ANALISIS KEAMANAN APLIKASI MOBILE DENPASAR PRAMA SEWAKA

S.F. Adiriyanto[1], I.G.A. Wibawa[2], dan G.A.V.M. Giri[3]

ABSTRAK

Denpasar Prama Sewaka merupakan sebuah aplikasi mobile yang menyatukan seluruh aplikasi mobile milik Pemerintah Kota Denpasar. Aplikasi mobile tersebut masih berada dalam tahap pengembangan, sehingga tentu masih memiliki banyak potensi kerentanan keamanan yang perlu diperhatikan. Hal ini umumnya dikarenakan oleh fokus utama yang terletak pada fungsionalitas dan pengembangan, bukan pada keamanan. Aplikasi yang sedang dalam tahap pengembangan cenderung memiliki kerentanan umum yang sering terjadi, seperti penyandian yang lemah, validasi input yang buruk, dan ketidakamanan pada sumber daya terkait jaringan. Dengan begitu, perlu dilakukan pengecekan kerentanan pada aplikasi mobile Denpasar Prama Sewaka demi menghindari risiko keamanan yang mungkin akan muncul. Dengan berfokus pada kemanan kode dan manifest dari aplikasi ini, akan digunakan MobSF pada Linux untuk melakukan pengecekannya.

Kata kunci : analisis keamanan, aplikasi mobile, Denpasar Prama Sewaka, pemerintah, kerentanan

ABSTRACT

Denpasar Prama Sewaka is a mobile application that integrates all the mobile applications owned by the Denpasar City Government. This mobile application is still in the development stage and, as such, it may have various security vulnerabilities that need to be addressed. This is typically due to the primary focus being on functionality and development rather than security. Mobile applications in the development phase tend to have common vulnerabilities that frequently occur, such as weak encryption, poor input validation, and insecurity related to network resources. Therefore, penetration testing of the Denpasar Prama Sewaka mobile application is essential to mitigate potential security risks. To prioritize the security of the code and manifest of this application, MobSF on Linux will be utilized to conduct the assessment.

Keywords: security analysis, mobile application, Denpasar Prama Sewaka, government, vulnerability

1. PENDAHULUAN

Teknologi yang semakin berkembang telah menghadirkan keuntungan besar, seperti akses mudah ke berbagai aplikasi dan website dari mana saja. Namun, bersama dengan kenyamanan ini, muncul pula tantangan serius dalam hal keamanan (Alanda, Satria, Mooduto & Kurniawan, 2019). Keberadaan kerentanan keamanan dalam aplikasi pemerintahan dapat memberikan peluang bagi penyerang untuk mengakses data sensitif dan bahkan mengganggu layanan publik. Keamanan aplikasi dari pemerintahan Kota Denpasar tentu merupakan aspek yang krusial dalam era digital ini. Pemerintah

[1] *Prodi Informatika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Udayana, shiennyflorensia@gmail.com*
[2] *Prodi Informatika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Udayana, gede.arta@unud.ac.id*
[3] *Prodi Informatika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Udayana, vida@unud.ac.id*
Submitted: 7 Oktober 2024 *Revised: 26 Oktober 2024* *Accepted: 26 Oktober 2024*

bertanggung jawab atas data pribadi warga, termasuk informasi sensitif seperti identitas dan keuangan (Katoch & Garg, 2023). Dengan ancaman serangan siber terus berkembang seperti peretasan, pencurian data, dan serangan lainnya, sangat perlu dilakukan pengujian kerentanan untuk mengidentifikasi dan mengatasi masalah sebelum menjadi serius (Alhamed & Rahman, 2023).

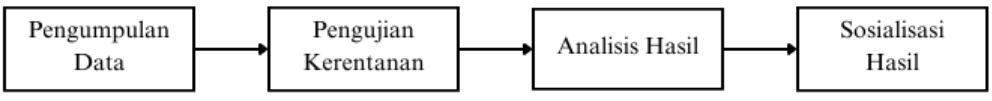
Denpasar Prama Sewaka yang sering disingkat dengan DPS merupakan sebuah aplikasi mobile yang menyatukan seluruh aplikasi mobile milik Pemerintah Kota Denpasar. Di dalam aplikasi ini juga ditambahkan fitur-fitur yang mempermudah respons aparatur pemerintah terhadap pengaduan online, portal web Denpasar, jelajah Denpasar, koordinasi online, dashboard data center, dan lainnya untuk kepentingan Masyarakat Kota Denpasar menuju Denpasar Smart City. Aplikasi mobile ini masih berada dalam tahap pengembangan, sehingga tentu masih memiliki banyak potensi kerentanan keamanan yang perlu diperhatikan (Bertoglio & Zorzo, 2017). Dengan begitu, perlu dilakukan analisis kerentanan pada aplikasi mobile Denpasar Prama Sewaka, terutama pada bagian kode serta manifest demi menghindari risiko keamanan yang mungkin akan muncul.

