
Livrable Semaine 49

Implémentation

Authentification-session/cookie

pour Simul8

2024-2025

Sidney Richards, Yassine Laghdas, Loïc Phrakousonh, Joan Casas, Thomas Aussenac
G2B-11

Sommaire :

I - Implémentation Inscription :	3
II - Implémentation Connexion avec Session/Cookie:	5
III - Demonstration :	8

I - Implémentation Inscription :

Voici le code de [inscription.php](#) qui est le formulaire d'inscription d'un compte au site :

```
4 <meta charset="utf-8" />
5 <title>Formulaire d'inscription</title>
6 <link rel="stylesheet" href="style.css">
7 </head>
8 <body>
9 <div class="register-container">
10 <div class="register-box">
11 <h2>Créer un compte</h2>
12 <form action="TraitInscription.php" method="post">
13 <div class="register-group">
14 <label for="first-name">Prénom</label>
15 <input type="text" id="first-name" name="prenom" required>
16 </div>
17 <div class="register-group">
18 <label for="last-name">Nom</label>
19 <input type="text" id="last-name" name="nom" required>
20 </div>
21 <div class="register-group">
22 <label for="username">Identifiant</label>
23 <input type="text" id="username" name="login" required>
24 </div>
25 <div class="register-group">
26 <label for="email">Adresse Email</label>
27 <input type="email" id="email" name="email" required>
28 </div>
29 <div class="register-group">
30 <label for="phone">N° de téléphone</label>
31 <input type="text" id="phone" name="numero" required>
32 </div>
33 <div class="register-group">
34 <label for="password">Mot de passe</label>
35 <input type="password" id="password" name="mdp" required>
36 </div>
37 <div>
38 <label><button type="submit" name="valider" value="valide" class="btn-register">S'inscrire</button></label>
39 </div>
40 </form>
41 </div>
42 </div>
43 </body>
```

Une fois que nous validons l'inscription nous sommes redirigé vers la page [TraitInscription.php](#) pour traiter l'inscription voici son code :

```

R?php
include('connect.inc.php');

if(isset($_POST["valider"]) && isset($_POST["login"]) && isset($_POST["nom"]) && isset($_POST["prenom"]) && isset($_POST["email"]) && isset($_POST["numero"]) && isset($_POST["mdp"])){
    $login=htmlspecialchars($_POST["login"]);
    $nom=htmlspecialchars($_POST["nom"]);
    $prenom=htmlspecialchars($_POST["prenom"]);
    $email=htmlspecialchars($_POST["email"]);
    $numero=htmlspecialchars($_POST["numero"]);
    $mdp=htmlspecialchars($_POST["mdp"]);

    $motifEmail = '#^[a-zA-Z0-9.-]@[a-zA-Z0-9.-]{2,}.[a-zA-Z]{2,4}$#';
    if(!preg_match(pattern: $motifEmail, subject: $email)){
        header(header: "Location: inscription.php?msgErreur=Veuillez entrée un email valide (exemple@gmail.com)");
    }

    $motifNumero = '#^[01-9]{4}$#';
    if(!preg_match(pattern: $motifNumero, subject: $numero)){
        header(header: "Location: inscription.php?msgErreur=Veuillez entrée un numéro valide ".$numero);
    }

    $testEmail=$conn->prepare("SELECT * FROM Comptes WHERE email= :mail");
    $testEmail->execute(['mail'=>$email]);

    if ($testEmail->rowCount() >= 1) {
        header(header: "Location: inscription.php?msgErreur=Cet email est déjà utilisé");
    }

    $testId=$conn->prepare("SELECT * FROM Comptes WHERE identifiant= :id");
    $testId->execute(['id'=>$login]);

    if ($testId->rowCount() >= 1) {
        header(header: "Location: inscription.php?msgErreur=Cet identifiant est déjà utilisé");
    }

    $mdp=password_hash(password: $mdp, algo: PASSWORD_BCRYPT);

    try{
        $insert=$conn->prepare("INSERT INTO Comptes (nom, prenom, email, identifiant, mdp, estAdmin, numeroTelephone) VALUES (:nom, :prenom, :email, :identifiant, :mdp, false, :numeroTelephone)");
        $insert->execute(['nom'=>$nom, 'prenom'=>$prenom, 'email'=>$email, 'identifiant'=>$login, 'mdp'=>$mdp, 'numeroTelephone'=>$numero]);
        header(header: "Location: FormConnexion.php?msgSucces=Inscription réussie, veuillez vous connecter");
    }catch(PDOException $e){
        header(header: "Location: inscription.php?msgErreur=Erreur lors de l'insertion");
    }
}
}
else{
    header(header: "Location: inscription.php?msgErreur=Veuillez remplir tout les champs");
}
}

