BAB 2
LANDASAN TEORI

2.1. Tinjauan Pustaka

Berdasarkan permasalahan yang ada, penulis menggunakan berbagai referensi yang berhubungan dengan penelitian yang telah dilakukan sebelumnya. Pertama, penulis Purwantoro, 2017 dengan judul "Implementasi Metode *Online Scanner* Untuk Mencari Kerentanan Keamanan (*Vulnerability*) *Server* (Studi Kasus: Website www.unsika.ac.id)" Hasil pengujian yaitu prosedur pemindaian dapat dilakukan antara server pemindai yang digunakan melalui jalur *internal* (LAN) dan eksternal (layanan web). sucuri.net menyediakan informasi tentang sumber daya perangkat keras, perangkat lunak, dan alat keamanan. Setiap penyedia pemindaian kerentanan *online* memberikan informasi yang berbeda sesuai dengan layanan yang disediakan oleh penyedia tersebut[6].

Pada tahun 2019, penulis Riadi I., dkk, dengan penelitian berjudul "Analisis Keamanan *Website Open Journal System* Menggunakan Metode *Vulnerability Assessment*". Hasilnya menunjukkan bahwa pengujian alat OWASP pada OJS menghasilkan kerentanan tinggi 70, kerentanan sedang 1929, dan kerentanan rendah 4050. Jumlah kerentanan yang terdeteksi adalah 6049. Hasilnya menunjukkan bahwa OJS versi 2.4.7 mencakup berbagai kelemahan atau kerentanan yang tidak disarankan untuk digunakan, versi saat ini yang dirilis oleh *Public Knowledge Project* OJS harus digunakan sebagai gantinya (PKP) [5].

Pada tahun 2020, penulis Setiawan H., dkk, dengan penelitian berjudul *"*Analisis Kerentanan Menggunakan *Interactive Application Security Testing (IAST)* Untuk Aplikasi Situs Web Pemerintah X*"*. Hasilnya menunjukkan bahwa sebanyak 249 risiko kerentanan diidentifikasi dari prosedur ini. Berdasarkan dokumen OWASP Top 10-2017, kerentanan keamanan ditemukan pada injeksi (A1), otentikasi rusak (A2), paparan data sensitif (A3), kontrol akses rusak (A5), kesalahan konfigurasi keamanan (A6), lintas situs scripting (A7), menggunakan komponen dengan kerentanan yang diketahui (A9), dan pencatatan dan pemantauan yang tidak memadai (A10). Hasil analisis kerentanan menunjukkan bahwa perbaikan pada aplikasi berbasis web X-Government diperlukan[7].

Pada tahun 2020, penulis Mayasari R. dkk, dengan penelitian berjudul "Analisis *Vulnerability* pada Website Universitas Singaperbangsa Karawang menggunakan *Acunetix Vulnerability*". Hasil penelitian menunjukkan terdapat *error information CRLF injection/HTTP response splitting* antara variabel *input id* dan *cross-site scripting* pada variabel *input idjp* pada website Universitas Singaperbangsa Karawang, dan prosedur *Vulnerabilities scanning* pada website Universitas Singaperbangsa Karawang membutuhkan waktu lebih dari 12 jam, menghasilkan beberapa informasi tentang keamanan[8].

Tabel 2.1 Rangkuman Tinjauan Pustaka

Penulis	Tahun	Judul	Metode	Hasil	Perbandingan dengan Penelitian Sekarang
Purwantoro [6]	2017	Implementasi Metode *Online Scanner* Untuk Mencari Kerentanan Keamanan *(Vulnerability) Server* (Studi Kasus: *Website* www.unsika.ac.id)	*Online Scanner*	Tergantung pada layanan yang diberikan, setiap pemasok pemindaian kerentanan online memberikan berbagai informasi. Situs web sucuri.net menyediakan detail lengkap, termasuk sumber daya perangkat keras, perangkat lunak, dan solusi keamanan.	Subjek penelitian web server, lokasi penelitian, metode pengujian pendeteksi kerentanan menggunakan *Online Scanner.*
Riadi I., dkk.[5]	2019	Analisis Keamanan *Website Open Journal System*	*Vulnerability Assessment*	Pengujian alat OWASP pada OJS menghasilkan kerentanan tinggi 70, kerentanan sedang 1929, dan	Subjek penelitian web server, lokasi penelitian, *Tools* pendeteksi *Vulnerability*

Penulis	Tahun	Judul	Metode	Hasil	Perbandingan dengan Penelitian Sekarang
		Menggunakan Metode *Vulnerability Assessment*		kerentanan rendah 4050. Jumlah kerentanan yang terdeteksi adalah 6049. Hasilnya menunjukkan bahwa OJS versi 2.4.7 mencakup berbagai kelemahan atau kerentanan yang tidak disarankan untuk digunakan, versi saat ini yang dirilis oleh *Public Knowledge Project* OJS harus digunakan sebagai gantinya (PKP)	menggunakan framework OWASP Versi 4.
Setiawan H., dkk. [7]	2020	Analisis Kerentanan Menggunakan *Interactive Application*	*Interactive Application Security Testing (IAST)*	Terdapat 249 risiko kerentanan diidentifikasi dari prosedur ini. Berdasarkan dokumen OWASP Top 10-2017, kerentanan keamanan ditemukan pada injeksi (A1),	Subjek penelitian web server, lokasi penelitian,, Tools yang dapat digunakan untuk melakukan pengujian keamanan menggunakan pendekatan IAST.

