Android Application Penetration Testing Report

1. Introduction

The purpose of this project is to perform penetration testing on a vulnerable Android application by simulating real-world attack scenarios. The testing is guided by OWASP Mobile Top 5 vulnerabilities (M1–M5). This helps identify weaknesses in Android apps and recommend remediation.

2. Lab Setup

Environment:

- Emulator: Genymotion license for root access (running Android OS)
- Kali Linux: Attacker machine
- Proxy Tool: Burp Suite (to intercept HTTP/HTTPS traffic)
- Analysis Tools: Jadx, APKTool (reverse engineering of apk), Frida

Setup Steps:

1. Installed Genymotion and configured an Android virtual device.
2. Installed Burp Suite CA certificate on emulator to intercept HTTPS.
3. Installed vulnerable app (InsecureBankv2/DVIA) using adb install.
4. Used Jadx and APKTool for reverse engineering APK.
5. Used Frida for runtime testing and bypassing checks.

3. Vulnerability Testing

M1: Improper Platform Usage

- Test: Checked AndroidManifest for exported components.
- Finding: Exported activities accessed without authentication.
- Remediation: Set exported=false and enforce permission checks.

M2: Insecure Data Storage

- Test: Examined app data directories and SharedPreferences.
- Finding: Credentials stored in plaintext.
- Remediation: Use EncryptedSharedPreferences, KeyStore.

M3: Insecure Communication

- Test: Intercepted traffic with Burp.
- Finding: App accepted self-signed certificate; credentials visible.
- Remediation: Implement TLS 1.2+, enable certificate pinning.

M4: Insecure Authentication

- Test: Performed brute-force login attempts using Burp Intruder.
- Finding: No account lockout, weak session management.
- Remediation: Add lockouts, MFA, secure session handling.

M5: Insufficient Cryptography

- Test: Decompiled APK and reviewed encryption functions.
- Finding: Hardcoded AES key and weak ECB mode.
- Remediation: Use AES-GCM, keys from KeyStore, avoid hardcoding.

4. Summary Table

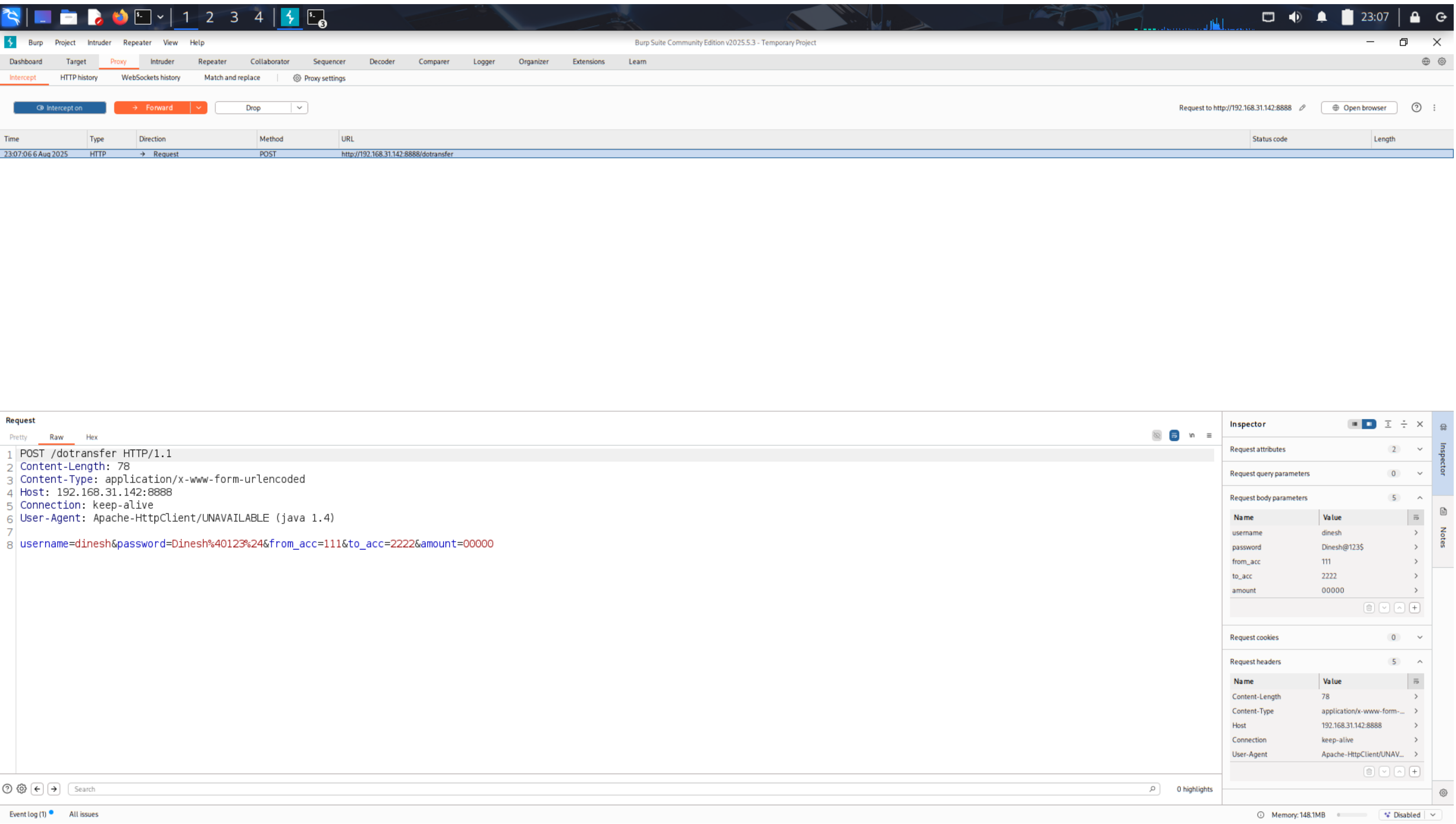
Vulnerability	Tool Used	Evidence	Status	Mitigation
M1	Jadx, adb	Exported activity triggered	Vulnerable	Restrict exports
M2	adb	Plaintext credentials found	Vulnerable	Encrypt storage
M3	Burp Suite	HTTPS intercepted	Vulnerable	TLS + pinning
M4	Burp	Brute-force possible	Vulnerable	Lockout, MFA
M5	Jadx, Frida	Hardcoded key found	Vulnerable	AES-GCM + KeyStore

5. Conclusion

Learnings: Learned static and dynamic Android app testing, how to intercept traffic, reverse engineer APKs, and exploit weaknesses. Limitations: Emulator lacks hardware-based protections like Trusted Execution Environment. Future Work: Expand tests to full OWASP Mobile Top 10, integrate automated scanning, and test production-grade apps.

