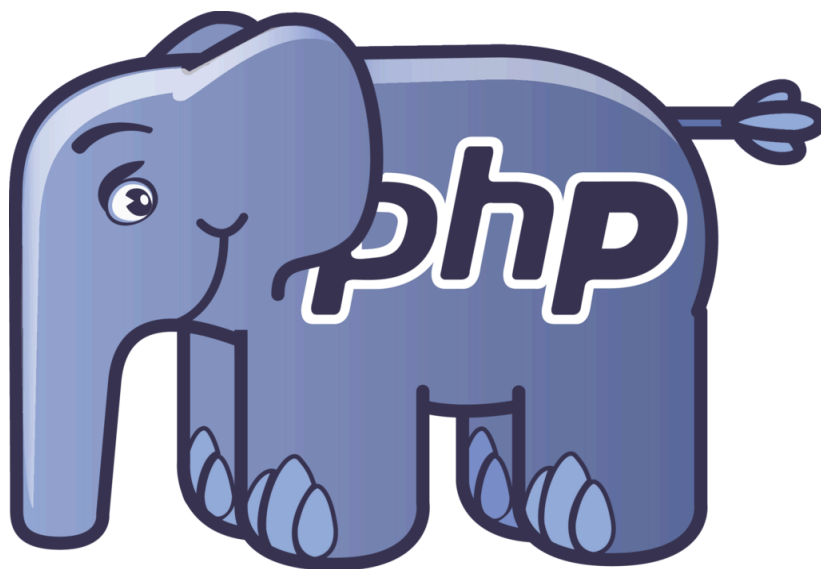


## SAE 3.01 Authentification session/cookie



Ho Nicolas, Gaches Luca, Robin Gourgues et Bouyssou Melvin

## Table des matières :

Introduction	3
Authentification	4
login.php	4
Page sécurisé pour toute Session client et admin	6
Trace d'exécution	8
Connexion et cookie	8
Essaie des page sécurisé	9
Connexion page sécurisé client et admin depuis aucune session	9
Connexion au page sécurisé avec une session client	11
Connexion en tant qu'admin	15

## Introduction

### Contexte et consigne :

La société pour laquelle nous travaillons est Style & Semelle, spécialisée dans la conception, la fabrication, et la vente de chaussures tendance. Avec une gamme de produits allant de ses propres créations esthétiques aux modèles de grandes marques internationales, l'entreprise s'adresse à un public varié et exigeant.

Pour soutenir sa croissance et améliorer ses performances, Style & Semelle souhaite mieux exploiter ses données existantes et optimiser la gestion de son activité commerciale. Cela inclut une gestion précise des stocks, des commandes, et des relations avec les clients et les fournisseurs. Dans ce cadre, l'entreprise identifie un besoin critique d'extension et de modernisation de sa base de données.

Notre mission consiste à réaliser la connexion au site ainsi que la gestion des Session pour sécuriser le site et la gestion des cookies.

## Authentification

### login.php

#### Création de la session

```
<?php
session_start();
?>
```

#### Formulaire de connexion

```
<div class="login-form">
  <h1>Connexion</h1>
  <form action="traitementLogin.php" method="post">
    <div class="mb-3">
      <label for="email" class="form-label">Email</label>
      <input type="email" id="email" name="email" class="form-control" required
        value="<?php echo isset($_COOKIE['email']) ? $_COOKIE['email'] : ''; ?>"
      </div>
    <div class="mb-3">
      <label for="password" class="form-label">Mot de passe</label>
      <div class="input-group">
        <input type="password" id="password" name="password" class="form-control" required>
        <button class="btn btn-outline-secondary" type="button" id="togglePassword">
          <i class="bi bi-eye-slash" id="eyeIcon"></i>
        </button>
      </div>
    </div>
    <div class="form-check mb-3">
      <input type="checkbox" id="remember" name="remember" class="form-check-input"
        <?php echo isset($_COOKIE['email']) ? 'checked' : ''; ?>
      <label for="remember" class="form-check-label">Se souvenir de moi</label>
    </div>
    <button type="submit" class="btn btn-primary">Connexion</button>
  </form>
  <a href="inscription.php">Pas encore inscrit ?</a>
  <a href="index.php">Se connecter en tant qu'invité</a>
<?php
if (isset($_GET["erreur"])) {
  echo '<div class="alert alert-danger mt-3" role="alert">';
  if ($_GET["erreur"] == "email") {
    echo "Cet email n'est pas enregistré.";
    echo '<a href="inscription.php" class="alert-link">Inscrivez-vous</a>';
  } elseif ($_GET["erreur"] == "motdepasse") {
    echo "Mot de passe incorrect.";
  } else {
    echo "Erreur de connexion.";
  }
  echo '</div>';
}
?>
</div>
```

