

27/04/2022

# Dossier de projet



Application de gestion de stock

Version 1



CHRISTIAN MARAIS.  
DWWM-AFPAR

CHRISTIAN MARAIS  
DWWM-2021-2022

PAGE { 0 }



## TABLE DES MATIERES

<b>CHAPITRE 1 - COMPÉTENCES COUVERTES .....</b>	<b>3</b>
I. Compétences couvertes par le projet : .....	3
<b>CHAPITRE 2 - RÉSUMÉ DE PROJET .....</b>	<b>4</b>
<b>CHAPITRE 3 - CAHIER DES CHARGES DU PROJET.....</b>	<b>5</b>
I. Présentation d'ensemble du projet: .....	5
II. Acteurs impliqués dans le projet.....	5
III. Les objectifs de l'application : .....	5
IV. Description fonctionnelle des besoins : .....	6
V. Les périmètres de l'application .....	6
VI. Contexte technique : .....	7
VII. Charte graphique: .....	7
A. Existant .....	7
B. Couleurs et typographies :.....	7
<b>CHAPITRE 4 - SPÉCIFICATION TECHNIQUE DU PROJET .....</b>	<b>8</b>
I. Conception .....	8
II. Choix des technologies :.....	8
III. Environnement technique .....	9
<b>CHAPITRE 5 - RÉALISATIONS ET EXTRAITS DE CODES .....</b>	<b>10</b>
I. Maquettage et wireframe : .....	10
II. Design des pages et composants : .....	11
III. Graphe de dialogue.....	12
IV. Dictionnaire de données et arborescence .....	14
V. MCD de l'application .....	15
VI. MPD de l'application.....	16
VII. Extraits de code js .....	17
A. Code qui gère l'animation de la sidebar.....	17
B. Code qui gère le modal :.....	17
C. Code qui gère la librairie chart.js :.....	17
VIII. Extraits de code PHP .....	19
A. Classe Autoload : .....	19



B. Extrait de code de la classe Controller : .....	20
C. Extrait de code de la classe Model : .....	21
D. Extrait de la classe Article, fille de la classe Model et présentation des transactions par PDO ..	21
E. Extrait de code de la classe model statistique montrant les appels de procédures : .....	22
F. Extrait du code de la view Layout :.....	22
G. Méthode qui génère les notifications.....	23
H. Extrait de code de la classe Admin : .....	23
I. Description de la méthode principale qui gère les permissions dans la classe Security .....	25
<b>CHAPITRE 6 – PRÉSENTATION DU JEU D’ESSAI.....</b>	<b>27</b>
I. Gestion des permissions :.....	27
II. Nouvelle sortie de marchandises .....	27
<b>CHAPITRE 7 – VEILLE SUR LES VULNÉRABILITÉS DE SÉCURITÉ .....</b>	<b>28</b>
I. Les injections SQL .....	28
II. Scripts intersites ou failles xss .....	28
I. La fixation de session.....	29
II. Faille include.....	29
III. Falsification de demandes intersites ou failles csrf.....	29
IV. Attaques par force brute.....	30
V. Cryptage de mots de passe et recommandations de sécurité.....	30
VI. Le détournement ou vol de session .....	30
<b>CHAPITRE 8 – SITUATIONS DE TRAVAIL AYANT NÉCESSITÉ UNE RECHERCHE .....</b>	<b>31</b>
I. Défaut de rewrite-engine sur le serveur linux :.....	31
II. Défaut de rollback de PDO en cas d’échec d’une transaction : .....	31
III. Défaut de permission pour l’utilisation de procédures stockées utilisant du LMD : .....	32
<b>CHAPITRE 9 – EXTRAITS DES SITES ANGLOPHONES UTILISÉS DANS LA RECHERCHE.....</b>	<b>33</b>
<b>ANNEXES .....</b>	<b>35</b>

# CHAPITRE 1 - COMPÉTENCES COUVERTES

## I. COMPETENCES COUVERTES PAR LE PROJET :

Vous trouverez ci-dessous la liste des compétences couvertes lors de la réalisation du projet.

Activités Types		Compétences	
FRONT-END			
A T 1	Développer la partie front-end d'une application web ou web mobile en intégrant les recommandations de sécurité	C1 - Maquetter une application	✓
		C2 - Réaliser une interface utilisateur web statique et adaptable	✓
		C3 - Développer une interface utilisateur web dynamique	✓
BACK-END			
A T 2	Développer la partie back-end d'une application web ou web mobile en intégrant les recommandations de sécurité	C5 - Développer les composants d'accès aux données	✓
		C6 - Développer la partie back-end d'une application web ou web-mobile	✓
		C7 - Développer les composants d'accès aux données	✓



## CHAPITRE 2 - RÉSUMÉ DE PROJET

DWWM 2022

RESUME DE PROJET

AFPAR

**AATTI** est un centre de formation d'apprenti qui exerce à la Réunion depuis 2012. L'AATTI a vu son nombre de formations augmenter. Ses formations ont besoin de beaucoup de ressources afin d'assurer un confort pédagogique optimal. Pour cela chaque formation a son stock de fournitures et de ressources.

Le problème est que la gestion des fournitures se faisait auparavant par des registres papiers signés qui étaient source d'erreur et l'objet de perte. De plus tout le monde n'avait pas de visuels sur ces derniers.

Lorsque je me suis présenté pour un stage, mon tuteur CHAN-KUI Liam, responsable technique, m'a demandé de mettre en place une solution numérique interne pour résoudre ces problèmes et améliorer leur gestion.

Après consultation de la DSI/équipe technique, la plateforme doit être accessible selon les modalités suivantes : création de comptes directement sur la plateforme par l'administrateur ou le responsable de l'organisme.

Aucun contenu ou fonctionnalité de la plateforme n'est accessible hors authentification.

