

Open doors at the local gym

Black Alps 2021

The beginning



The badge

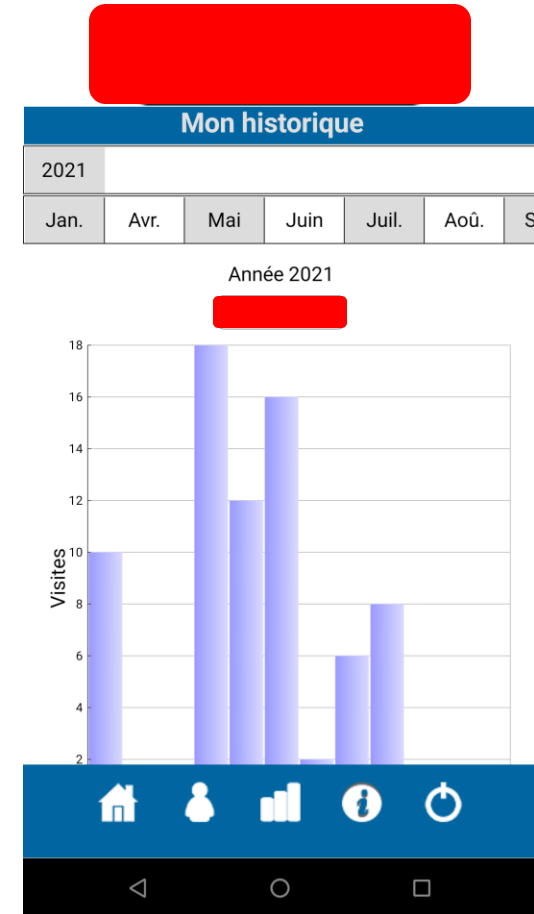
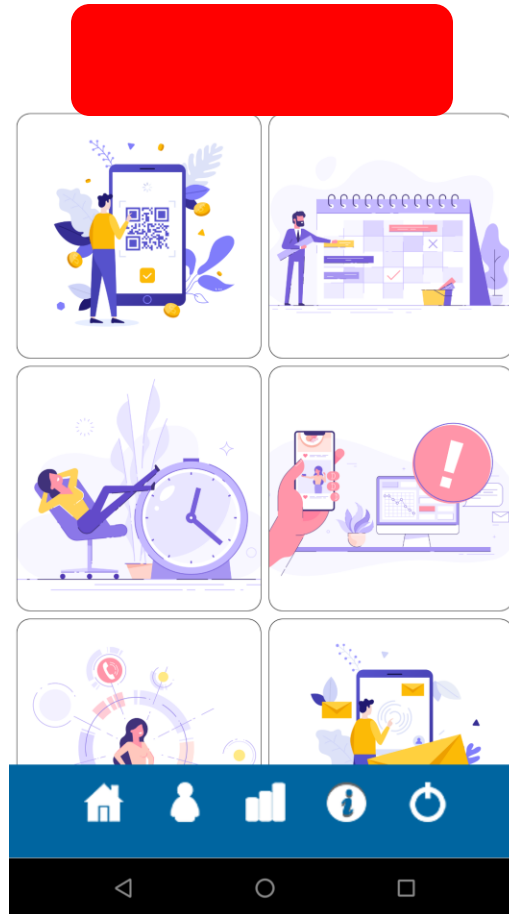
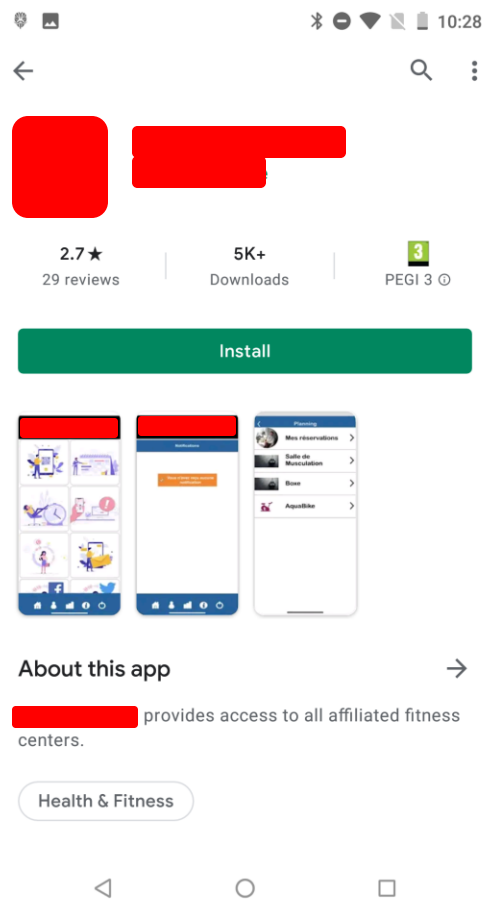
- MIFARE Classic 1k
- Weak PRNG
- Uses default key
- Memory extraction with the Proxmark 3
- Authentication based on its content



