Pràctica 5.3 - Sistema d’autenticació amb Sessions, Galetes i Base de Dades

Objectiu

Crear un sistema d'autenticació d'usuaris que combini sessions (per mantenir el login actiu), galetes (per "recordar-me") i PDO (per validar credencials i gestionar usuaris a la base de dades).

Descripció

Desenvolupeu una aplicació web amb autenticació que permeti:

1. Registre de nous usuaris a la base de dades
2. *Login* amb validació de credencials des de la BD
3. Opció "Recordar-me" que usi galetes per mantenir el login entre sessions
4. Pàgina privada accessible només per usuaris autenticats (sessions)
5. *Logout* que netegi sessions i galetes
6. Registre d'activitat dels usuaris a la base de dades

Requeriments Tècnics

Base de Dades

Crea una base de dades anomenada `autenticacio` amb les següents taules:

```
CREATE DATABASE IF NOT EXISTS autenticacio CHARACTER SET utf8mb4 COLLATE
utf8mb4_unicode_ci;

USE autenticacio;

CREATE TABLE usuaris (
    id INT AUTO_INCREMENT PRIMARY KEY,
    nom_usuari VARCHAR(50) NOT NULL UNIQUE,
    contrasenya VARCHAR(255) NOT NULL,
    nom_complet VARCHAR(100) NOT NULL,
    email VARCHAR(100) NOT NULL UNIQUE,
    data_registre DATETIME DEFAULT CURRENT_TIMESTAMP
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_unicode_ci;

CREATE TABLE activitat (
    id INT AUTO_INCREMENT PRIMARY KEY,
    usuari_id INT NOT NULL,
    accio VARCHAR(50) NOT NULL,
    data_hora DATETIME DEFAULT CURRENT_TIMESTAMP,
    ip_client VARCHAR(45),
    FOREIGN KEY (usuari_id) REFERENCES usuaris(id) ON DELETE CASCADE
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_unicode_ci;

-- Inserir usuari de prova (contrasenya: 1234)
INSERT INTO usuaris (nom_usuari, contrasenya, nom_complet, email) VALUES
('admin', '$2y$10$92IXUNpkjO0rOQ5byMi.Ye4oKoEa3Ro9llC/.og/at2.uheWG/igi',
'Administrador', 'admin@example.com'),
```

```
('joan', '$2y$10$92IXUNpkjO0rOQ5byMi.Ye4oKoEa3Ro9llC/.og/at2.uheWG/igi', 'Joan Garcia', 'joan@example.com');
```

Nota: Les contrasenyes estan xifrades amb `password_hash()`. La contrasenya de prova és `1234` per ambdós usuaris.

Estructura de l'Aplicació

Pàgines necessàries:

1. **index.php** - Pàgina d'inici (pública)
2. **registre.php** - Formulari de registre de nous usuaris
3. **login.php** - Formulari de login
4. **privada.php** - Pàgina accessible només per usuaris autenticats
5. **logout.php** - Tancar sessió
6. **config.php** - Configuració de connexió PDO (opcional)

Funcionalitats Requerides

1. Registre d'Usuaris (registre.php)

- Formulari amb: nom d'usuari, contrasenya, nom complet, email
- Valideu que el nom d'usuari i email no existeixin ja
- Xifra contrasenya amb `password_hash()`
- Inseriu nou usuari a la BD amb PDO
- Registreu acció "registre" a la taula activitat
- Redirigiu a *login* després de registre exitós

2. Login (login.php)

Formulari:

- Camp: nom d'usuari
- Camp: contrasenya
- Casella de selecció (*checkbox*): "Recordar-me" (opcional)
- Botó: Entra

Procés de *login*:

1. Valideu credencials amb PDO i `password_verify()`
2. Si correcte:
    - Creeu sessió: deseu ID, nom d'usuari i nom complet
    - Si "Recordar-me" és activat: creeu galetes que caduquin en 30 dies
    - Registreu acció "login" a la taula activitat
    - Redirigiu a pàgina privada
3. Si incorrecte:
    - Mostreu error
    - Manteniu formulari

3. Auto-login amb Galetes

- A totes les pàgines, comproveu si existeixen galetes de "recordar-me"
- Si existeixen i no hi ha sessió activa:
    - Valideu galetes amb la BD
    - Creeu sessió automàticament
    - Registreu acció "auto-login"

4. Pàgina Privada (privada.php)

- Comproveu autenticació (sessió o galetes vàlides)
- Si no autenticat: redirigiu a login
- Mostreu:
    - Nom complet de l'usuari
    - Data i hora de la darrera autenticació (últim *login* de la taula activitat)
    - Historial de les últimes 10 accions de l'usuari
    - Enllaç per tancar sessió

5. Logout (logout.php)

- Esborreu totes les variables de sessió
- Destruïu sessió
- Elimineu galetes de "recordar-me"
- Registreu acció "*logout*" abans de destruir sessió
- Redirigiu a pàgina d'inici

Especificacions Tècniques

Sessions

Estructura de la sessió:

```
$_SESSION['usuari'] = array(
    'id' => 1,
    'nom_usuari' => 'joan',
    'nom_complet' => 'Joan Garcia',
    'autenticat' => true
);
```

Galetes "Recordar-me"

```
// Creeu galetes (caducitat: 30 dies)
setcookie('recordar_id', $usuari_id, time() + (30 * 24 * 60 * 60), '/');
setcookie('recordar_token', $token, time() + (30 * 24 * 60 * 60), '/');
```

Important: No deseu la contrasenya a les galetes. Empreu un *token* únic generat.

