BAB III

METODOLOGI PENELITIAN

3.1 Jenis dan Pendekatan Penelitian

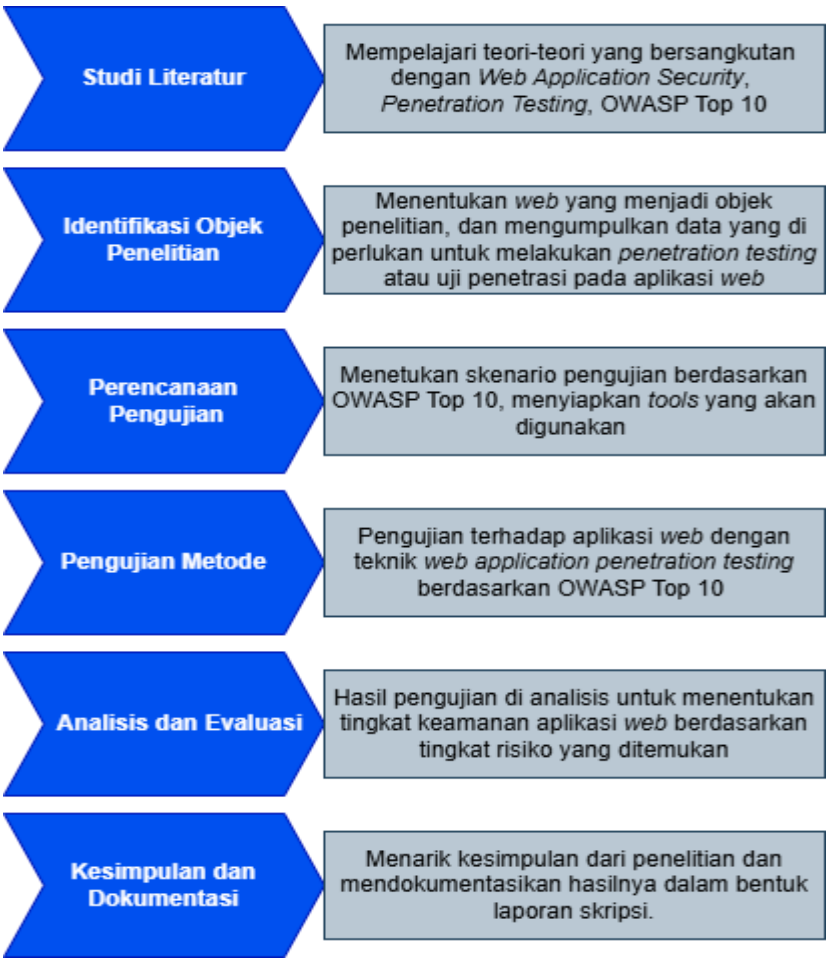
Penelitian ini merupakan penelitian terapan dengan pendekatan deskriptif kualitatif dan teknis eksperimental terbatas. Disebut terapan karena hasil penelitian diarahkan untuk memberikan rekomendasi perbaikan keamanan pada aplikasi *web* SINTESYS. Disebut teknis eksperimental terbatas karena pengujian dilakukan melalui simulasi serangan terkendali terhadap skenario tertentu tanpa merusak sistem atau mengubah data.

3.2 Objek Penelitian

Objek penelitian adalah aplikasi *web* SINTESYS Universitas Siliwangi . Aplikasi ini dipilih karena berperan sebagai salah satu layanan akademik berbasis *web* yang berhubungan dengan data dan aktivitas pengguna di lingkungan perguruan tinggi. Pengujian dilakukan hanya pada ruang lingkup yang diizinkan dan tidak mencakup sistem lain di luar objek penelitian

3.3 Tahapan Penelitian

Alur penelitian pada gambar terdiri dari lima bagian utama dalam alur penelitian, pertama aadalah studi literatur, identifikasi objek penelitian, perencanaan pengujian, pengujian metode, analisis dan evaluasi serta kesimpulan dan dokumentasi



Gambar 3.1 Alur Penelitian

Penjelasan mengenai alur penelitian dapat dijelaskan sebagai berikut :

a. Studi Literatur

Pada tahap ini, berbagai referensi dan teori yang berhubungan dengan keamanan aplikasi *web* dikumpulkan. Studi literatur mencakup pemahaman tentang konsep keamanan aplikasi, metode pengujian keamanan berbasis *web application penetration testing,* dan standar keamanan yang digunakan dalam OWASP Top 10. Langkah ini juga berusaha untuk menganalisis penelitian sebelumnya yang relevan

untuk mendapatkan pemahaman tentang metode yang digunakan dan kemungkinan kemajuan yang dapat dibuat dalam penelitian ini.

