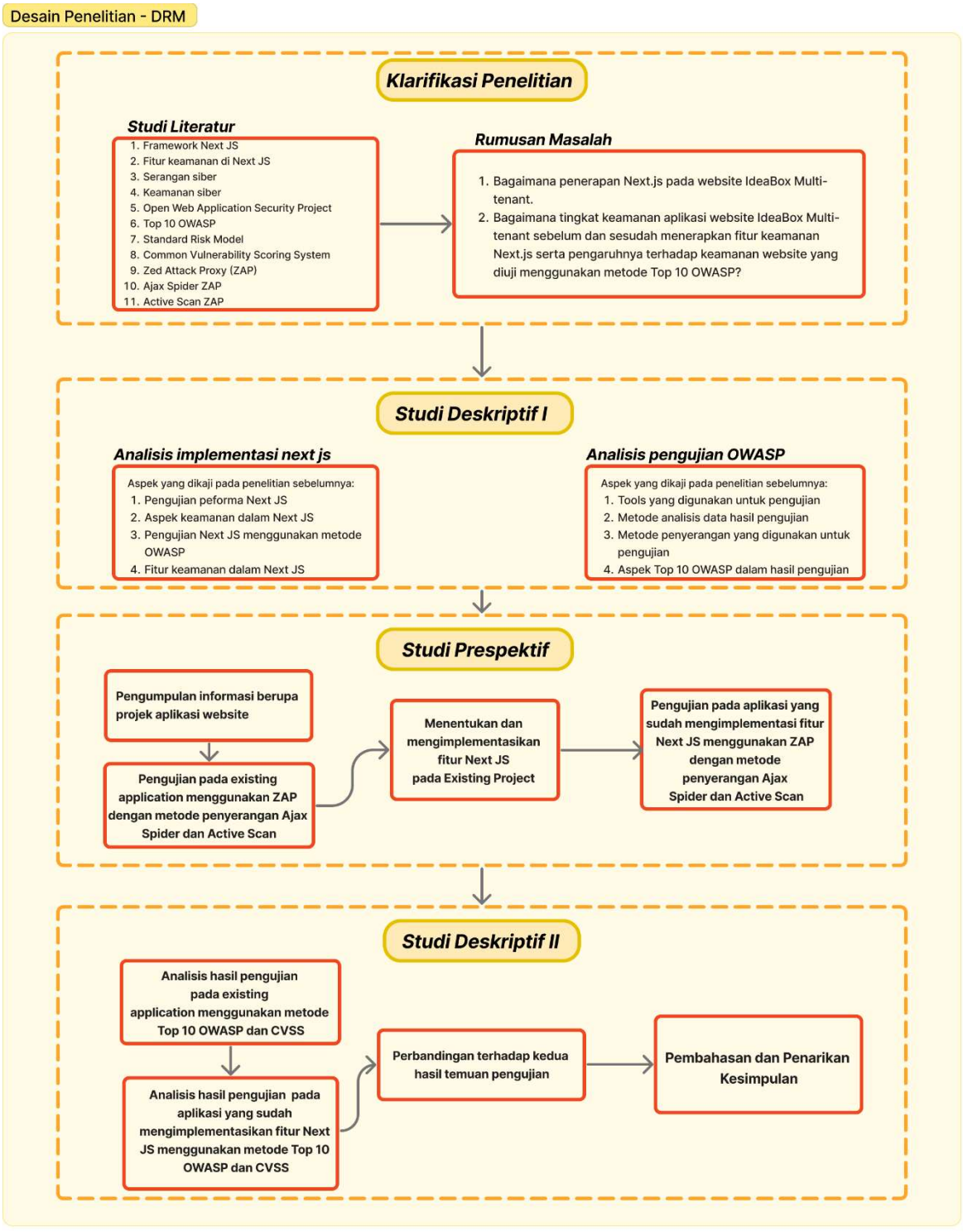
BAB III
METODE PENELITIAN

3.1 Desain Penelitian

Desain penelitian berfungsi untuk menggambarkan beberapa tahapan yang dilakukan pada penelitian ini. Penelitian ini dilakukan dengan urutan yang mengacu pada *Design Research Methodology* (DRM). Menurut Blessing dkk. (1998) pada penelitiannya yang berjudul "*An Overview of Descriptive Studies in Relation to a General Design Research Methodology*", DRM merupakan kumpulan metode dan panduan pendukung yang akan berfungsi sebagai landasan untuk melaksanakan penelitian perancangan. Dalam konteks penelitian perancangan, DRM bertujuan untuk menghasilkan pengetahuan dan pemahaman yang mendalam tentang desain dan pengembangan produk, serta menerapkan pemikiran kreatif dan strategi desain yang efektif.

DRM dapat mencakup langkah-langkah seperti identifikasi masalah desain, perancangan konsep, pembuatan prototipe, pengujian, dan iterasi. Tujuannya adalah untuk memahami bagaimana desain berkontribusi pada tujuan dan kebutuhan pengguna, serta bagaimana proses perancangan dapat ditingkatkan (Blessing et al., 1998). Adapun desain penelitian dari penelitian ini didefiniskan pada Gambar 3.1.



Gambar 3.1 Desain Penelitian

3.1.1. Klarifikasi Penelitian

Klarifikasi penelitian merupakan langkah awal dari DRM, pada bagian ini, penulis mengambil topik terkait implementasi fitur *Next.js* pada sebuah aplikasi website untuk menguji tingkat keamanannya dalam perlindungan data pengguna, langkah pengujiannya akan dilakukan menggunakan metode *TOP 10 OWASP* dari OWASP. Adapun langkah-langkah yang dilakukan di tahap klarifikasi penelitian yaitu melakukan studi literatur guna untuk mengumpulkan data dan teori-teori yang relevan dan dapat digunakan sebagai landasan dalam penelitian ini.

