Jurnal Teknik Informatika (JUTIF)
Vol. 4, No. 6, Desember 2023, pp. 1327-1338
DOI: https://doi.org/10.52436/1.jutif.2023.4.6.1064
p-ISSN: 2723-3863
e-ISSN: 2723-3871

DESIGN OF A SECURITY VETTING FRAMEWORK FOR MOBILE SPBE APPLICATIONS BASED ON THE ANDROID OPERATING SYSTEM

Yopie Maulana Syahrizal[*1], Muhammad Salman[2]

[1,2]Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Indonesia
Email: [1]yopie.maulana@ui.ac.id, [2]muhammad.salman@ui.ac.id

(Article received: May 25, 2023; Revision: June 04, 2023; published: Desember 23, 2023)

Abstract

The increasing number of mobile device users in Indonesia has encouraged the government to utilize mobile applications as an SPBE service function. The mobile SPBE application is a form of SPBE service in the form of application that can be operated on a mobile device. The mobile SPBE application can of course provide benefits to its users, however, there are security risks that need to be anticipated. So through BSSN Regulation Number 4 of 2021 it is mandated that every government agency must implement SPBE security and identify security requirements that have not been implemented in the mobile SPBE application. So the security vetting framework becomes important and necessary to identify and validate security requirements that have not been implemented. However, there is currently no such framework. Therefore, in this research, a framework design was proposed for vetting the security of the mobile SPBE application based on the Android operating system. The design of the security vetting framework adopts NIST SP 800-163r1 which is integrated with application security testing using automated tools and manual testing. Manual testing was carried out according to the OWASP MASTG standard taking into account API security testing based on OWASP API Security. Then the results of application security testing are used to validate the mobile SPBE application security requirements. Based on the simulation results of the framework design on a sample SPBE mobile ABC application owned by a local government in Indonesia, violations were found against several mobile SPBE application security requirements. Then based on the simulation results, the framework design can validate all mobile SPBE application security requirements and is expected to be a reference for government agencies to carry out security vetting for mobile SPBE applications.

Keywords: *Framework, mobile, NIST SP 800-163r1, security, SPBE application.*

PERANCANGAN KERANGKA KERJA PEMERIKSAAN KEAMANAN PADA APLIKASI SPBE *MOBILE* BERBASIS SISTEM OPERASI *ANDROID*

Abstrak

Meningkatnya jumlah pengguna perangkat *mobile* di Indonesia mendorong pemerintah untuk memanfaatkan aplikasi *mobile* sebagai fungsi layanan SPBE. Aplikasi SPBE *mobile* merupakan salah satu bentuk layanan SPBE berupa aplikasi yang berjalan pada perangkat *mobile*. Aplikasi SPBE *mobile* tentunya dapat memberikan manfaat bagi penggunanya, namun terdapat risiko keamanan yang perlu diantisipasi. Maka melalui Peraturan BSSN Nomor 4 Tahun 2021 diamanatkan bahwa setiap instansi pemerintah harus menerapkan keamanan SPBE dan mengidentifikasi persyaratan keamanan yang belum diterapkan pada aplikasi SPBE *mobile.* Sehingga kerangka kerja pemeriksaan keamanan aplikasi SPBE *mobile* menjadi penting dan diperlukan untuk mengidentifikasi dan memvalidasi persyaratan keamanan yang belum diterapkan. Namun saat ini belum terdapat kerangka kerja tersebut. Oleh karena itu, pada penelitian ini dikembangkan sebuah rancangan kerangka kerja untuk melakukan pemeriksaan keamanan pada aplikasi SPBE *mobile* berbasis sistem operasi android. Rancangan kerangka kerja pemeriksaan keamanan dengan mengadopsi dari *NIST SP 800-163r1* yang diintegrasikan dengan pengujian keamanan aplikasi menggunakan *tool* otomatis dan pengujian secara manual. Pengujian manual dillakukan berdasarkan standar *OWASP MASTG* dengan mempertimbangkan pengujian keamanan *API* berdasarkan *OWASP API Security*. Kemudian hasil pengujian keamanan aplikasi digunakan untuk memvalidasi persyaratan keamanan aplikasi SPBE *mobile.* Berdasarkan hasil simulasi rancangan kerangka kerja pada sampel aplikasi SPBE *mobile* ABC milik salah satu pemerintah daerah di Indonesia, ditemukan pelanggaran terhadap beberapa persyaratan keamanan aplikasi SPBE *mobile.* Kemudian berdasarkan hasil simulasi, rancangan kerangka kerja tersebut dapat memvalidasi semua persyaratan keamanan aplikasi SPBE *mobile* dan diharapkan dapat menjadi referensi bagi instansi pemerintah untuk melakukan pemeriksaan keamanan aplikasi SPBE *mobile*.

Kata kunci: *Aplikasi SPBE, kerangka kerja, keamanan, mobile, NIST SP 800-163r1*.

1. PENDAHULUAN

Saat ini teknologi memberikan peranan penting bagi masyarakat dalam menjalankan aktivitas sehari-hari. Salah satu tren teknologi yang sedang diminati masyarakat saat ini adalah perangkat *mobile*. Berdasarkan data *Statista* [1] bahwa jumlah pengguna *smartphone* di Indonesia diperkirakan mencapai 210,77 juta pengguna pada tahun 2021 dan diperkirakan terus meningkat hingga tahun 2025 [2].

Dengan adanya perangkat *mobile* tentunya dapat memberikan kemudahan kepada masyarakat untuk memenuhi kebutuhan sehari-hari seperti bebelanja *online*, mememesan makanan *online*, melakukan transaksi perbankan dan lain-lain. Bahkan pemerintah Indonesia dalam penyelenggaraan pemerintahan juga memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan pemerintahan kepada masyarakat yang disebut layanan SPBE (Sistem Pemerintahan Berbasis Elektronik) dan salah satu layanan SPBE yang memanfaatkan perangkat *mobile* adalah aplikasi SPBE berbasis *mobile* sebagaimana tercantum dalam Peraturan Presiden Nomor 95 Tahun 2018 tentang SPBE [3].

Namun dibalik kemudahan dan manfaat-manfaat yang dirasakan masyarakat tentunya terdapat risiko keamanan yang perlu diantisipasi ketika menggunakan aplikasi *mobile*. Menurut laporan dari *NowSecure.com* yang berjudul "*High-Tech Mobile Apps Expose Data*" pada tahun 2023 mengungkapkan bahwa ratusan aplikasi *mobile* berteknologi tinggi memiliki kerentanan keamaman dan privasi. Diantaranya 99% aplikasi teknologi tinggi miliki minimal 1 atau lebih risiko keamanan, 86% aplikasi berteknologi tinggi menggunakan izin yang berbahaya (*dangerous permission*) dan 42% aplikasi berteknologi tinggi menggunakan kriptografi yang lemah [4].

Kerentanan keamanan pada aplikasi *mobile* dapat disalahgunakan oleh penyerang seperti pengungkapan data sensitif, penyalahgunaan hak akses dan lain-lain. Untuk mengantisipasi kemungkinan adanya kerentanan dan untuk menjamin keamanan aplikasi SPBE, Pemerintah melalui Peraturan Badan Siber dan Sandi Negara (BSSN) Nomor 4 Tahun 2021 mengamanatkan bahwa setiap instansi pusat dan pemerintah daerah harus menerapkan keamanan SPBE yang memenuhi standar teknis dan prosedur keamanan SPBE.

Selain itu peraturan tersebut juga mengamanatkan bahwa instansi pusat dan pemerintah daerah harus mengidentifikasi persyaratan keamanan yang belum diterapkan pada aplikasi SPBE [5]. Sehingga kerangka kerja untuk mengetahuhi sejauh mana persyaratan keamanan SPBE diterapkan pada aplikasi SPBE menjadi penting dan dibutuhkan oleh instansi pusat dan pemerintah daerah. Namun saat ini belum terdapat kerangka kerja tersebut. Oleh karena itu, suatu kerangka kerja pemeriksaan keamanan aplikasi SPBE diperlukan oleh instansi pusat dan pemeritah daerah untuk mengidentifikasi dan memvalidasi persyaratan keamanan aplikasi SPBE yang belum diterapkan. Proses pemeriksaan keamanan aplikasi SPBE bertujuan untuk memastikan bahwa aplikasi SPBE memenuhi persyaratan keamanan aplikasi SPBE sesuai Peraturan BSSN Nomor 4 Tahun 2021.