### traitLogin.php

```
<?php
if (isset($_POST["email"]) && isset($_POST["password"])) {
    $email = htmlentities(string: $_POST["email"]);
    $email = strtolower(string: $email);

    // En base de données
    require_once("./connect.inc.php");
    $verifLogs = $conn->prepare(query: "SELECT * FROM UTILISATEUR WHERE email = :email");
    $verifLogs->bindParam(param: ":email", var: &$email);
    $verifLogs->execute();
    $user = $verifLogs->fetch(mode: PDO::FETCH_ASSOC);

    if ($user) {
        // Vérifiez le mot de passe en le comparant à celui stocké
        if (password_verify(password: $_POST["password"], hash: $user["PASSWORD"])) {
            session_start();
            $_SESSION["is_logged_in"] = true;
            $_SESSION["user"] = $user;
            if (isset($_POST["remember"])) {
                setcookie("email", $email, time() + 3600 * 24 * 365);
            } else {
                setcookie("email", "", time() - 3600);
            }
            header(header: "Location: index.php");
        } else {
            header(header: "Location: login.php?erreur=motdepasse");
        }
    } else {
        header(header: "Location: login.php?erreur=email");
    }
}
```

### deconnexion.php

```
<?php
session_start();
session_unset();

header(header: "location: login.php");
?>
```

### header.php

```
<?php
if (session_status() === PHP_SESSION_NONE) {
    session_start();
}
require_once("./connect.inc.php");
require_once("connectionSecurise.php");
```

### connexionSecurise.php

```
<?php
require_once 'config.php';
if (session_status() === PHP_SESSION_NONE) {
    session_start();
}
if(isset($securePage) && $securePage === true){
    if (!isset($_SESSION['user'])) {
        header(header: "Location: " . BASE_URL . "login.php");
        exit();
    }
}
?>
```

### connexionSecuriseAdmin.php

```
<?php
require_once 'config.php';
if (session_status() === PHP_SESSION_NONE) {
    session_start();
}
if(isset($securePage) && $securePage === true){
    if (!isset($_SESSION['user'])) {
        header(header: "Location: " . BASE_URL . "login.php");
        exit();
    }
    elseif ($_SESSION['user']['IDROLE'] != '1') {
        header(header: "Location: " . BASE_URL . "index.php");
        exit();
    }
}
?>
```

### config.php

```
<?php
define(constant_name: 'ROOT_PATH', value: dirname(path: __DIR__));
define(constant_name: 'INCLUDES_PATH', value: ROOT_PATH . '/includes');
define(constant_name: 'BASE_URL', value: 'http://193.54.227.208/~R2024SAE3009/');
?>
```

## Page sécurisée pour toute Session client et admin

compte.php

```
<?php
$securePage = true;
require_once 'connect.inc.php';
require_once 'includes/header.php';
require_once 'includes/connectionSecurise.php';
?>
```

Page sécurisé uniquement pour admin

zdashboard.php

```
<?php
$securePage = true;

require_once 'connect.inc.php';
require_once 'includes/connectionSecuriseAdmin.php';
require_once 'includes/header.php';
echo "hello faut sécuriser ces pages";
?>
```

Droit différent

[+ Options](#)

				IDROLE	NOMROLE	DESCROLE
<input type="checkbox"/>	Éditer	Copier	Supprimer	1	Admin	L'utilisateur possédant se role a acces au dashboa...
<input type="checkbox"/>	Éditer	Copier	Supprimer	2	Client	L'utilisateur possédant se role peut visiter le si...

