# HOW TO SECURELY STORE PASSWORD IN A DATABASE:

When you save a user’s password in a database, you must never use plaintext. That is bad practice and can cause big damage if your database is compromised by hackers. They would have access to the passwords of all your users and considering the fact that most people use the same password everywhere, this would mean the hackers would have access to the ID and passwords of many users in many websites. From there one, it is only a matter of trial and error for the hackers to try different combinations on different website and retrieve sensitive information.

We use a combination of techniques to store passwords in the database and prevent from them from compromised by a motivated attacker. This will be explored in the below section of the report.

## ENCRYPTION:

The first method is to encrypt our passwords, which involves creating a key that will first change the plaintext to a cipher. This key would then have a decryption method to convert the cipher back to a plaintext, in order to recognise the password.

This isn’t the best of choices, as people tend to have simple passwords that you can guess. Once you have found one password, you can write a script to find the encryption key and retrieve all the passwords stored in your database.