

Forum:[Hack Forums](#)

Thread: [Membr QR Code Generator Decryption](#)

Fatsoldiot - July 3, 2023, 3:34 am

First post here, wondering if it is possible to figure out how this QR Code is generated.

The gym I go to uses the service "Membr" which means they have an app which generates a QR Code which is scanned to enter the gym.

The QR Code is generated every time the menu is opened and lasts for 15 seconds or until it is closed where the menu would have to be opened again to generate a new one.

An example of the QR Code is:

imgur (dot) com (slash) Y3eEh7q

The code has 3 distinct parts:

1. The QR Code itself, which so far has always decoded as the string "30097258" which might change depending on the day but I have not tested that much
2. The random letter + random number that generates seemingly randomly at the center of the QR Code
3. The date and time underneath the code which may or may not have any actual real bearing on if the code is accepted by the scanner

One thing that stands out to me is that the QR Code always returns "30097258" and not a url with a secret key (which would make things a lot easier), which I believe means that they are using the letter + number for authentication. My cryptography is not that great so I was wondering if it is even possible to generate the letter+number correctly or if it is just completely impossible as they are communicating over the server.

However, one slight issue with that is that, as far as I can tell, the QR Code generates completely fine without being connected to any Wi-Fi or mobile data networks which I take to mean that they do not work together over the server. As far as I know, this means that the scanner and the mobile app should be using the same algorithm to generate the string based on the same parameters.

Of course, I have just begun to look at this and I do not know what factors could potentially change in the future such as the string "30097258". I would like to experiment with various factors but it is not easy to do so in the actual gym so mostly all testing must be kept to a minimum. However one thing I would like to test is if changing the date and/or time of my device would affect the generation if the string is generated by a basic method pseudorandomly

I might be barking up the wrong tree here but I would like to understand how the algorithm works. For clarification, I have no need to replicate the QR Code to enter for free, especially since I doubt that that is possible, but I just want to understand how this works and would appreciate it if any of the far more experienced people on this app would help me to understand.