1.
    a. a. Candidate 1: se poate “ghici” pattern ul foarte usor
    b. b. Candidate 2: la fel ca in cazul Candidate 1, pattern-ul este foarte usor de “ghicit”
    c. c. Dupa un timp, seed-ul va ajunge sa aiba valoarea 0 si va ramane la aceasta valoare
2.
    a. Poate ajuta la sugerarea unei parole greu de spart utilizatorului
    b. Poate ajuta la generarea de url unic in cazul in care utilizatorul ar trebui sa faca o plata sau sa isi schimbe parola
    c. Poate ajuta la generarea unui token de acces sau a unei chei de criptare
    d. Pentru a stoca parolele am folosit modulul keyring pentru ca foloseste credentialele sistemului de operare pentru a putea cripta datele pe care trebuie sa le salveze.
3.
    a. Cand se initializeaza PRNG-ul, este folosit acelasi seed de fiecare data.
    b. CWE - 336
    c. Printr-un atac brute force care incearca toate seed-urile posibile din spatiul de valori, este posibila gasirea seed-ului corect. CWE - 339
    d. CAPEC - 112
       If the secret was chosen algorithmically, cryptanalysis can be applied to the algorithm to discover patterns in this algorithm. (This is true even if the secret is not used in cryptography.) Periodicity, the need for seed values, or weaknesses in the generator all can result in a significantly smaller secret space.
    e. CWE - 335: The software uses a Pseudo-Random Number Generator (PRNG) but does not correctly manage seeds. (CVE-2020-10256)
       CWE - 338: The product uses a Pseudo-Random Number Generator (PRNG) in a security context, but the PRNG's algorithm is not cryptographically strong. (CVE-2019-10755)
       CWE - 330: The software uses insufficient random numbers or values in a security context that depends on unpredictable numbers. (CVE-2020-5408)
    f.
        i. Toate CVE urile de mai jos au legatura cu CWE 338
           -> CVE-2021-37553
           -> CVE-2021-29245
           -> CVE-2021-27913
           -> CVE-2021-3990
           -> CVE-2021-3692
           -> CVE-2021-3678
           -> CVE-2021-3538
           -> CVE-2021-3047
           -> CVE-2021-0131