LeaveHomeSafe:
The Good, the Bad, the Ugly!

DeepSec

Vienna, Austria

deepsec.net

2023-11-17

@11:50 am CET

> Abraham Aranguren

> admin@7asecurity.com

> @7asecurity

> @7a_

+ 7asecurity.com

Agenda

LeaveHomeSafe: The Good, the Bad, the Ugly!

- → Who am I
- → Introduction
- → Assignment Limitations
- → Good impressions
- → Bad impressions
- → Ugly Impressions
- → Conclusion
- → Q & A

About Abraham Aranguren

→ CEO at **7ASecurity**, pentests & security training
public reports, presentations, etc.: https://7asecurity.com/publications

→ **Co-Author** of **Mobile**, **Web** and **Desktop (Electron)** app 7ASecurity courses: https://7asecurity.com/training

→ **Security Trainer** at Blackhat USA, HITB, OWASP Global AppSec, LASCON, 44Con, HackFest, Nullcon, SEC-T, etc.

→ Former Team Lead & Penetration Tester at **Cure53** and **Version 1**

→ Author of Practical Web Defense: www.elearnsecurity.com/PWD

→ Founder and leader of **OWASP OWTF**, and **OWASP flagship project**: owtf.org

→ Some presentations: www.slideshare.net/abrahamaranguren/presentations

→ Some **sec certs**: CISSP, OSCP, GWEB, OSWP, CPTS, CEH, MCSE: Security, MCSA: Security, Security+

→ Some **dev certs**: ZCE PHP 5, ZCE PHP 4, Oracle PL/SQL Developer Certified Associate, MySQL 5 CMDev, MCTS SQL Server 2005

SECURITY

Public Mobile Pentest Reports 2022-2023

Free & Fast way to learn about security = Read public pentest reports! :)
Download from: https://7asecurity.com/publications

2023 Public Pentest Reports:

→ Pentest-Report **K-9 Mail**, Fuzzing, Threat Model & Supply Chain Audit (OSTIF) 04.2023
→ Pentest-Report **ArgoVPN** Mobile, Servers & Privacy (OTF) 03.2023
→ Pentest-Report **Bridgefy** Web & Mobile apps, Cloud & Privacy Audit (OTF) 02.2023

2022 Public Pentest Reports:

→ Pentest-Report **minivpn Go client & Desktop Apps** (OTF) 08.2022
→ Pentest-Report **Amnezia VPN Mobile & Desktop Apps** (OTF) 07.2022
→ Pentest-Report **Linux Foundation LFX Platform** (OSTIF) 06.2022 (possibly in 2023)
→ **Pentest-Report LeaveHomeSafe Mobile Apps (OTF) 04.2022**
  - **COVID19 contact-tracing app enforced in Hong-Kong**
→ Pentest-Report **WEPN Web, API, Mobile & Device** (OTF) 03.2022

Older Public Mobile Pentest Reports - I

Smart Sheriff mobile app mandated by the South Korean government:

Public Pentest Reports:

→ Smart Sheriff: Round #1 - https://7asecurity.com/reports/pentest-report_smartsheriff.pdf

→ Smart Sheriff: Round #2 - https://7asecurity.com/reports/pentest-report_smartsheriff-2.pdf

Presentation:“Smart Sheriff, Dumb Idea, the wild west of government assisted parenting”

Slides:https://www.slideshare.net/abrahamaranguren/smart-sheriff-dumb-idea-the....

Video: https://www.youtube.com/watch?v=AbGX67CuVBQ

Chinese Police Apps Pentest Reports:

→ "BXAQ" (OTF) 03.2019 - https://7asecurity.com/reports/analysis-report_bxaq.pdf

→ "IJOP" (HRW) 12.2018 - https://7asecurity.com/reports/analysis-report_ijop.pdf

→ "Study the Great Nation" 09.2019 - https://7asecurity.com/reports/analysis-report_sgn.pdf

Presentation: “Chinese Police and CloudPets”

Slides: https://www.slideshare.net/abrahamaranguren/chinese-police-and-cloud-pets

Video: https://www.youtube.com/watch?v=kuJJ1Jjwn50

Older Public Mobile Pentest Reports - II

Other pentest reports:

- → imToken Wallet - https://7asecurity.com/reports/pentest-report_imtoken.pdf
- → Whistler Apps - https://7asecurity.com/reports/pentest-report_whistler.pdf
- → Psiphon - https://7asecurity.com/reports/pentest-report_psiphon.pdf
- → Briar - https://7asecurity.com/reports/pentest-report_briar.pdf
- → Padlock - https://7asecurity.com/reports/pentest-report_padlock.pdf
- → Peerio - https://7asecurity.com/reports/pentest-report_peerio.pdf
- → OpenKeyChain - https://7asecurity.com/reports/pentest-report_openkeychain.pdf
- → F-Droid / Baazar - https://7asecurity.com/reports/pentest-report_fdroid.pdf
- → Onion Browser - https://7asecurity.com/reports/pentest-report_onion-browser.pdf

More here:

https://7asecurity.com/publications

Introduction

Introduction

In the wake of the global upheaval caused by the **COVID-19 pandemic**

An array of **contact tracing apps** emerged

Including the **Hong Kong government's LeaveHomeSafe app**.

An obvious question emerged:

Is the Chinese government using this to spy on people?

