MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA

PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA
NOMOR TAHUN 2015

TENTANG

PERANGKAT LUNAK SISTEM ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA
MENTERI KOMUNIKASI DAN INFORMATIKA,

Menimbang :

a. bahwa untuk melaksanakan Ketentuan Pasal 7 ayat (2) Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, perlu menetapkan Peraturan Menteri tentang Persyaratan Perangkat Lunak Sistem Elektronik;
b. bahwa Sistem Elektronik berdasarkan asas Risiko terbagi menjadi: Sistem Elektronik Strategis, Sistem Elektronik Tinggi dan Sistem Elektronik Rendah berdasarkan ketentuan Pasal 3 ayat (1) Peraturan Menteri Komunikasi dan Informatika No (...) Tahun 2015 Tentang Sistem Manajemen Pengamanan Informasi;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b perlu menetapkan Peraturan Menteri Komunikasi dan Informatika tentang Persyaratan Perangkat Lunak Sistem Elektronik.

Mengingat :

1. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843);
2. Undang-Undang Republik Indonesia Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038;
3. Undang-Undang Republik Indonesia Nomor 38 Tahun 2009 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);
4. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);
5. Peraturan Menteri Komunikasi dan Informatika Nomor: 17/PER/M.KOMINFO/10/2010 tentang Organisasi dan Tata Kerja Kementerian Komunikasi dan Informatika.

MEMUTUSKAN:

Menetapkan : PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA TENTANG PERANGKAT LUNAK SISTEM ELEKTRONIK.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Menteri ini yang dimaksud dengan:

1. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
2. Penyelenggara Sistem Elektronik, yang selanjutnya disebut PSE adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada Pengguna Sistem Elektronik untuk keperluan dirinya, dan/atau keperluan pihak lain.
3. Pelayanan Publik adalah kegiatan atau rangkaian kegiatan dalam rangka pemenuhan kebutuhan pelayanan sesuai dengan peraturan perundangundangan bagi setiap warga negara dan penduduk atas barang, jasa, dan/atau pelayanan administratif yang disediakan oleh penyelenggara pelayanan publik.
4. Penyelenggara Sistem Elektronik untuk pelayanan publik, yang selanjutnya disebut PSE Pelayanan Publik meliputi Institusi penyelenggara negara yang terdiri dari lembaga negara dan/atau lembaga pemerintahan dan/atau Satuan Kerja Penyelenggara di lingkungannya; Korporasi berupa Badan Usaha Milik Negara dan/atau Badan Usaha Milik Daerah dan/atau Satuan Kerja Penyelenggara di lingkungannya; Lembaga independen yang dibentuk berdasarkan Undang-Undang dan/atau Satuan Kerja Penyelenggara di lingkungannya; atau Badan hukum lain yang menyelenggarakan Pelayanan Publik dalam rangka pelaksanaan Misi Negara.
5. Keamanan Informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi.
6. Perangkat Lunak adalah satu atau sekumpulan program komputer, prosedur, dan/atau dokumentasi yang terkait dalam pengoperasian Sistem Elektronik.
7. Standar adalah seperangkat aturan teknis yang harus dipatuhi suatu organisasi dalam rangka menerapkan pengamanan perangkat lunak.
8. Standar *The Open Web Application Security Project - Application Security Verification Standard* yang selanjutnya disingkat Standar OWASP ASVS adalah standar verifikasi teknis keamanan perangkat lunak dan lingkungannya untuk melindungi terhadap kerentanan.

9. Menteri adalah menteri yang ruang lingkup tugas dan fungsinya membidangi komunikasi dan informatika.
10. Direktur Jenderal adalah direktur jenderal yang ruang lingkup tugas dan fungsinya membidangi aplikasi informatika.

BAB II
ASAS DAN RUANG LINGKUP

Pasal 2

(1) Penerapan Perangkat Lunak Sistem Elektronik terhadap Penyelenggara Sistem Elektronik untuk Pelayanan Publik berdasarkan asas risiko.

(2) Ruang lingkup Perangkat Lunak Sistem Elektronik sebagaimana dimaksud pada ayat (1) mencakup semua kode termasuk kode sumber yang dikembangkan atau dimodifikasi dan dokumentasinya dalam rangka untuk menciptakan perangkat lunak.

BAB III
PERSYARATAN

Pasal 3

(1) Persyaratan Perangkat Lunak Sistem Elektronik terbagi 2 (dua) meliputi:
   a. Persyaratan Administrasi; dan
   b. Persyaratan Teknis.

(2) Persyaratan Administrasi sebagaimana dimaksud pada ayat 1 huruf a merupakan informasi yang harus dimiliki oleh perangkat lunak meliputi:
   a. Pengembang;
   b. Nama perangkat lunak;
   c. Versi;
   d. Jenis layanan;
   e. Rentang jumlah pemakai;
   f. Siklus hidup produk perangkat lunak yang meliputi: masa ketersediaan di pasaran (*General Availability*), Pemberitahuan masa berakhirnya produk (*End of Life Announcement),* masa terakhir pemesanan *(Last Order Date)*, masa berakhirnya produk (*End of Life)*, masa dukungan layanan pemeliharaan (*Maintenance Support)*, dan masa berakhirnya dukungan (*End of Support)*
   g. Berbasis web atau desktop; dan
   h. Sistem Operasi yang didukung.

(3) Persyaratan Teknis dalam Peraturan Menteri ini mengacu pada standar OWASP ASVS.

(4) Persyaratan Teknis dalam Peraturan Menteri ini tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

(5) Level Persyaratan Teknis sebagaimana dimaksud pada ayat (4) terdiri dari:

a. Level 1;
b. Level 2; atau
c. Level 3.

(6) Level Persyaratan Teknis sebagaimana dimaksud pada ayat (5) dilakukan melalui proses audit.

BAB IV
SISTEM ELEKTRONIK

Pasal 4

Sistem Elektronik berdasarkan asas Risiko dalam peraturan perundang-undangan terbagi menjadi:

a. Sistem Elektronik Strategis;
b. Sistem Elektronik Tinggi; dan
c. Sistem Elektronik Rendah.

BAB V
PENERAPAN PERSYARATAN PERANGKAT LUNAK SISTEM ELEKTRONIK

Pasal 5

Penyelenggara Sistem Elektronik wajib melakukan pendaftaran dengan menyerahkan kelengkapan Persyaratan Administrasi Perangkat Lunak.

