BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil analisis keamanan aplikasi Jogja Istimewa (JOGIS) menggunakan Mobile Security Framework (MobSF) berbasis Docker, dapat disimpulkan bahwa aplikasi JOGIS memiliki tingkat keamanan pada kategori menengah (medium). Hasil analisis statis menunjukkan bahwa struktur aplikasi telah tersusun dengan baik, namun masih ditemukan beberapa kelemahan pada aspek konfigurasi keamanan, penggunaan permission, serta implementasi kode yang berpotensi menimbulkan risiko keamanan apabila tidak dilakukan perbaikan. Analisis statis menggunakan MobSF berhasil mengidentifikasi sejumlah temuan keamanan dengan tingkat risiko low, medium, dan high, dengan dominasi temuan berada pada kategori medium. Temuan tersebut meliputi penggunaan *weak cryptography*, *raw SQL query*, penyimpanan pada *external storage*, penggunaan *temporary file*, serta beberapa konfigurasi aplikasi yang masih dapat ditingkatkan. Berdasarkan hasil tersebut, dapat disimpulkan bahwa aplikasi belum berada pada kondisi kritis, namun masih memerlukan peningkatan pada beberapa aspek keamanan untuk mengurangi potensi eksploitasi dan kebocoran data.

Berdasarkan evaluasi terhadap OWASP Mobile Top 10, sebagian temuan berkaitan dengan kategori kerentanan seperti *Insufficient Cryptography*, *Client Code Quality*, dan *Insecure Data Storage*. Sementara itu, evaluasi berdasarkan OWASP MASVS Privacy menunjukkan bahwa penggunaan permission sensitif pada aplikasi umumnya telah mendukung kebutuhan fungsional aplikasi, namun tetap perlu menerapkan prinsip *least privilege* agar risiko terhadap privasi pengguna dapat diminimalkan. Secara keseluruhan, penggunaan MobSF berbasis Docker terbukti mampu mendukung proses analisis keamanan aplikasi Android secara terstruktur dan menghasilkan informasi awal mengenai kondisi keamanan aplikasi JOGIS. Hasil penelitian ini diharapkan dapat menjadi acuan bagi pengembang dalam melakukan evaluasi dan peningkatan keamanan aplikasi sehingga perlindungan terhadap data pengguna maupun layanan yang disediakan dapat ditingkatkan.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran yang dapat diberikan sebagai berikut:

a. Bagi Pengembang Aplikasi

Pengembang disarankan untuk melakukan evaluasi terhadap konfigurasi aplikasi, khususnya pada bagian *AndroidManifest.xml*, serta memastikan bahwa fitur yang berpotensi membuka celah keamanan telah dikonfigurasi dengan tepat. Selain itu, pengelolaan *permission* perlu diperhatikan agar tidak memberikan akses berlebih yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.

b. Peningkatan Keamanan Sistem

Perlu dilakukan peningkatan pada aspek keamanan, seperti penerapan enkripsi data, pengamanan komunikasi jaringan, serta penggunaan metode autentikasi yang lebih kuat untuk melindungi data pengguna dari potensi kebocoran.

c. Pengujian Keamanan Lanjutan

Penelitian selanjutnya disarankan untuk menggunakan kombinasi tools yang lebih variatif, sebagai pembanding agar hasil evaluasi keamanan dapat di ukur dari berbagai macam aspek dan sudut pandang.

d. Bagi Instansi Terkait

Instansi pemerintah atau pihak terkait dapat mempertimbangkan penerapan proses evaluasi keamanan aplikasi secara berkala dan mempublikasikannya sebelum aplikasi didistribusikan kepada masyarakat, guna memastikan bahwa standar keamanan telah terpenuhi dan masyarakat tidak risau data nya tersebar.

e. Pengembangan Penelitian Selanjutnya

Penelitian selanjutnya dapat mengembangkan teknik pengujian keamanan dengan menambahkan pendekatan lain sesuai kebutuhan penelitian sehingga hasil evaluasi keamanan aplikasi dapat menjadi lebih beragam dan mendalam.

5.3 Keterbatasan Penelitian

Penelitian ini memiliki beberapa keterbatasan salah satu nya penelitian hanya menggunakan metode analisis statis dengan bantuan Mobile Security Framework (MobSF), sehingga hasil yang diperoleh terbatas pada informasi yang dapat diidentifikasi dari struktur dan konfigurasi aplikasi tanpa mengamati perilaku aplikasi saat dijalankan. Kedua, objek penelitian hanya berfokus pada aplikasi Jogja Istimewa (JOGIS), sehingga hasil penelitian tidak dapat digeneralisasikan untuk seluruh aplikasi layanan publik berbasis Android. Ketiga, penelitian dilakukan berdasarkan berkas APK yang tersedia pada saat pengujian, sehingga hasil analisis dapat berubah apabila terdapat pembaruan atau perubahan pada versi aplikasi di masa mendatang. Penelitian ini juga tidak melakukan pengujian terhadap sisi server maupun infrastruktur backend yang digunakan oleh aplikasi, sehingga ruang lingkup analisis hanya terbatas pada keamanan aplikasi Android dari sisi klien (client-side).