Beberapa penelitian telah dilakukan berkaitan dengan penelitian ini yaitu diantaranya membahas mengenai analisis penilaian kerentanan pada aplikasi *mobile* yang menyediakan layanan *e-governance* di Pemerintah Madhya Pradesh [6], perancangan kerangka kerja penilaian keamanan dan privasi pada aplikasi telemedicine di Indonesia [7], perancangan sistem validasi keamanan berdasarkan *OWASP Top 10 mobile* 2014 untuk memverifikasi persyaratan keamanan yang berlaku di Pemerintah Taiwan [8] dan analisis kerentanan pada aplikasi *mobile parental control* berdasarkan persyaratan keamanan *OWASP* [9]. Namun beberapa penelitian tersebut [8] hanya berfokus pada validasi persyaratan keamanan secara otomatis sehingga beberapa persyaratan keamanan tidak dapat dilakukan validasi dan persyaratan keamanan yang digunakan tidak berkaitan dengan persyaratan keamanan aplikasi SPBE *mobile.* Selain itu standar *OWASP mobile top 10* yang digunakan dalam penelitian bukan yang termutakhir.

Berdasarkan latar belakang tersebut, pada penelitian ini dikembangkan rancangan kerangka kerja pemeriksaan keamanan aplikasi SPBE untuk memvalidasi penerapan standar keamanan aplikasi SPBE. Adapun aplikasi SPBE yang menjadi target pemeriksaan dalam perancangan kerangka kerja ini adalah aplikasi SPBE *mobile* berbasis sistem operasi *android*. Aplikasi SPBE berbasis *mobile* merupakan aplikasi yang dapat berjalan pada perangkat *mobile* [5]. Aplikasi *mobile* berbasis sistem operasi *android* dipilih dengan mempertimbangkan data dari Statista bahwa jumlah pengguna sistem operasi *android* mendominasi di Indonesia yaitu sekitar 89.79% dibandingkan dengan sistem operasi *iOS* sekitar 10,12% [10]. Selain itu, jumlah unduh aplikasi *mobile* di seluruh dunia terus meningkat setiap tahunnya hingga tahun 2022 mencapai 255 milyar aplikasi mobile telah diunduh [11].

Proses perancangan kerangka kerja pemeriksaan keamanan mengadopsi dari tahapan umum pada *NIST Spesial Publication 800-163r1* yang diintegrasikan dengan pengujian keamanan aplikasi menggunakan *tool* otomatis dan pengujian keamanan aplikasi secara manual, serta hasil temuan kerentanan dianalisis dengan pendekatan risiko *OWASP Mobile Top 10* [12] dan penghitungan tingkat *severity* berdasarkan *Common Vulnerability Scoring System* (CVSS) 3.1

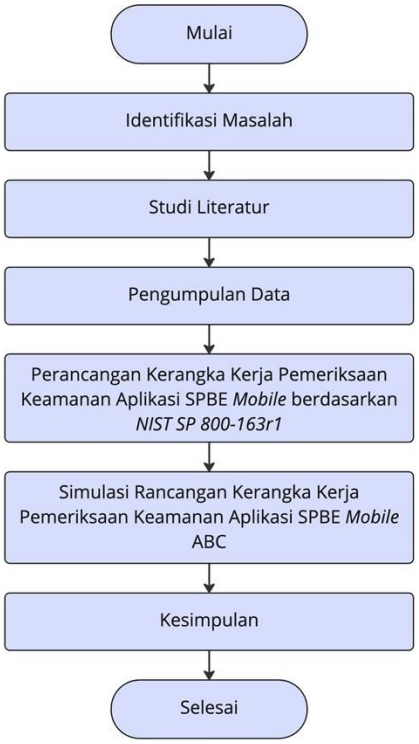
[13]. Untuk *tool* otomatis menggunakan *open source* dengan pendekatan metode analisis statik yang dipilih berdasarkan hasil evaluasi penilaian *tool* otomatis yang memenuhi kriteria penilaian yang telah ditentukan. Untuk pengujian keamanan aplikasi secara manual menggunakan pendekatan metode analisis statis dan dinamis berdasarkan standar prosedur pengujian keamanan aplikasi *mobile OWASP MASTG (Mobile Application Testing Guide*) [14] dengan mempertimbangkan pengujian keamanan API berdasarkan *OWASP API Security* [15]. Selanjutnya dilakukan proses validasi terhadap persyaratan keamanan untuk memastikan aplikasi memenuhi persyaratan keamanan aplikasi SPBE *mobile* dan menentukan apakah aplikasi SPBE *mobile* disetujui atau ditolak untuk diterapkan pada perangkat *mobile* organisasi. Hasil Penelitian ini diharapkan dapat menjadi rujukan bagi instansi pusat maupun pemerintah daerah dalam mendukung validasi penerapan standar keamanan aplikasi SPBE berbasis *mobile*.

2. METODE PENELITIAN

Penelitian pada paper ini dilakukan dalam 6 (enam) tahapan yaitu tahap identifikasi permasalahan, kemudian melakukan studi literatur, melakukan pengumpulan data, melakukan perancangan kerangka kerja dan melakukan tahapan simulasi rancangan kerangka kerja serta menyusun kesimpulan.

Adapun tahapan penelitian ditunjukan pada gambar 1 dengan deskripsi kegiatan untuk setiap tahapan sebagai berikut:

1. Melakukan identifikasi permasalahan
   Proses identifikasi permasalahan dilakukan untuk menentukan latar belakang penelitian. Pada penelitian ini, permasalahan yang berhasil teridentifikasi adalah perlu adanya kerangka kerja pemeriksaan keamanan aplikasi SPBE *mobile* untuk memvalidasi penerapan standar keamanan aplikasi SPBE *mobile* sesuai Peraturan BSSN Nomor 4 Tahun 2021.
2. Melakukan studi literatur
   Pada tahap ini dilakukan studi literatur dengan mengumpulkan data pustaka terkait metode-metode pemeriksaan keamanan aplikasi *mobile* berbasis sistem operasi *android* untuk memvalidasi persyaratan keamanan yang ditentukan oleh suatu standar atau regulasi tertentu.
3. Pengumpulan data
   Pada tahapan ini dilakukan proses pengumpulan data dengan sumber dari karya tulis ilmiah, standar atau peraturan yang terkait dengan persyaratan keamanan aplikasi SPBE *mobile*, perancangan kerangka kerja pemeriksaan keamanan aplikasi SPBE *mobile* dan pengujian keamanan aplikasi *mobile* serta standar lainnya yang berkaitan.



Gambar 1. Tahapan Penelitian

4. Perancangan Kerangka Kerja Pemeriksaan Keamanan Aplikasi SPBE *Mobile*
   Pada tahap ini dilakukan perancangan kerangka kerja pemeriksaan keamanan aplikasi SPBE *mobile* berdasarkan tahapan umum standar *NIST SP 800-163r1* tentang panduan pemeriksaan keamanan aplikasi *mobile*. Adapun dalam perancangan kerangka kerja pemeriksaan aplikasi *mobile* perlu menentukan beberapa hal meliputi:
   a. Menentukan persyaratan keamanan aplikasi SPBE *mobile*
   b. Menentukan metode dan *tool* pengujian aplikasi SPBE *mobile*
   c. Menentukan kriteria persetujuan/ penolakan aplikasi SPBE *mobile*
5. Simulasi rancangan kerangka kerja
   Pada tahap ini dilakukan simulasi hasil rancangan kerja pemeriksaan keamanan pada aplikasi SPBE *mobile* ABC yang dikelola salah satu pemerintah daerah di Indonesia.
6. Kesimpulan merupakah hasil perancangan kerangka kerja dan hasil simulasi rancangan kerangka kerja pemeriksaan keamanan aplikasi SPBE *mobile*.

2.1. Peraturan BSSN Nomor 4 Tahun 2021

Peraturan BSSN Nomor 4 tahun 2021 merupakan standar teknis dan prosedur keamanan SPBE sebagai pedoman bagi instansi pusat maupun pemerintah daerah untuk melakukan penerapan keamanan aplikasi SPBE. Standar teknis keamanan aplikasi SPBE berbasis *mobile* berdasarkan peraturan ini terdiri atas terpenuhinya fungsi penyimpanan data

dan persyaratan privasi, kriptografi, autentikasi dan manajemen sesi, komunikasi jaringan, interaksi *platform*, kualitas kode dan pengaturan *build* dan ketahanan [5].

Untuk memenuhi fungsi-fungsi tersebut dijabarkan dalam bentuk prosedur-prosedur yang terdiri dari fungsi penyimpanan data dan persyaratan privasi sebanyak 5 (lima) prosedur, fungsi kriptografi sebanyak 5 (lima) prosedur, fungsi autentikasi dan manajemen sesi sebanyak 8 (delapan) prosedur, fungsi komunikasi jaringan sebanyak 2 (dua) prosedur, fungsi interaksi platform sebanyak 6 (enam) prosedur, fungsi kualitas kode dan pengaturan *build* sebanyak 8 (delapan) prosedur, dan fungsi ketahanan sebanyak 9 (sembilan) prosedur. Secara keseluruhan terdiri dari 43 (empat puluh tiga) prosedur untuk standar keamanan aplikasi SPBE berbasis *mobile*.

