Evaluasi Keamanan pada Kelas *Assurance Vulnerability Assessment* Aplikasi PeSankita Berdasarkan *Common Criteria Evaluation Methodology Version* 3.1 *Revision* 5:2017

Muhammad Aqil Hilmi[1)], Amiruddin Amiruddin[2)]
1) Badan Siber dan Sandi Negara, muhammad.aqil@bssn.go.id
2) Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, amiruddin@poltekssn.ac.id

Abstrak

Pada saat ini telah banyak dirancang aplikasi *instant messenger* untuk mendukung dan memudahkan aktivitas komunikasi. Salah satu aplikasi tersebut adalah PeSankita, yang merupakan salah satu produk instant messenger buatan Indonesia. Aplikasi *instant messenger* perlu dievaluasi keamanannya agar menimbulkan kepercayaan pengguna terhadap keamanan data, baik yang disimpan maupun yang dipertukarkan menggunakan aplikasi tersebut. Salah satu standar yang dapat digunakan untuk melakukan evaluasi keamanan aplikasi *secure chat* adalah Common Criteria for IT Security Evaluation Version 3.1 Revision 5:2017 (CC) khususnya Common Criteria Evaluation Methodology Version 3.1 Revision 5:2017 (CEM). Pada penelitian ini telah dilakukan evaluasi keamanan aplikasi PeSankita pada kelas *Assurance Vulnerability Assessment* (AVA) yaitu kelas penilaian kerentanan yang mungkin terdapat dalam aplikasi sebagai *Target of Evaluation* (TOE). Evaluasi dilakukan berdasarkan data mengenai TOE yang telah didapatkan sebelumnya. Hasil yang didapatkan dari proses pengujian yang disertai dengan bukti evaluasi menunjukkan bahwa TOE, dalam hal ini PeSankita, tidak seperti yang diklaim oleh pengembang aplikasi tersebut karena masih ditemukan serangan tingkat dasar pada aplikasi PeSankita versi 1.4.23 pada pengujian *client code quality* dan *reverse engineering*.

Kata kunci: Common Criteria, Criteria Evaluation, kelas AVA, PeSankita, TOE

Abstract

Currently, many instant messenger applications have been designed to support and facilitate communication activities. One such application is PeSankita, which is an instant messenger product made in Indonesia. Instant messenger applications need to be evaluated for security in order to create user confidence in the security of data, both stored and exchanged using the application. One of the standards that can be used to evaluate the security of secure chat applications is the Common Criteria for IT Security Evaluation Version 3.1 Revision 5:2017 (CC), especially the Common Criteria Evaluation Methodology Version 3.1 Revision 5:2017 (CEM). In this study, an evaluation of the security of the PeSankita application has been carried out in the Assurance Vulnerability Assessment (AVA) class, which is an assessment class of vulnerabilities that may be contained in the application as a Target of Evaluation (TOE). The evaluation was carried out based on data regarding TOE that has been obtained previously. The results obtained from the testing process accompanied by evaluation evidence indicate that TOE, in this case PeSankita, is not as claimed by the application developer because basic level attacks are still found in the PeSankita application version 1.4.23 on client code quality and reverse engineering testing.

Keywords: *Common Criteria, Criteria Evaluation*, AVA class, PeSankita, TOE

.

1. PENDAHULUAN

Pemanfaatan Internet sebagai media komunikasi turut berperan sebagai motivasi dilakukannya inovasi pada teknologi *instant messaging* atau perpesanan instan. Beragam aplikasi perpesanan instan (*instant messenger*) dirancang agar dapat memudahkan dan mengefisienkan aktivitas komunikasi penggunanya. Beberapa aplikasi *instant messenger* seperti WhatsApp, Telegram, Line, dan WeChat sangat populer di Indonesia, namun tidak satu pun dari aplikasi tersebut yang merupakan produk lokal [1]. Padahal kehadiran produk local tentu akan mendukung kemajuan Indonesia dan mewujudkan kedaulatan bangsa Indonesia melalui kemandirian teknologi. Dalam rangka tujuan tersebut, XecureIT yang merupakan salah satu perusahaan IT lokal, mengembangkan aplikasi *instant messenger* PeSankita yang diklaim sebagai aplikasi pengirim pesan yang aman alias *secure chat* [2].

Sebelum disebarluaskan ke publik, suatu aplikasi *instant messenger* hendaknya dievaluasi untuk mengetahui kelayakan aplikasi tersebut. Evaluasi keamanan aplikasi menjadi sangat penting untuk membentuk kepercayaan pengguna terhadap keamanan data yang disimpan ataupun dipertukarkan. Badan Siber dan Sandi Negara (BSSN) merupakan lembaga pemerintah yang berfungsi melaksanakan sertifikasi dan pengujian produk keamanan perangkat teknologi informasi, melalui Subdirektorat Fasilitasi Standardisasi dan Sertifikasi Keamanan Perangkat TI, Direktorat Pemantauan dan Pengendalian Produk Keamanan Siber dan Sandi, Deputi Bidang Pemantauan dan Pengendalian [3]. Salah satu standar yang dapat digunakan dalam penilaian kesesuaian spesifikasi keamanan produk tersebut adalah *Common*

Criteria for IT Security Evaluation Version 3.1 *Revision* 5:2017 (CC), dengan metode pengujian *Common Criteria Evaluation Methodology Version* 3.1 *Revision* 5:2017 (CEM).