### Les fonctionnalités attendues :

- Fonctionnalité 1 : Créer et gérer des formations
- Fonctionnalité 2 : Créer et gérer des comptes « utilisateur »
- Fonctionnalité 3 : Créer et gérer des groupes.
- Fonctionnalité 4 : Créer et gérer des domaines de formation
- Fonctionnalité 5 : Ajouter des éléments dans le stock
- Fonctionnalité 6 : Retirer des éléments du stock

### Il est possible d'accéder aux fonctionnalités suivant les rôles :

- **Super admin** : C'est un administrateur qui a tous les droits d'administration sur la plateforme
- **Responsable de l'organisme** : C'est un administrateur de l'organisation. Cet utilisateur peut gérer les comptes utilisateurs de l'organisation sur lequel il est affecté, gérer les différents domaines de son organisme
- **Formateur** : Cet utilisateur aura accès à son espace de formation il a un visuel sur son stock et peut retirer des produits (avec un historique).
- **Responsable logistique** : Cet utilisateur aura un visuel sur tous les stocks de l'entreprise. Il fera des contrôles réguliers afin de confirmer son stock.

La plateforme a été réalisée sous Php7.4, Html5 et Bootstrap4.6 pour être déployée dans un environnement linux.



## CHAPITRE 3 - CAHIER DES CHARGES DU PROJET

### I. PRESENTATION D'ENSEMBLE DU PROJET:

La gestion des fournitures du centre de formation AATI se faisait auparavant par registres papiers signés et était source d'erreur et objet de perte et tout le monde n'avait pas de visuels sur ce dernier. On m'a demandé d'apporter des solutions au travers d'une application.

### II. ACTEURS IMPLIQUES DANS LE PROJET

Nom et Prénom	Rôle projet	Société	E-mail de contact
CHAN-KUI Liam	Chef de projet	AATI	#####@aati.re
MARAIS Christian	Développeur	Stagiaire AATI/AFPAR	#####@outlook.fr
Utilisateur X	Testeur	1 Formateur AATI	#####@aati.re

### III. LES OBJECTIFS DE L'APPLICATION :

La solution envisagée devra dans ses missions :

1. Eliminer les erreurs
2. Garantir la persistance des données des stocks.
3. Rendre sa gestion accessible 24/24 en tous lieux
4. Produire des documents transférables
5. être proposée sous une interface web graphique et pouvoir être hébergée en locale et en ligne.
6. Proposer des outils visuels graphiques à des fins statistiques

Elle devra proposer les bases utilisables d'une première version qui sera enrichie et développé par la suite.



## IV. DESCRIPTION FONCTIONNELLE DES BESOINS :

Les fonctionnalités attendues sont :

- Fonctionnalité 1 : Créer et gérer des formations
- Fonctionnalité 2 : Créer et gérer des comptes « utilisateur »
- Fonctionnalité 3 : Créer et gérer des groupes.
- Fonctionnalité 4 : Créer et gérer des domaines de formation
- Fonctionnalité 5 : Ajouter des éléments dans le stock
- Fonctionnalité 6 : Retirer des éléments du stock

L'accès aux fonctionnalités de la plateforme devra se faire via un système de rôle. 4 rôles de base ont été définis :

- **Super admin :**
  - ✓ Il peut créer et gérer des formations (ex : ARH, FPA, AR ...),
  - ✓ Il peut gérer l'accès à la plateforme (compte utilisateur)
  - ✓ Il peut gérer l'attribution des droits,
  - ✓ Il a un visuel sur le stock de toutes les formations.
- **Responsable de l'organisme :**
  - ✓ Il peut gérer les comptes utilisateurs de l'organisation sur lequel il est affecté,
  - ✓ Il peut gérer les différents domaines de son organisme (exemple : FPA, ADVF, AEPE etc...) et la gestion des droits,
  - ✓ Il a un visuel sur le stock de toutes les formations.
  - ✓ Il peut aussi ajouter ou retirer des produits du stock
  - ✓ Il recevra un email en cas de réapprovisionnement.
- **Formateur :**
  - ✓ Il aura accès à son espace de formation (formateur FPA aura accès à l'espace FPA),
  - ✓ Afin gérer les ressources de sa formation il a un visuel sur son stock
  - ✓ Il peut retirer des produits (avec un historique).
- **Responsable logistique :**
  - ✓ Il aura un visuel sur tous les stocks de l'entreprise.
  - ✓ Il devra créer les produits, alimenter le nombre de produits,
  - ✓ Il fera des contrôles réguliers afin de confirmer son stock.

## V. LES PERIMETRES DE L'APPLICATION

Elle gérera les stocks sur le site du siège et sera rédigée en français. Elle sera utilisée par un groupe autorisé du personnel de l'AATI :



Utilisateurs	Utilisations	Matériels
1. Le pôle informatique	Consultation, gestion des utilisateurs	
2. La Direction	Consultation	
3. Le pôle administratif et logistique:	Consultation, entrée et sortie de marchandises, gestion des produits	
4. Le pôle formation :	Consultation,sortie	

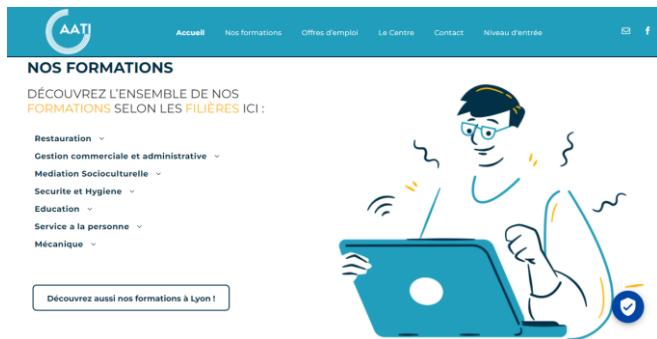
## VI. CONTEXTE TECHNIQUE :

**L'hébergement :** l'application a pour fin d'être dans un premier temps hébergé sur les serveurs de l'AATI. Le développement peut se faire sur une machine locale, l'idée n'est pas imposé. Le livrable devra être ensuite chargé sur les serveurs de l'AATI, sur une machine virtuelle fonctionnant sous Debian 10.

## VII. CHARTE GRAPHIQUE:

### A. Existant

Le CFA AATI possède un logo, des couleurs et une charte graphique existants. On m'a demandé d'inclure au projet la charte graphique de l'entreprise en m'appuyant sur celle utilisée sur le site.



### B. Couleurs et typographies :

The image displays a color palette and typography specifications for the AATI website. On the left, there's a yellow square and a dark blue rectangle. Overlaid on the blue rectangle is the CSS code: `--alt-color : hsl(0, 0%, 100%);`, `--first-color-l:hsl(213, 32%, 100%);`, and `--first-color:hsl(192, 70%, 43%);`. Below this is a dark blue box containing the text "Almost before we knew it, we had left t". To the right, there's a detailed typography specification for the font Montserrat: Family: Montserrat, Style: normal, Weight: 400, Size: 12px, Line Height: ?, Color: #525252. Below that is a list of letters: AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz.



