BAB 3
METODE PENELITIAN

3.1 Metode Penelitian

Penelitian ini melakukan *risk assessment* pada aplikasi *e-commerce* di Indonesia menggunakan tahapan-tahapan berdasarkan NIST (*National Institute of Standards and Technology*) SP 800-30. Adapun tahapan metode yang dilakukan terdapat pada Gambar 3.1.

Gambar 3. 1 Metode penelitian

Tahapan-tahapan metode penelitian yang dilakukan berdasarkan NIST SP 800-30 yaitu:

1. **Identifikasi Aplikasi**

   Pada tahap ini, melakukan proses identifikasi awal terhadap potensi risiko keamanan pada aplikasi *e-commerce* di Indonesia yang akan diuji. Langkah pertama yang dilakukan yaitu mengidentifikasi aplikasi *e-commerce* yang akan dianalisis yang terdiri dari lima aplikasi populer di Indonesia yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak. Aplikasi dikumpulkan dengan mengunduh melalui Google Play Store yang di *install* pada

smartphone android dan kemudian dilakukan *back up* data dari *smartphone* android ke laptop untuk dilakukan identifikasi selanjutnya. Kemudian menentukan aset informasi penting yang menjadi fokus analisis yang meliputi info aplikasi, izin aplikasi, data pengguna yang dibagikan dan dikumpulkan, fitur keamanan, dan mekanisme autentikasi yang diterapkan pada setiap aplikasi. *Output* dari tahap ini yaitu untuk mendapatkan data lengkap dari aplikasi yang akan dianalisis serta identifikasi awal terhadap aset informasi potensi risiko keamanan yang terkait.

2. Pemindaian Kerentanan dengan MobSF

Pada tahap ini yaitu melakukan pemindaian kerentanan pada file APK dari aplikasi *e-commerce* yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak menggunakan *Mobile Security Framework* (MobSF) dengan pendekatan analisis statis (*static analysis*). Fokus utama dari pendekatan ini adalah pemeriksaan terhadap struktur internal aplikasi melalui analisis kode sumber dan konfigurasi yang terdapat dalam file APK. Penelitian ini tidak mencakup pengujian langsung terhadap sistem *backend* (seperti *server, database*, atau API). Meskipun kebocoran informasi umumnya terjadi pada sisi *backend*, pengujian dalam penelitian ini difokuskan pada sisi *frontend*, yaitu dengan melakukan analisis statis terhadap file APK. Analisis ini bertujuan untuk mengidentifikasi potensi kerentanan yang dapat menyebabkan kebocoran data dari sisi pengguna, seperti *hardcoded secrets*, izin akses berbahaya, algoritma kriptografi, konfigurasi SSL/TLS, dan penyimpanan data yang tidak aman. Dalam tahap pemindaian kerentanan menggunakan MobSF dengan pendekatan analisis statis akan mengidentifikasi kerentanan terkait *hardcoded secrets*, *weak cryptography*, *insecure data storage*, *dangerous permissions*, dan SSL/TLS *misconfiguration*.

a. *Hardcoded Secrets*

Mengidentifikasi adanya penyimpanan informasi sensitif seperti API *keys, credentials*, atau token secara langsung di dalam *source code* aplikasi. Tujuan deteksi ini yaitu untuk menilai potensi pencurian akses

ke layanan *backend* atau *database* yang berisiko menyebabkan kebocoran data pengguna ataupun akses tidak sah ke sistem aplikasi.

b. *Weak Cryptography*

Menilai penggunaan algoritma kriptografi yang sudah tidak aman atau usang. Tujuannya adalah untuk memastikan bahwa aplikasi menggunakan algoritma kriptografi modern dan kuat yang mampu melindungi integritas dan kerahasiaan data pengguna.

c. *Insecure Data Storage*

Menilai praktik penyimpanan data sensitif pada perangkat pengguna seperti informasi *login* atau transaksi yang disimpan dalam bentuk *plaintext* atau tanpa mekanisme proteksi seperti enkripsi. Tujuan deteksi ini adalah untuk mengidentifikasi potensi risiko apabila perangkat pengguna dicuri, hilang, atau disusupi *malware* sehingga data pribadi tidak terekspos tanpa perlindungan.