Kegiatan evaluasi keamanan dilakukan oleh evaluator melalui evaluasi keamanan produk Teknologi dan Informasi (TI) pada kelas *Security Assurance Requirements* (SAR) yang terdiri dari *Assurance Profile Evaluation* (APE), *Assurance Configuration Evaluation* (ACE), *Assurance Security Target Evaluation* (ASE), *Assurance Development* (ADV), *Assurance Guidance Documents* (AGD), *Assurance Life-Cycle Support* (ALC), *Assurance Test* (ATE), dan *Assurance Vulnerability Assessment* (AVA) [4]. AVA adalah kelas penilaian keamanan berupa analisis kerentanan yang mungkin terdapat dalam aplikasi yang menjadi *Target of Evaluation* (TOE), di mana kerentanan tersebut bisa saja muncul pada saat pengembangan ataupun dalam pengoperasian produk. Evaluasi dilakukan berdasarkan data-data mengenai TOE yang didapatkan sebelumnya. Hasil yang didapatkan dari proses pengujian beserta bukti evaluasi akan digunakan untuk memvalidasi tingkat keamanan TOE. Evaluator harus mendokumentasikan setiap tahapan yang dilakukan.

Berkaitan dengan hal tersebut, pada penelitian ini telah dilakukan evaluasi keamanan pada kelas AVA terhadap aplikasi PeSankita berdasarkan CEM. Evaluasi kelas AVA dilakukan oleh peneliti yang selanjutnya disebut sebagai evaluator yang mencari kerawananan aplikasi PesanKita sebagai TOE berdasarkan klaim keamanan dari pihak pengembang dan pencarian dari sumber lain terkait TOE. Kemudian dari kerawanan yang telah teridentifikasi dilakukan pengujian untuk membuktikan keamanan TOE. Hasil dari pengujian yang disertai dengan bukti pengujian menjadi penilaian apakah TOE sudah menerapkan fungsi keamanannya sesuai dengan klaimnya atau belum.

2. LANDASAN TEORI

Bagian ini membahas konsep dan teori yang berkaitan dan mendukung penelitian, yaitu *Common Criteria for IT Security Evaluation Version* 3.1 *Revision* 5:2017 dan *Common Evaluation Methodology for IT Security Evaluation Version* 3.1 *Revision* 5:2017, *Assurance Vulnerability Assessment*, dan PeSankita.

2.1. *Common Criteria* (CC) dan *Common Evaluation Methodology*

CC merupakan standar evaluasi keamanan produk teknologi informasi (TI). Dokumen CC mengatur mengenai persyaratan keamanan suatu produk dan ukuran jaminan bahwa kebutuhan keamanan tersebut telah diterapkan pada produk TI [5]. dokumen CC terdiri dari 3 bagian, yaitu [5]:

a. *Common Criteria part* I, memuat pengenalan dokumen CC, konsep dan prinsip umum evaluasi, dan pengenalan model umum evaluasi
b. *Common Criteria part* II, memuat *Security Functional Requirements* (SFR) atau *template* standar seperangkat komponen fungsional TOE.
c. *Common Criteria part* III, memuat *Security Assurance Requirements* (SAR) atau *template* standar seperangkat komponen jaminan TOE.

Selain ketiga dokumen tersebut, dokumen pendukung yang dapat digunakan adalah *Common Evaluation Methodology* (CEM). Dokumen ini berisi penjelasan mengenai metodologi untuk melakukan evaluasi keamanan produk TI mengunakan CC sebagai dasarnya. Proses evaluasi keamanan suatu produk bertujuan untuk membentuk tingkat kepercayaan dan memastikan bahwa fungsionalitas keamanan pada suatu produk telah diterapkan dengan benar dan telah sesuai dengan persyaratan keamanan yang ditentukan [5].

2.2. *Assurance Vulnerability Assessment* (AVA)

AVA merupakan salah satu kelas pada SAR yang bertujuan untuk menilai kerentanan yang mungkin terdapat dalam TOE pada saat fase pengembangan ataupun dalam pengoperasian produk. Evaluasi kerentanan pada kelas AVA menggunakan komponen penjaminan AVA_VAN. Pada evaluasi kerentanan pengembangan produk, celah keamanan dapat diperoleh dengan melihat fitur keamanan yang diimplementasikan pada produk.

Kelas AVA memiliki satu famili yang disebut *vulnerability analysis* atau dalam dokumen CC ini dikodekan mejadi VAN. Famili ini memiliki 5 level yang dikodekan dengan AVA_VAN.1 sampai dengan AVA_VAN.5, di mana setiap level memiliki perbedaan kebutuhan persyaratan dalam melakukan pengujian, semakin besar level semakin banyak persyaratan yang dibutuhkan dalam melakukan pengujian, seperti yang terlampir pada dokumen CEM. Pada AVA_VAN.2, evaluator membutuhkan data mengenai kerawanan dari produk TI dengan mencari infromasi kerawanan secara publik (misal: dideskripsikan pada web), dan ditambahkan dengan ancaman potensial pada fungsi keamanan pada aplikasi yang telah diidentifikasi oleh pengembang produk TI yang akan dievaluasi.