5.4 Saran Untuk Penelitian Selanjutnya

Penelitian selanjutnya dapat memperluas ruang lingkup analisis dengan menerapkan metode pengujian keamanan yang berbeda atau menggunakan kombinasi beberapa tools analisis keamanan aplikasi Android sebagai pembanding agar mendapat sudut pandang yang berbeda. Penelitian juga dapat dilakukan pada objek yang lebih beragam, seperti aplikasi layanan publik dari instansi lain maupun aplikasi dengan karakteristik yang berbeda sehingga diperoleh gambaran yang lebih luas mengenai kondisi keamanan aplikasi Android.

Penggunaan tools keamanan lainnya sebagai pembanding juga dapat dilakukan untuk meningkatkan validitas hasil analisis. Penelitian berikutnya juga dapat mengkaji aspek keamanan pada sisi server atau backend yang berinteraksi dengan aplikasi sehingga evaluasi keamanan dapat dilakukan secara lebih menyeluruh. Dengan demikian, hasil penelitian yang diperoleh diharapkan dapat memberikan gambaran yang lebih lengkap mengenai keamanan aplikasi mobile dan layanan digital yang mendukungnya.

DAFTAR PUSTAKA

[1] Hidayatullah, “DETEKSI MALWARE ANDROID MENGGUNAKAN METODE CONVOLUTIONAL NEURAL NETWORK (CNN) SKRIPSI,” 2024.

[2] K. Alfalqi, R. Alghamdi, and M. Waqdan, “Android Platform Malware Analysis,” vol. 6, no. 1, pp. 140–146, 2015.

[3] A. Sakti and D. C. Arifin, “Analisis Malware pada Perangkat Android Menggunakan Tools Mobsf (Mobile Security Framework) terhadap berbagai aspek kehidupan manusia , termasuk dalam hal komunikasi , transaksi untuk merusak , mencuri data , atau mendapatkan akses tidak sah terhadap pe,” pp. 263–270, 2025.

[4] A. Cahya, F. Nugraha, R. N. Yasa, B. Siber, and P. Siber, “Perbandingan Keamanan Aplikasi Pesan Instan Android Menggunakan MobSF (Mobile Security Framework) Berdasarkan Beberapa Standar,” 2022.

[5] Y. Dwi *et al.*, “Analisis Malware Menggunakan Metode Analisis Statis dan Dinamis untuk Pembuatan IOC Berdasarkan STIX Versi 2 . 1,” no. 1, 2017.

[6] F. Nugraha, “Analisis Mitigasi Keamanan Aplikasi Mobile menggunakan Metode Statis dan Dinamis pada MobSF Security Mitigation Analysis of Mobile Application Using Static and Dynamic Methods with MobSF,” vol. 15, pp. 583–598, 2026.

[7] T. B. Subakja, M. Fronita, and T. K. Ahsyar, “Analisis perbandingan keamanan aplikasi transportasi online berbasis android menggunakan mobile security framework (mobsf),” vol. 10, no. 2, pp. 1823–1837, 2025.

[8] F. P. E. Putra, U. Ubaidi, A. Hamzah, W. A. Pramadi, and A. Nuraini, “Systematic Literature Review: Security Gap Detection On Websites Using Owasp Zap,” *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 348–355, 2024, doi: 10.47709/brilliance.v4i1.4227.

[9] S. Alam, “Application Security Testing to Support Digital-Based Cultural Ecosystem in Jogja Smart Province,” *J. Pengabdi. Kpd. Masy. (Indonesian J. Community Engag.*, vol. 9, no. 3, p. 158, 2023, doi: 10.22146/jpkm.80089.

[10] R. (2024) Campbell, “Efektivitas Aplikasi Jogja Istimewa dalam Pelayanan Publik di Daerah Istimewa Yogyakarta,” *J. Mhs. Wacana Publik*, *4(1), 15–23.*, vol. 1, no.