Pasal 6

Penyelenggara Sistem Elektronik wajib menggunakan Perangkat Lunak yang level Persyaratan Teknisnya sesuai dengan risiko Sistem Elektronik.

Pasal 7

Kesesuaian sebagaimana dimaksud pada Pasal 6 adalah sebagai berikut:

a. Perangkat Lunak yang digunakan dalam Sistem Elektronik Strategis harus memenuhi Persyaratan Teknis Level 3.
b. Perangkat Lunak yang digunakan dalam Sistem Elektronik Tinggi harus memenuhi Persyaratan Teknis minimal Level 2.
c. Perangkat Lunak yang digunakan dalam Sistem Elektronik Rendah harus memenuhi Persyaratan Teknis minimal Level 1.

Pasal 8

(1) Penyelenggara Sistem Elektronik wajib menjamin perolehan dan/atau akses terhadap kode sumber dan

dokumentasi atas Perangkat Lunak kepada Auditor.

(2) Tata cara perolehan dan/atau akses terhadap kode sumber dan dokumentasi atas Perangkat Lunak diatur dalam Peraturan Menteri tersendiri.

Pasal 9

Kewajiban Penggunaan Perangkat Lunak sebagaimana dimaksud pada Pasal 6 merupakan bagian dari Sertifikasi Sistem Manajemen Pengamanan Informasi.

BAB VI
AUDIT

Pasal 10

(1) Setiap Perangkat lunak yang digunakan untuk Pelayanan Publik harus menjalani proses audit.

(2) Audit dilakukan oleh Auditor Perangkat Lunak yang ditetapkan oleh Menteri.

(3) Menteri menetapkan daftar Auditor Perangkat Lunak.

(4) Ketentuan lebih lanjut mengenai Penetapan Auditor Perangkat Lunak diatur dengan Peraturan Menteri.

BAB VII
TATA CARA AUDIT

Pasal 11

(1) Auditor melakukan audit Perangkat Lunak terhadap Persyaratan Teknis.

(2) Auditor Perangkat Lunak harus menyerahkan hasil audit kepada Menteri.

(3) Berdasarkan hasil audit sebagaimana dimaksud pada ayat (2), Menteri c.q. Direktur Jenderal menetapkan level Persyaratan Teknis Perangkat Lunak.

(4) Penetapan Level Persyaratan Teknis Perangkat Lunak sebagaimana dimaksud pada ayat (3) paling lambat 14 (empat belas) hari kerja setelah hasil audit dinyatakan lengkap.

(5) Menteri c.q. Direktur Jenderal menyusun daftar Hasil Penetapan Level Persyaratan Teknis Perangkat Lunak.

BAB VIII
PERIODE AUDIT

Pasal 12

(1) Audit berkala dilakukan paling sedikit 1 (satu) kali dalam setahun.
(2) Audit ulang dilakukan paling lama 6 (enam) bulan sejak dilakukan pemutakhiran Perangkat Lunak.

Pasal 13

(1) Dalam hal Penyelenggara Sistem Elektronik melakukan perubahan pada perangkat lunak yang mengakibatkan perubahan level Persyaratan Teknis, maka Penyelenggara Sistem Elektronik wajib mendaftarkan ulang perangkat lunak tersebut.

(2) Pendaftaran sebagaimana dimaksud pada ayat (1) sekurang-kurangnya dilakukan 1 kali dalam setahun.

BAB IX
PENGAWASAN

Pasal 14

(1) Menteri melakukan pengawasan terhadap Perangkat Lunak yang digunakan oleh Penyelenggara Sistem Elektronik.

(2) Pengawasan sebagaimana dimaksud pada ayat (1) dilakukan secara berkala 1 (satu) tahun sekali atau sewaktu-waktu melalui pemantauan, pengendalian, pemeriksaan, penelusuran, dan pengamanan.

(3) Ketentuan mengenai pengawasan atas penyelenggaraan Sistem Elektronik dalam sektor tertentu wajib dibuat oleh Instansi Pengawas dan Pengatur Sektor terkait setelah berkoordinasi dengan Menteri.

BAB X
SANKSI

Pasal 15

(1) Penyelenggara Sistem Elektronik yang melakukan pelanggaran ketentuan pada Pasal 5, Pasal 6, Pasal 7, dan Pasal 8 ayat (1), Pasal 13 ayat (1) dan ayat (2) dikenai sanksi administratif.

(2) Sanksi administratif yang dimaksud pada ayat (1) dapat berupa:
a. teguran tertulis;

b. dikeluarkan dari daftar sebagaimana dimaksud dalam Pasal 10.

(3) Sanksi administratif sebagaimana dimaksud pada ayat (1) diberikan oleh Menteri atau pimpinan Instansi Pengawas dan Pengatur Sektor terkait sesuai dengan ketentuan peraturan perundang-undangan.

(4) Pimpinan Instansi Pengawas dan Pengatur Sektor terkait dapat memberikan sanksi administratif sebagaimana dimaksud pada ayat (3) setelah berkoordinasi dengan Menteri.

BAB XI
KETENTUAN PERALIHAN

Pasal 16

(1) Dalam hal Peraturan Menteri mengenai Penetapan Auditor Perangkat Lunak belum diundangkan pada saat Peraturan Menteri ini mulai berlaku, Menteri dapat menunjuk Auditor yang berkompeten.

(2) Peraturan Menteri mengenai Penetapan Auditor Perangkat Lunak harus sudah ditetapkan paling lama 2 (dua) tahun setelah diundangkannya Peraturan Menteri ini.

(3) Pada saat Peraturan Menteri ini mulai berlaku, Penyelenggara Sistem Elektronik yang telah beroperasi sebelum berlakunya Peraturan Menteri ini wajib memenuhi Persyaratan Perangkat Lunak dalam jangka waktu paling lama 2 (dua) tahun sejak berlakunya Peraturan Menteri ini.

(4) Pada saat Peraturan Menteri ini mulai berlaku, Penyelenggara Sistem Elektronik yang telah memenuhi persyaratan perangkat lunak dengan menggunakan Standar selain OWASP ASVS sebelum berlakunya Peraturan Menteri ini, wajib menyesuaikan dengan Peraturan Menteri ini dalam jangka waktu paling lama 2 (dua) tahun sejak berlakunya Peraturan Menteri ini.

