BAB II
TINJAUAN PUSTAKA DAN DASAR TEORI

2.1 Tinjauan Pustaka

Dalam penulisan skripsi ini penulis menggali berbagai informasi dan menemukan beberapa penelitian terkait yang sebelumnya pernah dilakukan oleh pihak lain.Dari penelitian tersebut kemudian dijadikan sebagai referensi dalam penyelesaian tugas akhir. Adapun beberapa penelitian terkait yang dijadikan sebagai acuan yaitu :

Dimas Febriyan Priambodo, dkk (2022), Penetration Testing Web XYZ Berdasarkan OWASP Risk Rating. Uji penetrasi pada WebsiteXYZ Kabupaten XYZ dilaksanakan dengan mengacu kepada Open Web ApplicationSecurity Project(OWASP) Top10-2021.Penetration testingdilaksanakandengan metode black boxuntuk mendapatkan hasil pengukuran tingkat kerentanan pada aplikasi. Keseluruhan penilaian kerentanan dilakukan dalam empat tahap yaitu planning, information gathering, vulnerability scanningmenggunakan 2 tools otomatis yaitu Vega dan OWASP ZAP sebagai upaya untuk mendapatkan cakupan yang lebih luas terkait kerentanan yang ditemukan dikuti dengan validasi dilanjutkan tahap analysis and eporting. Hasil tahap vulnerability scanning menghasilkan 9 jenis kerentanan dengan sebaran 2 high, 1 medium, dan 6 low. Pengujian penetrasi untuk validasi mengacu pada dokumen panduan WebSecurity Testing Guide(WSTG) versi 4.2. Hasil proses akhir berupa rekomendasi dapat digunakan sebagai referensi pengembang aplikasi web untuk menangani kerentanan khususnya hilangnya ketersediaan layanan dan kebocoran data.

I Made Edy Listartha, dkk (2022), Melakukan analisis kerentanan website SMA negeri 2 amlapura menggunakan metode owasp (open web application security project). Penelitian ini menghasilkan 2 faktor untuk memperkirakan Likelihood dan Impact, dari masing-masing faktor terdapat 3 resiko yang ditemukan yaitu risk severity High, risk severity

Medium dan risk severity Low. Hasil penilaian resiko ini dapat membantu para pengelola dan pengembang sistem untuk menyadari resiko yang mungkin terjadi sehingga dapat mengambil tindakan untuk mencegah dan mengatasi resiko tersebut.

Rahmad Ashar (2022), Analisis Keamanan Open Website Menggunakan Metode OWASP dan ISSAF. Pada penilitiannya penulis melakukan analisis keamanan pada open website milik Diskominfo Kerinci dengan menggunakan dua metode yaitu metode Open Web Application Security Project (OWASP) dan metode Information Systems Security Assessment Framework (ISSAF).

Bahrun Ghozali, Kusrini, dan Sudarmawan (2017), Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) untuk Penilaian Risk Rating. pada penelitian ini dilakukan analisis kerentanan pada salah satu website sistem informasi development yang menggunakan framework Codeigniter dan PHP Native.penelitian ini menggunakan metode OWASP risk rating, dan ditemukan bahwa tidak ada jaminan n platform web application development menggunakan framework atau PHP Native terhindar dari celah keamanan.

Jai Narayan Goela dan BM Mehtreb (2015), yaitu Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. memberikan gambaran lengkap tentang Penilaian Kerentanan dan Pengujian Penetrasi, dan penggunaannya sebagai teknologi pertahanan siber. Menjelaskan perlunya meningkatkan penggunaan VAPT untuk keamanan sistem yang lengkap. makalah ini akan sangat membantu peneliti selanjutnya untuk mendapatkan pengetahuan lengkap tentang proses, alat, teknik VAPT dan penggunaannya sebagai teknologi pertahanan dunia maya. Akan sangat membantu untuk mengembangkan teknik dan alat VAPT baru.

2.2 Dasar Teori

2.2.1 OWASP

Open Worldwide Application Security Project (OWASP) adalah yayasan nirlaba yang bekerja untuk meningkatkan keamanan perangkat lunak. Melalui proyek perangkat lunak sumber terbuka yang dipimpin komunitas, ratusan cabang lokal di seluruh dunia, puluhan ribu anggota, dan konferensi pendidikan dan pelatihan terkemuka, Yayasan OWASP adalah sumber bagi pengembang dan ahli teknologi untuk mengamankan web.