Tugas Akhir Program Studi Sistem Informasi
Universitas Atma Jaya Yogyakarta

1, pp. 1689–1699, 2016, [Online]. Available: http://www.biblioteca.pucminas.br/teses/Educacao_PereiraAS_1.pdf%0Ahttp://www.anpocs.org.br/portal/publicacoes/rbcs_00_11/rbcs11_01.htm%0Ahttp://repositorio.ipea.gov.br/bitstream/11058/7845/1/td_2306.pdf%0Ahttps://direitoufma2010.files.wordpress.com/2010/

[11] E. Tansen and D. W. Nurdiarto, "ANALISIS DAN DETEKSI MALWARE DENGAN METODE HYBRID ANALYSIS MENGGUNAKAN FRAMEWORK MOBSF," vol. 4, no. 2, pp. 191–201, 2020.

[12] M. N. Khoiroh, S. Santosa, M. Ramli, and D. E. Estiningsih, "Pengaruh Penggunaan Media Statis-Dinamis pada Sistem Reproduksi Manusia terhadap Penguasaan Konsep Siswa The Effect Static and Dynamic Media on Human Reproductive System to Student Conceptual Understanding," vol. 14, no. 2008, pp. 449–454, 2015.

[13] I. Himawan *et al.*, "APLIKASI APK DENGAN METODE STATIC ANALYSIS," vol. 02, no. 02, pp. 122–127, 2022.

[14] M. I. Karuniawan, "Penerapan Analisis Dinamis Untuk Pengujian Aplikasi Sia Umj Mobile," 2016.

[15] O. S. Adebayo, "Improved Malware Detection Model with Apriori Association Rule and Particle Swarm Optimization," vol. 2019, 2019, doi: 10.1155/2019/2850932.

[16] M. N. Maajid *et al.*, "MEMBANGUN SISTEM DETEKSI MALWARE MENGGUNAKAN MALICE PADA," vol. 7, no. 6, pp. 2842–2845, 2021.

[17] A. and A. Iman, Anandika Nur, Budiyono, "ANALISIS MALWARE PADA SISTEM OPERASI ANDROID MENGGUNAKAN PERMISSION-BASED MALWARE," vol. 6, no. 2, pp. 7845–7851, 2019.

[18] R. B. Hadiprakoso, N. Qomariasih, N. Yasa, R. Kriptografi, and P. Siber, "IDENTIFIKASI MALWARE ANDROID MENGGUNAKAN PENDEKATAN ANALISIS HIBRID DENGAN DEEP LEARNING," pp. 77–84, 2021.

[19] R. Hidayat, N. F., and Ferdiana, "The Development of Mobile Client Application in Yogyakarta Tourism and Culinary Information System Based on Social Media Integration. International Journal of Advanced Computer Science & Applications," *Maj. Geogr. Indones.*, vol. 3, no. 10, pp. 71–75, 2012.

Tugas Akhir Program Studi Sistem Informasi
Universitas Atma Jaya Yogyakarta

[20] D. Priyawati, S. Rokhmah, and I. C. Utomo, “Website Vulnerability Testing and Analysis of Internet Management Information System Using OWASP,” *Int. J. Comput. Inf. Syst. Peer Rev. J.*, vol. 3, no. 3, pp. 143–147, 2022, doi: 10.29040/ijcis.v3i3.90.

[21] R. Budiarto Hadiprakoso, W. Rendra Aditya, F. Nevia Pramitha, and P. Siber dan Sandi Negara, “Statistical Analysis of Android Malware Detection Using Supervised Machine Learning Algorithm,” *CyberSecurity Digit. Forensics*, vol. 5, no. 1, pp. 2–5, 2022.

[22] L. Li, “Static Analysis of Android Apps : A Systematic Literature Review,” 2017.

[23] B. B. Rad, H. J. Bhatti, and M. Ahmadi, “An Introduction to Docker and Analysis of its Performance,” *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 17, no. 3, pp. 1–9, 2017, [Online]. Available: https://www.researchgate.net/publication/318816158

[24] M. B. Imtias, K. Umam, H. Mustofa, and M. H. Subowo, “Comparative Analysis of Penetration Testing Frameworks: OWASP, PTES, and NIST SP 800-115 for Detecting Web Application Vulnerabilities,” *J. Appl. Informatics Comput.*, vol. 9, no. 6, pp. 3689–3696, 2025, doi: 10.30871/jaic.v9i6.9846.

[25] M. Bach-Nutman, “Understanding The Top 10 OWASP Vulnerabilities,” 2020, [Online]. Available: http://arxiv.org/abs/2012.09960

[26] I. M. Almomani and A. Al Khayer, “A Comprehensive Analysis of the Android Permissions System,” *IEEE Access*, vol. 8, pp. 216671–216688, 2020, doi: 10.1109/ACCESS.2020.3041432.