Pada penelitian ini, diperoleh informasi berdasarkan literatur bahwa pihak pengembang mengklaim fitur keamanan yang diterapkan pada aplikasi PeSankita adalah *Evaluation Assurance Level* (EAL) 2 [6]. Artinya pihak pengembang telah menerapkan fitur keamanannya dan menjamin tingkat evaluasinya tahan pada tingkat 2. Oleh karena itu, evaluasi keamanan yang dilakukan pada penelitian ini dilakukan pada AVA.VAN.2 yang bertujuan untuk membuktikan klaim dari pengembang mengenai aplikasinya.

Kelas AVA_VAN.2 memiliki beberapa langkah dalam proses evaluasi yaitu:

1. Pemeriksaan TOE dan Dokumen ST, ADV, dan AGD
2. Memastikan TOE terkonfgurasi sesuai AGD dan melakukan pencarian kerawanan dengan memanfaatkan informasi secara publik. Pada penelitian ini, langkah ini menggunakan OWASP *Mobile Top Ten Porject* [7].
3. Pencarian potensial ancaman memanfaatkan dokumen ST dan ADV.
4. Menyusun kandidat pengujian
5. Melakukan pengujian TOE
6. Melakukan penghitungan *attack potential calculation* (APC).

2.3. Penghitungan APC

Attack Potential Calculation (APC) atau kalkulasi potensi serangan merupakan penghitungan nilai serangan yang dilakukan oleh evaluator yang digunakan pada saat melakukan pengujian pada proses evaluasi TOE [4]. APC digunakan untuk mengukur pengujian yang dilakukan oleh evaluator sesuai dengan analisis kerentanan untuk menentukan apakah TOE tahan terhadap serangan dengan asumsi potensi serangan yang sama, kurang atau pun melebihi dari perhitungan APC dibandingkan dengan komponen AVA.

Pada Tabel 1, 2 dan 3 diberikan rangkuman beberapa hal yang terkait APC yakni nilai potensi serangan, tingkat ketahanan TOE, dan nilai faktor APC.

Tabel 1. Nilai Potensi Serangan [4]

Potensi Serangan	Nilai
Dasar	0-9
Di atas Dasar	10-13
Menengah	14-19
Tinggi	20-24
Di atas Tinggi	≥25

Tabel 2. Ketahanan Komponen terhadap Potensi Serangan [4]

Komponen AVA	Tingkat Ketahanan TOE	Kerawanan *residual*
VAN.1	Dasar	Di atas Dasar
VAN.2	Dasar	Di atas Dasar
VAN.3	Diatas Dasar	Menengah
VAN.4	Menengah	Tinggi
VAN.5	Tinggi	Lebih dari tinggi

Pada Tabel 3, terdapat beberapa istilah yang dijelaskan sebagai berikut:

Waktu Dibutuhkan merupakan jumlah total waktu yang digunakan oleh penyerang unutk mengidentifikasi potensi kerentanan tertentu yang terdapat pada TOE.

Keahlian mengacu pada tingkat pengetahuan umum dari prinsip dasar, tipe produk atau metode serangan. Tingkat identifikasi keahlian dari paling rendah ke paling tinggi adalah sebagai berikut:

a. Awam, tanpa keahlian khusus
b. Mahir, berpengetahuan mengenai keamanan pada suatu produk
c. Ahli, terbiasa dengan algoritme, protokol, konsep keamananan dan metode serangan pada suato produk
d. Beragam Keahlian, memiliki keahlian yang beragam dalam menghadapi situasi pada tingkat ahli

Tabel 3. Nilai Faktor APC [4]

Faktor	Nilai
Waktu dibutuhkan	
≤satu hari	0
≤ dua hari	1
≤ dua minggu	2
≤ satu bulan	4
≤ dua bulan	7
≤ tiga bulan	10
≤ empat bulan	13
≤lima bulan	15
≤enam bulan	17
> Enam bulan	19
Keahlian	
Awam	0
Mahir	3
Ahli	6
Beragam keahlian	8
Pengetahuan terhadap TOE	
Publik	0
Terbatas	3
Sensitif	7
Kritikal	11
Jendela Peluang	
Akses tidak perlu / tidak terbatas	0
Mudah	1
Moderat	4
Susah	10
Tidak ada	
Peralatan	
Standar	0
Spesialis	4
Bespoke	7

Pengetahuan terhadap TOE diartikan sebagai keahlian spesifik yang bersangkutan dengan TOE. Tingkatan yang teridentifikasi adalah sebagai berikut:

a. Publik, informasi yang diperoleh dari publik
b. Terbatas. Informasi mengenai prodk dikendalikan pada organisasi dan berdasarkan perjanjian non-pengungkapan.
c. Sensitif, Informasi hanya dimiliki oleh suatu tim dan dibatasi aksesnya hanya pada anggota tim
d. Kritikal, Informasi dimiliki oleh beberapa individu dan dikontrol ketat.

