Tudorache Alexandru-Theodor

Grupa 342

Laborator 6

Securitatea Sistemelor Informatice

1.

Candidate 1 -> prin operatia *seed = seed^seed*, dupa prima rulare seed-ul va ajunge la 0, ceea ce il va face inutil.

Candidate 2 -> din cauza operatiei *seed = seed + seed / 2*, seed-ul poate fi usor prezis la fiecare pas, ceea ce il face inutil.

Candidate 3 -> prin shiftarea la dreapta cu 2 biti, dupa un anumit numar de astfel de operatii seed-ul va ajunge sa fie 0, ceea ce il va face inutil.

2.

a) Parola: O functionalitate ca aceasta poate fi folosita intr-o aplicatie informatica pentru a-i sugera utilizatorului o parola puternica, in loc sa existe posibilitatea de a-si alege una slaba.

Un scenariu de utilizare:  
Un utilizator doreste sa-si creeze un cont pe o anumita platforma. Platforma respectiva ii va sugera o parola puternica generata folosind o functionalitate precum cea prezentata.

b) URL-safe String: un astfel de String poate fi folosit pentru generarea unui URL.  
Un scenariu de utilizare:

Generarea id-ului unui user, care va fi accesat, de exemplu, folosind url-ul website.com/users/id.

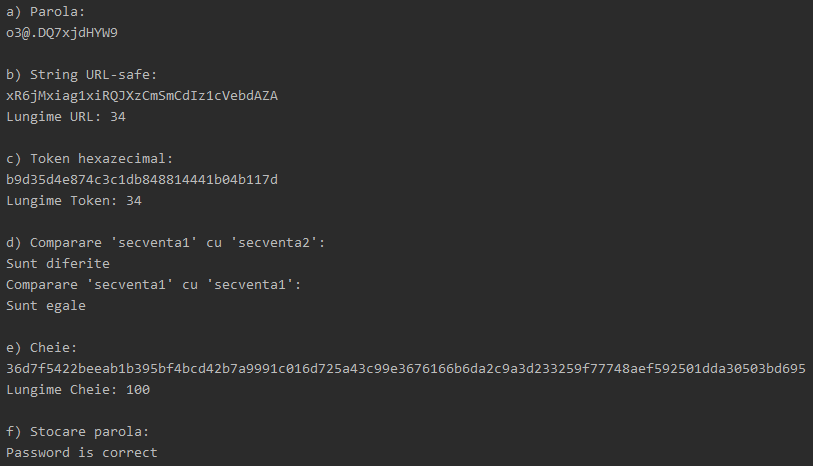
c) Hex Token: un asfel de token poate fi folosit pentru generarea unei chei de criptare.

Un scenariu de utilizare:

Vrem sa criptam un mesaj folosind OTP. Pentru criptarea acestuia vom avea nevoie de o cheie secreta. Aceasta poate fi reprezentata de tokenul nostru.

f) Am folosit biblioteca hashlib pentru a encripta parola ca in cazul in care un inamic patrunde in “baza de date” sa nu poata citi parola fara sa o decripteze.

Posibil output al programului:



3.

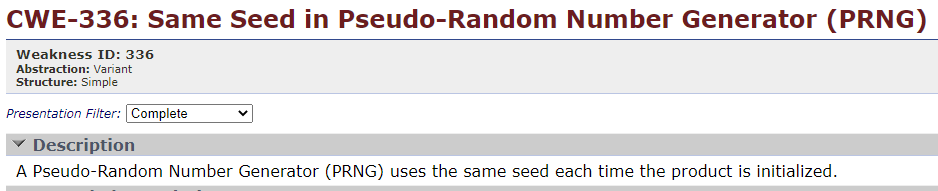
a) Pentru generarea AccountID:

Deoarece se foloseste mereu acelasi seed, la fiecare rulare a codului va fi generat acelasi ID.

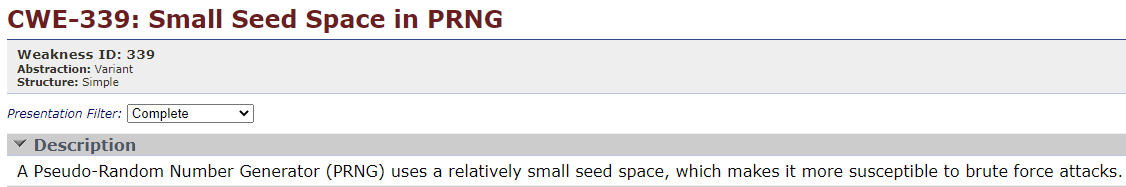
Pentru generarea SessionID:

Deoarece functia srand se foloseste de id-ul user-ului, pentru acelasi user va fi generat mereu acelasi sessionID. (Adica fiecare user va avea un singur session id, diferit de cele ale celorlalti useri)

