Practical exercises and questions:

In the following section there will be three exercises about Broken Access Control and Cross Site Request Forgery. We suggest you to follow the exercises in the order in which they are presented.

Exercise 1: In the following exercise you will experience what happens if administration panels are not sufficiently protected.
You can find the lab here: https://portswigger.net/web-security/access-control/lab-unprotected-admin-functionality

Objective: The goal of the exercise is to delete another user of the application named Carlos. Keep in mind that this lab has an unprotected admin panel.

A suggestion in case you are lost: *Try to access the* `robots.txt` *file. You may find something interesting!*
(If you want to find out more about `robots.txt` *files, read the brief "focus" below)*

"Focus": `robots.txt`
The `robots.txt` *is a text file, usually found in the root directory. This file is used to communicate with search engines. A robots.txt file tells search engine crawlers which URLs the crawler can access on the site. In fact, with this file, you can simply manage access to folders or resources avoiding overloading the site with many requests. The directives in this file are not strict rules followed by any crawler but are simply guidelines. With these instructions you can suggest not to access specific pages or directories. Remember that this file does not protect against unauthorized access.*

Exercise 2: In the following exercise you will experience what happens when static files are accessible to any user. Files may contain sensitive information…
You can find the lab here: https://portswigger.net/web-security/access-control/lab-insecure-direct-object-references
Objective: The goal of the exercise is to find the password of another user of the application named Carlos. Keep in mind that this lab stores user chat logs directly on the server's file system and retrieves them using static URLs.

A suggestion in case you are lost: *You should ask yourself how file names work and how you can retrieve those files… Try to access other files, not just the ones you are supposed to. You may find something useful!*

Exercise 3: In the following exercise you will experience what happens if critical functionalities of the application are vulnerable to CSRF attacks.
You can find the lab here: https://portswigger.net/web-security/csrf/lab-no-defenses

Objective: The goal of the exercise is to change the viewer's email address using some HTML that performs a CSRF attack. The only thing you know is that the email change functionality is vulnerable to CSRF. Use these credentials to access the application: Username: wiener – Password: peter

A suggestion in case you are lost: *You may find out how the requests are generated, then you can try to write your own. You can write a pre complied request to be somehow sent... Use the exploit server to deliver the attack.*

Questions:
In this little section you will find some simple questions to test your comprehension of the topic.

1. Simply describe what "Access control" means
2. Name some of the problems Broken Access Control can lead to
3. Describe what Cross-Site Request Forgery is
4. What are the key actors necessary for a CSRF attack?