```

Nous vérifions les différents champs avec plusieurs REGEX
Et le mot de passe de l'utilisateur est également crypté avec la fonction `password_hash()` :

```
$mdp=password_hash(password: $mdp, algo: PASSWORD_BCRYPT);
```

Voici un exemple de mot de passe crypté dans la BD :

horizon	\$2y\$10\$En6UJQBzksTWEKud5u99Geec/ahwj8kSphlD9rwrUoZ...	1
---------	--	---

Voici un exemple de la page d'inscription sur le site :

Non sécurisé 193.54.227.208/~R2024SAE3001/inscription.php

Créer un compte

Prénom

Nom

Identifiant

Adresse Email

N° de téléphone

Mot de passe

S'inscrire

Lorsque nous détectons une erreur sur un champ nous le signalons à l'utilisateur :

Non sécurisé 193.54.227.208/~R2024SAE3001/inscription.php

Créer un compte

Prénom

Nom

Identifiant

Adresse Email

N° de téléphone

Mot de passe

S'inscrire

Veuillez renseigner ce champ.

II - Implémentation Connexion avec Session/Cookie:

Voici le code de [FormConnexion.php](#) qui est le formulaire de connexion, on peut voir que nous récupérons un cookie “Csouvenir” si il existe pour directement mettre l'identifiant du compte si l'utilisateur à coché “Se souvenir de moi”:

```

<!DOCTYPE html>
<html lang="fr">
<head>
  <meta charset="UTF-8">
  <title>Formulaire de Connexion</title>
  <link rel="stylesheet" href="style.css">
</head>
<body>
  <div class="login-container">
    <div class="login-box">
      <h2>Connexion</h2>
      <form action="TraitConnexion.php" method="POST">
        <?php
          if(isset($_GET["msgErreur"])){
            echo "<div class='error-msg'" . htmlspecialchars(string: $_GET["msgErreur"]) . "</div>";
          }

          $loginValue = isset($_COOKIE['Csouvenir']) ? $_COOKIE['Csouvenir'] : '';
        ?>
        <div class="form-group">
          <label for="login">Identifiant:</label>
          <input type="text" id="login" name="login" value="<?php echo htmlspecialchars(string: $loginValue); ?>">
        </div>
        <div class="form-group">
          <label for="mdp">Mot de passe:</label>
          <input type="password" id="mdp" name="mdp">
        </div>
        <div class="form-group checkbox-group">
          <label for="souvenir">
            <input type="checkbox" id="souvenir" name="souvenir"> Se souvenir de moi
          </label>
        </div>
        <div class="form-group">
          <input type="submit" name="conec" value="Se connecter" class="btn-login">
        </div>
      </form>
    </div>
  </div>
</body>
</html>

```

Une fois que nous validons la connexion nous sommes redirigé vers la page [TraitConnexion.php](#) pour traiter la connexion voici son code :

```

1 k?php
2 session_start();
3 include('connect.inc.php');
4
5 if (isset($_POST["conne"]) && isset($_POST["login"]) && isset($_POST["mdp"])) {
6     $login = htmlentities(string: $_POST["login"]);
7     $mdp = htmlentities(string: $_POST["mdp"]);
8
9     $compte = $conn->prepare("SELECT * FROM Comptes WHERE identifiant = :login");
10    $compte->execute(['login' => $login]);
11
12
13
14    if ($compte->rowCount() >= 1) {
15        $row = $compte->fetch(PDO::FETCH_ASSOC);
16        if (password_verify(password: $mdp, hash: $row['mdp'])) {
17            $_SESSION['Suser'] = $login;
18
19
20            if (!empty($_POST["souvenir"])) {
21                setcookie("Csouvenir", $login, time() + 300);
22            }
23
24            $adminCheck = $conn->prepare("SELECT estAdmin FROM Comptes WHERE identifiant = :login");
25            $adminCheck->execute(['login' => htmlentities(string: $login)]);
26
27            if ($adminCheck->rowCount() >= 1) {
28                $verif = $adminCheck->fetch();
29                if ($verif['estAdmin'] == 1) {
30                    $_SESSION['Sadmin'] = true;
31                }
32            }
33            header(header: "Location: accueil.php");
34            exit();
35        } else {
36            header(header: "Location: FormConnexion.php?msgErreur=Erreur de connexion, identifiant ou mot de passe incorrect");
37        }
38    } else {
39        header(header: "Location: FormConnexion.php?msgErreur=Erreur de connexion, identifiant ou mot de passe incorrect");
40    }
41
42 } else {
43     header(header: "Location: FormConnexion.php?msgErreur=Erreur de connexion, veuillez remplir tout les champs");
44     exit();
45 }
46 ?>

