**MR.PR3D4T0R**

**5. Hasil Security Penetration Testing Fase 1**

**5.1 Allow Backup True**

|  |
| --- |
| Deskripsi: |
| Kami mendeteksi bahwa aplikasi Diva menginzinkan backup dengan debuggabel hal ini berbahaya karena data aplikasi Diva bias saja di curi mengunakan Android Debug Bridge(ADB) |
| Risiko: |
| High |
| Sumber: |
| AndroidManifest.xml |
| Standar: |
| MSTG-STORAGE-8 |
| Bukti: |
|  |
| Informasi Pendukung |
| <https://developer.android.com/reference/android/app/backup/BackupAgent>  <https://developer.android.com/reference/android/app/backup/BackupAgentHelper.html> |
| Solusi |
| Kami menyarankan untuk mengubah Value dari android:allowBackup="true" menjadi android:allowBackup="false " |
|  |
| Status |
| OPEN |

**5.2 Insecure Logging Vulnerability**

|  |
| --- |
| Deskripsi: |
| Kami mendeteksi Aplikasi Diva mengunnakan logging di mana aplikasi lain di dalam android tersebut dapat mengakses dan mengetahui proses dari aplikasi yang di lakukan oleh aplikasi Diva. |
| Risiko: |
| High |
| Sumber: |
| LogActivity |
| Standar: |
| MSTG-STORAGE-3 |
| Bukti: |
|  |
| Informasi Pendukung |
| <https://github.com/OWASP/owasp-mastg/blob/master/Document/0x05d-Testing-Data-Storage.md#testing-logs-for-sensitive-data-mstg-storage-3>  <https://www.guardsquare.com/manual/configuration/examples#logging> |
| Solusi |
| Kami menyarankan mengunakan ProGuard untuk menentukan semua fungsi log terhapus |
| Status |
| OPEN |

**5.3 HardCoding Vulnerability**

|  |
| --- |
| Deskripsi: |
| Kami Mendeteksi aplikasi Diva menyertakan Informasi rahasia di dalam code di mana inforamasi sensitive ini tidak seharunya di ikut sertakan di dalam code karena dapat di gunakan dalam hal-hal yang buruk |
| Risiko: |
| High |
| Sumber: |
| HardcodeActivity |
| Standar: |
| MSTG-CRYPTO-1 |
| Bukti: |
| Kami juga mendeteksi bahwa source code aplikasi Diva menuliskan beberapa data user |
| Informasi Pendukung |
| <https://github.com/OWASP/owasp-mastg/blob/master/Document/0x04g-Testing-Cryptography.md#common-configuration-issues-mstg-crypto-1-mstg-crypto-2-and-mstg-crypto-3> |
| Solusi |
| Kami menyarankan untuk tidak menyimpan data rahasia di dalam source codenya |
| Status |
| OPEN |

**5.4 Insecure Data Storage**

|  |
| --- |
| Deskripsi: |
| Kami mendeteksi bahwa Diva applikasi menyimpan data login ke sharePreferences hal ini praktik yang kurang aman karena aplikasi lain bisa mengetahui kredensial login user di aplikasi Diva. |
| Risiko: |
| High |
| Sumber: |
| InsecureDataStorage1Activity |
| Standar: |
| MSTG-STORAGE-2 |
| Bukti: |
| 1. Menginzinkan menyimpan data login ke SharedPreferences       2. Kami juga mendeteksi Diva aplikasi menyimpan data di lokasi yang local database      3. Kami juga mendeteksi bahwa Diva aplikasi melakukan penyimpanan data login di folder sementara yaitu di tmp hal ini praktik yang kurang aman karena data login bisa saja di curi oleh aplikasi lain yang berjalan pada aplikasi.      4. Kami juga mendeteksi bahwa Diva application melakukan penyimpanan data penting ke sdcard hal ini praktik yang kurang aman karena data bisa saja di curi oleh aplikasi pihak ke tiga. |
| Informasi Pendukung |
| <https://developer.android.com/reference/android/content/SharedPreferences.html> |
| Solusi |
| Kami menyarankan untuk melakukan enkripsi pada saat menyimpan data penting ke sharepreferensi. |
| Status |
| OPEN |