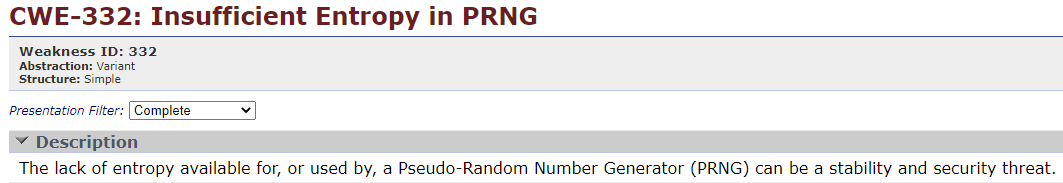
b)



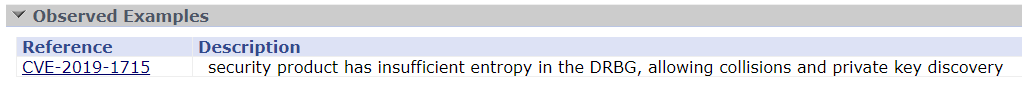
c)

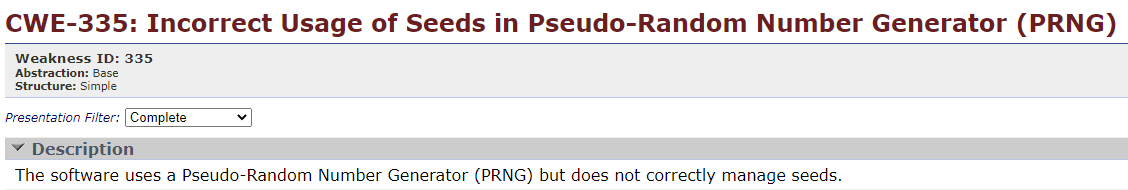


e)

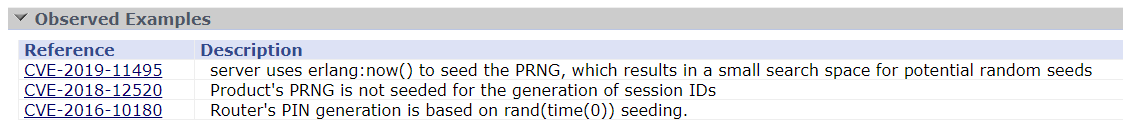


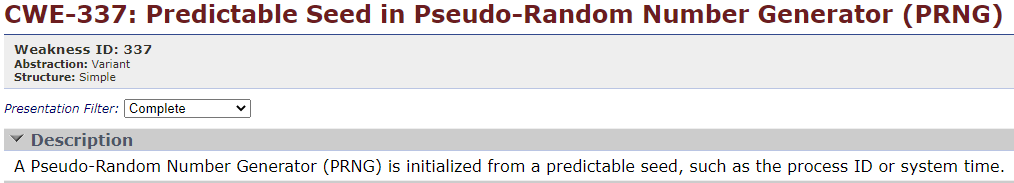
CVE:



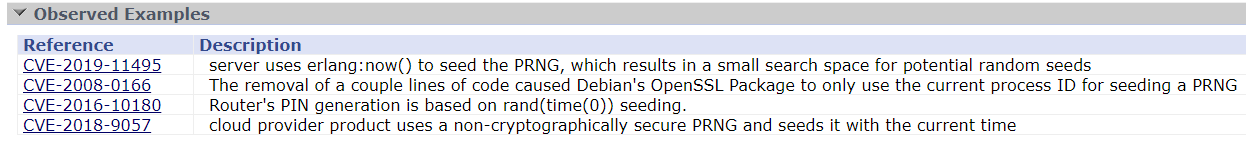


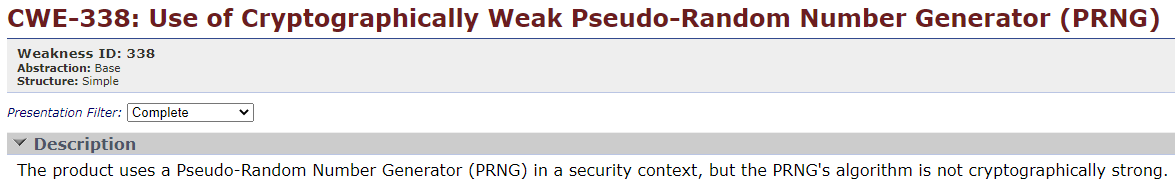
CVE:



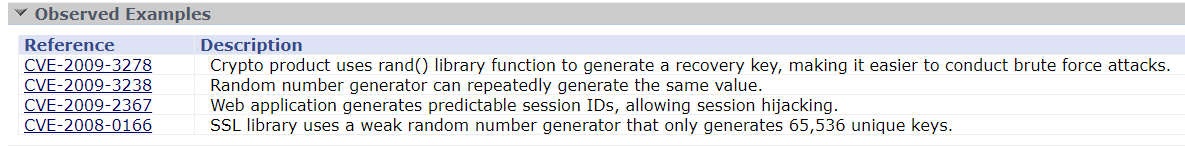


CVE:





CVE:



f)

Am identificat 4 inregistrati CVE din 2021 care au legatura cu PRNG:

