Universitas Esa Unggul

Smart, Creative and Entrepreneurial

VALIDASI KEMANAN

www.esaunggul.ac.id

Validasi Perangkat Lunak Mobile (CRI-562)

Pertemuan 10

Dosen Pengampu: Harry Kurniawan

Prodi Teknik Informatika - Fakultas Ilmu Komputer

Keamanan

- Keamanan dapat menjadi bisnis yang penting, misalnya, saat hacker mencuri data pelanggan sehingga menjadikannya bagian yang sangat penting dalam proses pengembangan dan pengujian aplikasi mobile

Keamanan

- Pengujian keamanan adalah topik yang kompleks yang membutuhkan pengetahuan di berbagai bidang, seperti komunikasi client-server, arsitektur perangkat lunak, dan arsitektur sistem.
- Karena sifatnya yang kompleks dan banyak keahlian khusus yang dibutuhkan, pengujian keamanan paling baik dilakukan oleh para ahli, diantaranya metode pengujian dengan penetrasi manual, man-in-the-middle, fuzzing, scanning, dan audit aplikasi mobile.

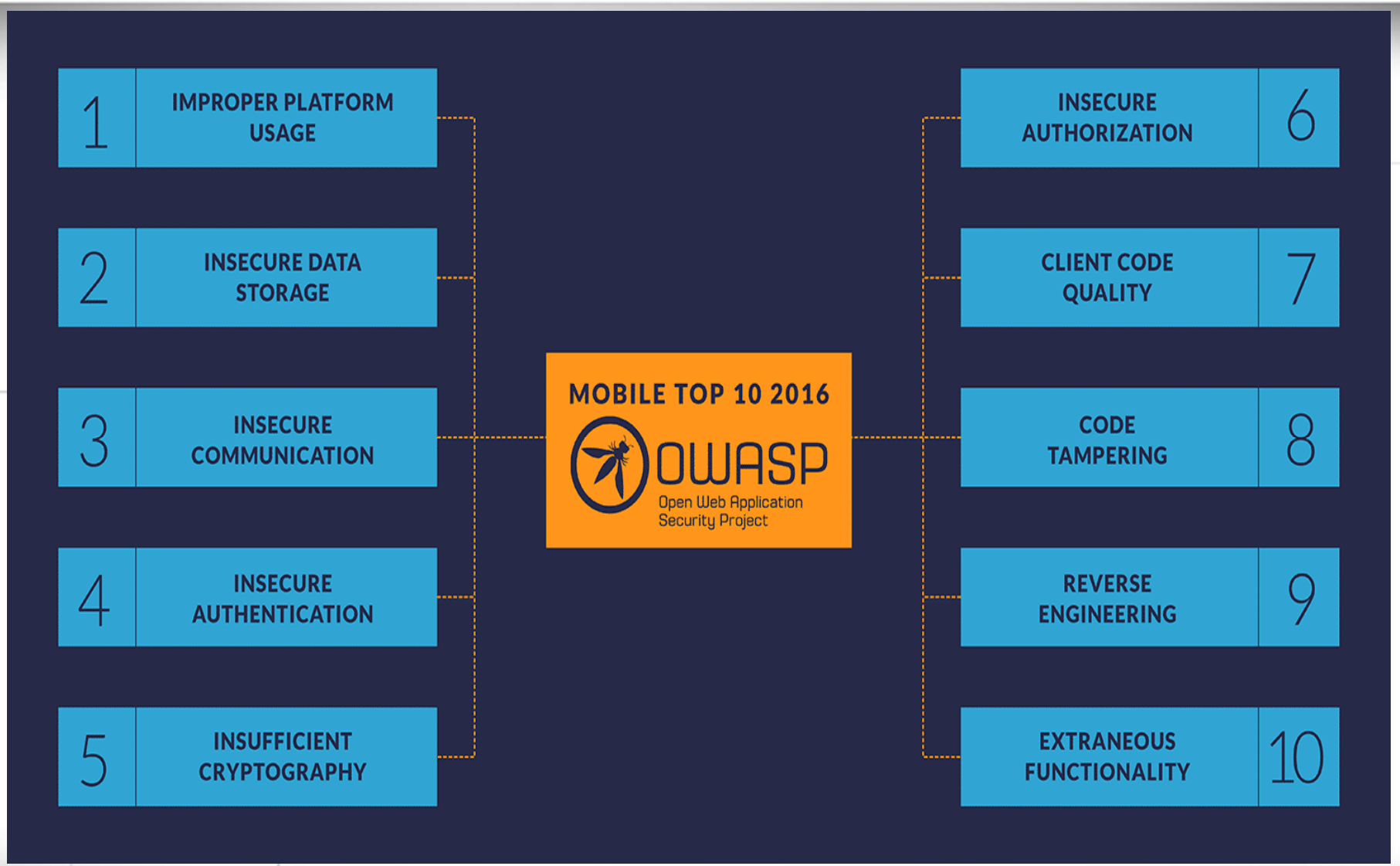
Keamanan