**5.5 Input Validation Vulnerability**

|  |
| --- |
| Deskripsi: |
| Kami mendeteksti bahwa aplikasi Diva memiliki keretanan sql injection di mana kami bisa mengetahui isi dari data base di dalam aplikasi diva |
| Risiko: |
| High |
| Sumber: |
| Aplikasi diva  Input Validation Input |
| Standar: |
| MSTG-ARCH-2 |
| Bukti: |
|  |
| Informasi Pendukung |
|  |
| Solusi |
|  |
| Status |
| OPEN |

**5.6 Input Validation Vulnerability**

|  |
| --- |
| Deskripsi: |
| Kami mendeteksi bahwa aplikasi Diva mengizinkan untuk membaca url apapun dan juga file di dalam system android. Hal praktik yang kurang aman karena dapat membocorkan informasi sensitive pengguna. |
| Risiko: |
| High |
| Sumber: |
| Input Validation part2 |
| Standar: |
|  |
| Bukti: |
|  |
| Informasi Pendukung |
| https://github.com/OWASP/owasp-mastg/blob/master/Document/0x05h-Testing-Platform-Interaction.md#testing-custom-url-schemes |
| Solusi |
| Kami menyarankan untuk melakukan sanitasi pada script Code untuk menghindari pembacaan file di dalam system melalui url. |
| Status |
| OPEN |

5.7 Access Control Vulnerability

|  |
| --- |
| Deskripsi: |
| Kami mendeteksi bahwa Diva applikasi dapat di akses APICredsActivity dari external dan memunculkan data sensitive kredensial API. |
| Risiko: |
| High |
| Sumber: |
| AndroidManifest.xml |
| Standar: |
|  |
| Bukti: |
| 1. Kami melihat bahwa aplikasi diva mengizinkan pihak lain menjalankan fungsi aplikasi dari luar, dan acktifivity dari log bisa di ketahui oleh pihak aplikasi lain.          1. Access control 2 kami juga mendeteksi bahwa kami dapat melewati proses authentikasi pada Tveeter Api,        1. Access Control3 kami mendeteksi bahwa kami dapat melakukan bypass private notes dari luar aplikasi tanpa harus melakukan login di sebabkan karena memberi Izin exported=”true” pada bagian AndroidManifest.xml   Dan ini hasilnya kami bisa mengakases Private Note dari luar Aplikasi. |
| Informasi Pendukung |
| <https://developer.android.com/training/basics/intents/filters?hl=id>  <https://developer.android.com/guide/components/intents-filters?hl=id#Receiving> |
| Solusi |
| 1. Kami merekomendasikan untuk Mengatur action dan category yang benar pada Intent Filter && Kami menyarankan untuk mengubah exported="true" menjadi”false” |
| Status |
| OPEN |

**5.8 HardCoding issue part 2**

|  |
| --- |
| Deskripsi: |
| Kami mendeteksi bahwa Aplikasi Diva memiliki kerentan pada coding yang mana menyertakan data penting sebagai code autentikasi. |
| Risiko: |
| High |
| Sumber: |
| libdivajni.so |
| Standar: |
| MSTG-CRYPTO-1 |
| Bukti: |
| Kami mencoba menganalisa source code yang mana akan membuatkan class baru DivaJni.class    Dan setelah kami menganalisa code DivaJni.class kami megetahui ada libarary asli dengan nama divajni    Dan setelah itu kami mencari string pada file libdivajni.so dan mencoba menginput ke user vendor key dalam aplikasi dan hasilnya berhasil dengan string  olsdfgad;lh |
| Informasi Pendukung |
| <https://github.com/OWASP/owasp-mastg/blob/master/Document/0x04g-Testing-Cryptography.md#common-configuration-issues-mstg-crypto-1-mstg-crypto-2-and-mstg-crypto-3> |
| Solusi |
| Kami menyarankan untuk tidak menyimpan data login atau data sensitive di dalam source codenya. |
| Status |
| OPEN |

5.9 Input Validation Vulnerability

|  |
| --- |
| Deskripsi: |
| Kami mendeteksi bahwa Aplikasi Diva rentan terhadap seranga DOS di mana aplikasi tidak dapat mengalami crash dengan menginputkan beberapa strings ke dalam kolom input. |
| Risiko: |
| High |
| Sumber: |
|  |
| Standar: |
|  |
| Bukti: |
|  |
| Informasi Pendukung |
|  |
| Solusi |
|  |
| Status |
| OPEN |