Analisis kode dan manifest dari sebuah aplikasi mobile sangat penting karena memberikan wawasan mendalam tentang kerentanan keamanan yang mungkin ada dalam aplikasi tersebut (Enck, Octeau, McDaniel & Chauduri, 2011). Kode sumber aplikasi mengandung instruksi dan logika yang menjalankan fungsionalitasnya, dan jika ada kelemahan dalam kode tersebut, penyerang dapat memanfaatkannya untuk mencuri data, meretas sistem, atau bahkan merusak integritas aplikasi. Selain itu, manifest aplikasi berisi informasi tentang izin yang diberikan oleh pengguna, akses jaringan, dan sumber daya lain yang dapat dimanfaatkan oleh aplikasi. Jika manifest tidak dikonfigurasi dengan benar, aplikasi dapat memiliki akses yang tidak perlu ke data atau layanan yang rentan terhadap serangan. Dengan menganalisis kode dan manifest, dapat diidentifikasi kerentanan potensial seperti validasi input yang lemah, kerentanan terhadap serangan SQL injection, penyandian yang buruk, dan masalah izin yang tidak terelakkan (Al-Delayel, 2022).

2. METODE PELAKSANAAN

Dalam pembuatan laporan ini, dilakukan pengecekan aplikasi mobile Denpasar Prama Sewaka dengan menggunakan MobSF. MobSF dengan kepanjangan *Mobile Security Framework* merupakan sebuah alat *open-source* yang dikembangkan untuk mengidentifikasi dan menganalisis kerentanan keamanan dalam aplikasi mobile, baik aplikasi Android maupun iOS (Isnaini & Suhartono, 2023). Alat penguji kerentanan aplikasi mobile ini mendukung berbagai macam fitur, seperti analisis kode sumber, pemindai berkas biner, analisis malware, dan banyak lagi, sehingga memudahkan pengguna dalam mengidentifikasi masalah potensial yang mungkin ada dalam aplikasi mobile (Anwar, Sumerli, Hady, Rahayu, & Kraugusteeliana, 2023).

Berdasarkan hal tersebut, langkah-langkah yang dilakukan dalam uji kerentanan aplikasi mobile Denpasar Prama Sewaka dapat dilihat pada **Gambar 2.1**. Berikut juga merupakan penjelasannya:



Gambar 2.1. Tahapan Uji Kerentanan Aplikasi Mobile Denpasar Prama Sewaka

a. Pengumpulan Data

Aplikasi mobile Denpasar Prama Sewaka akan diunduh terlebih dahulu untuk mendapatkan kode serta manifestnya. Selanjutnya adalah mempersiapkan segala alat yang dibutuhkan untuk melakukan uji kerentanan aplikasi tersebut, yaitu Kali Linux dan MobSF. MobSF ini

akan dijalankan dengan menggunakan Kali Linux 2023.2, versi kedua dari 2023 Kali Rolling yang dirilis pada tanggal 30 Mei 2023.

Kali Linux merupakan sebuah distribusi Linux yang dikhususkan untuk keperluan keamanan komputer dan uji penetrasi (Tambunan, Yuniati, & Setyoko, 2022). Distribusi Linux ini didesain dan dikembangkan oleh Offensive Security, sebuah perusahaan yang fokus pada pelatihan dan layanan keamanan siber. Kali Linux merupakan alat yang sangat populer di kalangan profesional keamanan siber, etika hacker, dan para peneliti keamanan.

b. Pengujian Kerentanan

Pada tahapan ini, akan dilakukan penginstallan dan pengkonfigurasian MobSF di dalam lingkungan Kali Linux. MobSF kemudian digunakan untuk melakukan analisis pada kode dan manifest dari aplikasi mobile Denpasar Prama Sewaka.

c. Analisis Hasil

Berdasarkan hasil yang didapatkan dari pengujian yang dilakukan, kerentanan yang ditemukan akan ditinjau secara rinci dan diklasifikasikan menjadi 3 tingkat, yaitu High, Warning, dan Info berdasarkan dampak dan keparahan kerentanan tersebut. Selanjutnya, akan diteliti pula cara untuk mengatasi kerentanan yang sudah ditemukan (Hanifurohman & Hutagalung, 2019).

d. Sosialisasi Hasil

Pada tahap ini, hasil analisis yang sudah didapatkan dan ditinjau akan dijelaskan kepada Kepala serta staff dari bidang yang berhubungan, yaitu Bidang Persandian Dinas Komunikasi, Informatika dan Statistik Kota Denpasar dengan harapan dapat membantu tim dalam meningkatkan keamanan aplikasi mobile Denpasar Prama Sewaka.