1. Alat dan Sumber Daya
2. Komunitas dan Jaringan
3. Pelatihan Pendidikan

Selama hampir dua dekade perusahaan, yayasan, pengembang, dan sukarelawan telah mendukung OWASP Foundation dan pekerjaannya.

2.2.2 Risiko Keamanan

OWASP Top 10 adalah laporan yang diperbarui secara berkala yang menguraikan masalah keamanan untuk keamanan aplikasi web, dengan fokus pada 10 risiko paling kritis. Berikut adalah risiko keamanan OWASP Top 10 terbaru pada tahun 2021:

1. Broken Access Control
   Kontrol akses pada titik ini mengacu pada kontrol sistem akses ke informasi dan fungsinya. Kontrol akses yang rusak memungkinkan penyerang melewati proses otorisasi dan melakukan hal-hal yang biasanya hanya dapat dilakukan oleh admin.
2. Cryptographic Failures
   kegagalan untuk melindungi data sensitif yang seharusnya tidak dapat diakses publik.
3. Injection

Injeksi kode terjadi ketika penyerang mengirimkan data yang tidak valid ke aplikasi web dengan maksud membuatnya melakukan sesuatu yang tidak dirancang/diprogram untuk dilakukan oleh aplikasi tersebut.

4. Insecure Design

   Tambahan baru untuk Sepuluh Teratas OWASP, berada di nomor empat dalam daftar, adalah desain yang tidak aman. Ini berfokus pada pengembangan aplikasi web dari awal siklus hidupnya.

5. Securtiy Misconfiguration

   Kategori ini naik satu tingkat dari daftar 10 teratas sebelumnya yang diterbitkan pada tahun 2017. Kategori sebelumnya untuk Entitas Eksternal XML (XXE) telah ditambahkan ke kategori ini. Ada banyak kemungkinan kesalahan konfigurasi keamanan.

6. Vulnerable and Outdated Components

   Bahkan situs web sederhana seperti blog pribadi memiliki banyak ketergantungan, plugin, ekstensi, dan kode pihak ketiga. Gagal memperbarui setiap perangkat lunak di backend dan frontend situs web berisiko masuk ke keamanan lebih cepat daripada nanti. Penyerang secara aktif mencari komponen yang rentan di situs web dan mengeksploitasinya secara agresif untuk menyebarkan malware, spam, dan phishing

7. Identification and Authentication Failures

   Kerentanan autentikasi yang rusak dapat memungkinkan penyerang menggunakan metode manual dan/atau otomatis untuk mencoba mendapatkan kendali atas akun apa pun yang mereka inginkan dalam sistem – atau bahkan lebih buruk lagi – untuk mendapatkan kendali penuh atas sistem.

8. Software and Data Integrity Failures

   Kegagalan ini dapat terjadi dalam berbagai bentuk, terutama karena seiring dengan perkembangan web, semakin umum penggunaan kode dan layanan pihak ketiga dalam aplikasi web.

9. Security Logging and Monitoring Failures

   Tidak memiliki proses pencatatan dan pemantauan yang efisien dapat meningkatkan kerusakan situs web yang disusupi.

10. Server-Side Request Forgery

    Cacat SSRF terjadi setiap kali aplikasi web mengambil sumber jarak jauh tanpa memvalidasi URL yang disediakan pengguna. Ini memungkinkan penyerang memaksa aplikasi untuk mengirim permintaan yang dibuat ke tujuan yang tidak terduga, bahkan ketika dilindungi oleh firewall, VPN, atau jenis lain dari daftar kontrol akses jaringan (ACL).

2.2.3 Analisis Kerentanan (Vulnerability Analysis)

Vulnerability Analysis adalah kegiatan yang dilakukan untuk mengetahui suatu celah keamanan yang terdapat didalam suatu sistem. Vulnerability Analysis sangat sering disamakan dengan Penetration Testing, namun nyatanya kedua layanan ini jelas berbeda, meskipun mempunyai tujuan yang sama yaitu berfungsi untuk analisis celah keamanan suatu sistem. Perbedaan dari keduanya terletak dari metode, tools yang digunakan, hingga waktu yang dibutuhkan. Perbedaan yang lebih jelas antara keduanya adalah VA dilakukan pemeriksaan secara otomatis dengan menggunakan tools yang ada untuk memastikan adanya risiko keamanan, sedangkan PT dilakukan pemeriksaan secara lebih detail yang dilakukan oleh pentester professional dengan melakukan simulasi penyerangan secara langsung untuk memastikan celah keamanan yang ada.

