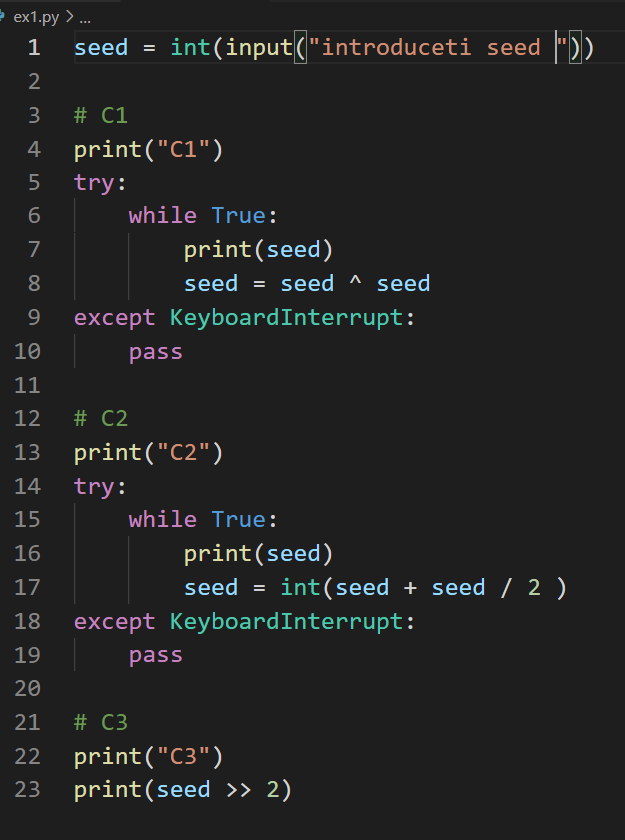
Laborator 6 – Securitatea Sistemelor Informatice

****

**Excercitiul 1**

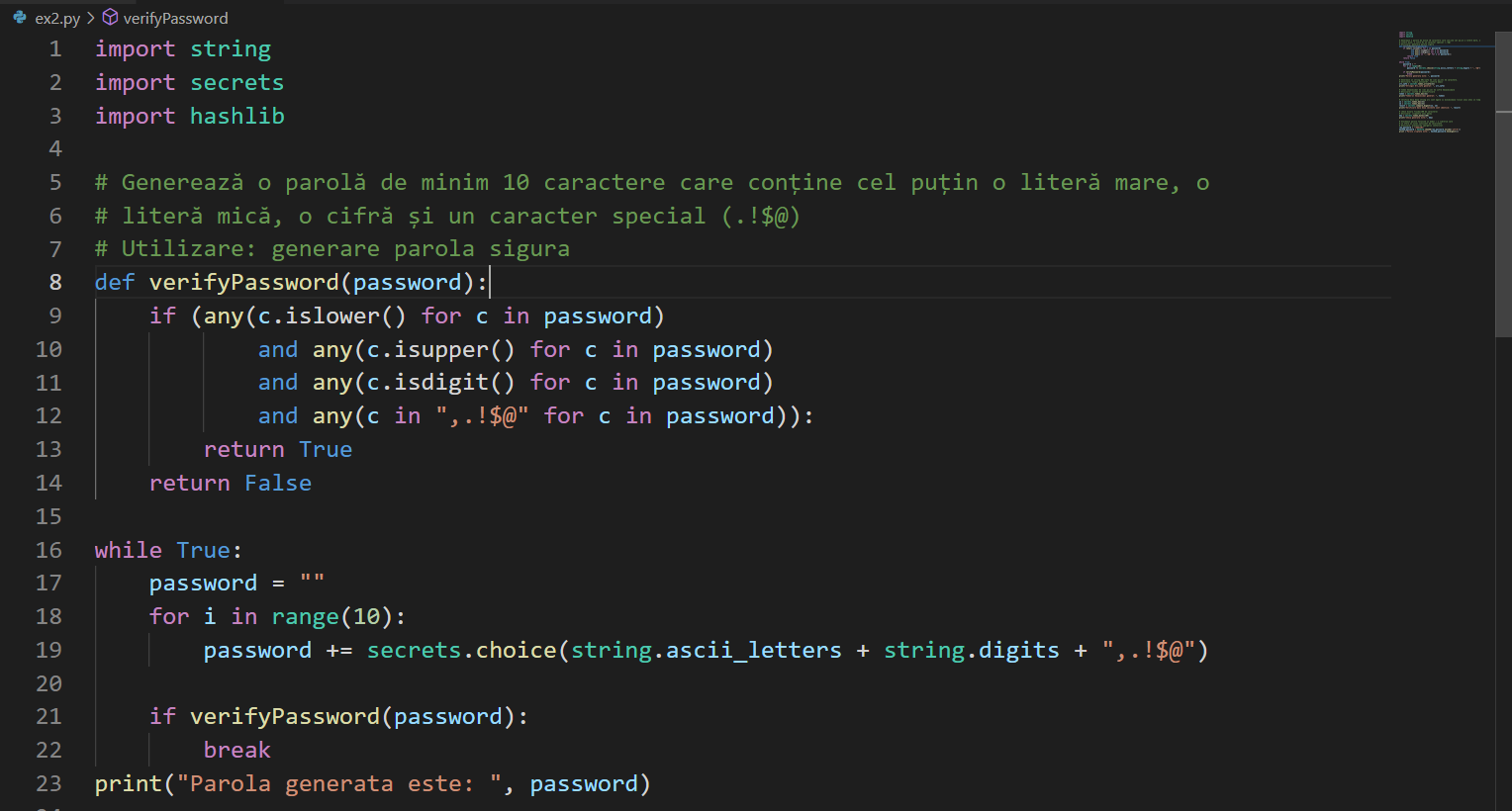
C1 va avea mereu ca rezultat valoarea 0.

