

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



BÁO CÁO BÀI TẬP 3: TÌM HIỂU CÔNG CỤ KIỂM THỬ

Môn: Kiểm thử xâm nhập

Giảng Viên : Đinh Trường Duy

Nhóm BTL: Nhóm 07

Sinh viên thực hiện:

Vũ Ngọc Phương

B20DCAT142

Ninh Chí Hường

B20DCAT094

Hoàng Trung Kiên

B20DCAT098

Nguyễn Văn Khang

B20DCAT102

Nguyễn Trần Minh

B20DCAT126

Lê Đình Quân

B20DCAT146

Hà Nội – 2024

Mục lục

I. Tìm hiểu công cụ Công cụ MobSF.....	3
1. Giới thiệu.	3
2. Chức năng chính của MobSF.....	3
3. Ưu nhược điểm của MobSF.....	4
II. Cài đặt sử dụng công cụ MobSF.	5
1. Cài đặt	5
2. Kết luận và đánh giá chung mức độ bảo mật của ứng dụng:.....	10
3. Biện pháp khắc phục.....	10

I. Tìm hiểu công cụ Công cụ MobSF.

1. Giới thiệu.

Mobile Security Framework (MobSF) là nền tảng nghiên cứu bảo mật dành cho các ứng dụng di động trên Android, iOS và Windows Mobile. MobSF có thể được sử dụng cho nhiều trường hợp sử dụng khác nhau như bảo mật ứng dụng di động, kiểm tra thâm nhập, phân tích phần mềm độc hại và phân tích quyền riêng tư. Trình phân tích tĩnh hỗ trợ các tệp nhị phân ứng dụng di động phổ biến như APK, IPA, APPX và mã nguồn. Trong khi đó, Trình phân tích động hỗ trợ cả ứng dụng Android và iOS, đồng thời cung cấp nền tảng để kiểm tra thiết bị tương tác, dữ liệu thời gian chạy và phân tích lưu lượng mạng. MobSF tích hợp liền mạch với quy trình DevSecOps hoặc CI/CD của bạn, được hỗ trợ bởi các API REST và công cụ CLI, giúp nâng cao quy trình làm việc bảo mật của bạn một cách dễ dàng.

2. Chức năng chính của MobSF.

- MobSF có thể thực hiện nhiều loại phân tích khác nhau và chức năng, bao gồm:
 - + **Phân tích tĩnh:** Phân tích mã nguồn ứng dụng để tìm kiếm các lỗ hổng bảo mật tiềm ẩn.
 - + **Phân tích động:** Thực thi ứng dụng trên thiết bị thực hoặc giả lập để giám sát hành vi của nó và xác định các mối đe dọa tiềm ẩn.
 - + **Phân tích phần mềm độc hại:** Xác định xem ứng dụng có chứa phần mềm độc hại hay không.
 - + **Kiểm tra API web:** Phân tích các API web được sử dụng bởi ứng dụng để tìm kiếm các lỗ hổng bảo mật.
 - + **Báo cáo chi tiết:** MobSF tạo ra các báo cáo chi tiết về kết quả phân tích, giúp bạn dễ dàng xác định và sửa chữa các lỗ hổng bảo mật.
 - + **Tích hợp với các công cụ khác:** MobSF có thể tích hợp với các công cụ khác, chẳng hạn như Burp Suite và ZAP, để cung cấp cho bạn một cái nhìn toàn diện hơn về bảo mật ứng dụng của mình.

3. Ưu nhược điểm của MobSF.

– Ưu điểm của MobSF:

