CHALLENGE - EMDEE FIVE FOR LIFE

- We are given with an IP and a port referring to a website
- In this website we can see a string that we need to MD5 encrypt
- The challenge is to encrypt as fast as we can
- We can try to do it manually by

```
$ echo '{string}' | md5sum
```

- Then copy and paste the result, but we will fail
- In particular we obtain the next string and a "Too slow" label
- We need to script
- However before scripting we need to know some informations

1. Which HTTP method we will need to supply the answer (POST I suppose)
2. Which HTTP POST parameter we need to set with the answer

- All of these answers can be obtained by setting up a proxy on localhost:8080
- Then opening BurpSuite in Intercept Mode
- Finally, clicking on Submit in the web page
- The following solution is given in Python code

```
import requests
import subprocess
from bs4 import BeautifulSoup
from hashlib import md5


URL = "http://{IP}:{port}/"
COOKIES = {"PHPSESSID" : {cookie}}


def try_solution(hash_txt: str | None=None):
    if hash_txt is None:
        resp = requests.get(URL)
        html_text = resp.text
        soup = BeautifulSoup(html_text, features="lxml")
        hash_txt = soup.body.find('h3', attrs={'align':'center'}).text

    md5_hash = md5(hash_txt.encode()).hexdigest()

    print(f"{hash_txt} -> {md5_hash}")
```

```
    resp = requests.post(URL, data={"hash" : md5_hash}, cookies=COOKIES)
    soup = BeautifulSoup(resp.text, features="lxml")
    hash_txt = soup.body.find('h3', attrs={'align':'center'}).text

    return hash_txt, resp.text


if __name__ == "__main__":
    hash_txt = None
    for _ in range(2):
        hash_txt, resp = try_solution(hash_txt)
        print(resp)
```

- Notice that you will need to change the IP, the PORT and the COOKIE
- Finally, run the code

```
$ python solve.py
```

- At the second attempt you will find the flag