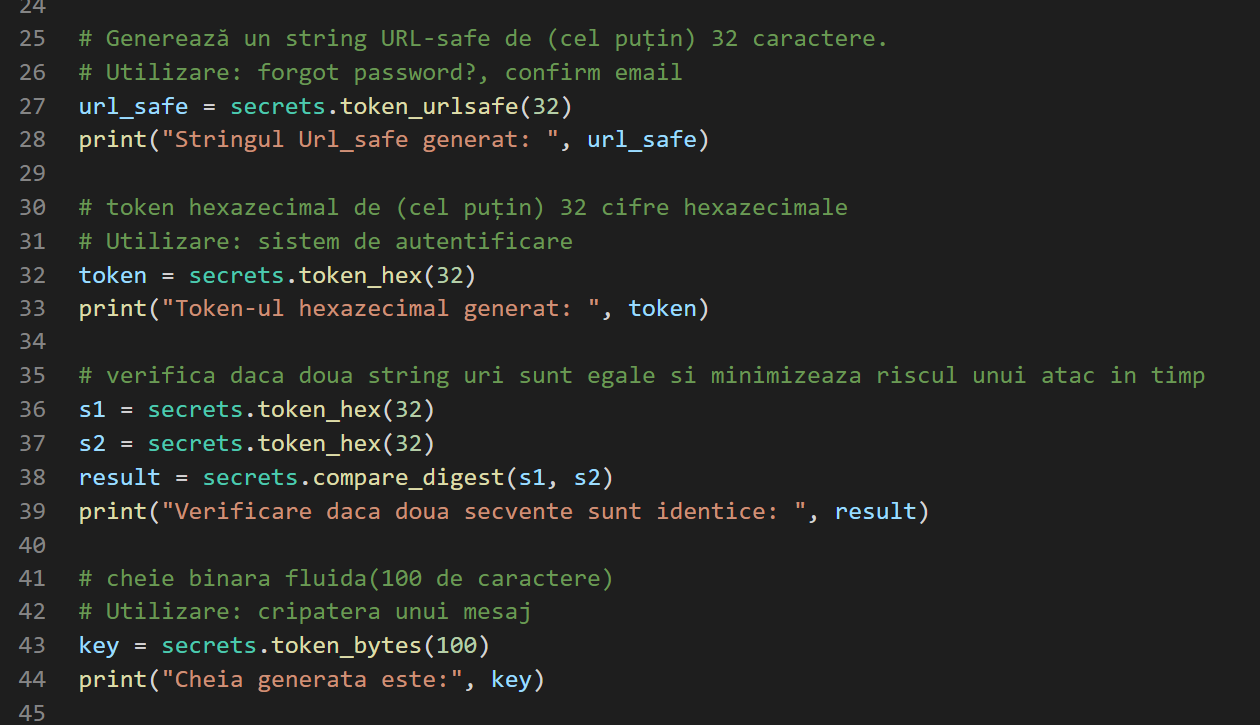
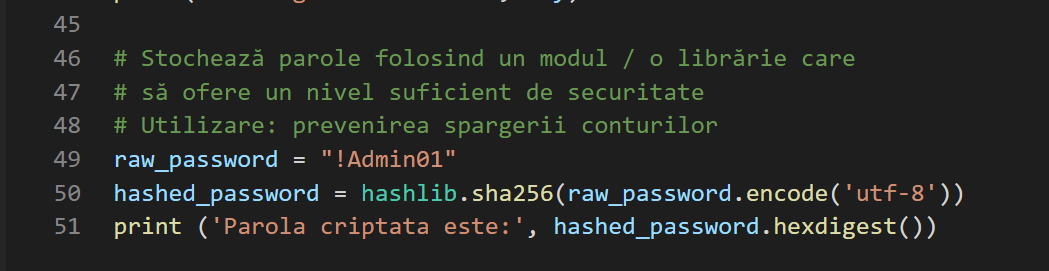
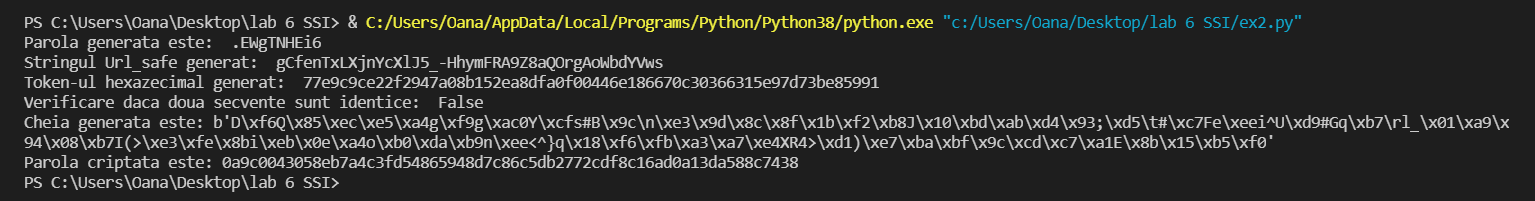
C2 calculeaza starile urmatoare, seed avand mereu valoarea constanta 0.