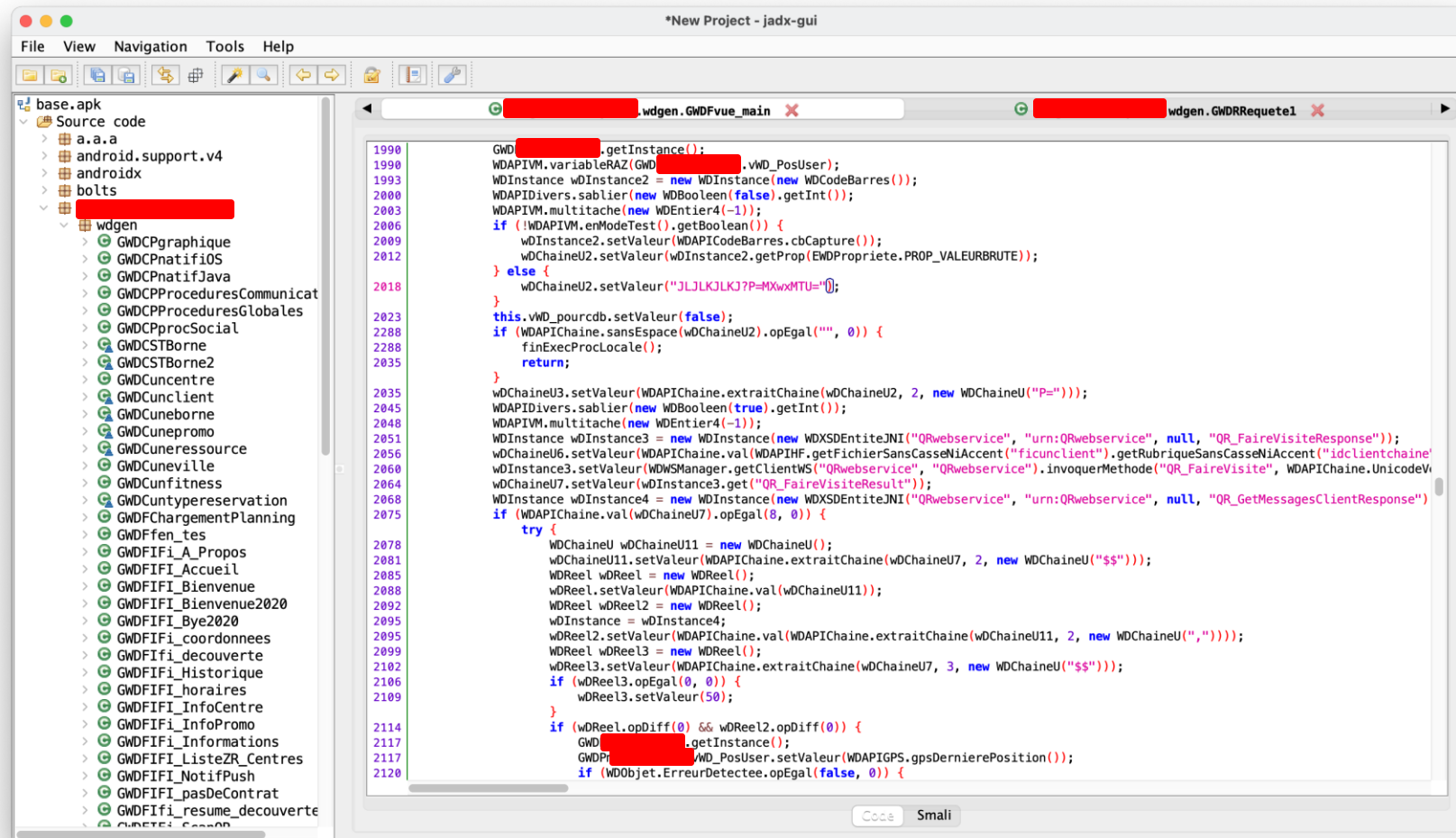
00000000	96 72 e0 7d 79 08 04 00	02 17 7a f9 75 87 27 1d	.r. }y.....z.u.'
00000010	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
*			
00000030	ff ff ff ff ff ff ff 07	80 69 ff ff ff ff ff ffi.....
00000040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000050	[REDACTED]		206XXXXXX.....
00000060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00000070	ff ff ff ff ff ff ff 07	80 69 ff ff ff ff ff ffi.....
00000080	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00