6. References

- OWASP Mobile Top 10 documentation
- Frida, Jadx, APKTool official documentation
- InsecureBankv2 and DVIA vulnerable app projects



Burp Suite Community Edition v2025.5.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://192.168.31.142:8888
Open browser
Status code
Length
Request
Pretty Raw Hex
Search
0 highlights
Inspector
Event log (1) All issues
Memory: 148.1MB
Disabled
Notes

Time	Type	Direction	Method	URL
23:07:06 6 Aug 2025	HTTP	→ Request	POST	http://192.168.31.142:8888/dotransfer

```
POST /dotransfer HTTP/1.1
Content-Length: 78
Content-Type: application/x-www-form-urlencoded
Host: 192.168.31.142:8888
Connection: keep-alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

username=dinesh&password=Dinesh%40123%24&from_acc=111&to_acc=2222&amount=00000
```

Request attributes 2

Request query parameters 0

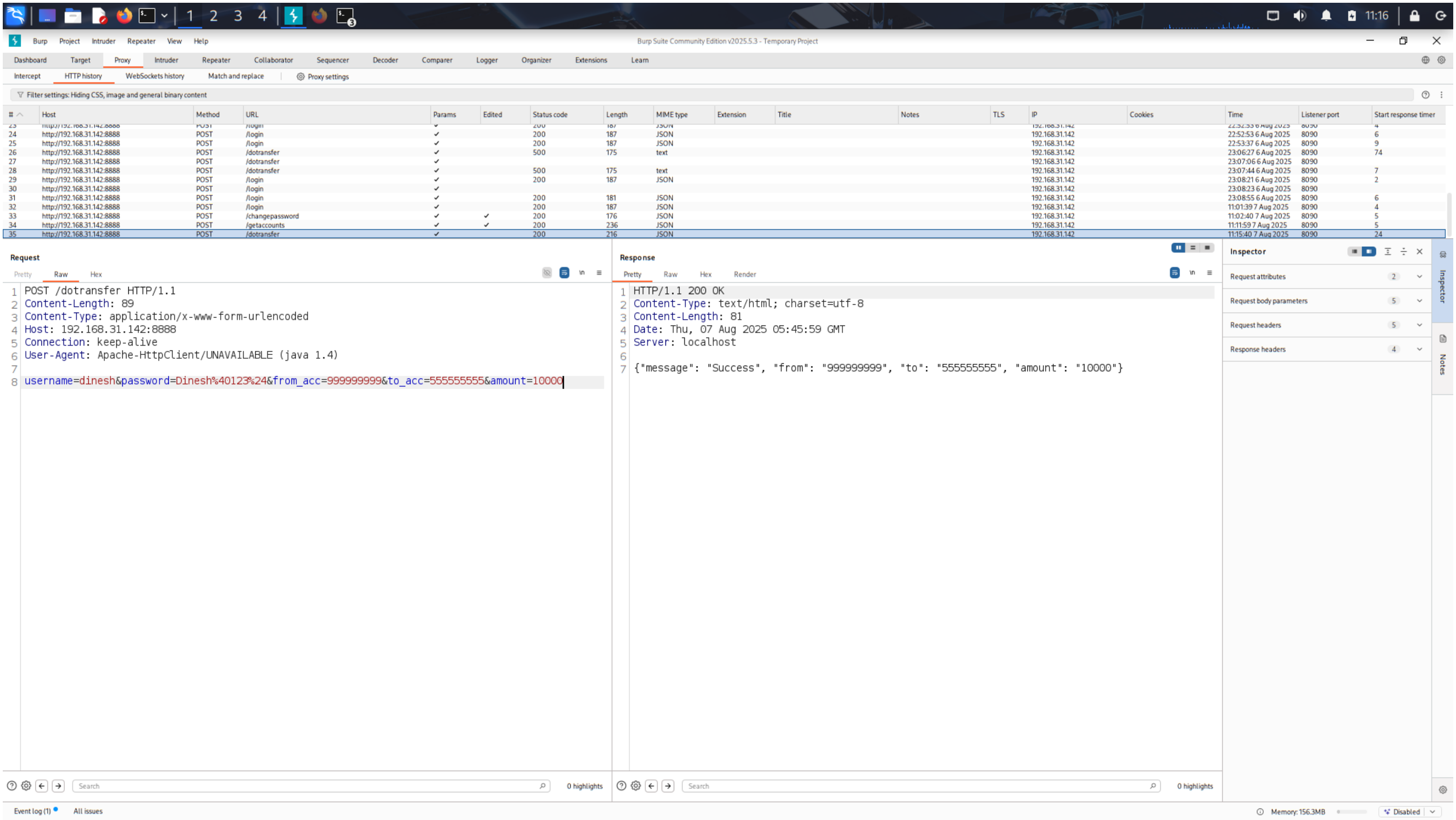
Request body parameters 5

Name	Value
username	dinesh
password	Dinesh@123$
from_acc	111
to_acc	2222
amount	00000

Request cookies 0

Request headers 5

Name	Value
Content-Length	78
Content-Type	application/x-www-form-...
Host	192.168.31.142:8888
Connection	keep-alive
User-Agent	Apache-HttpClient/UNAV...


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.5.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response timer
23	http://192.168.31.142:8888	POST	/login	✓		200	187	JSON					192.168.31.142		22:52:53 6 Aug 2025	8090	4
24	http://192.168.31.142:8888	POST	/login	✓		200	187	JSON					192.168.31.142		22:52:53 6 Aug 2025	8090	6
25	http://192.168.31.142:8888	POST	/login	✓		200	187	JSON					192.168.31.142		22:53:37 6 Aug 2025	8090	9
26	http://192.168.31.142:8888	POST	/dotransfer	✓		500	175	text					192.168.31.142		23:06:27 6 Aug 2025	8090	74
27	http://192.168.31.142:8888	POST	/dotransfer	✓									192.168.31.142		23:07:06 6 Aug 2025	8090	
28	http://192.168.31.142:8888	POST	/dotransfer	✓		500	175	text					192.168.31.142		23:07:44 6 Aug 2025	8090	7
29	http://192.168.31.142:8888	POST	/login	✓		200	187	JSON					192.168.31.142		23:08:21 6 Aug 2025	8090	2
30	http://192.168.31.142:8888	POST	/login	✓									192.168.31.142		23:08:23 6 Aug 2025	8090	
31	http://192.168.31.142:8888	POST	/login	✓		200	181	JSON					192.168.31.142		23:08:55 6 Aug 2025	8090	6
32	http://192.168.31.142:8888	POST	/login	✓		200	187	JSON					192.168.31.142		11:01:39 7 Aug 2025	8090	4
33	http://192.168.31.142:8888	POST	/changepassword	✓	✓	200	176	JSON					192.168.31.142		11:02:40 7 Aug 2025	8090	5
34	http://192.168.31.142:8888	POST	/getaccounts	✓	✓	200	236	JSON					192.168.31.142		11:11:59 7 Aug 2025	8090	5
35	http://192.168.31.142:8888	POST	/dotransfer	✓		200	216	JSON					192.168.31.142		11:15:40 7 Aug 2025	8090	24