Introduction

Mandatory Use of LeaveHomeSafe App Draws Grumbles | HKIBC News

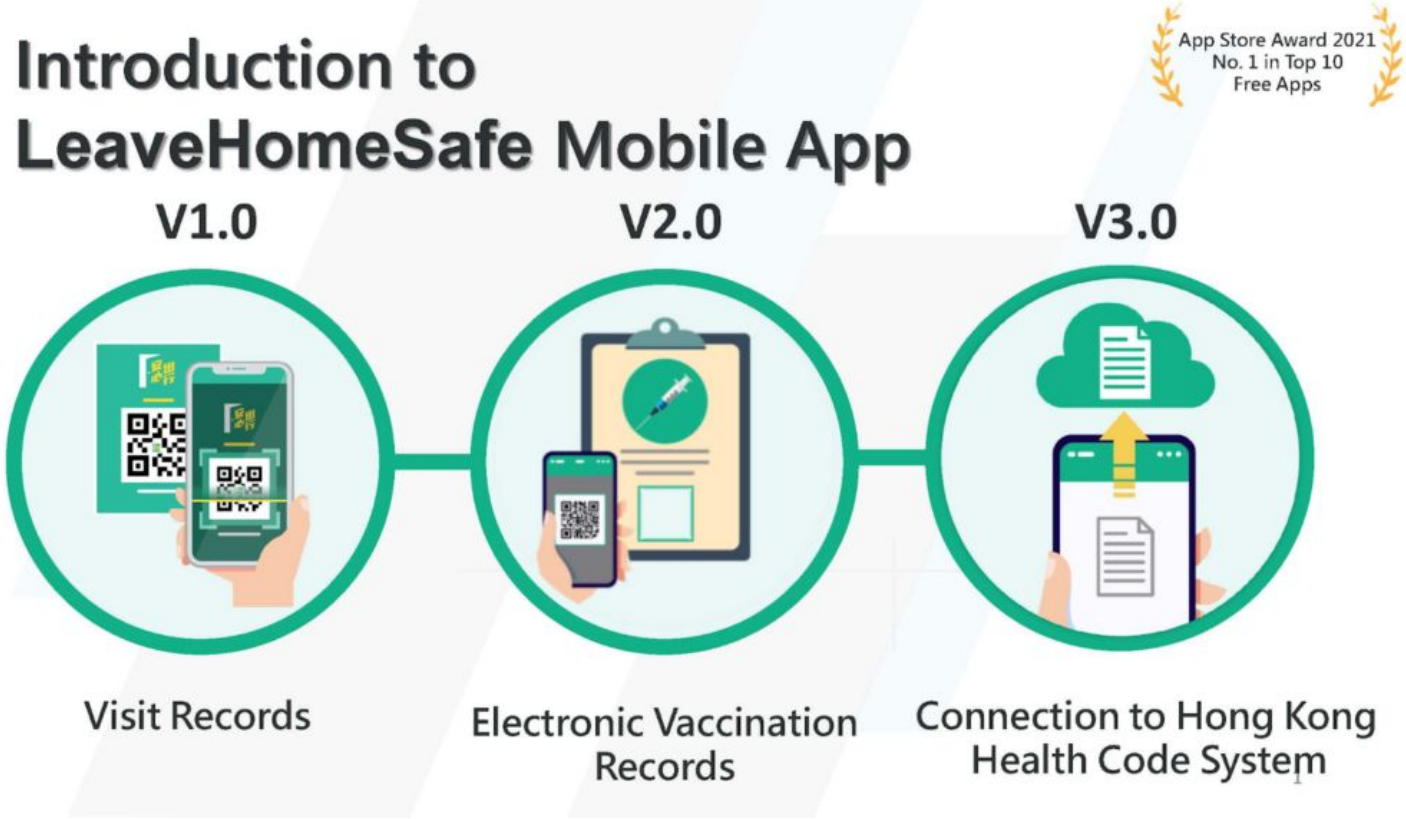
Nov 25, 2021 #Covid #LeaveHomeSafe

“The mandatory use of the #LeaveHomeSafe app to enter eateries and entertainment venues has not been fully welcomed.

Some residents said they will stop going to the cinema because of privacy concerns.”

https://www.youtube.com/watch?v=ossfGYINARk

Introduction



Project Background

- November 2020:
  - Hong Kong Government introduces the LeaveHomeSafe Android and iOS apps

- Initially:
  - Adoption was limited
  - < 0.5M downloads in the first two weeks.

- Why?
  - **privacy concerns** among Hong Kong citizens
  - Some **obtained secondary mobile devices** to keep **sensitive content separate**.

Project Background

- Reponse to initial LeaveHomeSafe concerns about **Excessive permissions**:
  - Reduction from **15** to **7**
  - **Privacy statement** asserting compliance with the **Personal Data Ordinance**.

  https://www.pcpd.org.hk/english/news_events/media_statements/press_20210219.html

- February 2021:
  - HK government tied relaxed operating hours for restaurants
  - reopening of various establishments to app usage
  - and customer information registration.

Project Background

- This policy evolved due to **Chinese government encouragement**
- Aiming to **reduce second phone** use
- Establish **real-name registration**.
  https://www.rfa.org/english/news/china/tracking-11012021133415.html/ampRFA

- November 2021:
  - **government mandated app use for entry into various public venues**
  - required vaccination of restaurant employees.

  https://www.humanresourcesonline.net/leavehomesafe-mobile-app-mandatory-at-all-restaurants-starting-december-9

Project Background

- **Violations** faced **fines of 5,000 HKD**,
- non-compliant restaurants were downgraded in operating privileges.

https://hongkongfp.com/2022/02/28/hong-kong-contact-tracing-app-leavehomesafe-stops-alerting-users-about-restaurants-visited-by-covid-patients/

- These actions led to a **substantial increase in app downloads**
- Reaching over **8 million by late June**
- Raising **suspicions of artificial inflation**.

https://www.thestandard.com.hk/breaking-news/section/4/191586/'Magical-number'-as-over-8-million-downloads-for-LeaveHomeSafe:-Alfred-Sit

Project Background

- The **government** attempts to **address privacy concerns:**
  - public statements
  - emphasizing data encryption and third-party assessments.

https://www.info.gov.hk/gia/general/202205/03/P2022050300874.htm

- **May 2022:**
  - **FactWire revealed facial recognition capabilities** in the app
  - sparking additional privacy and social control concerns.

https://www.factwire.org/en/leavehomesafe-app-has-built-in-facial-detection-module-government-admits/

What were the concerns?

What were the concerns?

- **Personal Data Security**:
  - Contact tracing apps accessing user data raise misuse and **unauthorized access concerns**.
  - Data security is vital; improper protection could risk data exposure to criminals.

- **Government Surveillance**:
  - Use of contact tracing apps for surveillance raises **civil liberty concerns**.

- **Data Retention**:
  - Storage duration varies, impacting **potential misuse** as it extends.

What were the concerns?

- **Consent and Transparency**:
  - Users must be informed and provide consent before data processing.

- **Third-Party Access**:
  - Some apps share data with third parties, raising questions about data **access and usage**.

Balancing contact tracing **effectiveness** and **user privacy** is **challenging**;
some argue certain apps lean too far in one direction.

Addressing the concerns

Addressing the concerns

- Project solicited by the **Hong Kong Democracy Council (HKDC)**
- Funded by the **Open Technology Fund (OTF)**
- Executed by **7ASecurity** in April and May 2022
- Public report: https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

- The project attempted to address concerns about:
  - **Potential Security and privacy risks** from the LeaveHomeSafe apps.

Note: In **Hong Kong**, this **COVID-19 digital contact tracing app** was required in

- Government venues
- Hospitals
- Markets
- Shopping malls, supermarkets
- Places of worship
- and more.

The Audit Methodology

- **Blackbox methodology** was employed:
  - No access to user data
  - No documentation
  - No source code

- **Test limitations:**
  - No Hong Kong Health Code System credentials
  - No valid vaccination status QR codes
  - No valid COVID testing status QR codes.

The Audit Methodology

- A team of 4 senior testers handled project preparation, execution, and finalization.
- Testing efforts concentrated on:
  - Decompilation
  - Reverse engineering
  - Runtime analysis

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

Audit Prologue

- **The Good**:
  - While the results were subpar, there are a few **positive highlights** worth acknowledging.

- **The Bad**:
  - ***Identified Vulnerabilities - 8***
  - ***Hardening Recommendations - 4***
  - ***Total - 12***

- **The Ugly**:
  - The **disclosure** process revealed:
    i. Poor journalism: Failed to treat a pentest report as evidence.
    ii. Lack of maturity by the Hong Kong government:
      - Attempting to save face by dismissing the report as **inaccurate**.

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

The Good

The Good

- Android and iOS apps:
  - Securely **protect** sensitive data – **no exposure in logs or encrypted files**
  - Do not leak Hong Kong Health Code System **credentials** in **HTTP caching artifacts**

- Android app:
  - Explicitly **disables backups**
  - Explicitly **disables clear-text HTTP traffic**

- iOS app:
  - Employs No insecure **custom URL schemes = No URL hijacking** in iOS
  - Implements **No ATS exceptions** = no clear-text HTTP leaks in iOS

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

The Good

- **Hardcoded Google API keys** in the Android and iOS apps**:**
  - Properly restricted to deter misuse.

- Android and iOS apps:
  - **Effectively secure application secrets** using the platform-specific hardware-backed security features: The **Android KeyStore** & **iOS KeyChain**.
  - All user information and **visit records** are **encrypted** when stored.

- The **Firebase device registration: ← really cool approach!**
  - Effectively **balances** COVID-19 **contact tracing** vs. **user privacy**
  - Enabling notifications for users.
  - **Without** any PII tracking (!)

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

The Bad

LHS-01-003 WP1:
Leaks
via
Missing Security Screen
on
Android & iOS
(Low)

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

LHS-01-003 WP1: Leaks via Missing Security Screen on Android & iOS (Low)

- Android and iOS apps:
  - **Fail** to **render a security screen** when they are **backgrounded**.

- **Attackers** with **physical access** to an unlocked device:
  - Can see **data displayed** by the apps before they **disappeared** into the **background**.