(5) Pada saat Peraturan Menteri ini mulai berlaku, Penyelenggara Sistem Elektronik yang baru beroperasi wajib memenuhi Persyaratan Perangkat Lunak paling lambat 1 (satu) tahun sejak beroperasinya Sistem Elektronik.

(6) Pada saat Peraturan Menteri ini mulai berlaku, Perangkat lunak yang sudah terpasang sebelum berlakunya Peraturan Menteri ini, wajib menyesuaikan dengan Peraturan Menteri ini dalam jangka waktu paling lama 2 (dua) tahun sejak berlakunya Peraturan Menteri ini.

BAB XII
KETENTUAN PENUTUP

Pasal 17

Peraturan Menteri ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Menteri ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 2015

MENTERI KOMUNIKASI DAN INFORMATIKA
REPUBLIK INDONESIA,

RUDIANTARA

Diundangkan di Jakarta
pada tanggal

MENTERI HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

YASONNA HAMONANGAN LAOLY

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2015 NOMOR...

LAMPIRAN
PERATURAN MENTERI KOMUNIKASI DAN
INFORMATIKA REPUBLIK INDONESIA
NOMOR TAHUN 2015
TENTANG PERSYARATAN PERANGKAT LUNAK
SISTEM ELEKTRONIK

LAMPIRAN
KRITERIA PERSYARATAN PERANGKAT LUNAK

Persyaratan Perangkat Lunak mencakup 13 (tiga belas) area persyaratan:

1. Otentikasi;
2. Manajemen Sesi;
3. Kontrol Akses;
4. Validasi Input;
5. Kriptografi pada Verifikasi Statis;
6. Penanganan Error dan Pencatatan Log;
7. Proteksi Data;
8. Keamanan Komunikasi;
9. Keamanan HTTP;
10. Kontrol Kode Berbahaya;
11. Logic Bisnis;
12. Berkas dan Sumber Daya; dan
13. Aplikasi Mobile.

Setiap area persyaratan memiliki beberapa Persyaratan Teknis. Persyaratan Teknis yang diberikan tanda centang (✓) artinya Persyaratan Teknis tersebut harus dipenuhi oleh Perangkat Lunak sesuai dengan levelnya.

1. Otentikasi

NO	PERSYARATAN TEKNIS	LEVEL PERSYARATAN TEKNIS		
		Level 1	Level 2	Level 3
1	Otentikasi disyaratkan untuk seluruh halaman dan sumber daya kecuali yang secara spesifik terbuka untuk umum (Prinsip Mediasi Komplit untuk Otentikasi)	✓	✓	✓
2	Teks *password* yang diketik oleh pengguna tidak ditampilkan untuk seluruh kotak isian *password*	✓	✓	✓
3	Seluruh kontrol otentikasi diperkuat pada sisi server (*server side*)	✓	✓	✓
4	Kontrol otentikasi (meliputi pustaka yang memanggil layanan otentikasi eksternal) diimplementasikan secara terpusat.			✓

5	Terdapat penanganan kegagalan kontrol otentikasi yang diterapkan secara aman, untuk memastikan penyerang tidak dapat login.	✓	✓	✓
6	Kotak isian *password* memperbolehkan penggunakan *passphrase*, tidak membatasi panjang *passphrase* maupun kompleksitas *password*, dan menyediakan persyaratan minimum kekuatan *password*, sebagai perlindungan terhadap penggunaan *password* yang umum dipakai.		✓	✓
7	Semua fungsi otentikasi identitas akun yang memungkinkan perolehan kembali akses ke akun tersebut (seperti *registration, update profile, forgot username, forgot password, disabled / lost token, help desk or Interactive Voice Response*), memiliki tingkat perlindungan yang sama dengan mekanisme otentikasi utama.		✓	✓
8	Pengguna dapat secara mudah mengubah dokumen kredensial menggunakan mekanisme yang resisten terhadap serangan sebagai mekanisme otentikasi utama			✓
9	Seluruh hasil dari autentikasi tercatat dalam log. Termasuk *request* dengan informasi yang kurang lengkap.(yang dibutuhkan dalam investigasi keamanan).			✓
10	*Password* akun dilengkapi dengan *salt* (*cryptography*) yang unik terhadap akun tersebut (misal identitas pengguna, pembuatan akun) dan menggunakan bcrypt, scrypt atau *Password Based Key Derivation Function 2* (PBKDF2) sebelum menyimpan *password*.			✓
11	Kredensial dan informasi identitas pengguna lainnya yang ditangani oleh aplikasi tidak dilewatkan melalui jalur yang tidak terenkripsi (atau dienkripsi secara lemah).	✓	✓	✓
12	Fungsi *forgot password* dan jalur pemulihan lainnya tidak mengungkapkan *password* saat ini, dan *password* baru tidak dikirim dalam bentuk teks kepada pengguna.	✓	✓	✓
13	Fungsi login, reset *password* atau *forgot account* tidak memungkinkan enumerasi *username.*	✓	✓	✓
14	Kerangka kerja aplikasi maupun komponen aplikasi lainnya tidak menggunakan *password default* (seperti “admin/*password*”).	✓	✓	✓
15	Fitur *resource governor* tersedia dan diimplementasikan untuk melindungi serangan *brute force* vertikal (satu akun terhadap semua “*Password*1”). Tidak ada penundaan untuk input kredensial yang tepat. Kedua mekanisme tersebut harus aktif secara bersamaan sebagai perlindungan terhadap serangan diagonal dan terdistribusi.		✓	✓

