Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.3 (Agustus 2023)

STATIC ANALYSIS USING MOBILE SECURITY FRAMEWORK FOR SMART HOME APPLIANCES

Rahman Abdillah[1], Andreas Adi Trinoto[2], Imam Himawan[3]

Program Studi Teknik Informatika,
Fakultas Teknik dan Ilmu Komputer
Universitas Indraprasta PGRI

rabdil.bu@gmail.com[1], a.trinoto@gmail.com[2],
imamhimawann@gmail.com[3]

Received: June 18 , 2023**. Revised:** July 18, 2023**. Accepted:** July 22, 2023**. . Issue Period:** Vol.7 No.3 (2023), Pp.760-765

Abstrak: Kerentanan keamanan yang terdapat pada aplikasi android dapat menjadi ancaman yang digunakan oleh hacker atau cracker untuk mencuri informasi pribadi yang terekam di smartphone. Aplikasi smart home adalah aplikasi yang menyimpan informasi pribadi beberapa pemilik yang akan berbahaya jika data dan informasi tersebut dicuri oleh orang yang tidak bertanggung jawab. Penelitian ini bertujuan untuk melakukan analisis statis terhadap keamanan empat aplikasi smart home yang umum digunakan. Alat yang digunakan adalah Mobile security framework (MobSF). Mobile security framework (MobSF) adalah salah satu alat yang dapat digunakan untuk menguji keamanan aplikasi, baik pengujian statis maupun dinamis. Hasil analisis keamanan menggunakan MobSF diharapkan dapat memberikan manfaat baik bagi pengembang aplikasi maupun pengguna aplikasi. Bagi pengembang aplikasi dapat dijadikan sebagai saran untuk terus meningkatkan aspek keamanan dan dari sisi pengguna aplikasi dapat mengetahui resiko keamanan dari setiap aplikasi smart home yang digunakan dan dapat memilih dengan bijak aplikasi mana yang memiliki tingkat keamanan yang lebih tinggi. Penelitian ini menggunakan metodologi pemeringkatan risiko OWASP untuk menganalisis dan mengukur tingkat keamanan dalam sebuah skor.

Kata kunci : Smart Home, MobSF, security pen-testing, OWASP.

Abstract: *Security vulnerabilities contained in the android application can be a threat used by hackers or crackers to steal personal information recorded on smartphones. Smart home applications are applications that store several owners' personal information which will be dangerous if this data and information are stolen by irresponsible people. This study aims to conduct a static analysis of the security of four commonly used smart home applications. The tools used are Mobile security framework (MobSF). Mobile security framework (MobSF) is one of the tools that can be used to test application security, both static and dynamic tests. The results of the security analysis using MobSF are expected to provide benefits for both application developers and application users. For application developers, it can be used as a suggestion to continue to improve the security aspect and from the user side of the application, they can be aware of the security risks for each smart home application used and can choose wisely which application has a higher security level. This study used OWASP risk rating methodology to analyze and measure security level in a score.*

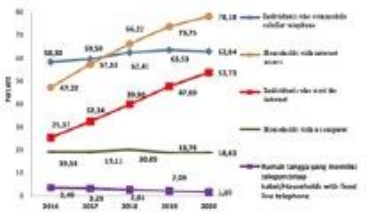
DOI: 10.52362/jisamar.v7i3.1161
Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional.

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.3 (Agustus 2023)

Keywords *: Smart Home, MobSF, security pen-testing, OWASP*

I. PENDAHULUAN

Badan Pusat Statistik merilis data penggunaan Teknologi Informasi dan Komunikasi (TIK) di Indonesia tahun 2020 yang mengalami perkembangan pesat. Perkembangan indikator TIK yang paling pesat adalah penggunaan internet di rumah tangga yang mencapai 78,18 persen, yang juga diikuti dengan peningkatan pengguna telepon seluler yang mencapai 62,84 persen [1].



Gambar 1. Tren Indikator TIK di Indonesia, 2016-2020 [1].