- **Malicious apps** & **physical attackers** could gain access to:
  - Sensitive user data
  - Visit records
  - Hong Kong Health Code System credentials
  - Other Personally Identifiable Information (PII)

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

LHS-01-003 WP1: Leaks via Missing Security Screen on Android & iOS (Low)

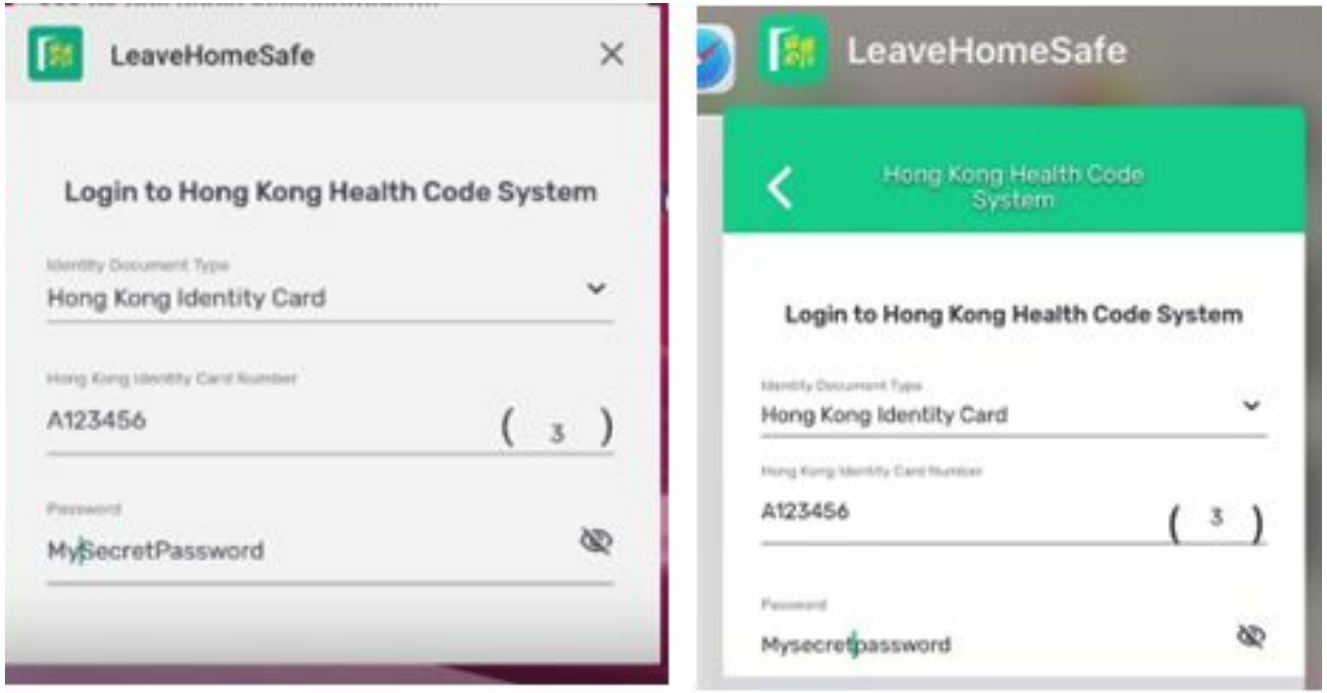
To **replicate** this issue in Android or iOS

- First, **navigate** to a **sensitive screen** within the application
- Next, **send** the application to the **background**
- Then, **show** the **open apps** and observe that the **text input** on the **sensitive** screen can be **read** by the user
- Notably, this text **remains readable** even after a device **reboot**

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

LHS-01-003 WP1: Leaks via Missing Security Screen on Android & iOS (Low)

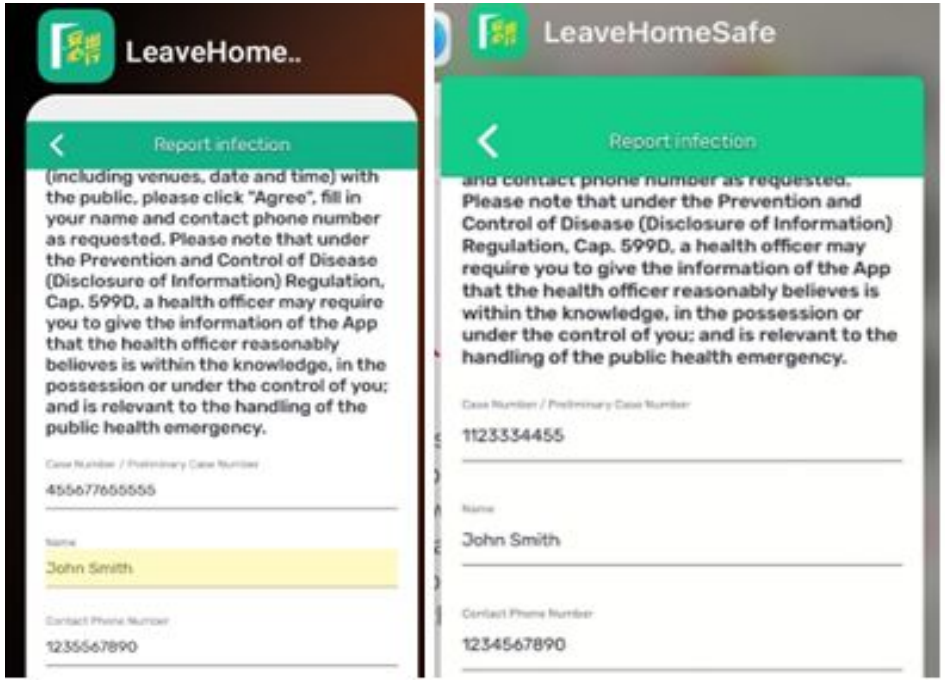
Example 1: ***Login leak on Android (left) and iOS (right)***



https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

LHS-01-003 WP1: Leaks via Missing Security Screen on Android & iOS (Low)

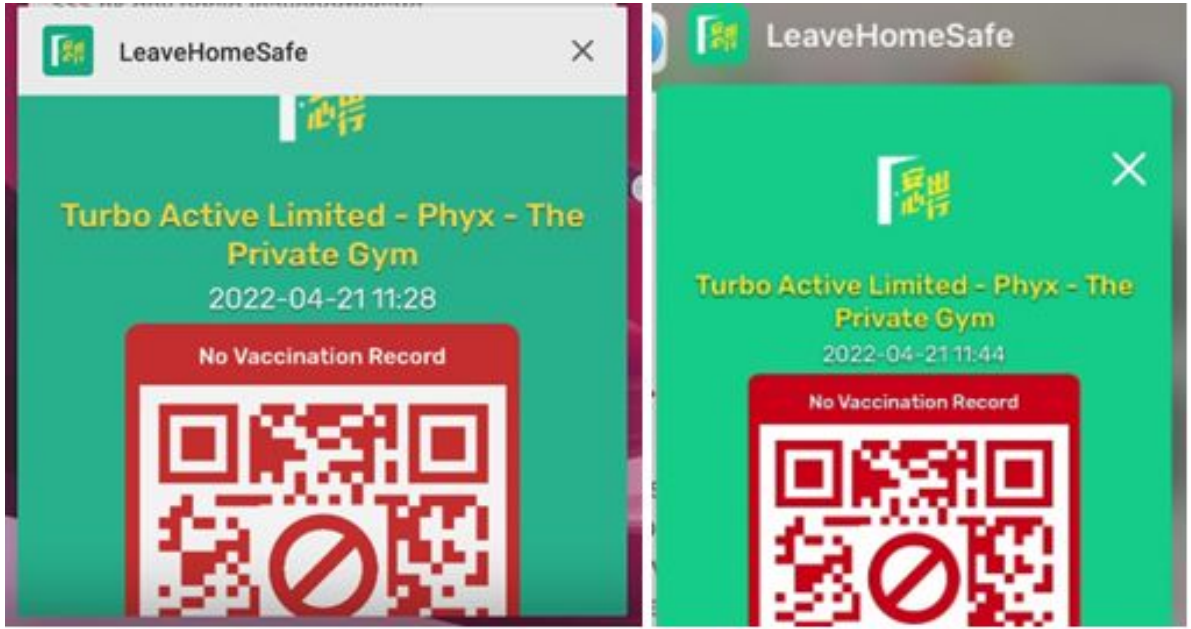
Example 2: *COVID infection leak on Android (left) and iOS (right)*