2.2. Standar *NIST Special Publication 800-163r1*

Salah satu standar yang dirilis oleh *NIST* pada tahun 2019 adalah *NIST SP 800-163r1: Vetting the Security of Mobile Applications*. *NIST SP 800-163r1* merupakan sebuah standar yang menjelaskan proses pemeriksaan aplikasi dan memberikan panduan tentang merencanakan dan mengimplementasikan proses pemeriksaan aplikasi, mengembangkan persyaratan keamanan untuk aplikasi *mobile*, mengidentifikasi *tools* yang sesuai untuk menguji aplikasi *mobile*, dan menentukan apakah aplikasi *mobile* dapat diterima untuk diterapkan di perangkat *mobile* organisasi. Berikut ini adalah tahapan proses pemeriksaan aplikasi *mobile* berdasarkan *NIST SP 800-163r1* [16]:

a. *App Intake*
Pada tahap ini aplikasi diterima dari *developer* (pengembang) untuk dianalisis. Selanjutnya dilakukan pencatatan berkaitan dengan informasi mengenai aplikasi seperti nama aplikasi, versi aplikasi termasuk informasi pengembang, waktu dan informasi relevan lainnya yang diperlukan untuk proses pemeriksaan aplikasi.

b. *App Testing*
Pada tahap ini dilakukan proses pengujian keamanan aplikasi berdasarkan metode dan alat uji yang telah ditentukan. Setelah dilakukan pengujian, maka perlu dibuat laporan yang mengidentifikasi setiap kerentanan aplikasi yang terdeteksi dan menyertakan skor yang memperkirakan kemungkinan bahwa kerentanan dapat dieksploitasi dan dampak yang mungkin ditimbulkan oleh kerentanan yang terdeteksi pada aplikasi.

c. *Approval/Rejection*
Pada tahap ini dilakukan evaluasi persyaratan keamanan aplikasi dengan memeriksa hasil pengujian aplikasi untuk memastikan bahwa aplikasi memenuhi semua persyaratan keamanan aplikasi. Selanjutnya menyusun rekomendasi untuk menyetujui atau menolak aplikasi untuk diterapkan di perangkat *mobile* organisasi. Hasil rekomendasi selanjutnya disediakan untuk pejabat yang berwenang, yang bertanggung jawab untuk menentukan dan memutuskan persetujuan atau penolakan aplikasi menggunakan hasil rekomendasi yang diberikan.

d. *Result Submission*
Pada tahap ini dilakukan proses penyerahan hasil pemeriksaan aplikasi mencakup laporan persetujuan/penolakan dan laporan hasil pengujian aplikasi.

2.3. Standar *OWASP MASTG*

OWASP MASTG (*Mobile Application Security Testing Guide*) adalah panduan lengkap untuk pengujian keamanan aplikasi *mobile* dan *reverse engineering* yang mencakup proses, teknik, dan alat yang digunakan selama melakukan analisis keamanan aplikasi *mobile* [14]. *MASTG* terdiri dari 3 (tiga) bagian utama yaitu panduan pengujian umum, panduan pengujian android dan panduan pengujian iOS. Panduan Pengujian umum berisi metodologi pengujian keamanan aplikasi *mobile* dan teknik analisis kerentanan umum yang diterapkan pada keamanan aplikasi *mobile*. Selain itu juga berisi kasus uji teknis tambahan yang tidak bergantung pada sitem operasi mobile, yaitu pengujian otentikasi dan manajemen sesi, pengujian komunikasi jaringan, dan pengujian kriptografi.

Sedangkan panduan pengujian android dan iOS mencakup pengujian keamanan *mobile* untuk platform Android dan iOS yang terdiri dari pengujian keamanan dasar, pengujian *tampering* dan *reverse engineering*, pengujian penyimpanan data, pengujian kriptografi API, pengujian autentikasi *local*, pengujian komunikasi jaringan, pengujian *platform API*, pengujian kualitas kode dan pengaturan *build*, dan pengujian pertahanan *anti-reversing*.

2.4. *OWASP API Security*

OWASP API Security Top 10 merupakan 10 risiko keamanan API teratas dan mengilustrasikan bagaimana risiko tersebut dapat dimitigasi [15]. Selain itu juga untuk masing-masing risiko keamanan API terdapat contoh skenario serangan yang dapat digunakan untuk pengujian keamanan API. Adapun *OWASP API Security Top 10* 2019 yaitu *broken object level authorization* (*API1:BOLA*), *broken user authentication* (*API2:BUA*), *excessive data exposure* (*API3:EDE*), *lack of resources and rate limiting (API4:LRRL), broken function level authorization (API5:BFLA), mass assignment (API6:MA), security misconfiguration (API7:SM*), *injection(API8), improper assets management (API9:IAM), insufficient logging & monitoring (API10:ILM).*.

3. HASIL DAN PEMBAHASAN

3.1. Persyaratan Keamanan Aplikasi SPBE *Mobile*

Aplikasi SPBE adalah suatu program komputer yang dirancang supaya melaksanakan tugas sebagai fungsi dari suatu layanan SPBE. Sedangkan aplikasi SPBE *mobile* termasuk pada kategori aplikasi *mobile* yang dapat berjalan pada perangkat *mobile* yang didalamnya terdapat sistem operasi sendiri [5].

Setiap aplikasi SPBE *mobile* harus menerapkan standar teknis dan prosedur keamanan aplikasi SPBE dan memenuhi persyaratan keamanan aplikasi SPBE *mobile* berdasarkan Peraturan BSSN Nomor 4 Tahun 2021 Pasal 25 ayat (1) huruf b. Adapun standar teknis keamanan yang menjadi persyaratan untuk setiap aplikasi SPBE *mobile* tertuang pada Pasal 28 dan 29 Peraturan BSSN Nomor 4 Tahun 2021. Untuk mempermudah dalam melakukan analisis, maka dilakukan kodifikasi terhadap persyaratan keamanan aplikasi SPBE *mobile*. Hasil proses kodifikasi terhadap persyaratan keamanan aplikasi SPBE *mobile* ditunjukan pada tabel 1.

Tabel 1. Kodifikasi Persyaratan Keamanan Aplikasi SPBE *Mobile*

Kode	Persyaratan Keamanan
Persyaratan Penyimpanan data dan privasi	
AM-11	Menyimpan seluruh data dan informasi yang dikecualikan hanya dalam fasilitas penyimpanan kredensial sistem
…..	…….
Persyaratan Kriptografi	
AM-21	Menghindari penggunaan kriptografi simetrik dengan *hardcoded key*
…..	…….
Persyaratan Autentikasi dan manajemen sesi	
AM-31	Menerapkan autentikasi pada *remote endpoint* terhadap aplikasi yang menyediakan akses pengguna untuk layanan jarak jauh
…..	…….
Persyaratan Komunikasi jaringan	
AM-41	Menerapkan *secure socket layer* atau *transport layer security* yang tidak obsolet secara konsisten
AM-42	Memverifikasi sertifikat *remote endpoint*
Persyaratan Interaksi *platform*	
AM-51	Memastikan aplikasi hanya meminta akses terhadap sumber daya yang diperlukan
…..	…….
Persyaratan Kualitas kode dan pengaturan *build*	
AM-61	Menandatangani aplikasi dengan sertifikat yang valid
…..	…….
Persyaratan Ketahanan	
AM-71	Mencegah aplikasi berjalan pada perangkat yang telah dilakukan modifikasi yang tidak sah
…..	…….
AM-79	Menerapkan metode *obfuscation*

3.2. Menentukan Metode dan *Tools* Pengujian Keamanan Aplikasi SPBE *Mobile*

Metode pengujian keamanan aplikasi SPBE *mobile* dalam proses pemeriksaan keamanan aplikasi menggunakan pendekatan pengujian keamanan aplikasi secara manual dan otomatis menggunakan *tools* gratis dan *open source*.

a. Kriteria Penilaian

Sebelum melakukan pengujian perlu menentukan kriteria penilaian berdasarkan persyaratan keamanan aplikasi *SPBE mobile* untuk menentukan *tool* dan prosedur pengujian yang sesuai dengan sasaran kasus uji atau kriteria penilaian. Adapun tabel 2 merupakan kriteria penilaian yang disusun dalam penelitian ini.