d. *Dangerous Permissions*

Mengidentifikasi permintaan izin akses (*permissions*) oleh aplikasi yang tidak sesuai dengan kebutuhan fungsionalitas utama aplikasi. Tujuan dari pemeriksaan ini adalah untuk menilai sejauh mana aplikasi meminta akses terhadap sumber daya perangkat yang mengancam privasi pengguna.

e. SSL/TLS *Misconfiguration*

Menilai apakah aplikasi melakukan konfigurasi keamanan komunikasi yang benar terutama implementasi SSL/TLS. Tujuan dari deteksi ini adalah memastikan bahwa jalur komunikasi aplikasi dengan *server backend* sudah dienkripsi dan tervalidasi dengan benar untuk menjaga kerahasiaan dan integritas data yang ditransmisikan.

3. Pemetaan Kerentanan ke OWASP Mobile Top 10 2024

Setelah mendapatkan hasil pemindaian kerentanan dari MobSF, tahapan selanjutnya yaitu pemetaan kerentanan yang ditemukan ke dalam kategori OWASP Mobile Top 10 2024. OWASP Mobile Top 10 2024 merupakan daftar sepuluh risiko keamanan paling kritis pada aplikasi *mobile*

modern. Pemetaan dilakukan agar setiap kerentanan yang ditemukan dapat diklasifikasikan secara sistematis ke dalam kategori yang tepat. Pada tahap ini memetakan hasil temuan kerentanan ke kategori OWASP Mobile Top 10 2024, yaitu:

1. M1: *Improper Credential Usage*
2. M2: *Inadequate Supply Chain Security*
3. M3: *Insecure Authentication/Authorization*
4. M4: *Insufficient Input/Output Validation*
5. M5: *Insecure Communication*
6. M6: *Inadequate Privacy Controls*
7. M7: *Insufficient Binary Protections*
8. M8: *Security Misconfiguration*
9. M9: *Insecure Data Storage*
10. M10: *Insufficient Cryptography*

Pada tahap ini akan menyesuaikan masing-masing temuan pemindaian kerentanan dengan kategori risiko pada OWASP Mobile Top 10 2024, kemudian menyusun tabel pemetaan antara hasil temuan dan kategori OWASP Mobile Top 10 2024. Pemetaan kerentanan ini bertujuan untuk mengklasifikasikan kerentanan secara standar agar memudahkan dalam proses analisis risiko lebih lanjut dan penyusunan rekomendasi mitigasi.

4. Analisis Risiko Berdasarkan NIST SP 800-30

Pada tahap ini dilakukan penilaian risiko terhadap masing-masing kerentanan yang telah diidentifikasi. Analisis risiko dilakukan berdasarkan NIST SP 800-30 dengan menilai dua komponen utama yaitu *likehood* dan *impact* kemudian menentukan *risk level*.

a. *Likehood*

Menilai seberapa besar kemungkinan kerentanan tersebut dieksploitasi oleh pihak tidak bertanggungjawab. Skala yang digunakan yaitu *High, Medium*, dan *Low*.

b. *Impact*

Menilai seberapa besar dampak terhadap aset informasi jika kerentanan tersebut berhasil dieksploitasi. Skala yang digunakan yaitu *High, Medium*, dan *Low*.

c. *Risk Level*

Menentukan tingkat risiko dengan menggabungkan nilai *likehood* dan *impact* kemudian mengkategorikan tingkat risikonya dengan skala *Very High, High, Medium, Low,* dan *Very Low*.

