


```
var Mdp = "azerty123"
```

CHIFFREMENT


On utilise ici un chiffrement symétrique, ce qui signifie que ce qui a été chiffré peut être déchiffré.

Les algorithmes sont très rapides mais si un pirate connaît l'algorithme utilisé, il peut décoder les mots de passe stockés dans une base de données.

<https://encode-decode.com/blowfish-encrypt-online/>

azerty123  R32QBZLsJmf5okUjqvWlxQ==
AES-128

azerty123  v2LsM9dObAi5
RC4


azerty123  YQ4X0YmapJ3gbxwuJ9etig==
Blowfish


HACHAGE


La propriété d'un hachage est qu'il est "impossible" de retrouver le mot de passe. L'idée est donc de hacher un champ de saisie et vérifier que le résultat correspond à celui stocké en BDD.

Cependant, le hachage donnant toujours le même résultat, on peut utiliser des tables "arc-en-ciel" pour retrouver le mot de passe.

<https://encode-decode.com/md5-generator-online/>

azerty123  882baf28143fb700b388a87ef561a6e5
MD5


azerty123  f3029a66c61b61b41b428963a2fc134154a5383096c776f3b4064733c5463d90
SHA-256


azerty123  d65cf4466a8715103cc475154277e3fb617248500879c204e02f935047e04343
RIPEMD-256

SALAGE

Cette fois, on ajoute d'abord une chaîne au mot de passe, que seul l'administrateur connaît. Idéalement une date de création de compte. Deux utilisateurs utilisant le même mot de passe n'auront ainsi pas le même résultat de hachage.

Si la BDD est compromise, le pirate peut chercher dans les données de l'utilisateur, la donnée utilisée comme sel, puis doit ensuite utiliser les tables "arc-en-ciel".

azerty123-13:14:05  c103363ffcca2605a820de5425a93481
MD5

azerty123-09:27:54  19ceddda25a597559231b97bbb65b3b9
MD5



L'inconvénient d'un hachage, est le risque de collision : deux mots de passe différents peuvent donner le même résultat. C'est une des raisons pour laquelle MD5 n'est désormais pas un bon choix pour une fonction de hachage.