BAB II
TINJAUAN PUSTAKA

A. PENELITIAN TERDAHULU

Penelitian yang telah dilakukan sebelumnya dan menjadi acuan dalam penelitian ini ditunjukan dalam Tabel 1.

Table 1. Penelitian terdahulu

No	Peneliti	Judul	Hasil	Penelitian yang akan dilakukan
1.	(Helmiawan et al., 2020)	Analysis of Web Security Using Open Web Application Security Project 10	Berdasarkan hasil eksploitasi menggunakan tools OWASP ZAP dan Web security pada tahapam sebelumnya, ditemukan beberapa jenis ancaman dengan tingkat ancaman yang berbeda-beda. Dari ancaman-ancaman tersebut perlu dilakukan optimasi untuk mencegah serangan dari kerentanan dan ancaman yang ditemukan	Mengananlisis kerentanan pada website fts.ump.ac.id dengan menggunakan metode OWASP WSTG v4.2
2.	(Priyawati et al., 2022)	Website Vulnerability Testing and Analysis of Internet Management Information	Hasil dari pengujian kerentanan sistem dengan menggunakan OWASP Zap tools ditemukan empat kerentanan yang harus	

		System Using OWASP	diperbaiki, yaitu A01-Broken Access Control, A03-Injection, A05-Kesalahan Konfigurasi Keamanan, dan A08-Kegagalan Integritas Perangkat Lunak dan Data. Integrity Failures. Hasil dari pengujian kerentanan sistem dengan menggunakan OWASP Zap tools ditemukan empat kerentanan yang harus diperbaiki, yaitu A01-Broken Access Control, A03-Injection, A05-Kesalahan Konfigurasi Keamanan, dan A08-Kegagalan Integritas Perangkat Lunak dan Data.	
3.	(Lala et al., 2021)	Secure Web development using OWASP Guidelines	Berdasarkan hasil analisis, dapat disimpulkan bahwa sebuah aplikasi web sederhana tanpa keamanan sangat rentan terhadap serangan dan dapat dengan mudah dilumpuhkan.	

			Permintaan SQL dasar untuk menghapus basis data akan dieksekusi tanpa pemeriksaan lebih dalam terhadap aplikasi web tersebut, dan ini saja sudah cukup untuk menjatuhkan aplikasi web.	
4.	(Wijayanto et al., 2020)	Analysis of Vulnerability Webserver Office Management of Information And Documentation Diskominfo using OWASP Scanner	Setelah melakukan pengujian terhadap website PPID Diskominfo, maka dapat dihasilkan bahwa kerentanan pada website PPID Diskominfo termasuk dalam jenis serangan Cross-Site Scripting, dengan ditemukannya risiko tinggi pada dua URL di website PPID Diskominfo, beberapa celah lainnya hanya notifikasi, dan status kerentanannya adalah low dan sedang.	
5.	(Mburano & Si, 2019)	Evaluation of Web Vulnerability Scanners Based	Terdapat variasi yang cukup besar dalam kinerja kedua pemindai	

		on OWASP Benchmark	ini antara tolok ukur OWASP dan tolok ukur Benchmark WAVSEP. Secara khusus, hasil tolok ukur kami perbandingan mengungkapkan bahwa untuk kedua pemindai dan keempat kategori kerentanan yang dibandingkan, skor di bawah WAVSEP jauh lebih tinggi daripada skor di bawah tolok ukur OWASP. Hal ini mencerminkan bahwa tolok ukur OWASP lebih menantang daripada tolok ukur WAVSEP dalam keempat kategori kerentanan ini. Oleh karena itu, kami merekomendasikan bahwa, jika pemindai akan dievaluasi pada empat kategori kerentanan ini, tolok ukur OWASP harus dipilih sebagai target utama.	

6.	(Devi & Kumar, 2020)	Testing for Security Weakness of Web Applications using Ethical Hacking	Dengan menggunakan pengujian penetrasi, kelemahan keamanan telah terdeteksi di semua area domain yang ditemukan peringatan tingkat menengah dan rendah dengan alat OWASP ZAP. Kerentanan yang berbeda seperti cookie tanpa secure flag, cross-site request forgery (CSRF), penulisan ulang URL dan peringatan pengungkapan kesalahan aplikasi telah terdeteksi oleh kedua alat tersebut dalam pengujian aplikasi web	
7.	(Kuncoro & Rahma, 2021)	Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review	Penelitian ini memberikan gambaran terkait pengujian keamanan sistem informasi khususnya berbasis aplikasi website. Pengujian keamanan sangat diperlukan dalam memberikan keamanan dan kenyaman kepada pengguna sistem. Dari hasil pencarian celah keamanan dan pengujian	