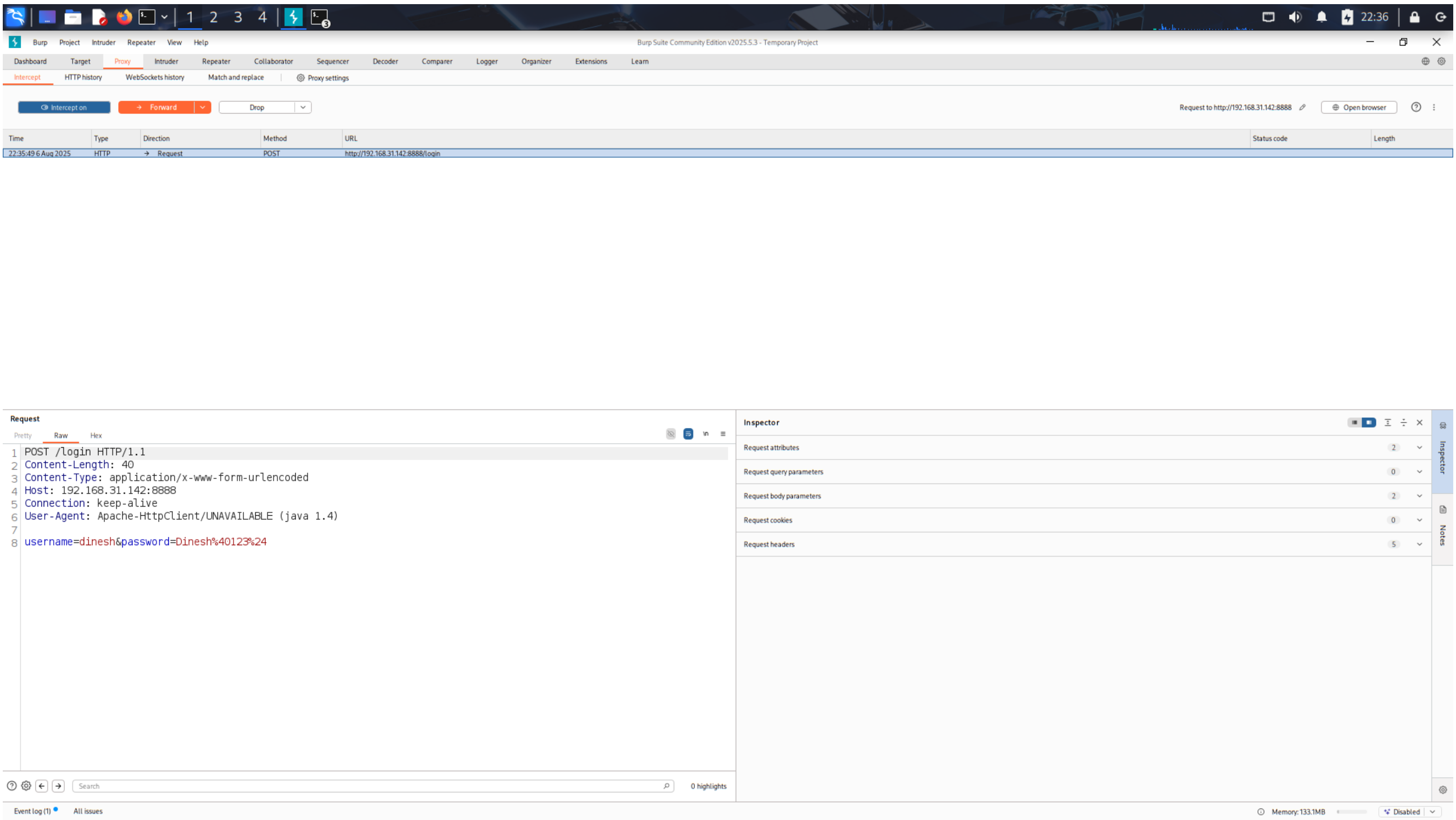
Request

```
POST /dotransfer HTTP/1.1
Content-Length: 89
Content-Type: application/x-www-form-urlencoded
Host: 192.168.31.142:8888
Connection: keep-alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

username=dinesh&password=Dinesh%40123%24&from_acc=999999999&to_acc=555555555&amount=10000
```

Response

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 81
Date: Thu, 07 Aug 2025 05:45:59 GMT
Server: localhost