Tabel 2. Kriteria Penilaian

Kriteria	Sasaran Kasus Uji
K1 (AM-11)	Kemampuan untuk mengidentifikasi kata sandi atau data sensitif lainnya yang disimpan secara tidak aman pada perangkat *mobile.*
K2 (AM-12)	Kemampuan untuk mengidentifikasi data sensitif yang dipertukarkan dengan pihak ketiga.
K3 (AM-13)	Kemampuan untuk mengidentifikasi *cache keyboard* dinonaktifkan saat memasukkan data sensitif
K4 (AM-14)	Kemampuan untuk mengidentifikasi masalah komunikasi antar-proses yaitu *content-provider* yang diekspos oleh aplikasi (*exported=true)*
K5 (AM-15)	Kemampuan mendeteksi pengungkapan data sensitif melalui *user interface*
…..	…….
K30 (AM-79)	Kemampuan untuk menentukan apakah kode aplikasi telah disamarkan (*obfuscated*) untuk mempersulit analisis keamanan

Untuk persyaratan autentikasi dan manajemen sesi hanya dapat dilakukan pengujian dengan pendekatan analisis dinamis sehingga termasuk pada fase pengujian manual atau pengujian API. Tabel 3 menunjukan kriteria penilaian pengujian untuk persyaratan autentikasi dan manajemen sesi.

Tabel 3. Kriteria Penilaian

Kriteria	Sasaran Kasus Uji
K1 (AM-11)	Kemampuan untuk mengidentifikasi kata sandi atau data sensitif lainnya yang disimpan secara tidak aman pada perangkat *mobile.*
K2 (AM-12)	Kemampuan untuk mengidentifikasi data sensitif yang dipertukarkan dengan pihak ketiga.
K3 (AM-13)	Kemampuan untuk mengidentifikasi *cache keyboard* dinonaktifkan saat memasukkan data sensitif
K4 (AM-14)	Kemampuan untuk mengidentifikasi masalah komunikasi antar-proses yaitu *content-provider* yang diekspos oleh aplikasi (*exported=true)*
K5 (AM-15)	Kemampuan mendeteksi pengungkapan data sensitif melalui *user interface*
…..	…….
K30 (AM-79)	Kemampuan untuk menentukan apakah kode aplikasi telah disamarkan (*obfuscated*) untuk mempersulit analisis keamanan

b. Evaluasi *Tool* Pengujian Otomatis

Pengujian otomatis menggunakan *tools* gratis dan *open source* dengan pendekatan analisis statis. Untuk melakukan evaluasi *tool* pengujian otomatis, beberapa *tool* pengujian *open source* hasil studi literatur dan hasil pencarian dari internet dengan pendekatan metode analisis statis dipilih yaitu *Mobile Security Framework (Mobsf) [17]*, *APKHunt [18]*, *Androbugs [19]*, dan *Yaazhini [20]*.

Sedangkan untuk aplikasi uji menggunakan aplikasi uji yang memiliki kerentanan umum atau isu-isu yang berkaitan dengan keamanan pada aplikasi *mobile* berbasis sistem operasi *android* yaitu

InsecureShop [21], *Hacking playground apps* [22], *androGoat* [23] dan *allSafe* [24].

Hasil evaluasi menunjukan bahwa *tool* dapat mendeteksi kerentanan-kerentanan pada aplikasi uji sebagaimana tertuang dalam tabel 4.

Tabel 4. Hasil Evaluasi *Tool* Pengujian Otomatis

Kriteria	Hasil Pengujian Otomatis			
	Mobsf	APKHunt	Androbugs	Yaazhini
K1(AM-11)	✓	✓	✓	✓
K2(AM-12)	x	✓	x	x
K3(AM-13)	x	✓	x	x
K4(AM-14)	✓	x	✓	✓
K5(AM-15)	x	✓	x	x
K6(AM-21)	✓	✓	x	✓
K7(AM-22,23,24)	✓	✓	x	✓
K8(AM-25)	✓	✓	x	✓
K9(AM-41,42)	✓	✓	✓	✓
K10(AM-51)	✓	✓	✓	x
K11(AM-52)	✓	✓	x	x
K12(AM-53)	✓	✓	x	✓
K13(AM-54)	✓	✓	✓	✓
K14(AM-55)	✓	✓	✓	✓
K15(AM-56)	x	✓	x	x
K16(AM-61)	✓	✓	x	x
K17(AM-62)	✓	✓	✓	✓
K18(AM-63)	✓	x	x	x
K19(AM-64)	x	✓	x	x
K20(AM-65)	x	x	x	x
K21(AM-66)	x	✓	x	x
K22(AM-67)	x	x	x	x
K23(AM-68)	x	✓	x	x
K24(AM-71,75)	✓	✓	✓	x
K25(AM-72)	x	✓	x	x
K26(AM-73,78)	x	✓	✓	x
K27(AM-74)	x	x	x	x
K28(AM-76)	x	x	x	x
K29(AM-77)	x	x	x	x
K30(AM-79)	x	✓	x	x

Berdasarkan tabel 4 hasil evaluasi terhadap *tools* pengujian otomatis diperoleh bahwa *Mobsf* dan *APKHunt* dapat memenuhi sasaran kasus uji (kriteria) lebih banyak sehingga dalam penelitian ini dapat digunakan sebagai *tool* pengujian otomatis dalam proses pemeriksaan keamaan aplikasi SPBE *mobile.*

c. Pemetaan Prosedur Pengujian Manual

Pengujian manual dilakukan dengan pendekatan analisis statis dan dinamis berdasarkan prosedur pengujian pada standar *OWASP MASTG* dan *API Security*. Pengujian manual dapat dilakukan untuk memvalidasi hasil pengujian otomatis atau melengkapi proses pengujian yang belum tercakup oleh pengujian otomatis seperti persyaratan autentikasi dan manajemen sesi. Berikut pada tabel 5 merupakan pemetaan prosedur pengujian *OWASP MASTG* terhadap kriteria penilaian yang telah ditentukan.

Tabel 5. Pemetaan Prosedur Pengujian *OWASP MASTG* terhadap Kriteria Penilaian

Kriteria	Prosedur *OWASP MASTG*
K1 (AM-11)	Menguji Penyimpanan Lokal untuk Data Sensitif *(MSTG-STORAGE-1* dan *MSTG-STORAGE-2)*
K2 (AM-12)	Menentukan Apakah Data Sensitif Dibagikan ke Pihak Ketiga *(MSTG-STORAGE-4)*
K3 (AM-13)	Menentukan Apakah Cache Keyboard Dinonaktifkan untuk Kolom Input Teks *(MSTG-STORAGE-5)*
K4 (AM-14)	*Menentukan Apakah Data Sensitif Diekspos melalui Mekanisme IPC (MSTG-STORAGE-6)*
…..	…….
K25 (AM-72)	Menguji Deteksi *Anti-Debugging (MSTG-RESILIENCE-2)*
K26 (AM-73, AM-78)	Menguji Pemeriksaan Integritas File *(MSTG-RESILIENCE-3 & 11)*
K27 (AM-74)	Menguji *Tool Reverse Engineering (MSTG-RESILIENCE-4)*
K28 (AM-76)	Menguji Pemeriksaan Integritas *Runtime (MSTG-RESILIENCE-6)*
K29 (AM-77)	Menguji Pengikatan Perangkat *(MSTG-RESILIENCE-10)*
K30(AM-79)	Menguji *Obfuscation (MSTG-RESILIENCE-9)*

Adapun pemetaan prosedur pengujian *OWASP MASTG/API Security* terhadap kriteria penilaian pengujian API ditunjukan pada tabel 6.

