

Projecte PHP 07

- A partir de l'estat anterior del projecte PHP:

A) XIFRAT DE LA CONTRASENYA

Fes que, en el procés de **registre de nous usuaris** de la botiga, la contrasenya es guardi en el fitxer **passwd.txt** de manera xifrada.

Per fer-ho utilitza la funció **password_hash()**, una funció que és compatible amb la que s'utilitzava amb anterioritat: **crypt()**. També es pot utilitzar la funció **md5()** per obtenir el hash, però, en qualsevol cas, es recomana utilitzar sempre la primera.

El resultat obtingut en aplicar **password_hash()** depèn de l'algorisme utilitzat quan es realitza l'operació. De moment, la longitud final del hash no és important, ja que es guardarà en una línia del fitxer **passwd.txt**.

La funció té el següent format:

password_hash (string **\$contrasenya**, integer **\$algorisme** [, array **\$opcions**]) : string

- **\$contrasenya** és la cadena amb la contrasenya de l'usuari.
- **\$algorisme** és un valor que indica quin algorisme utilitzar. Els valors més utilitzats d'entre els disponibles són (indicats en la funció **sense cometes**):
 - 1) **PASSWORD_BCRYPT**: utilitza l'algorisme CRYPT_BLOWFISH.
 - 2) **PASSWORD_ARGON2I**: utilitza l'algorisme Argon 2.
 - 3) **PASSWORD_DEFAULT**: el que s'utilitza si no s'especifica un altre. Pot canviar amb el temps.
- **\$opcions**: són les opcions que es permet aplicar sobre l'algorisme triat.

L'algorisme, cost i salt (cadena base) usats són retornats com a part del hash. Per tant, **tota la informació que és necessària per verificar el hash, està inclosa en ell**.

Per fer la **comprovació de la contrasenya** introduïda per l'usuari en el formulari de **login** (comparant-la amb la que s'ha emmagatzemat en el fitxer de text) s'utilitza la funció **password_verify()**, que té el següent format:

```
password_verify ( string $contrasenya , string $hash ) : bool
```

- **\$contrasenya**: La **contrasenya** que ha introduït l'usuari en el **formulari**.
- **\$hash**: El **hash amb el que es vol comparar** (el que està en el fitxer **passwd.txt**).
- Si coincideixen la funció retorna **true**, si no coincideixen retorna **false**.

Exemple de contrasenyes xifrades en el fitxer de text

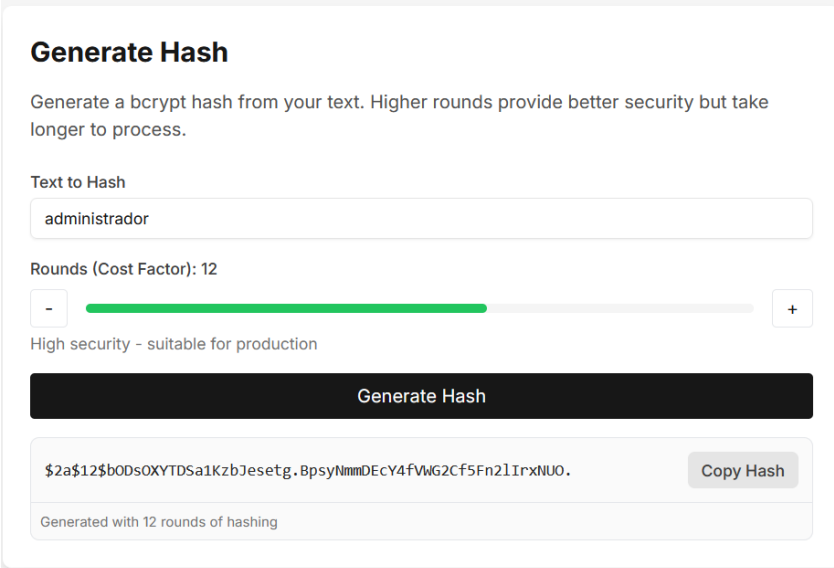
```
admin:admin@dam.com:$2a$12$mIInSMUAE19630qxWxKD9ehiZNpg5CaDsqdGJT4eWin0A0UgDK0ym:
anna:anna@simarro.org:$2y$10$QCpJMrvQbvqJQRZtYqxd/eAEd0A.fXi0Pl67ToDbSh3ScIjzHb0Rq:
raül:raul@simarro.org:$2y$10$VtHg9I1Al59B0ASe3v0YQ0x.0ZF1WqPHuzjExComWicgySU5GQrQu:
joan:joan@simarro.org:$2y$10$UqT8/jrI7juvy.rC5RvY4u540KyagPEdF5n50w0GtX7oj015gQXKq:
sara:sara@simarro.org:$2y$10$UstMLGLZ0GXzrs2jeLLYr.tZHhFCPUZv1i3ykmSoNYXn843ej.370:
robert:robert@simarro.org:$2y$10$6B4N2oDz7LPhd1N0/V7Jj.I2BPz4Fp9kW0FklZVQTJqZM/s8kE6AC:
vicent:vicent@simaro.org:$2y$10$eiIpHD/.L8l/QbzzVy2Ihep7R1/R02oZRZ9JhS7Unl0knCvYyUUG:
```

