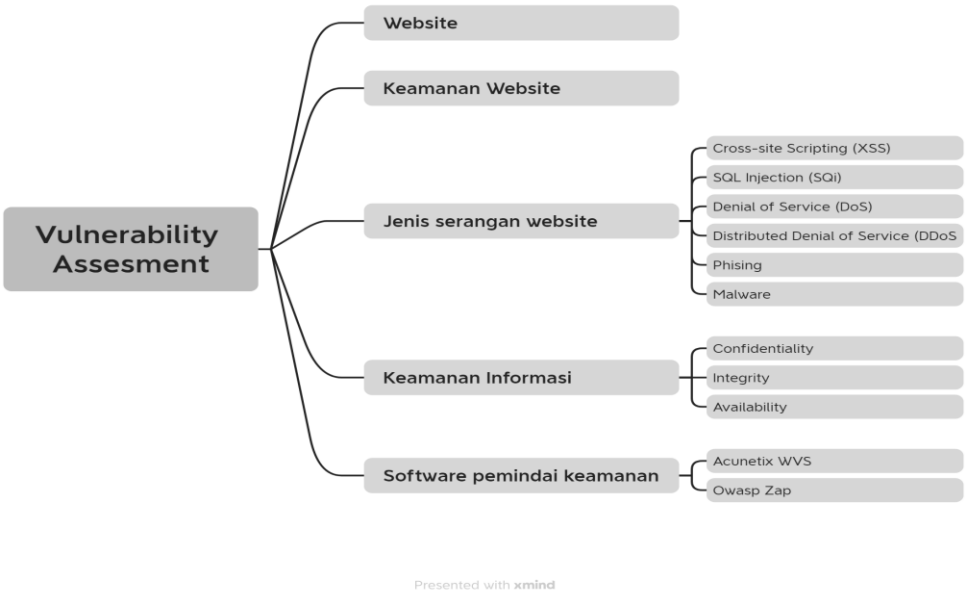
BAB II

LANDASAN TEORI



Gambar 2.1 Landasan Teori Website

2.1 Vulnerability Assesment

Vulnerability Assesment merupakan fase pendekatan untuk mengidentifikasi kerentanan yang ada dalam infrastruktur. Kerentanan dalam hal IT System dapat di defenisikan sebagai kelemahan potensial dalam sistem, atau jika dieksploitasi dapat mengakibatkan realisasi serangan terhadap system (Kumar, 2014).

2.2 Website

Website adalah alamat atu lokasi di dalam internet suatu halaman web, umumnya membuat dokumen HTML dan dapat berisi sejumlah foto atau gambar grafis, musik teks bahkan gambar yang bergerak. Dengan menggunakan teknologi tersebut, informasi dapat diakses selama 24 jam dalam satu hari dan dikelola oleh mesin (pardosi, 2002:2).

2.3 Jenis Serangan Website

Berikut adalah jenis-jenis serangan web (Jago Hosting, 2022) adalah

1. Cross-site Scripting (XSS)

   Cross site scripting (XSS) merupakan salah satu jenis serangan web yang perlu kamu hindari. Cara kerja serangan web ini adalah dengan memasukkan skrip dari sisi klien ke halaman web, kemudian mengakses informasi penting secara ilegal, meniru data dan identitas pengguna, juga memanipulasi pengguna agar membeberkan informasi penting.

2. SQL Injection (SQi)

   Jenis serangan web berikutnya adalah SQL injection. Penyerangan ini menggunakan SQi untuk mengambil akses informasi secara ilegal, kemudian mengubah pengguna baru, memanipulasi, hingga menghancurkan data penting.

3. Denial of Service (DoS) dan Distributed Denial of Service (DDoS)

   Perlu diketahui, jenis serangan web juga bisa menyerang website dengan cara membebani server yang ditargetkan, merusak infrastruktur dengan berbagai serangan atau traffic attacks. Serangan Dos dan DDoS bekerja ketika server tidak bisa lagi memproses permintaan masuk secara efektif, dan server menjadi lebih lambat, hingga akhirnya menolak perintah atau permintaan masuk dari pengguna sahnya.

4. Phising

   Phising adalah salah satu jenis serangan web yang menggunakan email, telepon atau teks untuk memanipulasi korban agar memberikan data penting atau sensitif dalam bentuk informasi login, atau detail kartu kredit. Serangan web phising ini

akan menyamar menjadi institusi resmi dan legal, kemudian akan mengirimkan URL yang digunakan untuk mengelabui pengguna.

5. Malware

Seperti yang telah dijelaskan sebelumnya, web security dapat melindungi website dari serangan malware yang berbahaya. Malware ini didesain oleh para hackers untuk melakukan eksploitasi dan merusak perangkat, server, hingga jaringan.

