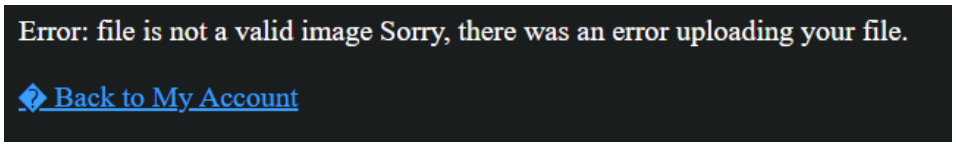
Remote code execution via polyglot web shell upload

1. This lab contains a vulnerable image upload function. Although it checks the contents of the file to verify that it is a genuine image, it is still possible to upload and execute server-side code.

2. While uploading the shell file, the uploading failed duo to invalid image.



3. I tried to manipulate the filename and provide the content of the file with jpg and png signature, but all these ways were useless. I knew that I should upload real image.

4. I think to inject the payload into the content of a real image. There is tool called **exiftool** in kali linux. This tool is command line utility for reading, writing and editing metadata in image, audio and many other file formats. I used this tool to inject my payload into the image.

5. In this case, I think that I can't inject parameter and get shell on the application. So, I will inject only one command that can read the content of `/home/carlos/secret` file.

6. In kali linux, I used exiftool to do this mission.

7. Now, I have a real image that contains my payload. I uploaded it to the website, and it uploaded successfully. When I opened the image in new tab, this was the result.

The payload ran and return the content of the file and the lab solved.