Task 5:

A description of the attack steps you performed to get access to file /var/gold.txt.

First, I uploaded a file to see how the request goes out and how the uploaded file is processed. If you look at the Download endpoint, we can see that via f parameter, we can set the file name to download. If you put in something random, you can also find the exception message where within it gives us the full path of the directory where files are stored. By uploading the premade .jsp script from Moodle, we can simply go to https://d0b100da-730b-4986-8f1e-71e512fad75f.i.vuln.land/uploadfile/shell.jsp and launch the jsp shell browser from there. From here, we simply navigate to /var/ and read the gold.txt file.

The content of file /var/gold.txt.

HL{New_is_always_better}