https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

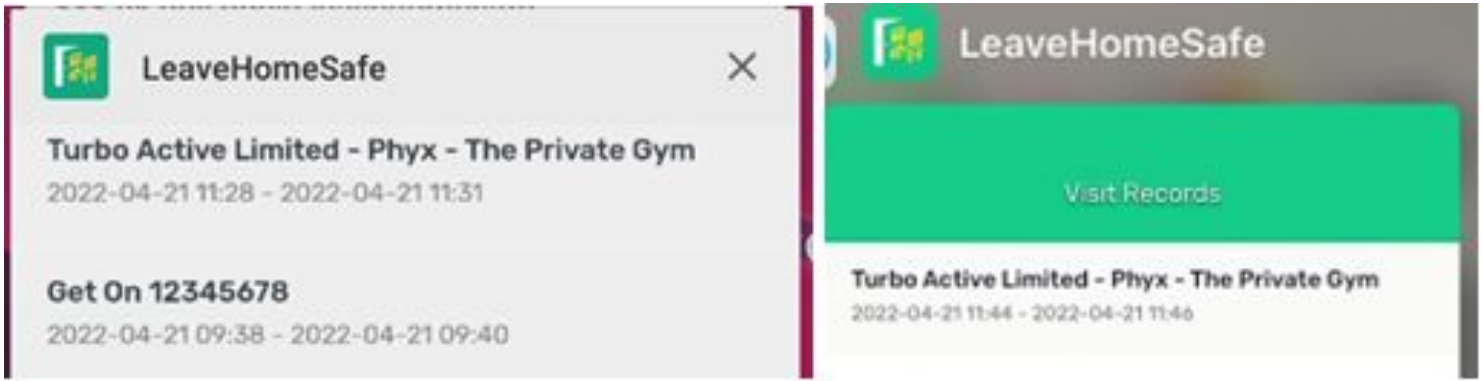
LHS-01-003 WP1: Leaks via Missing Security Screen on Android & iOS (Low)

Example 3: ***Possible visit leak on Android (left) & iOS (right)***



LHS-01-003 WP1: Leaks via Missing Security Screen on Android & iOS (Low)

Example 3: ***Possible visit record leaks on Android (left) and iOS (right)***



https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

LHS-01-002 WP1:
Possible Phishing
via
Task Hijacking
on Android (Medium)

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

LHS-01-002 WP1: Possible Phishing via Task Hijacking on Android (Medium)

- The **Android app** was **susceptible** to a number of **task hijacking attacks**.
- Vulnerable to **StrandHogg** and other techniques documented since 2015.

Malicious applications typically **exploit task hijacking** using one or more of the following techniques:

- **Task Affinity Manipulation**
- **Single Task Mode**
- **Task Reparenting**

Affected File:
AndroidManifest.xml

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

LHS-01-002 WP1: Possible Phishing via Task Hijacking on Android (Medium)

Affected Code:

```
<application android:theme="@style/AppTheme" android:label="@string/app_name"
[...]
<activity android:label="@string/app_name"
android:name="hk.gov.ogcio.leavehomesafe.MainActivity" android:exported="false"
android:launchMode="singleTask" android:screenOrientation="portrait"
[...]
<intent-filter>
<action android:name="android.intent.action.MAIN" />
<category android:name="android.intent.category.LAUNCHER" />
</intent-filter>
```


https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

PoC Demo

+ 7asecurity.com

https://7as.es/LeaveHomeSafe_74nfKZHYc/LHS-01-002_LHS_Task_Hijacking.mp4

Proposed Fix

```
<application android:theme="@style/AppTheme" android:label="@string/app_name"
android:icon="@mipmap/ic_launcher"
android:name="hk.gov.ogcio.leavehomesafe.MainApplication" [...]
android:taskAffinity="">
[...]
<activity android:label="@string/app_name"
android:name="hk.gov.ogcio.leavehomesafe.SplashActivity"
android:launchMode="singleInstance" >
<intent-filter>
<action android:name="android.intent.action.MAIN" />
<category android:name="android.intent.category.LAUNCHER" />
</intent-filter>
```


https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

LHS-01-007 WP1:
COVID Status Access
via
Unsafe SD Card Usage
(High)

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

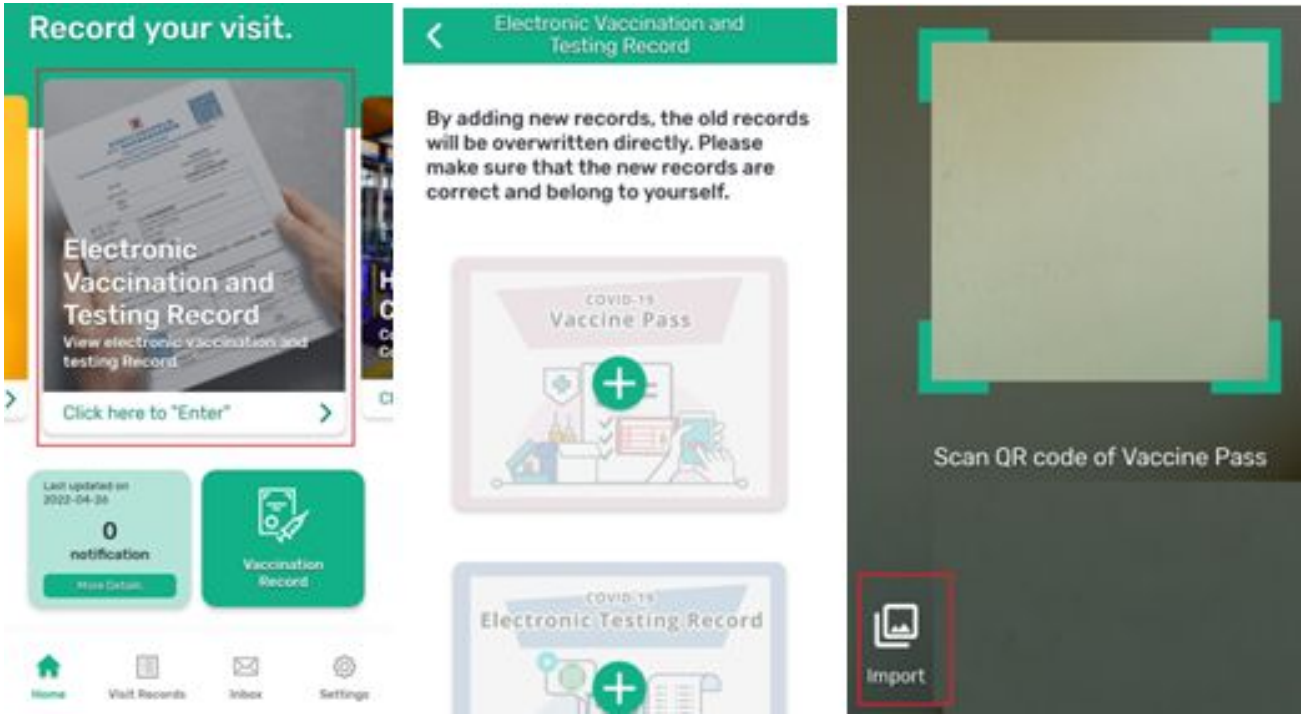
LHS-01-007 WP1: COVID Status Access via Unsafe SD Card Usage (High)

- LeaveHomeSafe **Android app:**
  - **Stores** COVID vaccination & COVID **test status images** in the **SD Card**.
  - When the user attempts to:
    - **Import** such **QR Codes** from safer locations, such as **Google Drive**
- Concerning because:
  - The **Android SD Card** is an **inappropriate location** for **sensitive data**
  - Example 1: Unskilled thief
    - E**xtract SD Card** + plug it to a computer = **read data**
    - without having to know the **PIN or unlock pattern**
  - Example 2: Malicious apps
    - Can read or modify anything stored in the **SD Card**
    - Only requirement = apps with **SD Card access**