# CHAPITRE 4 - SPÉCIFICATION TECHNIQUE DU PROJET

## I. CONCEPTION

*L'architecture : le pattern MVC et l'orienté Objet .*

*Le MVC est l'architecture moderne pour la conception de sites et d'applications web. Cette architecture présente l'avantage de séparer la partie graphique et le moteur de l'application. Un designer peut ainsi mettre à jour graphiquement sans qu'il ait besoin d'accéder au source de l'application et des données peuvent être rajoutées avec de légers rajouts dans le code. Cette architecture présente l'avantage d'une séparation du code en objets métiers via des classes, on est dans la Programmation Orienté Objet (POO). Cette technique avec les principes d'encapsulation et d'héritage renforcent la sécurité des sites en encapsulant les blocs de code sous des couches avec des niveaux d'accès. L'utilisation de classes rend également le code plus maintenable.*

## II. CHOIX DES TECHNOLOGIES :

### LES TECHNOLOGIES UTILISÉES DANS LE PROJET



**Serveur SGBD : le choix de MySQL**

*Une des fonctionnalités attendues est la persistance des données. Notre solution se tournera sur une solution SQL et un SGBD relationnel. Les plus populaires parmi les hébergeurs sont généralement les solutions gratuites MySQL ou MariaDB.*

**Le serveur http : le choix d'apache et le .htaccess**

*Le choix a été libre. Il s'est porté sur Apache2 en raison de la solidité et de la popularité de cette solution. La fonctionnalité qui nous intéresse particulièrement est l'utilisation du rewrite engine, le module de réécriture d'url d'Apache. Il permet de protéger l'arborescence des sites en la masquant à l'utilisateur.*

*Les autres technologies sont des technologies d'aide pour accélérer le développement comme :*



- la bibliothèque **JQuery** qui apporte des fonctionnalités dans le codage du langage javascript
- ou le Framework **Bootstrap** qui apportent des composants et des outils de mises en page pour le responsive.

Certaines apportent des fonctionnalités avancées sur des besoins décrits dans le cahier des charges comme :

- la classe **PHP mailer** qui propose des fonctions avancées dans l'envoi de mails
- ou **FPDF** dans la génération de fichiers PDF. Ces classes se basent sur les classes et méthodes PHP PDF et mail et proposent un usage bien plus avancé.

### III. ENVIRONNEMENT TECHNIQUE :



**L'environnement de développement :** Il n'est pas imposé. J'ai choisi VS CODE comme environnement de développement. Il est performant, propose des extensions et est installé sur ma machine de travail.

**Serveur de développement :** J'ai essentiellement travaillé sur LARAGON qui propose un serveur http apache2, un serveur de base de données MySQL, l'interface PhpMyAdmin pour la gestion de la BDD. J'ai également travaillé sur KSWEB sur Android ou sur une machine virtuelle linux après avoir installé les serveurs HTTP et SGBD, et PHP.

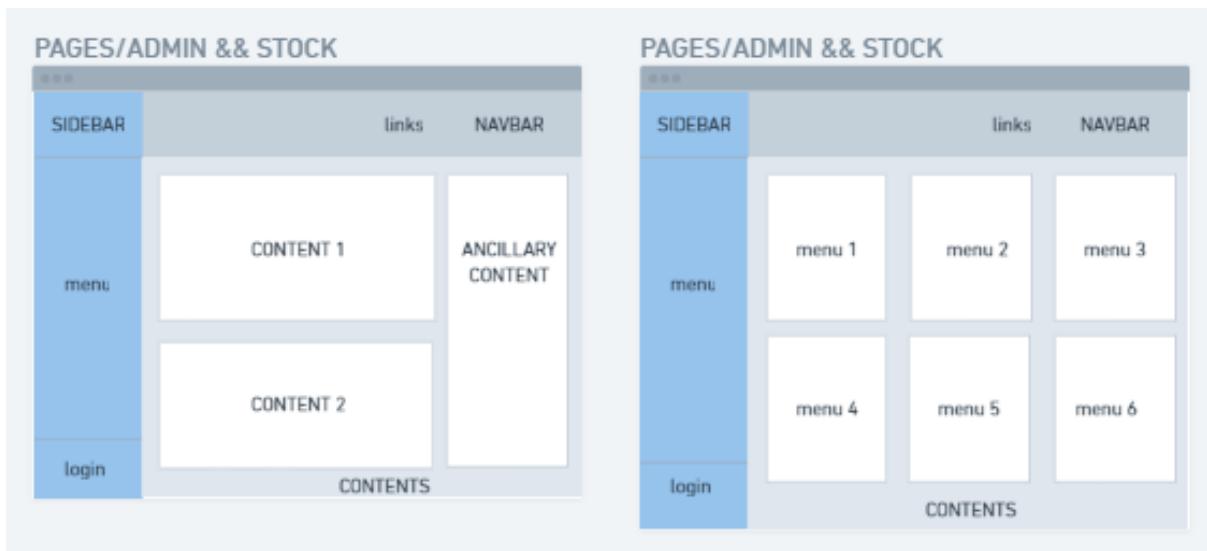
**Les logiciels :** Il faudra installer sur la machine virtuelle les logiciels nécessaire au fonctionnement de l'application à savoir :

- |                                      |  |
|--------------------------------------|--|
| ▶ Apache 2 pour le serveur HTTP      | ▶ MySQL 5 pour le serveur de base de données   |
| ▶ PHP 7.4 pour le préprocesseur HTML | ▶ PhpMyAdmin en interface de gestion de la BDD |
| ▶ PROFTPD pour le serveur FTP        |  |

Les instructions pour l'installation se feront en lignes de commande par accès sécurisé SSH via le logiciel PUTTY. L'upload des sources sur le serveur se fera via le logiciel Filezilla après l'installation du serveur ftp. Une recherche de documentation sera nécessaire dans la réalisation de cette étape du projet.

