PRACTICAL

Shaheed Sukhdev College of Business Studies
University of Delhi

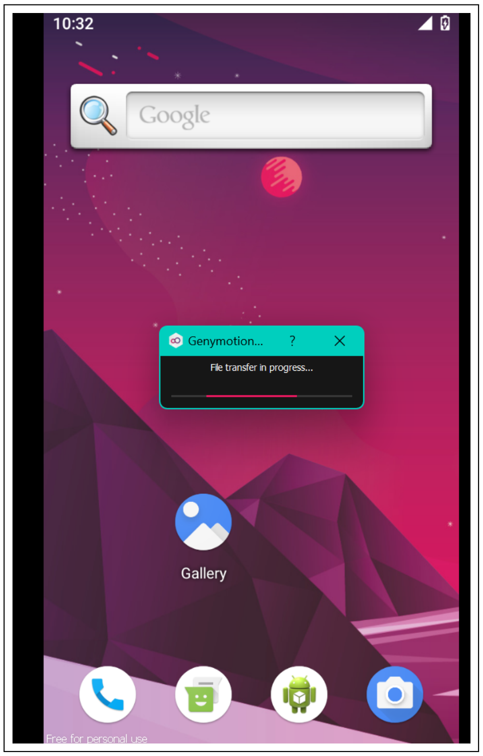
Post Graduate Diploma in Cyber Security and Law

Sakshi Garg • Roll no-23726 • Subject- Mobile Eco- System Security • Semester-II

Proof of Concept

Vulnerability and Penetration testing in Insecure Shop

1. Download the vulnerable apk in the device
   `https://github.com/optiv/InsecureShop/releases/download/v1.0/InsecureShop.apk`
2. Send this apk to GenyMotion

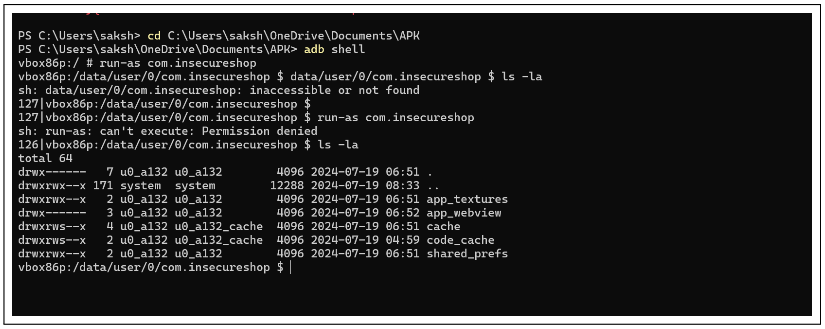


Vulnerability 2: Insecure Data Storage

Anyone can 'run-as' the application in order to view the contents of its internal storage.

Commands used-

(a) adb shell
(b) run-as com.insecureshop
(c) ls -la

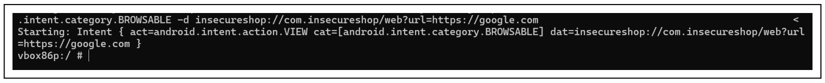


```
PS C:\Users\saksh> cd C:\Users\saksh\OneDrive\Documents\APK
PS C:\Users\saksh\OneDrive\Documents\APK> adb shell
vbox86p:/ # run-as com.insecureshop
vbox86p:/data/user/0/com.insecureshop $ data/user/0/com.insecureshop $ ls -la
sh: data/user/0/com.insecureshop: inaccessible or not found
127|vbox86p:/data/user/0/com.insecureshop $
127|vbox86p:/data/user/0/com.insecureshop $ run-as com.insecureshop
sh: run-as: can't execute: Permission denied
126|vbox86p:/data/user/0/com.insecureshop $ ls -la
total 64
drwx------   7 u0_a132 u0_a132        4096 2024-07-19 06:51 .
drwxrwx--x 171 system  system        12288 2024-07-19 08:33 ..
drwxrwx--x   2 u0_a132 u0_a132        4096 2024-07-19 06:51 app_textures
drwx------   3 u0_a132 u0_a132        4096 2024-07-19 06:52 app_webview
drwxrws--x   4 u0_a132 u0_a132_cache  4096 2024-07-19 06:51 cache
drwxrws--x   2 u0_a132 u0_a132_cache  4096 2024-07-19 04:59 code_cache
drwxrwx--x   2 u0_a132 u0_a132        4096 2024-07-19 06:51 shared_prefs
vbox86p:/data/user/0/com.insecureshop $
```