			celah keamanan dapat ditemukan beberapa kelemahan dan kerentanan pada sistem. Karena kelemahan tersebut dapat diekploitasi oleh pihak yang tidak berwenang dan tidak memiliki akses.	
8.	(Hariyadi & Nastiti, 2021)	Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta	Walaupun sebagian besar domain dan/atau sub-domain dari Universitas Duta Bangsa Surakarta tidak memiliki celah keamanan dengan kategori high, kecuali simpus.fikom.udb.ac.id tetapi berdasarkan penelusuran di zone-h.org ditemukan sebuah celah yang memungkinkan seorang penyerang dapat mengunggah sebuah berkas yang dapat dikategorikan sebagai web defacement seperti tampak pada Gambar 1. Hal ini menunjukan bahwa proses Vulnerability Identification dalam	

			melakukan pemindaian celah keamanan secara helicopter view.	
9.	(Mohmmad Muhsin, 2015)	Penerapan Pengujian Keamanan Web Server Menggunakan Metode OWASP versi 4 (Studi Kasus Web Server Ujian Online)	Hasil pengujian menggunakan OWASP versi 4 menunjukkan bahwa manajemen otentifikasi, otorisasi dan manajemen sesi belum diimplementasikan dengan baik sehingga perlu dilakukan perbaikan lebih lanjut oleh pihak stake holder Fakultas Teknik Universitas Muhammadiyah Ponorogo.	
10.	(Abdillah et al., 2023)	Analisis Kerentanan Website Mtss Al-Washliyah Bah Gunung Menggunakan Metode Open Web Application Security Project ZAP (OWASP ZAP)	Berdasarkan Hasil Pengujian OWASP ZAP karena ini merupakan bukan website asli melainkan website gratis dari pemerintah jadi website ini hanya memiliki 3 kerentanan yaitu: 1. Content Security Policy (CSP) Header Not Set 2. Missing Anti-clickjacking Header 3. X-Content-Type-Options Header Missing	

B. LANDASAN TEORI

1. Website

Website adalah serangkaian halaman web yang dapat diakses orang lain di seluruh dunia melalui URL tanpa harus dibatasi oleh lokasi dan waktu. Website ini terdiri dari teks, gambar, audio, video, animasi dan menjadi media untuk membaca atau mengunjungi informasi (Guntoro et al., 2020).

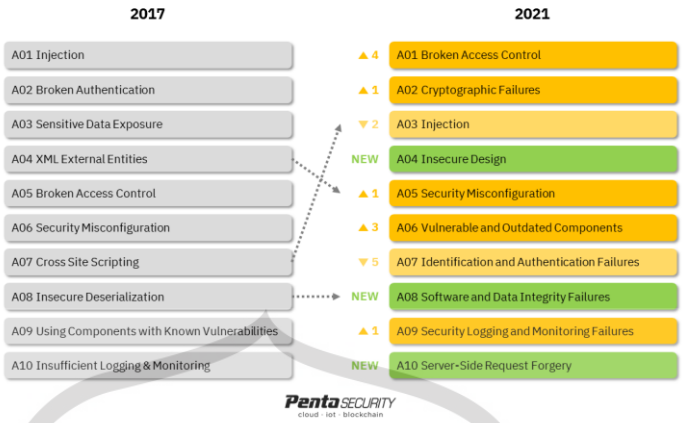
2. Vulnerability

Vulnerability website adalah celah atau kelamahan dalam system keamanan memungkinkan pihak yang tidak berwenang untuk mengakses, mengubah, atau merusak data yang tersimpan di dalamnya. CIA atau yang biasa dikenal dengan Confidentiality (kerahasiaan), Integrity (intergritas) dan Aviability (ketersediaan) merupakan salah satu parameter yang sering digunakan dalam menganalisis celah keamanan dan menjadi acuan dalam keamanan sebuah website. Parameter tersebut digunakan sebagai standar dan acuan dalam menilai baik atau buruknya sebuah keamanan pada suatu website (Guntoro et al., 2020).

3. OWASP WSTG (Web Security Testing Guide)

OWASP WSTG v.4.2 adalah sebuah panduan komprehensif yang dirancang untuk membantu para *developer* dan para professional keamanan untuk menguji aplikasi web. OWASP sendiri merupakan organisasi yang dibangun untuk menemukan celah keamanan dari sebuah aplikasi website (Guntoro et al., 2020). Pada gambar 1

merupakan perbandingan antara OWASP tahun 2017 dan 2021.