Tabel 6. Pemetaan Prosedur Pengujian *OWASP MASTG*/*API Security* terhadap Kriteria Penilaian Pengujian API

Kriteria	*OWASP MASTG*	*OWASP API Security*
K32 (AM-31)	*Memverifikasi Otentikasi yang Tepat (MSTG-AUTH-1)*	*API2:2019 Broken User Authentication*
K33 (AM-32)	Menguji Manajemen Sesi *Stateful (MSTG-AUTH-2)*	*API2:2019 Broken User Authentication*
K34 (AM-33)	Menguji Otentikasi *Stateless* (Berbasis Token) *(MSTG-AUTH-3)*	*API2:2019 Broken User Authentication*
…..	…….	
K39 (AM-38)	*Memverifikasi Otentikasi yang Tepat (MSTG-ARCH-2)*	*API1:2019 Broken Object Level Authorization*

3.3. Penentuan Kriteria Persetujuan/Penolakan Aplikasi SPBE *Mobile*

Persetujuan/penolakan aplikasi SPBE *mobile* dilakukan berdasarkan rekomendasi hasil validasi persyaratan keamanan aplikasi SPBE *mobile.* Validasi dilakukan dengan memeriksa temuan pada setiap prosedur atau metode pengujian yang telah dilakukan pada tahap pengujian keamanan aplikasi. Berikut pada tabel 7 merupakan daftar periksa metode pengujian keamanan aplikasi untuk memvalidasi persyaratan keamanan aplikasi SPBE *mobile.* Sedangkan pada tabel 8 ditunjukan kriteria untuk validasi persyaratan keamanan aplikasi SPBE *mobile* dan pada tabel 9 ditunjukan kriteria persetujuan/penolakan aplikasi SPBE *mobile.*

Tabel 7. Daftar Periksa Metode Pengujian terhadap Persyaratan Keamanan Aplikasi SPBE *Mobile*

Persyaratan Keamanan	Metode Pengujian		
	***Tool* Otomatis**	***OWASP MASTG***	***API Security***
AM-11	Ya	*MSTG-STORAGE-1&2*	Tidak
AM-12	Ya	*MSTG-STORAGE-4*	Tidak
AM-13	Ya	*MSTG-STORAGE-5*	Tidak
….	….	….	….
AM-31	Tidak	*MSTG-AUTH-1*	Ya
AM-32	Tidak	*MSTG-AUTH-2*	Ya
AM-33	Tidak	*MSTG-AUTH-3*	Ya
AM-34	Tidak	*MSTG-AUTH-4*	Ya
….	….	….	….
AM-76	Tidak	*MSTG-RESILIENCE-6*	Tidak
AM-77	Tidak	*MSTG-RESILIENCE-10*	Tidak
AM-79	Ya	*MSTG-RESILIENCE-9*	Tidak

Tabel 8. Kriteria Validasi Persyaratan Keamanan Aplikasi SPBE *Mobile*

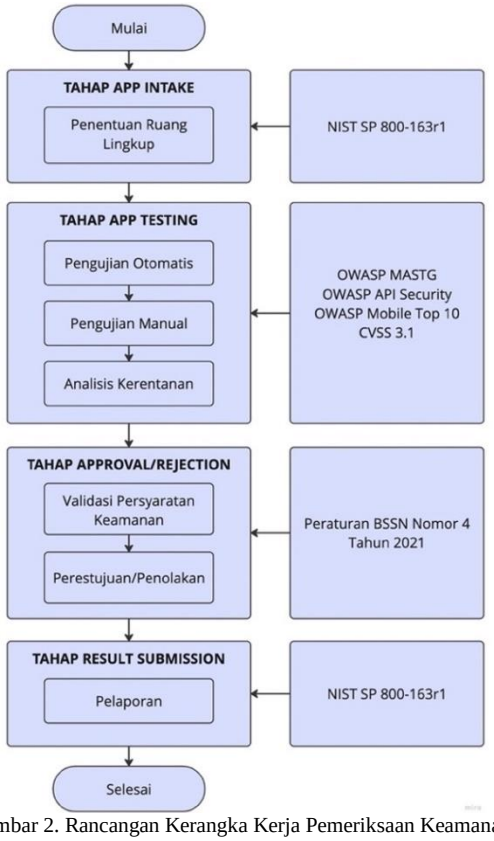
Validasi Persyaratan Keamanan		Temuan Pengujian Manual		
		Tidak Diuji	**Tidak Ada**	**Ada**
Temuan *Tool* Otomatis	Tidak Diuji	N/A	Lulus	Gagal
	Tidak Ada	Lulus	Lulus	Gagal
	Ada	Gagal	Gagal	Gagal

Tabel 9. Kriteria Persetujuan/Penolakan Aplikasi SPBE *Mobile*

Persetujuan/ Penolakan		Persyaratan Keamanan	
		LULUS (Sebagian)	**LULUS (Seluruh)**
Kerentanan (CVSS)	Informasional	Setuju	Setuju
	Rendah	Tolak	Setuju
	Sedang	Tolak	Tolak
	Tinggi	Tolak	Tolak
	Kritis	Tolak	Tolak

3.4. Rancangan Kerangka Kerja Pemeriksaan Keamanan Aplikasi SPBE *Mobile*

Secara umum rancangan kerangka kerja mengadopsi dari tahapan umum pemeriksaan keamanan aplikasi *mobile* berdasarkan *NIST SP 800-163r1* yang dikombinasikan dengan standar teknis untuk melakukan pengujian keamanan aplikasi dan analisis kerentanan yaitu standar *OWASP MASTG, OWASP API Security, OWASP Mobile Top 10* dan *Common Vulnerability Scoring System.* Hasil pengujian keamanan aplikasi digunakan untuk memvalidasi persyaratan keamanan aplikasi SPBE *mobile* berdasarkan peraturan BSSN Nomor 4 Tahun 2021 untuk memastikan bahwa aplikasi memenuhi semua persyaratan keamanan aplikasi SPBE *mobile*. Berikut ini pada gambar 2 merupakan rancangan kerangka kerja yang diajukan dalam penelitian ini.



Gambar 2. Rancangan Kerangka Kerja Pemeriksaan Keamanan Aplikasi SPBE *Mobile*

3.4.1. Tahap *App Intake*

Pada tahap ini dilakukan penetapan ruang lingkup pemeriksaan keamanan aplikasi SPBE *mobile* yaitu dengan melakukan pencatatan informasi mengenai aplikasi SPBE *mobile* yang akan dilakukan proses pemeriksaan keamanan seperti nama aplikasi, versi aplikasi, nilai *hash* aplikasi termasuk informasi pengembang, waktu pelaksaan pemeriksaan keamanan dan informasi relevan lainnya yang diperlukan untuk proses pemeriksaan keamanan aplikasi SPBE *mobile*.

3.4.2. Tahap *App Testing*

Pada tahap ini dilakukan proses pengujian keamanan aplikasi SPBE *mobile* berdasarkan metode pengujian yang telah ditetapkan pada bagian 3.2 yaitu terdiri dari pengujian otomatis, pengujian manual dan analisis kerentanan.

Pada pengujian otomatis dilakukan dengan menjalankan beberapa *tool* yang secara otomatis melakukan analisis statis dengan memeriksa kerentanan atau isu keamanan yang terdapat pada aplikasi SPBE *mobile.* Sedangkan pada pengujian manual dilakukan berdasarkan prosedur-prosedur pengujian yang terdapat pada standar *OWASP MASTG* dan juga berdasarkan pengujian *OWASP API Security*.

Selanjutnya kerentanan yang ditemukan dilakukan analisis dengan memetakan kerentanan terhadap kategori risiko *OWASP Mobile Top 10* [12]

dan dilakukan perhitungan tingkat *severity* berdasarkan *Common Vulnerability Scoring System* (CVSS) versi 3.1 [13].

3.4.3. Tahap *Approval/Rejection*

Pada tahap ini dilakukan proses persetujuan atau penolakan terhadap aplikasi SPBE *mobile*, apakah aplikasi SPBE *mobile* memenuhi persyaratan keamanan aplikasi SPBE *mobile* yang ditetapkan pada Peraturan BSSN Nomor 4 Tahun 2021. Tahap persetujuan/penolakan terdiri dari proses validasi persyaratan keamanan aplikasi SPBE *mobile* dan proses persetujuan/penolakan aplikasi SPBE *mobile*.

Pada aktivitas validasi persyaratan keamanan aplikasi dilakukan berdasarkan pada daftar periksa yang telah ditetapkan sebelumnya pada bagian 3.3 tabel 7. Pada aktivitas persetujuan/penolakan dilakukan dengan mempertimbangkan hasil rekomendasi dari aktivitas validasi persyaratan keamanan aplikasi SPBE *mobile*.

3.4.4. Tahap *Result Submission*

Pada tahap ini dilakukan proses penyusunan dan penyerahan laporan pemeriksaan keamanan aplikasi SPBE *mobile* yang mencakup laporan persetujuan/penolakan dan laporan hasil pengujian keamanan aplikasi SPBE *mobile*.

3.5. Simulasi Rancangan Kerangka Kerja Pemeriksaan Keamanan Aplikasi SPBE *Mobile*

Simulasi rancangan kerangka kerja dilakukan pada aplikasi SPBE *mobile* ABC berbasis sistem operasi android yang dikembangkan oleh salah satu instansi pemerintah daerah di Indonesia. Proses simulasi dilakukan berdasarkan alur proses hasil rancangan kerangka kerja pemeriksaan keamanan aplikasi SPBE *mobile* yang dijelaskan pada bagian 3.4. Adapun hasil rancangan kerangka kerja tersebut dilakukan simulasi terhadap aplikasi SPBE *mobile* ABC untuk dilakukan analisis dan pembahasan sebagai berikut:

3.5.1. Tahap *App Intake*

Pada tahap ini dilakukan penentuan ruang lingkup untuk melakukan pemeriksaan keamanan aplikasi SPBE *mobile*. Adapun hasil penentuan ruang lingkup pemeriksaan keamanan aplikasi ditunjukan pada tabel 10.