2.2.4 OWASP Risk Rating

Berdasarkan metodologi OWASP Risk Rating terdapat beberapa tahapan dalam menentukan tingkat keparahan dari risiko keamanan yang ditimbulkan, adapun tahapan-tahapannya yaitu Identifying a Risk, Analisis Likelihood, analisis Impact, Determining the Severity of the Risk, Deciding What to Fix.

2.2.4.1 Indetifying Risk

Langkah pertama adalah mengidentifikasi risiko keamanan yang ada. Perlu mengumpulkan informasi tentang kerentanan yang terlibat, dan dampak

eksploitasi apabila berhasil. Pada tahapan ini peneliti akan menggunakan Vulnerability Assesment tools seperti OWASP ZAP, Acunetix, atau Burp Suite untuk mengidentifikasi celah keamanan yang terdapat pada sistem target.

2.2.4.2 Estimating Likelihood

Langkah pertama setelah mengidentifikasi celah keamanan yaitu memperkirakan "Likelihood" atau kemungkinan risiko yang terjadi. pada tahapan ini bertujuan untuk memperkirakan apakah tingkat kemungkinan rendah,sedang, atau tinggi.

Untuk menentukan likelihood terdapat 2 faktor yang dapat digunakan yaitu threat agent factors dan Vulnerability Factors. Adapun cara untuk menentukan threat *agent factors* berdasarkan beberapa kriteria yaitu :

1) **Skill Level**

   Adalah seberapa terampil kelompok threat agents secara teknis ?

Tabel 2. 1 Skill Level

Skill	Nilai
tidak ada keterampilan teknis	(1)
beberapa keterampilan teknis	(3)
pengguna komputer tingkat lanjut	(5)
keterampilan jaringan dan pemrograman	(6)
keterampilan penetrasi keamanan	(9)

2) **Motive**

   Seberapa termotivasi kelompok agen ancaman ini untuk menemukan dan mengeksploitasi kerentanan ini?

Tabel 2. 2 Motive

Motive	Nilai
Hadiah rendah atau tidak ada	(1)
kemungkinan hadiah	(4)
hadiah tinggi	(9)

3) Opportunity

Sumber daya dan peluang apa yang diperlukan untuk kelompok agen ancaman ini untuk menemukan dan mengeksploitasi kerentanan ini?

Tabel 2. 3 Opportunity

Opportunity	Nilai
Diperlukan akses penuh atau sumber daya yang mahal	(0)
diperlukan akses atau sumber daya khusus	(4)
diperlukan beberapa akses atau sumber daya	(7)
tidak diperlukan akses atau sumber daya	(9)

4) Size

Seberapa besar kelompok agen ancaman ini ?

Tabel 2. 4 Size

Size	Nilai
Pengembang	(2)
administrator sistem	(2)

pengguna intranet	(4)
mitra	(5)
pengguna yang diautentikasi	(6)
pengguna Internet anonim	(9)

Faktor yang kedua adalah ***Vulnerability Factor*** Tujuannya di sini adalah untuk memperkirakan kemungkinan kerentanan khusus yang terlibat ditemukan dan dieksploitasi. cara untuk menentukan *Vulnerability Factors* berdasarkan beberapa kriteria yaitu :

1) **Ease of Discover**

   Seberapa mudah kelompok threat agents ini dalam menemukan celah keamanan ?

Tabel 2. 5 Ease of Discover

Ease of Discover	**Nilai**
Praktis tidak mungkin	(1)
sulit	(3)
mudah	(7)
Alat otomatis tersedia	(9)

2) **Ease of exploit**

   Seberapa mudah bagi kelompok threat agent untuk benar-benar memanfaatkan kerentanan ini?

Tabel 2. 6 Ease of Exploit

Ease of exploit	**Nilai**
Alat bantu otomatis teoritis	(1)

Sulit	(3)
Mudah	(5)
tersedia	(9)

3) Awareness

Seberapa terkenal kerentanan ini terhadap kelompok threat agent?

Tabel 2. 7 Awareness

Awareness	Nilai
Tidak diketahui	(1)
Tersembunyi	(4)
Jelas	(6)
Pengetahuan umum	(9)

4) Intrusion detection

Seberapa besar kemungkinan exploit untuk dideteksi?

Tabel 2. 8 Instrution Detection

Intrusion detection	Nilai
Deteksi aktif dalam aplikasi	(1)
login dan ditinjau	(3)
login tanpa review	(8)
tidak login	(9)

2.2.4.3 Estimating Impact

Saat mempertimbangkan dampak serangan yang berhasil, penting untuk disadari bahwa ada dua jenis dampak. Yang pertama adalah “Technical Impact” pada aplikasi, data yang digunakannya, dan fungsi yang

disediakannya. Yang lainnya adalah “Business Impact” pada bisnis dan perusahaan yang mengoperasikan aplikasi.