- + **Miễn phí và mã nguồn mở:** MobSF là một công cụ miễn phí và mã nguồn mở, có nghĩa là bất kỳ ai cũng có thể sử dụng và sửa đổi nó. Điều này khiến nó trở thành một lựa chọn hấp dẫn cho các cá nhân và tổ chức có ngân sách hạn hẹp.
- + **Dễ sử dụng:** MobSF có giao diện web trực quan giúp người dùng dễ dàng sử dụng và hiểu kết quả phân tích.
- + **Hỗ trợ nhiều nền tảng:** MobSF hỗ trợ các hệ điều hành di động phổ biến như Android, iOS và Windows Phone.
- + **Tính năng phong phú:** MobSF cung cấp nhiều tính năng khác nhau, bao gồm phân tích tĩnh, phân tích động, phân tích phần mềm độc hại và kiểm tra API web.
- + **Có thể mở rộng:** MobSF có thể mở rộng với các plugin tùy chỉnh, cho phép người dùng thêm các chức năng mới vào công cụ.
- + **Cộng đồng lớn:** MobSF có một cộng đồng người dùng lớn và tích cực, những người có thể cung cấp hỗ trợ và hướng dẫn.
- + **Cập nhật thường xuyên:** MobSF được cập nhật thường xuyên với các tính năng và bản sửa lỗi mới.

– Nhược điểm của MobSF:

- + **Có thể phức tạp đối với người mới bắt đầu:** Mặc dù MobSF có giao diện web trực quan, nhưng nó vẫn có thể phức tạp đối với người mới bắt đầu sử dụng công cụ phân tích bảo mật di động.
- + **Yêu cầu kiến thức về bảo mật di động:** Để sử dụng MobSF hiệu quả, người dùng cần có kiến thức cơ bản về bảo mật di động.
- + **Có thể mất thời gian để phân tích ứng dụng lớn:** Phân tích các ứng dụng di động lớn có thể mất nhiều thời gian, đặc biệt là khi sử dụng phân tích động.
- + **Có thể tạo ra nhiều cảnh báo sai:** MobSF có thể tạo ra nhiều cảnh báo sai, khiến người dùng khó xác định các lỗ hổng thực sự.

- + **Yêu cầu cài đặt:** MobSF cần được cài đặt trên máy tính cục bộ, điều này có thể không phù hợp với tất cả người dùng.

II. Cài đặt sử dụng công cụ MobSF.

1. Cài đặt

- Tải về: <https://github.com/MobSF/Mobile-Security-Framework-MobSF>

```

L$ git clone https://github.com/MobSF/Mobile-Security-Framework-MobSF.git
Cloning into 'Mobile-Security-Framework-MobSF'...
remote: Enumerating objects: 21029, done.
remote: Counting objects: 100% (50/50), done.
remote: Compressing objects: 100% (40/40), done.
^Cfetch-pack: unexpected disconnect while reading sideband packet

```

- Cài đặt môi trường ảo cho công cụ

```

L$ pip3 install virtualenv
zsh: /home/z3r0day/.local/bin/pip3: bad interpreter: /usr/bin/python3.10: no such file or directory
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: virtualenv in /usr/lib/python3/dist-packages (20.17.1+ds)
Requirement already satisfied: distlib<1,>=0.3.6 in /usr/lib/python3/dist-packages (from virtualenv) (0.3.6)
Requirement already satisfied: filelock<4,>=3.4.1 in /usr/lib/python3/dist-packages (from virtualenv) (3.9.0)
Requirement already satisfied: platformdirs<3,>=2.4 in /usr/lib/python3/dist-packages (from virtualenv) (2.6.0)

L$ virtualenv -p python3 venv
created virtual environment CPython3.11.2.final.0-64 in 652ms
creator CPython3Posix(dest=/home/z3r0day/Desktop/MobSF/Mobile-Security-Framework-MobSF-master/venv, clear=False, no_vcs_ignore=False, global=False)
seeder FromAppData(download=False, pip=bundle, setuptools=bundle, wheel=bundle, via=copy, app_data_dir=/home/z3r0day/.local/share/virtualenv)
added seed packages: pip==23.0.1, setuptools==66.1.1, wheel==0.38.4
activators BashActivator,CShellActivator,FishActivator,NushellActivator,PowerShellActivator,PythonActivator