Gambar 1. Perbandingan OWASP Top 10 Tahun 2017 dan 2021

a) A01:2021-Broken Access Control

A01:2021-Kontrol Akses Rusak naik dari posisi kelima; 94% aplikasi diuji untuk beberapa bentuk kontrol akses yang rusak. 34 *Common Weakness Enumerations* (CWE) yang dipetakan ke Kontrol Akses Rusak memiliki lebih banyak kemunculan dalam aplikasi daripada kategori lainnya.

b) A02:2021-Cyptographic Failures

A02:2021-Kegagalan Kriptografi bergeser satu posisi ke posisi #2, yang sebelumnya dikenal sebagai Paparan Data Sensitif, yang merupakan gejala umum daripada akar penyebabnya. Fokus baru di sini adalah pada kegagalan yang terkait dengan kriptografi yang sering kali menyebabkan paparan data sensitif atau kompromi sistem.

c) A03:2021-Injection

A03:2021-Injeksi turun ke posisi ketiga. 94% aplikasi diuji untuk beberapa bentuk injeksi, dan 33 CWE yang dipetakan ke dalam kategori ini memiliki kemunculan terbanyak kedua dalam aplikasi. Cross-site Scripting sekarang menjadi bagian dari kategori ini dalam edisi ini.

d) A04:2021-Insecure Design

A04:2021-Desain Tidak Aman adalah kategori baru untuk tahun 2021, dengan fokus pada risiko yang terkait dengan kelemahan desain. Jika kita benar-benar ingin "bergerak ke kiri" sebagai sebuah industri, maka diperlukan lebih banyak penggunaan pemodelan ancaman, pola dan prinsip desain yang aman, serta arsitektur referensi.

e) A05:2021-Security Misconfiguration

A05:2021-Kesalahan Konfigurasi Keamanan naik dari peringkat #6 pada edisi sebelumnya; 90% aplikasi diuji untuk beberapa bentuk kesalahan konfigurasi. Dengan semakin banyaknya pergeseran ke perangkat lunak yang sangat mudah dikonfigurasi, tidak mengherankan jika kategori ini naik peringkat. Kategori sebelumnya untuk Entitas Eksternal XML (XXE) sekarang menjadi bagian dari kategori ini.

f) A06:2021-Vulnerable and Outdated Components

A06:2021-Komponen yang Rentan dan Usang sebelumnya berjudul Menggunakan Komponen dengan Kerentanan yang Diketahui dan menempati urutan #2 dalam survei komunitas Top 10, tetapi juga memiliki data yang cukup untuk masuk dalam Top 10 melalui analisis data. Kategori ini naik dari peringkat #9 pada tahun 2017 dan merupakan masalah yang diketahui dan kami kesulitan untuk menguji dan menilai risikonya. Ini adalah satu-satunya kategori yang tidak memiliki Kerentanan dan Eksposur Umum (CVE) yang dipetakan ke CWE yang disertakan, sehingga eksploitasi default dan bobot dampak 5.0 diperhitungkan ke dalam skor mereka.

g) A07:2021-Identification and Authentication Failures

A07:2021-Kegagalan Identifikasi dan Otentikasi sebelumnya adalah Otentikasi Rusak dan turun dari posisi kedua, dan sekarang mencakup CWE yang lebih terkait dengan kegagalan identifikasi. Kategori ini masih menjadi bagian integral dari 10

Besar, tetapi peningkatan ketersediaan kerangka kerja standar tampaknya membantu.

h) A08:2021-Software and Data Integrity Failures

A08:2021-Kegagalan Integritas Perangkat Lunak dan Data adalah kategori baru untuk tahun 2021, yang berfokus pada pembuatan asumsi terkait pembaruan perangkat lunak, data penting, dan jalur pipa CI/CD tanpa memverifikasi integritas. Salah satu dampak dengan bobot tertinggi dari data Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) yang dipetakan ke dalam 10 CWE dalam kategori ini. Insecure Deserialization dari tahun 2017 sekarang menjadi bagian dari kategori yang lebih besar ini.

i) A09:2021-Seciruty Logging and Monitoring Faiures

A09:2021-Kegagalan Pencatatan dan Pemantauan Keamanan sebelumnya adalah Pencatatan & Pemantauan yang Tidak Memadai dan ditambahkan dari survei industri (#3), naik dari sebelumnya #10. Kategori ini diperluas untuk mencakup lebih banyak jenis kegagalan, sulit untuk diuji, dan tidak terwakili dengan baik dalam data CVE/CVSS. Namun, kegagalan dalam kategori ini dapat secara langsung berdampak pada visibilitas, peringatan insiden, dan forensik.