C3 face shiftare cu 2 biti, iar valoarea returnata va depinde de updatarea starii (0 daca este apdatata si aceeasi valoare in caz contrar).

Concluzie: valoarea va fi mereu constanta, deci nu e generare de numere pseudo-aleatoare, prin urmare secvenetele de cod C1-C3 nu definesc un PRNG.

**Exercitiul 2**





**Exercitiul 3**

* Ce problemă identificați în următoarele secvențe de cod?

Figura 1 (Java): este acelasi seed, deci la fiecare generare a numerelor se vor obtine aceleasi numere in ordine, astfel sistemul va deveni vulnerabil.

Figura 2 (PHP): seed-ul PRNG-ului este id-ul userului, deci la fiecare noua rulare a codului id-ul sesiunii va fi acelasi pentru ca seed-ul ramane acelasi, , astfel sistemul va deveni vulnerabil.

* Care este CWE ID asociat scenariilor de mai sus si problemei pe care acestea o ridică?

Weakness Id= 336

<https://cwe.mitre.org/data/definitions/336.html>

* Ce se întâmplă dacă nu se folosește același seed de fiecare dată, dar spațiul seed-urilor posibile este mic? Puteți găsi un CWE ID corespunzător acestui caz?

spatiul seed-urilor care este mai mic : Small Seed Space in PRNG (CWE-339) => un numar mai mic de posibile valori => creste probabilitatea de a afla seed-ul daca atacatorul foloseste *brute force*

<https://cwe.mitre.org/data/definitions/339.html>

* Căutați atacul identificat la punctul precedent în [5]. Identificați și aici o mențiune la seed?

CAPEC-112

<https://capec.mitre.org/data/definitions/112.html> - brute force

* Găsiți alte utilizări defectuoase ale PRNG explicate în alte CWE-uri. Există CVE-uri corespunzătoare acestora?

<https://cwe.mitre.org/data/definitions/338.html> - se pot folosi generatoare de numere care nu sunt proiectate pt criptografie (putere de procesare mica, surse finite etc).

<https://cwe.mitre.org/data/definitions/335.html> - seed utilizat necorespunzator.

* Căutați înregistrări CVE care se referă la vulnerabilități în legătură cu PRNG. Câte ați identificat ca fiind definite în acest an?

<https://www.cve.org/CVERecord?id=CVE-2021-3678>