```

Donc cette page va comparer directement l'identifiant et le mot de passe de la base de données et gère aussi si l'utilisateur a coché la case pour le cookie.

Pour le site nous avons **2 utilisateurs différents** : des Administrateurs et des Utilisateurs normaux pour les différencier nous avons ajouter un attribut "estAdmin" dans la table Comptes de notre base de données, si **estAdmin = 0** c'est un **Utilisateur normal** mais si **estAdmin=1** c'est un **Administrateur**

C'est pour cela que lors de la connexion nous vérifions si l'utilisateur qui tente de se connecter est un administrateur pour pouvoir créer une session "admin"

Voici le code que nous allons mettre pour les pages accessible uniquement par les Administrateurs :

```
<?php
session_start();

if (!isset($_SESSION['Sadmin']) or $_SESSION["Sadmin"] != true) {
    if(isset($_SESSION['Suser'])){
        header(header: "location: accueil.php");
        exit();
    }
    header(header: "location: FormConnexion.php");
    exit();
}
```

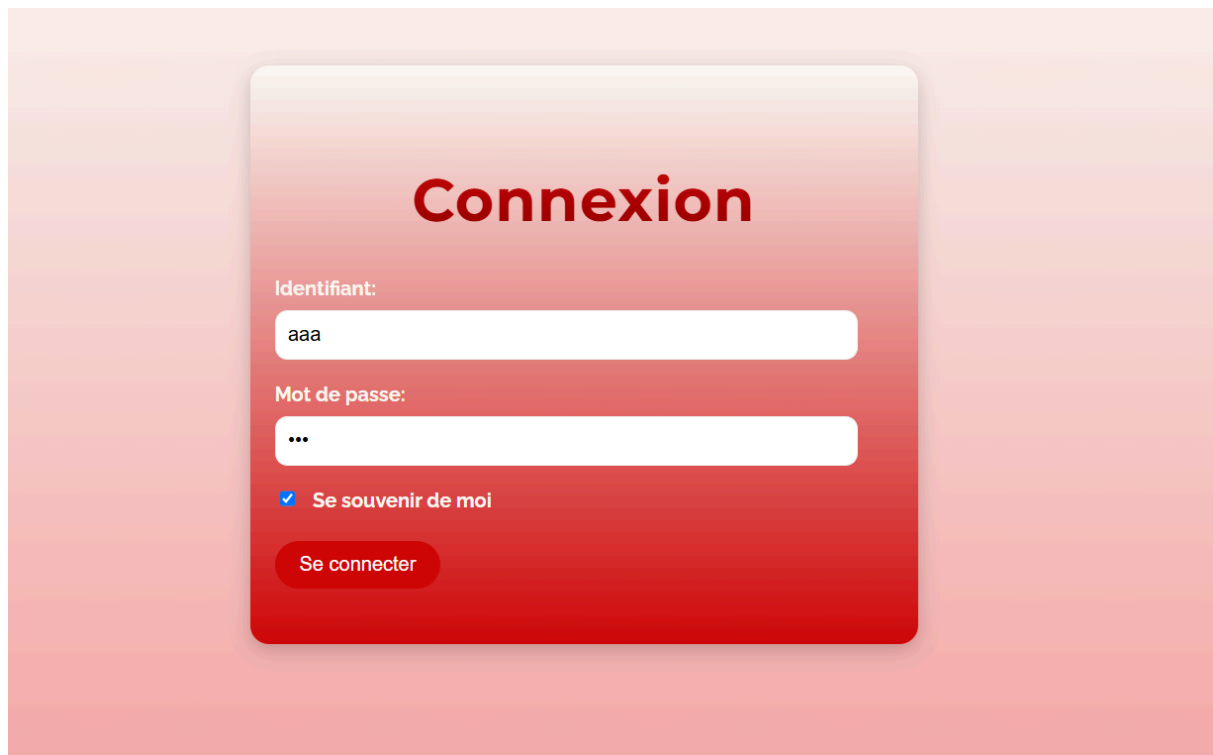
Ce code vérifie si l'utilisateur qui tente d'accéder à la page est un administrateur sinon il est renvoyé à la page de connexion s' il n'est pas connecté ou sinon à l'accueil.