Penulis	Tahun	Judul	Metode	Hasil	Perbandingan dengan Penelitian Sekarang
		Security Testing (IAST) Untuk Aplikasi Situs Web Pemerintah X		otentikasi rusak (A2), paparan data sensitif (A3), kontrol akses rusak (A5), kesalahan konfigurasi keamanan (A6), lintas situs scripting (A7), menggunakan komponen dengan kerentanan yang diketahui (A9), dan pencatatan dan pemantauan yang tidak memadai (A10). Hasil analisis kerentanan menunjukkan bahwa perbaikan pada aplikasi berbasis web X-Government diperlukan	*(Interactive Application Security Testing)*, seperti Jenkins, API ZAP, dan SonarQube, melakukan analisis berdasarkan hasil kerentanan yang ditemukan berdasarkan dokumen OWASP Top 10-2017
Mayasari R., dkk. [8]	2020	Analisis *Vulnerability* pada	*Acunetix Vulnerability*	Terdapat *error information CRLF injection/HTTP response splitting*	Subjek penelitian web server, lokasi penelitian, *Tools*

Penulis	Tahun	Judul	Metode	Hasil	Perbandingan dengan Penelitian Sekarang
		Website Universitas Singaperbangsa Karawang menggunakan *Acunetix Vulnerability*		antara variabel *input id* dan *cross-site scripting* pada variabel *input idjp* pada website Universitas Singaperbangsa Karawang, dan prosedur *vulnerability* scanning pada website Universitas Singaperbangsa Karawang membutuhkan waktu lebih dari 12 jam, menghasilkan beberapa informasi tentang keamanan	pendeteksi *Vulnerability*, *tool* pengujian kerentanan menggunakan *Acunetix Vulnerability.*

2.2. *Network Security* (Keamanan Jaringan)

Keamanan jaringan sangat penting untuk memantau akses jaringan dan mencegah penggunaan sumber daya jaringan yang tidak sah. Administrator jaringan mengontrol tugas keamanan jaringan. Fitur keamanan yang ditentukan oleh lima kriteria, termasuk Kerahasiaan *(Confidentiality)*, mengharuskan informasi hanya tersedia bagi yang memiliki otorisasi. Integritas *(Integrity)* mengharuskan informasi diperbarui hanya oleh personil yang berwenang; Ketersediaan *(Availability)* menetapkan yaitu informasi tersedia bagi mereka yang berwenang saat dibutuhkan. Selain itu, Otentikasi (*Authentication*) menuntut agar pengirim informasi diidentifikasi secara tepat, dan ada kepastian bahwa identitas yang diperoleh benar. *Non-Repudiation* menyiratkan bahwa pengirim dan penerima komunikasi tidak dapat menolak pengiriman dan penerimaan pesan[9]**.**

2.3. *Web Server*

Peran utama server web adalah untuk melayani permintaan file pada sistem file lokal. Klien menghubungi server web di seluruh jaringan dan mengirimkan permintaan yang berisi nama file yang diperlukan; jika file ada, server mengembalikan konten file. Server web sangat penting dalam sistem karena mengelola semua permintaan pengguna. Setiap kelambatan tingkat server web akan berdampak negatif pada pengalaman pengguna. Kinerja server web berkaitan dengan kapasitas server untuk menanggapi permintaan pengguna, yang secara langsung mempengaruhi emosi mereka.

Server Web berkinerja tinggi meminimalkan biaya perangkat keras yang diperlukan untuk menyesuaikan permintaan layanan tertentu dan memungkinkan fleksibilitas untuk mengubah platform perangkat keras dan sistem operasi berdasarkan pertimbangan biaya, ketersediaan, atau kinerja. Beberapa metrik kinerja relevan saat mengevaluasi kinerja server web. Ini termasuk penggunaan sumber daya dan waktu respons.