{"message": "Success", "from": "999999999", "to": "555555555", "amount": "10000"}
```

Inspector
Request attributes 2
Request body parameters 5
Request headers 5
Response headers 4
Search
0 highlights
Search
0 highlights
Event log (1)
All issues
Memory: 156.3MB
Disabled

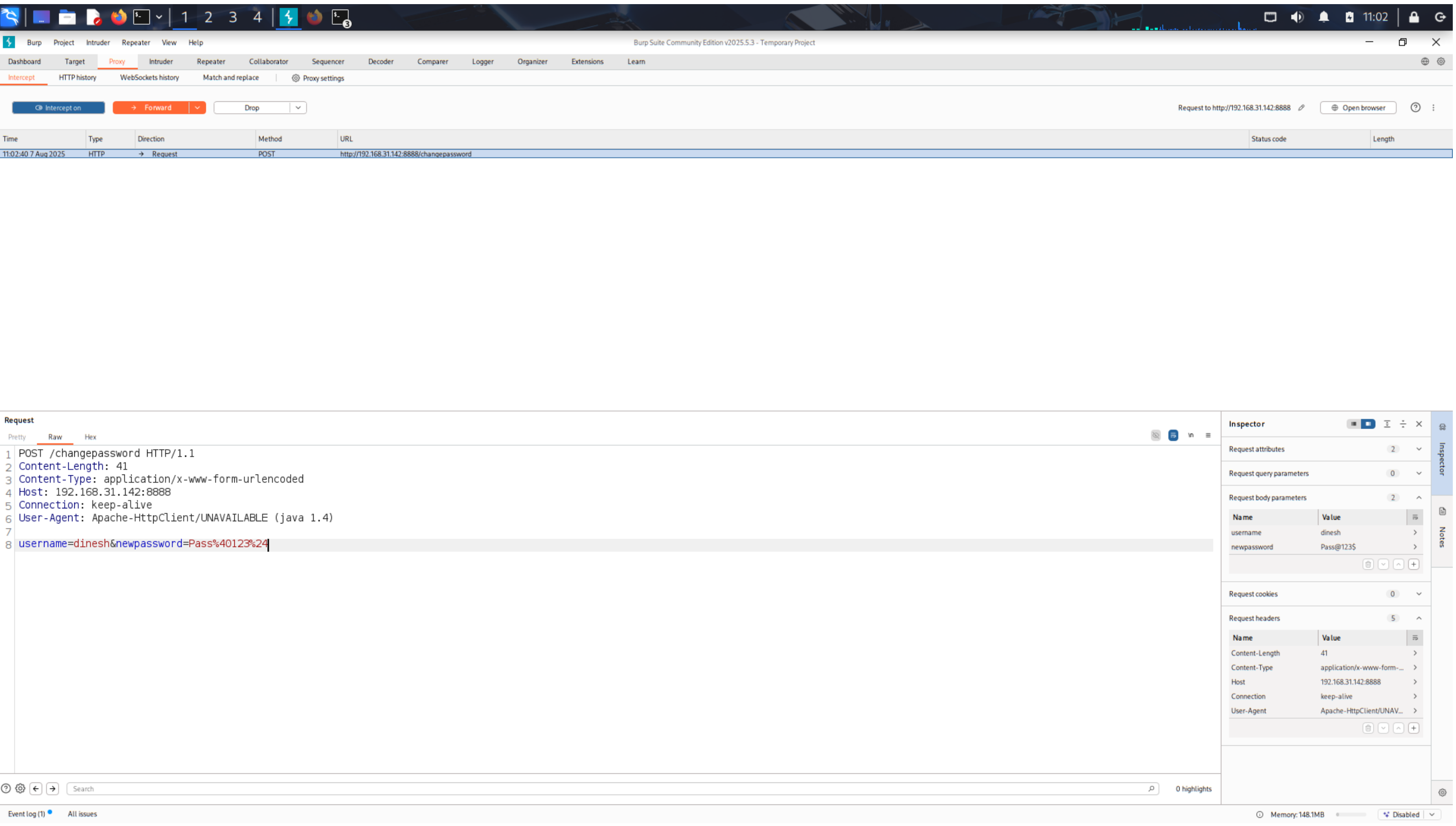

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.5.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://192.168.31.142:8888
Open browser

Time	Type	Direction	Method	URL	Status code	Length
22:35:49 6 Aug 2025	HTTP	→ Request	POST	http://192.168.31.142:8888/login		

Request

```
POST /login HTTP/1.1
Content-Length: 40
Content-Type: application/x-www-form-urlencoded
Host: 192.168.31.142:8888
Connection: keep-alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

username=dinesh&password=Dinesh%40123%24
```

Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 0
Request headers 5
Search
0 highlights
Event log (1)
All issues
Memory: 133.1MB
Disabled



Time	Type	Direction	Method	URL	Status code	Length
11:02:40 7 Aug 2025	HTTP	→ Request	POST	http://192.168.31.142:8888/changepassword		

```
POST /changepassword HTTP/1.1
Content-Length: 41
Content-Type: application/x-www-form-urlencoded
Host: 192.168.31.142:8888
Connection: keep-alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