b. Identifikasi Objek Penelitan

Pemilihan aplikasi *web* yang akan menjadi objek penelitian penelitian adalah fokus utama dari tahapan ini. Identifikasi dilakukan dengan mempertimbangkan atribut aplikasi, termasuk teknologi, fitur utama, dan kemungkinan ancaman keamanan. Selain itu ruang lingkup OWASP Top 10 dimodifikasi untuk menetapkan ruang lingkup pengujian, yang membuat pengujian menjadi lebih metodis dan terfokus. Koordinasi dengan pengelola aplikasi dilakukan sebelum melanjutkan ke tahap berikutnya untuk memastikan pengujian dilakukan dengan cara yang bertanggung jawab secara moral dan hukum.

c. Perencanaan Pengujian

Tahap selanjutnya adalah membuat recana dan strategi untuk pengujian keamanan ketika topik penelitian telah diputuskan. Proses perencanaan melibatkan pemilihan metodologi pengujian, seperti *black box, grey box,* atau *white bo testing,* dan membuat skenario pengujian berdasarkan daftar OWASP Top 10. Alat pengujian, termasuk *burp suite,* OWAS ZAP, SQLMap, dan Nmap, juga dipilih pada tahap ini. Selanjutnya, proses pencatatan temuan pengujian dibuat untuk menjamin bahwa setiap temuan dapat dinilai dengan tepat.

d. Pengujian Metode

Tahapan ini merupakan proses utama dalam penelitian ini, di mana pengujian penetrasi dilakukan terhadap aplikasi *web.* Langlah-langkah dalam pengujian keamanan adalah sebagai berikut :

1. ***Scanning***

Scanning adalah tahap awal yang sangat penting dalam langkah pengujian keamanan aplikasi *web* karena memberikan gambaran menyeluruh mengenai arsitektur sistem, layanan yang berjalan, serta potensi celah keamanan yang dapat dimanfaatkan dalam tahap eksploitasi selanjutnya.

2. **Pengujian Berdasarkan Kerangka Kerja OWASP Top 10**

Menguji setiap kerentanan yang telah di temukan dari hasil *scanning* yang telah dilakukan pada tahap sebelumnya dengan berdasarkan kerangka kerja OWASP Top 10 sebagai berikut :

a. A01:2021-*broken access control* kerentanan ini terjadi ketika aplikasi *web* tidak menerapkan pembatasan hak akses pengguna dengan benar.
b. A02:2021-*cryptographic failures* fokus kerentanan ini merujuk pada kegagalan dalam melindungi data yang sedang transit (*data-in-transit)* atau data yang disimpan *(data-at-rest)*
c. A03:2021-*injection* kategori ini mencakup celah di mana data yang dimasukkan oleh pengguna tidak disaring atau divalidasi oleh aplikasi *web*.
d. A04:2021-*inscure design* kategori yang berfokus pada kesalahan fase arsitektur dan desain sebelum pengodean dimulai.
e. A05:2021-*security misconfiguration* kerentanan ini terjadi ketika komponen sistem *(server web,database)* tidak dikonfigurasi dengan prinsip keamanan yang ketat..
f. A06:2021-*vulnerable and outdated components* kerentanan ini terjadi ketika aplikasi *web* menggunakan pustaka *(library)*, modul, *framework,* atau

sistem operasi pihak ketiga yang sudah memiliki celah keamanan public (CVE) atau sudah tidak didukung lagi oleh pengembangnya.

g. A07:2021-*identification and authentication failures* kategori kerentanan ini berkaitan dengan lemahnya sistem dalam memverifikasi identitas pengguna, sesi *login*, atau kredensial..

h. A08:2021-*software and data integrity failures* kategori kerentanan yang berfokus pada asumsi kode atau pustaka yang dimuat tanpa melakukan verifikasi integritas terlebih dahulu..

i. A09:2021-*security logging and monitoring failures* risiko kerentanan ini terjadi ketika aplikasi tidak mencatat aktivitas mencurigakan atau gagal memberikan peringatan dini saat terjadi upaya peretasan.

j. A10:2021-*server-side request forgery* (SSRF) kerentanan ini terjadi ketika aplikasi *web* melakukan penjemputan data (*fetching resource)* dari *URL* eksternal yang diinput oleh pengguna tanpa melakukan validasi terhadap alamat tujuan.

3.4 Lingkungan dan *Tools* Pengujian

Pengujian dilakukan menggunakan beberapa *tools* yang dipilih berdasarkan fungsi masing-masing. OWAS ZAP digunakan untuk pemindaian otomatis dan identifikasi awal *alert. Burp Suite* digunakan untuk observasi *request* dan validasi otorisasi secara terkendali. *SQLmap* digunakan untuk membantu pengujian indikasi *SQL Injection* pada parameter yang relevan. Paramspider dan Dalfox digunakan untuk membantu identifikasi parameter dan validasi potensi XSS. *Browser*

developer tools digunakan untuk memeriksa *respons header, cookie,* dan perilaku antar muka.

Tabel 3.1 *Tools* Penelitian

No	*Tools*	Fungsi dalam Penelitian	Output yang Diharapkan
1	OWAS ZAP	Pemindaian otomatis dan *passive active scan* terbatas	Daftar *alert, risk level, evidence* awal
2	*Burp Suite*	*Intercept* dan validasi aplikasi	Bukti kontrol akses dan perilaku *session*
3	*SQLmap*	Pengujian indikasi *SQL Injection* secara terkendali	Status rentan/tidak rentan pada parameter uji
4	Paramspider	Identikasi parameter indikasi XSS	Status eksekusi/tidak eksekusi *payload* uji
5	Dalfox	Validasi indikasi XSS menggunakan *payload*	Status rentan/tidak rentan aplikasi pada XSS

3.5 Skenario Pengujian

Skenario pengujian disusun berdasarkan temuan awal dan kategori OWASP Top 10 yang relevan. Setiap skenario memiliki indikator keberhasilan agar hasil pengujian dapat dinilai secara konsisten.

Tabel 3.2 Skenario Pengujian

No	Kategori OWASP	Skenario Uji	Indikator Keberhasilan	Status yang Dicatat
1	A03:2021 *Injection*	Pengujian *SQL Injection* pada parameter yang relevan	Terdapat *respons* yang menunjukan manipulasi *query, error database*, atau *bypass* autentikasi	*Positive/Negative*
2	A03:2021 *Injection*	Pengujian *Cross-Site Scripting* pada parameter *URL* atau input	*Payload* uji tereksekusi pada *browser*	*Positive/Negative*
3	A05:2021 *Security Misconfiguration*	Pengujian pemuatan halaman dalam *iframe*	Halaman target dapat dimuat oleh halaman pihak lain	*True Positive/False Positive*
4	A05/07:2021 *Session Management*	Pemeriksaan atribut *cookie* sesi	*Cookie* sensitif dapat diakses oleh *java script* atau tidak memiliki atribut aman	*True Positive/* Perlu Validasi Lanjutan
5	A01:2021 *Broken Access Control*	Pengujian akses objek langsung pada fitur akademik	Data akun lain dapat diakses melalui manipulasi *request*	*Positive/Negative*

3.6 Teknik Analisis Data

Data yang dianalisis dalam penelitian ini berupa hasil *alert* dari *tools,* bukti validasi manual, status keberhasilan skenario uji, dan dampak keamanan dari setiap temuan. Analisis dilakukan melalui empat langkah. Pertama, setiap *alert* diklasifikasikan berdasarkan tingkat risiko. Kedua, *alert* yang relevan divalidasi secara manual. Ketiga, temuan dipetakan ke dalam kategori OWASP Top 10 dan aspek CIA. Keempat, rekomendasi remediasi disusun berdasarkan prioritas risiko.

Tabel 3.3 Teknik Analisis Data

Status Temuan	Definisi
True Positive	Temuan otomatis atau indikasi awal berhasil dibuktikan melalui validasi manual
False Positive	*Alert* muncul pada *tools,* tetapi tidak terbukti sebagai celah setelah divalidasi
Negative Finding	Skenario uji tidak menunjukan kelemahan pada aspek yang diuji
Informational	Temuan bersifat informasi pendukung dan belum menunjukan dampak langsung tanpa bukti tambahan