Android Security & Exploitation

Aditya Gupta (@adi1391)

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

adi@attify.com

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

Bypassing SSL Pinning

Bypassing SSL Pinning manually

- App : SSLPinningExample.apk
- Decompile the APK
- Find the methods responsible for validating the trustness of the cert
- Patch the method by simply removing the code lines
- Refer to : Bypassing SSL Pinning paper by Denis Andzakovic

SSL Pinning

- Setting breakpoints at `HttpsURLConnection`
- Setting breakpoints at `HttpsURLConnection.setSocketFactory()`
- Modifying the local variables
- AndroidSSLTrustKiller by iSecPartners
- Will see more of it in iOS