Beberapa studi literatur tersebut diantaranya adalah mengkaji Framework *Next.js,* fitur security di Next.js, keamanan siber, serangan siber, aspek *confidentiality* di keamanan siber, standarisasi OWASP, *Top 10 OWASP,* standarisasi *injection* di OWASP dan *Common Vulnerability Scoring System*. Kajian tersebut dibahas pada BAB II yang berasal dari berbagai sumber seperti jurnal, artikel, buku, skripsi, tesis, dsb.

Dari studi literatur yang sudah dilakukan, didapat beberapa rumusan masalah dan tujuan penelitian yang dibahas pada BAB I.

3.1.2. Studi Deskriptif I

Pada tahap ini, penulis akan melakukan analisis penelitian-penelitian terdahulu yang relevan dengan topik penelitian, tujuan dari tahapan ini adalah memperdalam pehamaman terkait topik penelitian dengan cara membandingkannya dengan penelitian terdahulu yang relevan. Ada dua tahapan yang akan di analisis dari penelitian terdahulu, yang pertama yaitu analisis implementasi Next.js, dengan aspek yang dikaji mengenai pengujian peforma Next.js, aspek keamanan Next.js, Pengujian Next.js Menggunakan metode OWASP dan Fitur keamanan dalam Next.js, lalu tahapan kedua yang akan di analisis dari penelitian terdahulu adalah analisis pengujian OWASP, dengan aspek yang dikaji mengenai tools yang digunakan untuk pengujian, metode analisis data hasil pengujian, metode penyerangan yang digunakan untuk pengujian dan aspek Top 10 OWASP dalam hasil pengujian.

3.1.3. Studi Prespektif

Setelah melakukan pemahaman mendalam mengenai topik penelitian dan melakukan perbandingan dengan penelitian penelitian terdahulu yang relevan, selanjutnya dilakukan proses studi prespektif yaitu merancang tahap implementasi dan pengujian yang akan dilakukan, ada 3 tahapan yang akan dilakukan studi prespektif.