j) A10:2021-Server-Side Request Forgery (SSRF)

A10:2021-Pemalsuan Permintaan Sisi Server ditambahkan dari survei komunitas Top 10 (#1). Data menunjukkan tingkat kejadian yang relatif rendah dengan cakupan pengujian di atas rata- rata, serta peringkat di atas rata-rata untuk potensi Eksploitasi dan Dampak. Kategori ini mewakili skenario di mana anggota komunitas keamanan memberi tahu kami bahwa ini penting, meskipun tidak diilustrasikan dalam data saat ini.

4. OWASP ZAP

OWASP ZAP (Zed Attack Proxy) merupakan sebuah aplikasi yang digunakan untuk penetration testing dalam menemukan vulnerabilities/celah keamanan pada suatu aplikasi ataupun website. ZAP menyediakan scanner secara automatis (Guntoro et al., 2020).

5. Penetration Testing

Penetration testing adalah sebuah pengujian terhadap sebuah website yang bertujuan untuk mengevaluasi keamanan suatu website. Pengujian dilakukan dengan sebuah simulasi serangan terhadap sistem untuk menemukan celah keamanan yang dapat terjadi dari konfigurasi yang tidak benar, kelemahan dalam proses teknis, dan kelemahan lain yang dapat menjadi celah keamanan pada sistem tersebut. Hasil dari Penetration testing dapat menjadi sebuah laporan yang bisa menjadi masukan kepada pemilik sistem tentang celah keamanan terhadap sistem yang mereka miliki kemudian digunakan untuk proses evaluasi guna melakukan penambalan terhadap kebocoran celah yang ditemukan (IRAWAN, 2022). Berdasarkan objeknya, Pentetration testing terdapat enam jenis:

a. Network Service

Objek yang diuji dalam network service penetration test adalah infrastruktur jaringan. Tujuan utama dari jenis penetration test ini untuk mengidentifikasi kelemahan pada objek-objek network service seperti server, firewall, switch, router, printer, workstation, dan lain-lain.

b. Web Application

Web application penetration test digunakan untuk menemukan kerentanan dan kelemahan keamanan pada aplikasi berbasis web. Penetration test ini menggunakan beberapa teknik dan serangan yang tujuannya untuk menembus keamanan suatu web application. Beberapa elemen yang dipindai dalam upaya penetration test jenis ini antara lain web based application, browser dan komponen-komponen lainnya. Cara melakukan penetration test jenis ini mengalami

perubahan dari waktu ke waktu. Seiring perkembangan teknologi yang kian pesat, tingkat ancaman juga ikut berkembang.

c. *Client Side*

Client side penetration test digunakan untuk menemukan kelemahan keamanan pada client side application. Beberapa program atau aplikasi yang termasuk client side application antara lain Putty, email clients, web browsers, Macromedia Flash, dan lain-lain.

d. *Wirelles*

Wireless penetration test melibatkan identifikasi dan inspeksi koneksi yang menghubungkan perangkat-perangkat dalam satu jaringan wifi perusahaan. Beberapa perangkat yang menjadi objek pentest jenis ini antara lain, desktop, laptop, tablet, smartphones, dan Internet of Things (IoT).

e. *Social Engineering*

Social penetration test merupakan sebuah upaya untuk membujuk atau menebar trik kepada user untuk memberikan informasi sensitif. Beberapa data yang kerap menjadi sasaran upaya ini antara lain username dan password. Serangan cyber social engineering yang biasa dilakukan oleh pentester antara lain: Physing, Tailgating, Imposter, Name Dropping, Pre-texting, Dumpster Diving, Eaves Dropping, dan Gifts.

f. *Physical*

Physical penetration test merupakan upaya dari pentester untuk menembus hambatan fisik dari infrastruktur, bangunan, sistem, bahkan staf dari sebuah perusahaan.

6. Keamanan Data

Keamanan Data merupakan upaya perlindungan data dari ancaman untuk meminimalisir risiko bisnis, menjamin kelanjutan proses bisnis dan meningkatkan investasi. Jadi dapat diartikan bahwa keamanan informasi merupakan sebuah perlindungan dari ancaman yang dapat menggangu proses bisnis dalam sebuah sistem ataupun membahayakan kebocoran informasi dari sistem tersebut.