Homework 6

- Homework 6
  - Exercise 1: [attack] Just In Time **Never use your actual GASPAR password on COM-402 exercises (if the login form is not Tequila).**

Exercise 1: [attack] Just In Time

Please, try to do this exercise without looking into the files that are in the docker as it is simulating an external server to which you can only send POST requests.

In this exercise, you're being asked to guess credentials on a website.

You will run the website locally by doing:

```
docker run --rm -it -p 8080:8080 --name hw6ex1 com402/hw6ex1
```

Then, to login, you must send a POST request with a JSON body looking like:

{"token": yourguessedtoken }

to

http://0.0.0.0:8080/hw6/ex1

Note, remember to use the `JSON` body, and not the `form` body (we are not submitting a form). The Python syntax is slightly different from what you learned last week.

Don't try to brute force the token. There are much faster ways to guess the correct token.

For example, the developer here used a modified function to compare strings which express some very specific timing behavior for each valid character in the submitted token...

The response code is 500 when the token is invalid and 200 when the token is valid. Look at the body of the response, you can get some useful information too.

This exercise will require some patience and trial-and-error, as time in networks is never 100% accurate. In order to be precise, you should calibrate your measurements first, before trying to do any guessing on the token.

To verify that you retrieved the correct token check the file inside the docker container:

`/root/solution/solution.txt`