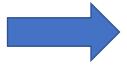
Open doors at the local gym

Black Alps 2021

The beginning





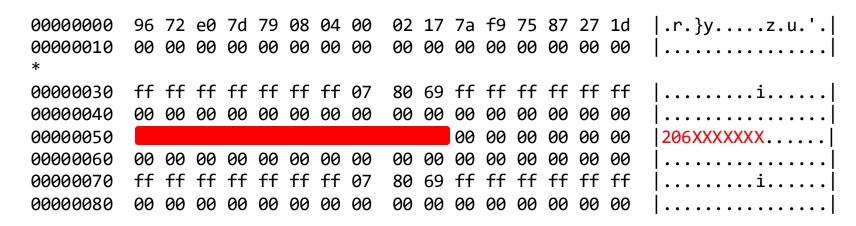






The badge

- MIFARE Classic 1k
- Weak PRNG
- Uses default key
- Memory extraction with the Proxmark 3
- Authentication based on its content

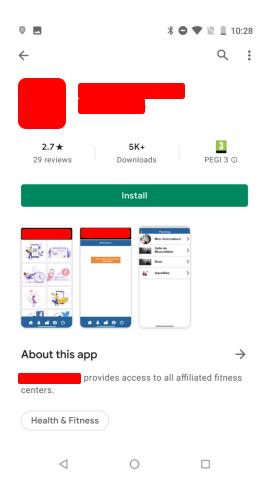




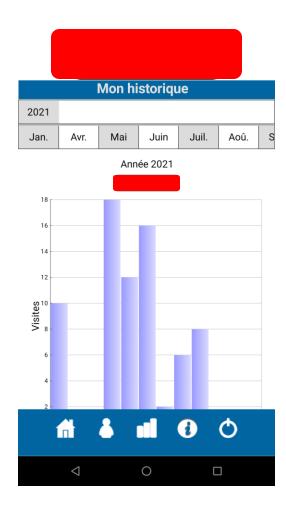




The app





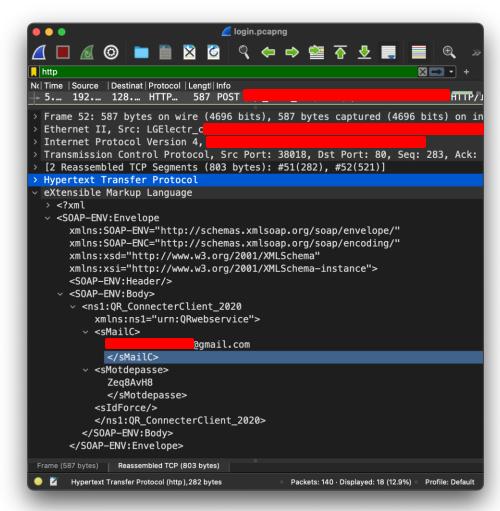


The app

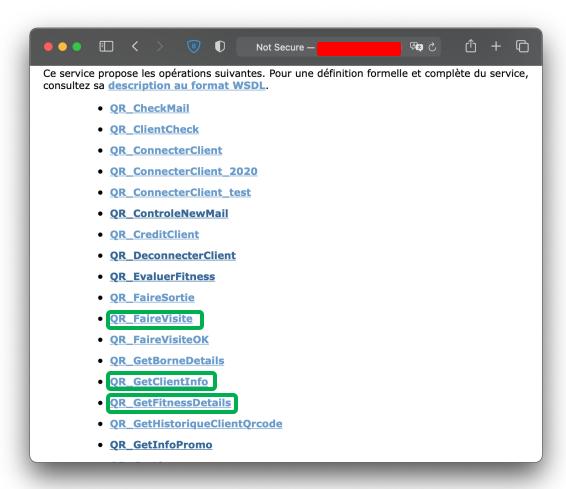
```
*New Project - jadx-qui
File View Navigation Tools Help
🛂 base.apk
                                                                       •
                                                                                                                                 .wdgen.GWDFvue_main 💥
                                                                                                                                                                                                                                              wdgen.GWDRRequete1 💥
  Source code
    > 🌐 a.a.a
                                                                                                                        .getInstance():
    android.support.v4
                                                                          1990
                                                                                                   WDAPIVM.variableRAZ(GWD
                                                                                                                                                     .vWD_PosUser);
    androidx
                                                                                                   WDInstance wDInstance2 = new WDInstance(new WDCodeBarres());
                                                                          1993
    > 🌐 bolts
                                                                          2000
                                                                                                   WDAPIDivers.sablier(new WDBooleen(false).getInt());
    × #
                                                                          2003
                                                                                                  WDAPIVM.multitache(new WDEntier4(-1));
        √ ⊞ wdgen
                                                                                                  if (!WDAPIVM.enModeTest().getBoolean()) {
                                                                          2006
                                                                                                        wDInstance2.setValeur(WDAPICodeBarres.cbCapture());
                2009
             > • GWDCPnatifiOS
                                                                          2012
                                                                                                        wDChaineU2.setValeur(wDInstance2.getProp(EWDPropriete.PROP_VALEURBRUTE));
                                                                                                  } else {
             > • GWDCPnatifJava
                                                                                                        wDChaineU2.setValeur("JLJLKJLKJ?P=MXwxMTU="());
                                                                          2018
             > GWDCPProceduresCommunicat
             > GWDCPProceduresGlobales
                                                                          2023
                                                                                                   this.vWD_pourcdb.setValeur(false);
             > GWDCPprocSocial
                                                                          2288
                                                                                                   if (WDAPIChaine.sansEspace(wDChaineU2).opEgal("", 0)) {
             > @ GWDCSTBorne
                                                                          2288
                                                                                                        finExecProcLocale();
             > G GWDCSTBorne2
                                                                          2035
             > • GWDCuncentre
                                                                          2035
                                                                                                   wDChaineU3.setValeur(WDAPIChaine.extraitChaine(wDChaineU2, 2, new WDChaineU("P=")));
             > 🚱 GWDCunclient
                                                                                                  WDAPIDivers.sablier(new WDBooleen(true).getInt());
                                                                          2045
             > @ GWDCuneborne
                                                                          2048
                                                                                                  WDAPIVM.multitache(new WDEntier4(-1));
             > G GWDCunepromo
                                                                                                   WDInstance wDInstance3 = new WDInstance(new WDXSDEntiteJNI("QRwebservice", "urn:QRwebservice", null, "QR_FaireVisiteResponse"));
                                                                          2051
             > G GWDCuneressource
                                                                          2056
                                                                                                  wDChaineU6.setValeur(WDAPIChaine.val(WDAPIHF.getFichierSansCasseNiAccent("ficunclient").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent("idclientchaine").getRubrigueSansCasseNiAccent(")