Pengklasifikasian analisis risiko berdasarkan pada *framework* NIST SP 800-30 yang dapat dilihat pada Tabel 3.1 sebagai berikut:

Tabel 3. 1 Matriks analisis risiko berdasarkan NIST SP 800-30

Likehood	***Impact***	***Risk Level***
Very High	*Very High*	*Very High*
High	*Very High*	*Very High*
Medium	*Very High*	*High*
Low	*Very High*	*High*
Very Low	*Very High*	*Medium*
Very High	*High*	*Very High*
High	*High*	*High*
Medium	*High*	*High*
Low	*High*	*Medium*
Very Low	*High*	*Medium*
Very High	*Medium*	*High*
High	*Medium*	*High*
Medium	*Medium*	*Medium*
Low	*Medium*	*Medium*
Very Low	*Medium*	*Low*
Very High	*Low*	*High*

Likehood	***Impact***	***Risk Level***
High	*Low*	*Medium*
Medium	*Low*	*Medium*
Low	*Low*	*Low*
Very Low	*Low*	*Very Low*
Very High	*Very Low*	*Medium*
High	*Very Low*	*Medium*
Medium	*Very Low*	*Low*
Low	*Very Low*	*Low*
Very Low	*Very Low*	*Very Low*

Tahap ini bertujuan untuk mengetahui tingkat risiko dan memberikan pemahaman mendalam tentang prioritas penanganan terhadap kerentanan yang ditemukan.

5. Evaluasi Risiko

Tahap evaluasi risiko bertujuan untuk menilai dan mengklasifikasikan tingkat keseluruhan risiko keamanan informasi pada aplikasi *e-commerce* yang dianalisis. Pada tahap evaluasi risiko akan dilakukan dengan menggabungkan hasil analisis risiko per kerentanan berdasarkan NIST SP 800-30 dan *security score* dari setiap aplikasi yang dihasilkan dari MobSF. Penggabungan ini bertujuan untuk menghasilkan evaluasi risiko yang lebih komprehensif baik dari segi spesifik per kerentanan maupun dari sisi tingkat keamanan aplikasi secara umum.

Pertama hasil analisis risiko per kerentanan yang dihasilkan dengan menggunakan parameter *likehood* (kemungkinan eksploitasi) dan *impact* (dampak jika terkena eksploitasi) yang menghasilkan *risk level* dengan pengklasifikasian tingkat risiko dalam tingkat *Very High, High, Medium, Low,* dan *Very Low*. Selanjutnya akan menggunakan *security score* yang dihasilkan dari MobSF setelah proses pemindaian kerentanan secara analisis statis untuk memberikan gambaran lebih jelas mengenai keamanan aplikasi secara umum. *Security score* ini tidak menggantikan analisis risiko per

kerentanan melainkan digunakan untuk memvalidasi dan memperkuat hasil evaluasi risiko. Pengklasifikasian tingkat risiko berdasarkan *security score* akan menggunakan skala risiko berdasarkan NIST SP 800-30, yang ditunjukkan pada Tabel 3.2:

Tabel 3. 2 Skor risiko berdasarkan NIST SP 800-30

Skor (0-100)	**Kategori Risiko**	**Deskripsi**
0-25	*Very High*	Keamanan sangat lemah, celah kritis ditemukan
26-50	*High*	Masih ada banyak celah keamanan yang perlu diperbaiki
51-75	*Medium*	Keamanan cukup baik, tetapi masih ada potensi risiko
76-90	*Low*	Keamanan cukup kuat, namun masih ada ruang untuk perbaikan
91-100	*Very Low*	Aplikasi sangat aman, hampir tidak ada risiko

Matriks penilaian evaluasi risiko berdasarkan pada *framework* NIST SP 800-30 yang dapat dilihat pada Tabel 3.3 sebagai berikut:

Tabel 3. 3 Matriks penilaian evaluasi risiko

Risk Level	**Bobot Skor**
Very High	5
High	4
Medium	3
Low	2
Very Low	1

6. Rekomendasi Mitigasi

Setelah melakukan evaluasi risiko, tahap selanjutnya yaitu penyusunan rekomendasi mitigasi untuk setiap kerentanan. Rekomendasi mitigasi disusun berdasarkan prinsip keamanan informasi (*confidentiality, integrity, availability*), berbasis *best practices* keamanan aplikasi *mobile*, dan memberikan solusi sesuai kategori risiko yang tercantum dalam OWASP Mobile Top 10 2024. Setiap rekomendasi dirancang untuk memberikan solusi konkret yang dapat mengurangi tingkat risiko yang diidentifikasi melalui proses analisis sebelumnya. Pada tahap ini akan membuat daftar rekomendasi mitigasi teknis untuk masing-masing kerentanan untuk memberikan saran dalam memperbaiki kerentanan yang ditemukan dan mengurangi tingkat risiko keamanan.

