Web shell upload via race condition

1. This lab contains a vulnerable image upload function. Although it performs robust validation on any files that are uploaded, it is possible to bypass this validation entirely by exploiting a race condition in the way it processes them.

2. I saw this lab's hint. I know why this lab is vulnerable. The backend takes my image that I uploaded and uploaded it already to the website then checks if it is valid image or not. If it is valid, the website will leave it and tell me that the image is uploaded successfully, and if not, the website will delete the image and tell me that the image is not valid.

3. I think that I can upload my shell file, and while checking, I can access the shell and get what I want. In this case, we can't send two requests in parallel. I need to send the request that is responsible for uploading the file, then send the second request that is responsible for accessing the shell file.

4. We will use Turbo Intruder in burpsuite. This extension does what we say in the previous point.

5. I intercept two requests (uploading and accessing) and pass them to turbo intruder and start the attack.

6. The get request responds with 200 OK and I got the secret key of carlos.