Pengguna internet di Indonesia setiap tahun mengalami peningkatan yang signifikan, yang juga terjadi pada tingkat penggunaan perangkat smartphone. Aplikasi smartphone telah banyak digunakan dalam berbagai aspek kehidupan, seperti ekonomi, pendidikan, sosial, hiburan, dll. Hal ini juga terjadi pada penggunaan smartphone untuk implementasi dalam rumah tangga. Beberapa perangkat keras rumah tangga dapat diatur dan dikontrol menggunakan aplikasi dari smartphone. Aplikasi menjadi bagian integral dari peralatan rumah tangga pintar. Pengguna dapat mengontrol perangkat keras itu dari smartphone mereka. Selain itu, dengan perilaku pengguna saat ini, hingga berbagai keunggulan dan fleksibilitas yang terkandung dalam penggunaan teknologi, juga menimbulkan kekhawatiran akan keamanan penggunaan aplikasi tersebut. Hal ini berdampak positif pada beberapa sektor peralatan rumah tangga pintar dan juga memicu munculnya berbagai keamanan aplikasi mobile, khususnya pada platform android. Oleh karena itu, perlu dilakukan analisis keamanan aplikasi dengan melakukan pengujian dan pengukuran tingkat keamanan aplikasi.

Meningkatnya akses teknologi informasi dan penggunaan smartphone secara langsung dipengaruhi oleh banyaknya migrasi layanan dan kebutuhan yang mendukung aktivitas kehidupan sehari-hari seperti komunikasi, navigasi, konsumsi media, hiburan, keuangan, kesehatan di smartphone. Rumah pintar adalah sebuah sistem yang digunakan untuk mengintegrasikan berbagai perangkat keras yang umumnya terdapat di sebuah rumah, antara lain penggunaan teknologi komputer, kontrol, komunikasi antar perangkat, dan pengelolaan perangkat melalui jaringan [2]. Salah satu website yang menghitung penggunaan berbagai jenis sistem operasi seluler yang digunakan di seluruh dunia, yaitu Global Stats, menyebutkan bahwa periode November 2020 hingga November 2021, terdapat 57,21% pengguna perangkat seluler yang menggunakan sistem operasi Android di Indonesia [3]. Hal ini tentu saja membuat aplikasi android menjadi sasaran utama para penjahat internet seperti hacker dan cracker. Sebagian besar aplikasi android digunakan oleh pengguna di seluruh dunia, tidak semua telah melewati proses pengujian keamanan dengan baik sesuai ISO/2700 [4]. Keamanan aplikasi seluler adalah area yang memerlukan pengujian dan penelitian terus-menerus untuk meningkatkan privasi dan keamanan data pengguna. Sebagian besar pengguna memiliki sangat sedikit atau tidak memiliki pengetahuan tentang aspek keamanan smartphone mereka. Kesalahan dan celah dapat ditemukan kapan saja dan jika tim pengembangan aplikasi tidak mengetahui kerentanan baru yang dapat merusak reputasi aplikasi dan yang terpenting data pengguna yang menggunakan aplikasi.

Tujuan dari penelitian ini adalah untuk meningkatkan pemahaman pengguna home smart terhadap celah keamanan pada aplikasi mobile smart home dan memberikan metode untuk melakukan analisis statis menggunakan Mobile Security Framework (MobSF) untuk melakukan pengujian keamanan aplikasi mobile smart home berbasis android. Analisis statis diimplementasikan dengan menganalisis Skor CVSS, Skor Keamanan, Deteksi Pelacak, dan Penyematan Sertifikat SSL. Metode yang digunakan dalam melakukan analisis

DOI: 10.52362/jisamar.v7i3.1161
Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional.

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.3 (Agustus 2023)

adalah Mobile Security Framework (MobSF) yang menggunakan model risiko OWASP. Penilaian model risiko keamanan ini memberikan tiga tingkat kemungkinan dan dampak, yaitu: rendah, tinggi, dan sedang. Kerentanan keamanan yang terdapat pada aplikasi dapat digunakan oleh penyerang untuk mencuri informasi penting pada smartphone, padahal informasi merupakan aset penting dan sangat berharga yang disajikan dalam berbagai format: catatan, verbal, elektronik, pos, dan audio-visual. Dalam beberapa penelitian yang telah dipublikasikan, belum ada penelitian yang menganalisis celah keamanan yang terdapat dalam aplikasi pintar rumahan yang banyak digunakan di Indonesia.