Tahap pertama adalah pengumpulan informasi bahan penelitian berupa projek aplikasi website yang berupa *domain* website yang akan digunakan dalam tahap pengujian.

Tahap kedua adalah melakukan pengujian pada aplikasi website IdeaBox Multi-tenant yang berteknologi React.js dan Laravel, menggunakan *Zed Attack Proxy* (ZAP) dengan metode penyerangan *AJAX Spider* dan *Active Scan*, pada tahapan ini penulis akan melakukan pengujian menggunakan metode *Automated Scan*, yaitu metode penyerangan *AJAX Spider* dan *Active Scan* dalam aplikasi ZAP, hasil pengujian yang diperoleh akan menggambarkan celah kerentanan keamanan dari berbagai aspek yang terdapat pada aplikasi website.

Tahap ketiga adalah menentukan dan mengimplementasikan fitur Next.js pada projek aplikasi website (IdeaBox Multi-tenant). Berdasarkan hasil studi literatur dan hasil pengujian yang telah dilakukan, kebutuhan fitur Next.js dan library yang akan digunakan pada penelitian ini antara lain adalah Next.js *Server-Side Rendering* untuk membantu mengurangi jenis serangan tertentu seperti XSS Attack dan memberikan kontrol yang lebih baik terhadap proses pengiriman konten pada website, Next.js *Middleware* sebagai otorisasi untuk memastikan hanya pengguna yang terotorisasi yang dapat mengakses dan mengubah data sensitif, *Formik* dan *Yup* untuk validasi dan sanitasi input user, *Nookies* untuk menjaga akses masuk pengguna (autentikasi), dan *bcrypt* untuk mengamankan data sensitif seperti kata sandi pengguna, *API keys*, dan token dengan cara enkripsi. Proses implementasi fitur atau library yang telah ditentukan terdiri dari beberapa langkah:

1. Membangun infrastruktur Next.js.
2. Memasang library yang dibutuhkan ke dalam projek.
3. Koding dan implementasi dengan menggunakan bahasa JavaScript.

Tahap keempat adalah melakukan pengujian pada aplikasi website yang sudah mengimplementasikan fitur Next.js, menggunakan *Zed Attack Proxy* (ZAP) dengan metode penyerangan *AJAX Spider* dan *Active Scan*, pada tahapan ini penulis akan melakukan pengujian menggunakan metode *Automated Scan*, yaitu metode penyerangan *AJAX Spider* dan *Active Scan* dalam aplikasi ZAP, hasil pengujian yang diperoleh akan menggambarkan celah kerentanan keamanan dari berbagai aspek yang terdapat pada aplikasi website.

3.1.4. Studi Deskriptif II

Guna mengetahui tingkat keberhasilan penelitian ini, diperlukan analisis dan pembahasan untuk mendapatkan data yang konkrit, pada tahap Studi Deskriptif II ini, terdapat 4 tahap yang akan dilakukan.

Tahap pertama adalah melakukan analisis hasil pengujian pada aplikasi website IdeaBox Multi-tenant yang berteknologi React.js menggunakan metode Top 10 OWASP dan CVSS. Pada tahap ini, penulis akan melakukan analisis data hasil pengujian yang sudah dilakukan pada aplikasi website yang belum menerapkan fitur Next.js, menggunakan metode Top 10 OWASP untuk mengklasifikasikan kerentanan yang teridentifikasi oleh sistem, lalu menghitung skor *Common Vulnerability Scoring System* pada masing masing instrumen Top 10 OWASP.

Tahap kedua adalah melakukan analisis hasil pengujian pada aplikasi website yang mengimplementasikan fitur Next.js, menggunakan metode Top 10 OWASP dan CVSS. Pada tahap ini, penulis akan melakukan analisis data hasil pengujian yang sudah dilakukan pada aplikasi website yang sudah menerapkan fitur Next.js, menggunakan metode Top 10 OWASP untuk mengklasifikasikan kerentanan yang teridentifikasi oleh sistem, lalu

menghitung skor *Common Vulnerability Scoring System* pada masing masing instrumen Top 10 OWASP.