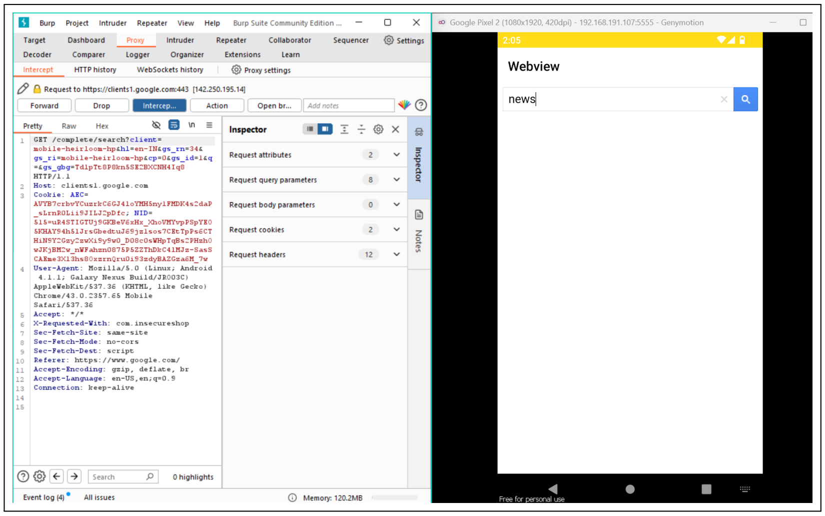
Vulnerability 3: Lack of SSL Certificate Validation

Command used-

adb shell am start -a android.intent.action.VIEW -c android.intent.category.BROWSABLE -d insecureshop://com.insecureshop/web?url=https://google.com



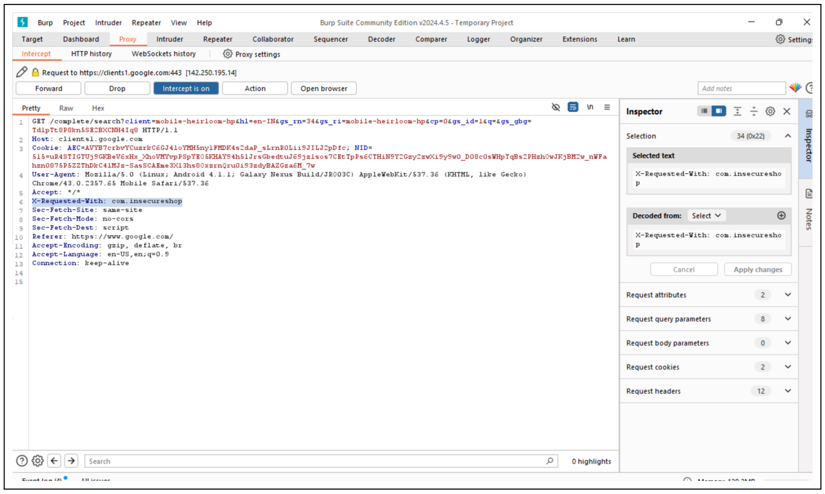
```
.intent.category.BROWSABLE -d insecureshop://com.insecureshop/web?url=https://google.com                    <
Starting: Intent { act=android.intent.action.VIEW cat=[android.intent.category.BROWSABLE] dat=insecureshop://com.insecureshop/web?url
=https://google.com }
vbox86p:/ #
```



Request to https://clients1.google.com:443 [142.250.195.14]

```
GET /complete/search?client=mobile-heirloom-hp&hl=en-IN&gs_rn=34&gs_ri=mobile-heirloom-hp&cp=0&gs_id=1&q=&gs_gbg=TdlpTt8P8kn5SE2BXCNH4Iq8 HTTP/1.1
Host: clients1.google.com
Cookie: AEC=AVYB7crbvYCuzrkC6GJ4loYMH5ny1FMDK4s2daP_sLrnROLii9JILJ2pDfc; NID=515=uR4STIGTUj9GKBeV6xHx_XhoVMYvpPSpYE05KHAY94h5lJrsGbedtuJ69jzlsos7CEtTpPs6CTHiN9Y2Gzy2zwXi9y9w0_D08c0sWHpTqBs2PHzh0wJKjBM2w_nWFahzn0875P5ZZThDkC41MJz-SasSCAEme3X13hs80xzrnQru0i93zdyBAZGza6M_7w
User-Agent: Mozilla/5.0 (Linux; Android 4.1.1; Galaxy Nexus Build/JR003C) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.65 Mobile Safari/537.36
Accept: */*
X-Requested-With: com.insecureshop
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

Try to search some stuff up and intercept the request. If someone can intercept the https request for the search query, then it is verified that the app does not properly validate SSL certs



Request to https://clients1.google.com:443 [142.250.195.14]

```
GET /complete/search?client=mobile-heirloom-hp&hl=en-IN&gs_rn=34&gs_ri=mobile-heirloom-hp&cp=0&gs_id=1&q=&gs_gbg=TdlpTt8P8kn5SE2BXCNH4Iq8 HTTP/1.1
Host: clients1.google.com
Cookie: AEC=AVYB7crbvYCuzrkC6GJ4loYMH5ny1FMDK4s2daP_sLrnROLii9JILJ2pDfc; NID=515=uR4STIGTUj9GKBeV6xHx_XhoVMYvpPSpYE05KHAY94h5lJrsGbedtuJ69jzlsos7CEtTpPs6CTHiN9Y2Gzy2zwXi9y9w0_D08c0sWHpTqBs2PHzh0wJKjBM2w_nWFahzn0875P5ZZThDkC41MJz-SasSCAEme3X13hs80xzrnQru0i93zdyBAZGza6M_7w
User-Agent: Mozilla/5.0 (Linux; Android 4.1.1; Galaxy Nexus Build/JR003C) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.65 Mobile Safari/537.36
Accept: */*
X-Requested-With: com.insecureshop
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

X-Requested-With: com.insecureshop

X-Requested-With: com.insecureshop