Voici le code d'une requête préparée qui permet d'ajouter un Administrateur a la base de données :

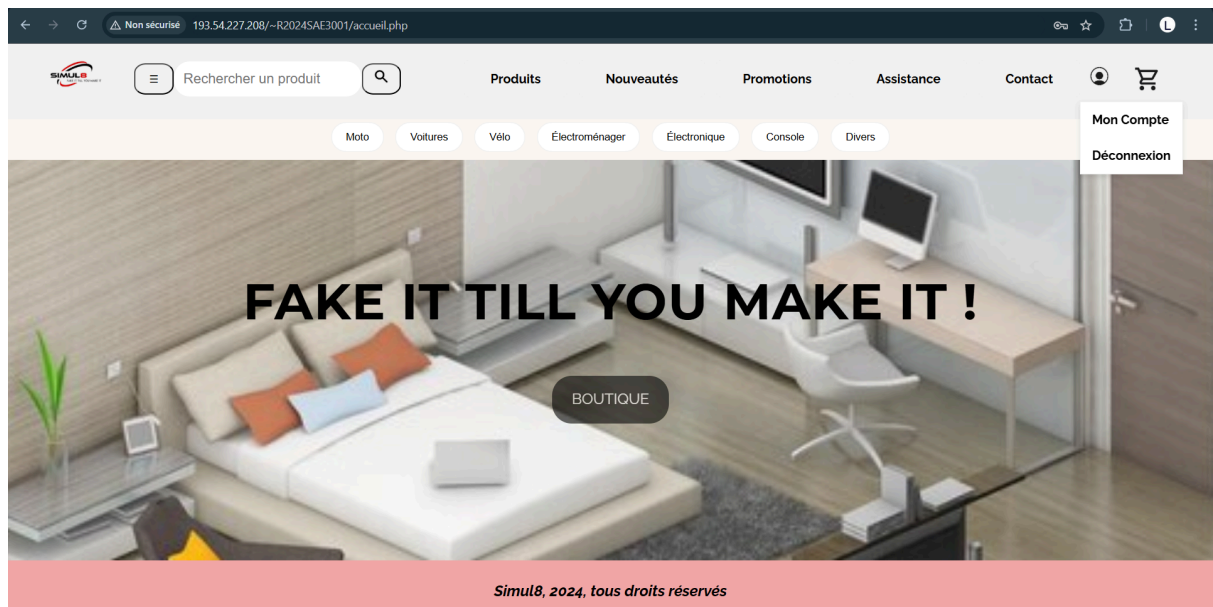
```
$req = $conn->prepare("INSERT INTO Comptes (nom, prenom, email,
identifiant, mdp, estAdmin, numeroTelephone) VALUES (:nom, :prenom,
:email, :identifiant, :mdp, :estadmin, :numeroTelephone)");
$req->execute(['nom' => "Admin", 'prenom' => "Martin", 'email' =>
"okay@gmail.com", 'identifiant' => "horizon", 'mdp' =>
password_hash("horizon", PASSWORD_BCRYPT), 'estadmin' => 1,
'numeroTelephone' => "0606060606"]);
```

III - Demonstration :

Démonstration avec un **utilisateur normal**, l'utilisateur se connecte au site normalement :