Di sisi lain, waktu respons mengacu pada saat klien memulai permintaan dengan memulai koneksi TCP dan ketika server mengirimkan *respons*. Waktu respons hanyalah penundaan yang diamati oleh klien dan dapat diubah, karena terutama tergantung pada ukuran konten yang diminta. Sebagaimana dinyatakan,

penggunaan server web terutama didasarkan pada kinerja yang diprediksi, dengan server web berkinerja tinggi memiliki pangsa pasar yang lebih besar daripada server web berkinerja rendah. Selain meningkatkan kepercayaan pengguna, server web berkinerja tinggi memberikan keunggulan kompetitif bagi server web yang bersangkutan[10].

2.4. *Vulnerability Assessment*

Vulnerability Assessment (Penilaian kerentanan) yaitu proses mendeteksi, mengukur, dan memprioritaskan (atau memberi peringkat atau penilaian) kerentanan sistem. Sistem teknologi informasi, sistem penyediaan energi, sistem penyediaan air, sistem transportasi, dan sistem komunikasi termasuk dalam upaya *Vulnerability Assessment.* Evaluasi dapat dilakukan oleh berbagai kelompok, dari kecil hingga besar[11].

Vulnerability Assessment sangat penting karena memberikan informasi kepada perusahaan tentang risiko dan kelemahan keamanan sistem dan membantu lebih memahami kelemahan keamanan dan risiko keseluruhan sistem yang rusak.

2.5. Jenis *Vulnerability Assessment*

Ada tiga bentuk dari Vulnerability Assessment :

1. Black-Box

Pengujian tanpa pengetahuan tentang sistem dan jaringan perusahaan.

2. White-Box

Mengetahui detail infrastruktur organisasi

3. Gray-Box

Mengetahui sebagian informasi mengenai sistem organisasi[12].

2.6. Kategori *Vulnerability Assessment Scan*

Berikut ini adalah contoh pemindaian *Vulnerability Assessment*:

1. *Network-based scans,*

Digunakan untuk mendeteksi pelanggaran keamanan jaringan.

2. Host-based scans

Digunakan untuk mengidentifikasi kerentanan di server atau host jaringan.

3. *Wireless network scans,*

Biasanya digunakan untuk mengidentifikasi titik akses jahat atau memvalidasi bahwa jaringan organisasi telah dikonfigurasi dengan aman.

4. *Application scans*,

Digunakan dalam pengujian situs web untuk mengidentifikasi kemungkinan kerentanan perangkat lunak,

5. *Database scans,*

Digunakan untuk mengidentifikasi kerentanan basis data untuk mencegah serangan berbahaya[13].

2.7. Alat *Vulnerability Assessment*

2.7.1. Kali Linux

Distribusi Linux *open-source* berbasis Debian yang dirancang untuk pengujian penetrasi lanjutan dan audit keamanan. Pengujian penetrasi, penelitian keamanan, forensik komputer, dan *reverse engineering* hanyalah beberapa dari alat Kali Linux yang digunakan. Selain itu, Kali Linux adalah solusi lintas platform yang dapat diakses secara bebas oleh para profesional dan penggemar keamanan informasi[14].

2.7.2. Nmap

Nmap berfungsi sebagai alat audit keamanan dan pengintaian *Open Source Network*. Nmap dirancang untuk memindai jaringan yang luas tetapi berfungsi dengan baik terhadap satu host. Nmap menggunakan paket *raw IP* untuk mendeteksi host mana yang dapat diakses di jaringan. *Output* dari Nmap adalah daftar target yang dipindai, dengan informasi tambahan untuk setiap target berdasarkan pengaturan[15].

2.7.3. Zenmap

Zenmap berfungsi sebagai alat berasal dari *user interface* pengguna grafis resmi untuk Nmap *Security Scanner*. Zenmap merupakan alat lintas platform, gratis, *Open source* yang membuat Nmap lebih mudah digunakan oleh pemula. Pemindaian yang sering digunakan dapat disimpan sebagai profil untuk

memfasilitasi eksekusi berulang. Hasil scan dapat disimpan dan diperiksa kemudian. Temuan pemindaian terbaru disimpan dalam database yang dapat dicari[16].

2.7.4. Nessus

Tenable, Inc. menciptakan Nessus, pemindai kerentanan berpemilik. Nessus menyediakan pemindai kerentanan jaringan *open source* yang menggunakan arsitektur Kerentanan Umum dan Eksposur untuk memungkinkan penautan silang yang mudah dari solusi keamanan yang sesuai. Faktanya, selama penilaian kerentanan dan pengujian penetrasi, termasuk serangan berbahaya, Nessus adalah salah satu dari banyak pemindai kerentanan yang digunakan.

Nessus berfungsi sebagai alat pengujian penetrasi, dan pemindai keamanan jarak jauh biasanya berjalan pada satu komputer untuk memindai layanan yang ditawarkan oleh komputer yang jauh. Program ini mengizinkan pengguna untuk membuat skrip dan melakukan pemeriksaan kerentanan khusus. Nessus bekerja dengan menganalisis setiap *port* di komputer, menentukan layanan apa yang dijalankannya, dan menguji layanan tersebut untuk mengetahui kerentanan yang dapat dimanfaatkan penyerang untuk meluncurkan serangan[17].

