Zero to Hero - Mobile Application Testing - Android Platform

IT Security (https://nileshsapariya.blogspot.com/search/label/IT%20Security?max-results=5)

(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiX0OUzUF_eWAZ00aFQoOhFlkBKNlYdptFztlebxZqAnVMrfZ5auuT_wFJyudFUsBNZXMaImDI72L8lLYE0aAfTZaoDa6dzLBpiDa3f-jZXlapLdjhivtMKI0p1ZUlDWFdHYDnTqluBTHc/s1600/AAEAAQAAAAAAAAT4AAAAJDcwZDY3NDlmLTQ5NGUtNGQyOC04MTQwLTBmM2Y4YTQzZDU1YQ.jpg)
Imagesource (https://www.oppsvt.org/wp-content/uploads/2015/06/mobile-security.jpg)

Hello Friends,

Writing this blog post for those who struggling with `Mobile Application Testing` OR those who don't know from where to start while doing mobile app sec testing.

BEFORE WE START :-

1 For those who are champ in mobile app sec just cheers.
2 This will take your: 15-30 mins (So if you think that you have time then only go ahead)
3 This post is about

3.1 - How to setup a testing environment for mobile app sec

Back in time when I was doing my first mobile application assessment to be honest I was very much confused that how shall I initiate the testing/setup/findings and bla bla... And trust me that's the reason
"Beginning is always tough".

So I wrote this blog post to help those new beginner who wanted to learn about mobile application testing. As of now I have covered only **`Android Platform`** other platform like iOS and Windows are almost same.

Content Covered:

Case 1 :- Setting up testing environment for capturing http/https traffic
Case 2 :- What is .APK File ?
Case 3 :- What is Certificate Pinning and how to bypass ?
Case 4 :- 2 ways to test mobile application.
Case 5 :- How to install .apk file in emulator
Case 6 :- Ever Green Findings you will find during mobile app sec.

Introduction:

We live in a mobile, personal world, where nearly a billion new mobile phones ship each year. Businesses that are most efficiently adapting to today’s “app economy” are the most successful at deepening customer engagement and driving new revenues in this ever-changing world.

Hackers are increasingly aiming targets to launch attacks on high-value mobile applications across all platforms. That's where mobile application security comes into the picture.

So Lets do this.

CASE 1:- For Android Device - Capturing http/https traffic

Device Type: Android

Requirement: Smart phone(Android),WiFi Connection, Laptop,Burp suite or Fiddler (Interception)

Before we start few assumption:-

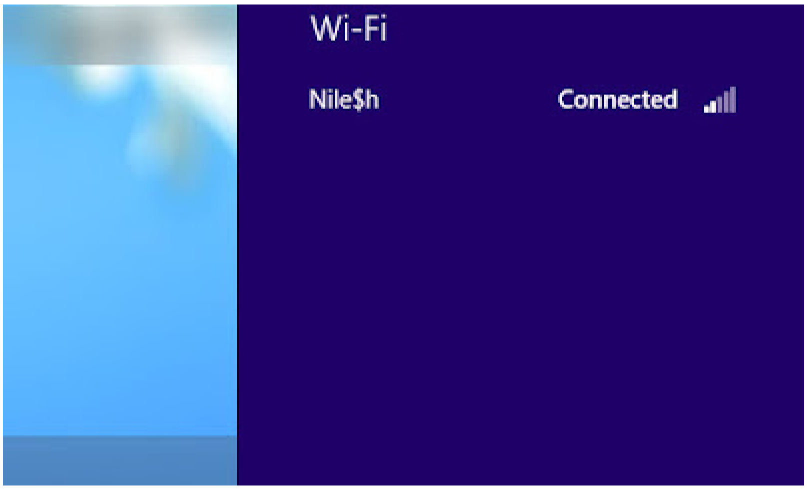
1. You have been given `**Mobile Device (Android)**` in which the application which needs to be test is Installed.
2. **Application with - No SSL Pinning**. Hold on If you not aware about what this term means than just move reading ahead at the end I have explained.

Step by Step Process for setting testing environment:

Step 1:

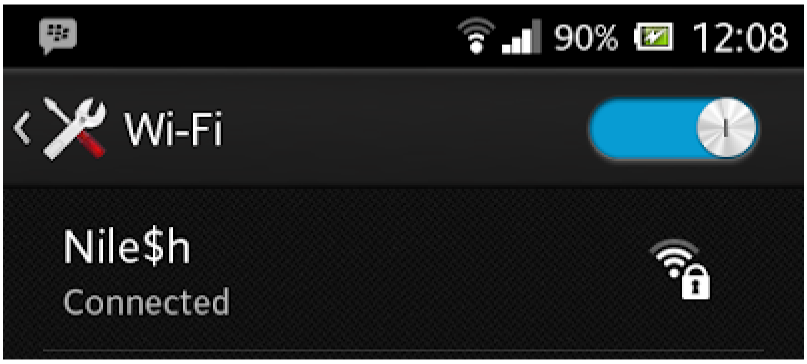
- Your **Mobile Device (Android)** and **Laptop** should be on same Wi-Fi
- If my laptop is connected to Nile$h SSID then my **Mobile Device (Android)** also be connected to Nile$h SSID and vice-versa.

Below screenshot represents the same.



(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgjHoMWQgl3klX19Wji46Ut-mZXHjRZTB1wEe4LqKPEzjAyaosGjjENAEN7sW6YK-6h3TBKvfuCcr0CZYRKmzCQU_5XXE6QuvirFvmvJ9blK8vQIaTUp7qPxvNs4BqhH6LLfGJuzMPdfaw/s1600/1_wifi.jpg)

Fig 1: Laptop connected to Nile$h SSID



(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhpkzxwnyVtkroR7Lh5MOzbGJziI81k2sAF-

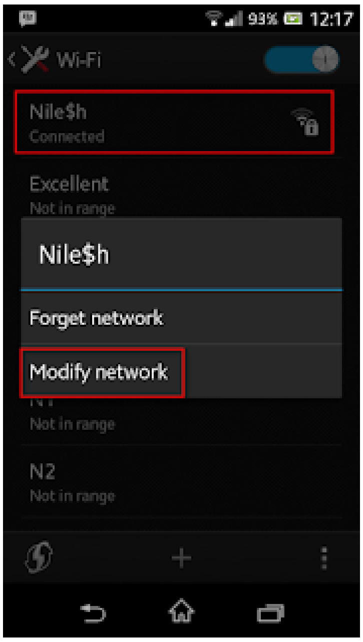
E6sX94uzZIjGA5I0os4MP3xIhfb7s_9FitHJgAdYExHRs41O2R8hNgmOgiIBnIgIc1x4CmwWNrE5oWeCn 6cLuxqjgQUdzkQaDCNy8A2dqA/s1600/Screenshot_2015-06-25-00-08-26.png)

Fig 2: Mobile device connected to Nile$h SSID

Note: Your both devices (**Mobile Device (Android)** and Laptop) Should be on same network.

Step 2:

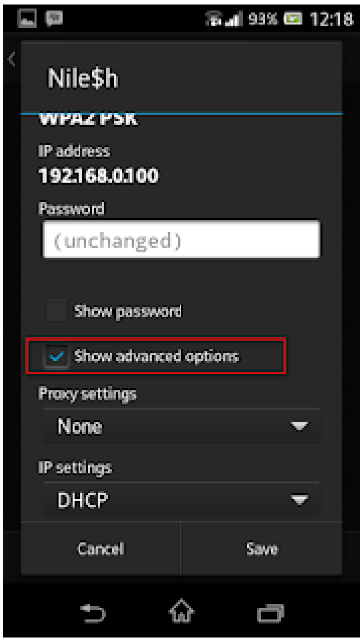
On your mobile device Press and hold on SSID name as shown below and select Modify network



(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhqf6G177vEmtNmMNltOT_J7nEok 8QVXwWWN48pSrD-tHEwnQA2FM6F-Hqzooi_KlYNoHIOvZm__qtRY2GJeV1xr2GtzlXtOYMcL_k5WH-EbCH-W872VsRWeh5Y0xxRPCB8rEspvtgH8lk/s1600/3.png)

Step 3:

Select => Show advanced option and Under Proxy setting click on manual


Nile$h

WPA2 PSK

IP address

192.168.0.100

Password

(unchanged)

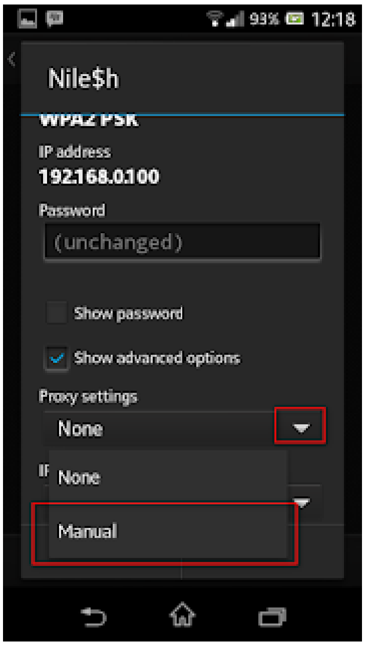
□ Show password

☑ Show advanced options

Proxy settings: None

IP settings: DHCP

(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg2W3VNf6UPgG6Hlp7ggQ5kmjbkVBChM4C9x8UdUR9wHQLQhYHyVUjUlfcp362gw6U2DFZVZSSPjZ3mcKYhLbx9AWxzGvhvQkl6Yg5SYjbQFF40L8xR_yWJeurjAoDSwF4zaBk6GXlTGJQ/s1600/4.png)


Nile$h

WPA2 PSK

IP address

192.168.0.100

Password

(unchanged)

□ Show password

☑ Show advanced options

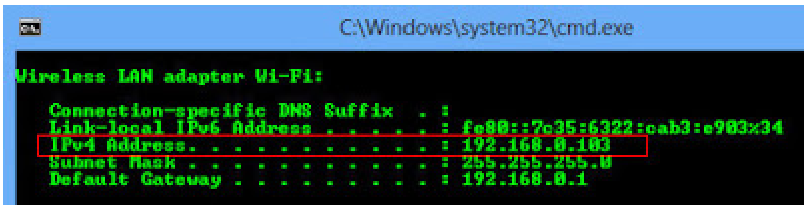
Proxy settings: None

(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhqnytphqOAGfzLBAKnBeLG5L_Tqk61COreVG4zUcCgx0tQbYWJUkWuzK1_Q9_FnRbrozNY-IU3QT3Mr52uoqiwW46VxLYtAy6dpK_KO5WguQPuzf6kMoP04P-WouUVCmjNnJxZiBh1wTo/s1600/5.png)

Step 4:

Now In this step we have to assign our Laptop IP address to **Mobile Device** setting as below:

My laptop IP Address is : 192.168.0.103



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7c35:6322:cab3:e903x34
   IPv4 Address. . . . . . . . . . . : 192.168.0.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

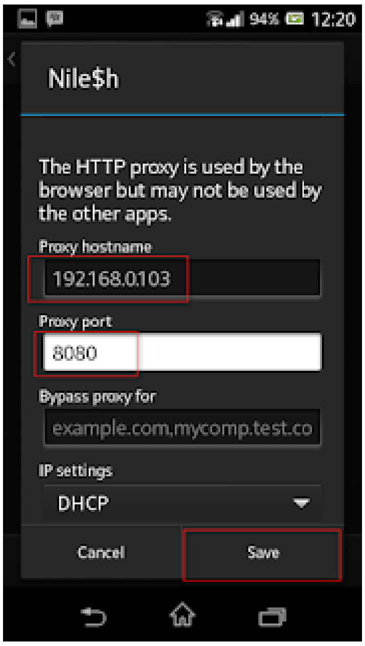
(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhMkh-hGcgbGWgDDZTBKZB8jlY_vKPQPw8Y6wjtHpqZPKe2WV6vBLLpA66XcRxJCw0kMfYeYYNXUToLYVXAVaDySYg2n6_g-Flu9crRoWkxwBBFypZhcwz24L89Pq8dyqgJ9PrMLdrh7VE/s1600/6_laptop+ip+address.jpg)

In mobile device fill details as below:

Proxy hostname : 192.168.0.103 (Your Laptop IP address)

Proxy port : 8080

Save the settings



The HTTP proxy is used by the browser but may not be used by the other apps.

Proxy hostname: 192.168.0.103

Proxy port: 8080

Bypass proxy for: example.com,mycomp.test.co

IP settings: DHCP

(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgNG1xCnCA_v1j4RetYbGOThgJQabzmZymbQaZz5oYoBY-AcfTY9IU-5t0WJ7Hm5MlYheGycKl9bwue6GSIck6ZTTxV4N2ERjMOY7jIuR7L9TVPFvi6M-Ox6W8I3ZbxZHv9hJfGsdOjwQo/s1600/7.png)

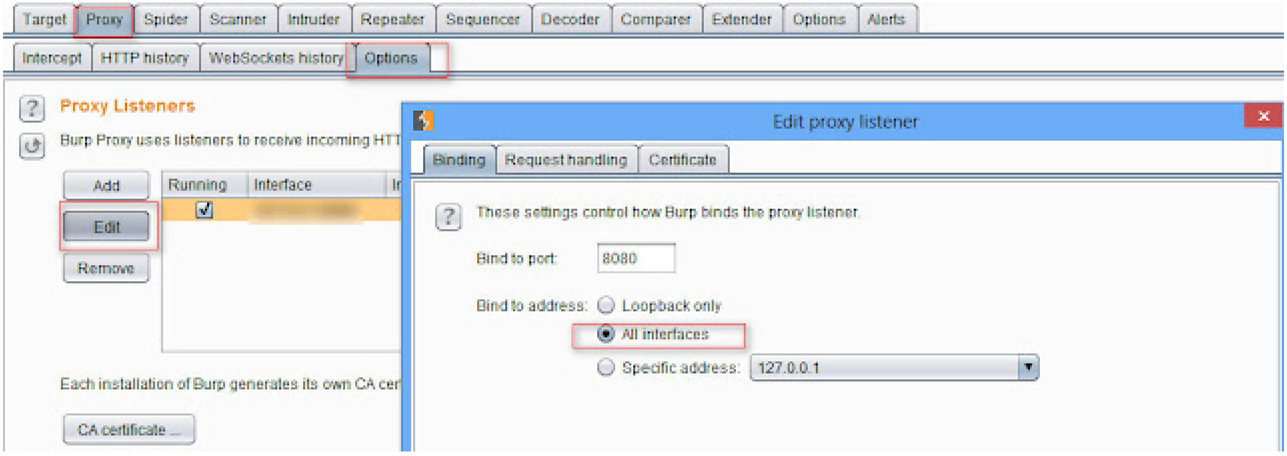
Now we have completed setting up Laptop and Mobile device.

The next step will be setting up **Interception proxy** and Installing its certificate in your mobile device.

But why ?

Now a days most of the android application transmits data over **SSL** which you cannot normally intercept using the above step. So to intercept the SSL traffic you need to import a **CA certificate** (of your host machine proxy which will be intercepting the android traffic) to the **android keystore**.

1 If you are using Burp Suite for interception then install burp suite certificate in your mobile device as below:- Open your burp suite and go to Proxy=>Options=>Edit=> Select All interfaces



Burp Proxy uses listeners to receive incoming HTT

Running	Interface	In
☑	[redacted]	

Each installation of Burp generates its own CA cer

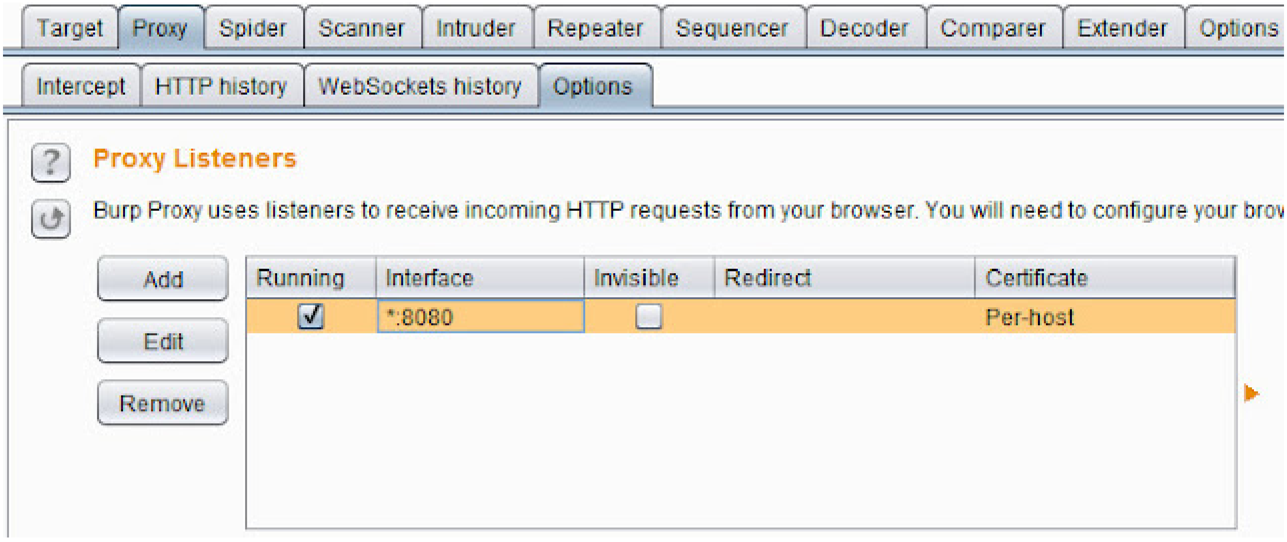
These settings control how Burp binds the proxy listener.

Bind to port: 8080

Bind to address: ○ Loopback only
● All interfaces
○ Specific address: 127.0.0.1

(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEh1CY2Lic3YBW7x6Qqc-Yu8lqKoy_8L39cIcRcM-wtVCnO3jV4InbduwuaBziyfdj_46sGUxOl2nN4Z8cGFLPMmkl2DjByJYBiar7cCtxP9Y-jyc0-It22XZfxOWzlqMbmYTcs2s6HJyCA/s1600/8_burp+setting.jpg)

It looks like as below :-



Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your brov

Running	Interface	Invisible	Redirect	Certificate
☑	*:8080	□		Per-host

(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhoFr_3QZcs4zkqdSAqMQ45CJtPQLqjbnui61b6Am907C8neNqODFuU_cr0SPHXrYhh-sq5rkj0LInzPOoUlgPAF0VevFdC9XSqtvFNQAjKbJ5lAnMksKT8Enc_HdCFnALCFNeFAMTwKa8/s1600/9_burp_Setting+_1.jpg)

Now open your Mozilla firefox browser and type:-

http://burp
Make sure your Burp intercept is on. Download the burp certificate and install in your mobile device.

2. If you are using Fiddler for interception then install fiddler certificate in your mobile device as follow:-

- Go to mobile browser and type http://ipv4.fiddler:8888 in your browser
(Port number should be same as you have set in your mobile setting)
- Download the certificate
- If you having hard time understanding the fiddler then read this How to use Fiddler When Burp Not working (https://nileshsapariya.blogspot.in/2016/04/how-to-use-fiddler-when-burp-not-working.html) . (Remember Fiddler is a savior)

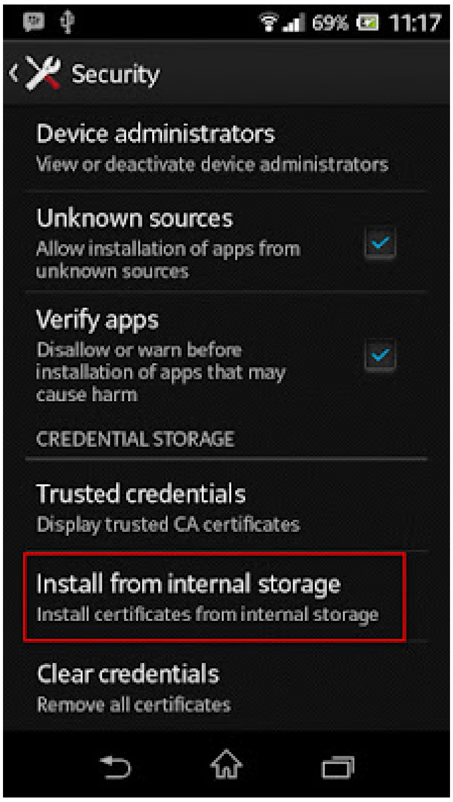
NOTE:-

While installing **Burp** OR **Fiddler** Certificate to your mobile device

Importing certificate into your mobile device:-

1] Copy the exported certificate into your mobile device, make sure you have copied that into INTERNAL STORAGE.

2] Then Go to Settings==>Security==> and select Install From internal storage



Device administrators
View or deactivate device administrators

Unknown sources ☑
Allow installation of apps from unknown sources

Verify apps ☑
Disallow or warn before installation of apps that may cause harm

CREDENTIAL STORAGE

Trusted credentials
Display trusted CA certificates

Install from internal storage
Install certificates from internal storage

Clear credentials
Remove all certificates

(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEj-3qZt_LbhB0ZVMPSqkM3xLWm-qZyi9JTQ-ym5gpYTu-2ZjplrfVLyJ3AiIuxHgKTXWnu6IlWoQgWgiip_JXC1yUrPutZto2zkCyCw8GZOqxGFu7XVuM4bJe6FHRfjjp8LcyiXP3nGtHI/s1600/9.jpg)

3] Pop-up window will comes up,simply click on OK.

4] Burp certificate is successfully installed on your mobile device.

At this point of time at one hand you will be having your Android phone and on other hand you will be checking burp suite or fiddler to play around.

Hey but we can use Emulator as well ?

Yes we can use emulator as well, though have you ever wonder why people use emulator to test the application.

Answer is :-

1 - If you are using rooted android device then its fine following CASE 1
2 - If you are using non - rooted device then I recommend to install .apk in emulator and test the app so that at the end of the day you can test the storage related findings :)

But which emulator should I use and how to install any idea ?

1 - Which emulator should I use - Genymotion

2 - How to Install Genymotion - Click here (https://nileshsapariya.blogspot.in/2016/08/how-to-install-genymotion-and.html)

So We have successfully created our test environment for testing mobile app sec. Great so lets move ahead.

Case 2: What is .APK File ?

Lets go back in time and say client gives you .apk file.

In terms of Industry Standards, before you test mobile application, testing team will provide you .apk file.

But what is APK File?

Just like Windows PC systems use a .exe file for installing software, Android does the same.
An APK file is the file format used for installing software (usually games or apps) on the Android operating system.

If your Android device lacks access to the Google Play Store, APK files may be your only option for installing apps on your device.

Some Tips:-

1. Before you can install it on your phone you will need to make sure that third-party apps are allowed on your device. So do below setting.
2. Go to Menu > Settings > Security > and check "Unknown Sources" to allow your phone to install apps from sources other than the Google Play Store.
3. If you like, you can also download an app like ES File Explorer (https://play.google.com/store/apps/details?id=com.estrongs.android.pop&referrer=utm_source%3DAndroidPIT%26utm_medium%3DAndroidPIT%26utm_campaign%3DAndroidPIT) so you can easily find files on your Android device.(only applicable for rooted devices)

Take away:-

File extension for the different mobile flavors

1. Android => .apk
2. iOS => .ipa
3. Windows => .xap ==> Burp Certificate to install is cacert.cer
4. Feature phone (Nokia, etc) => .jar [But how to test such .jar based application Answer is here (https://nileshsapariya.blogspot.in/2016/04/testing-jar-based-application.html)]

Case 3:- What is Certificate Pinning and how to bypass?

To know more about certificate pinning refer my article how to bypass ssl-pinning (https://nileshsapariya.blogspot.in/2017/02/how-to-bypass-ssl-pinning.html).

For those who don't like clicking on external links, I am providing a quick description. Its an extra layer of security which helps application to be more secure.

1 - If Certificate pinning is enable the you will not able to intercept the traffic
2- In that case you need to bypass the certificate pinning

So we understood now

- How to set up test environment for testing android mobile application
- What is .apk file and Certificate Pinning

Now lets move ahead.

Case 4:- 2 ways to test mobile application

1] Installing .apk in your mobile and test the application (CASE 1)
- In above case you have to open application by mobile phone and test the application.

2] By using Android SDK Tool OR My all time favorite Genymotion (https://nileshsapariya.blogspot.in/2016/08/how-to-install-genymotion-and.html)

(If you know other let me know will love to know more about it)

Case 5:- How to install .apk file in emulator

- Install .apk file in your emulator. (Just drag and drop .apk file in your emulator.)

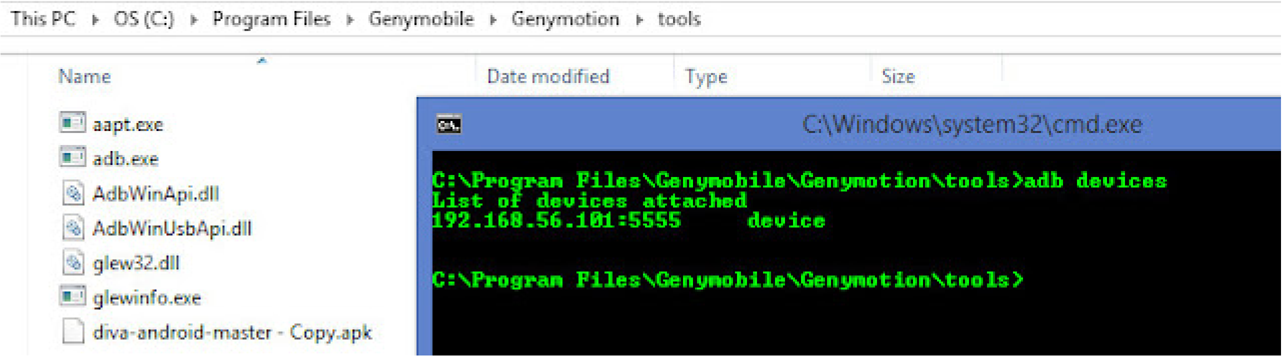
OR

- Before that check if your emulator is connected or not by following below step

  Step 1:- Go to C:\Program Files\Genymobile\Genymotion\tools

  Step 2:- Open your cmd and type
  command:-

```
adb devices
```



This PC ▸ OS (C:) ▸ Program Files ▸ Genymobile ▸ Genymotion ▸ tools
Name
Date modified
Type
Size
aapt.exe
adb.exe
AdbWinApi.dll
AdbWinUsbApi.dll
glew32.dll
glewinfo.exe
diva-android-master - Copy.apk
C:\Windows\system32\cmd.exe

```
C:\Program Files\Genymobile\Genymotion\tools>adb devices
List of devices attached
192.168.56.101:5555     device

C:\Program Files\Genymobile\Genymotion\tools>
```

(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgr0skbe_xkF2o_aASj2svDBIBu6D-t-I591KE0TGj2Kh4DuNeAEjNS9igXn81KhE6BxuoJ9CSx5VbzM1VPyEEVhdxWqli9TyBPHP3c8uhErtKxoTYIC5Thfr1cT5CPGSjkgca1DrsiV1A/s1600/1.jpg)

- Now its time to install your .apk. Type below command, but make sure you are in below directory
- C:\Program Files\Genymobile\Genymotion\tools

Command :- adb install "Path of file where your .apk is placed"
i.e. adb install C:\Users\Nilesh\Desktop\diva-beta.apk

Hey But what is "adb" ?

ADB = Android Debug Bridge

Adb is a command line tool that lets you communicate with an emulator instance or connected Android-powered device.

All adb clients use **port 5037** to communicate with the **adb server**.

Basically It is a **client-server program** that includes three components:

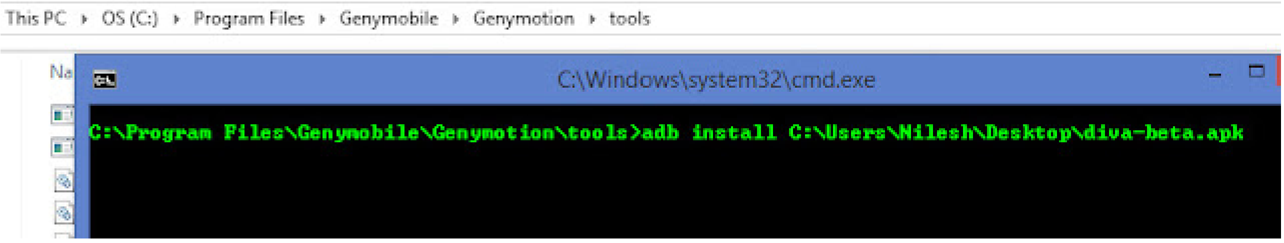
1. A client, which runs on your development machine. You can invoke a client from a shell by issuing an adb command.
2. A server, which runs as a background process on your development machine. The server manages communication between the client and the adb daemon running on an emulator or device.
3. A daemon, which runs as a background process on each emulator or device instance.

If you want to deep dive in it check this reference links (https://developer.android.com/tools/help/adb.html) hold on.. but after finishing this article so that you be in sync.

Below is the screenshot of above commands we have installed the DIVA.

DIVA is Damn Insecure and Vulnerable Application created by **Aseem Jakhar, Payatu Labs**.

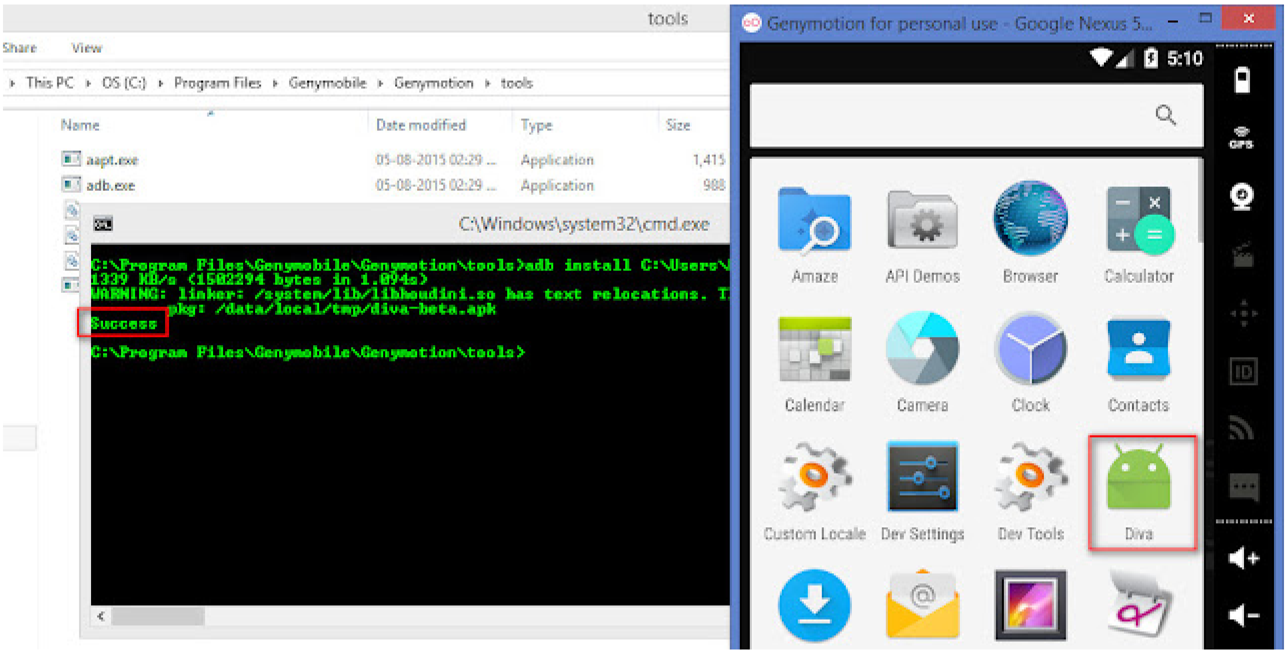
It contains various vulnerabilities including flaws in input validation, access control, hardcoding issues and a bunch more.



This PC › OS (C:) › Program Files › Genymobile › Genymotion › tools
C:\Windows\system32\cmd.exe

```
C:\Program Files\Genymobile\Genymotion\tools>adb install C:\Users\Nilesh\Desktop\diva-beta.apk
```

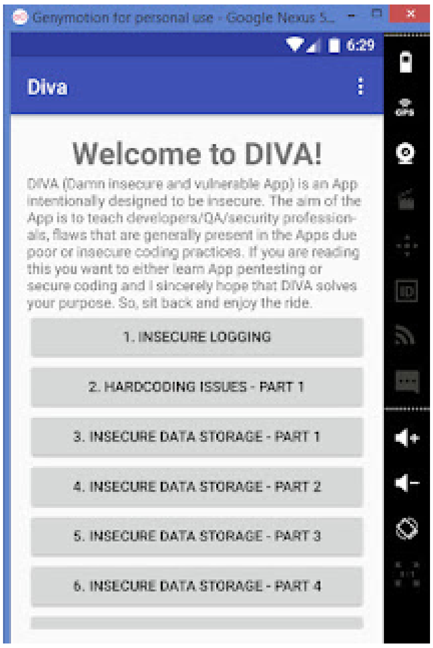
(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhuLNh-cOtEm7ba-jyxDBRCCDIkNSGtjL5PDLz-sW0K-23lVettDsmh0kF9nkz_DoPg4rt7XUNnAJsZlDjprKazd3HP3BdUVO1g1dSobaqRdI7XyV0JaEup4espYufqrZ32XcOPANauCOs/s1600/2016-04-24_143912.jpg)



```
C:\Program Files\Genymobile\Genymotion\tools>adb install C:\Users\
1339 KB/s (1502294 bytes in 1.094s)
WARNING: linker: /system/lib/libhoudini.so has text relocations. T
        pkg: /data/local/tmp/diva-beta.apk
Success

C:\Program Files\Genymobile\Genymotion\tools>
```

(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhdBeInBAXsQjzaOkSJ8zUhS1vKn9jDdumjYJz-iaN7keHG-N2Zc_fnfgya_dVFKJzH8TRR3iyZEeSAz-lebJouAM4fPRtunywLuemTLN5p6qei99EziKVa6PRibVkea4uvXwf7JmHorMo/s1600/sucess.jpg)



Welcome to DIVA!

DIVA (Damn insecure and vulnerable App) is an App intentionally designed to be insecure. The aim of the App is to teach developers/QA/security professionals, flaws that are generally present in the Apps due poor or insecure coding practices. If you are reading this you want to either learn App pentesting or secure coding and I sincerely hope that DIVA solves your purpose. So, sit back and enjoy the ride.

1. INSECURE LOGGING
2. HARDCODING ISSUES - PART 1
3. INSECURE DATA STORAGE - PART 1
4. INSECURE DATA STORAGE - PART 2
5. INSECURE DATA STORAGE - PART 3
6. INSECURE DATA STORAGE - PART 4

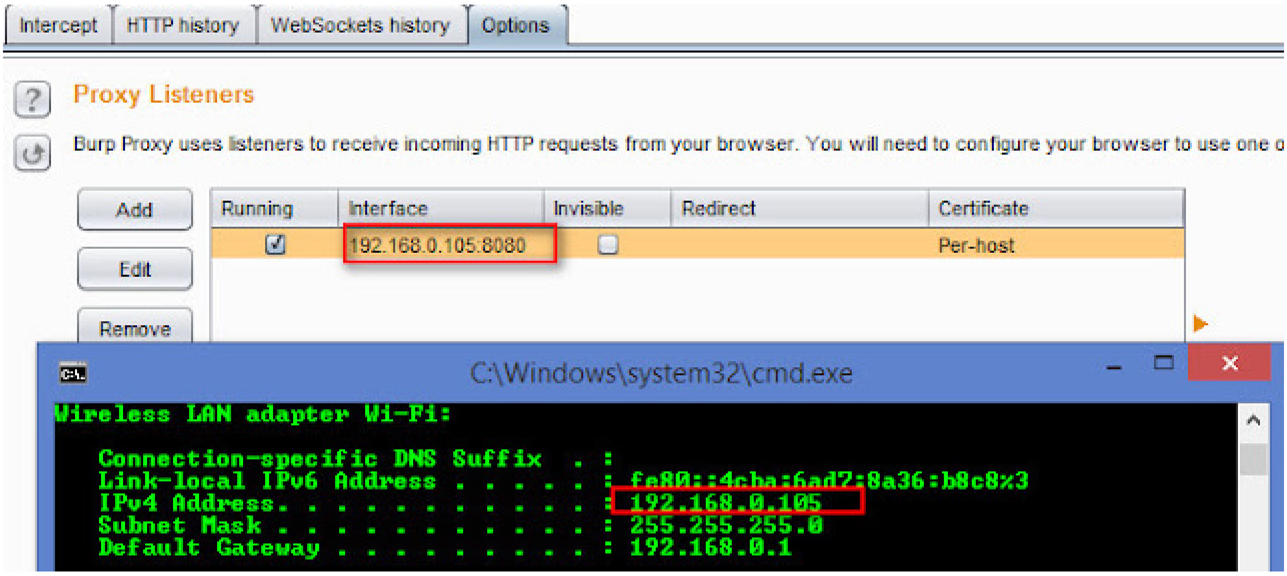
(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjTs91VNEZl0yG3P9AKO0JNOkMjv2526D97xWUsDO47A13M20xeje44Szq7TlePEZ8aYWkqSQ_FivnV2k6kckhu-uUmzWmz_bQDJkFRKS9WxCkVb2BPgnRK6XtQI-zW6rBoCeuJuXQG33o/s1600/DIVA.jpg)

So now we are all ready to hack the DIVA :)

Hey but how to intercept traffic OR Set up environment via emulator can you guide me ?

Sure its almost same as **CASE-1 Set Up**, follow simple steps:-

Step 1:- Set up burp suite
Assign your laptop wifi to burp suite with port 8080



Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one o

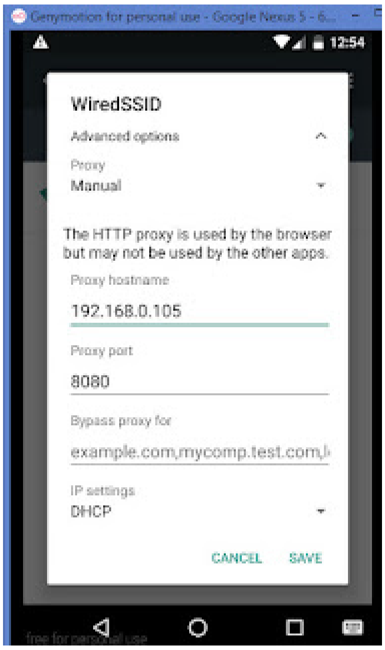
Running	Interface	Invisible	Redirect	Certificate
☑	192.168.0.105:8080	□		Per-host

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4cba:6ad7:8a36:b8c8%3
   IPv4 Address. . . . . . . . . . . : 192.168.0.105
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```

(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhxT7Remz42C7MyflblFOLQlpF3CYr7OoW_agycHFphnyJjncJstoqn4mfu-lGF9rhU69fvZ4TN1Z26oxM9ReJedqDH6Q85yfVXhzAjtexpqq9AhARmPwiRLtojPCY8iGt8tInQjvm_Tf4/s1600/1_burp+suite.jpg)

Step 2:- Set your laptop IP address under WiredSSID



WiredSSID

Advanced options

Proxy
Manual

The HTTP proxy is used by the browser but may not be used by the other apps.

Proxy hostname
192.168.0.105

Proxy port
8080

Bypass proxy for
example.com,mycomp.test.com,l

IP settings
DHCP

(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjpKKw6Qlkf1nAsfZipXWBQXnP5-IU-GJ2dWTHF4ozMdHEpu1Z4pexKi-QzVgbjhob7dUpicMlD0UNit728lTk8_Yu40aJkZnBhWxIemnDXwtDee7xqMovXq9t2-gd46LCaFUPZidGyTlY/s1600/2_.jpg)

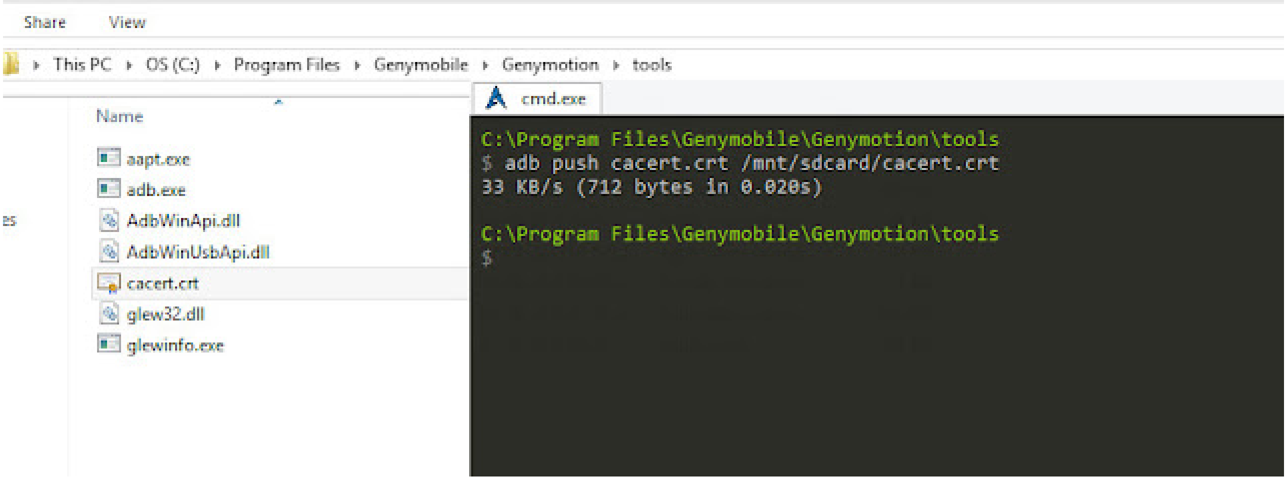
Step 3:- Installing burp certificate.

3.1 Download the burp certificate and change its extension to .crt
3.2 Move that certificate to below directory C:\Program Files\Genymobile\Genymotion\tools

Now you have to move that burp certificate in your emulator to do so run below commands.

- adb connect 192.168.56.101
- adb push cacert.crt /mnt/sdcard/cacert.crt

Where 192.168.56.101 is your emulator IP address



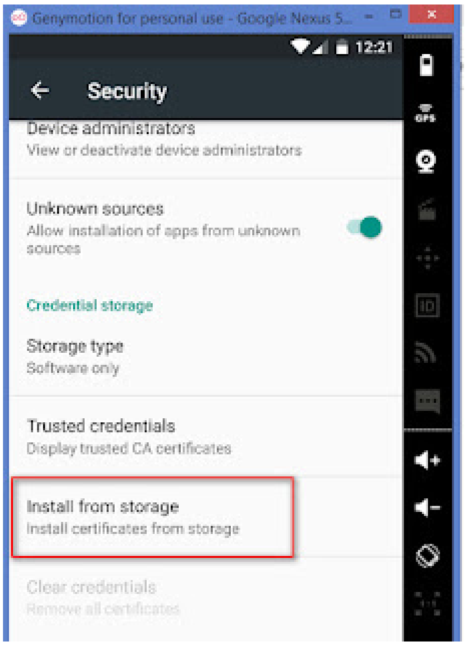
```
C:\Program Files\Genymobile\Genymotion\tools
$ adb push cacert.crt /mnt/sdcard/cacert.crt
33 KB/s (712 bytes in 0.020s)

C:\Program Files\Genymobile\Genymotion\tools
$
```

(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhqOg157lbcZ9egADMCNHrWJhxaCgb15hhsqpjOoCxMAGDTmlJcJaHsgeWNqM66T3y5d_i10Sq7dB65mfqKnwbmDbPpZ8BEcGkj6yiNgPWeWg6dt0wBQwXaBwwR3Y3CQPiI-ZaVdk9P55s/s1600/3_pushing+burp+certificate+in+mobile+emulator.jpg)

Step 4:-

- In the emulator go to Settings ==> Security
- In the Credential storage select “Install form SD Card”
- Now you can select the “cacert.crt” file present in the sd card
- Give the name cacert and click on ok
- It will ask you to set a lock screen click simply click ok and select a type of lock screen and confirm



Device administrators
View or deactivate device administrators

Unknown sources
Allow installation of apps from unknown sources

Credential storage

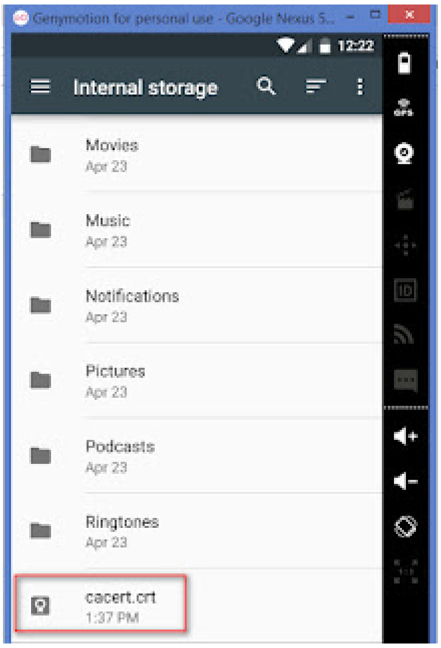
Storage type
Software only

Trusted credentials
Display trusted CA certificates

Install from storage
Install certificates from storage

Clear credentials
Remove all certificates

(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiir4T9rlSzhNwCe6tW4iTzZJjSeRGX0gj8SKysMTFbAbT5z-UJEoypuPQ6XbpotWh9A4ZKlJzIi2qh6YOhQFsVBEZf6DjX1LqH6KqTHCaG4hEl4CDkHW3KU77ds1xZ1V-ZVjZhbFXVQm0/s1600/4.jpg)



Movies
Apr 23

Music
Apr 23

Notifications
Apr 23

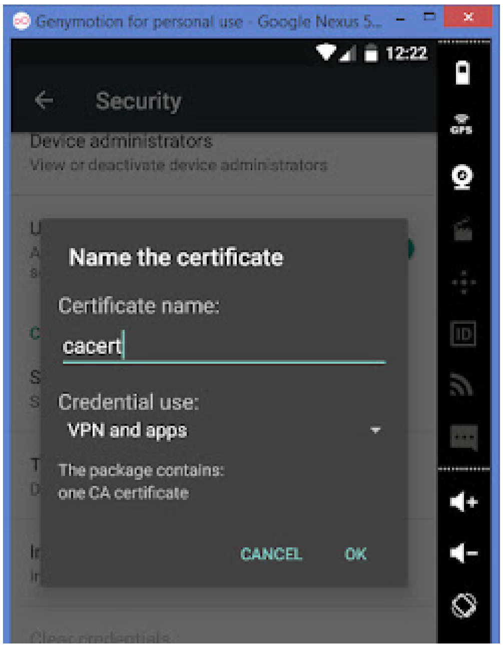
Pictures
Apr 23

Podcasts
Apr 23

Ringtones
Apr 23

cacert.crt
1:37 PM

(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjiiUPQusGqp_nIXS6CT921BLg3RsLJ1ooxCZTWQY_u1Y0koK0gJ41w4S8TRn86c653jkKFMUiGhDO-jOMQafkZ1KnfZvkuAHVhZC61i5C6RSol4g_MvGe5VQnKEJju3v9BaioRwDrLn5o/s1600/5.jpg)


Genymotion for personal use - Google Nexus 5...
12:22
Security
Device administrators
View or deactivate device administrators
CANCEL
OK
Clear credentials

Name the certificate

Certificate name:
cacert

Credential use:
VPN and apps

The package contains:
one CA certificate

(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiWzYO5eWoubxpwvJIEH3WkCkbidYYlfybM2YUr9i90dpae2BjNy6pP-kPKrkbryoMHHkjRKcundM1j_JWhAJgWAQvos0lZMLxl7WuujPpUPviN36wlU5RA1frEj82d7OWQID6SIAOP1fM/s1600/6_cacert.jpg)

Now you are all set to capture the traffic via emulator :)

So now we know all the way to setup the mobile application test bed. Now lets move and see what are different findings which we can think while testing mobile application.

Below is the list of "**Ever Green**" Findings you will find during the assessment of **Android application**

Case 6:- List of "Ever Green" Findings you will be finding in android application

List of evergreen findings in **"Android Application"**

1. Decompiling the apk file into source code to check for `` `Code Obfuscation` `` finding.
2. Sensitive information in clear text inside the `` `Local Storage` ``
3. Sensitive information in clear text inside the `` `Logs` ``
4. **Anti debugging** set to TRUE - In Android manifest file:- (Decompile the .apk file and check the manifest file)
5. **allowBackup** is set to TRUE - In Android manifest file:- (Decompile the .apk file and check the manifest file)
6. Application has set **insecure permissions** [App can read/write to External Storage] - In Android manifest file:- (Decompile the .apk file and check the manifest file)

For more in-depth detail of various bugs which you can find under mobile app sec refer :-
OWASP - Mobile Top 10 2016-Top 10 (https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10)

If you not sure how to test "Storage related findings" then refer my another blog How to test storage related findings (https://nileshsapariya.blogspot.in/2017/03/how-to-test-storage-related-findings.html)

Now we will see how to find those findings describe above.

1 - Reverse Engineering an android application OR Decompiling the apk file into source code

We can reverse engineer given .apk file to view the source code and add +1 finding code is not obfuscated if it is. Follow below simple steps

Step 1:- convert .apk to .zip file.
Step 2:- Extract .zip file content.
Step 3:- You will find classes.dex file in that folder.
Step 4:- Download dex2jar (https://sourceforge.net/projects/dex2jar/) and unzip it (Android applications are written using the java code.)
Step 5:- Put that classes.dex file in dex2jar folder.
Step 5:- Open command window at dex2jar location i.e. in my case

C:\Users\Nilesh\Desktop\M_Tools\New folder\dex2jar-2.0>

Step 6:- Run this command

```
> d2j-dex2jar.bat classes.dex
```

Step 7:- At this point of time classes-dex2jar.jar file will be created in your folder (dex2jar-2.0)

Step 8:- Download jd-gui and open that classes-dex2jar.jar file

Now you can play around with java code. And you have one finding to add in your sheet if developer miss to obfuscate the code ;)

2 Sensitive information in clear text inside the storage

Step 1:- Download the plugin for firefox - Sqlite-manager (https://addons.mozilla.org/en-us/firefox/addon/sqlite-manager/) - It is firefox extension.

After the installation you can find it in your browser under

Tools ==> SQLite Manager

Step 2:- Now you need to decompile the .apk file. To do this download apk tool or Appie.

then run the command

apktool d "apkfile.apk"

Step 3:- After de-compiling you will find many a files then check for the **.db file** and open that with Sqlite-manager (https://addons.mozilla.org/en-us/firefox/addon/sqlite-manager/)

Note:-

If you do not have "rooted device" or any "emulator" then you might not able to see the local storage of the device to deal with such situation you need to first take the entire device backup and then look for the findings related to storage.

Reference Link 1 (https://android.stackexchange.com/questions/20606/how-to-take-backup-of-all-installed-apks-from-phone-to-pc) and Link 2 (https://www.technipages.com/how-to-backup-your-entire-android-device)

If mobile device is rooted then you can follow above steps OR Download an app like **ES File Explorer** so that you can easily see internal storage related findings

To get above describe findings right away in one click you can use MOBSF security framework (https://github.com/ajinabraham/Mobile-Security-Framework-MobSF/releases).

OR

Below some of the checklist of different attacks which you need to keep in mind when you are about to perform a Mobile penetration test:-

- API assessment
- Flawed Broadcast Receivers
- Intent Sniffing and Injection
- Weak Authorization mechanism
- Local Encryption issues
- Vulnerable Activity Components
- Root Detection and Bypass
- Insecure Content Provider access
- Insecure Webview implementation
- Weak Cryptography implementation
- Application Patching
- Sensitive Information in Memory
- Insecure Logging mechanism
- Android Pasteboard vulnerability
- Application Debuggable
- Android keyboard cache issues
- Android Backup vulnerability
- Runtime Manipulation
- Insecure SDCard storage
- Insecure HTTP connections
- Parameter Manipulation
- Hardcoded secrets
- Username Enumeration issue
- Developer Backdoors
- Weak change password implementation
- Weak Pseudo Random Implementation
- Path Traversal
- Local SQL Injection
- Intent based Denial-Of-Service - SMS
- LockScreen Bypass
- Location Spoofing
- Dead Code

FAQ:-

1] Which is best emulator in which I can install my .apk if I don't want to load/Install app in my android device ?

- My all time Favorite Genymotion (https://www.genymotion.com/).
- Apart from this you can try AVD Manager (https://developer.android.com/tools/help/avd-manager.html) - which can run on Windows OS

- You can run .apk in VM Machine :- VM- MobileSec (https://mobisec.professionallyevil.com/) and Download link (https://sourceforge.net/projects/mobisec/files/)

Though go with Genymotion (https://www.genymotion.com/). Its savior ;)

2] Which are different tools which I might require to do Android testing ?

- Simply use Appie (https://manifestsecurity.com/appie/) – Android Pentesting Portable Integrated Environment.Its all in one.

3] Any demo application to test mobile app sec ?

- There are many but I recommend you to try DIVA Android (Damn Insecure and vulnerable App) (https://github.com/payatu/diva-android/) for Android by Aseem Jakhar

4] Any Solution available for DIVA ? As I am new in mobile app sec.

- Yes. Pentesting Android Apps (http://pentesteracademy.com/course?id=25) - DIVA (https://github.com/payatu/diva-android/) by Aditya Gupta (@adi1391)

5] Any scanning sort of tool or framework available which can automate the mobile app sec testing .

- Yes you should refer Mobile-Security-Framework-MobSF (https://github.com/ajinabraham/Mobile-Security-Framework-MobSF) and its documentation (https://github.com/ajinabraham/Mobile-Security-Framework-MobSF/wiki/1.-Documentation) by Ajin Abraham

6] Any MobileApp-Pentest-Cheatsheet Link.

- MobileApp-Pentest-Cheatsheet Link (https://github.com/sh4hin/MobileApp-Pentest-Cheatsheet) ; If you want to deep dive into mobile application penetration testing.

7] Good read - Introduction to the OWASP Mobile Security Testing Guide (https://b-mueller.gitbooks.io/the-owasp-mobile-security-testing-guide/content/0x03-Overview.html)

Last but not least :-

I hope you guys learn something new. If you have any suggestions or If you feel I missed out any points then do let me know OR DM. I'd love to add them to the post.

At the end of the day we all are `learner`.

+ I would like to thank my friends who taught me and helped me out to learn mobile app sec. They all know what I mean :)

Happy Mobile Hacking.

Share this

Google (https://plus.google.com/share?url=https://nileshsapariya.blogspot.com/2016/11/zero-to-hero-mobile-application-testing.html#google_vignette)

Facebook (https://www.facebook.com/sharer/sharer.php?u=https://nileshsapariya.blogspot.com/2016/11/zero-to-hero-mobile-application-testing.html#google_vignette)

Twitter (https://twitter.com/intent/tweet?text=Zero%20to%20Hero%20-%20Mobile%20Application%20Testing%20-%20Android%20Platform&url=https://nileshsapariya.blogspot.com/2016/11/zero-to-hero-mobile-application-testing.html#google_vignette)

+ More

Nilesh Sapariya ()

Author : Nilesh Sapariya