             > 😉 GWDCuneville
                                                                                                  wDInstance3.setValeur(WDWSManager.getClientWS("QRwebservice", "QRwebservice").invoquerMethode("QR_FaireVisite", WDAPIChaine.UnicodeVi
                                                                          2060
             > • GWDCunfitness
                                                                          2064
                                                                                                   wDChaineU7.setValeur(wDInstance3.get("OR FaireVisiteResult")):
                                                                                                   WDInstance wDInstance4 = new WDInstance(new WDXSDEntiteJNI("ORwebservice", "urn:ORwebservice", null, "OR GetMessagesClientResponse")
             GWDCuntypereservation
                                                                          2068
                                                                          2075
                                                                                                  if (WDAPIChaine.val(wDChaineU7).opEgal(8, 0)) {
             GWDFChargementPlanning
                                                                                                        try {
             > GWDFfen tes
                                                                          2078
                                                                                                              WDChaineU wDChaineU11 = new WDChaineU();
             > GWDFIFi A Propos
                                                                                                              wDChaineU11.setValeur(WDAPIChaine.extraitChaine(wDChaineU7, 2, new WDChaineU("$$")));
                                                                          2081
             > GWDFIFI Accueil
                                                                          2085
                                                                                                              WDReel wDReel = new WDReel();
             > GWDFIFI Bienvenue
                                                                          2088
                                                                                                              wDReel.setValeur(WDAPIChaine.val(wDChaineU11));
             > @ GWDFIFI_Bienvenue2020
                                                                                                              WDReel wDReel2 = new WDReel();
                                                                          2092
             > GWDFIFI Bye2020
                                                                          2095
                                                                                                              wDInstance = wDInstance4;
                                                                          2095
                                                                                                              wDReel2.setValeur(WDAPIChaine.val(WDAPIChaine.extraitChaine(wDChaineU11, 2, new WDChaineU(","))));
             > GWDFIFi_coordonnees
                                                                                                              WDReel wDReel3 = new WDReel();
                                                                          2099
             > @ GWDFIfi decouverte
                                                                                                              wDReel3.setValeur(WDAPIChaine.extraitChaine(wDChaineU7, 3, new WDChaineU("$$")));
                                                                         2102
              GWDFIFi Historique
                                                                          2106
                                                                                                              if (wDReel3.opEgal(0, 0)) {
             > @ GWDFIFI_horaires
                                                                          2109
                                                                                                                    wDReel3.setValeur(50);
             > GWDFIFI_InfoCentre
             > GWDFIFi_InfoPromo
                                                                          2114
                                                                                                              if (wDReel.opDiff(0) && wDReel2.opDiff(0)) {
             GWDFIFi Informations
                                                                          2117
                                                                                                                                           .getInstance();
                                                                                                                                            WD_PosUser.setValeur(WDAPIGPS.gpsDernierePosition());
             > GWDFIFI_ListeZR_Centres
                                                                          2117
                                                                                                                    if (WDObjet.ErreurDetectee.opEgal(false, 0)) {
                                                                         2120
             > GWDFIFI_NotifPush
             > • GWDFIFI_pasDeContrat
             > @ GWDFIfi_resume_decouverte
                                                                                                                                                                                        Smali
                CHRETE: Connon
```