Tabel 10. Hasil Penentuan Ruang Lingkup

Nama Aplikasi	ABC Super Apps (APK)
Target Sistem Operasi	Android (minSdkVersion="21" targetSdkVersion="31")
Versi Aplikasi	Versi 3.1.4
Hash Aplikasi	SHA256: 14e5eccee0184420d5a1abac18cc73f4 e8bfb70671c7485fa1079f4c64c3dafc
Informasi Developer	JDS
Persyaratan Keamanan	Peraturan BSSN Nomor 4 Tahun 2021

3.5.2. Tahap *App Testing*

Pada tahap ini dilakukan pengujian keamanan aplikasi SPBE *mobile* dengan pendekatan *tool* otomatis dan pengujian manual, serta analisis kerentanan untuk perhitungan *severity* setiap kerentanan yang ditemukan. Berdasarkan hasil pengujian menggunakan beberapa *tools* otomatis diperoleh hasil pengujian yang ditunjukan pada tabel 11.

Tabel 11. Hasil Pengujian *Tools* Otomatis

Kriteria	APKHunt	Mobsf	Hasil Pengujian
K7(AM-22,23,24)	✓	✓	Aplikasi menggunakan mode enkripsi CBC dengan padding PKCS7
	✓	✓	Aplikasi menggunakan algoritma hash SHA-1 yang dinyatakan lemah
K8(AM-25)	✓	✓	Aplikasi menggunakan Random Number Generator yang tidak aman
K10(AM-51)	✓	✓	Ditemukan *BroadcastReceiver* yang Belum diatur izin aplikasinya
K11(AM-52)	✓	✓	Aplikasi menggunakan SQLite Database yang rentan terhadap SQL Injection
K16(AM-61)	x	✓	Aplikasi rentan terhadap Kerentanan Janus
K19(AM-64)	✓	x	Aplikasi mengaktifkan StrictMode pada aplikasi production
K24(AM-71, AM-75)	✓	✓	Aplikasi memiliki kemampuan untuk mendeteksi perangkat yang di-root
	✓	x	Aplikasi memiliki kemampuan untuk mendeteksi emulator
K25(AM-72)	✓	✓	Aplikasi sudah menerapkan anti-debugging

Selanjutnya untuk melengkapi hasil pengujian otomatis maka dilakukan pengujian manual berdasarkan prosedur *OWASP MASTG*. Adapun hasil pengujian berdasarkan prosedur *OWASP MASTG* ditunjukan pada tabel 12.

Tabel 12. Hasil Pengujian *OWASP MASTG*

Prosedur *OWASP MASTG*	**Hasil Pengujian**
MSTG-STORAGE-4	Aplikasi mengirimkan data sensitif ke pihak ketiga (*third parties*)
MSTG-CRYPTO-1	Aplikasi menggunakan kunci simetris yang di *hardcode* pada *source code* aplikasi
MSTG-NETWORK-2	Mengaktifkan TLS 1.0 dan 1.1 yang sudah kadaluarsa
	SSL/TLS Rentan terhadap Serangan *Sweet32*
MSTG-CODE-9	*Native library libapp.so* belum mengaktifkan perlindungan biner *canary (canary=false)*
MSTG-RESILIENCE-3 dan 6	Aplikasi belum menerapkan mekanisme *integrity check*
MSTG-RESILIENCE-4	Aplikasi belum menerapkan mekanisme deteksi *tool reverse engineering*

MSTG-RESILIENCE-6	Aplikasi belum menerapkan anti hook (*runtime integrity check*)
MSTG-RESILIENCE-9	Aplikasi sudah menerapkan metode *obfuscation*
MSTG-RESILIENCE-10	Aplikasi sudah menerapkan *device binding*

Berikut pada tabel 13 merupakan hasil pengujian keamanan API berdasarkan prosedur *OWASP MASTG* dan *OWASP API Security*.

Tabel 13. Hasil Pengujian *OWASP MASTG*

Prosedur *OWASP MASTG*	**Hasil Pengujian**
MSTG-STORAGE-4	Aplikasi mengirimkan data sensitif ke pihak ketiga (*third parties*)
MSTG-CRYPTO-1	Aplikasi menggunakan kunci simetris yang di *hardcode* pada *source code* aplikasi
MSTG-NETWORK-2	Mengaktifkan TLS 1.0 dan 1.1 yang sudah kadaluarsa *SSL/TLS* Rentan terhadap Serangan *Sweet32*
MSTG-CODE-9	*Native library libapp.so* belum mengaktifkan perlindungan biner *canary (canary=false)*
MSTG-RESILIENCE-3 dan 6	Aplikasi belum menerapkan mekanisme *integrity check*
MSTG-RESILIENCE-4	Aplikasi belum menerapkan mekanisme deteksi *tool reverse engineering*
MSTG-RESILIENCE-6	Aplikasi belum menerapkan anti hook (*runtime integrity check*)
MSTG-RESILIENCE-9	Aplikasi sudah menerapkan metode *obfuscation*
MSTG-RESILIENCE-10	Aplikasi sudah menerapkan *device binding*

Berdasarkan kerentanan-kerentanan yang teridentifikasi, selanjutnya dilakukan analisis dengan melakukan kategorisasi risiko berdasarkan *OWASP Top 10 Mobile* dan melakukan perhitungan tingkat *severity* menggunakan kalkulator CVSS 3.1. Adapun hasil analisis kerentanan pada penelitian ini disampaikan pada tabel 14.

Tabel 14. Hasil Analisis Kerentanan

No	**Kerentanan**	**Hasil Analisis**	
		Kategori	***Severity***
1	Aplikasi menggunakan mode enkripsi CBC dengan padding PKCS7 yang rentan	*OWASP M5*	*Low (3.1)*
2	Aplikasi menggunakan algoritma hash SHA-1 yang dinyatakan lemah	*OWASP M5*	*Low (3.7)*
3	Aplikasi menggunakan *Random Number Generator* yang tidak aman	*OWASP M5*	*Low (3.7)*
4	Ditemukan *BroadcastReceiver* yang Belum diatur izin aplikasinya	*OWASP M1*	*Low (2.5)*
5	Aplikasi menggunakan *SQLite Database* yang rentan terhadap SQL Injection	*OWASP M7*	*Medium (4.7)*
6	Aplikasi rentan terhadap Kerentanan Janus	*OWASP M1*	*Medium (5.8)*
7	Aplikasi mengaktifkan *StrictMode* pada aplikasi *production*	*OWASP M7*	*Medium (4.0)*
8	Aplikasi mengirimkan data sensitif ke pihak ketiga (*third parties*)	*OWASP M2*	*Medium (4.7)*
9	Aplikasi menggunakan kunci simetris yang di *hardcode* pada *source code* aplikasi	*OWASP M9*	*Low (2.9)*
10	*TLS 1.0 & TLS 1.1 Enabled*	*OWASP M3*	*Medium (5.9)*
11	*SSL/TLS* Rentan terhadap Serangan *Sweet32*	*OWASP M3*	*Medium (5.9)*
12	*Native library libapp.so* belum mengaktifkan perlindungan biner *canary (canary=false)*	*OWASP M7*	*Low (2.9)*
13	Aplikasi belum menerapkan mekanisme *integrity check*	*OWASP M8*	*Medium (5.8)*
14	Aplikasi belum menerapkan mekanisme deteksi *tools reverse engineering*	*OWASP M9*	*Low (3.3)*
15	Aplikasi belum menerapkan anti *hook* (*runtime integrity check*)	*OWASP M8*	*Low (3.3)*
16	Pengungkapan Informasi Sensitif pada *JSON Web Token*	*OWASP M44*	*Low (3.7)*
17	Kebijakan kata sandi tidak diterapkan pada server	*OWASP M4*	*Low (3.7)*
18	Tidak Menerapkan Pembatasan Percobaan Login	*OWASP M4*	*Medium (5.6)*
19	Tidak Menerapkan Otorisasi pada beberapa Endpoint API	*OWASP M6*	*Medium (6.5)*
20	Kontrol Akses yang Tidak Tepat pada Fitur Reset Kata Sandi Menyebabkan Pengambilalihan Akun	*OWASP M6*	*High (7.3)*

3.5.3. Tahap *Approval/Rejection*

Pada tahap ini dilakukan validasi persyaratan keamanan aplikasi SPBE *mobile.* Validasi persyaratan keamanan aplikasi SPBE *mobile* berdasarkan daftar periksa pada tabel 7 dan kriteria validasi persyaratan keamanan aplikasi SPBE *mobile* pada tabel 8. Adapun hasil validasi persyaratan keamanan ditunjukan pada tabel 15.

