Laborator 5

Pseudo Random Generator

CWE: Common Weakness Enumeration

CAPEC: Common Attack Pattern Enumeration and Classification

CVE: Common Vulnerabilities and Exposures

Exercitiul 3

1.1. **Generarea unui AccountId**

```
import java.util.Random;
class Program {
    public static void main(String[] args) {
        long SEED = 1234567890;
        Random random = new Random(SEED);
        System.out.println(random.nextInt());
    }
}

// Output: -1210225942
```

Problema: este folosit acelasi seed, deci la fiecare rulare se obtine acelasi numar iar astfel sistemul va deveni vulnerabil

1.2. **Generearea unui SessionId**

```
<?php
function generateSessionID($userID) {
  srand($userID);
  $result = rand();
  echo $result;
}

generateSessionID(1234);

// Output: 411284887
```

Problema: deoarece seed-ul este mereu id-ul user-ului, la fiecare rulare sessionId-ul va fi identic pentru acelasi user deci sistemul va fi vulnerabil

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

CWE-336**: Same Seed in Pseudo-Random Number Generator**

- 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?

Creste posibilitatea ca atacatorul sa afle seed-ul printr-un atac de tipul *brute force*

CWE-339**: Small Seed Space in PRNG**

- Căutați atacul identificat la punctul precedent în CAPEC. Identificați și aici o mențiune la seed?

CAPEC-112**: Brute Force.** Spatiul seed-ului trebuie sa fie unul mai restrans pentru a avea probabilitate de succes mai mare

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

CWE-337**: Predictable Seed in Pseudo-Random Number Generator:** A Pseudo-Random Number Generator (PRNG) is initialized from a predictable seed, such as the process ID or system time.

CWE-338**: Use of Cryptographically Weak Pseudo-Random Number Generator:** he product uses a PRNG in a security context, but the PRNG's algorithm is not cryptographically strong.

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

Search Results

There are **67** CVE Records that match your search.

Name	Description
CVE-2022-39218	The JS Compute Runtime for Fastly's Compute@Edge platform provides the environment JavaScript is executed in wher Compute@Edge JavaScript SDK. In versions prior to 0.5.3, the `Math.random` and `crypto.getRandomValues` methoc sufficiently random values. The initial value to seed the PRNG (pseudorandom number generator) is baked-in to the fin WebAssembly module, making the sequence of random values for that specific WebAssembly module predictable. An at use the fixed seed to predict random numbers generated by these functions and bypass cryptographic security controls to disclose sensitive data encrypted by functions that use these generators. The problem has been patched in version 0 known workarounds exist.
CVE-2021-45489	In NetBSD through 9.2, the IPv6 Flow Label generation algorithm employs a weak cryptographic PRNG.
CVE-2021-45484	In NetBSD through 9.2, the IPv6 fragment ID generation algorithm employs a weak cryptographic PRNG.
CVE-2021-43799	Zulip is an open-source team collaboration tool. Zulip Server installs RabbitMQ for internal message passing. In version Server prior to 4.9, the initial installation (until first reboot, or restart of RabbitMQ) does not successfully limit the defau RabbitMQ opens; this includes port 25672, the RabbitMQ distribution port, which is used as a management port. Rabbit "cookie" which protects this port is generated using a weak PRNG, which limits the entropy of the password to at most practicality, the seed for the randomizer is biased, resulting in approximately 20 bits of entropy. If other firewalls (at th network level) do not protect port 25672, a remote attacker can brute-force the 20 bits of entropy in the "cookie" and l arbitrary execution of code as the rabbitmq user. They can also read all data which is sent through RabbitMQ, which inc message traffic sent by users. Version 4.9 contains a patch for this vulnerability. As a workaround, ensure that firewalls access to ports 5672 and 25672 from outside the Zulip server.
CVE-2021-3990	showdoc is vulnerable to Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)
CVE-2021-37553	In JetBrains YouTrack before 2021.2.16363, an insecure PRNG was used.
CVE-2021-3678	showdoc is vulnerable to Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)
CVE-2021-3047	A cryptographically weak pseudo-random number generator (PRNG) is used during authentication to the Palo Alto Netw web interface. This enables an authenticated attacker, with the capability to observe their own authentication secrets ov