

Créer un système d'inscription & connexion en PHP / MySQL

Version NON SÉCURISÉE

« Cette version DOIT uniquement être utilisée à des fins pédagogiques, jamais mise en ligne, car elle contient volontairement des failles graves. »

1. Objectif

Créer un système minimal :

- Formulaire d'inscription
- Enregistrement en base de données
- Formulaire de connexion
- Vérification du compte
- Système de session simple
- Déconnexion

Structure du projet

```
/A_projet_auth/  
  A_index.php  
  A_register.php  
  A_login.php  
  A_logout.php  
  A_config.php
```

2. Base de données

Nom de la base : **cours_auth**

Table **register** :

```
CREATE DATABASE cours_auth CHARACTER SET utf8mb4 COLLATE  
utf8mb4_unicode_ci;  
  
USE cours_auth;  
  
CREATE TABLE register (  
  id INT AUTO_INCREMENT PRIMARY KEY,  
  nom VARCHAR(50),  
  prenom VARCHAR(50),  
  mail VARCHAR(100),
```

```
    mdp VARCHAR(255)
);
```

3. Fichier de configuration MySQL — A_config.php

```
<?php
$connection = mysqli_connect("localhost", "root", "", "cours_auth");

if (!$connection) {
    die("Erreur : " . mysqli_connect_error());
}

// Afficher les erreurs SQL
mysqli_report(MYSQLI_REPORT_ERROR | MYSQLI_REPORT_STRICT);
?>
```

4. Page d'inscription : A_register.php

Formulaire (HTML)

Page simple qui envoie vers elle-même :

```
<?php
require('A_config.php');
session_start();

$message = "";

if (isset($_POST['submit'])) {

    // Entrées non filtrées
    $nom      = $_POST['nom'] ?? "";
    $prenom  = $_POST['prenom'] ?? "";
    $mail     = $_POST['mail'] ?? "";
    $mdp      = $_POST['mdp'] ?? "";

    // Requête non sécurisée (concaténation)
    $sql_check = "SELECT * FROM register WHERE mail='" . $mail . "' AND
mdp='" . $mdp . "'";

    // Exécution simple (pas de multi_query)
    $result = mysqli_query($connection, $sql_check);

    if (mysqli_num_rows($result) > 0) {
        $message = "Un compte existe déjà.";
    } else {
        // Insertion non sécurisée
```

```

        $sql_insert = "INSERT INTO register(nom, prenom, mail, mdp)
                        VALUES('" . $nom . "','" . $prenom . "','" . $mail
        . "','" . $mdp . "')";
        mysqli_query($connection, $sql_insert);

        header("Location: A_login.php");
        exit;
    }
}
?>
<!DOCTYPE html>
<html>
<head><meta charset="UTF-8"><title>Inscription (non sécurisée)</title>
</head>
<body>

<h1>Inscription (code vulnérable pour démonstration)</h1>

<?php if (!empty($message)) echo "<p style='color:red'>$message</p>"; ?>

<form method="post">
    <input type="text" name="nom" placeholder="Nom"><br><br>
    <input type="text" name="prenom" placeholder="Prénom"><br><br>
    <input type="text" name="mail" placeholder="Email"><br><br>
    <input type="text" name="mdp" placeholder="Mot de passe"><br><br>

    <input type="submit" name="submit" value="Créer le compte">
</form>

<p>Déjà un compte ? <a href="A_login.php">Connexion</a></p>

</body>
</html>

```

5. Page de connexion : A_login.php

```

<?php
require('A_config.php');
session_start();

$message = "";

if (isset($_POST['submit'])) {

    $mail = $_POST['mail'] ?? "";
    $mdp = $_POST['mdp'] ?? "";

    // Requête concaténée
    $sql_login = "SELECT * FROM register WHERE mail='$mail' AND
mdp='$mdp'";

```

```

$result = mysqli_query($connection, $sql_login);

// Accepte plusieurs résultats
if (mysqli_num_rows($result) > 0) {
    $row = mysqli_fetch_assoc($result);

    $_SESSION['user'] = $row['prenom'] ?? "Inconnu";

    header("Location: A_index.php");
    exit;
} else {
    $message = "Identifiants incorrects (démonstration : absence de
protection).";
}
}
?>
<!DOCTYPE html>
<html>
<head><meta charset="UTF-8"><title>Connexion (non sécurisée)</title>
</head>
<body>

<h1>Connexion</h1>

<?php if (!empty($message)) echo "<p style='color:red'>$message</p>"; ?>

<form method="post">
    <input type="text" name="mail" placeholder="Email"><br><br>
    <input type="text" name="mdp" placeholder="Mot de passe"><br><br>
    <input type="submit" name="submit" value="Connexion">
</form>

<p>Pas de compte ? <a href="A_register.php">Créer un compte</a></p>

</body>
</html>

```

6. Page d'accueil (après connexion) : A_index.php

```

<?php
session_start();
?>
<!DOCTYPE html>
<html>
<head><meta charset="UTF-8"><title>Accueil</title></head>
<body>

<h1>Accueil – Version NON sécurisée</h1>

```

```
<?php if (!isset($_SESSION['user'])): ?>

    <p>Vous n'êtes pas connecté.</p>
    <a href="A_login.php">Connexion</a> |
    <a href="A_register.php">Inscription</a>

<?php else: ?>

    <p>Bienvenue, <strong><?php echo $_SESSION['user']; ?></strong> !</p>
    <a href="A_logout.php">Déconnexion</a>

<?php endif; ?>

</body>
</html>
```

7. Déconnexion : A_logout.php

```
<?php
session_start();
session_destroy();
header("Location: A_index.php");
exit;
?>
```

8. Schéma de fonctionnement

```
[Formulaire HTML]
    ↓
[PHP : récupère $_POST]
    ↓
[PHP -> SQL INSERT or SELECT]
    ↓
[Connexion réussie ?]
    ├── Oui -> $_SESSION['user'] -> A_index.php
    └── Non -> message d'erreur
```

9. Remarque : Ce code est volontairement vulnérable

- Mot de passe en clair
- SQL injection possible
- Vérification mail+mdp incorrecte
- Pas de prepared statements
- Pas de filtrage des entrées

Cette version sert uniquement à comprendre la logique.