16	Semua kredensial otentikasi yang digunakan untuk mengakses layanan di luar aplikasi dienkripsi dan disimpan pada lokasi terproteksi (tidak dalam kode sumber).		✓	✓
17	Fitur *forgot password* dan jalur pemulihan lainnya mengirim tautan yang mengandung token aktivasi dengan pembatasan waktu. Tautan tidak mengandung *password* itu sendiri. Otentikasi tambahan berdasarkan *soft-token* (misalnya token SMS, aplikasi mobile *native*, dll) dapat juga diminta sebelum tautan tersebut dikirim.		✓	✓
18	Fungsi *forgot-password* tidak mengunci atau menonaktifkan akun sampai pengguna berhasil mengubah *password* tersebut. Hal ini untuk mencegah pengguna yang valid menjadi terkunci.		✓	✓
19	Tidak terdapat pertanyaan dan jawaban yang diketahui bersama (biasa disebut pertanyaan dan jawaban “rahasia”).		✓	✓
20	Sistem dapat dikonfigurasi untuk mencegah penggunaan beberapa *password* yang telah digunakan sebelumnya (jumlah dapat dikonfigurasi).		✓	✓
21	Otentikasi ulang (re-otentikasi), otentikasi bertahap atau adaptif, SMS atau otentikasi dua faktor lainnya, ataupun penandatanganan transaksi diwajibkan sebelum dilaksanakannya operasi sensitif aplikasi tertentu, sesuai dengan profil risiko aplikasi tersebut.			✓

2. Manajemen Sesi

NO	PERSYARATAN	LEVEL PERSYARATAN TEKNIS		
		Level 1	Level 2	Level 3
1	Aplikasi menggunakan fitur kontrol manajemen sesi bawaan (*default*) dari kerangka kerja	✓	✓	✓
2	Sesi dibatalkan ketika pengguna melakukan logout	✓	✓	✓
3	Sesi habis bila tidak ada aktivitas dalam jangka waktu tertentu	✓	✓	✓
4	Sesi habis dalam jangka waktu maksimum tertentu (parameter konfigurasi), terlepas dari ada atau tidaknya aktivitas pengguna.		✓	✓
5	Terdapat tautan logout untuk semua halaman yang memerlukan otentikasi	✓	✓	✓

6	Session ID tidak dicantumkan selain di *header Cookie*; khususnya di URL, pesan kesalahan, atau log. Proses ini mencakup verifikasi bahwa aplikasi tidak mendukung URL *rewriting* untuk *session cookies*.	✓	✓	✓
7	*Session ID* selalu diubah dalam proses login, untuk mencegah serangan fiksasi sesi (*session fixation*).		✓	✓
8	*Session ID* selalu diubah ketika terjadi otentikasi ulang.		✓	✓
9	Hanya *session ID* yang dihasilkan oleh kerangka kerja aplikasi yang dinyatakan valid oleh aplikasi.		✓	✓
10	Token untuk sesi yang terotentikasi memiliki panjang dan tingkat keacakan yang cukup, untuk menangkal serangan penebakan sesi (*session guessing*)		✓	✓
11	Token untuk sesi terotentikasi yang menggunakan *cookies*, disimpan di lokasi yang terproteksi pada situs tersebut. Restriksi terhadap atribut *domain cookie* tidak perlu diberlakukan, kecuali dibutuhkan oleh proses bisnis, misalnya untuk *single sign on*.		✓	✓
12	Token untuk sesi terotentikasi yang menggunakan *cookies* dan dikirimkan menggunakan HTTP, dilindungi dengan penggunaan fitur "Http Only"	✓	✓	✓
13	Token untuk sesi terotentikasi yang menggunakan *cookies*, dilindungi dengan fitur atribut "*secure*" dan *transport security header* yang aman (seperti *Strict-Transport-Security*: *max-age*=60000; *includeSubDomains*)	✓	✓	✓
14	Aplikasi tidak mengizinkan penggunaan sesi pengguna duplikat secara bersamaan, yang berasal dari mesin yang berbeda		✓	✓

3. Persyaratan Kontrol Akses

NO	PERSYARATAN TEKNIS	LEVEL PERSYARATAN TEKNIS		
		Level 1	Level 2	Level 3
1	Untuk layanan dan fungsi yang dilindungi, sistem membatasi akses pengguna berdasarkan otorisasi khusus yang dimiliki.	✓	✓	✓
2	Untuk URL yang dilindungi, sistem membatasi akses pengguna berdasarkan otorisasi khusus yang dimiliki.	✓	✓	✓

3	Untuk file data yang dilindungi, sistem membatasi akses pengguna berdasarkan otorisasi khusus yang dimiliki.	✓	✓	✓
4	Sistem memiliki perlindungan terhadap *direct object reference*, di mana pengguna hanya dapat mengakses data berdasarkan otorisasi yang dimiliki (Sebagai contoh, perlindungan terhadap *direct object reference tampering).*	✓	✓	✓
5	Fitur direktori browsing dinonaktifkan, kecuali diperlukan berdasarkan pertimbangan yang kuat.	✓	✓	✓
6	Sistem memiliki mekanisme penanganan kegagalan akses kontrol yang aman.	✓	✓	✓
7	Aturan kontrol akses yang sama, yang ditampilkan pada *layer* presentasi, diterapkan pada sisi server atas peran pengguna tersebut, di mana kontrol dan parameter tidak dapat diaktifkan kembali atau ditambahkan kembali dari pengguna yang memiliki hak akses yang lebih tinggi.		✓	✓
8	Atribut pengguna dan data, serta informasi kebijakan yang digunakan dalam kontrol akses tidak dapat dimanipulasi oleh pengguna kecuali berdasarkan kewenangan khusus.		✓	✓
9	Setiap kontrol akses diterapkan pada sisi server.	✓	✓	✓
10	Sistem menerapkan mekanisme yang terpusat (termasuk *libraries* yang dapat memanggil layanan otorisasi eksternal) untuk melindungi akses ke masing-masing jenis sumber daya yang dilindungi.			✓
11	Terdapat catatan elektronik untuk setiap keputusan kontrol akses, dan juga keputusan yang gagal.		✓	✓
12	Aplikasi/kerangka kerja menghasilkan token anti-*Cross Site Request Forgery* (CSRF) yang kuat, acak dan unik untuk pengguna dalam transaksi bernilai tinggi atau akses terhadap data sensitif, dan aplikasi harus memverifikasi keberadaan token ini dengan nilai yang tepat untuk pengguna tersebut saat melakukan proses permintaan.	✓	✓	✓
13	Sistem harus melindungi akses yang bersamaan atau akses yang terus-menerus terhadap fungsi yang harus diamankan, sumber daya, atau data. Sebagai contoh, penggunaan fitur *resource governor* untuk membatasi jumlah *edit* per jam atau untuk mencegah *scraping* terhadap seluruh database oleh pengguna individu.		✓	✓