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

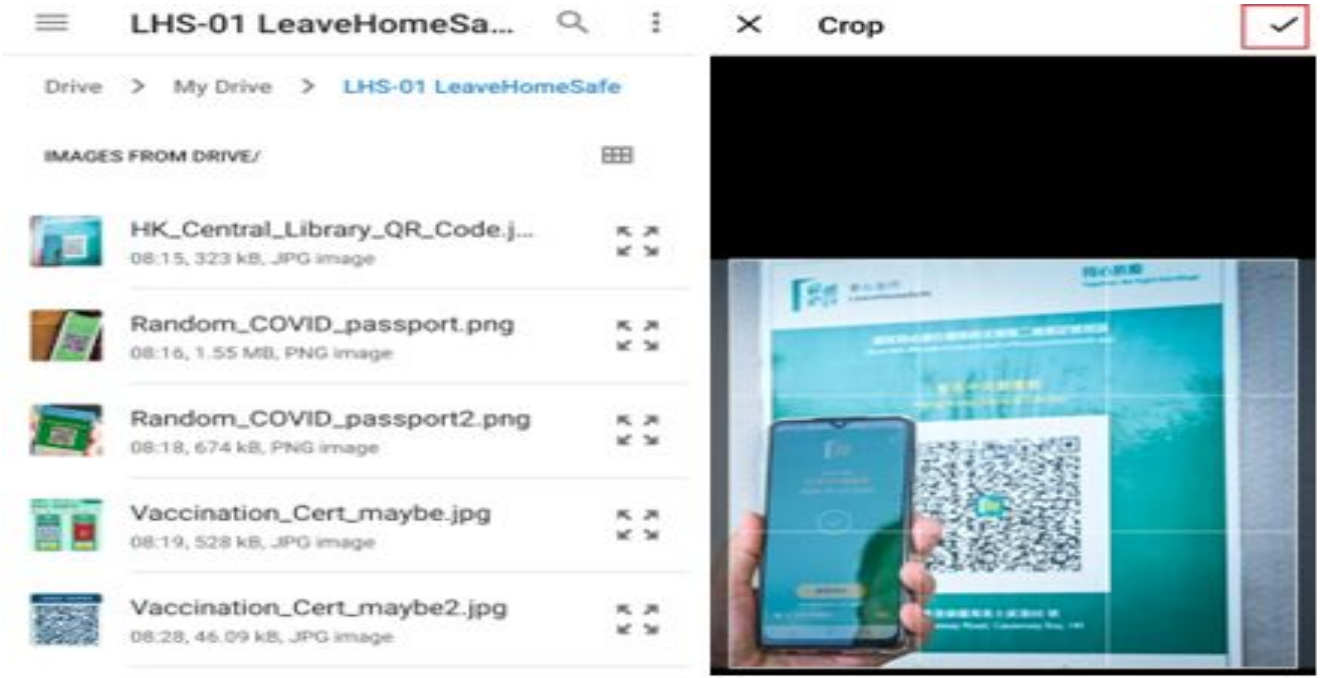
LHS-01-007 WP1: COVID Status Access via Unsafe SD Card Usage (High)

Fig.: Navigation to the Electronic Vaccination/Testing import



LHS-01-007 WP1: COVID Status Access via Unsafe SD Card Usage (High)

Fig.: Completing the Import process



LHS-01-007 WP1: COVID Status Access via Unsafe SD Card Usage (High)

ADB Command:

```
adb shell ls "/mnt/sdcard/Android/data/hk.gov.ogcio.leavehomesafe/files/Pictures/"
```

Output:

```
9e4e788e-1961-4c13-87fe-cced0906be31.jpg
```

LHS-01-007 WP1: COVID Status Access via Unsafe SD Card Usage (High)

Result:

- The **scanned image remains** in the **SD Card**
- **Trivial to download** to a computer using the following ADB command:

ADB Command:

```
adb pull
"/mnt/sdcard/Android/data/hk.gov.ogcio.leavehomesafe/files/Pictures/9e4e788e-1961-
4c13-87fe-cced0906be31.jpg"
```


https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

Recommendations

- **Avoid** the **SD Card** for **storing sensitive data**
- **Images** should be stored in the **internal storage** of the application (i.e. **/data/data/…**), where Android can **enforce permissions**
- If necessary, use **FileProvider** to **grant access** to relevant apps like the **Android Camera**.

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

Recommendations

- At a **minimum**, consider **encrypting** or **promptly deleting** used **SD Card QR Codes**, and do so when opening or closing the application.

- If this latter approach is chosen, even **shredding** may not **entirely erase** files on **flash storage**

- However, it will **reduce** the **forensic recovery** chances for an **attacker** with SD Card access.

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

LHS-01-008 WP1:
COVID Status Access
via
Auth Bypass
(High)

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

LHS-01-008 WP1: COVID Status Access via Auth Bypass (High)

The LeaveHomeSafe Android and iOS apps have a feature to:

- **Enable authentication** to **access** COVID **vaccination and test status**
- **PIN** or **fingerprint** required for access
- This feature can be **trivially bypassed** due to a **logic flaw**

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

LHS-01-008 WP1: COVID Status Access via Auth Bypass (High)

A **malicious attacker**, with **access** to an **unlocked device** could:

- **Gain access** to the user COVID vaccination and COVID test status

How?

- **Bypassable** with **simple screen tapping**
- Minimal **effort** and **skill** required for an **attacker**
- Current this **security control** offers **no protection**
- Issue **confirmed** on both **Android** and **iOS** apps

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

PoC

- **Navigate** to **app settings**
- **Enable Authentication**
- **Verify** that the **Fingerprint/PIN** appears to be required to **access** COVID vaccination or test status

NOTE: The steps to **enable authentication** are **identical** for Android

PoC

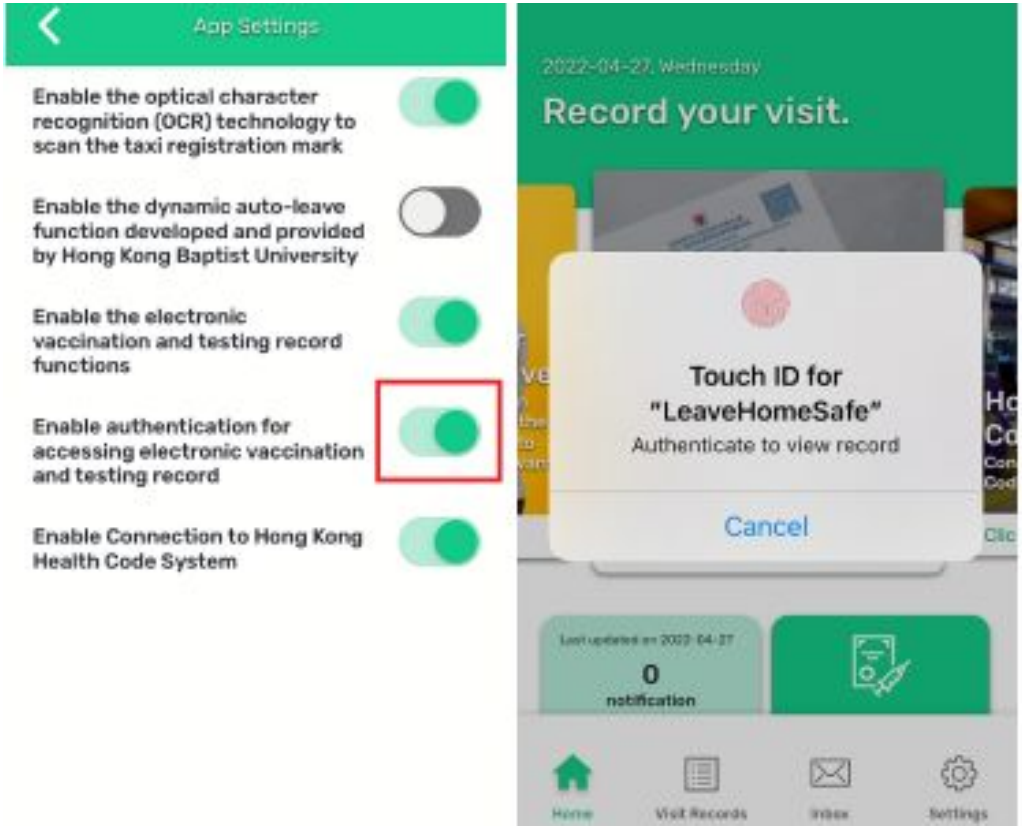


Fig.: Enabling authentication (iOS) requires Touch ID to access COVID status data