Jendela Peluang merupakan tingkatan dari kesempatan yang diberikan kepada penyerang untuk melakukan akses pada TOE dalam rangka melakukan pengujian. Tingkatan diidentifikasi sebagai berikut :

a. Akses tidak terbatas, serangan tidak ada resiko untuk terdeteksi dan tidak masalah untuk melakukan akses terus-menerus

b. Mudah, serangan diperlukan akses kurang dari satu hari dengan jumlah akses kurang dari sepuluh kali
c. Moderat, serangan diperlukan akses kurang dari satu bulan dengan jumlah akses kurang dari seratus
d. Sulit, serangan diperlukan akses selama satu bulan dengan jumlah akses setidaknya seratus
e. Tidak ada, lamanya waktu dimana aset yang akan dieksploitasi kurang dari lamanya waktu peluang yang diperlukan untuk melakukan serangan.

Peralatan merupakan perangkat yang dibutuhkan untuk mengidentifikasi dan mengeksploitasi kerentanan.
a. Standar, peralatan yang tersedia mudah diperoleh
b. Spesialis, peralatan yang tersedia didapatkan dengan membeli
c. Multiple Bespoke, peralatan dipesan lebih dahulu diperlukan untuk langkah-lagkah serangan yang berbeda.

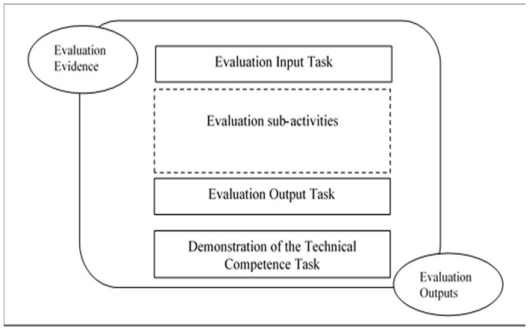
2.4. Aplikasi PESANKITA

PeSankita adalah aplikasi *secure chat* berbasis system operasi Android yang dikembangkan oleh salah satu perusahaan IT indoensia yaitu XecureIT [8]. Protokol kriptografi yang digunakan pada aplikasi ini adalah *signal,* dengan algoritme enkripsi AES-256 untuk menyediakan penamanan transmisi data, dan *DoubleRatchet* sebagai protokol pertukaran kunci. Pembagkitan kunci enkripsi pada aplikasi ini dilakukan menggunakan algortima X3DH, VedSA, dan VXEdSA [8].

3. METODE PENELITIAN

3.1. Metode Penelitian

Metode penelitian yang digunakan adalah CEM. Berdasarkan CEM, terdapat 4 hal yang dilakukan dalam melakukan proses evaluasi sebagaimana diberikan pada Gambar 1, yaitu *evaluation input task, evaluation sub-activities, evaluation output task,* dan *demontration of the technical.*



Gambar 1. Skema umum evaluasi [4]

Evaluasi keamanan yang dilakukan pada penelitian ini adalah analisis kerentanan berdasarkan AVA_VAN.2. Dalam hal ini, AVA_VAN.2 memiliki empat tahapan yang sesuai dengan skema umum evaluasi. Penjelasan ringkas keempat tahapan tersebut dirangkum pada Tabel 4.

Tabel 4. *Action Element*

Komponen	*Identifier*	*Action element*
AVA_ VAN.2	AVA_ VAN.2.1E	Evaluator memastikan informasi yang didapatkan sesuai TOE.
	AVA_ VAN.2.2E	Evaluator melakukan pencarian informasi sumber publik untuk mengidentifikasi potensi kerentanan dalam TOE.
	AVA_ VAN.2.3E	Evaluator melakukan analisis ancaman terhadap TOE menggunakan dokumen pendukung
	AVA_ VAN.2.4.E	Evaluator melakukan pengujian penetrasi untuk menentukan bahwa TOE tahan terhadap serangan potensi serangan Dasar.

3.2. Tahapan Penelitian

Berdasarkan dokumen CEM, terdapat 4 tahapan yang dilakukan oleh evaluator dalam melakukan proses evaluasi AVA_VAN.2 sebagaimana ditunjukkan pada Gambar 1. Penjelasan keempat tahapan tersebut diberikan pada bagian berikut ini.

3.2.1. *Evaluation Input Task*

Evaluation Input Task adalah tahapan pengumpulan hal-hal yang dibutuhkan pada saat proses evaluasi. Selain pengumpulan informasi, pada tahap ini juga dilakukan pemeriksaan untuk memastikan kesesuaian aplikasi TOE dengan *evaluation evidence.* Tabel 5 merangkum tahapan *evaluation input task* yang dipetakan pada *action element identifier* kelas AVA, dan dirincikan dengan penjelasan *work unit*.