II. RELATED WORK

Penelitian yang dilakukan berjudul "Membangun Sistem Pengujian Keamanan Aplikasi Android Menggunakan MobSF". Penelitian dilatarbelakangi banyaknya aplikasi yang disusupi oleh malware yang dapat menyebabkan kerusakan pada ponsel bahkan pencurian data pribadi pemilik yang tersimpan di ponsel. Hasil yang didapat dari file yang dianalisis berbeda-beda, tergantung sampel, metode analisis dan alat yang digunakan [5]. Penelitian yang dilakukan tentang Pengujian Keamanan Aplikasi Tracer Covid Berbasis Android, pada penelitian ini menggunakan MobSF dan drozer untuk memeriksa risiko dalam kode (analisis statis) dan menentukan permukaan serangan potensial pada empat aplikasi pelacakan Covid-19. Pengamatan dan temuan disusun dalam bentuk tabel, termasuk 10 masalah seluler teratas OWASP, serta CWE yang terdeteksi menggunakan MobSF. Permukaan serangan potensial terdeteksi menggunakan drozer[6].

Kajian yang dilakukan dengan judul Mobile Forensic Logical Extraction Pada Aplikasi Android E-Commerce, penelitian ini dilatarbelakangi oleh kurangnya pemahaman pengguna aplikasi tentang resiko izin akses yang diminta oleh aplikasi sebelum atau sesudah instalasi, membuat celah keamanan data pengguna untuk mengakses fitur pada perangkat smartphone seperti kamera, media penyimpanan, kontak, akun dan fitur lainnya. Berdasarkan temuan celah keamanan tersebut, disimpulkan bahwa aplikasi e-commerce yang digunakan oleh penggunanya mungkin juga mengandung malware atau virus serupa yang berpeluang mengambil data pribadi pengguna [7].

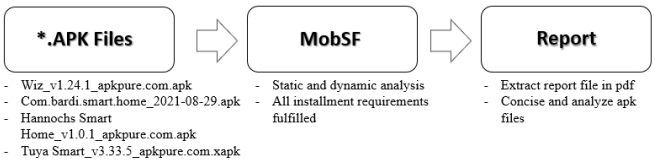
III. METODE

Sesuai dengan metode yang digunakan, hanya ada kebutuhan untuk perangkat lunak apk untuk melakukan analisis keamanan. Perangkat lunak yang dibutuhkan adalah Git, Python 3.8-3.9, JDK 8, Microsoft Visual C++ Build Tools, OpenSSL (non-light), wkhtmltopdf [8]. Dalam tulisan ini, penulis menggunakan aplikasi open source yang biasa digunakan untuk melakukan pengujian penetrasi aplikasi mobile. Oleh karena itu langkah ini dilakukan dengan melakukan instalasi sesuai dengan dokumentasi yang sudah terdapat pada paket source code aplikasi MobSF seperti pada Gambar 1.

Jalankan instalasi MobSF di Windows menggunakan perintah ini:

```
git clone https ://github.com/MobSF/Mobile-Security-Framework_MobSF.git
cd Mobile-Security-Framework-MobSF
```

setup.bat

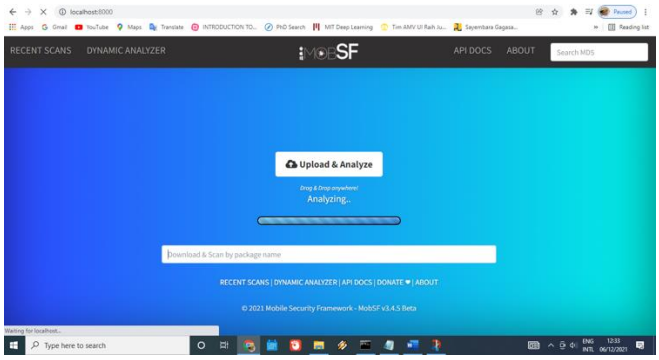


Gambar 2. Metodologi Penelitian

Jalankan aplikasi MobSF di Windows menggunakan perintah: run.bat 127.0.0.1:8000, lalu di web browser buka http://localhost:8000/

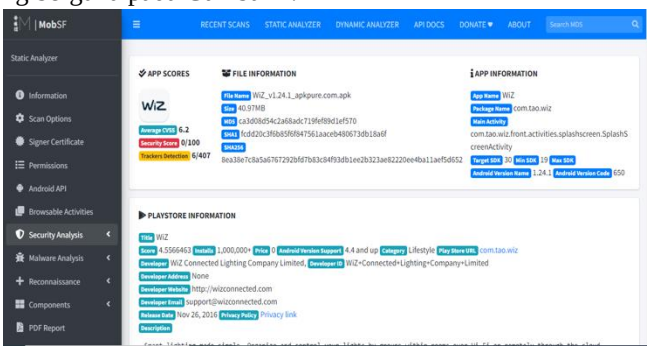
DOI: 10.52362/jisamar.v7i3.1161
Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional.