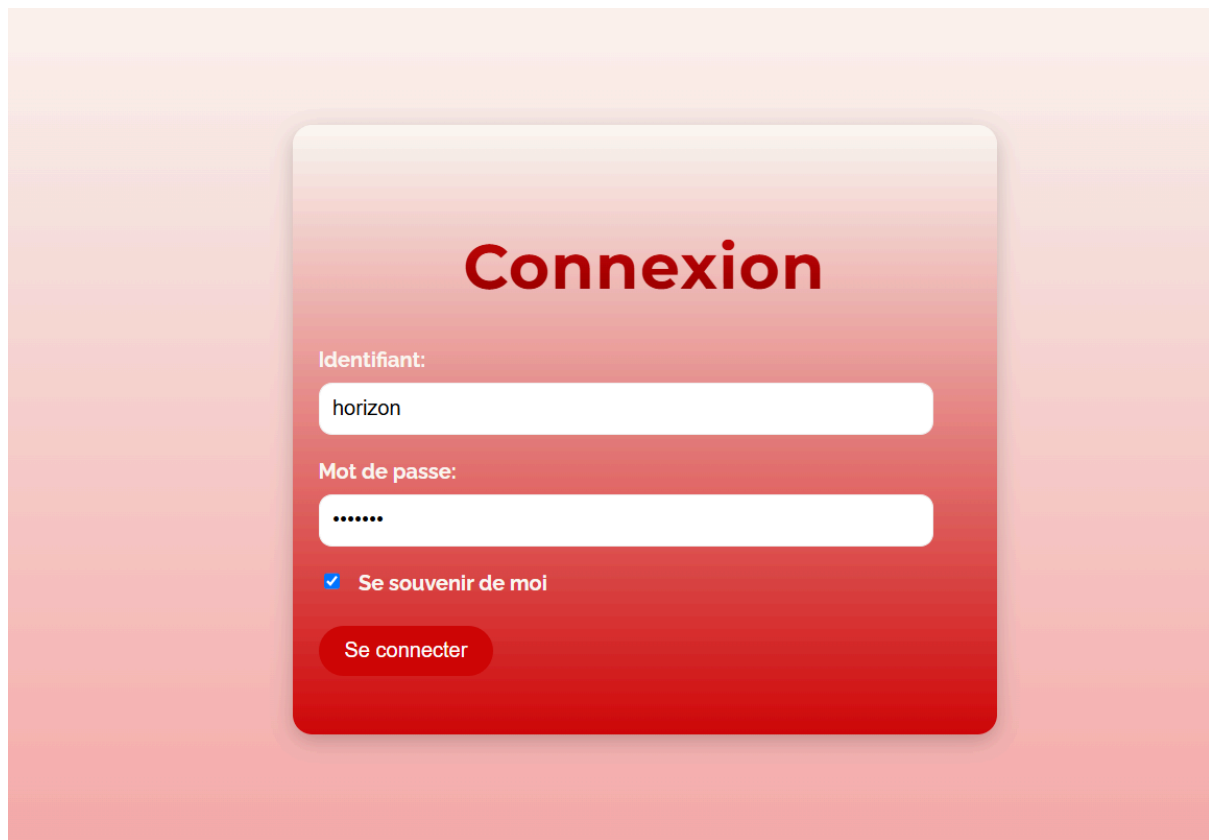


Ensuite il arrive sur la page d'accueil, lors du survol du compte il peut accéder à son compte et se déconnecter :



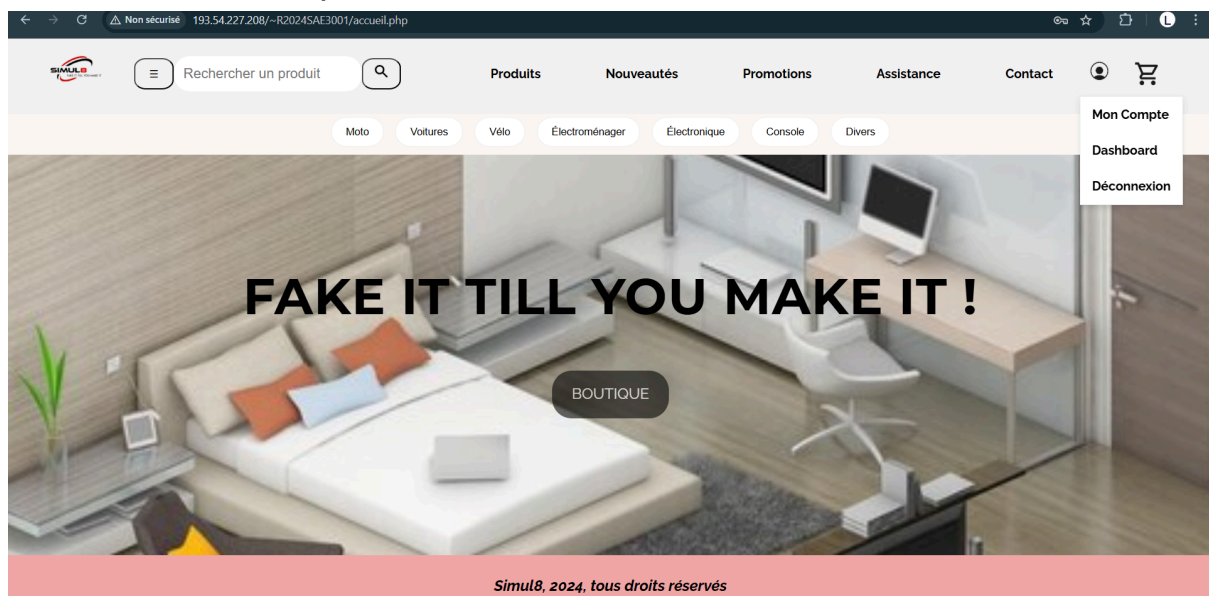
Et lorsqu'on tente d'accéder au dashboard.php (accessible uniquement par les administrateurs), nous sommes renvoyés à l'accueil.