4. Validasi Input

NO	PERSYARATAN TEKNIS	LEVEL PERSYARATAN TEKNIS		
		Level 1	Level 2	Level 3
1	*Runtime environment* memiliki kontrol keamanan untuk mencegah *buffer overflows*.	✓	✓	✓
2	Fungsi validasi input menghasilkan penolakan jika terjadi kesalahan validasi	✓	✓	✓
3	Karakter set, seperti UTF-8, dibuat sama untuk semua sumber masukan.		✓	✓
4	Validasi input atau encoding *routines* dilakukan dan diberlakukan pada sisi *server*.	✓	✓	✓
5	Sistem menggunakan kontrol validasi input tunggal yang untuk setiap jenis data yang diterima.			✓
6	Kegagalan validasi input saat login dicatat dalam *log file.*			✓
7	Proses kanonikalisasi diterapkan untuk setiap data input, pada semua dekoder atau *interpreter* akhiran, sebelum masuk ke proses validasi		✓	✓
8	*Runtime environment* memiliki modul kontrol keamanan untuk *SQL injection*	✓	✓	✓
9	*Runtime environment* memilki kontrol keamanan untuk mencegah *Lightweight Directory Access Protocol* (*LDAP*) *Injection*.	✓	✓	✓
10	*Runtime environment* memiliki kontrol keamanan untuk mencegah *OS Command Injection*.	✓	✓	✓
11	*Runtime environment* memiliki kontrol keamanan untuk mencegah serangan *XML* Entity Eksternal.	✓	✓	✓
12	*Runtime environment* memiliki kontrol untuk mencegah *XML injections*.	✓	✓	✓
13	Sistem memiliki kemampuan untuk melakukan filter terhadap data yang tidak dipercaya yang dapat menjadi *HTML* (termasuk elemen *HTML*, atribut *HTML*, data *Java Script*, *CSS blocks*, dan atribut *URI*) sesuai konteks yang berlaku.	✓	✓	✓
14	Parameter keamanan yang sensitif, seperti "*account Balance*", "*role*" atau "*password*" dilindungi dari penetapan/pengisian parameter secara otomatis yang berbahaya. Hal ini berlaku bilamana kerangka kerja aplikasi memperbolehkan penetapan/pengisian parameter massal secara otomatis yang berasal dari *inbound request* ke sebuah model.		✓	✓
15	Aplikasi memiliki mekanisme pertahanan terhadap serangan *HTTP parameter pollution*,		✓	✓

	terutama jika kerangka aplikasi tidak membuat perbedaan tentang sumber parameter permintaan (*GET*, *POST*, *cookies*, *header*, *environment*, dll)			
16	Sistem memiliki kontrol keamanan tunggal untuk jenis keluaran untuk *encoding / escaping* yang dilakukan oleh aplikasi.			✓

5. Kriptografi pada Verifikasi Statis

NO	PERSYARATAN TEKNIS	LEVEL PERSYARATAN TEKNIS		
		Level 1	Level 2	Level 3
1	Sistem memiliki fungsi kriptografi yang diimplementasikan di sisi server untuk melindungi rahasia dari pengguna aplikasi.		✓	✓
2	Modul kriptografi memiliki mekanisme untuk menangani kegagalan secara aman.		✓	✓
3	Akses terhadap *master secret* dilindungi dari akses yang tidak terotorisasi (*master secret* adalah kredensial aplikasi yang disimpan dalam bentuk *plaintext* di *disk* dan digunakan untuk melindungi akses terhadap informasi konfigurasi keamanan).		✓	✓
4	Agar nilai acak tidak mudah ditebak, hanya *random number generator* yang disetujui yang boleh digunakan dalam modul kriptografi. Nilai acak dapat berupa angka acak, nama file acak, GUIDs acak, dan *string* acak yang harus dihasilkan oleh *random number generator* tersebut.		✓	✓
5	Modul kriptografi yang digunakan oleh aplikasi divalidasi dengan menggunakan *Federal Information Processing Standards* (FIPS) 140-2 atau standar yang setara.			✓
6	Modul kriptografi beroperasi dalam mode disetujui sesuai dengan kebijakan keamanan yang diterbitkan.			✓
7	Terdapat kebijakan eksplisit untuk mengelola kunci kriptografi (seperti: *generated*, *distributed*, *revoked*, *expired*). Kebijakan ini dipastikan telah diberlakukan dengan benar.		✓	✓

6. Penanganan Error dan Pencatatan Log

NO	PERSYARATAN TEKNIS	LEVEL PERSYARATAN TEKNIS		
		Level 1	Level 2	Level 3
1	Pesan kesalahan atau *stack traces* tidak berisi data sensitif yang dapat membantu penyerang, untuk mendapatkan *session ID* dan informasi pribadi.	✓	✓	✓
2	Penanganan error pada perangkat terpercaya (*trusted devices*) harus berjalan dengan baik		✓	✓
3	Sistem memiliki kontrol untuk *logging* pada server		✓	✓
4	Secara *default* akses penggunaan *error handling logic* dalam kontrol keamanan adalah *denied*		✓	✓
5	*Logging* keamanan menyediakan kemampuan untuk mencatat peristiwa keberhasilan dan kegagalan yang diidentifikasi sebagai keamanan yang relevan.		✓	✓
6	Catatan log berisi : catatan waktu dari sumber terpercaya, tingkat *severity*, indikasi bahwa ini adalah peristiwa keamanan yang relevan (jika dikorelasikan dengan log lain), identitas pengguna yang menyebabkan peristiwa (jika ada user yang berhubungan dengan peristiwa tersebut), alamat IP sumber dari permintaan yang terkait dengan peristiwa tersebut, apakah peristiwa berhasil atau gagal, dan deskripsi peristiwa.		✓	✓
7	Sistem memiliki mekanisme untuk tidak melakukan eksekusi kode pada saat membaca log jika terdapat skrip/kode yang tertanam.			✓
8	S*ecurity log* harus terlindungi dari modifikasi dan akses yang tidak memiliki otorisasi.		✓	✓
9	Perangkat lunak menerapkan pencatatan tunggal pada level aplikasi.			✓
10	Isi dari log dapat berisi panjang dan keberadaan data sensitif namun tidak berisi data sensitif aplikasi itu sendiri yang dapat membantu seorang *attacker*, termasuk identifikasi sesi pengguna dan informasi yang pribadi/sensitif.		✓	✓
11	Tersedia perangkat analisa log, untuk membantu pencarian kejadian (*event*) berdasarkan kombinasi kriteria pencarian. Kriteria pencarian dapat mencakup pada semua *field* yang tersedia pada log, sesuai dengan format yang didukung oleh sistem.		✓	✓

