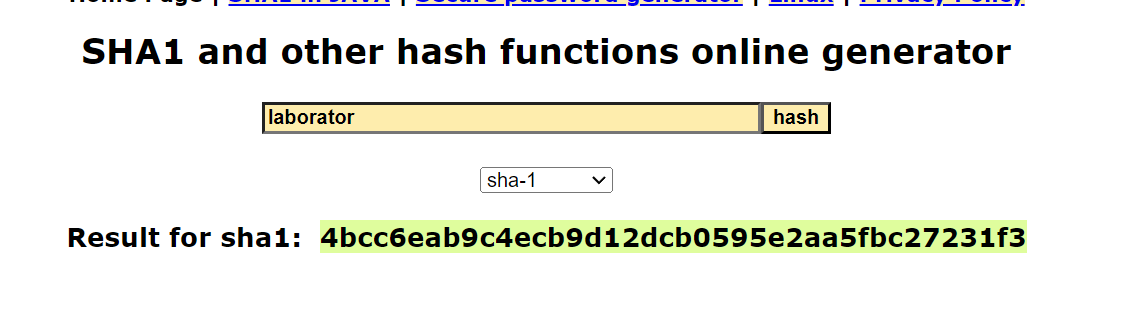
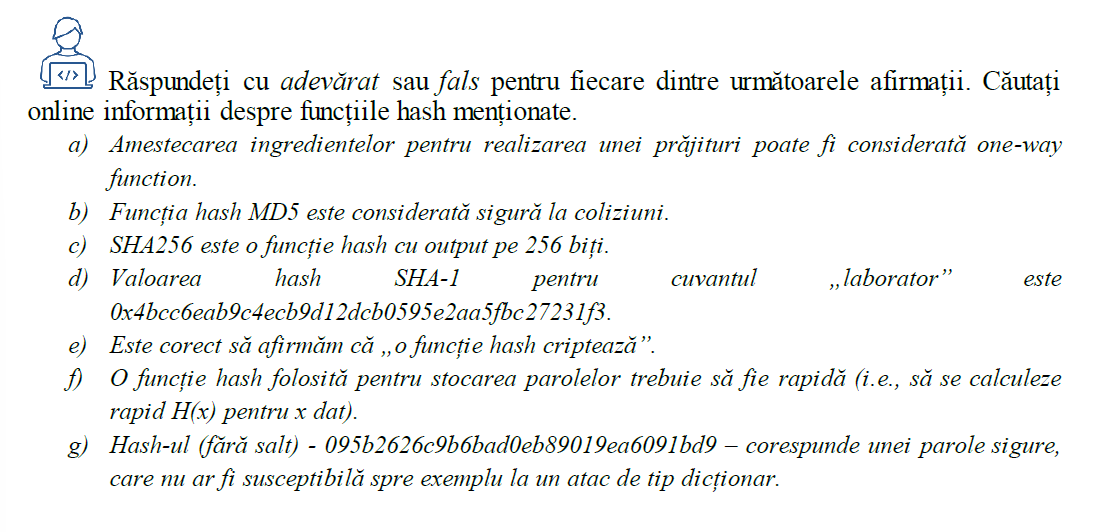
**Laborator 7**

1. Notiuni Introductive



a) Adevarat

b) Fals

c) Adevarat

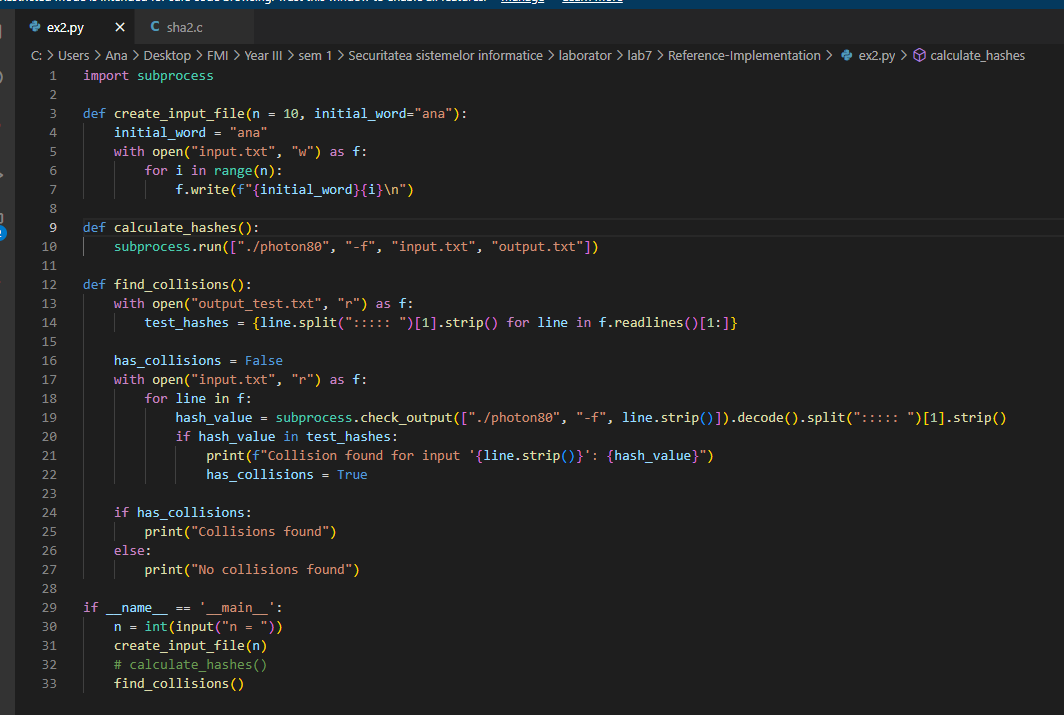
d) Adevarat

e) Fals, doar atribuie o valoare mai scurta si de lungime fixa inputului.

f) Fals

g) Fals

1. Securitatea funcției hash PHOTON-80/20/16



1. Stocarea parolelor

Exemplul 1 –

* Cheia de criptare e hardcodata
* Lipsa de diversificare a cheii (nu foloseste salt)
* Expunerea datelor prin intermediul folosirii unei liste (daca endpointul nu este securizat)
* Ar trebui ca parolele sa fie hash-uite in loc sa fie criptate pentru ca criptarea este un procedeu reversibil
* Nu valideaza datele de intare

Exemplul 2 –

* Nu sunt validate datele de intrare
* Folosirea unei variabile globare pentru stocarea conturilor
* Lipsa persistentei datelor (nu e folosita o baza de date)

Exemplul 3 –

* SHA256 nu este recomandat pentru hash-uirea parolelor pentru ca e rapid si susceptibil la atacuri de forta bruta
* Nu este folosit un salt

Exemplul 4 –

* Pentru SECURITY\_PASSWORD\_SALT ar trebui să fie furnizată o valoare unică pentru salt-ul parolei, ideal generată automat și diferită pentru fiecare utilizator, altfel parolele ar putea fi compromise printr-un rainbow table attack

Exemplul 5 –

* Foloseste MD5 care nu este recomandat pentru hash-uirea parolelor pentru ca este vulnerabil la atacuri rapide de coliziune