```

- Cài đặt các thành phần yêu cầu

```

L$ ./setup.sh
[INSTALL] Found Python 3.11.2
pip 23.0.1 from /home/z3r0day/Desktop/MobSF/Mobile-Security-Framework-MobSF-master/venv/lib/python3.11/site-packages/pip (python 3.11)
[INSTALL] Found pip
ERROR: Can not perform a '--user' install. User site-packages are not visible in this virtualenv.
[INSTALL] Installing Requirements
Requirement already satisfied: wheel in ./venv/lib/python3.11/site-packages (0.38.4)
Collecting poetry==1.6.1
  Downloading poetry-1.6.1-py3-none-any.whl (232 kB)
    232.8/232.8 kB 1.6 MB/s eta 0:00:00
Collecting build<0.11.0,>=0.10.0
  Downloading build-0.10.0-py3-none-any.whl (17 kB)
Collecting cachecontrol[filecache]<0.14.0,>=0.13.0
  Downloading cachecontrol-0.13.1-py3-none-any.whl (22 kB)
Collecting cleo<3.0.0,>=2.0.0
  Downloading cleo-2.1.0-py3-none-any.whl (78 kB)
    78.7/78.7 kB 6.1 MB/s eta 0:00:00
Collecting crashtest<0.5.0,>=0.4.1
  Downloading crashtest-0.4.1-py3-none-any.whl (7.6 kB)

```

```

[INFO] 10/May/2024 10:07:00 - Author: Ajin Abraham | opensecurity.in
[INFO] 10/May/2024 10:07:00 - Mobile Security Framework v3.9.8 Beta
REST API Key: 956a47a435aaa3751cb564282c976fef6b826a5d4fd1b415f62e92d818c69a49
[INFO] 10/May/2024 10:07:00 - OS Environment: Linux (kali 2023.2 kali-rolling) Linux-6.1.0-kali9-amd64-x86_64-with-glibc2.36
[INFO] 10/May/2024 10:07:00 - MobSF Basic Environment Check
[WARNING] 10/May/2024 10:07:00 - Dynamic Analysis related functions will not work.
Make sure a Genymotion Android VM/Android Studio Emulator is running before performing Dynamic Analysis.
[INFO] 10/May/2024 10:07:00 - Checking for Update.
Operations to perform:
  Apply all migrations: StaticAnalyzer, auth, contenttypes, sessions
Running migrations:
  No migrations to apply.
[INFO] 10/May/2024 10:07:01 - No updates available.
wkhtmltopdf 0.12.6
[INSTALL] Installation Complete