pwd crypté en bd

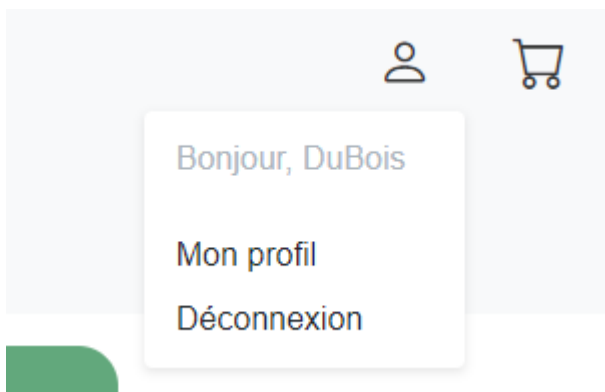
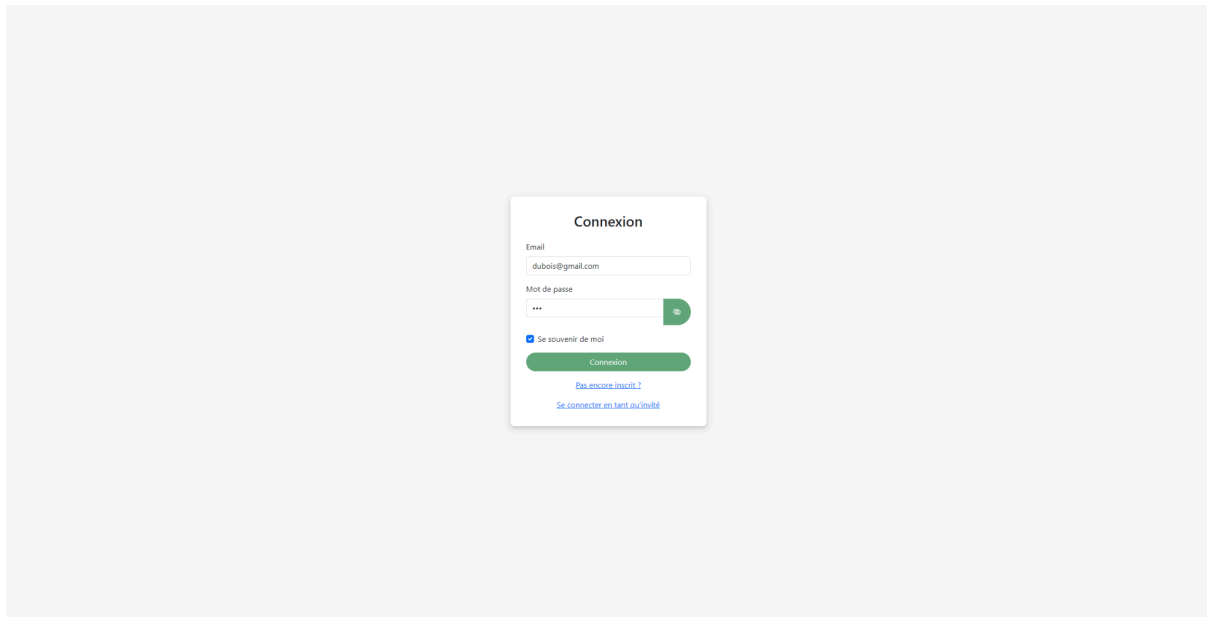
<input type="checkbox"/>	Éditer	Copier	Supprimer	75	2	Oliver	DuBois	dubois@gmail.com	\$argon2id\$v=19\$m=65536,t=4,p=1\$dUU3VklRlc0RFaVIyaTU4Qw\$wEFkgBs3tmOCVBZPjfV+KA3DTGhfbfMgMBQXnIQnRJk	0602027587	2000-01-01	2024-12-05
--------------------------	--------	--------	-----------	----	---	--------	--------	------------------	---	------------	------------	------------

pwd en entier

\$argon2id\$v=19\$m=65536,t=4,p=1\$dUU3VklRlc0RFaVIyaTU4Qw\$wEFkgBs3tmOCVBZPjfV+KA3DTGhfbfMgMBQXnIQnRJk