Tabel 15. Hasil Validasi Persyaratan Keamanan Aplikasi SPBE *Mobile*

Persyaratan Keamanan	Hasil Validasi (Temuan)			
	Tools	*MASTG*	*API*	Status
Persyaratan Penyimpanan Data dan Privasi				
AM-11	Tidak Ada	Tidak Ada	N/A	Lulus
AM-12	Tidak Ada	Ada	N/A	Gagal
AM-13	Tidak Ada	Tidak Ada	N/A	Lulus
AM-14	Tidak Ada	Tidak Ada	N/A	Lulus
AM-15	Tidak Ada	Tidak Ada	N/A	Lulus
Persyaratan Kriptografi				
AM-21	Tidak Ada	Ada	N/A	Gagal
AM-22	Ada	N/A	N/A	Gagal
AM-23	Ada	N/A	N/A	Gagal
AM-24	Tidak Ada	Tidak Ada	N/A	Lulus
AM-25	Ada	N/A	N/A	Gagal
Persyaratan Autentikasi dan Manajemen Sesi				
AM-31	N/A	Tidak Ada	Tidak Ada	Lulus
AM-32	N/A	Tidak Ada	Tidak Ada	Lulus
AM-33	N/A	Ada	Ada	Gagal
AM-34	N/A	Tidak Ada	Tidak Ada	Lulus
AM-35	N/A	Ada	Ada	Gagal
AM-36	N/A	Ada	Ada	Gagal
AM-37	N/A	Tidak Ada	Tidak Ada	Lulus
AM-38	N/A	Ada	Ada	Gagal
Persyaratan Komunikasi Jaringan				
AM-41	Ada	Ada	N/A	Gagal
AM-42	Tidak Ada	N/A	N/A	Lulus
Persyaratan Interaksi *Platform*				

AM-51	Ada	Tidak Ada	N/A	Gagal
AM-52	Ada	Tidak Ada	N/A	Gagal
AM-53	Tidak Ada	Tidak Ada	N/A	Lulus
AM-54	Tidak Ada	Tidak Ada	N/A	Lulus
AM-55	Tidak Ada	Tidak Ada	N/A	Lulus
AM-56	N/A	N/A	N/A	N/A
Persyaratan Kualitas Kode dan Pengaturan *Build*				
AM-61	Ada	N/A	N/A	Gagal
AM-62	Tidak Ada	Tidak Ada	N/A	Lulus
AM-63	Tidak Ada	Tidak Ada	N/A	Lulus
AM-64	Ada	N/A	N/A	Gagal
AM-65	N/A	N/A	N/A	N/A
AM-66	N/A	N/A	N/A	N/A
AM-67	N/A	N/A	N/A	N/A
AM-68	Ada	Ada	N/A	Gagal
Persyaratan Ketahanan				
AM-71	Tidak Ada	N/A	N/A	Lulus
AM-72	Tidak Ada	N/A	N/A	Lulus
AM-73	N/A	Ada	N/A	Gagal
AM-74	N/A	Ada	N/A	Gagal
AM-75	Tidak Ada	N/A	N/A	Lulus
AM-76	N/A	Ada	N/A	Gagal
AM-77	N/A	Tidak Ada	N/A	Lulus
AM-78	N/A	Ada	N/A	Gagal
AM-79	N/A	Tidak Ada	N/A	Lulus

Berdasarkan hasil validasi persyaratan keamanan ditemukan bahwa terdapat 19 persyaratan yang belum dipenuhi oleh aplikasi SPBE ABC.

Berdasarkan kriteria persetujuan/penolakan maka aplikasi SPBE ABC dinyatakan ditolak untuk dipublikasikan ke publik sebagaimana ditunjukan pada tabel 16 persyaratan keamanan yang belum dipenuhi.

Tabel 16. Penolakan Aplikasi SPBE *Mobile* ABC

Nama Aplikasi	Persyaratan yang belum dipenuhi	Status
ABC Super Apps (APK)	▪ Penyimpanan data dan privasi (AM-12) ▪ Kriptografi (AM-21, AM-22, AM-23, AM-25) ▪ Autentikasi dan Manajemen sesi (AM-33, AM-35, AM-36, AM-38) ▪ Komunikasi Jaringan (AM-41) ▪ Interaksi *Platform* (AM-51, AM-52) ▪ Kualitias Kode (AM-61, AM-64, AM-68) ▪ Ketahanan (AM-73, AM-74, AM-76, AM-78)	Ditolak

3.5.4. Tahap *Result Submission*

Berdasarkan hasil pengujian dan penolakan, maka aplikasi SPBE *mobile* ABC perlu dilakukan perbaikan terhadap kerentanan-kerentanan yang berhasil diidentifikasi. Adapun rekomendasi yang diberikan sebagai berikut:

a. Menggunakan algoritma kriptografi yang kuat dan terapkan sesuai *best practice*.
b. Menghindari penggunaan algoritma kriptografi seperti enkripsi, fungsi hash maupun pembangkit bilangan acak yang lemah dan tidak aman.
c. Terapkan *permission BroadcastReceiver* dengan baik sesuai dengan peruntukannya
d. Lakukan validasi terhadap input data yang diterima dari sisi pengguna
e. Menonaktifkan skema tanda tangan v1 dan hanya menggunakan skema tanda tanggan v2 ke atas untuk menandatangani aplikasi.
f. *StrictMode* dirancang hanya untuk penggunaan pra-produksi, sehingga direkomendasikan tidak diaktifkan dalam aplikasi produksi.
g. Hindari mengirimkan atau membagikan data sensitif ke aplikasi pihak ketiga (*tracker*) atau pihak yang tidak berhak atas data sensitif
h. Hindari melakukan *hardcode* kunci kriptografi simetris pada *source code* aplikasi.
i. Non aktifkan *TLS* 1.0/1.1 dan terapkan *SSL/TLS* 1.2 atau lebih baru pada sisi *backend/API server*
j. Lakukan konfigurasi pada *server SSL/TLS* untuk menonaktifkan algoritma yang mendukung *block cipher 64-bit (3DES)* yang sudah tidak digunakan lagi
k. Mengaktifkan fitur perlindungan *PIE* dan *stack smashing (canary dan pic)* pada *native library*
l. Aplikasi harus menerapkan metode *code integrity check* dengan merespon atau memperingatkan pengguna jika terjadi modifikasi aplikasi.
m. Menerapkan metode pendeteksian *tool reverse engineering* dengan merespon dengan cara tertentu terhadap keberadaan *tool* tersebut seperti memperingatkan pengguna dan meminta untuk menerima risikonya.
n. Aplikasi harus menerapkan metode *runtime integrity check* atau *anti hook* dengan merespon atau memperingatkan pengguna jika terjadi modifikasi saat aplikasi sedang berjalan.
o. Hindari menyertakan informasi sensitif dalam *JWT*, hapus informasi sensitif dalam *JWT*. Jika perlu menyimpan informasi sensitif dalam *JWT*, terapkan *JSON Web Encryption (JWE)*.
p. Terapkan pengecekan kekuatan *password* pada sisi server seperti panjang minimal untuk *password* adalah 8 karakter yang terdiri dari kombinasi karekter khusus, huruf kecil, angka dan huruf besar.
q. Terapkan beberapa perlindungan pada mekanisme percobaan login seperti penguncian akun setelah sejumlah upaya percobaan *password* salah, memblokir alamat IP penyerang, atau dan menerapkan *captcha*.
r. Menerapkan autorisasi untuk setiap *endpoint* API, sehingga hanya *authorized user* yang dapat mengakses data tersebut.
s. Menerapkan kontrol akses dengan benar dan batasi penggunaan token hanya satu kali untuk penggantian password.

4. DISKUSI

Pada penelitian sebelumnya Muhammad Sajidur Rahman dkk telah merancang kerangka kerja yang dinamakan SO{U}RCERER untuk melakukan pengujian keamanan aplikasi *android* dengan

mengacu pada *OWASP MASTG* dengan beberapa persyaratan keamanan *OWASP* [25]. Namun penelitian tersebut belum menggunakan standar *NIST SP 800-163r1* dan Peraturan BSSN Nomor 4 Tahun 2021. Selain itu, penelitian belum mempertimbangkan pengujian terkait interaksi dengan API seperti kasus uji pada *OWASP API Security Top 10 2019*. Keterbaruan pada rancangan kerangka kerja ini dibandingkan dengan penelitian terdahulu yaitu kerangka kerja ini disusun dengan mempertimbangkan pengujian manual berdasarkan *OWASP API Security top 10 2019* untuk memvalidasi persyaratan keamanan terkait dengan interaksi dengan server aplikasi sebagaimana dinyatakan pada penelitian [26], bahwa kerentanan yang paling kritis adalah kerentanan yang terkait dengan interaksi dengan server aplikasi.

