# Android Security & Exploitation


## Aditya Gupta (@adi1391)

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

**adi@attify.com**


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

# How do you make changes permanent

- Debugging and Hooking are good, but not permanent solutions

- Patching application by reversing might be too much complicated and time and effort consuming

- Can use Cydia substrate or Xposed framework to make changes whenever an API is called

# Hooking using Cydia Substrate

- Platform for customizing software
- Cydia provides an API using which we can hook into method and API calls
- Modify the behavior of other apps installed on the device
- Really convenient for permanent patching of apps
- Will use the example by GDS Security - Listlock (https://github.com/GDSSecurity/SubstrateDemo)

# Cydia Substrate API

- **MS.hookClassLoad** notifies whenever a particular class gets active

- Once we know that a class has been loaded, we can then use MS.hookMethod

- More info at http://www.cydiasubstrate.com/api/java/MS.hookClassLoad/

# Cydia Substrate API

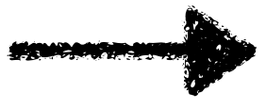
```
MS.hookClassLoad("AuthenticationMethod", new MS.ClassLoadHook()
{
public void classLoaded(Class<?> _class)
{
/* do something with _class argument */
/* Change variable values, change return type etc. */
});
```

# ListLock Bypass

- Reverse the application
- Identify the method responsible for validating the password
- How we can make the authentication successful

# ListLock Bypass

**Authenticate** class



**validatePassword** method

Hook into the method

Change the boolean return value to **TRUE**