Si volem generar el hash d'una contrasenya en concret, es pot **codificar manualment** utilitzant webs com [aquesta](#).

- En la secció **Generate Hash**, indiquem:
 - En el quadre **Text to Hash** el **password sense xifrar**.
 - En el quadre inferior establim el **cost o nombre de voltes (podem deixar 12)**.

The screenshot shows a web browser at <https://bcrypt-generator.com>. The page title is 'Bcrypt Generator'. Below the title, it says 'Bcrypt Hash Generator' and 'A simple tool to generate and verify bcrypt hashes. All processing happens in your browser for security.' The main section is 'Generate Hash', which includes the instruction 'Generate a bcrypt hash from your text. Higher rounds provide better security but take longer to process.' There is a text input field labeled 'Text to Hash' with the placeholder 'Enter text to hash'. Below it, 'Rounds (Cost Factor): 12' is shown with a slider and minus/plus buttons. A note says 'High security - suitable for production'. At the bottom is a 'Generate Hash' button.

- Després premem el botó **Generate Hash** i obtindrem el **password xifrat**, que podem introduir directament en el fitxer **passwd.txt**.
- Compte quan es **copia el valor**, també es copien **espais** abans i després de la cadena xifrada.



Generate Hash

Generate a bcrypt hash from your text. Higher rounds provide better security but take longer to process.

Text to Hash

administrador

Rounds (Cost Factor): 12

- +

High security - suitable for production

Generate Hash

\$2a\$12\$b0Ds0XYTDSa1KzbJesetg.BpsyNmmDEcY4fVwG2Cf5Fn2lIrxNU0.

Copy Hash

Generated with 12 rounds of hashing

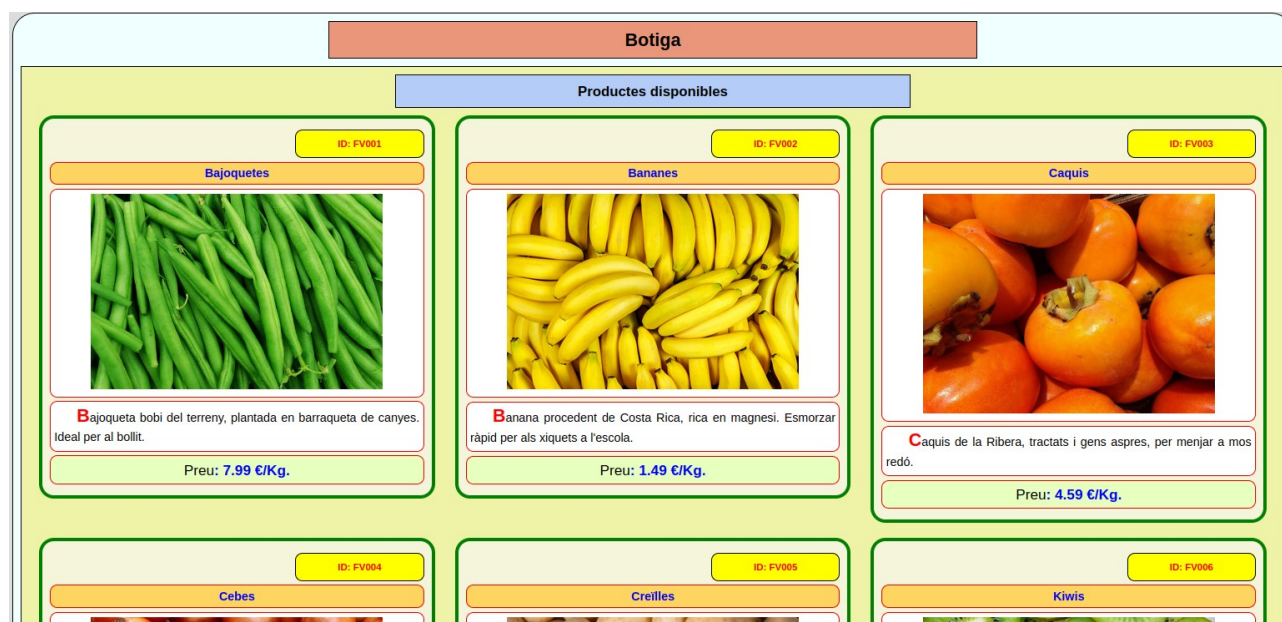
B) PREPARACIÓ DELS PRODUCTES PER AL CARRET DE LA COMPRA