Tahap ketiga adalah melakukan perbandingan terhadap kedua hasil temuan pengujian, pada tahap ini, penulis akan membandingkan semua hasil temuan setelah melakukan pengujian saat sebelum dan sesudah mengimplementasikan fitur NEXT.JS dengan menggunakan parameter yang sama, berdasarkan studi literatur terhadap penelitian terdahulu yang telah dilakukan. Parameter yang akan digunakan dalam perbandingan yang pertama yaitu vulnerability, *alerts* yang dihasilkan oleh *Zed Attack Proxy* (ZAP) memberikan informasi tentang kerentanan spesifik yang telah diidentifikasi dalam aplikasi. Lalu yang kedua yaitu total *vulnerability*, parameter ini memberikan gambaran tentang jumlah total kerentanan yang ditemukan dalam sebuah aplikasi. Lalu yang ketiga yaitu *Top 10 owasp vulnerability*, parameter ini memberikan gambaran tentang aspek apa saja yang rentan dalam Top 10 OWASP. Parameter keempat adalah rata rata CVSS score, rata-rata skor CVSS dari kerentanan yang ditemukan dapat memberikan gambaran keseluruhan tentang tingkat risiko yang dimiliki aplikasi. Parameter terakhir adalah status CVSS, berdasarkan hasil perhitungan rata rata skor CVSS, dapat disimpulkan kelas dampak kerentanan menggunakan penilaian CVSS.

Tahap keempat adalah pembahasan dan penarikan kesimpulan. Dari hasil perbandingan terhadap kedua hasil temuan pengujian yang sudah dilakukan, dapat dilakukan pembahasan dan akan menghasilkan sebuah kesimpulan untuk menunjukan tingkat kerentanan keamanan aplikasi website yang sudah mengimplementasi fitur Next.js.

3.2 Alat dan Bahan Penelitian

3.2.1 Alat Penelitian

Alat penelitian terdiri dari perangkat keras dan perangkat lunak, berikut perangkat keras yang digunakan dalam penelitian ini sebagai berikut.

a) Prosesor Intel Core i7-8665 8 CPU 2.1 GHz
b) RAM 8 GB DDR4

c) SSD 256 GB

Berikut perangkat lunak yang digunakan dalam penelitian ini sebagai berikut.

1. Microsoft Windows 11 Pro
2. Visual Studio Code
3. Node Package Manager (NPM)
4. Node JS
5. React JS
6. Next.js
7. JavaScript
8. Zed Attack Proxy 2.14.0
9. CVSS 3.0
10. Google Chrome
11. Git Bash
12. Formik (*libraries)*
13. Yup (*libraries)*
14. Nookies (*libraries)*
15. Bcrypt (*libraries)*

3.2.2 Bahan Penelitian

Beberapa bahan penelitian yang akan digunakan pada penelitian ini diantaranya adalah jurnal, buku, artikel ilmiah, serta dokumentasi resmi dari teknologi yang digunakan akan digunakan sebagai bahan penelitian untuk menunjang pemahaman penulis dalam proses implementasi dan pengujian penelitian ini.

3.3 Instrumen Penelitian

Melalukan eksperimen pengujian non-partisipan pada aplikasi website *IdeaBox Multi-Tenant* dengan menggunakan metode Top 10 OWASP. Dimana *Top 10 OWASP* merupakan framework dari OWASP yang populer dan banyak digunakan pada aplikasi website saat ini (Abdan, 2022). Pengujian *Top 10 OWASP* akan