12	Semua simbol yang tidak dapat dicetak, dan pemisah kolom, dikodekan dengan layak dalam log untuk mencegah *log injection*.			✓
13	Proses pencatatan log dipisahkan berdasarkan sumber yang terpercaya dan tidak terpercaya.			✓
14	Ketika integritas dan nirsangkal adalah suatu keharusan, pencatatan dalam log dilakukan sebelum transaksi dieksekusi. Jika pencatatan dalam log tidak berhasil (misalnya disk penuh, izin tidak cukup), aplikasi dapat berjalan dengan *fails safe*.			✓

7. Proteksi Data

NO	PERSYARATAN TEKNIS	LEVEL PERSYARATAN TEKNIS		
		Level 1	Level 2	Level 3
1	Fitur *caching* dari sisi *client*, termasuk fitur *autocomplete formulir* telah dimatikan agar tidak mengandung informasi yang sensitif	✓	✓	✓
2	Terdapat daftar data sensitif yang akan diproses oleh aplikasi. Terdapat kebijakan yang eksplisit dan sudah diterapkan mengenai bagaimana akses data sensitif tersebut harus dikontrol dan kapan data sensitif tersebut harus dienkripsi (baik data diam dan data bergerak).			✓
3	Sistem memiliki mekanisme untuk mengirimkan data sensitif ke server melalui *HTTP message body* dan tidak menggunakan parameter URL untuk mengirim data sensitif	✓	✓	✓
4	Semua data sensitif di *cache* atau di salinan temporer yang dikirim ke *client* dilindungi dari akses yang tidak sah atau dibersihkan / dibatalkan setelah pengguna yang berwenang mengakses data sensitif tersebut (misalnya, penggunaan *no-cache* dan *no-store Cache-Control header* ditetapkan) .		✓	✓
5	Semua *cache* atau salinan data temporer yang sensitif yang tersimpan di server dilindungi dari akses yang tidak sah atau dibersihkan / dibatalkan setelah pengguna yang berwenang mengakses data sensitif.		✓	✓
6	Sistem memiliki mekanisme untuk menghilangkan setiap jenis data sensitif dari aplikasi pada akhir periode retensi yang dipersyaratkan.			✓
7	Aplikasi meminimalkan jumlah parameter yang dikirim ke sistem yang tidak dipercaya, seperti pada *fields* yang tersembunyi, variabel Ajax,			✓

	cookies dan nilai-nilai *header*.			
8	Aplikasi memiliki kemampuan untuk mendeteksi dan memberi peringatan terhadap kejanggalan jumlah permintaan informasi atau pemrosesan transaksi dengan nilai tinggi untuk peran pengguna tersebut, seperti *screen scraping*, penggunaan otomatis *web service extraction*, atau *data loss prevention*. Misalnya, rata-rata pengguna tidak dimungkinkan mengakses lebih dari 5 catatan per jam atau 30 catatan per hari, atau menambah 10 teman ke dalam jaringan sosial per menitnya.			✓

8. Keamanan Komunikasi

NO	PERSYARATAN TEKNIS	LEVEL PERSYARATAN TEKNIS		
		Level 1	Level 2	Level 3
1	Jalur komunikasi harus menggunakan CA yang terpercaya untuk pembuatan setiap *Transport Layer Security* (TLS) dan setiap sertifikat yang valid	✓	✓	✓
2	Jika terjadi kegagalan pada koneksi TLS maka sistem tidak kembali pada koneksi HTTP tidak aman			✓
3	TLS digunakan untuk seluruh koneksi termasuk koneksi eksternal dan koneksi *back-end* yang menggunakan otentikasi atau yang meliputi data atau fungsi yang sensitif.		✓	✓
4	Kegagalan koneksi TLS di *back-end* tercatat dalam log.		✓	✓
5	Untuk semua *client certificate, certificate path* dibentuk dan diperiksa menggunakan *trust anchors* dan informasi revokasi yang telah dikonfigurasi.			✓
6	Semua koneksi ke sistem eksternal yang meliputi informasi atau fungsi sensitif dilakukan dengan otentikasi.		✓	✓
7	Semua koneksi ke sistem eksternal yang meliputi informasi atau fungsi sensitif menggunakan sebuah akun yang telah diatur untuk memiliki hak akses minimum yang diperlukan agar aplikasi dapat berfungsi dengan baik.		✓	✓
8	Terdapat standar tunggal implementasi TLS yang digunakan oleh aplikasi yang dikonfigurasi untuk berjalan pada mode operasi yang telah disetujui.			✓

9	Format karakter tertentu telah didefinisikan untuk seluruh koneksi (misal UTF-8)			✓

9. Keamanan HTTP

NO	PERSYARATAN TEKNIS	LEVEL PERSYARATAN TEKNIS		
		Level 1	Level 2	Level 3
1	Aplikasi hanya menerima kumpulan metode permintaan HTTP yang telah ditentukan, seperti GET dan POST dan metode yang tidak digunakan telah diblok secara jelas.	✓	✓	✓
2	HTTP *header* meliputi suatu *header* tipe konten yang menjelaskan kumpulan karakter yang aman (misal UTF-8)	✓	✓	✓
3	HTTP *header* pada permintaan dan respon hanya mengandung karakter ASCII yang dapat dicetak.		✓	✓
4	HTTP *header* dan/atau mekanisme lain untuk perambah versi lama telah dimasukkan untuk melindungi dari serangan *clickjacking*.	✓	✓	✓
5	HTTP *header* yang ditambahkan oleh *frontend* (misal *X-Real-IP*) dan digunakan oleh aplikasi, tidak bisa diketahui oleh pengguna.		✓	✓
6	HTTP *header*, *X-Frame-Options* digunakan untuk situs dengan konten yang tidak boleh dilihat menggunakan *X-Frame* pihak ketiga. Jalan tengah yang umumnya digunakan adalah dengan mengirimkan SAMEORIGIN, di mana hanya situs dengan *origin* yang sama yang dapat menampilkannya dalam *frame*.		✓	✓
7	HTTP *header* tidak memberikan versi komponen sistem informasi secara detail.		✓	✓