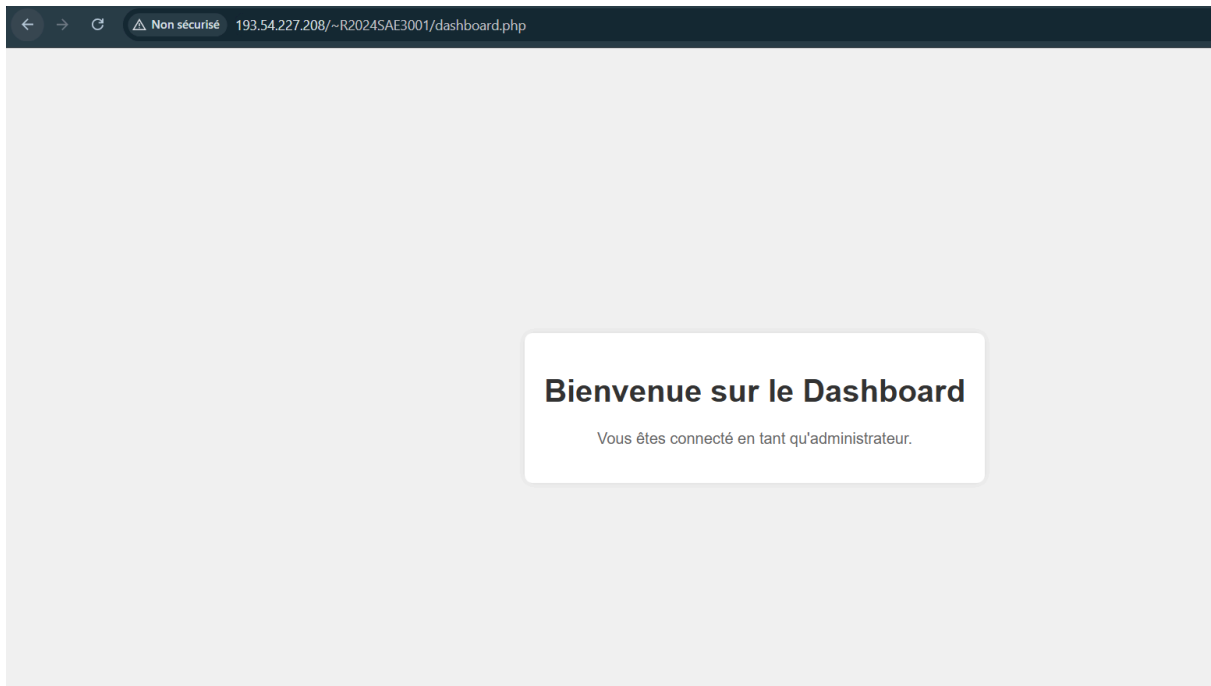
Démonstration avec un **Administrateur**, l'admin se connecte au site normalement :



The image shows a login form titled "Connexion" in large red letters. Below the title, there are two input fields: "Identifiant:" with the value "horizon" and "Mot de passe:" with a masked password ".....". There is a checkbox labeled "Se souvenir de moi" which is checked. At the bottom of the form is a red button labeled "Se connecter". The form is set against a light red gradient background.

Ensuite il arrive sur la page d'accueil, lors du survol du compte il peut accéder à son compte, accéder au **dashboard** et se déconnecter :





Donc il y a bien une gestion de droits différents selon certains utilisateurs.