Security in Organizations: Assignment 2

Group number 27

Elwin Tamminga
s1013846

Lucas van der Laan
s1047485

All the information gathered is from either the website https://demo.tiqr.org or the user manual https://tiqr.org/wp-content/uploads/2011/05/tiqr_manual_v1.0.pdf

A

- Cookie flags are not set, like HttpOnly, Secure, and SameSite. This makes it easier for an attacker to steal the steal and take over the session (PHPSESSID) that is used during the enrollment.
- The user's ID can be 2 million characters long. It can cause software bugs which could lead to more vulnerabilities.
- The QR code is displayed very clearly on the screen, this can be used by passerby's as well. Anyone can just walk by, or if someone has access to your screen (through malware), they can scan it. It's in the open, and many people do not actually go into a secluded area without prying eyes to do such things.
- You can create an account with anyone's name. There is no verification process to check if you used your real name.
- The animal icon that shows up in the PIN code removes the obfuscation from the PIN code and makes offline attacks with your device possible.

B

- A malicious user can steal the session of the user. When the user is done with the enrollment and logs in, then the malicious user is also logged into the same account.
- A malicious user that wants to do a Denial of Service attack on Tiqr can spam accounts with large data so the servers get overloaded and other can no longer sign up and maybe even log in.

- A malicious user can have the mobile application installed on their phone as well and scan the QR code instead. They can then use the Tiqr app to have access to the bank account.
- A malicious user can steal your identity or pretend to be you by creating an account in your name.
- A malicious user is watching your screen while you are entering the pin and they can then see all the animal icons, they then get access to your phone (through breaking and entering or other means) and enter all the numbers until they see the combination that they wanted. The attack is faster the more icons the person knows.

C

(a) All of the risks are not acceptable, since they either break the application or they allow a malicious user to mess with a normal user.

(b)
- A Secure session cookie makes it so that stealing a user's cookie is not possible unless they have already have access to the machine.
- Make sure that the input has proper input validation including a maximum length.
- Do not use a QR code for the enrollment process, make it so that a password is send to the user by email or a letter, which the user has to change after logging in for the first time. It can then also generate a QR code for 2FA.
- Identity verification using manual sign up using the person's identification could be employed, or use different means of identification verification.
- The animal icons need to be removed, they remove the obfuscation from the password and reduce the complexity by a lot.

D

No, even if the account will have 0 euro, someone still has access to the account that was supposed to be yours and other attacks are still possible.

E

No, there are missing security controls that protects against eavesdropping or manipulation of communication, because the QR code that is used during the enrolment process can be eavesdropped or an attacker can make a phishing website to let the target scan his login QR code to gain access. So the verification is also not reliable for releasing person identification data.

F

The life-cycle of the authentication is missing the identification of a natural or legal person.

G

A user could accidentally send €1050 instead of €10,50 or send the money to RABO 0XXXXXXX4 instead of RABO 0XXXXXXX5. Basically the user could send to the wrong amount of money and/or send money to the wrong person.

H

1. With the Raboscanner, you need a physical card and the physical scanner to access the login, instead of just a mobile app.
2. Before you can use the scanner, you need to enter the details from your bank card into the login website, instead of just a QR code.
3. The Raboscanner gives back a code again, instead of redirecting instantly like Tiqr.

I

Tiqr displays an animal every time the user enters a pin number, this means that the hiding dots are circumvented.

J

The malicious user can watch over the shoulder of the victim and see which numbers someone is entering by looking at the animal icon. It is more difficult to see the actual numbers being pressed by the user (because people tend to hide that), but people tend to not hide the result, since it's obfuscated anyways.

The malicious user can then steal the victim's phone and keep trying numbers until they see the icon that the victim also got. Since you do not need to submit the pin code until you have figured it out, you can keep doing offline guesses until you have found it. This completely circumvents the blocking after 3 failed attempts.

K

(a) No, because the PIN is the most important information that the user has, with a PIN code the user's money is now in the hands of the attacker.

(b) Simply removing the image that displays the combination would be the most relevant fix, because the images circumvent any and all obfuscation methods.

L

Compared to two-factor authentication systems that also requires a password, Tiqr is more vulnerable because an attacker only needs what you have (the app to scan his QR code), instead of also the victim's password.