2.4 Keamanan Informasi

Menuru CISCO, keamanan informasi adalah proses dan perangkat yang didesain untuk melindungi informasi penting dan rahasia suatu bisnis dari terjadinya modifikasi dan kerusakan. Selain itu, juga bisa diartikan sebagai perlindungan kepada informasi atau sistem informasi dari akses, penggunaan, gangguan, modifikasi, dan perusakan yang tidak diizinkan. Menurut (Sarno, Iffano, 2009) Keamanan informasi terdiri dari perlindungan terhadap aspek Confidentiality, Integrity dan Avalability yaitu:

1. Confidentiality (kerahasiaan) Aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
2. Integrity (integritas) Aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin pihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.

3. Availability (ketersediaan) Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, 11 memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait.

2.5 Software pemindai keamanan

1. Acunetix Web Vulnerability adalah sebuah software yang berfungsi untuk melakukan pemindaian atas kelemahan yang bisa terjadi di suatu situs, software ini mampu memeriksa kelemahan web server maupun aplikasi web-nya dengan cepat, selain itu software ini juga memberikan saran yang harus dilakukan apabila ditemukan kelemahan pada website tersebut (Perdana, 2010:5).
2. *Owasp Zap* (Zed Attack Proxy) adalah pemindai keamanan aplikasi *open-source* yang dibuat oleh organisasi *OWASP*, *Owasp Zap* adalah suatu proyek dari *OWASP* yang paling aktif karena terus dikembangkan. Fitur yang ada dalam *Owasp Zap* antara lain yaitu: *Intercepting Proxy, Active and Passive Scanners, spider scan, report Generation, Brute Force (using OWASP dirbuster code), Fuzzing(using fuzzdb & OWASP JBrosfuzz), Extensibility, Auto tagging, Port scanner, Parameter analysis, Smart card support, Session comparison, invoke external apps, Api+headless mode, Dynamis SSL Certificates, Anti CSRF token handling* (Owaspzap, 2016).

2.6 State Of The Art

Pada state of the art ini, diambil beberapa contoh penelititan terdahulu sebagai panduan ataupun contoh untuk penelitian yang dilakukan yang nantinya akan menajdi acuan dan perbandingan dalam melakukan penelitian ini.

Tabel 2.1 Literatur Review

No	Peneliti / tahun	Judul	Masalah Penelitian	Metode	Web Aplication Vulnerability Scaner	State Of The Art
1.	Mayasari, Rini Ali Ridha, Azhari Juardi, Didi Ahmad Baihaqi, Kiki / 2020	Analisis Vulnerability pada Website Universitas Singaperbangsa Karawang menggunakan Acunetix Vulnerability	Melakukan proses scanning vulnerability pada website Universitas Singaperbangsa Karawang	Metode kualitatif	1. Acunetix WVS	Analisis kerentanan keamanan sistem web Universitas Singaperbangsa Karawang
2.	Wibowo, Feri Harjono, H Wicaksono, Agung Purwo / 2019	Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS	Proses VA terhadap website jurnal ilmiah UMP berbasis OJS (Open Jurnal Sistem)	Metode penelitian terapan	1. OpenVas 2. Acunetix WVS	Melakukan perbandingan antara OpenVas dan Acunetik WVS terhadap website jurnal ilmiah UMP berbasis OJS (Open Jurnal Sistem)
3.	Rusdiana Banta, Cut Sanusi / 2019	Analisa Keamanan Website Terhadap Serangan Cross-Site Request Forgery (CSRF)	Menemukan celah kerentanan website Pemerintah Kabupaten Aceh Timur terhadap serangan CSRF	Metode Pengumpulan Data	1. Acunetix WVS	Melakukan persentase kerentanan dari kedelapan website terbesar dengan Rank Vulnerability dengan tipe high pada website
4.	Baykara, Muhammet / 2018	Investigation and Comparison of Web Application Vulnerabilities Test Tools	Menganalisis alat uji kerentanan web	Metode perbandingan	1. Netsparker,2.Acunetix 3. Vega, 4. Owasp Zap 5. Wapiti, 6. IronWASP	Evaluasi aplikasi web scanner kerentanan dan alat pengujian keamanan web
5.	Qasaimeh, Malik Shamlawi, Ala'A Khairallah, Tariq / 2018	Black box evaluation of web application scanners: Standards mapping approach	Melakukan dan Menganalisis alat uji kerentanan web	Metode Blackbox	1. Acunetix WVS 2. Burp Suite 3. NetSparker 4. Nessus 5. Owasp Zap	Mengidentifikasi kemungkinan kerentanan aplikasi web

