Hashbrown

In this tutorial, you will explore cryptographic techniques used in software! Questions 4 and 5 requires you to run the `hashbrown.out` executable provided.

Question 1

- What is the following string, `aHR0cHM6Ly9vbGQua2FsaS5vcmcva2FsaS1pbWFnZXMva2FsaS0yMDIzLjIv`, encoded with?

Hint

- You may use tools like CyberChef to figure out the encoded message.

Question 2

- For this tutorial (and other tutorials too), you are encouraged to use a virtual machine (VM) running Kali Linux. What is the SHA256 sum for the amd64 Kali Linux 2023.2 ISO?

Hint

- Kali Linux offers prebuilt VM images on their website. Like many software, a checksum is provided to verify the integrity of the downloaded software. While only the latest version of Kali Linux is listed on the main website, older versions are available from the URL obtained in Question 1.

Question 3

- Someone has asked you to run a program named `browserLockdown.exe` with a SHA256 hash of `aee20f9188a5c3954623583c6b0e6623ec90d5cd3fdec4e1001646e27664002c`. You are suspicious of this request and decide to investigate more. What is the software trying to masquerade as this program?

Hint

- You may use tools such as VirusTotal to find more information about hashes related to files.

Question 4

- To run the `hashbrown` program, the permissions of the binary must be set to 'execute'. What is the Linux command to do so?

Hint

- When downloading the binary onto the VM for the first time, its permissions are set to 'read' and 'write'.

```
$ ls -la

total 5652
```

```
drwxr-xr-x 1 parrot parrot      18 Oct  6 04:07 .
drwxr-xr-x 1 parrot parrot     200 Oct  6 04:06 ..
-rw-rw-rw- 1 parrot parrot 5784280 Oct  6 04:07 hashbrown
```

Question 5

- What is the vulnerability demonstrated by the `hashbrown` program, where 2 different pieces of data give the same hash output?
- What is the flag obtained from running the `hashbrown` program?

Hint

- The `hashbrown` program requires 2 different files to run.

```
$ ./hashbrown
 ____ ____ ____ ____ ____ ____ ____ ____ ____
||h |||4 |||5 |||h |||b |||r |||0 |||w |||n ||
||__|||__|||__|||__|||__|||__|||__|||__|||__||
|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|

Usage: ./hashbrown <path_to_file_1> <path_to_file_2>
```

- You need to provide files with the specific vulnerability for it to run successfully. Examples of such files can be found online, and you can use them to solve this challenge!

```
$ ./hashbrown file_1.png file_3.jpg
 ____ ____ ____ ____ ____ ____ ____ ____ ____
||h |||4 |||5 |||h |||b |||r |||0 |||w |||n ||
||__|||__|||__|||__|||__|||__|||__|||__|||__||
|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|

Access denied! File hashes are different!
```