1- Emmagatzemant una contrasenya de manera segura fent un hash de contrasenyes en PHP

a) Documentació:

- https://alexwebdevelop.com/php-password-hashing/ → Tutorial complet sobre com generar hash de contrasenyes xifrades per MySQL amb PHP.
- https://phppasswordhash.com/ => Eina de generació de contrasenyes i breu explicació sobre les funcions per generar hash de contrasenyes xifrades.

b) Primer executa **password.php** => S'introdueix el password **ClotFje23#** per l'usuari amb el **codi = 5** emmagazemada de manera segura utilitzant un **hash** de la contrasenya.

c) A continuació executa **lecturaTaula.php** => Es llegeix la taula **tlcli** de la base de dades **bdcli** i es comprova que per l'usuari amb el **codi = 5** s'ha emmagatzemat el hash de la contrasenya.

d) valida.php → Comprovació de contrasenyes utilitzant hash. En aquest cas, si utilitzem la contrasenya **ClotFje23#** per l'usuari amb **codi = 5** el resultat és correcte però si utilitzem **ClotFje23@** el resultat és incorrecte.

2- Altres mesures mínimes de segureta respecte dels password

a) En un formulari, aquesta informació s'hauria d'escriure de manera que no es pugi veure utilitzant per exemple una entrada de tipus password.

b) Si s'utilitza un formulari de creació de contrasenyes, hem d'assegurar-nos que la contrasenya introduïda segueixi els criteris mínims de 8 caràcters + minúscules + majúscules + caràcters especials. Utilitzant expressions regulars es pot fer que un formulari HTML obligui a utilitzar aquestes mesures de seguretat.

c) Si en compte d'utilitzar un formulari, la contrasenya es crea de manera autòmatica via PHP, hem d'assegurar-nos que el resultat també segueixi aquests criteris. A internet hi ha múltiple llocs a on es pot trobar codi PHP que genera contrasenyes segures.

d) S'ha de treballar amb un servidor de pàgines web o aplicacions que utilitzi **HTTPS**. Amb **HTTP** la informació viatja en una cadena de text que es pot llegir i en canvi amb **HTTPS** utilitza el protocol d'encriptació TLS/SSL que permet assegurar les comuniciacions utilitzant una combinació de encriptació de clau pública (asimètrica) i de clau simètrica.

Exemple:

- Utilitzant HTTP podem llegir un missatge així: **`This is a string of text that is completely readable`**
- En canvi, amb HTTPs seria: **`ITM0IRyiEhVpa6VnKyExMiEgNveroyWBPlgGyfkflYjDaaFf/Kn3bo3OfghBPDWo6AfSHlNtL8N7ITEwIXc1gU5X73xMsJormzzXlwOyrCs+9XCPk63Y+z0=`**

e) S'ha de tenir en compte que és millor enviar la contrasenya via **POST** perquè no es pugi veure el seu valor a la barra d'adreces.