Tabel 5. Tahap *Evaluation Input Task*

Action Element Identifier	*Action*	*Work unit*
AVA_ VAN.2.1E	AVA_ VAN.2-1	Evaluator memeriksa TOE untuk menentukan konfigurasi konsisten dengan ST
	AVA_ VAN.2-2	Evaluator memeriksa TOE untuk menentukan TOE dipasang dengan benar
AVA_ VAN.2.2E	AVA_ VAN.2-3	Evaluator mencari sumber informasi tersedia secara umum untuk mengidentifikasi potensi kerentanan dalam TOE

3.2.2. *Evaluation Sub-Activities* dan *Evaluation Output Task*

Evaluation sub-activities (AVA_VAN.2) merupakan tahapan penilaian kerentanan yang mungkin terdapat pada TOE berdasarkan *input task* yang telah didapatkan. Setelah *Evaluation sub-activities* dilakukan, selanjutnya evaluator menyusun *evaluation output task* yaitu pelaporan yang berisi deskripsi lengkap mengenai hasil evaluasi.

Berdasarkan dokumen CEM, langkah yang dilakukan pada tahap ini adalah seperti pada Tabel 6.

Tabel 6. Tahap *Evaluation Output Task*

Action Element Identifier	*Action*	*Work Unit*
AVA_ VAN.2.3.E	AVA_ VAN.2-4	Evaluator mengidentifikasi ancaman berdasarkan dokumen ST, ADV, dan AGD.
	AVA_ VAN.2-5	Evaluator mencatat kandidat pengujian TOE
AVA_ VAN.2.4.E	AVA_ VAN.2-6	Evaluator merencanakan uji penetrasi berdasarkan kandidat pengujian
	AVA_ VAN.2-7	Evaluator menghasilkan dokumentasi persiapan uji penetrasi
	AVA_ VAN.2-8	Evaluator melakukan uji penetrasi
	AVA_ VAN.2-9	Evaluator mencatat hasil aktual dari uji
	AVA_ VAN.2-10	Evaluator melaporkan upaya pengujian dan konfigurasi uji
	AVA_ VAN.2-11	Evaluator memeriksa hasil uji untuk menghitung APC
	AVA_ VAN.2-12	Evaluator melaporkan hasil uji yang dapat dieksploitasi

3.2.3. *Demonstration of Technical Competence Task*

Pada tahap ini, seorang evaluator melakukan demontrasi untuk menunjukkan proses dari hasil yang didapatkan pada proses evaluasi.

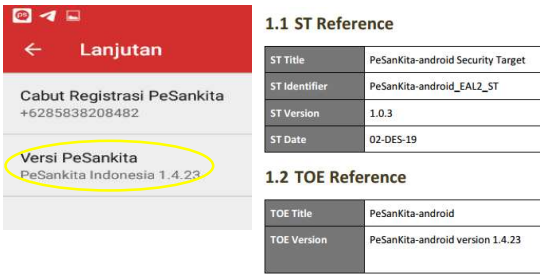
4. HASIL DAN PEMBAHASAN

Pada bagian ini dibahas mengenai proses dan hasil setiap tahap dalam evaluasi keamanan aplikasi yang menjadi TOE berdasarkan pada elemen tindakan evaluator pada dokumen CC dan CEM.

4.1. *Evaluation Input Task*

Pada tahap ini hanya terdapat 1 *action element* yaitu AVA_VAN.2.1.E. Beberapa hal yang dibutuhkan pada saat proses evaluasi yaitu dokumen ST, ADV, dan AGD. Selain pengumpulan data, juga dilakukan pemeriksaan TOE terhadap dokumen ST pada *work unit* AVA_VAN.2-1. Pemeriksaan TOE didasarkan pada dokumen AGD pada *work unit* AVA_VAN.2-2, serta pencarian secara publik mengenai informasi pendukung untuk mengidentifikasi kerawanan TOE pada *work unit* AVA_VAN.2-3.

Pada *work unit* AVA_VAN.2-1 dilakukan pemeriksaan TOE pada dokumen ST. Pemeriksaan yang dilakukan adalah kesesuaian versi dokumen ST dengan aplikasi PeSankita dan kesesuaian konfigurasi sistem minimum yang dibutuhkan untuk menjalankan TOE berdasarkan dokumen ST. Hasil penelitian menunjukkan bahwa tahapan ini telah terpenuhi sebagaimana ditampilkan pada Gambar 2 dan Tabel 7.



Gambar 2. Pemeriksaan TOE terhadap ST

Pada *work unit* AVA_VAN.2-2 dilakukan proses konfigurasi aplikasi sesuai dengan pedoman dari dokumen AGD. Tahapan proses konfigurasi pada PeSankita dimulai dengan melakukan pencarian aplikasi pada *platform* PlayStore, instalasi aplikasi, registrasi, dan verifikasi. Seluruh tahapan tersebut telah dilakukan mengikuti panduan dari dokumen AGD.