The app

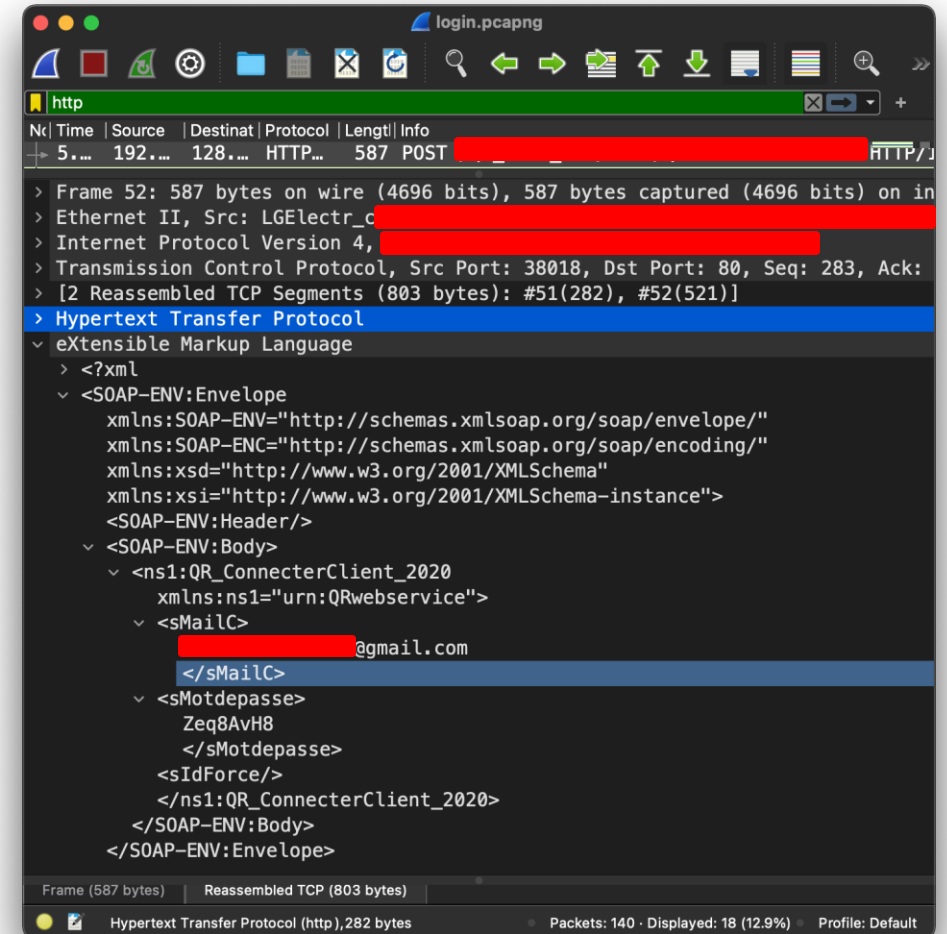


The app

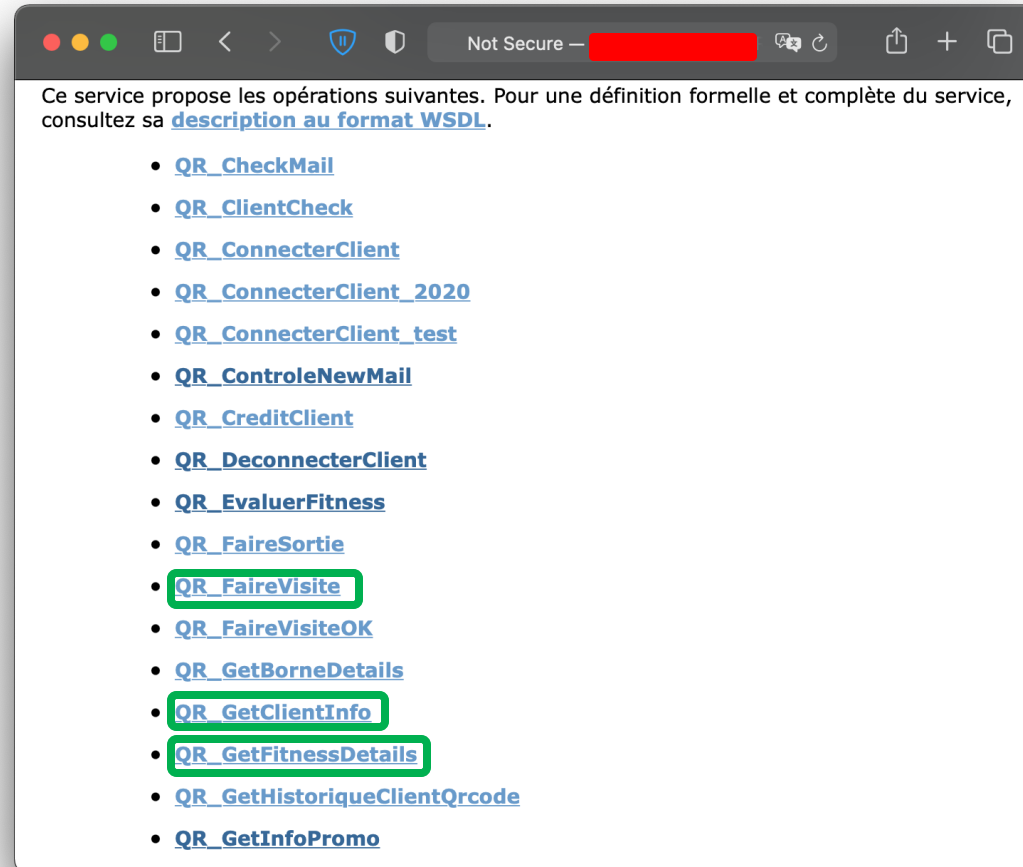


The app

- 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

Not Secure [redacted]

[Cliquez ici](#) pour la description complète de ce service.

QR_GetClientInfo

Pour tester cette opération, cliquez sur le bouton "Test".

Paramètre	Valeur
sIdFitness:	[redacted]
sIdClient:	[redacted]

Test

Not Secure [redacted]