Connexió PDO

```
$opcions = array(
    PDO::ATTR_ERRMODE => PDO::ERRMODE_EXCEPTION,
    PDO::ATTR_DEFAULT_FETCH_MODE => PDO::FETCH_ASSOC,
    PDO::MYSQL_ATTR_INIT_COMMAND => "SET NAMES utf8mb4"
);
```

```
try {
    $pdo = new PDO('mysql:host=localhost;dbname=autenticacio', 'usuari',
'contrasenya', $opcions);
} catch (PDOException $e) {
    die("Error de connexió: " . $e->getMessage());
}
```

Seguretat

- **Contrasenyes:** Empreu `password_hash()` i `password_verify()`
- **SQL Injection:** Empreu *prepared statements* SEMPRE
- **XSS:** Escapeu sortides amb `htmlspecialchars()`
- **Session Fixation:** Regenereu ID després de *login* amb `session_regenerate_id(true)`
- **CSRF:** Valideu l'origen de les sol·licituds (opcional)

Exemple de Funcionament

Escenari 1: Registre i autenticació

1. **Usuari es registra:**

   ```
   - Emplena formulari: maria / 1234 / Maria Pérez / maria@example.com
   - INSERT INTO usuaris amb contrasenya encriptada
   - INSERT INTO activitat: acció='registre'
   - Redirigir a login.php
   ```

2. **Usuari fa *login* amb "Recordar-me":**

   ```
   - Validar credencials: SELECT + password_verify()
   - Crear sessió: $_SESSION['usuari']
   - Crear galetes: recordar_id, recordar_token (30 dies)
   - INSERT INTO activitat: acció='login'
   - Redirigir a privada.php
   ```

3. **Mostrar pàgina privada:**

   ```
   - Comproveu sessió activa
   - SELECT últim login de la taula activitat
   - Mostreu: "Benvinguda Maria Pérez"
   - Mostreu: "Darrer accés: 2025-12-07 14:30:25"
   ```

Escenari 2: Auto-login amb Galetes

1. **Usuari tanca navegador i torna al cap d'uns dies:**

   ```
   - Sessió destruïda (navegador tancat)- Galetes encara existeixen-
   Comprovar galetes: isset($_COOKIE['recordar_id'])- SELECT usuari amb id de
   la galeta- Si vàlid: crear sessió automàticament- INSERT INTO activitat:
   acció='auto-login'- Accedir a privada.php directament
   ```

Escenari 3: Logout

1. **Usuari tanca sessió:**

```
- INSERT INTO activitat: acció='logout'- $_SESSION = array()-
session_destroy()- setcookie('recordar_id', '', time() - 3600)-
setcookie('recordar_token', '', time() - 3600)- Redirigir a index.php
```

Criteris d'Avaluació

1. **Sessions (30%):**
    - Gestió correcta de sessions
    - Protecció de pàgines privades
    - Regeneració d'ID després de login
    - Destrucció completa en logout
2. **Galetes (30%):**
    - Implementació de "Recordar-me"
    - Caducitat correcta (30 dies)
    - Validació de galetes
    - Esborrament en *logout*
3. **Base de Dades - PDO (30%):**
    - Registre d'usuaris
    - Validació de credencials
    - Registre d'activitat
    - *Prepared statements*
    - Gestió d'errors
4. **Seguretat (10%):**
    - Xifratge de contrasenyes
    - Validació d'entrada
    - Escapa sortides
    - Protecció contra SQL injection

Millores Opcionals

1. Afegiu verificació del correu electrònic en registre
2. Implementeu la recuperació de la contrasenya
3. Mostreu estadístiques d'ús (total d’autenticacions, temps de sessió)
4. Afegiu nivells d'usuari (admin, usuari normal)
5. Implementeu límit d'intents d’autenticació
6. Afegiu autenticació de dos factors (2FA) bàsica
7. Permeteu editar perfil d'usuari
8. Mostreu dispositius/IPs des d'on s'ha fet l’autenticació

Funcions Auxiliars Recomanades

```
// Comproveu si l'usuari és autenticat
function esta_autenticat() {
    return isset($_SESSION['usuari']) && $_SESSION['usuari']['autenticat'] ===
true;
}

// Protegiu pàgina
function requerir_autenticacio() {
    if (!esta_autenticat()) {
        header('Location: login.php');
        exit;
    }
}

// Registreu activitat
function registrar_activitat($pdo, $usuari_id, $accio) {
    $ip = $_SERVER['REMOTE_ADDR'];
    $stmt = $pdo->prepare("INSERT INTO activitat (usuari_id, accio, ip_client)
VALUES (?, ?, ?)");
    $stmt->execute(array($usuari_id, $accio, $ip));
}

// Xifreu contrasenya
function encriptar_contrasenya($contrasenya) {
    return password_hash($contrasenya, PASSWORD_DEFAULT);
}

// Verifiqueu contrasenya
function verificar_contrasenya($contrasenya, $hash) {
    return password_verify($contrasenya, $hash);
}
```

Notes Importants

- Empreu programació **procedimental** (no POO)
- Compatible amb **PHP 7.0+**
- **MAI** emmagatzemeu contrasenyes en text pla
- Empreu `password_hash()` i `password_verify()` per contrasenyes
- Les galetes de "recordar-me" NO han de contenir contrasenyes
- Regenereu ID de sessió després de login
- Valideu SEMPRE les dades d'entrada
- Empreu *prepared statements* per totes les consultes SQL
- Escapeu sortides amb `htmlspecialchars()`

Lliurament

Lliureu a la carpeta compartida:

1. Tots els fitxers PHP necessaris
2. Fitxer SQL amb creació de BD, taules i dades de prova
3. Captures de pantalla de:
    - Pàgina de registre
    - Pàgina d’autenticació
    - Pàgina privada amb historial
    - Funcionament de "Recordar-me"
4. Breu document explicant l'estructura i flux de l'aplicació