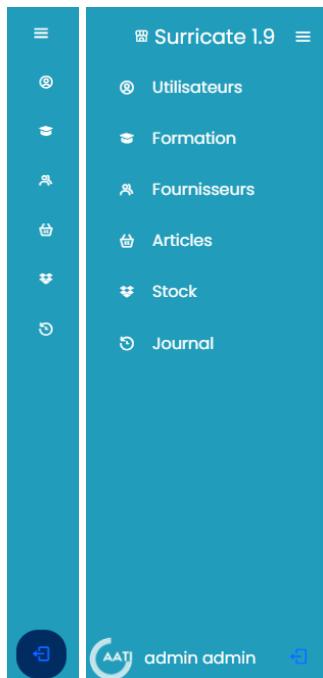
## CHAPITRE 5 - RÉALISATIONS ET EXTRAITS DE CODES

### I. MAQUETTAGE ET WIREFRAME :



## II. DESIGN DES PAGES ET COMPOSANTS :

### SIDEBAR



### NAVBAR

### BOUTONS :

Etat 1 :



Etat 2 :



### SEARCH-BOX :

id, libelle

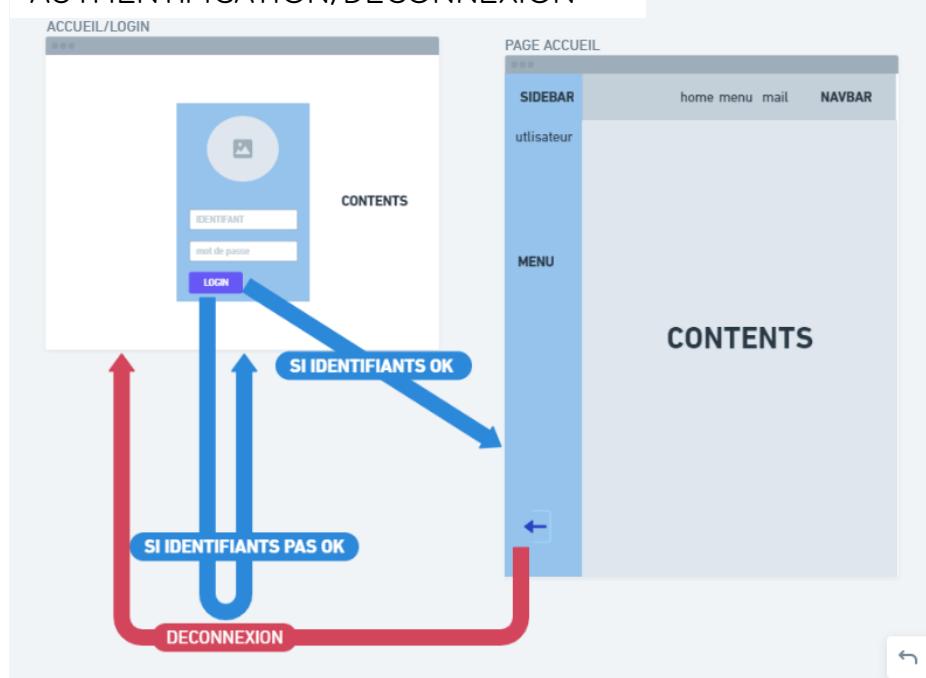
### NOTIFICATION- MODAL :

Tous les champs doivent être renseignés.