username=dinesh&newpassword=Pass%40123%24
```

Request attributes 2

Request query parameters 0

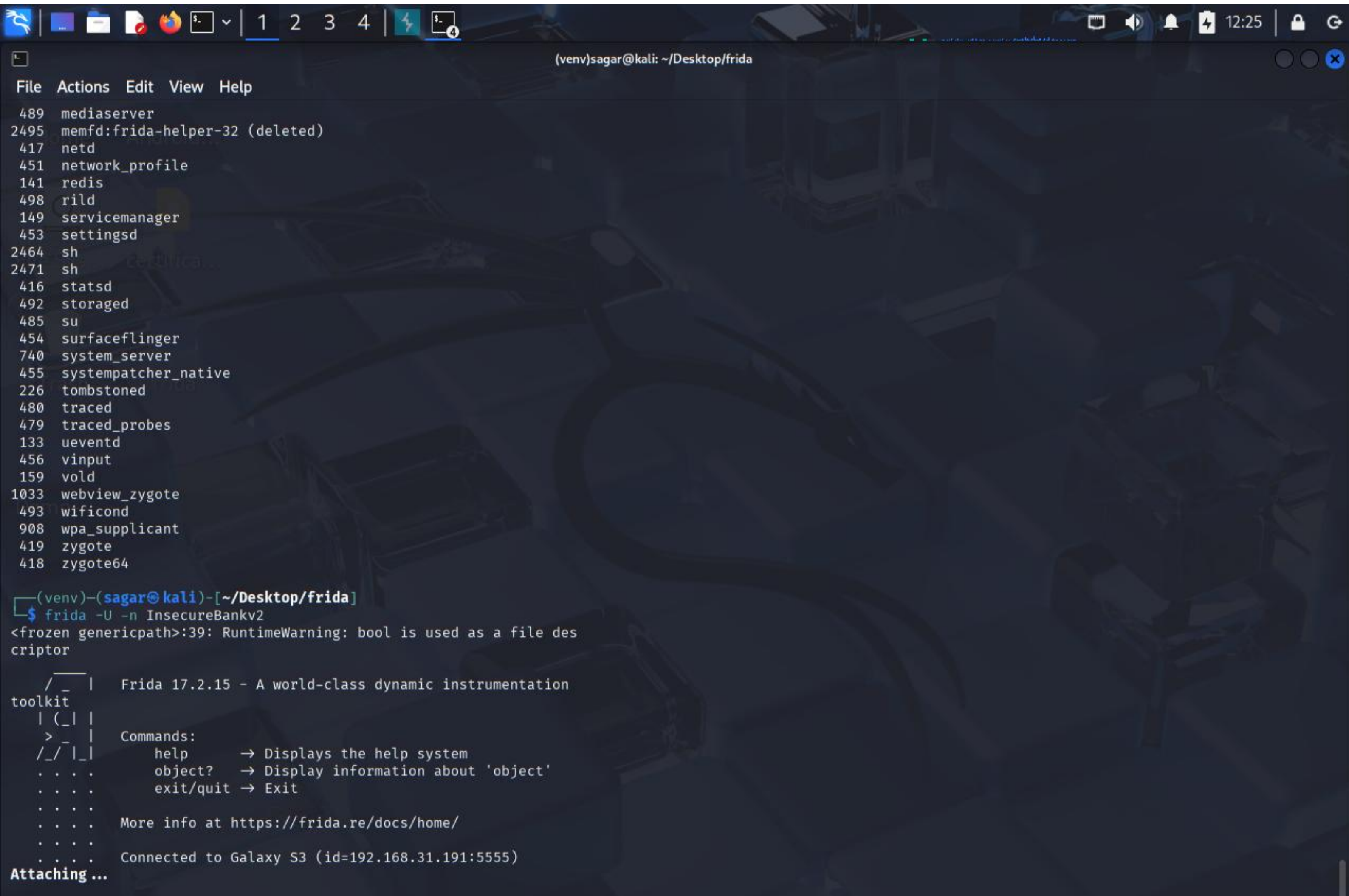
Request body parameters 2

Name	Value
username	dinesh
newpassword	Pass@123$

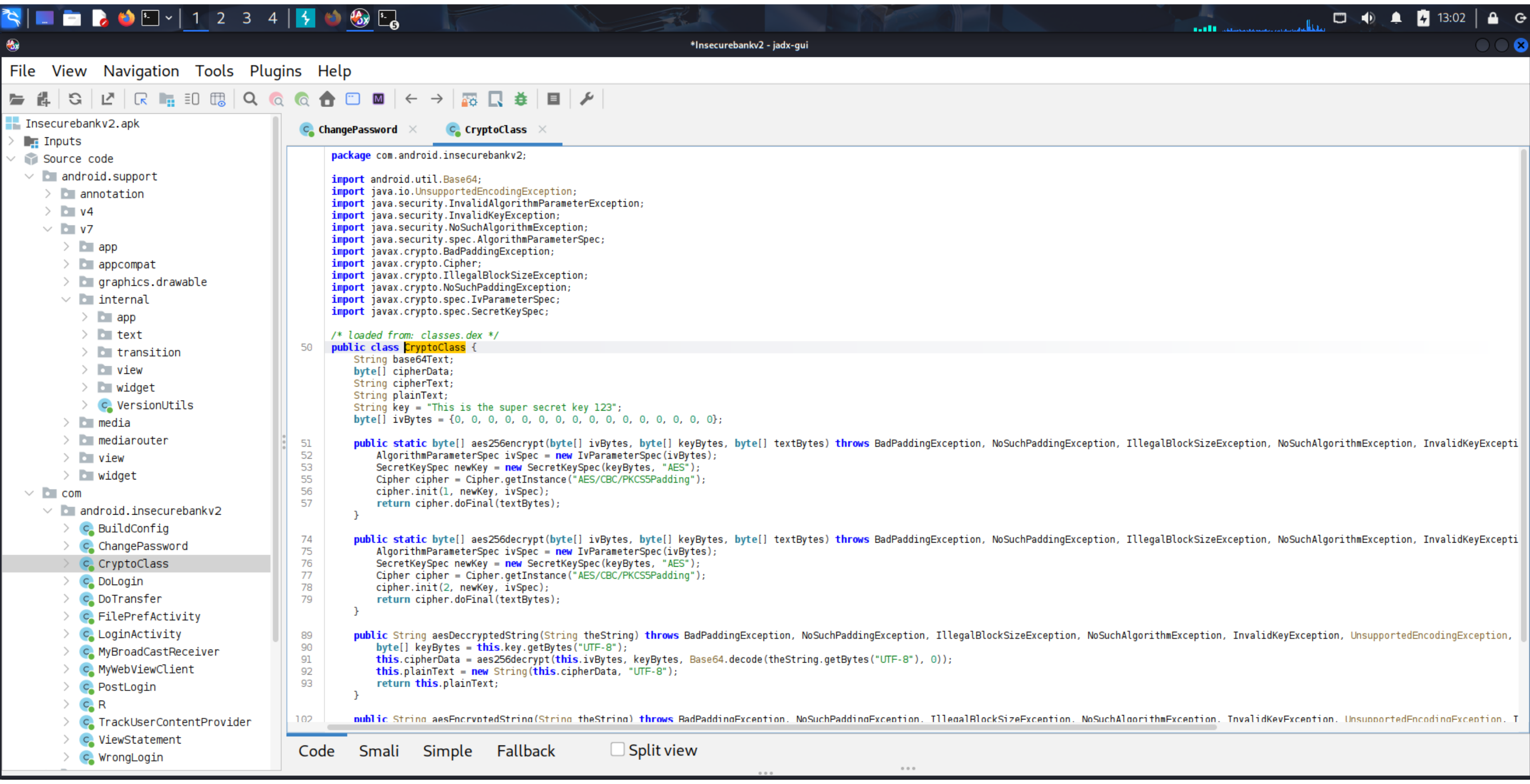
Request cookies 0

Request headers 5

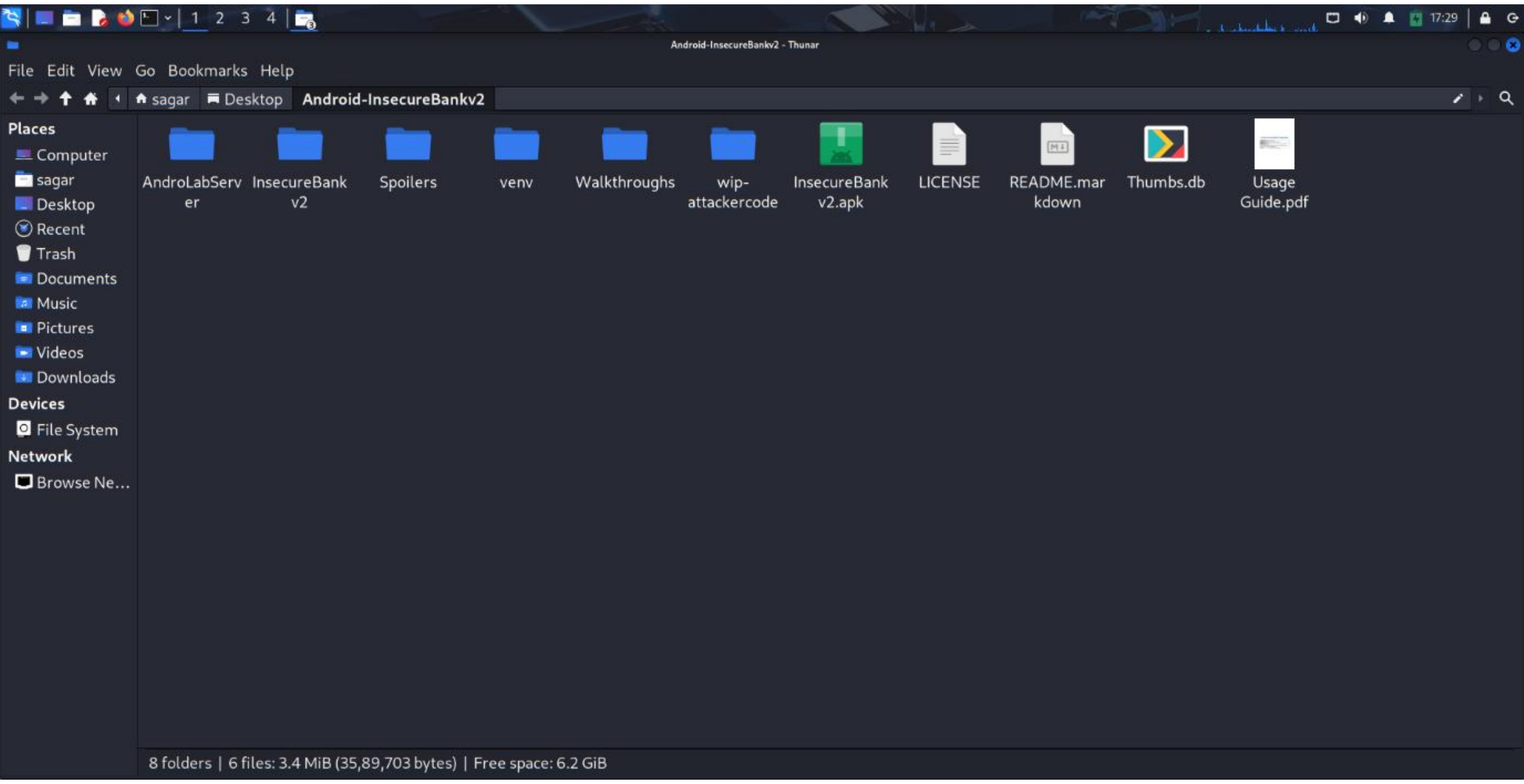
Name	Value
Content-Length	41
Content-Type	application/x-www-form-...
Host	192.168.31.142:8888
Connection	keep-alive
User-Agent	Apache-HttpClient/UNAV...



