Task 18 : 8. Software and Data Integrity Failures

What is Integrity?

When talking about integrity, we refer to the capacity we have to ascertain that a piece of data remains unmodified. Integrity is essential in cybersecurity as we care about maintaining important data free from unwanted or malicious modifications. For example, say you are downloading the latest installer for an application. How can you be sure that while downloading it, it wasn't modified in transit or somehow got damaged by a transmission error?

To overcome this problem, you will often see a **hash** sent alongside the file so that you can prove that the file you downloaded kept its integrity and wasn't modified in transit. A hash or digest is simply a number that results from applying a specific algorithm over a piece of data. When reading about hashing algorithms, you will often read about MD5, SHA1, SHA256 or many others available.

Let's take WinSCP as an example to understand better how we can use hashes to check a file's integrity. If you go to their Sourceforge repository, you'll see that for each file available to download, there are some hashes published along:

```
WinSCP-5.21.5-Setup.exe
  - MD5: 20c5329d7fde522338f037a7fe8a84eb
  - SHA-1: c55a60799cfa24c1aeffcd2ca609776722e84f1b
  - SHA-256: e141e9a1a0094095d5e26077311418a01dac429e68d3ff07a734385eb0172bea
```

These hashes were precalculated by the creators of WinSCP so that you can check the file's integrity after downloading. If we download the WinSCP-5.21.5-Setup.exe file, we can recalculate the hashes and compare them against the ones published in Sourceforge. To calculate the different hashes in Linux, we can use the following commands:

AttackBox

```
user@attackbox$ md5sum WinSCP-5.21.5-Setup.exe
20c5329d7fde522338f037a7fe8a84eb  WinSCP-5.21.5-Setup.exe
```

```
user@attackbox$ sha1sum WinSCP-5.21.5-Setup.exe
c55a60799cfa24c1aeffcd2ca609776722e84f1b  WinSCP-5.21.5-Setup.exe

user@attackbox$ sha256sum WinSCP-5.21.5-Setup.exe
e141e9a1a0094095d5e26077311418a01dac429e68d3ff07a734385eb0172bea
WinSCP-5.21.5-Setup.exe
```

Since we got the same hashes, we can safely conclude that the file we downloaded is an exact copy of the one on the website.

Software and Data Integrity Failures

This vulnerability arises from code or infrastructure that uses software or data without using any kind of integrity checks. Since no integrity verification is being done, an attacker might modify the software or data passed to the application, resulting in unexpected consequences. There are mainly two types of vulnerabilities in this category:

- Software Integrity Failures
- Data Integrity Failures

Answer the questions below :

1. Read the above and continue!
A. No answer needed