[27] K. W. Y. Au, Y. F. Zhou, Z. Huang, and D. Lie, “PScout: Analyzing the Android Permission Specification,” pp. 217–228, 2012, doi: 10.1145/2382196.2382222.

[28] Y. M. Tashtoush, A. Alsmadi, A. Al-abdi, N. Ababneh, and O. Almousa, “An Analysis of Android Web App Manifest,” *Jordan Univ. Sci. Technol.*, no. November, 2018.

[29] S. Malik and K. Khatter, “Behaviour analysis of android application,” *Int. J. Control Theory Appl.*, vol. 9, no. Specialissue11, pp. 5307–5322, 2016.

[30] F. Spoto, “Static Analysis of Android Programs,” 2012.

[31] J. Willemsen, “OWASP M a s v s,” pp. 1–35.

LAMPIRAN

No	Peran	Dosen	Revisi	Status	Halaman
1	Pembimbing 1	Emanuel Ristian Handoyo, S.T., M.Eng.	Perbaiki penomoran tabel agar konsisten antara daftar tabel, caption, dan isi naskah.	Sudah	ix; 29–53
2	Pembimbing 1	Emanuel Ristian Handoyo, S.T., M.Eng.	Pastikan setiap tabel dan gambar dibahas atau dirujuk pada paragraf sebelum/sesudahnya.	Sudah	29–53
3	Pembimbing 1	Emanuel Ristian Handoyo, S.T., M.Eng.	Perbaiki kalimat yang mengandung overclaim, seperti pernyataan "analisis statis lebih superior", serta cek seluruh naskah agar tidak ada klaim yang berlebihan.	Sudah	27
4	Pembimbing 1	Emanuel Ristian Handoyo, S.T., M.Eng.	Revisi judul menjadi "Analisis Keamanan Aplikasi Smart Province Menggunakan Framework OWASP MASVS-PRIVACY" (sesuai arahan).	Sudah	Sampul; i; ii
5	Pembimbing 2	Aloysius Bagas Pradipta Irianto, S.Kom., M.Eng., Ph.D.	Selesaikan seluruh revisi yang diberikan oleh dosen penguji.	Sudah	i–61
6	Penguji 2	Rangga Perwiratama, S.T., M.Kom.	Alihkan fokus pembahasan ke konteks e-Government/Smart Province atau integrasikan pembahasan MASVS-PRIVACY dan MobSF sebagai evaluasi keamanan yang lebih komprehensif.	Sudah	1–3
7	Penguji 2	Rangga Perwiratama, S.T., M.Kom.	Hilangkan klaim bahwa Static Analysis lebih superior dibanding Dynamic Analysis, karena keduanya memiliki tujuan yang berbeda.	Sudah	27
8	Penguji 2	Rangga Perwiratama, S.T., M.Kom.	Tambahkan proses verifikasi manual terhadap hasil MobSF, misalnya melalui dekompilasi kode, screenshot hasil analisis, atau pembahasan manual terhadap temuan.	Sudah	40
9	Penguji 3	Paulus Mudjihartono, S.T., M.T., Ph.D.	Ganti logo Universitas sesuai logo resmi UAJY.	Sudah	Sampul

10	Penguji 3	Paulus Mudjihartono, S.T., M.T., Ph.D.	Hapus tanda kurung pada judul skripsi.	Sudah	Sampul; i; ii
11	Penguji 3	Paulus Mudjihartono, S.T., M.T., Ph.D.	Perbaiki keyword menjadi "Analisis Statik APK", bukan "Analisis APK".	Sudah	iii
12	Penguji 3	Paulus Mudjihartono, S.T., M.T., Ph.D.	Periksa kembali konsistensi daftar tabel dengan nomor dan caption tabel pada isi naskah.	Sudah	ix; 29–53
13	Penguji 3	Paulus Mudjihartono, S.T., M.T., Ph.D.	Pastikan seluruh gambar dirujuk pada isi naskah dan tidak ada gambar yang langsung muncul setelah subbab tanpa penjelasan.	Sudah	29–53
14	Penguji 3	Paulus Mudjihartono, S.T., M.T., Ph.D.	Perbaiki format paragraf agar seluruh paragraf menggunakan indentasi yang konsisten.	Sudah	1–61
15	Penguji 3	Paulus Mudjihartono, S.T., M.T., Ph.D.	Tambahkan referensi yang mendukung bahwa penggunaan Static Analysis sudah memadai untuk ruang lingkup penelitian.	Sudah	27
16	Penguji 3	Paulus Mudjihartono, S.T., M.T., Ph.D.	Tambahkan penjelasan pada naskah mengenai asal-usul dan interpretasi Security Score 51/100 yang diperoleh dari MobSF.	Sudah	42