## Trace d'exécution

### Connexion et cookie






Année 2024-2025, groupe 1A2

Reconnexion après déconnexion et se souvenir de moi cocher

**Connexion**

Email

Mot de passe  
 

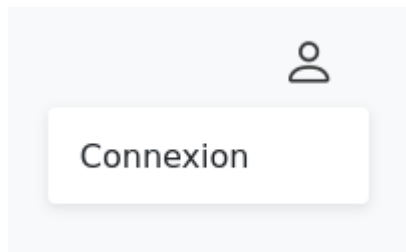
☒ Se souvenir de moi

[Pas encore inscrit ?](#)  
[Se connecter en tant qu'invité](#)

Année 2024-2025, groupe 1A2

## Test des pages sécurisées

Connexion page sécurisé client et admin depuis aucune session



`http://193.54.227.208/~R2024SAE3009/compte.php`

### Connexion

Email

Mot de passe

☐ Se souvenir de moi

Connexion

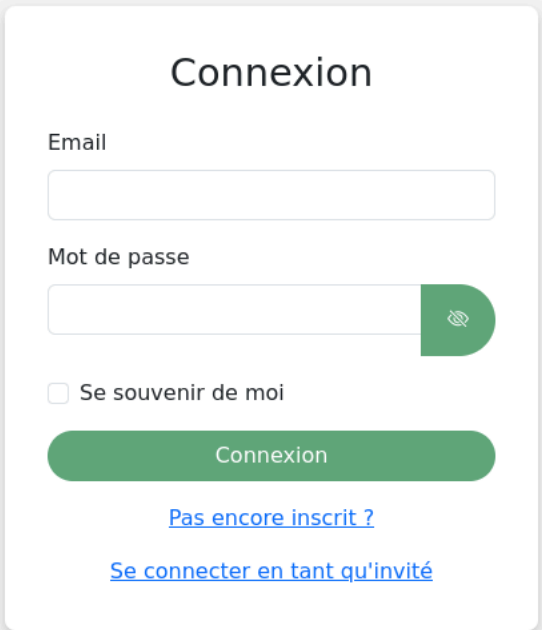
[Pas encore inscrit ?](#)

[Se connecter en tant qu'invité](#)

Lorsqu'on essaie d'accéder à la page **compte.php**, qui nécessite une session user ou admin, sans session client ou admin, c'est-à-dire sans être connecté, on est redirigé vers la page **login.php**.

Année 2024-2025, groupe 1A2

`http://193.54.227.208/~R2024SAE3009/zdashboard.php|`



The screenshot shows a login form with the title "Connexion". It contains two input fields: "Email" and "Mot de passe". The "Mot de passe" field has a green eye icon to toggle visibility. Below the fields is a checkbox labeled "Se souvenir de moi". A green button labeled "Connexion" is positioned below the checkbox. At the bottom of the form, there are two blue links: "Pas encore inscrit ?" and "Se connecter en tant qu'invité".

Lorsqu'on essaie d'accéder à la page **zdashboard.php**, qui nécessite une session admin, sans session admin c'est-à-dire sans être connecté en tant qu'admin, on est redirigé vers la page **login.php**.

Année 2024-2025, groupe 1A2


## Connexion au page sécurisé avec une session client

IDROLE 2 = client

IDROLE	int	<input type="text" value="2"/>	2
NOM	varchar(128)	<input type="text"/>	Oliver
PRENOM	varchar(128)	<input type="text"/>	DuBois
EMAIL	varchar(128)	<input type="text"/>	dubois@gmail.com

compte.php

193.54.227.208/~R2024SAE3009/compte.php

**Style et Semelle.**

Rechercher...

Homme Femme Enfant

### Informations personnelles

Nom : DuBois  
Prénom : Oliver  
Email : dubois@gmail.com  
Telephone : 0698390985  
Date de naissance : 2000-01-01  
Date d'inscription : 2024-12-06

Modifier ses informations personnelles

Supprimer mon compte

### A faire

adresse livraison  
adresse facturation

### Informations Commande

Suivre ma commande

Voir l'historique de vos commandes

[Conditions d'utilisation](#) [Conditions générales de vente](#) [Informations sur l'entreprise](#)  
[Politique de confidentialité](#)

© 2024 Style et Semelle. Tous droits réservés.

