Android Security & Exploitation

Aditya Gupta (@adi1391)

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

adi@attify.com

Certifications : http://securitytube-training.com
Pentester Academy : http://PentesterAcademy.com

Introduction to Drozer

Introduction to Drozer

- Framework written for Android Application Assessment and Exploitation by MWR InfoSecurity
- Written on iPython
- Has modules such as Leaking Content Providers, LFI, Scanning, Reverse Shell etc
- Extensible via own modules

Drozer Kung Fu

- To get a list of all the installed apps
  - run app.package.list

- To find the attack surface
  - run app.package.attacksurface [package-name]

- Finding the content providers
  - run app.provider.finduri [package-name]

- Querying the content provider
  - run app.provider.query [content uri]

Drozer Kung Fu

- To get a list of all the debuggable apps
  - run app.package.debuggable

- To find the vulnerable content providers
  - run scanner.provider.finduris -a [package-name]

- Reading files via content providers
  - run app.provider.read [content-uri]/../../[file-name]

- Insering values in content provider
  - run app.provider.insert[content uri] --[type] [value-name] [values]