The app

- No obfuscation
- No authentication
 - Purpose of the token ?!
 - E-Mail / password sent in cleartext
- No encryption
- All communications over HTTP
 - Leaks the URL of the webservice
 - Leaks the URL of the pictures



The webservice



The webservice – My personal data

••• • < >	(1)	Not Secure —	@ &	Ů + Ö
Cliquez ici pour la description complète de ce service.				
QR_GetClientInfo				
Pour tester cette opération, cliquez sur le bouton "Test".				
Paramètre Valeur				
sIdFitness:				
sIdClient:				
		Test		
••• • • >	₩ •	Not Secure —	C	ů + ©
This NO Et al.				
This XML file does not appear to have any style information associated with it. The document tree is shown below.				
▼ <soap-env:envelope xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> ▼<soap-env:body> ▼<ns1:qr_getclientinforesponse xmlns:ns1="urn:QRwebservice"> ▼<qr_getclientinforesult> Monsieur FR Suisse Fitness\206\Photos\2021010518533782_380.jpg 20201202074740547_20191022085816 12 mois 20191014 20230331 0 0 380 12 0 Ggmail.com </qr_getclientinforesult></ns1:qr_getclientinforesponse></soap-env:body></soap-env:envelope>				

The webservice – The gym information

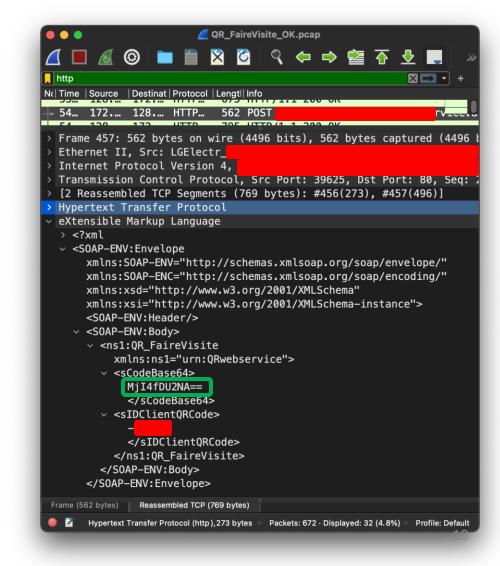


The door





b64decode("MjI4fDU2NA==") = 228|564



Open doors at the local gym Black Alps 2021

Conclusion

- No authentication
- No encryption
- Access to personal data
 - First name, last name, ...
 - Picture
 - Presence
- Remote door control
- And probably more ... ;-)

Bonuses

- #1

 "Bonjour oui désolé notre système de ticket est réservé normalement pour notre clientèle"
- #2

 "Due to the vacation period processing this issue is going to take some additional time"
- #3

 "Souvent copiés, jamais égalés!"

Thank you for your attention