Tabel 7. Pemeriksaan Konfigurasi Sistem Berdasarkan Persyaratan Minimum Sistem

No	Komponen	Persyaratan Minimum	Spesifikasi Sistem
1	Ssitem Operasi	Andorid System versi 5.0 (Lollipop)	Andorid System versi 5.1.1 (Lollipop)
2	Memory	1 GB RAM	1 GB RAM
3	Processor	Arm-68v8, Armeabi-v7A, Intel x86, dan Intel x86_64	Armeabi v7A
4	Penyimpanan	128 MB	60 GB
5	Pendukung	SDK versi 19	SDK versi 22

Pada *work unit* AVA_VAN.2-3 dilakukan pencarian informasi pada ranah publik sebagai pendukung dalam mengidentifikasi kerawanan potensial pada aplikasi. Pada tahap ini peneliti memanfaatkan buku yang diterbitkan oleh organisasi *Open Web Application Security Project* (OWASP) yaitu *Mobile Security Testing Guide* (MSTG). Buku ini dibuat berdasarkan pemetaan OWASP mengenai 10 kerawanan yang sering terjadi pada aplikasi *Mobile* yaitu OWASP *Mobile Top Ten.*

Pada tahap ini juga dilakukan pemindaian terhadap aplikasi PeSankita menggunakan *Mobile Security Framework* (MOBSF) untuk mendapatkan kerawanan potensial yang terdapat pada aplikasi. Berdasarkan pemindaian yang telah dilakukan didapatkan empat kerawanan pada aplikasi Pesan Kita, yaitu *insecure data storage, insufficient cryptography, client code quality,* dan *reverse engineering.*

4.2. *Evaluation Sub-Activities Task* dan *Evaluation Output Task*

Pada tahapan ini terdapat dua *action element* yaitu AVA_VAN.2.3.E dan AVA_VAN.2.4.E. Masing-masing *action element* memilik sejumlah *work unit.*

Pada *action element* AVA_VAN.2.3.E terdapat 2 *work unit* yaitu AVA_VAN.2-4 dan AVA_VAN_2-5. *Action element* AVA_VAN.2-4 memiliki 6 *work unit* yaitu AVA_VAN.2-6, AVA_VAN.2-7, AVA_VAN.2-8, AVA_VAN.2-9, AVA_VAN.2-10, AVA_VAN.2-11, dan AVA_VAN.2-12

Pada *work unit* AVA_VAN.2-4 dilakukan pencarian potensi ancaman melalui dokumen ST. Pada dokumen ST terdapat penjelasan mengenai fitur kemananan aplikasi PeSankita. Dari fitur keamanan yang terdapat pada aplikasi PeSankita maka terdapat skenario ancaman pada aplikasi. Hal tersebut kemudian menjadi kandidat pengujian pada evaluasi ini.

Pada dokumen ST disebutkan bahwa terdapat beberapa fitur kemanan yang diterapkan. Fitur-fitur kemanan tersebut adalah *Identification and Authentication, Cryptographic Operation* dan *User Data Protection* [9]. Oleh karena itu, skenario ancaman dari pengujian aplikasi PeSankita adalah *Insecure communication* untuk fitur keamanan *Identification and Authentication, Insufficient cryptography* untuk fitur keamanan *Insufficient cryptography* dan *Insecure data storage* untuk fitur keamanan *User Data Protection*.

Pada *work unit* AVA_VAN.2-5 dilakukan pencatatan kandidat pengujian. Kandidat pengujian tersebut ditentukan berdasarkan pada *work unit* AVA_VAN.2-3 dan AVA.VAN.2-4. Pada AVA_VAN.2-3 ditemukan kerawanan yaitu *Insecure data storage, Insufficient cryptography, Client code quality, Reverse engineering* sedangkan pada *work unit* AVA_VAN.2-4 ditemukan kerawanan berupa *Insecure communication, Insufficient cryptography* dan *Insecure data storage.* Dua diantaranya telah teridentifikasi sebagai kerawanan pada AVA_VAN.2-3. Oleh karena itu, kandidat pengujiannya adalah *Insecure data storage* (1)*, Insufficient cryptography* (2)*, Client code quality* (3)*, Reverse engineering* (4), dan *Insecure Communication* (5).

Untuk *work unit* AVA_VAN.2-6, persiapan pengujian terhadap kandidat pengujian yang telah ditentukan sebelumnya adalah melakukan pemasangan dan konfigurasi alat yang dibutuhkan dalam proses pengujian. Alat-alat yang digunakan pada proses pengujian adalah sebagai berikut:

1. NoxPlayer [10]
2. GenyMotion [11]
3. MOBSF [12]
4. Drozer [13]
6. ADB [15]
7. Apktool [16]
8. Apk Signer [17]
9. Xposed Installer [18]

Pada *work unit* AVA_VAN.2-7 dilakukan persiapan pengujian yaitu dengan mengkonfigurasi alat-alat yang digunakan dalam pengujian. Selain, itu, ditentukan juga hasil yang diharapkan dari setiap pengujian yang akan dilakukan. Hasil yang diharapkan yang ditentukan pada tahap selanjutnya digunakan untuk menentukan apakah pengujian berhasil mengeksplotasi aplikasi.

Pada Tabel 8 dirangkum mengenai *work unit* ini. Pengujian aplikasi PesanKita dilakukan berdasarakan lima kandidat yang telah ditentukan sebelumnya pada *work unit* AVA_VAN.2-5 menggunakan peralatan dan konfigurasi yang telah dilakukan pada *work unit* AVA_VAN.2-6 dan AVA_VAN.2-7. Rangkuman penjelasan ke-5 kandidat pengujian, alat yang diperlukan, dan pengujian yang dilakukan dirangkum pada Tabel 9.