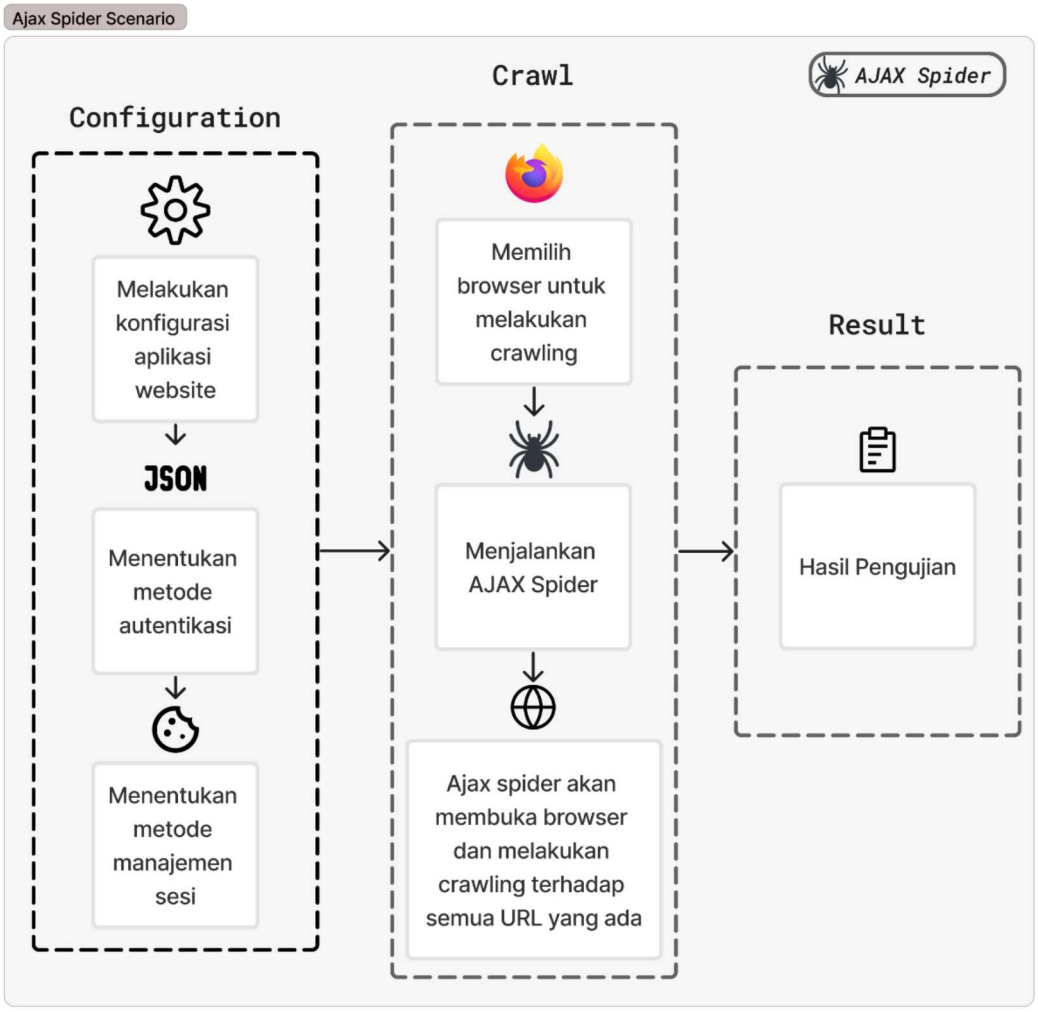
menggunakan metode penyerangan *Ajax Spider* dan *Active Scan* dari aplikasi *Zed Attack Proxy* (ZAP) yang merupakan *tools* yang paling aktif karena masih terus dikembangkan. (Yudiana et al., 2021).

Untuk menentukan tingkat resiko dari masing masing kerentanan yang dikategorisasikan oleh *Top 10 OWASP*, akan dihitung dengan kalkulator khusus dari NIST (*National Institute of Standards and Technology*) yang disebut CVSS (*Common Vunlnerability Scoring System*) dengan rentang score 0.0 sampai 10.0 menggunakan *Base Metrics*.