3. HASIL DAN PEMBAHASAN

Pada analisis kode, ditemukan sebanyak 5 kerentanan yang dibagi menjadi 1 high, 3 warning, dan 1 info. Penjelasan lebih lanjut mengenai kerentanan yang ditemukan dapat dilihat pada Tabel 3.1.

Tabel 3.1. Hasil Analisis Kode Aplikasi Denpasar Prama Sewaka beserta Sarannya

Tingkat	Isu	Standar	Saran
High	Aplikasi menggunakan mode enkripsi CBC dengan padding PKCS5/PKCS7. Konfigurasi ini rentan terhadap serangan padding oracle	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	• Identifikasi dan ubah algoritma kriptografi yang tidak aman • Tambahkan integritas checking • Ikuti pedoman keamanan
Warning	Berkas dapat mengandung informasi sensitif yang di-hardcode seperti username, password, dll.	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	• Enkripsi data • Hindari penyimpanan data teks terbuka • Pembersihan data setelah penggunaan • Penggunaan keamanan OS

	Aplikasi dapat membaca/menulis ke penyimpanan eksternal. Aplikasi lain dapat membaca data yang ditulis ke penyimpanan eksternal	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage	• Gunakan internal storage, file permissions, dan direktori khusus aplikasi • Gunakan content providers • Batasi akses izin • Gunakan encrypted database
	Aplikasi menggunakan generator angka acak yang tidak aman	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	• Penggunaan dan pembaruan pustaka kriptografi • Penggunaan SecureRandom • Pengujian kualitas keacakan • Gunakan entropi yang memadai
Info	Aplikasi mencatat informasi. Informasi sensitif seharusnya tidak pernah dicatat	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	• Penghapusan informasi sensitif • Pengaturan level logging yang sesuai • Gunakan pustaka log kustom • Enkripsi log • Pemeriksaan manual logging

Adapun pada analisis manifest ditemukan 9 kerentanan dengan 4 high dan 5 medium. Penjelasan beserta saran dari kerentanan-kerentanan yang ditemukan ini dapat dilihat pada Tabel 3.2.

Tabel 3.2. Hasil Analisis Manifest Aplikasi Denpasar Prama Sewaka beserta Sarannya

Tingkat	**Isu**	**Deskripsi**	**Saran**
High	Clear text traffic diaktifkan untuk Aplikasi [android:usesCleartextTraffic=true]	Aplikasi menggunakan jaringan cleartext traffic seperti cleartext HTTP, FTP stacks, DownloadManager, dsb.	• Gunakan HTTPS • Nonaktifkan cleartext traffic • Periksa penggunaan pustaka • Gunakan penandatanganan SSL/TLS
	Broadcast Receiver (androidx.media.session.MediaButtonReceiver) tidak terlindungi. [android:exported=true]	Terdapat Penerima Siaran dibagikan dengan aplikasi lain sehingga dapat diakses oleh aplikasi lain di perangkat.	• Tetapkan android:exported ke "false" • Gunakan permission protection level • Lakukan uji pustaka pihak ketiga • Pemantauan keamanan secara berkala • Pantau aktivitas aplikasi lainnya
	Aktivitas (com.google.firebase.auth.internal.GenericIdpActivity) tidak terlindungi. [android:exported=true]	Terdapat aktivitas yang dibagikan dengan aplikasi lain sehingga dapat diakses oleh aplikasi lain di perangkat.	
	Aktivitas (com.google.firebase.auth.internal.RecaptchaActivity) tidak terlindungi. [android:exported=true]		
Warning	Aplikasi dapat diinstal pada versi Android yang rentan [minSdk=23]	Aplikasi dapat diinstal pada Android versi lama yang memiliki beberapa kerentanan yang belum diperbaiki	• Tingkatkan minSdkVersion • Perbarui dependensi pustaka • Nonaktifkan dukungan versi rendah
	Broadcast Receiver (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) yang	Terdapat Penerima Siaran dibagikan dengan aplikasi lain sehingga dapat diakses oleh aplikasi lain	• Periksa izin dan tingkat perlindungannya

	seharusnya diperiksa dilindungi oleh izin	di perangkat. Ia dilindungi oleh izin yang tidak didefinisikan dalam aplikasi yang dianalisis	• Atur tingkat perlindungan yang sesuai • Nonaktifkan Exported • Gunakan izin yang sesuai • Pemantauan keamanan secara berkala • Pantau aktivitas aplikasi lainnya
	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) yang seharusnya diperiksa dilindungi oleh izin		
	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) yang seharusnya diperiksa dilindungi oleh izin		
	Layanan (com.google.android.gms.auth.api.signin.RevocationBoundService) yang seharusnya diperiksa dilindungi oleh izin	Terdapat layanan yang dibagikan dengan aplikasi lain sehingga dapat diakses oleh aplikasi lain di perangkat. Ia dilindungi oleh izin yang tidak didefinisikan dalam aplikasi yang dianalisis	