Tabel 8. *Work unit* AVA_VAN.2-7

Kandidat Pengujian	Konfigurasi alat	Hasil diharapkan
1	Konfigurasi NoxPlayer dan ADB	Mendapat informasi kredensial yang disimpan
2	*Text editor*	Menemukan algoritme lemah sehingga dapat dimanfaatkan untuk eksploitasi
3	Drozer	*Activity* dapat di-*bypass* dan ditemukan kerentanan injeksi
4	Apktool	Mendapatkan kode sumber aplikasi dan memodifikasi
5	Fiddler4, NoxPlayer, dan Xposed Installer	Menangkap paket data sehingga mendapatkan informasi sensitif

Tabel 9. *Work unit* AVA_VAN.2-8

Kandidat Pengujian	Alat diperlukan	Pengujian yang dilakukan
1	ADB, dan SQLite Manager	Membuka direktori aplikasi pada penyimpanan basis data, kemudian mengambil basis data tersebut dan membukanya.
2	*Text editor*	Menemukan kode sumber pada aplikasi yang menyatakan algoritme SHA-1 digunakan.
3	Drozer	Melakukan *bypass activity* dengan melakukan *export activity* dengan drozer
4	Apktool, dan *Text editor*	Memecah file apk sehigga didapatkan kode sumber kemudian memodifikasi kode sumber tersebut agar memerpcayai *certificate authority* yang ada pada perangkat android.
5	Fiddler dan Xposed Installer	Melakukan penangkapan paket data menggunakan Fiddler dengan melakukan *SSLUnpinning* terlebih dahulu.

Pada *work unit* AVA_VAN.2-9 dilakukan pencatatan terhadap hasil yang didapatkan pada *work unit* AVA.VAN.2-8. Setelah dilakukan pencatatan hasil yang didapatkan akan dibandingkan dengan hasil yang diharapkan yang telah ditentukan sebelumnya. Pada Tabel 10 dirangkum perbandingan hasil yang didapatkan dengan hasil yang diharapkan.

Pada *work unit* AVA_VAN.2-10 dilakukan penguraian pengujian yang telah dilakukan pada *work unit* AVA_VAN.2-8. Hal- hal yang diuraikan adalah konfigurasi uji, TOE *Security Functionality Interface*

(TSFI), dan penilaian pengujian yang dilakukan sebagaimana dirangkum dalam Tabel 11.

Tabel 10. Perbandingan Hasil

Kandidat Pengujian	Hasil yang diharapkan	Hasil yang diperoleh
1	Mendapat informasi kredensial yang disimpan	Mendapat beberapa data : 1. Nomor telepon pengguna 2. Nomor telepon penerima pesan 3. Komponen kriptografi (*encryption salt, master secret, asymetric master secret curve 25519*) terenkripsi 4. Empat basis data dengan dua diantaranya terenkripsi
2	Menemukan algoritme lemah sehingga dapat dimanfaatkan untuk eksploitasi	Ditemukan algoritme lema yang digunakan yaitu SHA-1 dimana SHA-1 Telah memiliki kolisi.
3	*Activity* dapat di-*bypass* dan ditemukan kerentanan injeksi	1. *Activity* pada aplikasi dapat di-*bypass* 2. Tidak ditemukan kerawanan injeksi
4	Mendapatkan kode sumber aplikasi dan memodifikasi	Aplikasi berhasil dimodifikasi
5	Menangkap paket data sehingga mendapatkan infromasi sensitif	Fiddler4 dapat menangkap paket-paket data yang ditransmisikan akan tetapi tidak didapatkan informasi sensitif.

Tabel 11. Pelaporan Pengujian

Kandidat Pengujian	Konfigurasi	TSFI	Penilaian
1	Menghubungkan adb dengan NoxPlayer	Antarmuka pengguna	Tidak didapatkan informasi sensitif
2	Melakukan pemecahan file apk menjadi kode sumber	Antarmuka non-pengguna	Didapatkan algoritme SHA-1 yang digunakan
3	Menghubungkan drozer *console* dan *agent*	Antarmuka pengguna	Terdapat *activity* yang di-*bypass*
4	Pemasangan apktool dan apksigner	Antarmuka pengguna	*Reverse engineering* berhasil dilakukan dan aplikasi berhasil dimodifikasi
5	Pemasangan sertifikat Fiddler4, memodifikasi proxy, dan konfigurasi Xposed Installer	Antarmuka pengguna	SSL *pinning* dapat di *bypass* akan tetapi tidak didapatkan informasi sensitif

Pada *work unit* AVA_VAN.2-11 diperiksa kembali hasil semua pengujian yang telah dilakukan. Kemudian, akan ditentukan APC dengan penghitungan digunakan untuk melihat ketahanan terhadap tingkat serangan tertentuk. Hal ini untuk menentukan keberhasilan aplikasi dalam proses evaluasi yang dilakukan. Hasil penghitungan APC dari pengujian yang dilakukan diberikan pada Tabel 12.