Crea un fitxer nou anomenat **productes.php** en la carpeta **include** que contindrà una llista dels productes que tindrà la botiga i que l'usuari que hi accedisca podrà adquirir més endavant. Com a mínim, cada producte ha de tenir un **identificador únic** (no necessàriament numèric), un **nom**, una **imatge** (només el nom amb l'extensió), un **preu** i una xicoteta **descripció**. Aquests valors estaran en un **array** que conté **arrays associatius** amb la informació.

Les imatges poden ubicar-se una carpeta **productes** dins de la carpeta d'imatges del projecte (inclús en una subcarpeta **botiga**).

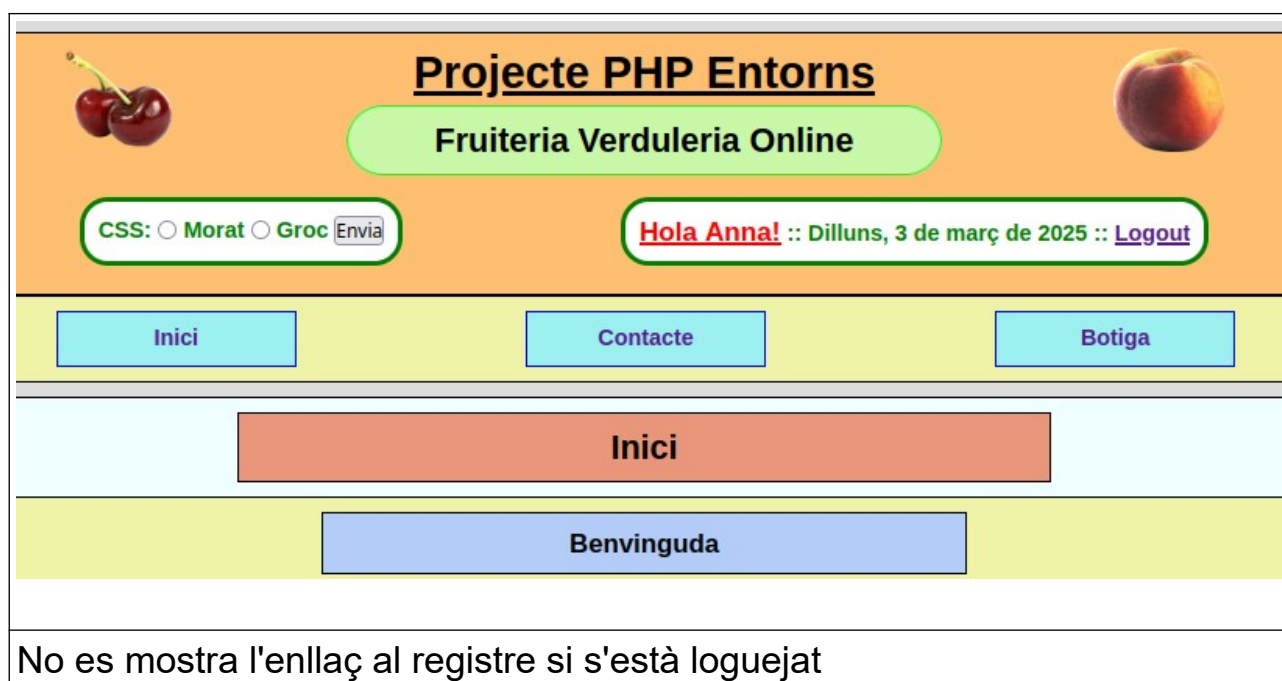
En el fitxer **botiga.partial.php**, que fins ara estava 'en construcció', mostra la informació de tots els productes existents en l'array. Simplement es cridarà a una funció **mostraProductes(\$rutaFitxer)**, a la que se li passa la ruta al fitxer dels productes i que estarà implementada en el fitxer **funcions.php**.