7. Pelaporan

Tahap akhir dari penelitian yang dilakukan yaitu pelaporan. Pada tahap ini yaitu merangkum semua tahapan penelitian dengan menyajikan laporan hasil dari identifikasi aplikasi, pemindaian kerentanan dengan MobSF, pemetaan kerentanan ke OWASP Mobile Top 10 2024, analisis risiko berdasarkan NIST SP 800-30, evaluasi risiko, dan rekomendasi mitigasi yang akan disajikan dalam bentuk tabel dan grafik perbandingan

tingkat risiko keamanan setiap aplikasi yang dianalisis untuk memudahkan pemahaman. Laporan ini bertujuan sebagai referensi dan panduan praktis dalam meningkatkan keamanan aplikasi *e-commerce* di Indonesia bagi pengguna dan pengembang aplikasi.

3.2 Bahan dan Alat Penelitian

Bahan penelitian dalam penelitian ini menggunakan lima aplikasi *e-commerce* terpopuler di Indonesia yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak. Berikut detail versi aplikasi yang dianalisis:

a. Shopee : Versi 3.48.31
b. Tokopedia : Versi 3.309.0
c. Lazada : Versi 7.73.0
d. Blibli : Versi 12.2.0
e. Bukalapak : Versi 11.5.1

Lima aplikasi tersebut dipilih berdasarkan popularitas, jumlah pengguna aktif, dan cakupan pasar yang signifikan dalam sektor *e-commerce* di Indonesia. Aplikasi-aplikasi ini di unduh melalui Google Play Store dan di *install* di *smartphone* android. Aplikasi tersebut di *download* melalui Google Play Store untuk memastikan aplikasi yang akan dianalisis adalah versi resmi dan aman.

Penelitian ini menggunakan perangkat keras dan perangkat lunak. Alat utama dalam penelitian ini berupa komputer dan *smartphone* android dengan spesifikasi cukup baik untuk menjalankan berbagai sistem operasi. *Smartphone* android digunakan untuk mengunduh dan *install* aplikasi-aplikasi *e-commerce* yang akan dianalisis. Selain itu penelitian ini juga menggunakan perangkat lunak yang digunakan untuk melakukan pengujian dan analisis.

Dalam penelitian ini menggunakan komputer dengan sistem operasi:

1. Sistem Operasi: Windows 11 Pro
2. *Processor*: Intel(R) Celeron(R) N4020 CPU @ 1.10GHz 1.10 GHz
3. RAM: 8 GB
4. Penyimpanan: 256 GB
5. *System Type*: 64-bit *operating system*, x64-*based processor*

Dalam penelitian ini menggunakan *smartphone* android dengan sistem operasi:

1. Versi Android: 9.0
2. *Processor*: Delapan *Core*
3. RAM: 3 GB
4. Internal: 32 GB

Dalam penelitian ini menggunakan perangkat lunak atau *tools*:

1. Docker Desktop
2. *Mobile Security Framework* (MobSF)

   Untuk melakukan pemindaian kerentanan keamanan pada aplikasi-aplikasi *e-commerce* yang akan diuji.