6.	Sagar, Deepika Kukreja, Sahil Brahma, Jwngfu Tyagi, Shobha Jain, Prateek / 2018	Studying Open Source Vulnerability Scanners for Vulnerabilities in Web Applications	Melakukan dan Menganalisis alat uji kerentanan web	Metode Perbandingan	1. Owasp Zap 2. Skipfish 3. W3af	Melakukan pengujian dan menganalisi alat uji dan menyimpulkan mana yang lebih baik
7.	Muhamad Akbar, S.T, M.IT dan Imam Perdana / 2018	Analisa Perbandingan Aplikasi Web antara Nikto dan Acunetix	Melakukan analisis mengenai celah – celah keamanan web	Metode Perbandingan	1. Nikto 2. Acunetix WVS	Untuk mengetahui perbandingan dari kedua aplikasi

Tabel 2.2 Penelitian Terdekat

No	Peneliti / tahun	Judul	Masalah Penelitian	Metode	Web Aplication Vulnerability Scaner	State Of The Art
1.	Qasaimeh, Malik Shamlawi, Ala'A Khairallah, Tariq / 2018	Black box evaluation of web application scanners: Standards mapping approach	Melakukan dan Menganalisis alat uji kerentanan web	Metode Blackbox	1. Acunetix WVS 2. Burp Suite 3. NetSparker 4. Nessus 5. Owasp Zap	Mengidentifikasi kemungkinan kerentanan aplikasi web
2.	Rendi / 2019	Perbaningan owasp zap dan nessus untuk mendeteksi vulnerability web dengan menggunakan black box testing	Mengetahui perbandingan kemampuan owasp zap dan nessus	Metode Blackbox	1. Owasp Zap 2. Nessus	Melakukan perbandingan wavs antara nessus dan owasp zap

Tabel 2.2 merupakan penelitian yang dijadikan acuan terkait perbandingan *Vulnerability Assessment (VA)* dengan menggunakan metode *blackbox testing.* Penelitian Qasaimeh, Malik Shamlawi, Ala'A Khairallah, Tariq (2018) melakukan identifikasi kemungkinan kerentanan.

Tabel 2.3 Matkriks Penelitian

No	Peneliti / tahun	Judul Penelitian	Ruang Lingkup																					
			Metode		Web Application Vulnerability Scaners																		Objek	
			Black box	White box	Acutix	Cenzic	N-Stalker	Rapid7	Netsparker	OWASP ZAP	W3AF	Iron WASP	Vega	Skipfish	Wapiti	Arachni	Nessus	Websecurify	Burpsuite	Nexpose	WPScan	Rips	DVWA	Studi Kasus
1	Bau et al. / 2010	State of the Art: Automated Black-BoxWeb Application Vulnerability Testing	✓		✓	✓	✓	✓																
2.	Suteva, Zlatkovski & Mileva / 2013	Evaluation and Testing Of Several Free/Open Source Web Vulnera Bility Scanners	✓				✓		✓	✓	✓	✓												
3	Mukho padhyay, Goswami & Mandal / 2014	Web Penetration Testing using Nessus and Metasploit Tool	✓		✓						✓			✓	✓	✓	✓	✓						✓
4	Shah & Mehtre / 2014	An Automated Approach to Vulnerability Assessment and Penetration Testing using Net-Nirikshak 1.0	✓																					✓

5	Dirgahayuprayudi & Fajaryanto /2015	Penerapan motede ISSAF dan OWASP versi 4 untuk uji kerentanan web	✓		✓																			✓
6	Joshi & singh / 2016	Performance Evaluation of Web Application Security Scanners for More Effective Defense	✓		✓				✓											✓				✓
7	Sagar et. al / 2018	Studying Open Source Vulnerability scanners For Vulnera Bilities in Web Applications	✓							✓	✓			✓									✓	
8	Hasan &Meva / 2018	Web Application Safety by Penetration Testing	✓		✓						✓										✓			✓	
9	Sando / 2021	Perbandingan Acunetix WVS dan Owasp Zap dalam menedeteksi vulnerability assessment berdasarkan keamanan informasi web kampus xyz			✓					✓														✓

Tabel 2.3 Matriks Penelitian nomor 9 merupakan kebaruan penelitian terkait perbandingan *Vulnerability Assessment (VA)* dengan menggunakan Metode Terapan terhadap hasil pemindaian dari kedua *software Acunetix WVS* dan *Owasp Zap* dengan parameter *SQL Injection, Cross-site Scripting (XXS), CSRF (Cross-Site Request Forgery)*.