VAPT For

Damn Vulnerable Bank

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Application can be installed on a vulnerable android version | | | | | | | |
| **Impact** | Info | **Risk Rating** | Low | | | | |
| **Ease of Exploit** | Easy | | | **Likelihood** | Low |  |  |
| **URL / Impacted System** | Damn vulnerable app | | | | | | |
| **Description** | | | | | | | |
| This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8. | | | | | | | |
| **Impact** | | | | | | | |
| Application will be more vulnerable with the previous versions as there are less fixed bugs. | | | | | | | |
| **Remediation** | | | | | | | |
| Should restrict the application to be installed on all versions and only latest version should support the packages. | | | | | | | |
| **Evidence** | | | | | | | |
| A picture containing text, electronics  Description automatically generated | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 2.Clear text traffic is enabled for application | | | | | | | |
| **Impact** | High | **Risk Rating** | High | | | | |
| **Ease of Exploit** | Difficult | | | **Likelihood** | Medium |  |  |
| **URL / Impacted System** | Damn vulnerable app | | | | | | |
| **Description** | | | | | | | |
| The “android:usesCleartextTraffic” attribute indicates whether the app intends to use cleartext network traffic, such as cleartext HTTP.  The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". | | | | | | | |
| **Impact** | | | | | | | |
| The disclosure of sensitive information can result in identity theft, regulatory fines, and civil as well as criminal penalties. | | | | | | | |
| **Remediation** | | | | | | | |
| Explicitly set the attribute android:usesCleartextTraffic value to false and define an Android Network Security Config.  The default value for apps that target API level 27 or lower is true. Apps that target API level 28 or higher default to false. | | | | | | | |
| **Evidence** | | | | | | | |
|  | | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3.Application data can be backed up | | | | | |
| **Impact** | Info | **Risk Rating** | Low |  |  |
| **Ease of Exploit** | Easy | **Likelihood** | High |  |  |
| **URL / Impacted System** | Damn vulnerable app | | | | |
| **Description** | | | | | |
| Android performs by default a full backup of applications including the private files stored on /data partition. The Backup Manager service uploads those data to the user's Google Drive account. | | | | | |
| **Impact** | | | | | |
| This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device. | | | | | |
| **Remediation** | | | | | |
| If the application contains sensitive data that you don't want to be restored, you can disable backup mode by setting the attribute android:allowBackup to false in the application tag. | | | | | |
| **Evidence** | | | | | |
|  | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4.Insertion of sensitive information into log file | | | | | | | | |
| **Impact** | | Info | **Risk Rating** | Low | | | | |
| **Ease of Exploit** | Easy | | | | **Likelihood** | Medium |  |  |
| **URL / Impacted System** | Damn Vulnerable app | | | | | | | |
| **Description** | | | | | | | | |
| Information written to log files can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information. | | | | | | | | |
| **Impact** | | | | | | | | |
| Logging sensitive user data often provides attackers with an additional, less-protected path to acquiring the information. | | | | | | | | |
| **Remediation** | | | | | | | | |
| It is highly recommended that the sensitive information should not be disclosed as attacker can manipulate the information and get access to the account.  Make sure that the web application does not pass any sensitive information in URLs. | | | | | | | | |
| **Evidence** | | | | | | | | |
| A picture containing timeline  Description automatically generated  Graphical user interface, text, application  Description automatically generated | | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 5. [App can read/write to External Storage. Any App can read data written to External Storage.](https://github.com/MobSF/owasp-mstg/blob/master/Document/0x05d-Testing-Data-Storage.md#external-storage) | | | | | | | |
| **Impact** | Info | **Risk Rating** | Low | | | | |
| **Ease of Exploit** | Easy/Difficult/Theoretical/Automated Tools Available | | | **Likelihood** | High |  |  |
| **URL / Impacted System** | Damn vulnerable app | | | | | | |
| **Description** | | | | | | | |
| During installation, installed file permissions are set to allow anyone to modify those files. | | | | | | | |
| **Impact** | | | | | | | |
| This can result in data loss, Identity theft, Privacy violation, Fraud. | | | | | | | |
| **Remediation** | | | | | | | |
| URL caching, keyboard press caching maybe help in this | | | | | | | |
| **Evidence** | | | | | | | |
| Graphical user interface, text, application  Description automatically generated | | | | | | | |