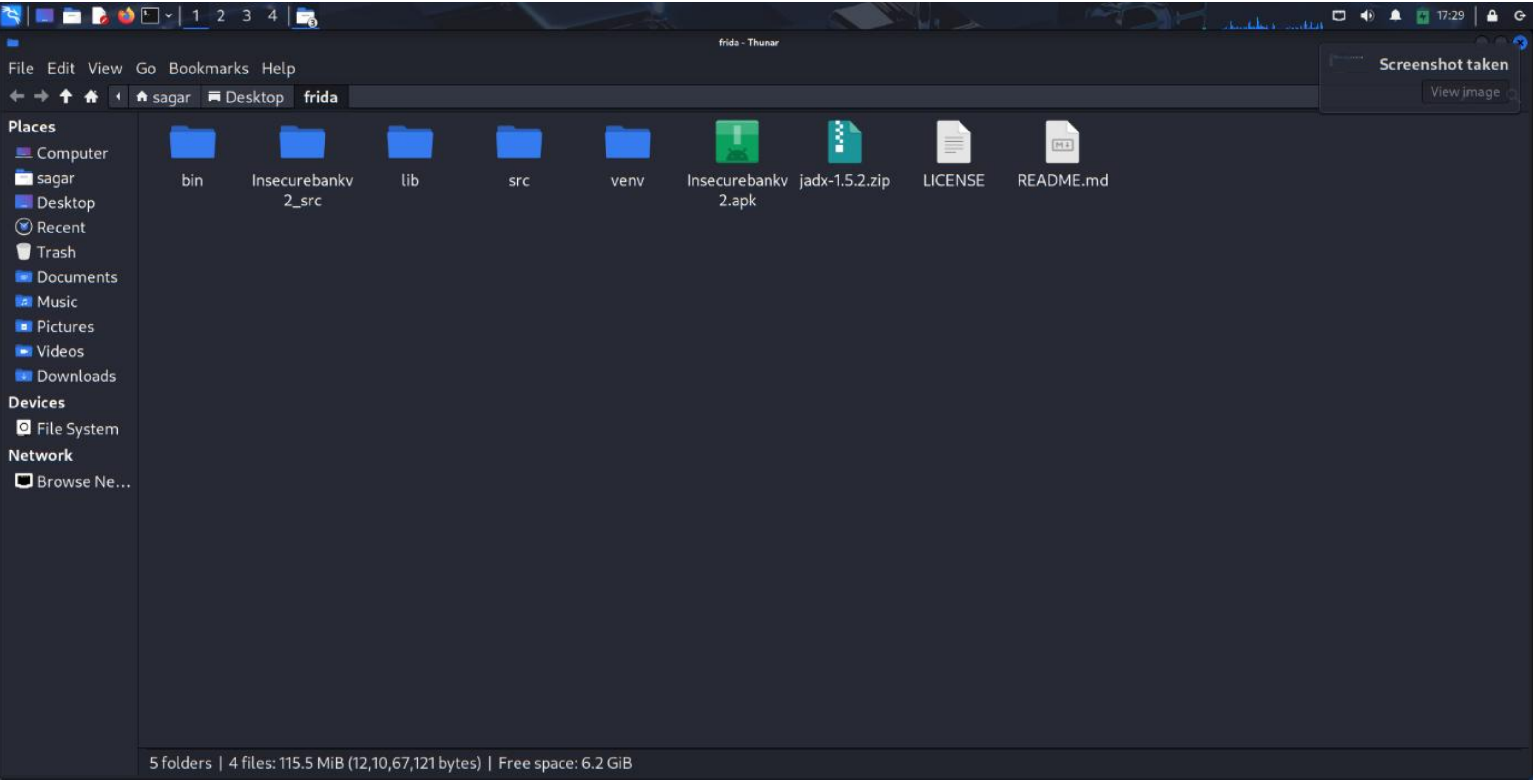
```
 489  mediaserver
2495  memfd:frida-helper-32 (deleted)
 417  netd
 451  network_profile
 141  redis
 498  rild
 149  servicemanager
 453  settingsd
2464  sh
2471  sh
 416  statsd
 492  storaged
 485  su
 454  surfaceflinger
 740  system_server
 455  systempatcher_native
 226  tombstoned
 480  traced
 479  traced_probes
 133  ueventd
 456  vinput
 159  vold
1033  webview_zygote
 493  wificond
 908  wpa_supplicant
 419  zygote
 418  zygote64