PoC

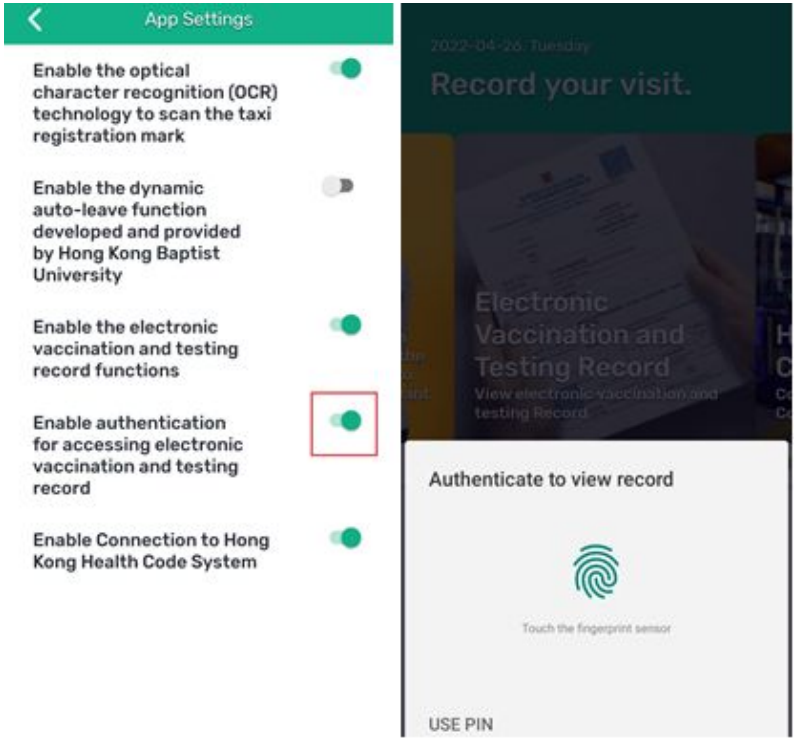


Fig.: Authentication (Android) requires the Fingerprint or PIN for COVID status data

PoC

- Optionally, **restart** the device and **open** the app again
- **Verify intended restrictions**
- On **iOS**, confirm **Touch ID** is still **required**
- Then **disable authentication** and **confirm access**