```

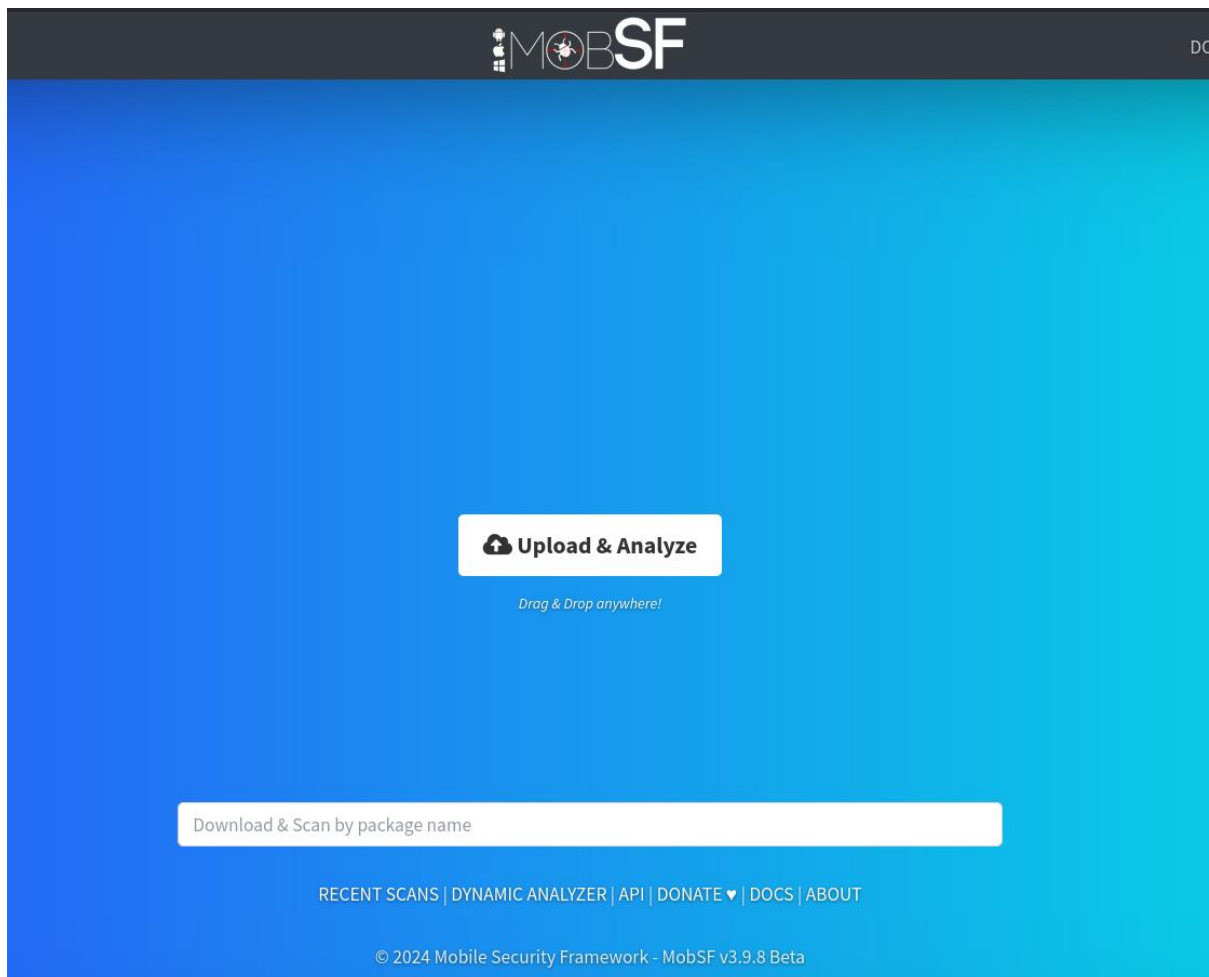
- Chạy công cụ

```

$ ./run.sh
[2024-05-10 17:07:52 +0700] [201890] [INFO] Starting gunicorn 21.2.0
[2024-05-10 17:07:52 +0700] [201890] [INFO] Listening at: http://[::]:8000 (201890)
[2024-05-10 17:07:52 +0700] [201890] [INFO] Using worker: gthread
[2024-05-10 17:07:52 +0700] [201901] [INFO] Booting worker with pid: 201901

```

- Truy cập localhost:8000

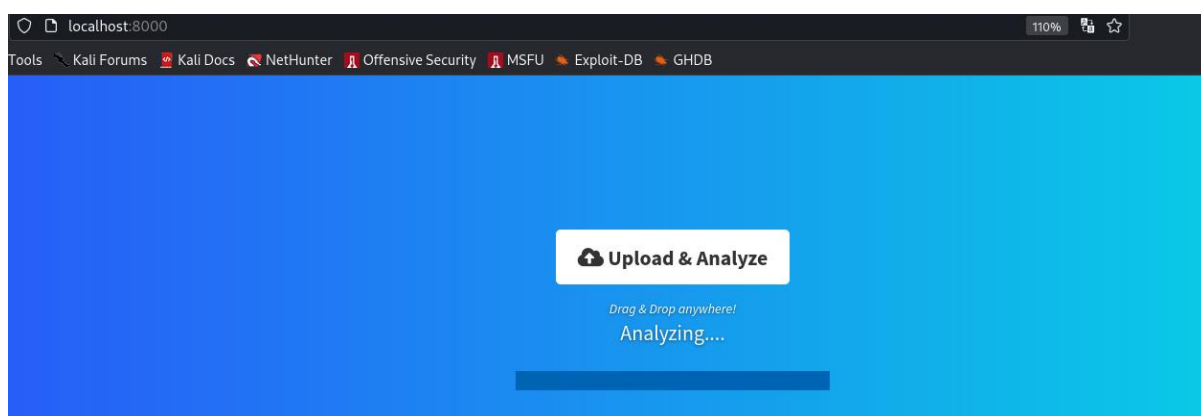


- Tiến hành phân tích:
 - File sử dụng để phân tích: <https://github.com/dineshshetty/Android-InsecureBankv2>

```
L$ git clone https://github.com/dineshshetty/Android-InsecureBankv2.git
Cloning into 'Android-InsecureBankv2'...
remote: Enumerating objects: 1791, done.
remote: Counting objects: 100% (189/189), done.
remote: Compressing objects: 100% (36/36), done.
remote: Total 1791 (delta 160), reused 153 (delta 153), pack-reused 1602
Receiving objects: 100% (1791/1791), 61.07 MiB | 2.04 MiB/s, done.
Resolving deltas: 100% (625/625), done.
```