Redirection vers login.php car nous ne sommes pas en session client ou admin

Année 2024-2025, groupe 1A2

193.54.227.208/~R2024SAE3009/zdashboard.php|

**Connexion**

Email

Mot de passe



☐ Se souvenir de moi

[Pas encore inscrit ?](#)

[Se connecter en tant qu'invité](#)

[Connexion](#)

Redirection vers la page login.php car nous ne sommes pas en session admin

**Style et Semelle.** Recherche...  

Homme Femme Enfant

**Informations personnelles**

Nom : Oliver  
Prénom : Dubois  
Email : dubois@gmail.com  
Telephone : 0603027587  
Date de naissance : 2000-01-01  
Date d'inscription : 2024-12-05

[Modifier ses informations personnelles](#)  
[Supprimer mon compte](#)

**A faire**

adresse livraison  
adresse facturation

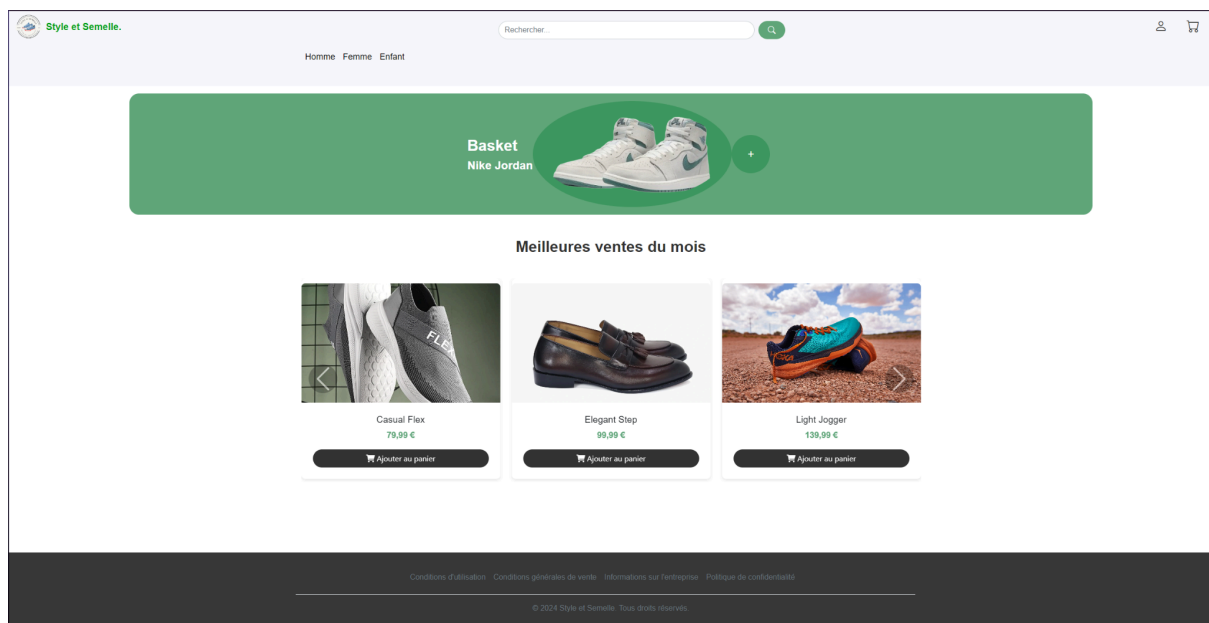
**Informations Commande**

[Suivre ma commande](#)  
[Voir l'historique de vos commandes](#)

Année 2024-2025, groupe 1A2

Connexion à la page dashboard qui est une page admin

193.54.227.208/~R2024SAE3009/zdashboard.php|



Un compte client n'a pas les droits pour aller sur cette page alors il est redirigé vers la page d'accueil.

Année 2024-2025, groupe 1A2

## Connexion en tant qu'admin

IDROLE 1 = admin

IDROLE	int	<input type="text" value="1"/>
NOM	varchar(128)	<input type="text" value="Gourgues"/>
PRENOM	varchar(128)	<input type="text" value="Robin"/>
EMAIL	varchar(128)	<input type="text" value="admin4@gmail.com"/>

## Année 2024-2025, groupe 1A2