- Pengujian penetrasi adalah pendekatan yang digunakan untuk menemukan kelemahan keamanan dalam aplikasi yang memungkinkan akses ke fitur dan data dengan cara yang tidak sah.

OWASP Mobile Application Security Verification

OWASP

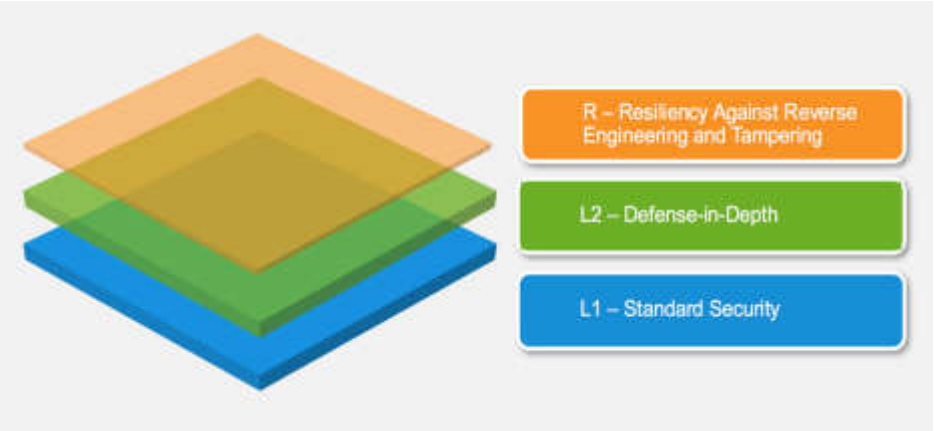
- OWASP tadinya fokus pada aplikasi web, namun telah memiliki “OWASP Mobile Security Testing Guide” dan telah banyak digunakan sebagai acuan.
- Secara rutin OWASP setiap tahun mengeluarkan 10 kategori masalah keamanan terbanyak pada aplikasi mobile, yang dijelaskan pada gambar:


1 IMPROPER PLATFORM USAGE
2 INSECURE DATA STORAGE
3 INSECURE COMMUNICATION
4 INSECURE AUTHENTICATION
5 INSUFFICIENT CRYPTOGRAPHY
MOBILE TOP 10 2016
OWASP
Open Web Application Security Project
6 INSECURE AUTHORIZATION
7 CLIENT CODE QUALITY
8 CODE TAMPERING
9 REVERSE ENGINEERING
10 EXTRANEOUS FUNCTIONALITY

OWASP

- OWASP membagi verifikasi keamanan aplikasi menjadi 8 bagian.
- Setiap bagian mempunyai tingkatan keamanan yang berbeda, ditandai dengan:

OWASP



Tingkatan	Definisi
L1	Level keamanan standar yang harus diimplementasikan oleh semua aplikasi
L2	Level keamanan tinggi, dipakai pada aplikasi yang menyimpan atau mengolah data sensitif seperti kartu kredit, debit, riwayat kesehatan, dsb.
R	Aplikasi bisa melakukan anti reverse engineering dan tempering

OWASP

- **A. Penyimpanan Data dan Privasi**

No	Deskripsi	L 1	L 2
A1	Fasilitas penyimpanan kredensial sistem digunakan secara tepat untuk menyimpan data sensitif, seperti kredensial pengguna atau kunci kriptografi	x	x
A2	Tidak ada data sensitif yang ditulis ke log aplikasi	x	x
A3	Tidak ada data sensitif yang dibagikan dengan pihak ketiga kecuali jika itu adalah bagian penting dari arsitektur	x	x
A4	Cache keyboard dinonaktifkan pada input teks yang memproses data sensitif	x	x
A5	Clipboard dinonaktifkan pada form teks yang mungkin berisi data sensitif.	x	x
A6	Tidak ada data sensitif, seperti password atau pin, yang ditampilkan melalui antarmuka pengguna	x	x

OWASP

- **A. Penyimpanan Data dan Privasi (lanjutan)**

	Deskripsi	L1	L2
A7	Tidak ada data sensitif yang disertakan dalam backup yang dihasilkan oleh sistem operasi mobile		x
A8	Aplikasi akan menghapus data sensitif dari tampilan saat di latarbelakang		x
A9	Aplikasi tidak menyimpan data sensitif dalam memori lebih lama dari yang diperlukan, dan memori dibersihkan secara eksplisit setelah digunakan		x
A10	Aplikasi menerapkan kebijakan keamanan akses perangkat minimum, seperti mengharuskan pengguna untuk mengatur password pada perangkat		x
A11	Aplikasi ini Mengedukasi pengguna tentang jenis-jenis identitas pribadi informasi yang diproses, serta praktik terbaik keamanan yang harus dilakukan pengguna dalam menggunakan aplikasi		x

OWASP

- **B. Kriptografi**

	Deskripsi	L 1	L 2
B1	Aplikasi tidak bergantung pada kriptografi simetris dengan kunci hardcoded sebagai satu-satunya metode enkripsi.	x	x
B2	Aplikasi ini menggunakan implementasi kritografi yang telah terbukti dan dikonfigurasi dengan parameter yang sesuai standar industri	x	x
B3	Aplikasi tidak menggunakan protokol kriptografi atau algoritma yang dianggap sudah tidak aman.	x	x
B4	Aplikasi tidak menggunakan kembali kunci kriptografi yang sama untuk beberapa tujuan.	x	x
B5	Semua nilai acak dihasilkan dengan menggunakan generator bilangan acak yang aman	x	x

OWASP

C. Komunikasi Jaringan

	Deskripsi	L 1	L 2
C1	Data pada jaringan dienkrips menggunakan TLS. Jaringan yang aman digunakan secara konsisten di seluruh aplikasi tanpa kecuali	x	x
C2	Pengaturan TLS harus sesuai dengan *best practice* saat ini, atau semirip mungkin jika sistem operasi seluler tidak mendukung standar yang disarankan.	x	x
C3	Aplikasi memverifikasi sertifikat X.509 dari endpoint jarak jauh saat jaringan terbentuk. Hanya sertifikat yang ditandatangani oleh CA tepercaya yang diterima.	x	x
C4	Aplikasi menggunakan sertifikat digital internal, atau pin sertifikat endpoint atau pasangan kunci publik, dan selanjutnya tidak membuat koneksi dengan endpoint yang menawarkan sertifikat atau kunci yang berbeda, walaupun ditandatangani oleh CA yang tepercaya.		x
C5	Aplikasi tidak bergantung pada hanya satu jalur komunikasi yang tidak aman (email atau SMS) untuk operasi sensitif seperti pendaftaran dan pemulihan akun.		x

Sekian