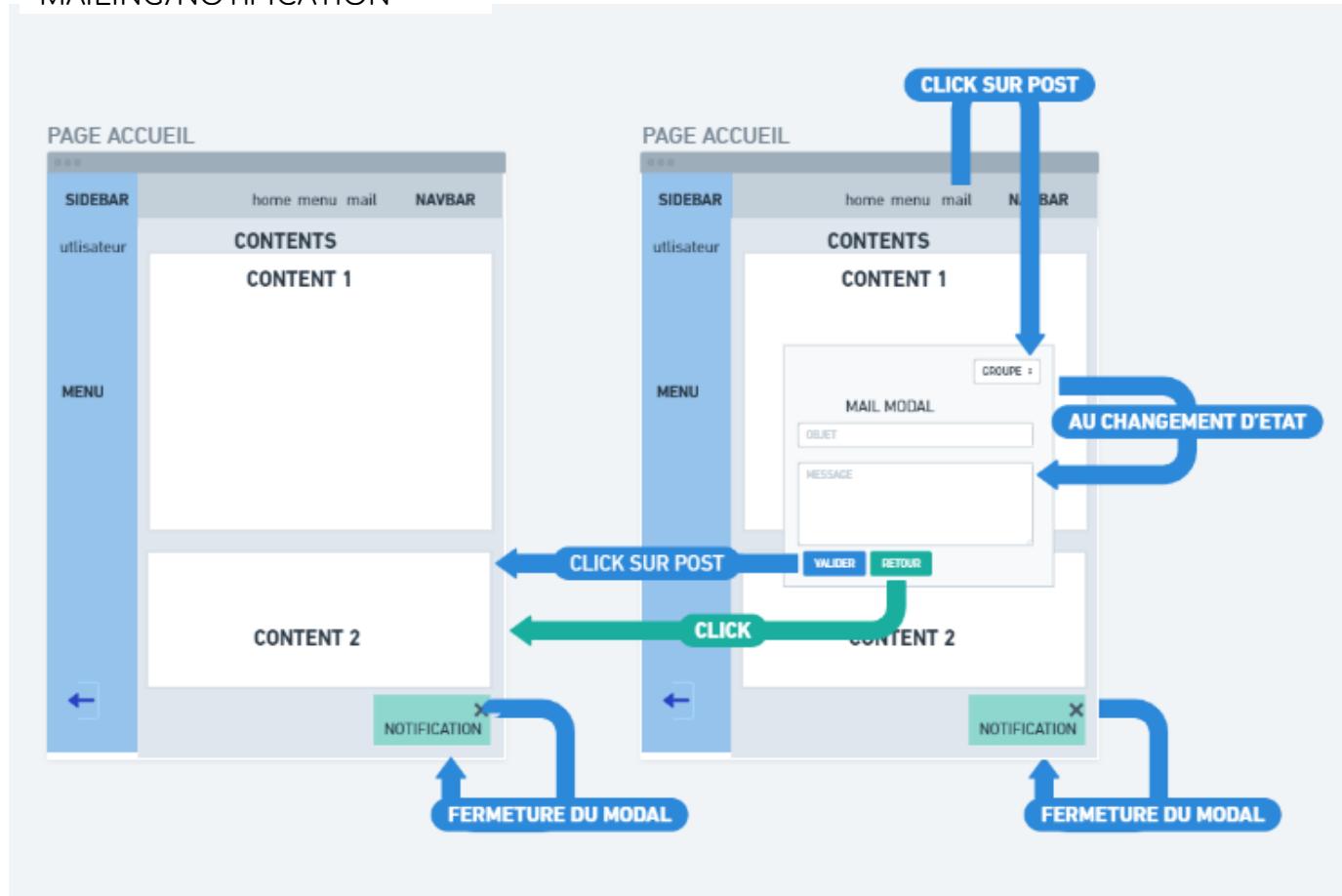


### III. GRAPHE DE DIALOGUE

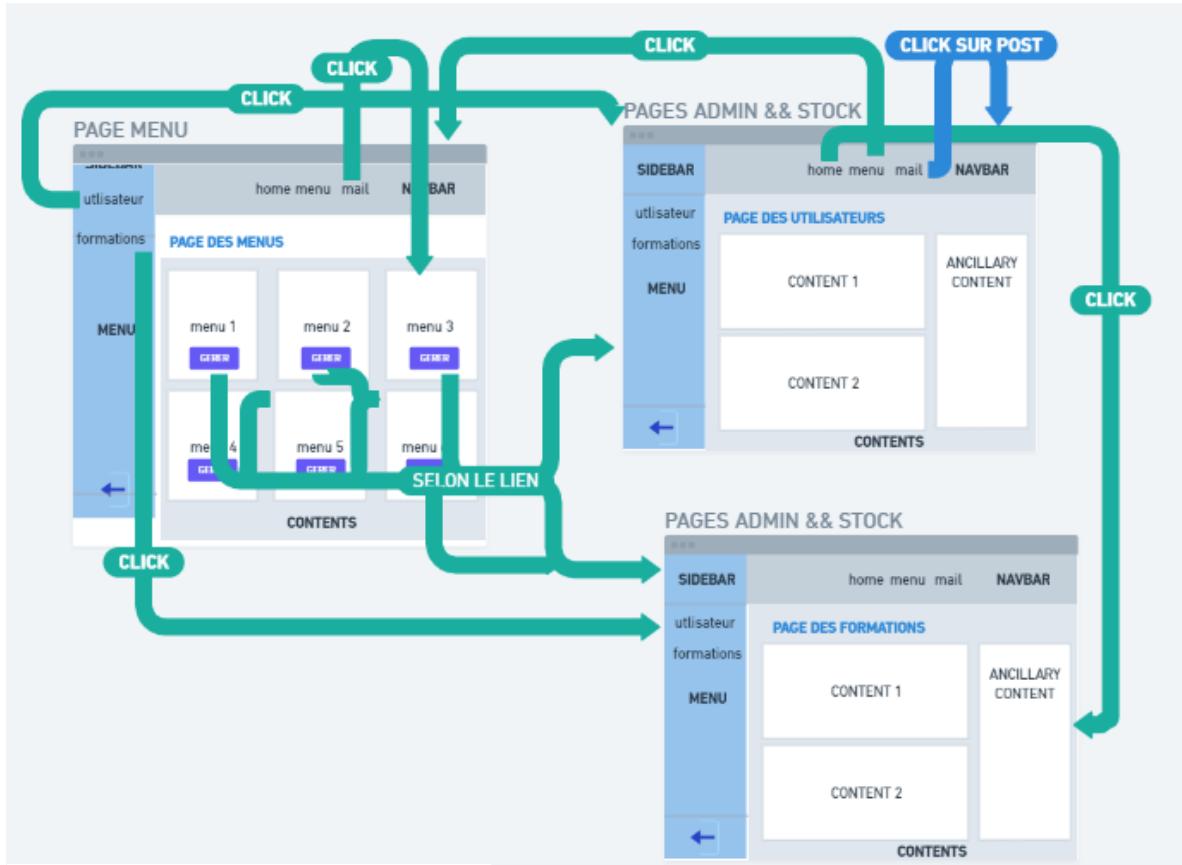
#### AUTHENTIFICATION/DECONNEXION



#### MAILING/NOTIFICATION



## MENUS



## ERREURS ET PERMISSIONS



## IV. DICTIONNAIRE DE DONNEES ET ARBORESCENCE

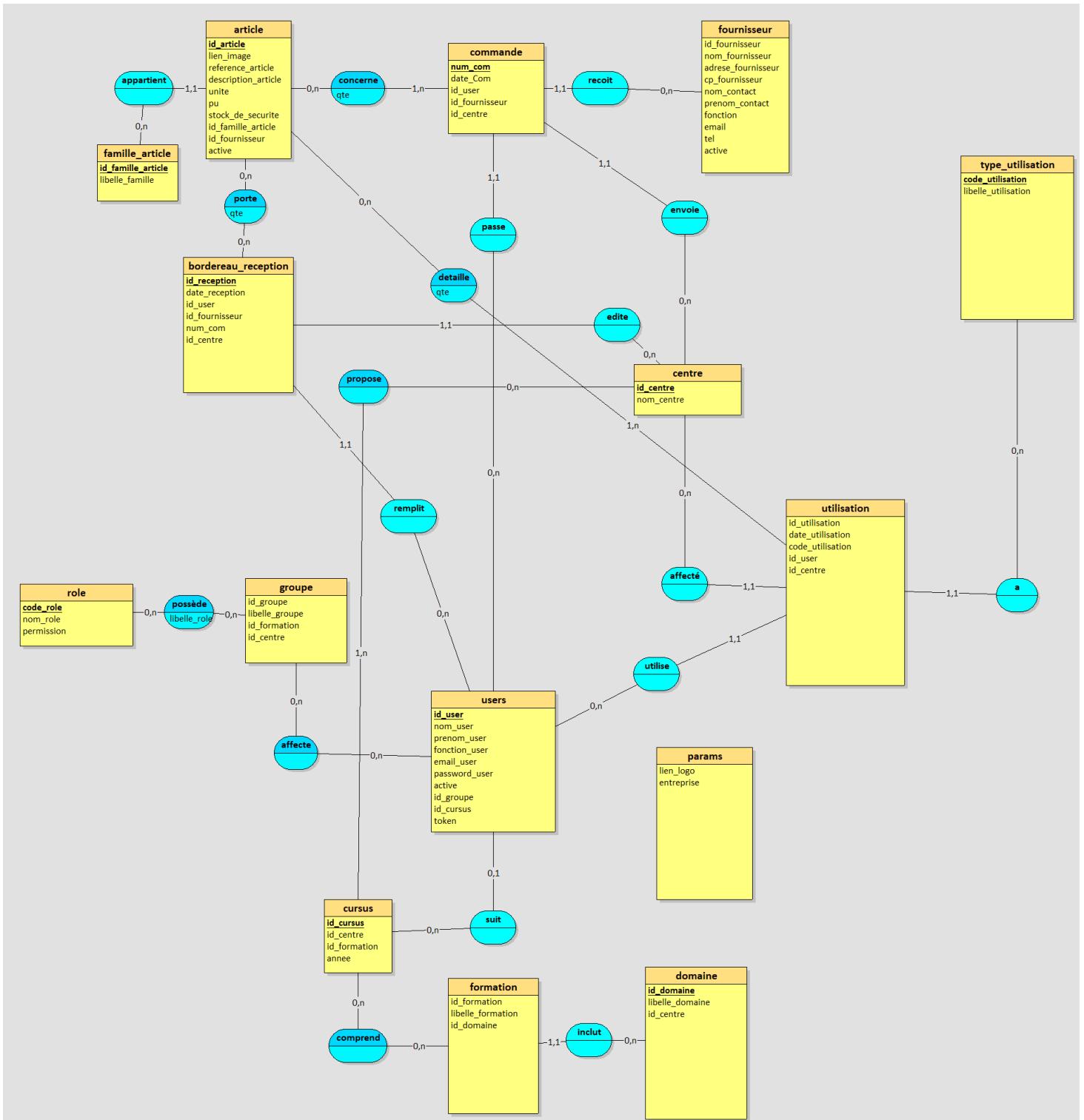
```

autoload
  Autoload.php
> css
> images
> js
> node_modules
  < src
    < app
      Controller.php
      Model.php
      Router.php
    < assets
      < css
        # backend-style.css
        # login-style.css
        # style.css
        # style.css.map
        style.scss
      < Js
        script.js
      < snippets
        > admin
        > blank
        > formateurs
        > Resp_log
        > Resp.orga
      < config
        > Log
        DB.php
        File.php
        Image.php
        Log.php
        Mail.php
        Methodes.php
        Pdf.php
        Security.php
        Sources.php
      < controllers
        Admin.php
        Api.php
        Auth.php
        Pages.php
        Stock.php
      < lib
        > FPDF
        PHPMailer-master
      < models
        Article.php
        Categorie.php
        Formation.php
        Fournisseur.php
        Groupe.php
        Role.php
        Statistique.php
        Stocks.php
        Utilisateur.php
      < views
        > admin
        > layouts
        > pages
        > stock
      > temp
      .htaccess
      aatibdd_v1 copy.sql
      index.php
  