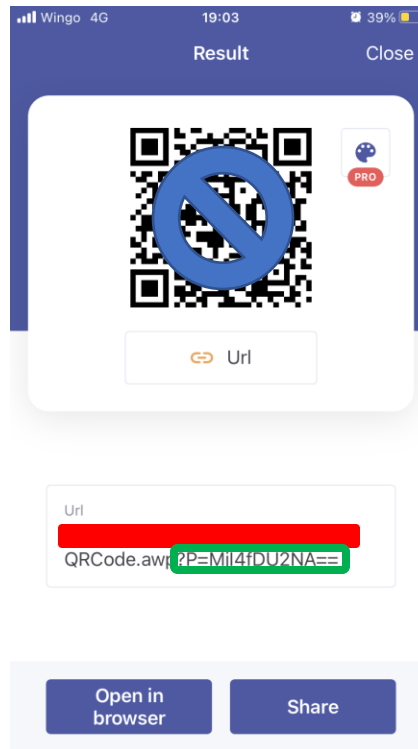
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <ns1:QR_GetClientInfoResponse xmlns:ns1="urn:QRwebservice">
      <QR_GetClientInfoResult>
        Monsieur|[redacted]910101|[redacted]|||[redacted]
        FR||Suisse||Fitness\206\Photos\2021010518533782_380.jpg||20201202074740547_20191022085816||12 mois
        |[redacted]|20191014||20230331||0||0||380||12||0||[redacted]||[redacted]@gmail.com|||||||
      </QR_GetClientInfoResult>
    </ns1:QR_GetClientInfoResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

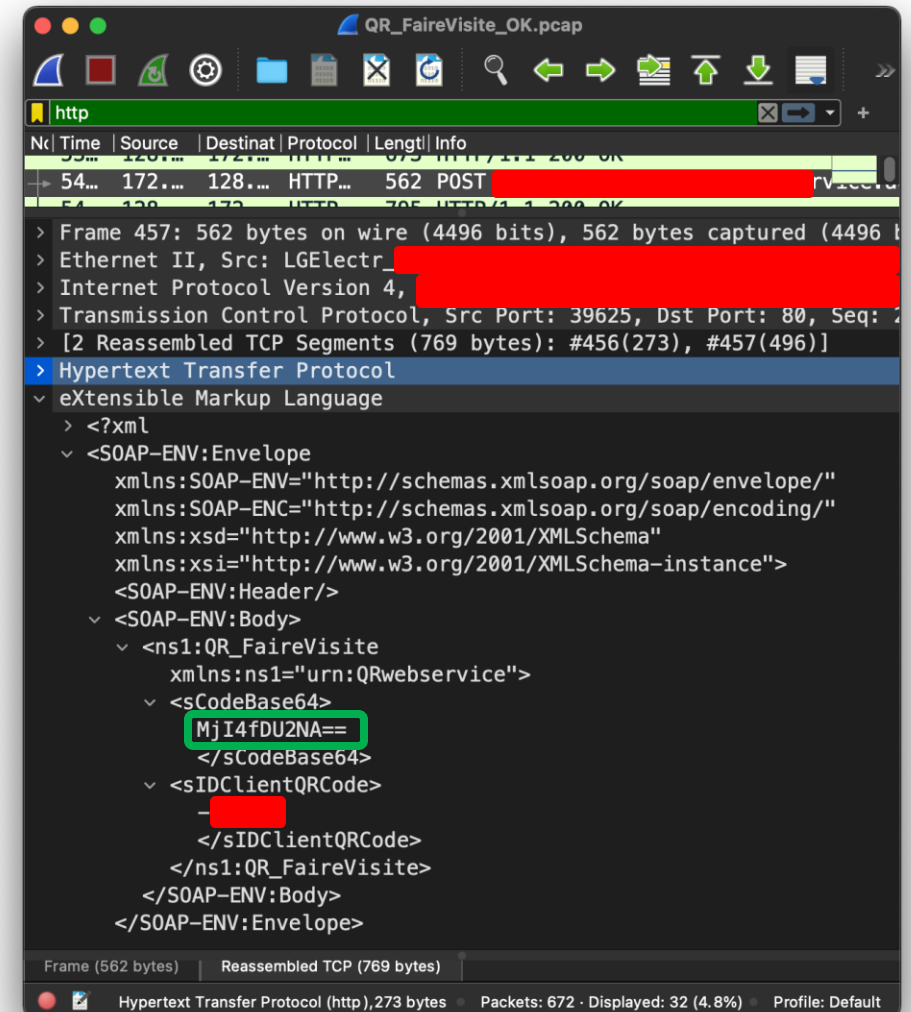

The webservice – The gym information




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