Universitas Esa Unggul

Smart, Creative and Entrepreneurial

Review W8-W13

www.esaunggul.ac.id

Validasi Perangkat Lunak Mobile (CRI-562)

Pertemuan 13

Dosen Pengampu: Harry Kurniawan

Prodi Teknik Informatika - Fakultas Ilmu Komputer

Perbaikan Teks Input

Perbaikan Teks Input

1. Ekstrak APK sehingga mendapatkan source codenya
   - Tool: www.javadecompilers.com/apk
2. Install Android Studio dan jalankan
   - https://developer.android.com/studio/index.html

Perbaikan Teks Input

3. Sambungkan handphone ke PC dengan kabel data dan Install driver handphone di PC
4. Aktifkan “developer mode” di Android
   - https://www.kingoapp.com/root-tutorials/how-to-enable-usb-debugging-mode-on-android.htm

Stress Test

Stress Test

Pengertian:

Sebuah proses pengujian yang dirancang untuk mendorong aplikasi mencapai *breaking point*

Stress Test

Tujuannya:

- Memunculkan masalah yang mungkin tidak muncul dalam kondisi normal
- Menentukan ketahanan perangkat lunak
- Memastikan sistem gagal dan pulih dengan cara yang dapat diterima.

Stress Test

Apa keuntungan stress test?

- Pada dasarnya adalah bagian dari manajemen risiko
- Tes stres membantu menemukan :
  - Sinkronisasi dan penjadwalan bug
  - Masalah interlock (koneksi antar modul)
  - Masalah prioritas
  - Masalah memori
  - Kehilangan data & corrupt

Validasi Keamanan

Validasi Keamanan

- OWASP adalah salah satu lembaga yang paling banyak menjadi referensi untuk keamanan mobile app.

OWASP

- **A. Penyimpanan Data dan Privasi**

No	Deskripsi	App1	App 2
A1	Fasilitas penyimpanan kredensial sistem digunakan secara tepat untuk menyimpan data sensitif, seperti kredensial pengguna atau kunci kriptografi		
A2	Tidak ada data sensitif yang ditulis ke log aplikasi		
A3	Tidak ada data sensitif yang dibagikan dengan pihak ketiga kecuali jika itu adalah bagian penting dari arsitektur		
A4	Cache keyboard dinonaktifkan pada input teks yang memproses data sensitif		
A5	Clipboard dinonaktifkan pada form teks yang mungkin berisi data sensitif.		
A6	Tidak ada data sensitif, seperti password atau pin, yang ditampilkan melalui antarmuka pengguna		

OWASP

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

	Deskripsi	App1	App 2
A7	Tidak ada data sensitif yang disertakan dalam backup yang dihasilkan oleh sistem operasi mobile		
A8	Aplikasi akan menghapus data sensitif dari tampilan saat di latarbelakang		
A9	Aplikasi tidak menyimpan data sensitif dalam memori lebih lama dari yang diperlukan, dan memori dibersihkan secara eksplisit setelah digunakan		
A10	Aplikasi menerapkan kebijakan keamanan akses perangkat minimum, seperti mengharuskan pengguna untuk mengatur password pada perangkat		
A11	Aplikasi ini Mengedukasi pengguna tentang jenis-jenis identitas pribadi informasi yang diproses, serta praktik terbaik keamanan yang harus dilakukan pengguna dalam menggunakan aplikasi		

OWASP

- **B. Kriptografi**

	Deskripsi	App1	App 2
B1	Aplikasi tidak bergantung pada kriptografi simetris dengan kunci hardcoded sebagai satu-satunya metode enkripsi.		
B2	Aplikasi ini menggunakan implementasi kritografi yang telah terbukti dan dikonfigurasi dengan parameter yang sesuai standar industri		
B3	Aplikasi tidak menggunakan protokol kriptografi atau algoritma yang dianggap sudah tidak aman.		
B4	Aplikasi tidak menggunakan kembali kunci kriptografi yang sama untuk beberapa tujuan.		
B5	Semua nilai acak dihasilkan dengan menggunakan generator bilangan acak yang aman		

OWASP

C. Komunikasi Jaringan

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

Validasi Iklan

Validasi Iklan

A. Validasi Akses Tidak Valid

No	Validasi	App 1	App 2
1	Klik atau tayangan yang dihasilkan oleh penayang yang mengeklik sendiri iklan aktif mereka		
2	Tayangan atau klik iklan berulang dari satu pengguna atau lebih		
3	Penayang yang menganjurkan agar mengeklik iklan mereka (contohnya dapat mencakup: kata-kata apa pun yang mendorong pengguna untuk mengeklik iklan; penerapan iklan yang dapat meningkatkan volume klik tidak sengaja; dsb.)		
4	Alat klik atau sumber lalu lintas otomatis, robot, atau perangkat lunak lain yang menipu		

Validasi Iklan

B. Validasi Penempatan (1/2)

No	Validasi	App 1	App 2
1	Iklan tidak boleh ditempatkan di area yang akan diklik secara acak oleh pengguna atau tersentuh jari pengguna di layar.		
2	Iklan tidak boleh ditempatkan pada layar 'buntu'. Harus disediakan cara untuk keluar dari layar tanpa mengeklik iklan (misalnya, tombol 'kembali' atau 'menu').		
3	Iklan tidak boleh ditempatkan dalam aplikasi yang berjalan di latar belakang perangkat atau di luar lingkungan aplikasi tersebut.		

Validasi Iklan

B. Validasi Penempatan (2/2)

No	Validasi	App 1	App 2
4	Iklan tidak boleh ditempatkan dengan cara yang akan mencegah penayangan konten inti aplikasi.		
5	Iklan tidak boleh ditempatkan dengan cara yang mengganggu penjelajahan atau interaksi dengan konten inti dan fungsi aplikasi. Contohnya: iklan pengantara yang terpicu setiap kali pengguna mengeklik dalam aplikasi.		
6	Penayang tidak diizinkan untuk menempatkan iklan pada laman yang bukan berbasis konten seperti layar terima kasih, kesalahan, masuk, atau keluar		

Validasi Iklan

C. Validasi Kebijakan Konten

No	Validasi	App 1	App 2
1	Konten vulgar		
2	Konten yang menganjurkan agar menentang seseorang, kelompok, atau organisasi		
3	Materi yang dilindungi hak cipta		
4	Narkoba, alkohol, dan konten yang berkaitan dengan tembakau		
5	Konten hacking and cracking		
6	Konten kekerasan		
7	Konten yang berkaitan dengan senjata		
8	Aplikasi yang menggunakan karakteristik Merek Google		
9	Pelanggaran Hak Cipta		
10	Aplikasi yang menawarkan program kompensasi		
11	Konten buatan pengguna		
12	Konten ilegal lainnya		

Q & A