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

PoC

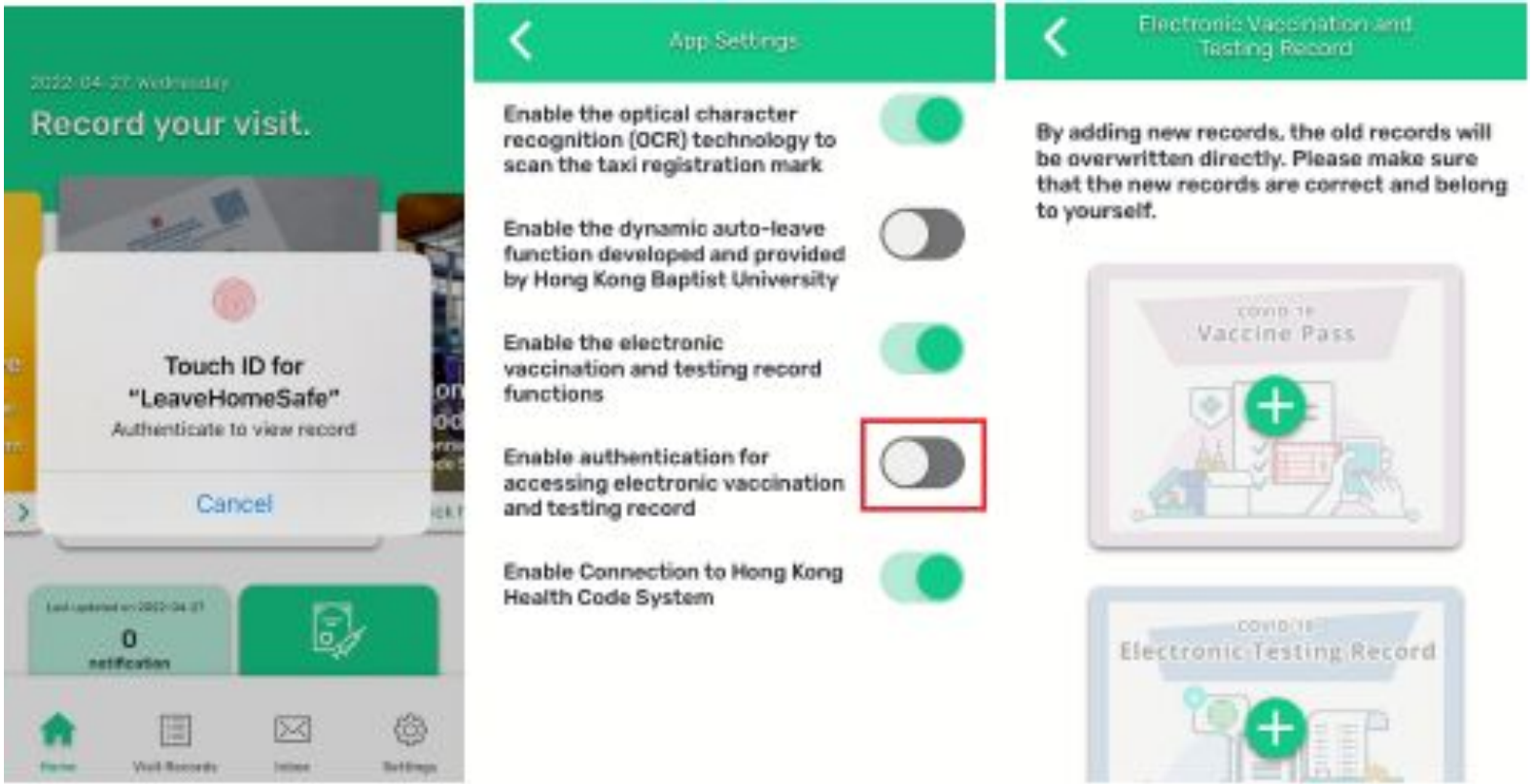


Fig.: Auth bypass in iOS

PoC

Following the same steps on **Android results** in an **identical bypass**

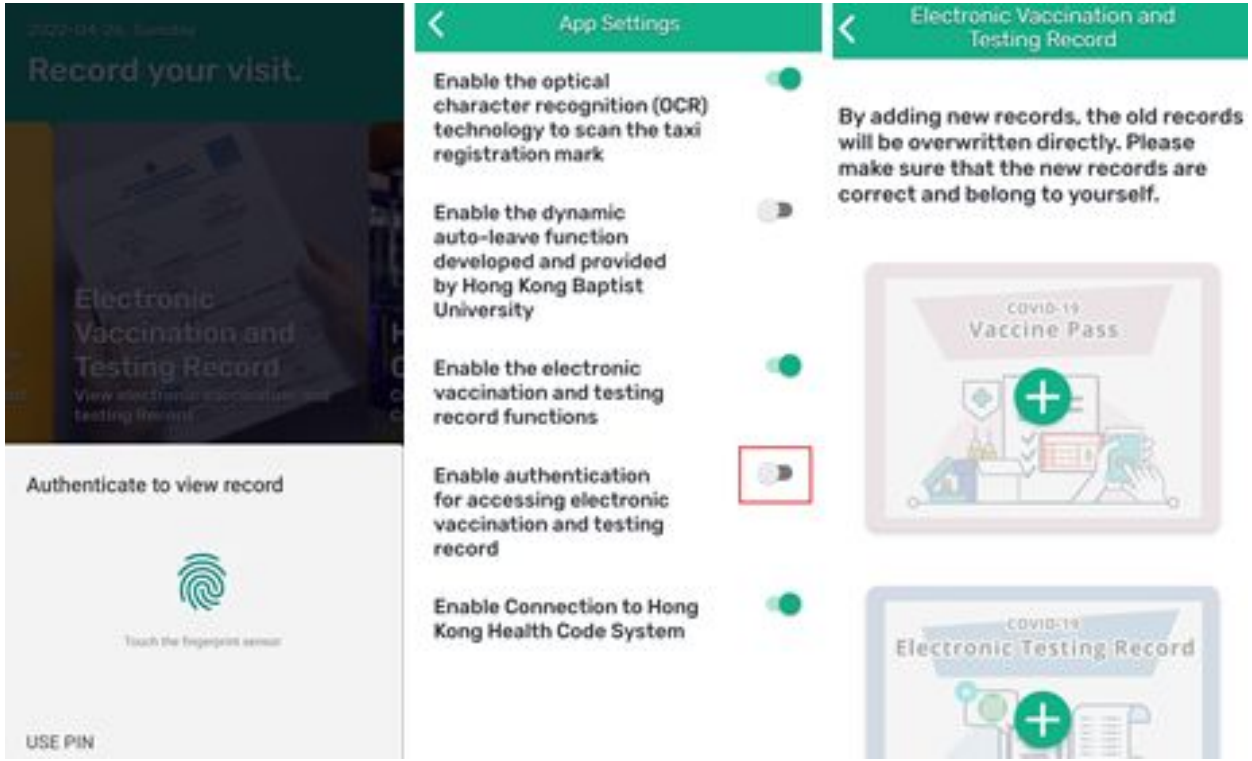


Fig.: Auth bypass in Android

DEMO

LeaveHomeSafe 3.3.0 Retest 2022-07-29:
Part 03 - COVID Status Access via Auth Bypass (High)
https://www.youtube.com/watch?v=qAl0AhhVeC8

Recommendations

- It is recommended to require:
  - The **Fingerprint or PIN**
  - Whenever the "**Enable authentication for accessing electronic vaccination and testing record**" setting is **enabled** or **disabled**.

- Furthermore, this feature should **ideally protect**
  - The **entire** application
  - Including the **user Visit Record, the Hong Kong Health Code System screens, etc.**

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

LHS-01-001 WP1:
MitM without Warnings
via
invalid TLS Certificates
(Critical)

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

LHS-01-001 WP1: MitM without Warnings via invalid TLS Certificates (Critical)

- LeaveHomeSafe Android app (v3.2.3) **lacks TLS certificate validation**
  - risking **MitM attacks** without **warnings** (!)

- A **malicious attacker**, with:
  - A **valid domain name** on the internet
  - and able to **manipulate network communications** (i.e.public Wi-Fi without guest isolation, BGP Hijacking, ISP MitM, DNS rebinding)
- Could **intercept traffic** without warnings
  - between the LeaveHomeSafe **application** and its **backend server**

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

LHS-01-001 WP1: MitM without Warnings via invalid TLS Certificates (Critical)

- For example, an **attacker** could:
  - **Intercept the login** to the Hong Kong Health Code System
  - **Gain access** to the **Hong Kong Identity Card ID** and **password** of the use
  - Obtain the **personal One Time Password** (OTP) provided by the Hong Kong Centre for Health Protection (CHP)
  - **Intercept user-reported** COVID infections

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

PoC

Step 1: Configure MitM using CA-signed certificates for an invalid hostname

- The Android device's **HTTP proxy settings** were updated to:
  - Use a **test proxy server**
  - with the ability to create **trusted CA-signed certificates**
- The **proxy server** was set to:
  - Always use **7asecurity.com certificates**
  - regardless of the **inbound host header**.

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

PoC

Simulates a **malicious attacker:**

- Able to supply a **valid certificate** for *7asecurity.com* to TLS clients.

NOTE: This configuration is:

1. **Invalid**
2. Should result in **security warnings** for any **TLS connection attempt**
3. Warnings should occur for any host that is not *7asecurity.com*.

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

PoC

Fig.: Proxy settings for CA-signed certificates with a hostname of 7asecurity.com

+ 7asecurity.com

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

PoC

Step 2: Verify the Android browser shows Security Warnings

The setup **supplies CA-signed certificates** for **7asecurity.com** to:

- All **TLS clients**
- Regardless of the **hostname** they attempt to connect to

Appropriate TLS validation should reject such certificate, which can be verified in the Android browser as follows:

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

PoC

Run the following ADB Command:

ADB Command:

```
adb shell am start -a "android.intent.action.VIEW" -d https://www.leavehomesafe.gov.hk
```

Fig.: The Android browser shows security warnings, as expected

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

PoC

Step 3: Confirm the complete lack of warnings in LeaveHomeSafe

- Open the **LeaveHomeSafe** application
- Try to login to the Hong Kong Health Code System
- **Use any randomly generated HKID**, and any **random password**

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

PoC

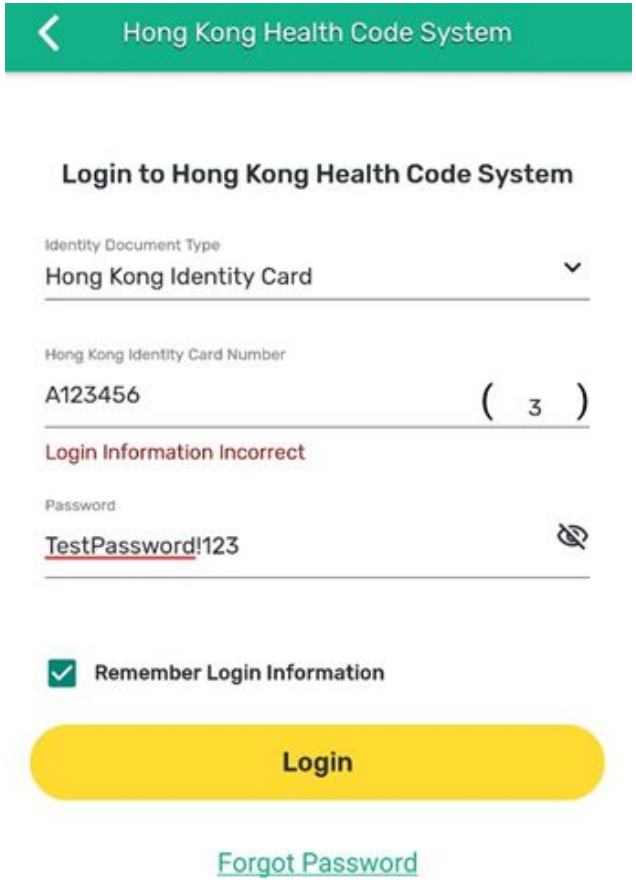


Fig.: Attempt to login with invalid credentials

PoC

Observe the captured login credentials without user warnings:

```
POST /lhsapi/loginV2 HTTP/1.1
Host: apply.ehc.gov.hk
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=utf-8
Content-Length: 197
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.1
Connection: close

{"docType":"0","docNum":"A1234563","docCountryCode":"HKG","hashId":"3600dd5f-9d40
-414a-b239-3205d0a29f7e","password":"TestPassword!123","lhsInstallDate":"16505259
35885","se cretCode":"JTp#-v4jN#@v"}
```

PoC

This issue can be further confirmed by submitting a report for COVID infection, entering any random OTP:

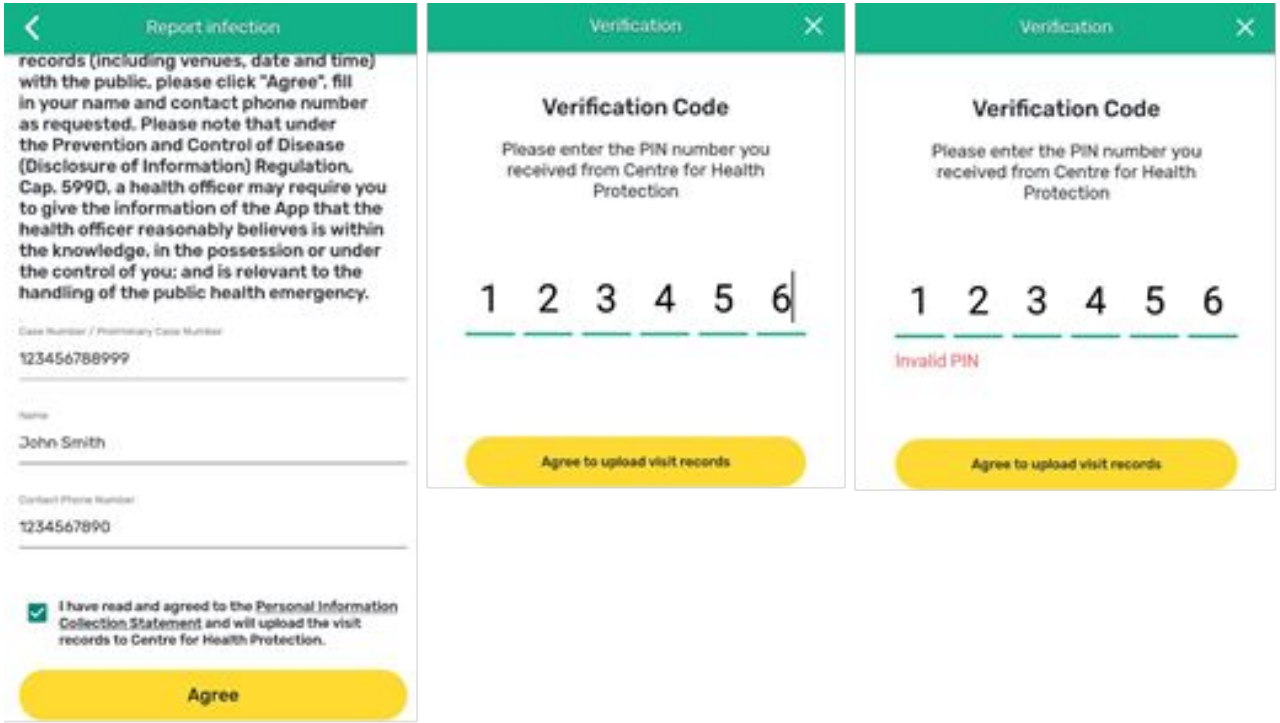


Fig.: Steps to report an infection

PoC

- No **user warnings** appeared after following the steps
- Confirm **successful OTP interception** in the **captured HTTP request**
- Which includes the **personal OTP** from Hong Kong CHP and case number

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

PoC

Resulting HTTP Request:

```
POST /app/pin/verify HTTP/1.1
Host: app.regqr.gov.hk
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=utf-8
Content-Length: 113
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.1
Connection: close

{"verifyCode":"123456","uploadBatchSize":1,"caseNum":"123456788999","uid":"03f949
24-43 60-4ced-a3f4-dcc09d013a2a"}
```

PoC

Affected File (decompiled):

hk/gov/ogcio/leavehomesafe/e.java

Affected Code (decompiled):

```
public class e implements HostnameVerifier {
   public e(MainApplication mainApplication) {
   }

    @Override  // javax.net.ssl.HostnameVerifier
   public boolean verify(String str, SSLSession sSLSession) {
      Log.d("XANA", "verify: " + str);
       if (str.contains("regqr.gov.hk") || str.contains("leavehomesafe.gov.hk") ||
 str.contains("ehc.gov.hk")) {
          return true;
       }
       return HttpsURLConnection.getDefaultHostnameVerifier().verify(str,
sSLSession);
   }
}
```

DEMO

LeaveHomeSafe 3.3.0 Retest 2022-07-29:
Part 02 - MitM via invalid TLS Certificates (Critical)

https://www.youtube.com/watch?v=oaXh9GMf1-4

Recommendations

- **Improve** the **TLS validation** of the Android app to resolve this issue.
- The **OWASP Pinning CheatSheet** could then be used to **secure TLS communications** further, so the application only trusts the **expected server certificates**.

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

The Ugly

Source: https://cdn.wallpapersafari.com/58/27/M3af4N.jpg

The Disclosure

Timeline:

- **2022-06-24** – Initial disclosure email attaching the **full pentest report**
- **2022-06-24** – **Automated** acknowledgement received
- **2022-07-04** – **Friendly** disclosure **reminder** follow-up sent, attaching the pentest report again
- **2022-07-04** – **Automated** acknowledgement received
- **2022-07-12** – **Friendly** disclosure **reminder** follow-up sent, attaching the pentest report again
- **2022-07-12** – **Automated** acknowledgement received
- **2022-07-19** – **Friendly** disclosure **reminder** follow-up sent, attaching the pentest report again

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

The Disclosure

Timeline:

- **2022-07-19** – **Automated** acknowledgement received
- **2022-07-26** – **Public Disclosure**
- **2022-07-28** – An **official Government response is issued**: […]The OGCIO expressed deep **regrets** and **strongly opposed** to the **inaccurate** report and **unfair accusation**.
- **2022-07-29** – 7ASecurity **confirms** LeaveHomeSafe 3.3.0 was released on 2022-06-02, 22 days before the report was shared, strongly suggesting nothing was fixed.
- **2022-07-29** – 7ASecurity further validates LeaveHomeSafe 3.3.0 (**the latest version**) **remains vulnerable** to (at least) the **highest impact findings**

https://7asecurity.com/reports/pentest-report-leavehomesafe.pdf

Hong Kong government’s reaction

Hong Kong government's reaction

*The Hong Kong government has **slammed** a report by an overseas cybersecurity firm as "**inaccurate**" after the company claimed the city's "Leave Home Safe" Covid-19 risk-exposure app was **vulnerable** to **data leaks** and **phishing attacks**.*

- South China Morning Post

Source: https://www.scmp.com/news/hong-kong/health-environment/article/3186966/hong-kong-government-slams-inaccurate-report

Hong Kong government's reaction

*The Office of the **Government Chief Information Officer** (OGCIO), which is responsible for the operation of the LeaveHomeSafe app, **hit back** at **7ASecurity's** "**inaccurate report**" and "**unfair allegation**" in a statement last Thursday.*

- Hong Kong Free Press

Source:
https://hongkongfp.com/2022/08/01/independent-audit-finds-security-flaws-in-hong-kong-covid-19-contract-tracing-app-govt-dismisses-report-as-inaccurate/

Hong Kong government's reaction

*Hong Kong's government has **rejected** an overseas cybersecurity firm's claim that **flaws** in the LeaveHomeSafe app **could expose sensitive user information**, saying there have been **no security or privacy-related incidents** and the report conducted by the company is **inaccurate** and **unfair**.*

\- The Standard

Source: https://www.thestandard.com.hk/breaking-news/section/4/192851/Govt-dismisses-report-of-security-flaw-in-LeaveHomeSafe-app

Hong Kong government's reaction

*How a **US influence** operation **<u>undermines</u>** Hong Kong's Covid efforts.*

*With no **expertise** in public health or pandemic control, the **irresponsible** operation behind the US-sponsored expose of 'Leave Home Safe' **security flaws** may well cost local lives*

- **South China Morning Post**

Source: https://www.scmp.com/comment/opinion/article/3187067/how-us-influence-operation-undermines-hong-kongs-covid-efforts

Conclusion

- A penetration test **report** serves as **concrete evidence**.
- Most journalists clearly do not understand this and somehow consider “random politician statements” to carry “equal weight” (!)
- This **pattern** underscores a **notable deficiency** in the realm of **information security journalism**.

This happens because:

1. Most journalists **do not understand pentest reports**.
2. They often overlook the critical concept that a **pentest report**, containing **tangible evidence**, **can be validated** by a **third-party source** or similar authoritative entity.

Conclusion

TLDR;

If you are a journalist and don’t understand pentest reports:

- Hire an independent third party able to download the app + verify the finding
- Armed with the (now double) evidence: Call out the politician BS

Questions


what
why
when
?
who
?
where
what
why
QUESTIONS
who
?
where
what
?
how
how
where
?

Q & A

Free Pentest Contest 2023:
https://7asecurity.com/blog/2023/06/free-pentest-contest-2023/

1000 USD off your next pentest → code: **DEEPSEC1000**

- sales@7asecurity.com / https://7asecurity.com/#contact
- Public pentest reports → https://7asecurity.com/publications

40% off any training course → code: **DEEPSEC40**

- https://store.7asecurity.com/discount/DEEPSEC40
- **Free workshops → https://7asecurity.com/free**

> admin@7asecurity.com

> @7asecurity

> @7a_

> @owtfp [OWASP OWTF - owtf.org]

+ 7asecurity.com