Dilaksanakan pula sosialisasi untuk memaparkan hasil analisis keamanan dari aplikasi ini di hadapan Kepala serta staff dari Bidang Persandian Dinas Komunikasi, Informatika dan Statistik Kota Denpasar yang dapat dilihat pada **Gambar 3.1**.

Gambar 3.1. Sosialisasi Hasil Pengecekan Aplikasi Mobile Denpasar Prama Sewaka

4. KESIMPULAN

Melalui analisis keamanan yang sudah dilaksanakan, ditemukan total sebanyak 14 kerentanan pada kode serta manifest yang digunakan di aplikasi mobile Denpasar Prama Sewaka. Pada analisis kode, kerentanan yang ditemukan sebanyak 1 high, 3 warning, dan 1 info, sedangkan pada analisis manifest ditemukan kerentanan sebanyak 4 high dan 5 medium. Hal ini tentu sangat perlu untuk segera ditindaklanjuti supaya tidak terjadi kebocoran informasi ke pihak-pihak luar. Melalui saran-saran yang sudah diberikan, kiranya masalah kerentanan ini dapat diselesaikan dengan baik.

UCAPAN TERIMA KASIH

Ucapan terima kasih disampaikan kepada Universitas Udayana, khususnya Program Studi Informatika, atas kesempatan yang diberikan dalam menjalani program Praktik Kerja Lapangan. Terima kasih juga kepada Kepala Dinas KOMINFO Kota Denpasar dan Kepala serta staff Bidang Persandian KOMINFO Kota Denpasar atas izin yang diberikan untuk melaksanakan kegiatan PKL di kantor pemerintahan Kota Denpasar ini. Tidak kalah pentingnya, terima kasih kepada Dosen Pembimbing yang selalu bersedia memberikan dukungan dan bimbingan pada kegiatan PKL ini. Dengan semua kontribusi dan dukungan yang diberikan, kegiatan PKL terlaksana dengan baik dan sesuai rencana.

DAFTAR PUSTAKA

Al-Delayel, S.A. (2022). Security Analysis of Mobile Banking Application in Qatar. *arXiv.* pp. 1-7.

Alanda, A., Satria D., Mooduto, H.A. and Kurniawan B. (2019). Mobile Application Security Penetration Testing Based on OWASP. IOP Conf. **Vol. 846**, pp. 1-11.

Alhamed, M. and Rahman, M.M.H. (2023). A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. *Appl. Sci*. **Vol. 13,** pp. 3-4.

Anwar, C., Sumerli, C.H., Hady, S., Rahayu, N. and Kraugusteeliana K. (2023). The Application of Mobile Security Framework (MOBSF) and Mobile A pplication Security Testing Guide to Ensure the Security in Mobile Commerce Applications. *Jurnal Sistim Informasi dan Teknologi*. **Vol. 5**, pp. 97-100.

Bertoglio, D.D. and Zorzo, A.F. (2017). Overview and open issues on penetration test. *Journal of the Brazilian Computer*. **Vol. 23,** pp. 1-16.

Enck, W., Octeau, D., McDaniel, P. and Chauduri, S. (2011). A Study of Android Application Security. Pp. 1-17.

Hanifurohman, C. and Hutagalung, D.D. (2019). ANALISA KEAMANAN APLIKASI MOBILE E-COMMERCE BERBASIS ANDROID MENGGUNAKAN MOBILE SECURITY FRAMEWORK. *PROSIDING SEMINAR NASIONAL*. **Vol. 1**.

Isnaini, K.N. and Suhartono, D. (2023). Security Analysis of Simpel Desa using Mobile Security Framework and ISO 27002:2013. *INTENSIF*. **Vol.7,** pp-84-90.

Katoch, S. and Garg, V. (2023). Security Analysis on Android Application Through Penetration Testing using Reverse Engineering. *2023 3rd International Conference on Smart Data Intelligence (ICSMDI)*. pp. 216-222.

Tambunan, A.R., Yuniati T. and Setyoko, Y.A. (2022). Implementasi Static Analysis Dan Background Process Untuk Mendeteksi Malware Pada Aplikasi Android Dengan Mobile Security Framework. LEDGER. **Vol. 1,** pp 1-4.