┌──(venv)─(sagar㉿kali)-[~/Desktop/frida]
└─$ frida -U -n InsecureBankv2
<frozen genericpath>:39: RuntimeWarning: bool is used as a file des
criptor
     ____
    / _  |   Frida 17.2.15 - A world-class dynamic instrumentation 
toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
   . . . .
   . . . .   Connected to Galaxy S3 (id=192.168.31.191:5555)
Attaching...
```



```java
package com.android.insecurebankv2;

import android.util.Base64;
import java.io.UnsupportedEncodingException;
import java.security.InvalidAlgorithmParameterException;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.security.spec.AlgorithmParameterSpec;
import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.SecretKeySpec;

/* loaded from: classes.dex */
public class CryptoClass {
    String base64Text;
    byte[] cipherData;
    String cipherText;
    String plainText;
    String key = "This is the super secret key 123";
    byte[] ivBytes = {0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0};

    public static byte[] aes256encrypt(byte[] ivBytes, byte[] keyBytes, byte[] textBytes) throws BadPaddingException, NoSuchPaddingException, IllegalBlockSizeException, NoSuchAlgorithmException, InvalidKeyExcepti
        AlgorithmParameterSpec ivSpec = new IvParameterSpec(ivBytes);
        SecretKeySpec newKey = new SecretKeySpec(keyBytes, "AES");
        Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
        cipher.init(1, newKey, ivSpec);
        return cipher.doFinal(textBytes);
    }

    public static byte[] aes256decrypt(byte[] ivBytes, byte[] keyBytes, byte[] textBytes) throws BadPaddingException, NoSuchPaddingException, IllegalBlockSizeException, NoSuchAlgorithmException, InvalidKeyExcepti
        AlgorithmParameterSpec ivSpec = new IvParameterSpec(ivBytes);
        SecretKeySpec newKey = new SecretKeySpec(keyBytes, "AES");
        Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
        cipher.init(2, newKey, ivSpec);
        return cipher.doFinal(textBytes);
    }

    public String aesDeccryptedString(String theString) throws BadPaddingException, NoSuchPaddingException, IllegalBlockSizeException, NoSuchAlgorithmException, InvalidKeyException, UnsupportedEncodingException,
        byte[] keyBytes = this.key.getBytes("UTF-8");
        this.cipherData = aes256decrypt(this.ivBytes, keyBytes, Base64.decode(theString.getBytes("UTF-8"), 0));
        this.plainText = new String(this.cipherData, "UTF-8");
        return this.plainText;
    }