Untuk menentukan tingkat kemungkinan kerentanan terjadi dari masing masing kerentanan yang dikategorisasikan oleh *Top 10 OWASP*, akan menggunakan metode *Standad Risk Model* dari OWASP. Menggunakan step pertama yaitu mengidentifikasi resiko, kedua melakukan perhitungan terhadap semua parameter atau faktor untuk menentukan *likelihood* (kemungkinan), keempat menentukan tingkat kemungkinan kerentanan terjadi.

3.3.1 Skenario Pengujian *Ajax Spider* ZAP

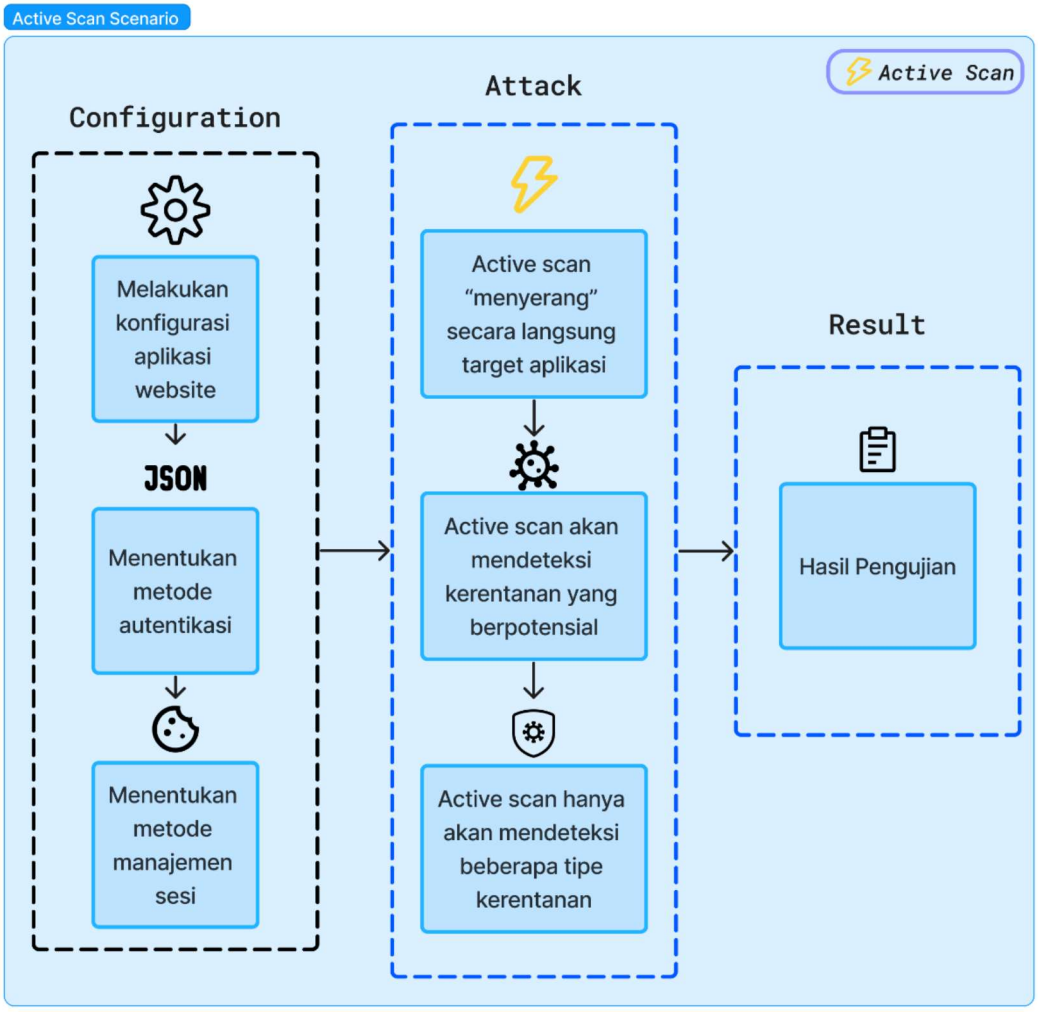
Pengujian ini dilakukan untuk mengidentifikasi potensial kerentanan keamanan pada aplikasi web. Metode Ajax Spider ZAP digunakan untuk secara otomatis mengeksplorasi aplikasi web dan mendeteksi interaksi dinamis antara komponen-komponen dalam aplikasi. Skenario dari pengujian menggunakan metode penyerangan Ajax Spider ZAP didefinisikan pada Gambar 3.2.