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.3 (Agustus 2023)



Gambar 3. Layar Beranda MobSF

Seperti yang dapat kita lihat dari Gambar 3, MobSF siap digunakan untuk menganalisis file apk dengan mode analisis statis. Selanjutnya, pengguna perlu menyeret dan melepaskan file apk ke Layar Beranda MobSF. Setelah file apk dijatuhkan dan dianalisis, halaman dengan hasil analisis akan muncul. Ada menu di sisi kiri yang memungkinkan pengguna untuk menavigasi halaman dengan cepat (hasilnya cukup banyak). Berikut adalah informasi yang berguna pada Gambar 4.



Gambar 4. Hasil analisis Wiz

IV. PEMBAHASAN DAN HASIL

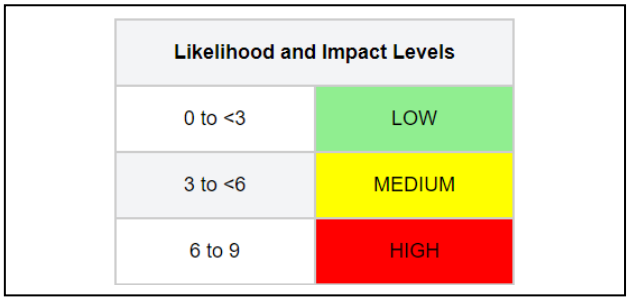
Berdasarkan aplikasi smart home, kami mengulas 4 aplikasi yang sudah banyak digunakan. Berdasarkan metodologi pemeringkatan risiko OWASP, pendekatan OWASP disajikan berdasarkan metodologi standar dengan menggunakan mode risiko standar [8] :

Risk = Likelihood x Impact

Ada 6 langkah pendekatan untuk analisis risiko, yaitu langkah 1: Mengidentifikasi risiko, langkah 2: faktor untuk memperkirakan kemungkinan, langkah 3: faktor untuk memperkirakan dampak, langkah 4: menentukan tingkat keparahan risiko, langkah 5: memutuskan apa yang harus diperbaiki, dan langkah 6: menyesuaikan model peringkat risiko Anda.

DOI: 10.52362/jisamar.v7i3.1161
Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional.

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.3 (Agustus 2023)



Gambar 5. Model risiko OWASP Tingkat Kemungkinan dan Dampak

Dari keempat aplikasi smart home tersebut, kami memiliki kesimpulan sebagai berikut:

Tabel 1. HASIL HOME SMART APPS

	CVSS Score	Security Score	Tracker Detection	SSL Certificate Pinning
Wiz_v1.24.1_apkpure.com.apk	6,2	0/100	6/407	Secure
com.bardi.smart.home_2021-08-29.apk	6,5	10/100	4/407	Secure
Hannochs Smart Home_v1.0.1_apkpure.com.apk	6,5	10/100	4/407	Secure
Tuya Smart_v3.33.5_apkpure.com.xapk	6,5	10/100	1/407	Secure

1. *CVSS Score* (Panduan Pengujian OWASP)
   Sistem Penilaian Kerentanan Umum (CVSS). Pelaporan data uji keamanan mencakup informasi berikut. CVSS menyediakan cara untuk menangkap karakteristik utama kerentanan dan menghasilkan skor numerik yang mencerminkan tingkat keparahannya. Kerentanan skor CVSS berdasarkan 11 metrik berbeda yang disusun menjadi tiga kelompok terpisah: Metrik Skor Dasar, Metrik Skor Lingkungan, dan Metrik Skor Temporal.
2. Security Score
   Skor Keamanan MobSF adalah sistem penilaian kerangka kerja itu sendiri yang menentukan elemen mana dari aplikasi yang dipindai yang dianggap rentan oleh pemindai MobSF. Implementasi WebView yang tidak aman, eksekusi kode yang dikontrol pengguna di WebView adalah lubang keamanan kritis (Hannochs).
3. Trackers Detection
   Subbagian ini melaporkan pelacak pihak ketiga yang dapat digunakan oleh setiap aplikasi. MobSF menggunakan open source Exodus-Privacy webapp untuk menganalisis pelacak yang terdeteksi di APK aplikasi [9]. Aplikasi Tuya hanya memiliki analitik google firebase sebagai analitik pelacak, sedangkan Bardi dan Hannochs memiliki Facebook Analytics, Facebook Login, Facebook Share, dan Google Firebase Analytics sebagai pelacak. Aplikasi Wiz memiliki enam pelacak.
4. SSL Certificate Pinning
   Penyematan Sertifikat adalah lapisan keamanan tambahan untuk melindungi dari serangan man-in-the-middle. Ini memastikan bahwa hanya Otoritas Sertifikat (CA) bersertifikat yang dapat menandatangani sertifikat untuk domain aplikasi, dan bukan CA mana pun di penyimpanan sertifikat [10]. Pengembang