    public String aesEncryptedString(String theString) throws BadPaddingException, NoSuchPaddingException, IllegalBlockSizeException, NoSuchAlgorithmException, InvalidKeyException, UnsupportedEncodingException, I
```



8 folders | 6 files: 3.4 MiB (35,89,703 bytes) | Free space: 6.2 GiB



bin

Insecurebankv2_src

lib

src

venv

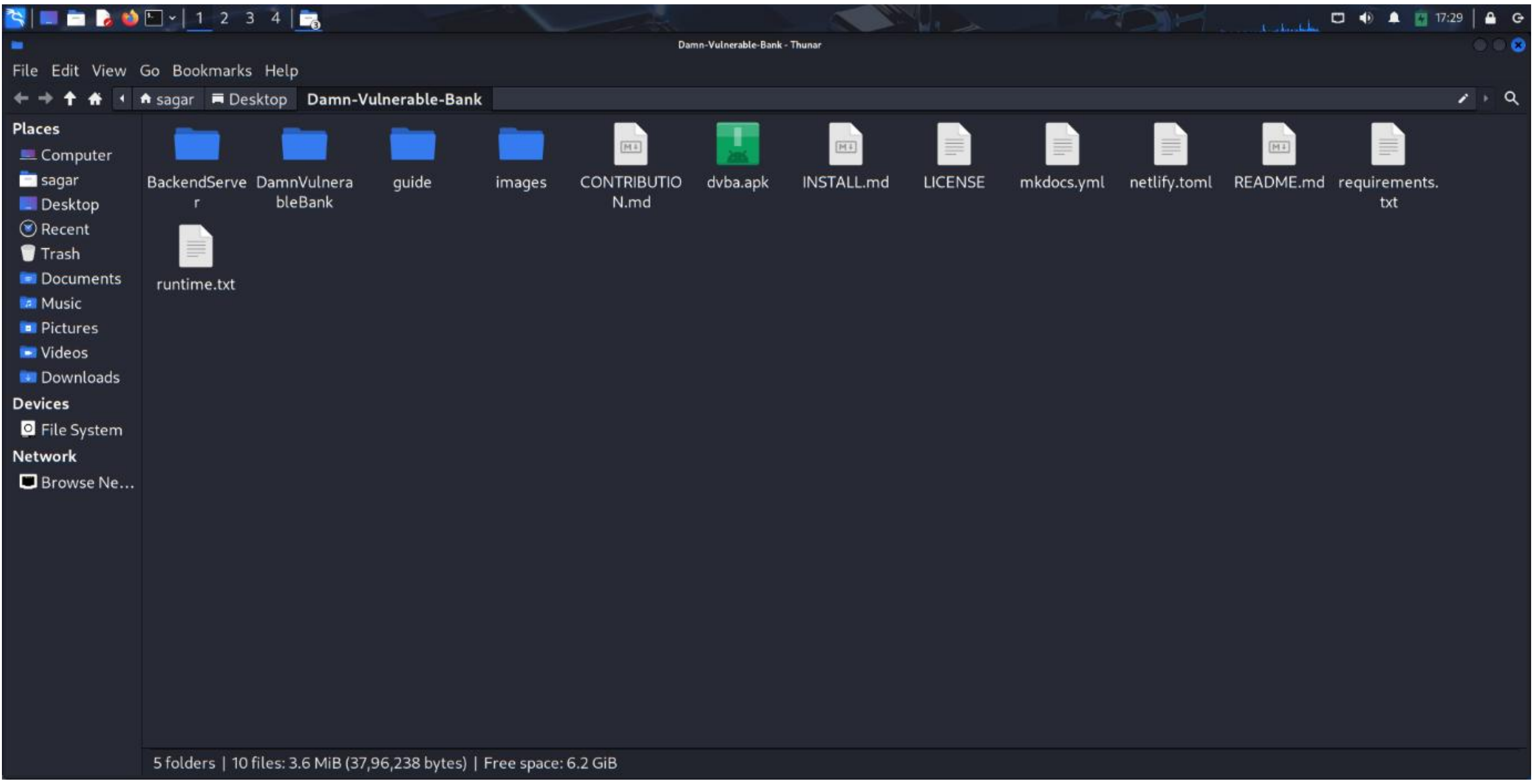
Insecurebankv2.apk

jadx-1.5.2.zip

LICENSE

README.md

5 folders | 4 files: 115.5 MiB (12,10,67,121 bytes) | Free space: 6.2 GiB



BackendServer

DamnVulnerableBank

guide

images

CONTRIBUTION.md

dvba.apk

INSTALL.md

LICENSE

mkdocs.yml

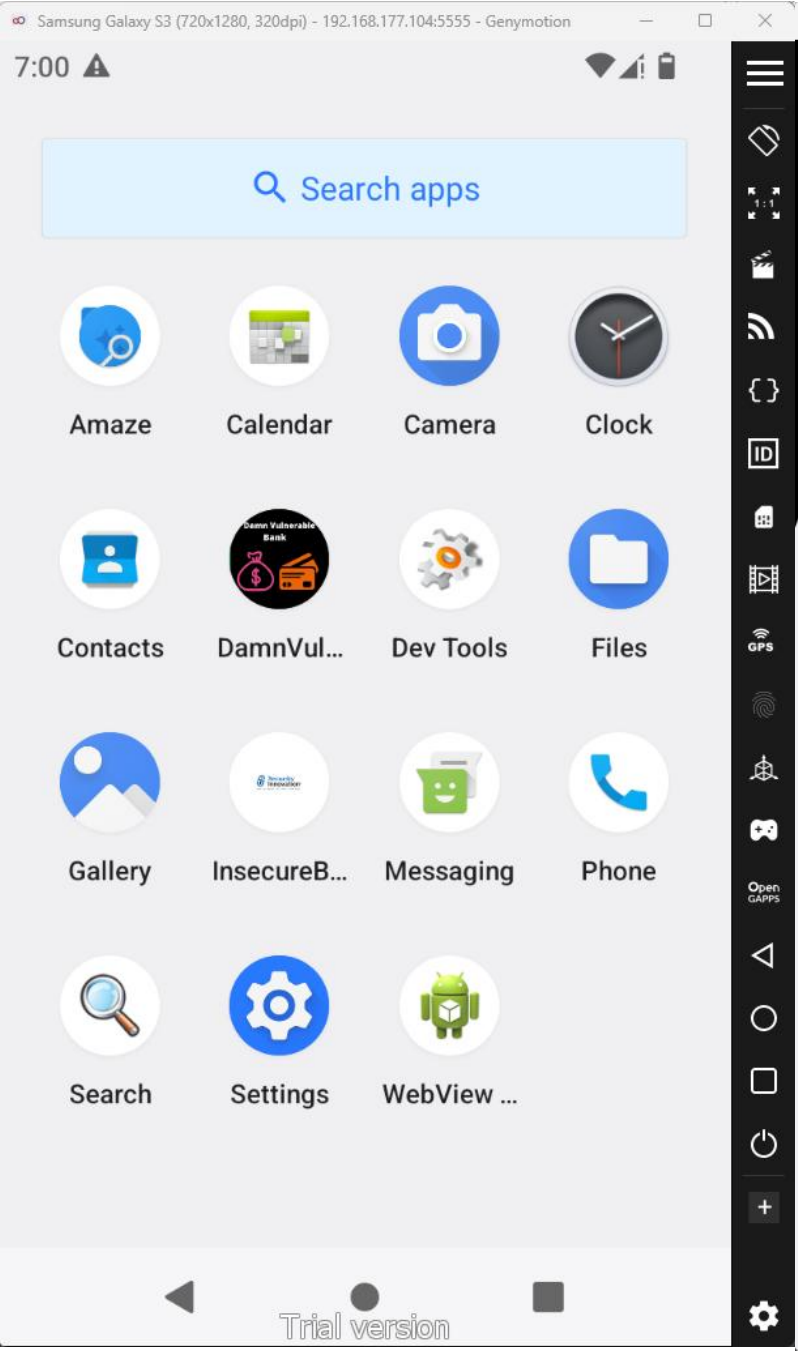
netlify.toml

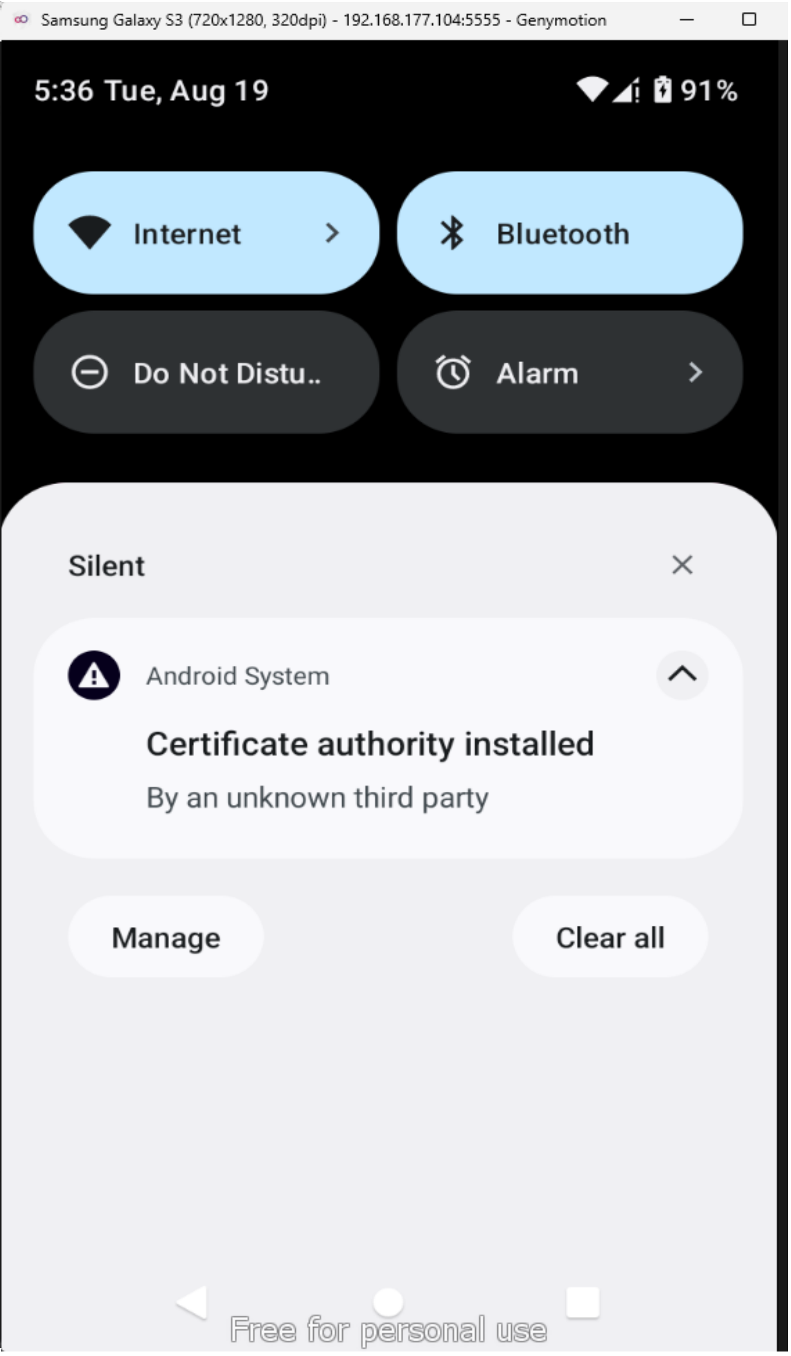
README.md

requirements.txt

runtime.txt

5 folders | 10 files: 3.6 MiB (37,96,238 bytes) | Free space: 6.2 GiB





Certificate authority installed

By an unknown third party