Gambar 3.2 Skenario Pengujian Ajax Spider

3.3.2 Skenario Pengujian *Active Scan* ZAP

Pengujian ini dilakukan untuk mengidentifikasi potensial kerentanan keamanan pada aplikasi web. Metode *Active Scan* ZAP digunakan untuk secara otomatis melakukan penyerangan secara langsung terhadap target aplikasi serta mendeteksi potensial kerentanan keamanan yang ada. *Active Scan* hanya dapat mendeteksi beberapa tipe kerentanan. Skenario dari pengujian menggunakan metode penyerangan *Active Scan* ZAP didefinisikan pada Gambar 3.3.



Gambar 3. 3 Skenario Pengujian *Active Scan*

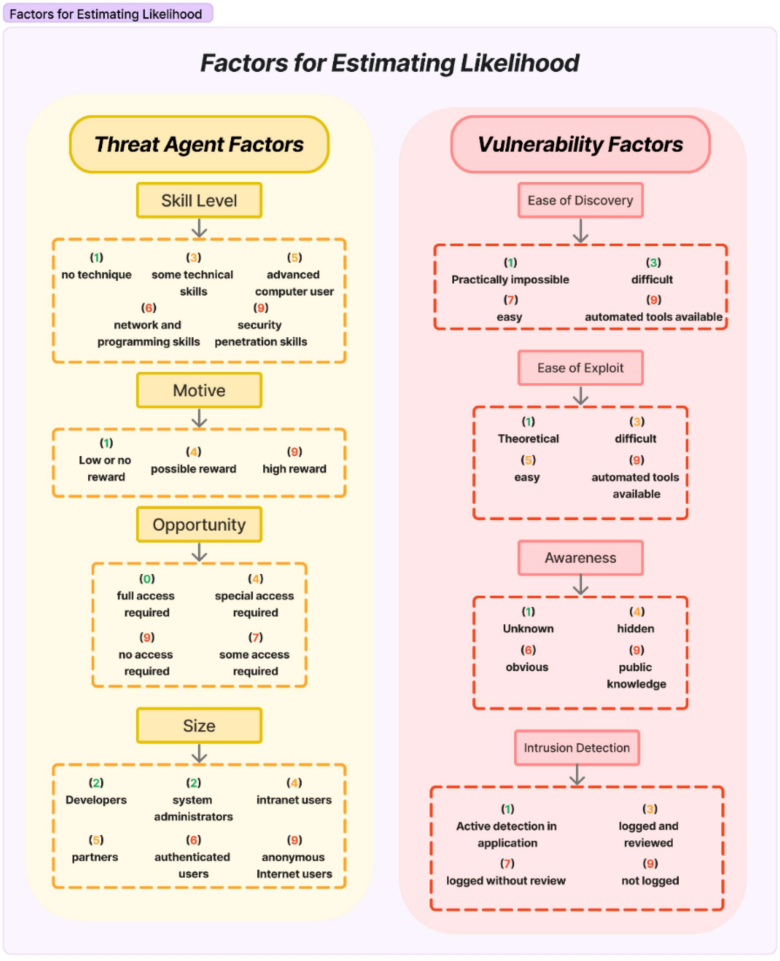
3.3.3 Tingkat Kemungkinan Kerentanan *Top 10 OWASP*

Tingkat kemungkinan kerentanan terjadi pada kerentanan yang ditemukan Top 10 OWASP akan diukur menggunakan metode *Standard Risk Model* dari OWASP yang diuraikan pada Tabel 3.1.