10. Kontrol Kode Berbahaya

NO	PERSYARATAN TEKNIS	LEVEL PERSYARATAN TEKNIS		
		Level 1	Level 2	Level 3
1	Tidak terdapat kode berbahaya dalam semua kode yang dikembangkan ataupun dimodifikasi dalam pembuatan aplikasi.			✓
2	Integritas *intrepreted code, libraries, executable* dan file konfigurasi diverifikasi menggunakan *checksum* atau *hashes*.			✓

3	Seluruh kode yang menerapkan atau menggunakan kontrol otentikasi tidak mengandung kode berbahaya.			✓
4	Seluruh kode yang menerapkan atau menggunakan kontrol manajemen sesi tidak mengandung kode berbahaya.			✓
5	Seluruh kode yang menerapkan atau menggunakan kontrol akses tidak mengandung kode berbahaya.			✓
6	Seluruh kontrol validasi *input* tidak mengandung kode berbahaya.			✓
7	Seluruh kode yang menerapkan atau menggunakan kontrol validasi *output* tidak mengandung kode berbahaya.			✓
8	Seluruh kode yang mendukung atau menggunakan modul kriptografi tidak mengandung kode berbahaya.			✓
9	Seluruh kode yang menerapkan atau menggunakan kontrol log dan penanganan kesalahan (*error handling*) tidak mengandung kode berbahaya.			✓
10	Seluruh aktivitas berbahaya telah melalui mekanisme *sandbox* yang memadai.			✓
11	Data sensitif secepat mungkin dibersihkan dari memori setelah tidak dibutuhkan dan ditangani lagi sesuai dengan fungsi dan teknik yang didukung oleh kerangka kerja/*library*/sistem operasi.			✓

11. Logik Bisnis

NO	PERSYARATAN TEKNIS	LEVEL PERSYARATAN TEKNIS		
		Level 1	Level 2	Level 3
1	Pemrosesan atau verifikasi terhadap seluruh alur logika bisnis yang bernilai tinggi, dilakukan pada lingkungan terpercaya, seperti server yang dilindungi dan dimonitor.		✓	✓
2	Pemalsuan transaksi bernilai tinggi tidak dapat dilakukan, seperti mengizinkan pengguna A (*attacker*) untuk memproses transaksi sebagai pengguna B (*victim*) dengan melakukan perubahan atau melakukan pengulangan sesi, status transaksi, transaksi atau identitas pengguna.		✓	✓

3	Parameter logika bisnis bernilai tinggi seperti (namun tidak terbatas pada): harga, bunga, diskon, informasi data pribadi, saldo, ID saham, dll tidak dapat diubah secara seketika.		✓	✓
4	Aplikasi memiliki mekanisme perlindungan terhadap serangan yang berkaitan dengan penyangkalan, seperti log transaksi yang terlindungi dan dapat diverifikasi, *audit trail* atau log sistem. Pada sistem dengan kritikalitas tinggi, dilakukan monitoring *real time* terhadap aktivitas pengguna dan juga transaksi, untuk mendeteksi anomali.		✓	✓
5	Aplikasi memiliki mekanisme perlindungan terhadap serangan yang berkaitan dengan kebocoran informasi. Serangan dapat berupa akses langsung terhadap obyek, *brute force* terhadap sesi pengguna, atau serangan lainnya.		✓	✓
6	Aplikasi memiliki kontrol deteksi dan pengaturan sumber daya (*governor*) yang memadai, sebagai perlindungan terhadap serangan *brute force* (seperti pemanggilan fungsi tertentu secara terus-menerus) atau *denial of service*.		✓	✓
7	Aplikasi memiliki kontrol akses yang memadai, untuk mencegah serangan yang bertujuan untuk meningkatkan kewenangan (*elevation of privilege*). Serangan ini dapat berupa akses yang dilakukan oleh pengguna anonim terhadap data atau fungsi yang dilindungi, atau akses terhadap detail pengguna yang dilakukan oleh pengguna lainnya, atau penggunaan fungsi dengan tingkat kewenangan yang tinggi.		✓	✓
8	Aplikasi hanya menjalankan proses alur logika bisnis secara berurutan, di mana setiap langkah dijalankan dalam rentang waktu yang normal untuk dijalankan oleh manusia, tidak dijalankan dalam urutan yang salah, tidak terdapat langkah yang terlewatkan, tidak terdapat langkah yang dijalankan oleh pengguna lainnya, ataupun transaksi yang dijalankan terlalu cepat.		✓	✓
9	Aplikasi memiliki otorisasi tambahan (seperti otentikasi *step up* atau adaptif) untuk sistem dengan kritikalitas/nilai yang lebih rendah, dan atau pemisahan tugas untuk aplikasi dengan kritikalitas/nilai yang lebih tinggi. Hal ini ditujukan untuk menegakkan kontrol terhadap *fraud*, disesuaikan dengan risiko aplikasi dan *fraud* yang terjadi sebelumnya.		✓	✓

10	Aplikasi memiliki nilai batas terkait fungsi bisnis, dan menempatkannya di lokasi yang terpercaya (seperti di server yang terlindungi). Nilai batas ini diterapkan pada level pengguna, per hari atau secara harian, serta dilengkapi dengan notifikasi dan reaksi otomatis (yang dapat dikonfigurasi) jika terjadi serangan otomatis maupun serangan yang tidak normal. Contoh batasan ini mencakup (namun tidak terbatas pada): memastikan pengguna SIM *card* baru tidak memakai lebih dari $10 per hari untuk akun telepon baru; sebuah forum memungkinkan lebih dari 100 pengguna baru per hari atau mencegah *posting* atau pesan pribadi sebelum akun diverifikasi; sebuah sistem kesehatan tidak memperbolehkan dokter untuk mengakses catatan pasien melebihi jumlah pasien yang dapat mereka tangani dalam sehari; atau sistem keuangan perusahaan kecil yang memungkinkan lebih dari 20 pembayaran faktur atau total transaksi $ 1000 per hari bagi keseluruhan pengguna. Dalam setiap kasus, nilai batas dan total dalam bisnis harus bersifat wajar bagi usaha yang bersangkutan. Hal yang tidak wajar adalah bila tidak terdapat nilai batas bisnis, peringatan atau penegakan aturan.		✓	✓