3.3 Jalan Penelitian

Penelitian ini melakukan *risk assessment* pada aplikasi *e-commerce* di Indonesia berdasarkan NIST SP 800-30 dengan pendekatan analisis statis. Tahapan-tahapan dari penelitian yang dilakukan berdasarkan pada *National Institute of Standards and Technology* (NIST) SP 800-30 yang meliputi identifikasi aplikasi, pemindaian kerentanan dengan MobSF, pemetaan kerentanan ke OWASP Mobile Top 10 2024, analisis risiko berdasarkan NIST SP 800-30, evaluasi risiko, rekomendasi mitigasi, dan pelaporan. Adapun tahapan jalan penelitian yang akan dilakukan yaitu sebagai berikut:

1. **Identifikasi Aplikasi**

   Tahap awal ini dilakukan untuk mengidentifikasi aplikasi *e-commerce* yang akan dianalisis, yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak. Aplikasi diunduh dari Google Play Store, kemudian file APK diperoleh melalui proses *backup* dari perangkat android. Selanjutnya, dilakukan identifikasi terhadap aset informasi penting seperti info aplikasi, izin aplikasi, data pengguna, fitur keamanan, dan mekanisme autentikasi yang digunakan. Tujuan dari tahap ini adalah untuk mengetahui data lengkap aplikasi dan identifikasi awal potensi risiko.

2. Pemindaian Kerentanan dengan MobSF

Pada tahap ini, file APK dari masing-masing aplikasi dianalisis menggunakan *Mobile Security Framework* (MobSF) dengan pendekatan analisis statis. Pemindaian dilakukan terhadap struktur internal aplikasi seperti *permission*, penggunaan API, konfigurasi SSL/TLS, algoritma kriptografi, dan *source code*. Fokus utama kerentanan yang diidentifikasi meliputi *hardcoded secrets, weak cryptography, insecure data storage, dangerous permissions,* dan SSL/TLS *misconfiguration.*

3. Pemetaan Kerentanan ke OWASP Mobile Top 10 2024

Setelah pemindaian kerentanan, dilakukan pemetaan kerentanan ke dalam kategori OWASP Mobile Top 10 tahun 2024, seperti M1: *Improper Credential Usage*, M5: *Insecure Communication*, M9: *Insecure Data Storage*, dan sebagainya. Pemetaan ini bertujuan untuk mengklasifikasikan kerentanan secara standar dan memudahkan analisis risiko lebih lanjut.

4. Analisis Risiko Berdasarkan NIST SP 800-30

Pada tahap ini dilakukan untuk menentukan tingkat risiko dari setiap kerentanan yang ditemukan. Penilaian dilakukan dengan menilai komponen *likelihood* (kemungkinan eksploitasi) dan *impact* (dampak terhadap aset informasi), yang kemudian digabungkan untuk menentukan *risk level* (*very high, high, medium, low, very low*) menggunakan matriks risiko standar.

5. Evaluasi Risiko

Tahap evaluasi risiko dilakukan dengan menggabungkan hasil analisis risiko spesifik per kerentanan dan *security score* yang dihasilkan dari MobSF. *Security score* digunakan sebagai indikator tambahan tingkat keamanan aplikasi secara keseluruhan. Klasifikasi tingkat keamanan menggunakan skala risiko berbasis skor 0-100, dengan kategori dari *very high* hingga *very low*. Evaluasi ini bertujuan untuk menyusun prioritas mitigasi berdasarkan kombinasi kedua hasil tersebut.

6. Rekomendasi Mitigasi

Setelah melakukan evaluasi risiko, rekomendasi mitigasi disusun untuk setiap kerentanan yang ditemukan. Rekomendasi berbasis pada prinsip keamanan informasi (*confidentiality, integrity, availability*), *best practices* keamanan aplikasi mobile, serta mengacu pada kategori OWASP Mobile Top 10 2024. Setiap mitigasi bertujuan untuk mengurangi tingkat risiko dan memperbaiki keamanan aplikasi.

7. Pelaporan

Tahap terakhir adalah penyusunan laporan yang mencakup seluruh tahapan mulai dari identifikasi aplikasi, pemindaian kerentanan, pemetaan ke OWASP Mobile Top 10 2024, analisis risiko berdasarkan NIST SP 800-30, evaluasi risiko, hingga rekomendasi mitigasi. Laporan ini disajikan dalam bentuk tabel, grafik perbandingan tingkat risiko antar aplikasi, dan kesimpulan untuk menjadi referensi peningkatan keamanan aplikasi *e-commerce* di Indonesia.