Tema 5 – Lab SSI

Ex 1:

Candidate 1

Nu defineste un PRNG deoarece de la al doilea pas incolo toate numerele vor fi 0 deoarece

un numar X xor X va fi intotdeauna 0.

Candidate 2

Formula este una banala, e foarte usor pentru cineva sa o ghiceasca doar uitandu-se prin valori, lipseste cantitatea de aleator; nici asta nu defineste un PRNG

Candidate 3

Acest algoritm face o simpla shiftare pe biti; returneaza un singur rezultat, nu o secventa pseudo-random, deci nu defineste un PRNG

Ex 2:

a)

```
import secrets

mici = "abcdefghijklmnopqrstuvwxyz"
mari = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
numere = "012456789"
speciale = ".!$@"
for i in range(2):
    x = secrets.choice(mici)
    y = secrets.choice(mari)
    z = secrets.choice(numere)
    q = secrets.choice(speciale)
    print(x, end="")
    print(y, end="")
    print(z, end="")
    print(q, end="")

x = secrets.choice(mici)
y = secrets.choice(mari)
```

```
print(x, end="")
print(y, end="")
```

Exemplu : generare sugestii de parole pentru utilizatori

b)

```
import secrets

print(secrets.token_urlsafe((32)))
```

Exemplu: token asignat sesiunii de autentificare a unui utilizator

c)

```
import secrets

print(secrets.token_hex(32))
```

Exemplu: generare key random pentru criptarea unor mesaje

d)

```
import secrets

a=input()
b=input()
print(secrets.compare_digest(a, b))
```

e)

```
import secrets

print(secrets.token_bytes(100))
```

f)

```
import secrets
import hashlib

parola_normala = "@admin!ADMIN@"
```

```
parola_hashuita = hashlib.sha256(parola_normala.encode('utf-8'))
print(parola_hashuita.hexdigest())
```

Ex 3:

a) CWE-336: Same Seed in Pseudo-Random Number Generator (PRNG)

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

b) CWE-339: Small Seed Space in PRNG; se poate folosi un atac de tip brute-force

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

c) CAPEC-112

https://capec.mitre.org/data/definitions/112.html

d) CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)

https://cwe.mitre.org/data/definitions/338.html

e) CVE-2022-39218

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39218