

---

# ANDROID PENETRATION TESTING LAB – GOATDROID

---

By Cloudi

December 6, 2017

Mobile Security

No Comments

---

## What is GoatDroid?

OWASP GoatDroid is a fully functional and self-contained training environment for educating developers and testers on Android security. GoatDroid requires minimal dependencies and is ideal for both Android beginners as well as more advanced users. The project currently includes two applications: FourGoats, a location-based social network, etc.

## Description

OWASP GoatDroid is a fully functional and self-contained training environment for educating developers and testers on Android security. GoatDroid requires minimal dependencies and is ideal for both Android beginners as well as more advanced users. The project currently includes two applications: FourGoats, a location-based social network, and Herd Financial, a mobile banking application. There are also several features that greatly simplify usage within a training environment or for absolute beginners who want a good introduction to working with the Android platform.

GoatDroid is composed of the following components:









- GUI application used to present information, interact with the SDK and control the web services
- Android applications containing horribly vulnerable code
- Embedded Jetty web server
- Embedded Derby database

## Configuration

Download application in here:

<https://github.com/downloads/jackMannino/OWASP-GoatDroid-Project/OWASP-GoatDroid-0.9.zip>

Extract the contents:

|   |                   |                      |                     |          |
|---|-------------------|----------------------|---------------------|----------|
|  | db                | 24/09/2012 8:39 PM   | File folder         |          |
|  | goatdroid_apps    | 24/09/2012 8:40 PM   | File folder         |          |
|  | lessons           | 24/09/2012 8:36 PM   | File folder         |          |
|  | top10             | 24/09/2012 8:36 PM   | File folder         |          |
|  | config            | 06/12/2017 10:19 ... | File                | 1 KB     |
|  | goatdroid-0.9.jar | 24/09/2012 8:36 PM   | Executable Jar File | 6,872 KB |
|  | jetty.csr         | 24/09/2012 8:36 PM   | CSR File            | 1 KB     |
|  | keystore          | 24/09/2012 8:36 PM   | File                | 2 KB     |

Goatdroid apps contains two vulnerable apps:

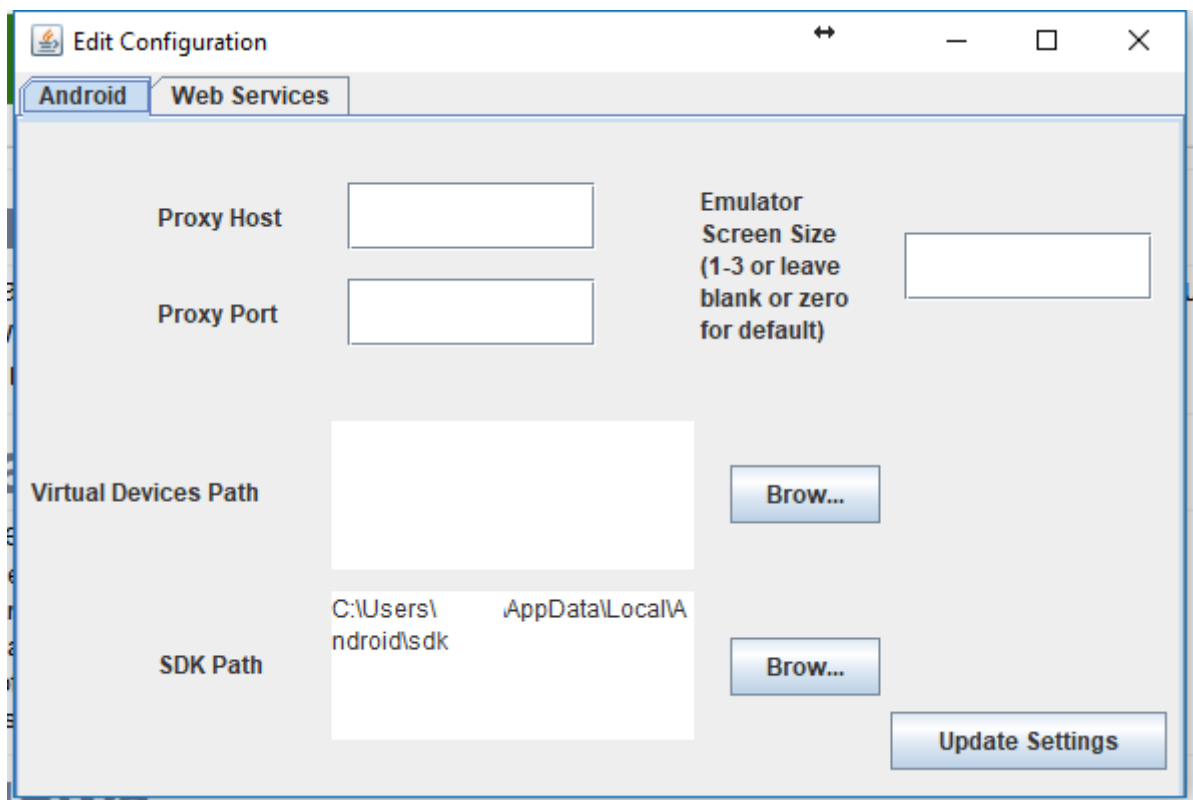
1. FourGoats
2. HerdFinancial

We will be installing these two apps in the AVD. Also, goatdroid-0.9.jar will launch the server for these two apps to communicate with.

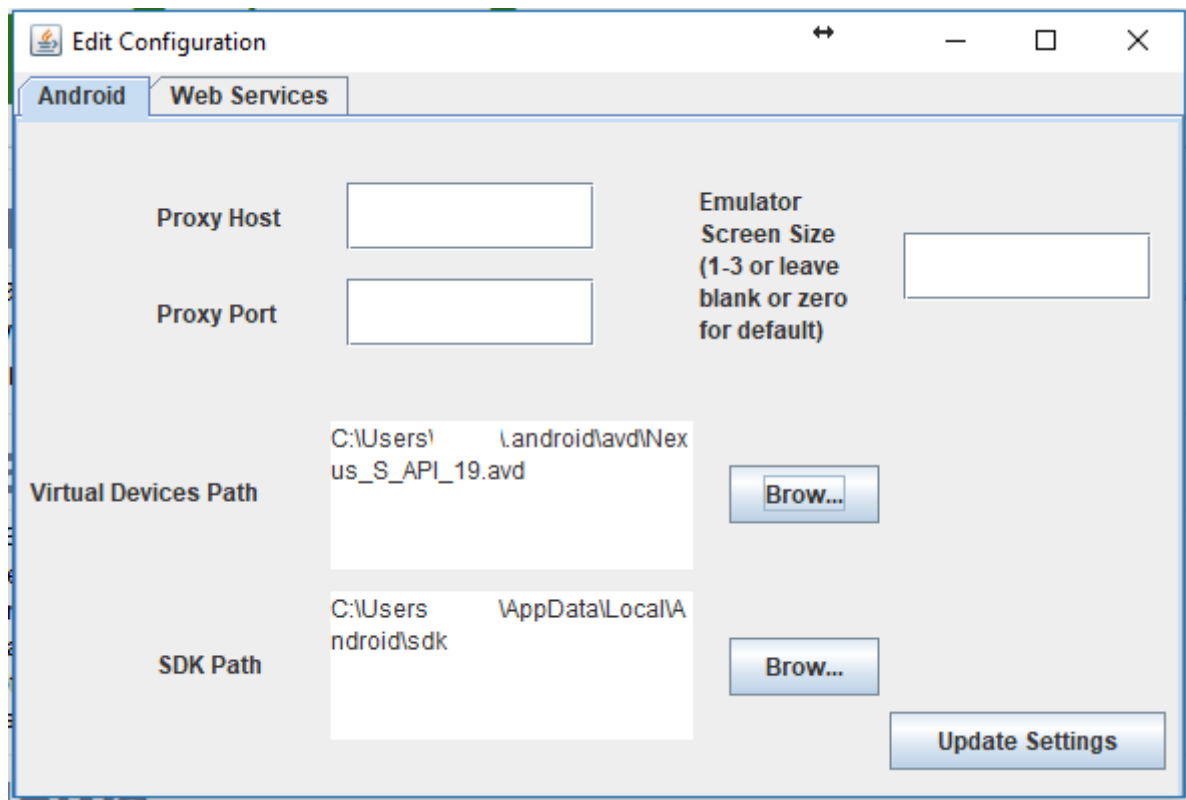
Let us launch goatdroid-0.9.jar:



You can specify the location of the virtual device and the SDK path in order to identify the virtual device that this application is going to access.  
Menu bar -> Configure -> Edit Configuration



Select your virtual devices Path and SDK path:



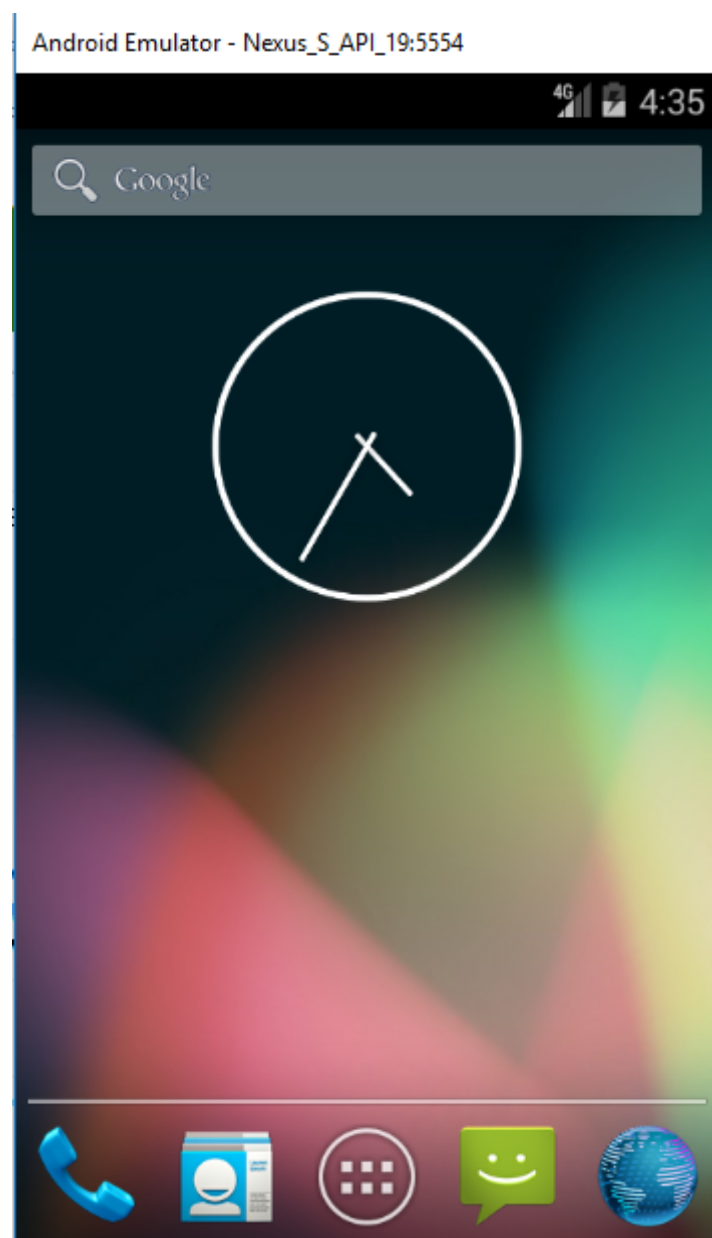
Within the GoatDroid GUI, select an app and then press the “Start Web Service” button.



Result:



Run emulator:

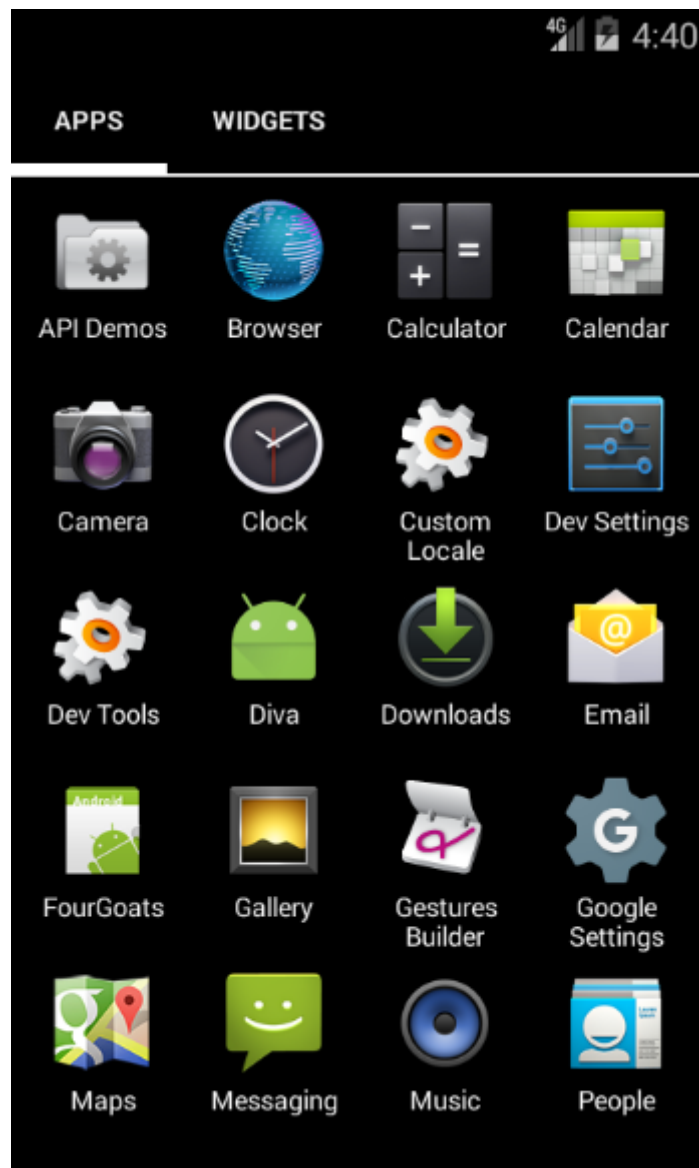


Check devices connected with adb:  
#adb devices

```
H:\alvasky\Android malware Course\Labs\OWASP-GoatDroid-0.9\OWASP-GoatDroid-0.9\goatdroid_apps\FourGoats\android_app>adb devices
adb server is out of date. killing...
* daemon started successfully *
List of devices attached
emulator-5554    device
```



Push the app of your choice either by using the GoatDroid GUI option or by using the following command:  
./adb install path-to-app/package.apk

```
H:\alvasky\Android malware Course\Labs\OWASP-GoatDroid-0.9\OWASP-GoatDroid-0.9\goatdroid_apps\FourGoats\android_app>adb install FourGoats.apk
652 KB/s (1256313 bytes in 1.879s)
WARNING: linker: libdvm.so has text relocations. This is wasting memory and is a security risk. Please fix.
  pkg: /data/local/tmp/FourGoats.apk
Success
```



Launch the application:

4G 4:41

 Login 


Username

Password

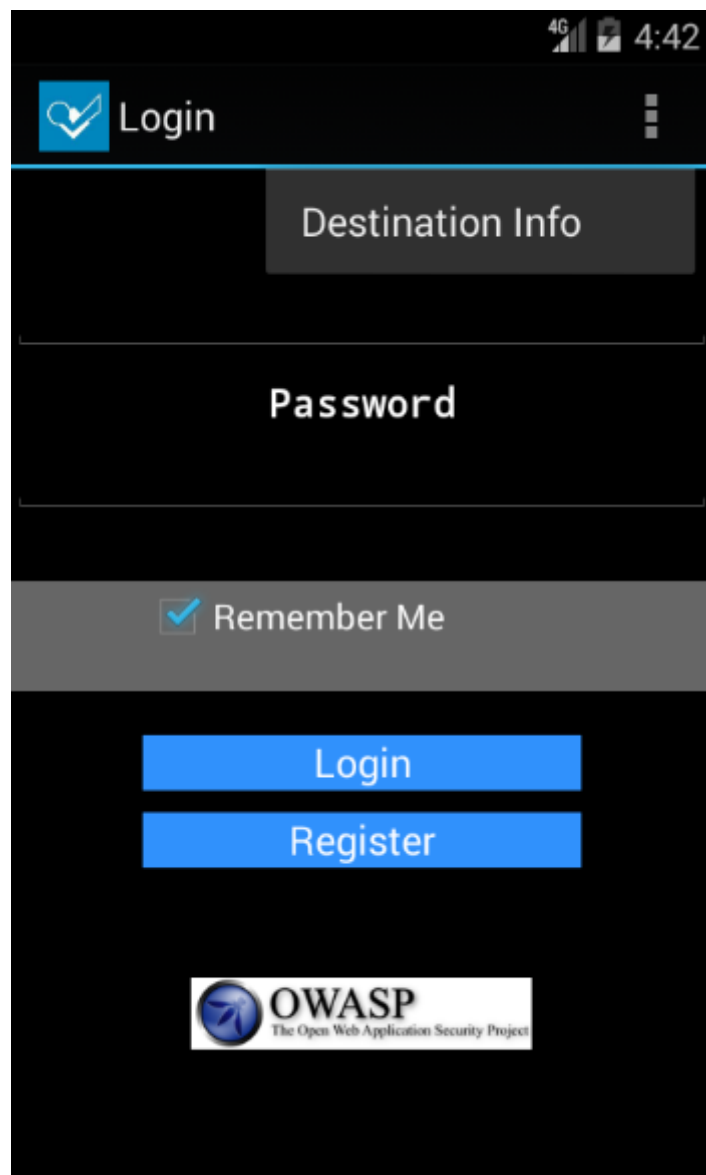
☒ Remember Me

Login

Register

 **OWASP**  
The Open Web Application Security Project

Press the menu button and select Destination Info:



A screenshot of a mobile application's login screen. The interface is dark-themed with blue and grey accents. At the top, a status bar shows '4G' signal, battery level, and the time '4:42'. Below this is a header bar with a blue checkmark icon and the word 'Login' on the left, and a three-dot menu icon on the right. The main content area consists of several sections: a grey box labeled 'Destination Info' with an empty input field below it; a section labeled 'Password' with an empty input field below it; a grey bar containing a checked checkbox and the text 'Remember Me'; and two blue buttons labeled 'Login' and 'Register' stacked vertically. At the bottom, there is a white rectangular box containing the OWASP logo (a blue circle with a white arrow) and the text 'OWASP The Open Web Application Security Project'.

4G 4:42

Login


Destination Info

Password

☒ Remember Me

Login

Register

 **OWASP**  
The Open Web Application Security Project

Enter the IP address of the host where the web service is listening, which should be your computer's IP address. This is not 127.0.0.1. The default port is 9888 for HTTPS.

The screenshot shows a mobile application interface with a black background and white text. At the top, there is a status bar with '4G' signal, a battery icon, and the time '4:47'. Below the status bar is a header bar with a blue icon of a checkmark inside a square on the left, followed by the text 'Destination Info' in white. To the right of the header bar is a vertical ellipsis menu icon. The main content area consists of several input fields and a button. The first field is labeled 'Host (Or IP)' and contains the text '192.168.1.28'. The second field is labeled 'HTTPS Port (Default:9888)' and contains the text '9888'. The third field is labeled 'Proxy Host' and is empty. The fourth field is labeled 'Proxy Port' and is empty. At the bottom of the form is a large blue button with the text 'Save' in white.

4G 4:47

Destination Info

Host (Or IP)

192.168.1.28

HTTPS Port (Default:9888)

9888

Proxy Host

Proxy Port

Save

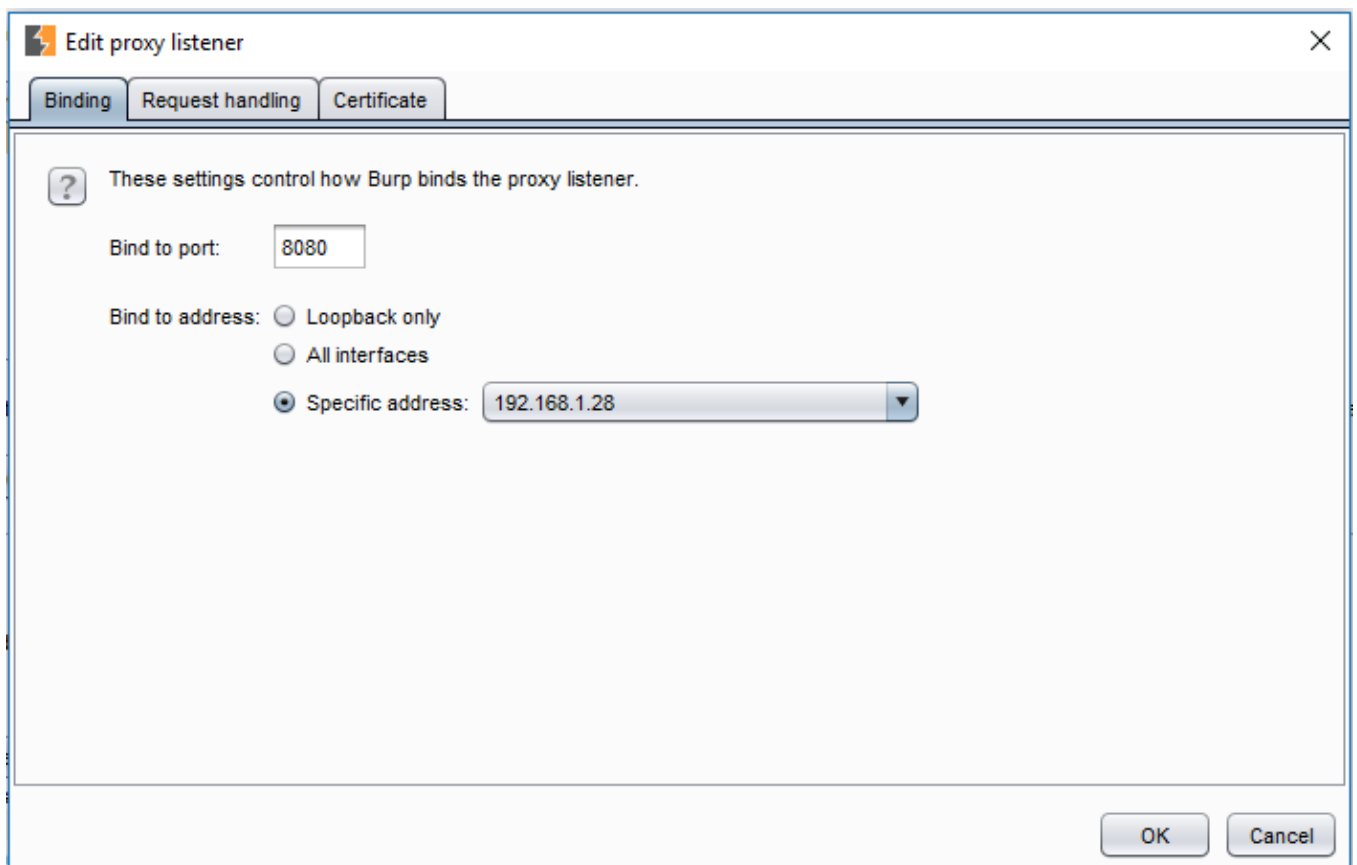
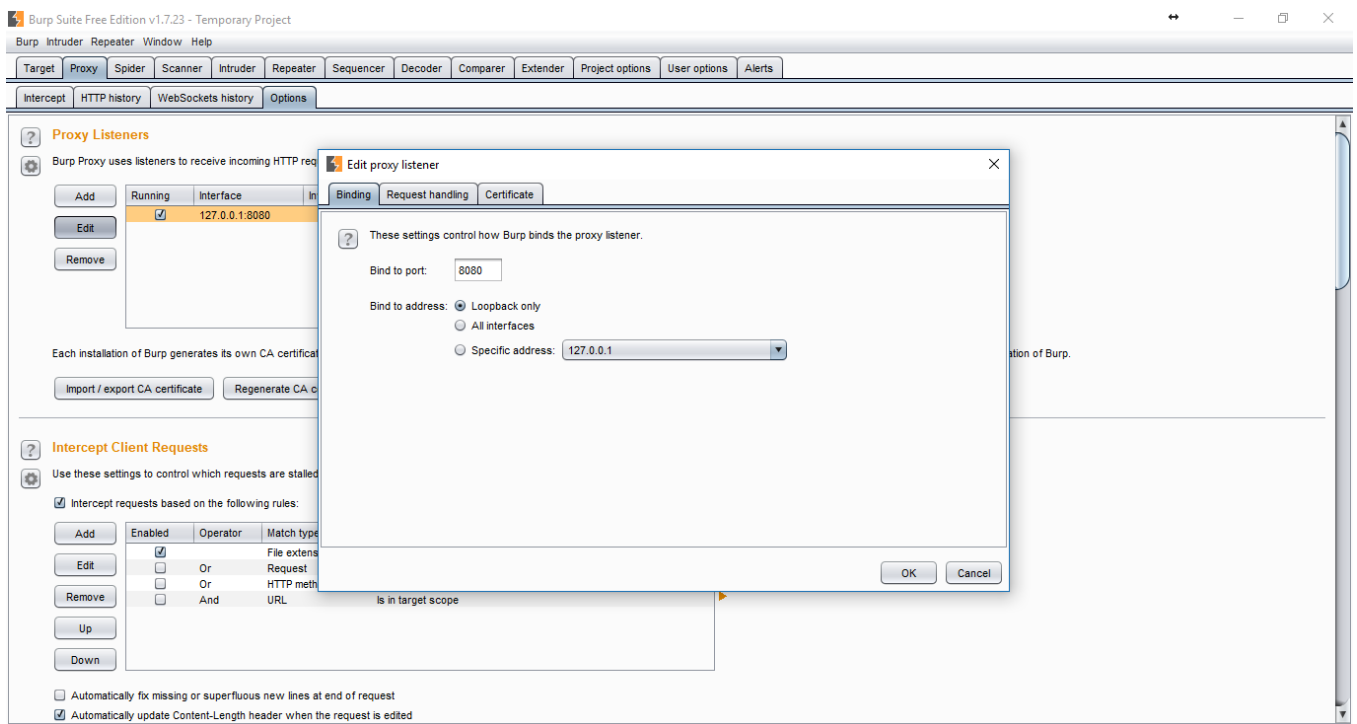
Optionally, configure the IP address for a proxy. If you wish to use an intercepting proxy to test the web services, you will want to use this.

In this post, I use Burp Suite.

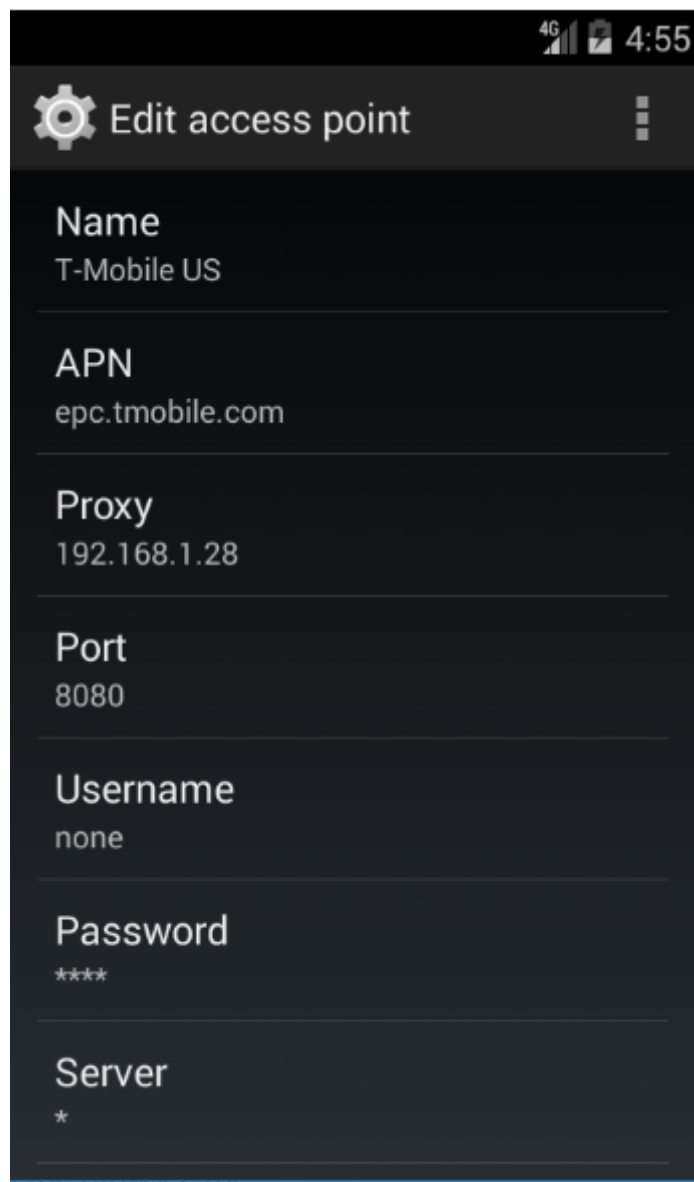
Config Burp Suite Proxy:

First, we will configure Burp Suite to listen on external interfaces. In Proxy → Options → Proxy Listeners → Edit → Binding select "Specific address" or you can also select it to listen on "All interfaces." This will allow the virtual device to connect to Burp Suite.

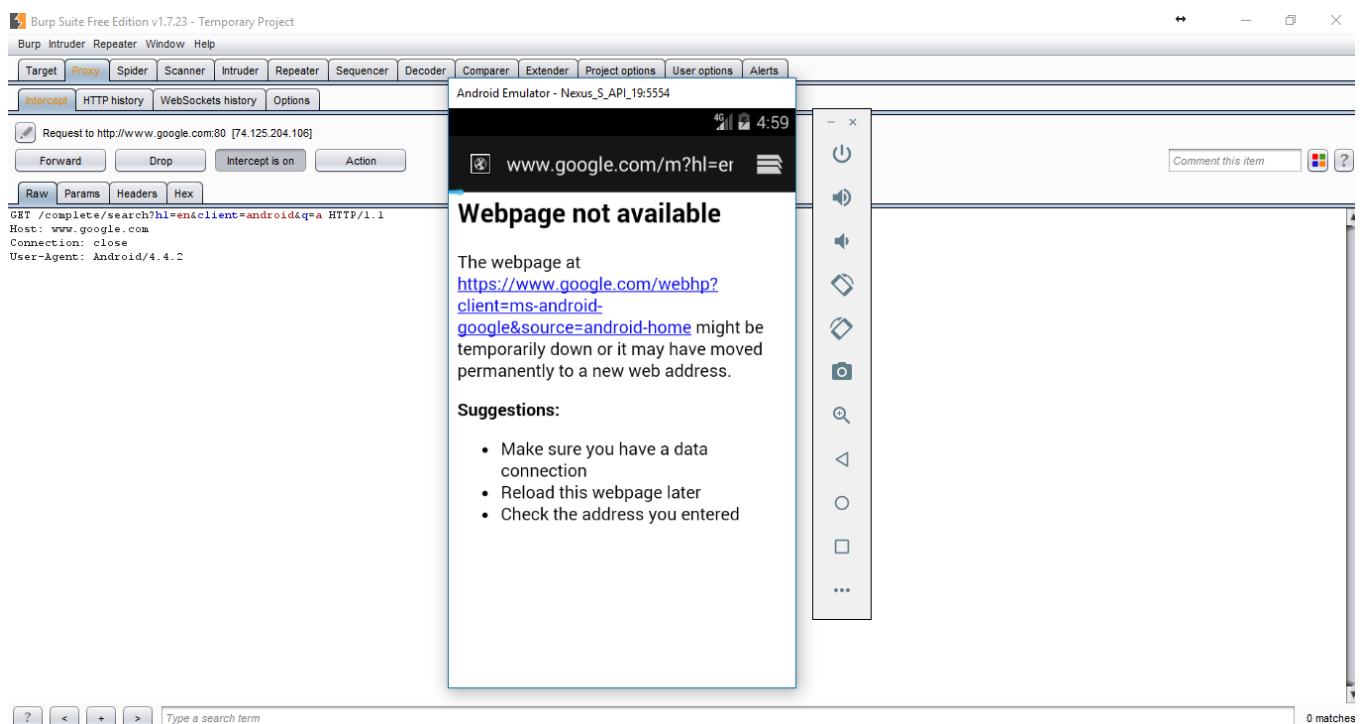




To connect to Burp Suite inside the virtual device, go to Settings → Wireless and networks → more → VPN → Mobile networks → Access Point Names → Select the default APN of the device and Edit Access point. Set the proxy and port as the IP of the main system and the port on which Burp is running. Refer to the screenshot below:



This will allow Burp Suite to intercept all the requests generated by this virtual device. As you can see in the screenshot below, when we launched the browser, the request generated to Google was intercepted by the Burp Suite proxy in the middle, which confirms that our settings are correct and are working fine.



Now, log into the application with the default credentials. In most GoatDroid apps, you may be able to register for new accounts as well.

Here I introduced the GoatDroid Lab to you. Please practice with the rest of the lab. Leave a comment if you have any difficulty during the practice.

Reference:

<https://github.com>

<http://resources.infosec>