Web Applications [2024/2025]

Lab 14: MFA with TOTP

In this lab you will require that some users, after login, must authenticate with a second factor to be able to perform some operations. In particular, the use of a TOTP will be required, based on a shared secret with the server that is already stored in the database. Thus, the database must be changed accordingly, adding a TOTP secret set for some users.

1. Implement a 2FA method using TOP for some users

Add a new page where some users are directed after login, in order to enter a TOTP that will allow them to perform specific operations, detailed later. Such redirection should happen only when, after authentication, the server responds that such specific user can do 2FA. If the 2FA is successful, such condition will be remembered in the session and will remain valid as long as the session is valid.

In this lab, only users that successfully performed MFA can add, edit and delete the films, differently from the previous lab where any user could perform any operation on their own films.

Follow the programming pattern shown during the lectures:

- Create an authenticated API endpoint that can receive the TOTP code.
- Validate such TOTP code on the server and remember the result in the session. Then, allow add, edit and delete operations on the server only if the 2FA was successful. As a convenience for the user, disable the add, edit and delete buttons in case the user cannot perform such operation (because the user has no 2FA enabled, or because the 2FA failed).

Hints:

1. *For the TOTP secret, you can use the same from the lecture examples, reported below, and for simplicity you can use the same secret for all users that can perform 2FA.*
2. *To generate the TOTP code to be entered in the form, scan the QR-code provided in the lecture examples (or below) with apps such as Google authenticator, Microsoft authenticator, or any app supporting TOTPs. Alternatively, past the secret key string on https://totp.danhersam.com/ and use the code shown there.*

Secret: `LXBSMDTMSP2I5XFXIYRGFVWSFI`