DOI: 10.52362/jisamar.v7i3.1161
Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional.

aplikasi menerapkan Penyematan Sertifikat untuk menghindari rekayasa balik, yang memungkinkan pengembang untuk menentukan sertifikat mana yang diizinkan oleh aplikasi. Alih-alih mengandalkan toko sertifikat. Implementasi SSL yang tidak aman. Mempercayai semua sertifikat atau menerima sertifikat yang ditandatangani sendiri merupakan Lubang Keamanan yang penting. Sebaliknya, aplikasi Hannochs rentan terhadap serangan MITM dibandingkan dengan tiga aplikasi rumah pintar lainnya.

V. KESIMPULAN

Studi ini berhasil menghasilkan hasil pengujian keamanan dari Mobile security framework. MobSF dapat membuat laporan yang menyimpulkan bahwa empat aplikasi pintar rumahan memiliki beberapa lubang kerentanan. Studi ini mengimplementasikan analisis keamanan dalam tahap analisis statis yang merupakan tahap pertama dalam analisis keamanan kerangka kerja keamanan seluler. Biasanya, pengujian keamanan mengimplementasikan analisis statis dan dinamis baik sebagai tandem. Hasilnya perlu dibandingkan dengan metode analitik lain berdasarkan standar verifikasi keamanan aplikasi seluler OWASP untuk pengujian komprehensif. Kerangka kerja keamanan seluler menggunakan standar dalam metodologi OWASP Mobile Security. Kemungkinan dan Tingkat Dampak menggunakan model risiko OWASP menggunakan pengujian komprehensif yang mencakup proses, teknik, dan alat yang digunakan untuk pengujian keamanan aplikasi seluler. Selain itu masih perlu dilakukan penelitian lebih lanjut dengan menggunakan analisis dinamik untuk mendapatkan hasil yang lengkap.

REFERENASI

[1] B.-S. Indonesia, “Telecommunication statistics in Indonesia, 2020. BPS-Statistics Indonesia.” 2021.
[2] M. Li, W. Gu, W. Chen, Y. He, Y. Wu, and Y. Zhang, “Smart home: architecture, technologies and systems,” *Procedia Comput Sci*, vol. 131, pp. 393–400, 2018.
[3] Statcounter, “Mobile Operating System Market Share ,” *https://gs.statcounter.com/android-version-market-share/mobile-tablet/indonesia (accessed December. 06, 2021)*, 2021.
[4] A. A. Putra, O. D. Nurhayati, and I. P. Windasari, “Perencanaan dan Implementasi Information Security Management System Menggunakan Framework ISO/IEC 20071,” *Jurnal Teknologi dan Sistem Komputer*, vol. 4, no. 1, pp. 60–66, 2016.
[5] A. Kartono, A. Sularsa, and S. J. I. Ismail, “Membangun Sistem Pengujian Keamanan Aplikasi Android Menggunakan Mobsf,” *eProceedings of Applied Science*, vol. 5, no. 1, 2019.
[6] N. Kohli and M. Mohaghegh, “Security Testing Of Android Based Covid Tracer Applications,” in *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, IEEE, 2020, pp. 1–6.
[7] N. Anwar, S. A. Akbar, A. Azhari, and I. Suryanto, “Ekstraksi Logis Forensik Mobile pada Aplikasi E-Commerce Android,” 2020.
[8] B. T. K. Dewi and M. A. Setiawan, “Kajian Literatur: Metode dan Tools Pengujian Celah Keamanan Aplikasi Berbasis Web,” *AUTOMATA*, vol. 3, no. 1, 2022.
[9] V. Kouliaridis, G. Kambourakis, E. Chatzoglou, D. Geneiatakis, and H. Wang, “Dissecting contact tracing apps in the Android platform,” *PLoS One*, vol. 16, no. 5, p. e0251867, 2021.
[10] K. E. CİBALIK and C. Koçak, “Detection of SSL/TLS Implementation Errors in Android Applications,” *Gazi University Journal of Science Part C: Design and Technology*, vol. 9, no. 2, pp. 211–219, 2021.

DOI: 10.52362/jisamar.v7i3.1161
Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional.