Burp Suite for android:

Aakash R
CB.SC.P2CYS23011

Configuring an Android device to work with Burp Suite

Step 1: Configure a dedicated proxy listener in Burp

To enable Burp to intercept the HTTP traffic generated by the Android device, we need to configure a proxy listener and bind it to an open port.

1. In Burp, open the **Settings** dialog.
2. Go to **Tools > Proxy**.
3. Under **Proxy Listeners**, click **Add**.
4. On the **Binding** tab, set **Bind to port** to any available port.
5. Set **Bind to address** to **All interfaces**.
6. Click **OK** and confirm the entries when prompted.

Burp is now ready to receive HTTP traffic on the assigned port and forward it to the target web server.

Step 2: Configure your device to proxy traffic through Burp

1. On your Android device, go to the network and internet settings.
2. Open the network details for the Wi-Fi network that you want to use for testing.
3. Enter edit mode.
4. In the advanced settings, choose the option to configure a proxy manually.
5. Set the **Proxy hostname** to the IP address of the machine you're using to run Burp.
6. Set the **Proxy port** to the port you assigned to the new proxy listener you configured in Burp. For more information, see Configure a dedicated proxy listener in Burp
7. Save your changes and then connect to the Wi-Fi network. Your device's web traffic is now proxied through Burp.

Step 3: Add Burp's CA certificate to your device's trust store

Each installation of Burp has its own built-in certificate authority (CA). To work with any HTTPS traffic in Burp, we need to add the associated CA certificate to your device's trust store.

This enables Burp to impersonate the target web server during the TLS handshake. As a result, we can read and modify our HTTPS traffic in Burp just like we would with unencrypted HTTP traffic.

In Burp, open the **Settings** dialog.

- Go to **Tools > Proxy**.
- Under **Proxy Listeners**, click **Import / export CA certificate**.
- In **CA Certificate** dialog, select **Export > Certificate in DER format** and click **Next**.
- Enter a filename and location for the certificate. Note that you need to explicitly include the .der file extension.
- Click **Next**. The dialog indicates that the certificate was successfully exported.
- Add the certificate to your device's trust store.

Step 4: Test the configuration

- In Burp, go to the **Proxy > Intercept** tab.
- Use the button to turn the **Intercept** feature on.
- On your Android device, open the browser.
- Browse to any site using HTTPS. If you've completed the configuration successfully, the page should load without any security warnings and you should see your traffic in Burp on the **Proxy > HTTP history** tab.