```

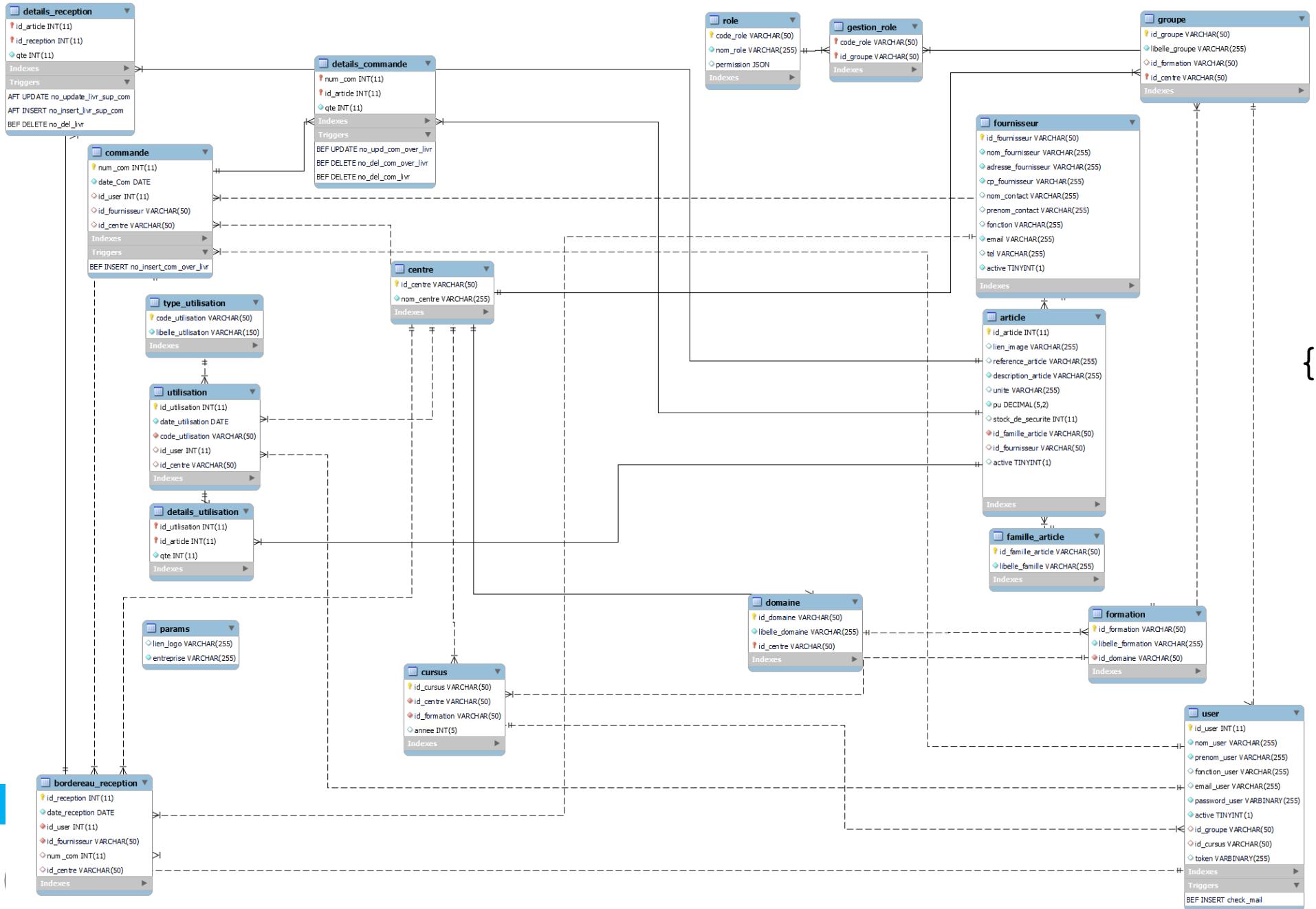
Table	Column	Type	Default Value	Nullable	Character Set	Collation
article	id_article	int(11)		NO	latin1	latin1_swedish_d
article	active	tinyint(1)	1	YES	latin1	latin1_swedish_d
article	reference_article	varchar(255)		YES	latin1	latin1_swedish_d
article	description_article	varchar(255)		NO	latin1	latin1_swedish_d
article	lien_image	varchar(255)		YES	latin1	latin1_swedish_d
article	unite	varchar(255)		YES	latin1	latin1_swedish_d
article	stock_de_securite	int(11)	0	YES	latin1	latin1_swedish_d
article	id_famille_article	varchar(50)		NO	latin1	latin1_swedish_d
article	pu	decimal(5,2)		NO	latin1	latin1_swedish_d
article	id_fournisseur	varchar(50)		YES	latin1	latin1_swedish_d
bordereau_reception	num_com	int(11)		YES	latin1	latin1_swedish_d
bordereau_reception	date_reception	date		NO	latin1	latin1_swedish_d
bordereau_reception	id_fournisseur	varchar(50)		NO	latin1	latin1_swedish_d
bordereau_reception	id_user	int(11)		NO	latin1	latin1_swedish_d
bordereau_reception	id_centre	varchar(50)		YES	latin1	latin1_swedish_d
bordereau_reception	id_reception	int(11)		NO	latin1	latin1_swedish_d
centre	nom_centre	varchar(255)		NO	latin1	latin1_swedish_d
centre	id_centre	varchar(50)		NO	latin1	latin1_swedish_d
commande	id_fournisseur	varchar(50)		YES	latin1	latin1_swedish_d
commande	date_Commande	date		NO	latin1	latin1_swedish_d
commande	num_com	int(11)		NO	latin1	latin1_swedish_d
commande	id_centre	varchar(50)		YES	latin1	latin1_swedish_d
commande	id_user	int(11)		YES	latin1	latin1_swedish_d
cursus	annee	int(5)		YES	latin1	latin1_swedish_d
cursus	id_formation	varchar(50)		NO	latin1	latin1_swedish_d
cursus	id_centre	varchar(50)		NO	latin1	latin1_swedish_d
cursus	id_cursus	varchar(50)		NO	latin1	latin1_swedish_d
detais_commande	id_article	int(11)		NO	latin1	latin1_swedish_d
detais_commande	num_com	int(11)		NO	latin1	latin1_swedish_d
detais_commande	qte	int(11)		NO	latin1	latin1_swedish_d
detais_reception	id_article	int(11)		NO	latin1	latin1_swedish_d
detais_reception	qte	int(11)		NO	latin1	latin1_swedish_d
detais_reception	id_reception	int(11)		NO	latin1	latin1_swedish_d
detais_utilisation	qte	int(11)		NO	latin1	latin1_swedish_d
detais_utilisation	id_utilisation	int(11)		NO	latin1	latin1_swedish_d
detais_utilisation	id_article	int(11)		NO	latin1	latin1_swedish_d
domaine	id_centre	varchar(50)		NO	latin1	latin1_swedish_d
domaine	id_domaine	varchar(50)		NO	latin1	latin1_swedish_d
domaine	libelle_domaine	varchar(255)		NO	latin1	latin1_swedish_d
famille_article	libelle_famille	varchar(255)		NO	latin1	latin1_swedish_d
famille_article	id_famille_article	varchar(50)		NO	latin1	latin1_swedish_d
formation	libelle_formation	varchar(255)		NO	latin1	latin1_swedish_d
formation	id_formation	varchar(50)		NO	latin1	latin1_swedish_d
formation	id_domaine	varchar(50)		NO	latin1	latin1_swedish_d
fournisseur	tel	varchar(255)		YES	latin1	latin1_swedish_d
fournisseur	nom_contact	varchar(255)		YES	latin1	latin1_swedish_d
fournisseur	fonction	varchar(255)		YES	latin1	latin1_swedish_d
fournisseur	id_fournisseur	varchar(50)		NO	latin1	latin1_swedish_d
fournisseur	nom_fournisseur	varchar(255)		NO	latin1	latin1_swedish_d
fournisseur	cp_fournisseur	varchar(255)		NO	latin1	latin1_swedish_d
fournisseur	prenom_contact	varchar(255)		YES	latin1	latin1_swedish_d
fournisseur	adresse_fournisseur	varchar(255)		NO	latin1	latin1_swedish_d
fournisseur	active	tinyint(1)	1	NO	latin1	latin1_swedish_d
fournisseur	email	varchar(255)		NO	latin1	latin1_swedish_d
gestion_role	code_role	varchar(50)		NO	latin1	latin1_swedish_d
gestion_role	id_groupe	varchar(50)		NO	latin1	latin1_swedish_d
groupe	id_formation	varchar(50)		YES	latin1	latin1_swedish_d
groupe	libelle_groupe	varchar(255)		NO	latin1	latin1_swedish_d
groupe	id_groupe	varchar(50)		NO	latin1	latin1_swedish_d
groupe	id_centre	varchar(50)		NO	latin1	latin1_swedish_d
params	entreprise	varchar(255)		NO	latin1	latin1_swedish_d
params	lien_logo	varchar(255)		YES	latin1	latin1_swedish_d
role	code_role	varchar(50)		NO	latin1	latin1_swedish_d
role	permission	json		YES	latin1	latin1_swedish_d
role	nom_role	varchar(255)		NO	latin1	latin1_swedish_d
type_utilisation	libelle_utilisation	varchar(150)		NO	latin1	latin1_swedish_d
type_utilisation	code_utilisation	varchar(50)		NO	latin1	latin1_swedish_d
user	token	varbinary(255)		YES	latin1	latin1_swedish_d
user	email_user	varchar(255)		YES	latin1	latin1_swedish_d
user	id_groupe	varchar(50)		YES	latin1	latin1_swedish_d
user	prenom_user	varchar(255)		NO	latin1	latin1_swedish_d
user	id_user	int(11)		NO	latin1	latin1_swedish_d
user	fonction_user	varchar(255)		YES	latin1	latin1_swedish_d
user	password_user	varbinary(255)		NO	latin1	latin1_swedish_d
user	nom_user	varchar(255)		NO	latin1	latin1_swedish_d
user	id_cursus	varchar(50)		YES	latin1	latin1_swedish_d
user	active	tinyint(1)	1	NO	latin1	latin1_swedish_d
utilisation	date_utilisation	date		NO	latin1	latin1_swedish_d
utilisation	id_user	int(11)		YES	latin1	latin1_swedish_d
utilisation	id_utilisation	int(11)		NO	latin1	latin1_swedish_d
utilisation	code_utilisation	varchar(50)		NO	latin1	latin1_swedish_d
utilisation	id_centre	varchar(50)		YES	latin1	latin1_swedish_d