AndroLabServer InsecureBankv2 InsecureBankv2.apk LICENSE README.markdown Spoilers Thumbs.db 'Usage Guide.pdf' Walkthroughs wip-attackercode

- Upload file apk lên công cụ phân tích mã nguồn:



- Kết quả phân tích:
 - Các lỗi phân quyền dựa trên cơ sở phân tích mã nguồn:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPING
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.	
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.	Show Files
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.	
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	Show Files
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.	
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.	
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.	Show Files
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.	Show Files
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external	Allows an application to write to external storage.	Show Files

- Các lỗ hổng bảo mật dựa trên phân tích MANIFEST

Q MANIFEST ANALYSIS

SUPPRESSED
0

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable patched Android version Android 4.0.3-4.0.4, [minSdk=15]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.	
2	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.	
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.	
4	Activity (com.android.insecurebankv2.PostLogin) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (22) of the app to 29 or higher to fix this issue at platform level.	
5	Activity (com.android.insecurebankv2.PostLogin) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
6	Activity (com.android.insecurebankv2.DoTransfer) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable	

- Phân tích các quyền nguy hiểm chung của toàn bộ app:

ABUSED PERMISSIONS

0/45

```
android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE,  
android.permission.SEND_SMS, android.permission.GET_ACCOUNTS,  
android.permission.READ_CONTACTS,  
android.permission.ACCESS_NETWORK_STATE,  
android.permission.ACCESS_COARSE_LOCATION
```

Other Common Permissions are permissions that are commonly abused by known malware.

- Liệt kê toàn bộ activity chính có trong ứng dụng:

ACTIVITIES

▼ Showing all **10** activities

com.android.insecurebankv2.LoginActivity
com.android.insecurebankv2.FilePrefActivity
com.android.insecurebankv2.DoLogin
com.android.insecurebankv2.PostLogin
com.android.insecurebankv2.WrongLogin
com.android.insecurebankv2.DoTransfer
com.android.insecurebankv2.ViewStatement
com.android.insecurebankv2.ChangePassword
com.google.android.gms.ads.AdActivity
com.google.android.gms.ads.purchase.InAppPurchaseActivity

- Hiển thị đoạn mã có khả năng khai thác cao trong một số các activity chính:

```
89.         protected void onPostExecute(Double result) {
90.         }
91.
92.         protected void onProgressUpdate(Integer... progress) {
93.         }
94.
95.         public void postData(String valueIWantToSend) throws ClientProtocolException, IOException, JSONException, InvalidKeyException, NoSuchAlgori
96.         {
97.             HttpResponse responseBody;
98.             DefaultHttpClient defaultHttpClient = new DefaultHttpClient();
99.             HttpPost httpPost = new HttpPost(DoLogin.this.protocol + DoLogin.this.serverip + ":" + DoLogin.this.serverport + "/login");
100.            HttpPost httpPost2 = new HttpPost(DoLogin.this.protocol + DoLogin.this.serverip + ":" + DoLogin.this.serverport + "/devlogin");
101.            List<NameValuePair> nameValuePairs = new ArrayList<>(2);
102.            nameValuePairs.add(new BasicNameValuePair("username", DoLogin.this.username));
103.            nameValuePairs.add(new BasicNameValuePair("password", DoLogin.this.password));
104.            if (DoLogin.this.username.equals("devadmin")) {
105.                httpPost2.setEntity(new UrlEncodedFormEntity(nameValuePairs));
106.                responseBody = defaultHttpClient.execute(httpPost2);
107.            } else {
108.                httpPost.setEntity(new UrlEncodedFormEntity(nameValuePairs));
109.                responseBody = defaultHttpClient.execute(httpPost);
110.            }
111.            InputStream in = responseBody.getEntity().getContent();
```

- Phân tích các giá trị khóa, biến được hardcoded có giá trị cao:


POSSIBLE HARDCODED SECRETS

▼ Showing all 25 secrets

```
"loginScreen_password" : "Password:"
"loginScreen_username" : "Username:"
MU3VGnFcvu612xTEKnGZJFOWurNoeRHlUpI0GCgSFQ=
qfDkyRZiTzGgubBzouWMEqfI8Qqw5CcMB2eo7wr2iH9X2v+qIFOYNd9v9ffS1x0
ir8bk+FXNtfVxQqTx81BUFTZKH1YNLABcK0MWI1xDng=
2RUillTqy9QCgJa1LFspH1z+fWwdgPABYGuJcpTf13CMmYA3W3Y+TBVqeDwkRNkY
w41pUAmd6TXdoU2/Z72GoKBjAyNw4B9JmpSTu2qFRaDsl7+5gLrSinCAebksSHto
EwZMQOzAsSbCW+73vnMc0IIA0IXmhdEPDWA4pBmTQFs=
eRIYZ7vwE2B0WWejblqyBziYzuBt9JW024X3YOHX2vY=
VECoKGI0d10uMKpilFkK46zikClkVy7m5Sv4INe3KRY=
Y6D/YxzOCnVSZVsavLV5KYCoa8QyT30GvMdLessm7RE=
KgIVFfxGq7C7ko+bqcJ8DTs8uzcctZAmISX4/fuAvTk=
3oIDJEetfykDk8YoOpv5sOi1YNQ0s4EIre7qVmQxm2HQzIUqU6cNsaZxD6S5UMW
4xZN7GqinxNwVj4iMqrRi7x6pRkbvrTHS+6N7nioqQ4QK45BALEp7Vftlp3TGnlt
PrVDFjRPs1s5jwZQRK3+ZFXo9PTI3zDMIRzL0PE43M8=
Z17IzPChrfQy4VaYpiQXook7JJBjQR06QL2GGTFiGqU=
cs4+HQqNuLJCSjPmayUCjMLdoEEgnhD+nTANe4ooENEnhW/TpxD13dq38SjFLmkW
gcr/blkg3lQG930U0ghKqsUNHy1ZHGL5GjwbOVxLHrc=
FaKwm3zfK+Dhq4JqMMBs2A+ODqwwgRuoVlqzQMyOaB4=
6NX7jQU62u42sQ6Bcog9+pwW2loP1J/qgDKEENUU4ZU=
SxPdgyHHu8QFxBqcnBJfZgRiWxxWH3ut4/9iPAvil=
Fych2TPIScblJxRIDoDvUow7d3sVUDiaLAvtmgpWr8g7e+3+ib/JMLjt3f841gO
3mNwt4SZ3Etv5TihUa/RqouLnZPiat8RAS1ApJt5MxhvfiYxahkXg2hSNsePN+7M
M/9MnPtadNpsJGLBqvtFaALd0ql4JyMOqfSncPhl=
AK+A2I0KMMcK37UYcOExFBr2JDYu9VluAHdYuT1VPLHst51ZSG89jehZq7ujXyH
```

2. Kết luận và đánh giá chung mức độ bảo mật của ứng dụng:

APP SCORES

 **Security Score** 28/100

Trackers Detection 3/432

 **MobSF Scorecard**

FILE INFORMATION

File Name InsecureBankv2.apk

Size 3.3MB

MD5 5ee4829065640f9c936ac861d1650ffc

SHA1 80b53f80a3c9e6bfd98311f5b26ccddcd1bf0a98

SHA256 b18af2a0e44d7634bbcdf93664d9c78a2695e050393fcfb5e8b91f902d194a4

APP INFORMATION

App Name InsecureBankv2

Package Name com.android.insecurebankv2

Main Activity com.android.insecurebankv2.LoginActivity

Target SDK 22 **Min SDK** 15 **Max SDK**

Android Version Name 1.0 **Android Version Code** 1

3. Biện pháp khắc phục.

- Loại bỏ hoặc thay thế các đoạn hardcoded
- Hạn chế quyền truy cập thiết bị của ứng dụng
- Mã hóa các chuỗi tĩnh trong mã nguồn
- Sử dụng các giải pháp bên thứ 3 để hạn chế việc dịch ngược ứng dụng