Pada penelitian ini dilakukan simulasi terhadap hasil rancangan kerangka kerja pemeriksaan keamanan pada aplikasi SPBE *mobile* ABC milik salah satu instransi pemerintah daerah. Hasil simulasi menunjukan bahwa semua persyaratan keamanan dapat dilakukan validasi dengan beberapa metode pengujian yaitu pengujian otomatis, pengujian berdasarkan *OWASP MASTG* dan *OWASP API Security*. Sedangkan pada penelitian sebelumnya hanya berfokus pada pendekatan validasi persyaratan keamanan menggunakan *tool* otomatis atau berdasarkan *OWASP MASTG* belum mempertimbangkan pengujian terhadap keamanan API, sehingga beberapa peryaratan keamanan tidak dapat divalidasi.

5. KESIMPULAN

Pada penelitian ini telah dilakukan perancangan Kerangka Kerja Pemeriksaan Keamanan pada Aplikasi SPBE *Mobile* berbasis sistem operasi android. Perancangan kerangka kerja mengacu pada tahapan umum berdasarkan standar *NIST SP 800-163r1* yang terdiri tahap *app intake*, tahap *app testing*, tahap *approval/rejection* dan tahap *result submission*. Pada tahap *app testing* mengkombinasikan metode pengujian otomatis dan pengujian manual untuk memvalidasi semua persyaratan keamanan aplikasi SPBE *mobile* yang tertuang pada peraturan BSSN nomor 4 tahun 2021.

Untuk melakukan pengujian otomatis telah ditentukan kriteria penilaian *tool* untuk pengujian otomatis dan berdasarkan hasil evaluasi telah dipilih beberapa *tool* untuk pengujian otomatis. Sedangkan pada pengujian manual telah dipetakan prosedur pengujian *OWASP MASTG* dan *OWASP API Secutity* terhadap persyaratan keamanan aplikasi SPBE *mobile.* Hasil pemetaan dapat digunakan sebagai daftar periksa untuk melakukan validasi persyaratan keamanan aplikasi SPBE *mobile.* Selain itu juga telah dibuat kriteria persetujuan/penolakan aplikasi SPBE *mobile.*

Adapun pengembangan penelitian lebih lanjut yang dapat dilakukan yaitu diantaranya melakukan perancangan sistem pemeriksaan keamanan aplikasi SPBE *mobile* secara otomatis berdasarkan hasil rancangan kerangka kerja pada penelitian ini atau dapat juga melakukan perancangan kerangka kerja pemeriksaan keamanan aplikasi SPBE untuk jenis lainnya, misalkan aplikasi SPBE berbasis web, serta penyesuaian metode yang lebih efektif dan efisien, sehingga dapat mendukung instansi pusat maupun pemerintah daerah dalam melakukan validasi persyaratan keamanan aplikasi SPBE.

UCAPAN TERIMA KASIH

Ucapan terima kasih penulis sampaikan kepada Kementerian Komunikasi dan Informatika Republik Indonesia yang telah mendukung dan sekaligus membiayai penelitian ini.

Ucapan terima kasih juga penulis sampaikan kepada instansi pengelola aplikasi SPBE yang telah memberikan ijin untuk melakukan penelitian terhadap aplikasi SPBE yang menjadi sampel dalam simulasi rancangan kerangka kerja yang telah disusun.

DAFTAR PUSTAKA

[1] Statista. "Number of smartphone users in Indonesia from 2019 to 2021 with forecasts until 2028." [Online]. Available: https://www.statista.com/statistics/266729/smartphone-users-in-indonesia/ (accessed 5 Januari, 2023).

[2] Statista. "Smartphone market in Indonesia - Statistics and facts." [Online]. Available: https://www.statista.com/topics/5020/smartphones-in-indonesia/#topicOverview (accessed 5 Januari, 2023).

[3] Kementerian Sekretariat Negara Republik Indonesia, "Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik," Jakarta, 2018.

[4] NowSecure. "High-Tech Mobile Apps Expose Data." [Online]. Available: https://www.nowsecure.com/blog/2023/03/29/high-tech-mobile-apps-expose-data/ (accessed 29 Maret, 2023).

[5] Badan Siber dan Sandi Negara, "Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 Tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Dan Standar Teknis Dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik," Jakarta, 2021.

[6] A. Ankur and S. Patel, "Finding Vulnerabilities in E-Governance Apps of Android Platform," *in 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS)*, pp. 185-191, 2022.

[7] R. A. Pratama, "Perancangan Kerangka Kerja Penilaian Keamanan dan Privasi pada Aplikasi Telemedicine Mobile Berbasis Sistem Operasi Android," Magister, Teknik Elektro, Universitas Indonesia, Jakarta, 2021.

[8] C.-W. Tien, T.-Y. Huang, T.-C. Huang, W.-H. Chung, and S.-Y. Kuo, "MAS: Mobile-Apps Assessment and Analysis System," *in 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, pp. 145-148, 2017.

[9] Eric B. Blancaflor, Gerardine Anne J. Anson, Angela Mae V. Encinas, Kiel Cedrick T. Huplo, Mark Anthony V. Marin, and S. L. G. Zamora, "A Vulnerability Assessment on the Parental Control Mobile Applications' Security: Status based on the OWASP Security Requirements," presented at the The 11th Annual International Conference on Industrial Engineering and Operations Management, Singapore, 2021.

[10] Statista. "Market share of mobile operating systems in Indonesia from January 2013 to October 2022, by operating system." [Online]. Available: https://www.statista.com/statistics/262205/market-share-held-by-mobile-operating-systems-in-indonesia/ (accessed 10 Januari, 2023).

[11] Statista. "Number of mobile app downloads worldwide from 2016 to 2022." [Online]. Available: https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/ (accessed 10 Januari, 2023).

[12] OWASP. "OWASP Mobile Top 10 2016." [Online]. Available: https://owasp.org/www-project-mobile-top-10/ (accessed 10 Maret, 2023).

[13] Forum of Incident Response and Security Teams, "Common Vulnerability Scoring System Version 3.1 Calculator." [Online]. Available: https://www.first.org/cvss/calculator/3.1/.

[14] Sven Schleier, Carlos Holguera, Bernhard Mueller, and J. Willemsen, "OWASP Mobile Application Security Testing Guide v1.5.0," 2022. [Online]. Available: https://github.com/OWASP/owasp-mastg/releases/tag/v1.5.0.

[15] OWASP, "OWASP API Security Top 10 2019," 2019. [Online]. Available: https://owasp.org/www-project-api-security/.

[16] M. Ogata, J. Franklin, J. Voas, V. Sritapan, and S. Quirolgico, "NIST SP 800-163 Revision 1: Vetting the Security of Mobile application," 2019.

[17] A. S. e. al. "Mobile Security Framework (MobSF)." [Online]. Available: https://github.com/MobSF/Mobile-Security-Framework-MobSF (accessed 1 April, 2023).

[18] S. Kalaria and M. Chawda. "APKHunt | OWASP MASVS Static Analyzer." [Online]. Available: https://github.com/Cyber-Buddy/APKHunt (accessed 31 Maret, 2023).

[19] Y.-C. Lin. "AndroBugs Framework." [Online]. Available: https://github.com/AndroBugs/AndroBugs_Framework (accessed 3 April, 2023).

[20] Vegabird. "Yaazhini - Android application APK scanner." [Online]. Available: https://www.vegabird.com/yaazhini/ (accessed 2 April, 2023).

[21] R. Gandhi. "InsecureShop." [Online]. Available: https://github.com/hax0rgb/InsecureShop (accessed 3 April, 2023).

[22] S. Schleier. "MASTG Hacking Playground." [Onilne]. Available: https://github.com/OWASP/MASTG-Hacking-Playground (accessed 3 April, 2023).

[23] s. patnayak. "AndroGoat." [Online]. Available: https://github.com/satishpatnayak/AndroGoat (accessed 3 April, 2023).

[24] K. Balajti-Tóth. "AllSafe." [Online]. Available: https://github.com/t0thkr1s/allsafe (accessed 3 April, 2023).

[25] M. S. Rahman, B. Kojusner, R. Kennedy, P. Pathak, L. Qi, and B. Williams, "SO{U}RCERER : Developer-Driven Security Testing Framework for Android Apps," *in Automated Software Engineering Conference's Workshop on Advances in Mobile App Analysis (A-Mobile'21)*, 2021.

[26] M. Antonishyn and O. Misnik, "Analysis of testing approaches to Android mobile application vulnerabilities," *CEUR Workshop Proceedings*, vol. 2577, 22, pp. 270-280, 2019.