

Android Security & Exploitation



Aditya Gupta (@adi1391)

Founder, Attify (<http://attify.com>)

adi@attify.com

Certifications : <http://securitytube-training.com>

Pentester Academy : <http://PentesterAcademy.com>

Android Permissions

Android Permissions

- Defined in `AndroidManifest.xml` file
- Have to be specified by the developer
- Can't be added later on
- All or None Flaws : for eg : Android <4.0 doesn't need `READ_EXTERNAL_STORAGE` to read SD Card

AndroidManifest.xml

- Specifies properties of the application
- Package Name
- Activities, Services, Broadcast Receivers etc.
- Permissions definitions and usage
- Info on external libraries
- SharedUID

Going deeper

- Each app is assigned to a unique UID
- In some cases, two apps could even have a same UID
- Apps could belong to multiple GIDs depending on the permissions needed by the app
- Stored at `/data/system/packages.xml`
- Permission to group mappings located at `/etc/permissions/platform.xml`