Langkah selanjutnya adalah memperkirakan besarnya “*impact”* atau dampak risiko yang ada. Diketahui terdapat dua jenis dampak yaitu *Technical Impact* dan juga *Business impact.* Adapun kriteria untuk memperkirakan **“*Technical Impact*“** yaitu :

1) **Loss of confidentiality**

   Berapa banyak data yang bisa diungkapkan dan seberapa sensitif?

Tabel 2. 9 Loss of Confidentiality

Loss of confidentiality	**Nilai**
Data yang diungkapkan minimum dan tidak sensitif	(2)
minimal data kritis yang diungkapkan	(6)
data non-sensitif ekstensif diungkapkan	(6)
data kritis dan ekstensif diungkapkan	(7)
semua data diungkapkan	(9)

2) **Loss of integrity**

   Berapa data yang bisa rusak dan seberapa rusaknya?

Tabel 2. 10 Loss of Integrity

Loss of integrity	**Nilai**
Minimal data yang sedikit korup	(1)

data yang sangat korup minimal	(3)
data yang sedikit korup yang luas	(5)
data korup yang sangat serius	(7)
Semua data benar -benar korup	(9)

3) Loss of Availability

Berapa banyak layanan yang bisa hilang dan seberapa vitalnya?

Tabel 2. 11 Loss of Availability

Loss of Availability	Nilai
Layanan sekunder minimal terputus	(1)
layanan utama minimal terputus	(5)
layanan sekunder yang luas terputus	(5)
layanan utama yang luas terputus	(7)
semua layanan benar -benar hilang	(9)

4) Loss of Accountability

Apakah tindakan agen ancaman dapat dilacak kepada individu?

Tabel 2. 12 Loss of Accountability

Loss of Accountability	Nilai
Sepenuhnya dapat dilacak	(1)

mungkin dapat dilacak	(7)
sepenuhnya anonim	(9)

Factor yang kedua adalah *Business Impact.* Berikut adalah kriteria pada *Business Impact :*

1) **Financial Damage**

   Seberapa besar kerugian finansial yang dihasilkan dari pembobolan?

Tabel 2. 13 Financial Damage

Loss of confidentiality	**Nilai**
Kurang dari biaya untuk memperbaiki kerentanan	(1)
pengaruh kecil terhadap laba tahunan	(3)
berpengaruh signifikan terhadap laba tahunan	(7)
kebangkrutan	(9)

2) **Reputation Damage**

   Apakah pembobolan dapat menghasilkan hilangnya reputasi yang membahayakan bisnis ?

Tabel 2. 14 Reputation Damage

Reputation Damage	**Nilai**
Kerusakan minimal	(1)
Kehilangan akun utama	(4)
Kehilangan reputasi	(5)

kerusakan merek	(9)

3) Non-Compliance

Bagaimana pembobolan yang dilakukan terhadap jenis pelanggaran?

Tabel 2. 15 Non-Compliance

Non-Compliance	Nilai
Pelanggaran ringan	(2)
Pelanggaran yang jelas	(5)
pelanggaran profil tinggi	(7)

4) Privacy Violation

Seberapa besar informasi personal yang dapat diungkapkan ?

Tabel 2. 16 Privacy Violation

Privacy Violation	Nilai
Satu individu	(3)
ratusan orang	(5)
ribuan orang	(7)
jutaan orang	(9)

2.2.4.4 Determining the Severity of the Risk

Pada langkah ini, perkiraan keseluruhan *likelihood* dan perkiraan keseluruhan *impact* disatukan untuk menghitung tingkat keparahan keseluruhan dari risiko ini. Ini dilakukan dengan mencari tahu apakah kemungkinannya rendah, sedang, atau tinggi dan kemudian melakukan hal

yang sama untuk dampaknya. Skala 0 hingga 9 dibagi menjadi tiga bagian. Berikut adalah gambar untuk menentukan level keseluruhan Likelihood dan impact.

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

Gambar 2. 1 Likelihood and Impact Levels

Lalu untuk menentukan nilai severitynya dapat disesuaikan seperti pada gambar di bawah :

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

Gambar 2. 2 Overall Risk Severity

2.2.4.5 Deciding What to Fix

Setelah risiko aplikasi diklasifikasikan, akan ada daftar prioritas tentang apa yang harus diperbaiki. Sebagai aturan umum, risiko yang paling parah harus diperbaiki terlebih dahulu