2.8. Tipe Ancaman *Web Vulnerability*

2.8.1. *SQL Injection Vulnerability Attack*

Setiap organisasi yang mengoperasikan situs webnya di database SQL rentan terhadap serangan ini jika tidak memiliki validasi input yang tepat dalam formulir webnya. Akibatnya, siapa pun dapat memasukkan perintah SQL berbahaya ke dalam string input formulir online, cookie web, atau permintaan halaman (browser) dan dapat memperoleh, mengubah, dan menghapus data yang disimpan dalam database dengan menempatkan integritas data, otentikasi, otorisasi , dan kerahasiaan berisiko. Serangan dilakukan pada aplikasi berbasis data karena perilaku program ini seringkali bergantung pada data yang diberikan. Oleh karena itu, serangan ini cukup mudah untuk diterapkan. Namun, kurangnya pemahaman dan pelaksanaan protokol keamanan oleh bisnis menyebabkan kebocoran data akibat serangan SQLI.

2.8.2. *Broken Authentıcatıon and Sessıon Management Vulnerabılıty Attack*

HTTP merupakan protokol tanpa kewarganegaraan. Beberapa bentuk protokol diperlukan yang dapat melacak aktivitas pengguna tertentu yang mengunjungi situs web dan disediakan sebagai masukan dalam query GET atau POST. Ini dilakukan dengan memberikan ID sesi atau token kepada pengguna ketika dia mengunjungi situs web apa pun. ID sesi ini digunakan untuk mengidentifikasi pengguna tersebut selama pertukaran informasi (permintaan HTTP dan respons HTTP) (permintaan HTTP dan respons HTTP). Periode sesi dibuat sesingkat mungkin untuk tujuan keamanan. Jika sesi tidak dikelola dengan baik selama konstruksi situs web, penyerang dapat memanfaatkan atau mencuri id sesi pengguna yang masuk dan bisa mendapatkan hak potensial. ID sesi sering dibuat sebagai string panjang acak, sehingga sulit bagi pengguna untuk menebak yang berikutnya. Situs web dapat terkena serangan fiksasi sesi jika sesi dan otentikasi tidak ditangani dengan tepat saat membangun atau mengembangkan situs web.

2.8.3. *Cross-Site Scrıptıng Attack*

Dua pertiga dari semua program online rentan terhadap serangan c*ross-site scripting* atau *XSS Attack*. Skrip berbahaya dijalankan di sisi klien, biasanya di browser pengguna. Akibatnya, komunikasi antara pengguna dan situs web yang rentan terganggu. Misalkan situs web dinamis tunduk pada serangan SQLI atau otentikasi rusak dan serangan manajemen sesi. Dalam hal ini, ada kemungkinan lebih besar bahwa situs web akan terkena serangan XSS. Sama seperti serangan SQLI yang ditujukan untuk aplikasi berbasis SQL dengan melewatkan kueri SQL, serangan XSS menargetkan halaman HTML di mana penyusup menyuntikkan kode berbahaya ke halaman web HTML. Ini adalah kejahatan dunia maya paling populer yang digunakan untuk mencuri sesi atau menyerang seluruh jaringan sosial perusahaan[18].

2.8.4. *Vulnerability Assessments Vs. Penetration Testing*

Meskipun *Vulnerability Assessment* dapat menggabungkan *Penetration testing*, keduanya adalah prosedur yang berbeda. *Vulnerability Assessment*

terutama ditujukan untuk mengidentifikasi kerentanan, sedangkan *Penetration testing* mengevaluasi efektivitas pertahanan siber dengan mengeksploitasi kelemahan untuk mendapatkan akses sistem. Salah satu perbedaan antara *Penetration testing* dan *vulnerability assessment*, yaitu penyerang mencoba untuk mendapatkan akses ke salah satu administrator sistem dan mengumpulkan informasi tentang target dengan membaca berbagai file sampai data nama pengguna dan kata sandi yang tidak terenkripsi ditemukan dan dialihkan ke server penting lainnya. Sementara *vulnerability assessment* bertujuan untuk menemukan kelemahan dan tidak melakukan serangan tambahan. *Vulnerability assessment* berusaha mengidentifikasi kelemahan tersebut. Penilaian risiko dapat ditingkatkan atau diturunkan berdasarkan kemampuan konsultan untuk memanfaatkan hasil dari prosedur pengujian otomatis (bagian pemindaian). *Vulnerability assessment* mencari pada skala yang lebih luas untuk menemukan semua kelemahan, sedangkan *Penetration testing* sering berfokus pada metode serangan yang lebih khusus[19]–[21].