12. Berkas dan Sumber Daya

NO	PERSYARATAN TEKNIS	LEVEL PERSYARATAN TEKNIS		
		Level 1	Level 2	Level 3
1	URL yang dialihkan (*redirect* dan *forward*), tidak mengandung data yang belum divalidasi.	✓	✓	✓
2	Dilakukan proses kanonikalisasi untuk nama *file* dan data alamat yang diterima dari sumber yang tidak terpercaya, untuk mencegah serangan *path traversal*.	✓	✓	✓
3	*File* yang diperoleh dari sumber yang tidak dipercaya dipindai terlebih dahulu menggunakan *antivirus scanner*, untuk mencegah unggahan konten yang berbahaya,	✓	✓	✓
4	Dilakukan proses kanonikalisasi dan validasi input, untuk parameter yang diperoleh dari sumber yang tidak dipercaya dan digunakan dalam manipulasi nama file, alamat atau obyek *file system*. Hal ini ditujukan untuk mencegah serangan *local file inclusion*.	✓	✓	✓

5	Dilakukan proses kanonikalisasi, validasi *input*, dan *output encoding* terhadap parameter yang diperoleh dari sumber yang tidak terpercaya, terutama ketika *input* digunakan untuk proses eksekusi, seperti di *header*, *source* atau *template inclusion.*	✓	✓	✓
6	*Cross domain resource sharing* untuk *remote IFRAME* dan HTML5 tidak memperbolehkan masuknya konten eksternal (*remote*) yang sembarang.	✓	✓	✓
7	*File* yang diperoleh dari sumber yang tidak terpercaya disimpan di luar lokasi *webroot*.		✓	✓
8	Server web maupun server aplikasi dikonfigurasikan untuk menolak akses ke *resources* eksternal (*remote*) secara *default*.		✓	✓
9	Kode aplikasi tidak mengeksekusi data yang diunggah dan berasal dari dari sumber yang tidak dipercaya.		✓	✓
10	Konfigurasi *cross domain resource sharing* untuk *Flash, Silverlight* atau *Rich Internet Application* (RIA) lainnya mencegah akses *remote* yang tidak terotentikasi atau tidak terotorisasi.		✓	✓

13. Aplikasi Mobile

NO	PERSYARATAN TEKNIS	LEVEL PERSYARATAN TEKNIS		
		Level 1	Level 2	Level 3
1	*Client* memvalidasi sertifikat SSL	✓	✓	✓
2	*Unique Device ID* (UDID) tidak digunakan sebagai kontrol keamanan	✓	✓	✓
3	Aplikasi mobile tidak menyimpan data sensitif ke *shared resources* pada perangkat (misalnya kartu memori *SD* atau *shared folder*)	✓	✓	✓
4	Data sensitif tidak disimpan dalam *database* SQLite pada perangkat.	✓	✓	✓
5	Kunci rahasia atau *password* tidak di *hard-coded* dalam *executable*.		✓	✓
6	Aplikasi *mobile* mencegah bocornya data sensitif melalui fitur *snapshot* otomatis dari iOS.		✓	✓
7	Aplikasi tidak dapat dijalankan pada perangkat dengan keadaan *jailbroken* atau *rooted*.		✓	✓

8	Batas waktu sesi ditetapkan pada nilai yang wajar.		✓	✓
9	Dilakukan pemeriksaan terhadap hak akses yang diminta, beserta *resources* yang diberikan otorisasi untuk diakses (*AndroidManifest.xml, iOS Entitlements*).		✓	✓
10	*Crash log* tidak menyimpan data sensitif.		✓	✓
11	Aplikasi dalam bentuk biner disamarkan.			✓
12	Semua data uji telah dihapus dari *container* aplikasi (.ipa, APK, .bar).		✓	✓
13	Aplikasi tidak mencatat data sensitif ke log sistem atau *filesystem*.		✓	✓
14	Aplikasi mencegah penggunaan fitur *autocomplete* untuk teks sensitif pada *input fields*, seperti *password*, informasi pribadi atau kartu kredit.		✓	✓
15	Aplikasi mobile menerapkan *certificate pinning* untuk mencegah *proxying* lalu lintas data aplikasi.			✓
16	File konfigurasi tidak menyimpan konfigurasi yang salah (misalnya *Debugging flags* aktif, akses *read/write* untuk publik), dan pengaturan konfigurasi menetapkan nilai yang paling aman secara *default*.			✓
17	*3rd-party libraries* yang digunakan terus diperbaharui, dan tidak mengandung kerentanan yang sudah diketahui.			✓
18	Data aplikasi *web*, seperti lalu lintas data melalui HTTPS, tidak di-*cache*.			✓
19	Data sensitif tidak dikirimkan melalui *query string,* namun melalui *POST request* (melalui SSL), dengan dilengkapi token CSRF.			✓
20	Setiap nomor rekening pribadi tidak disimpan secara utuh ke dalam perangkat.			✓
21	Aplikasi memanfaatkan teknik *Address Space Layout Randomization (ASLR).*			✓
22	Data yang dicatat melalui penggunaan *keyboard* (*iOS*) tidak mengandung informasi kredensial, informasi keuangan atau data sensitif lainnya.			✓
23	Aplikasi *Android* tidak membuat file dengan hak akses MODE_WORLD_READABLE atau MODE_WORLD_WRITABLE			✓
24	Data sensitif disimpan menggunakan mekanisme kriptografi yang aman (bahkan ketika disimpan dalam *keychain iOS*).			✓

25	Aplikasi dilengkapi dengan mekanisme *anti-debugging* dan *reverse engineering* yang diimplementasikan dalamnya.			✓
26	Aplikasi Android tidak melakukan *export* terhadap *activities, intents, content providers*, dll. yang sensitif.			✓
27	*Mutable structure* digunakan untuk string sensitif seperti nomor akun, dan ditimpa dengan nilai lain ketika tidak digunakan (untuk meminimalisir kerugian dari serangan analisis memori)			✓
28	Pada sistem Android, validasi data menyeluruh pada input dilakukan pada *intent*, *content provider*, dan *broadcast receiver* yang terekspos.			✓