Tabel 3.1
Skala Penilaian Tingkat Kemungkinan Terjadi Kerentanan

Scale	*Likelihood Level*
0 – 2	*Low*
3 – 5	*Medium*
6 - 9	*High*

Untuk mendapatkan nilai skala untuk mengukur tingkat kemungkinan kerentanan terjadi, dibutuhkan faktor pengambilan nilai dari masing-masing parameter yang diuraikan pada Gambar 3.4 menurut dokumentasi resmi dari OWASP.



Gambar 3.4 *Factors for estimating likelihood.*

3.3.4 Tingkat Resiko Kerentanan *Top 10 OWASP*

Tingkat resiko kerentanan *Top 10 OWASP* akan diukur menggunakan kalkulator CVSS 3.0 dengan skala penilaian tingkat keparahan kualitatif yang diuraikan pada Tabel 3.2.

Tabel 3.2
Skala Penilaian Tingkat Keparahan Kualitatif CVSS

Rating	***CVSS Score***
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

3.4 Analisis Data

Untuk menentukan tingkat kemungkinan kerentanan dan tingkat resiko *Top 10 OWASP* akan dilakukan analisis data menggunakan persamaan atau fungsi yang didapatkan dari hasil studi literatur yang dilakukan.

3.4.1 Faktor Untuk Mengukur *Likelihood*

Untuk dapat menentukan tingkat kemungkinan kerentanan terjadi terhadap masing masing kerentanan *Top 10 OWASP*, akan menggunakan skor rata rata yang didapat dari hasil perhitungan terhadap semua faktor dan parameter untuk mengukur *likelihood*. Berdasarkan dokumentasi resmi dari OWASP, rata rata skor *likelihood* didefinisikan sebagai:

$$AVG\ Likelihood = \frac{Threat\ Agent\ Factors\ Score + Vulnerability\ Factors\ Score}{Total\ Parameter} \quad (1)$$

$$AVG\ Likelihood = \frac{SL+M+OP+S+Eod+Eoe+A+ID}{8} \quad (2)$$

3.4.2 Persamaan Tingkat Resiko Kerentanan *Top 10 OWASP*

Untuk dapat menentukan tingkat resiko dari masing masing kerentanan *Top 10* OWASP, akan menggunakan skor dari perhitungan *Base Metrics* CVSS. Skor *Base Metrics* merupakan fungsi dari persamaan subskor mertrik *Impact* dan *Exploitability*. Berdasarkan dokumentasi resmi dari CVSS, skor *base metrics* didefinisikan sebagai berikut:

$$\boldsymbol{If}\ (Impact\ sub\ score \leq 0)\ then\ 0$$

$$\boldsymbol{Else}:$$

$$\boldsymbol{Scope\ unchanged}\ ?\ Round\ up\ (Minimum\ [(Impact + Exploitability), 10])$$

$$\boldsymbol{Scope\ changed}\ ?\ Round\ up\ (Minimum\ [1.08 * (Impact + Exploitability), 10])$$

$$\boldsymbol{ISC} = Scope\ Unchanged\ 6.42 * ISC_{Base}$$

$$\boldsymbol{ISC} = Scope\ Changed = 7.5 * [ISC_{Base} - 0.029] - 3.25 * [ISC_{Base} - 0.02]^{15}$$

$$\boldsymbol{Where},$$

$$ISC_{Base} = 1 - \left[\left(1 - Impact_{Conf}\right) * \left(1 - Impact_{Integ}\right) * \left(1 - Impact_{Avail}\right)\right]$$

$$\boldsymbol{Expoloitability\ Score}\ (\boldsymbol{ES}) = 8.22 * AV * AC * PR * UI$$