab and xy office in East Java. Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika (JITEKI), 9(2), 455–492. https://doi.org/10.26555/jiteki.v9i2.26183

[10] Zen, B. P., Gultom, R. A. G., Reksoprodjo, A. H. S., Penginderaan, P. T., Pertahanan, F. T., & Pertahanan, U. (2020). Analisis security assessment menggunakan metode penetration testing dalam menjaga kapabilitas keamanan teknologi informasi pertahanan negara, 105–122. Retrieved from https://scholar.google.co.id/citations?view_op=view_citation&hl=en&user=LHgcshQAAAAJ&cstart=20&pagesize=80&sortby=pubdate&citation_for_view=LHgcshQAAAAJ:u-x6o8ySG0sC