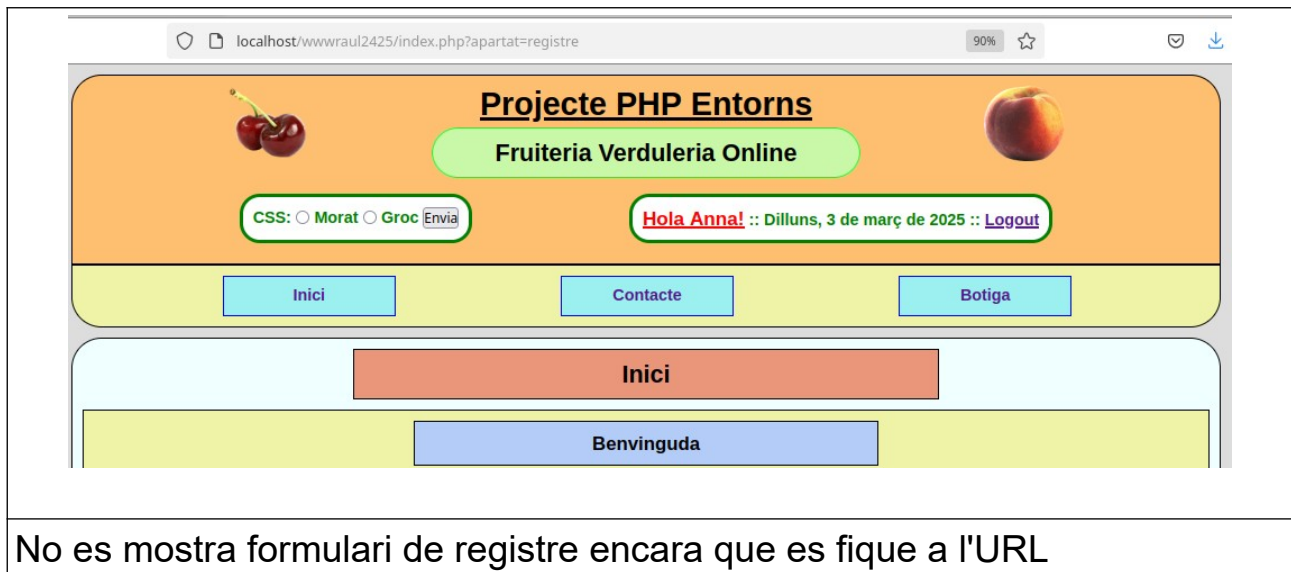
Fes que l'**accés a l'array de cada producte siga a través d'un index** que es corresponga amb l'**identificador únic** del producte. Fes que hi haja almenys 6 productes entre els que triar.



C) ENLLAÇ REGISTRE

Modifca el fitxer [menu.partial.php](#) per fer que quan l'usuari s'haja **autenticat correctament**, no aparega l'enllaç al registre del menú. Fes també en el fitxer [principal.partial.php](#) que encara que s'indique l'apartat en l'URL, si s'està autenticat, no aparega el formulari de registre i mostre el contingut de l'apartat d'inici.





No es mostra formulari de registre encara que es fique a l'URL

D) GIT

En acabar de realitzar les tasques d'aquest enunciat, crea un commit del que has fet i puja-ho al teu repositori de Github. Pots afegir-li també una etiqueta.

Les instruccions a executar són les següents:

```
$ git add --all
$ git commit -m "Enunciat Projecte PHP 07 El teu nom"
$ git push origin master
$ git log --oneline
$ git tag v7.0
$ git push --tags origin master
$ git status
$ git log --oneline
```

Obtenim al final, si tot és correcte:

```
professor@professor:/var/www/html/wwwraul2425$ git log --oneline
c11b020 (HEAD -> master, tag: v7.0, origin/master) Enunciat Projecte PHP07 Raül Valls
8ffec56 (tag: v6.2) eliminada cookie d'usuari eliminat per admin
fbcc72c (tag: v6.1) modificats estils i placeholders
c7b2fd7 (tag: v6.0) Enunciat Projecte PHP 06 Raül Valls
6c10a97 (tag: v5.1) Correcció logout diferent index.php
b3e0a1b (tag: v5.0) Enunciat Projecte PHP 05 Raül Valls
010482a (tag: v4.0) Enunciat Projecte PHP 04 Raül Valls
fb03358 (tag: v3.0) Enunciat Projecte PHP 03 Raül Valls
5b20c70 (tag: v2.1) Prova canvi git
b54787f (tag: v2.0) Enunciat Projecte PHP 02 Raül Valls
a592ef0 (tag: v1.2) Problema amb Sense Valor Registre
91e58ba (tag: v1.1) Afegit favicon
b20c303 (tag: v1.0) Commit Inicial Projecte PHP Raül Valls
```

```
git log --oneline
```