Tabel 12. Faktor dan Nilai Penghitungan APC

Insecure data storage	
Faktor	**Nilai**
Waktu dibutuhkan	4
Keahlian	1
Pengetahuan Terhadap TOE	3
Jendela Peluang	0
Peralatan	1
Total	9
Insufficient cryptography	
Faktor	**Nilai**
Waktu dibutuhkan	4
Keahlian	0
Pengetahuan Terhadap TOE	3
Jendela Peluang	0
Peralatan	0
Total	7
Client code quality	
Faktor	**Nilai**
Waktu dibutuhkan	4
Keahlian	2
Pengetahuan Terhadap TOE	3
Jendela Peluang	0
Peralatan	0
Total	9
Rerverse engineering	
Faktor	**Nilai**
Waktu dibutuhkan	4
Keahlian	3
Pengetahuan Terhadap TOE	2
Jendela Peluang	0
Peralatan	0
Total	9
Insecure Communication	
Faktor	**Nilai**
Waktu dibutuhkan	4
Keahlian	1
Pengetahuan Terhadap TOE	3
Jendela Peluang	0
Peralatan	0
Total	8

Tabel 13. Pelaporan Hasil

Pengujian	Sumber	Keberhasilan	APC
1	Buku	Tidak tereksploitasi	9
2	Buku	Tidak tereksploitasi	7
3	Buku	Tereksploitasi	9
4	Buku	Tereksploitasi	9
5	Buku	Tidak tereksploitasi	8

Pada *work unit* AVA_VAN.2.12 diperoleh hasil uji penetrasi yang dilakukan dapat dieksploitasi atau tidak dapat dieksploitasi, kemudian dijelaskan mengenai pengujian TOE yang dilakukan evaluator diketahui sumbernya, keberhasilan, dan hasil penghitungan APC. Berdasarkan hasil pada Tabel 13 dijelaskan bahwa terdapat 2 (dua) pengujian yang tereksploitasi dengan tingkat serangan dasar yaitu pengujian 3 dan 4. Adapun pengujian 1, 2, dan 5 tidak dapat tereksploitasi dengan tingkat serangan dasar.

4.3. *Demonstration of The Technical Competence Task*

Pada tahap ini, evaluator melakukan demonstrasi untuk menjelaskan mengenai proses pengujian yang telah dilakukan. Demonstrasi dilakukan dengan mengirimkan video yang menunjukkan proses pengujian. Dari hasil demontrasi yang telah dilakukan, tahapan ini dinyatakan berhasil oleh penguji.

5. KESIMPULAN

Berdasarkan evaluasi yang telah dilakukan, didapatkan lima kandidat pengujian. Dari lima kandidat pengujian kemudian pengujian dilakukan sehingga didapatkan hasil tiga pengujian dengan tingkat serangan dasar tidak berhasil dieksploitasi dan dua pengujian dengan tingkat serangan dasar berhasil dieksplotasi. Berdasarkan hasil kajian, dapat disimpulkan bahwa aplikasi PeSankita versi 1.4.23 belum berhasil dalam evaluasi keamanan berdasarkan kelas AVA_VAN.2 karena masih terdapat serangan dasar yang belum dimitigasi.

REFERENSI

[1] R. Manasse, "10 Aplikasi Chatting Terbaru & Terbaik untuk HP Android 2019," JalanTikus, 12 Januari 2019. [Online]. Available: https://jalantikus.com/tips/aplikasi-chatting/. [Accessed 23 November 2019].

[2] BisnisNews, "Aplikasi Alternatif PesanKita Lebih Aman Pengganti WhatsApp," Bisnis News, 15 April 2019. [Online]. Available: http://bisnisnews.id/detail/berita/aplikasi-alternatif-pesankita-lebih-aman-pengganti-whatsapp. [Accessed 23 November 2019].

[3] Kepala Badan Siber dan Sandi Negara, Peraturan Badan Siber Dan Sandi Negara Nomor 2 Tahun 2018 Tentang Organisasi Dan Tata Kerja Badan Siber Dan Sandi Negara, Indonesia, 2018.

[4] Common Criteria, Common Evaluation Methodology for Information Technology Security Evaluation, 2017.

[5] Common Criteria, Common Criteria for Information Technology Security Evaluation Part 1 : Introduction and general model, 2017.

[6] D422 BSSN, "PesanKita-android SECURITY TARGET v 1.0.2," BSSN, Depok, 2019.

[7] https://owasp.org/www-project-mobile-top-10/

[8] A. Amiruddin dan M. F. Rohmani, "Perancangan Spesifikasi Keamanan untuk Pengembangan Aplikasi Secure Chat Berdasarkan Common Criteria for It Security Evaluation," JTIIK, Vol 8 ed. 6, 2021, Bogor, 2019.

[9] D422 BSSN, "PeSankita-android Architecture and Design Implementation v 1.0.0," BSSN, Depok, 2019.

[10] https://www.techspot.com/downloads/6751-nox-app-player.html

[11] https://www.genymotion.com/

[12] https://github.com/MobSF/Mobile-Security-Framework-MobSF

[13] https://labs.withsecure.com/tools/drozer

[14] https://www.telerik.com/fiddler

[15] https://developer.android.com/studio/command-line/adb

[16] https://ibotpeaches.github.io/Apktool/

[17] https://play.google.com/store/apps/details?id=com.haibison.apksigner&hl=en&gl=US

[18] https://repo.xposed.info/module/de.robv.android.xposed.installer