## V. MCD DE L'APPLICATION



## VI. MPD DE L'APPLICATION



{ 16 }

## VII. EXTRAITS DE CODE JS

### A. Code qui gère l'animation de la sidebar.

```
document.querySelectorAll('.menu').forEach(item => {
    item.addEventListener('click', event => {
        sub_menu.forEach(item =>{
            item.classList.remove('active');
        });
        item.parentElement.querySelectorAll('.sub-menu').forEach(item =>{

            item.classList.toggle('active');
            sidebar.classList.add("active");
            content.classList.add('active');
        });
    });
});
```

### B. Code qui gère le modal :

```
*****Modal notification *****
//(document.querySelector('.modal_notification p').innerText.length >-1)?document.querySelector('.modal_notification').classList.add('active'):'';
//document.querySelector('.modal_notification i').addEventListener('click',function(){
//  document.querySelector('.modal_notification').classList.remove('active') ;
//})
let y=50;
let x=0;

document.querySelectorAll('.modal_notification').forEach(item =>{
/*console.log(item.querySelector('.modal_text'));*/
(item.querySelector('.modal_text').innerText.length >0)?item.classList.add('active'):'';

item.style.transform = 'translate('+x+'%, '+y+'%)';
y=y+20;
x=x-7;
console.log(item.style.transform);
item.querySelector('i').addEventListener('click',function(){
    item.classList.remove('active');
})
})
```

### C. Code qui gère la librairie chart.js :

```
let sorties =new Array();
document.querySelectorAll('.Sorties').forEach(item=>{
    sorties.push(item.innerText);
});
let securite =new Array();
document.querySelectorAll('.stock_de_securite').forEach(item=>{
    securite.push(item.innerText);
});
let marge =new Array();
document.querySelectorAll('.Marge_beneficiaire').forEach(item=>{
    marge.push(item.innerText);
});
let entree =new Array();
document.querySelectorAll('.EntréesDivers').forEach(item=>{
    entree.push(item.innerText);
```



```

});

let labels =new Array();
document.querySelectorAll('.reference_article').forEach(item=>{
    labels.push(item.innerText);
});

let livraisons =new Array();
document.querySelectorAll('.Livraison').forEach(item=>{
    livraisons.push(item.innerText);
});

const ctx = document.getElementById('myChart');
const myChart = new Chart(ctx, {
    type: 'bar',
    data: {
        labels: labels,
        datasets: [
            {
                label: 'Sorties',
                data: sorties,
                backgroundColor: [
                    'maroon'
                ],
                borderColor: [
                    'maroon',
                ],
                borderWidth: 1
            },
            {
                label: 'Stock disponible',
                data: marge,
                backgroundColor: [
                    'green'
                ],
                borderColor: [
                    'green',
                ],
                borderWidth: 1
            }
        ]
    },
    options: {
        plugins: {
            title: {
                display: true,
                text: 'Répartition du volume de marchandises'
            },
            responsive: true,
            scales: {
                x: {
                    stacked: true,
                },
                y: {
                    stacked: true
                }
            }
        }
    }
});

```

## VIII. EXTRAITS DE CODE PHP

### A. Classe Autoload :

On centralise toutes les inclusions de fichiers au travers de la méthode autoloadClass().

```
namespace Suricate;

/**
 * Autoload Classes
 */

class Autoload{

    /**
     * contient les noms de dossiers des classes à lancer via l'autoload
     */
    private const CLASSES_SOURCES = [
        'app',
        'controllers',
        'models',
        'config',
        'lib'
    ];
    /**
     * (M) Méthode qui démarre l'autoload et s'occupe du démarrage automatique de méthodes au
     lancement
     * (O) rien
     * (I) rien
     */
    public static function init(){//initialise et démarre la classe autoload
        // define("ROOT_INDEX",str_replace('public/index.php','','$_SERVER['SCRIPT_FILENAME']]));//on
        // définit une constante PHP pour le ROOT du dossier
        define("ROOT",str_replace('index.php','','$_SERVER['SCRIPT_FILENAME']]));
        spl_autoload_register(function($class){
            self::namespaceToClass($class); //on traduit les namespaces en classe pour l'autoload des
            classes
            self::autoloadClass($class);
        });
        Log::init(); // on lance d'abord le log
        Security::init(); // puis la sécurité
        Router::init(); //enfin on lance le routeur
    }
    /**
     * (M) Méthode qui fera les appels de fichier à chaque appel de classe
     * (O) rien
     * (I) le string du nom de classe à lancer
     * @param string class string du nom de classe. Respecter la convention camelCase
     */
    private static function autoloadClass($class) {

        $sources = array_map( function($sources) use($class) {
            return ROOT.'src/'. $sources . '/' . $class . '.php';
        }, self::CLASSES_SOURCES );

        foreach($sources as $s){
            if(file_exists($s)){
                require_once $s;
            }
        }
    }
    /**
     * (M) Méthode qui transforme les namespace en nom de classe. Lors des appels de classes l'autoload
     appelle les classes suivant le système de namespace ce qui pose problème pour les appels de fichiers.
     Cette méthode résout ce problème.
    */
}
```

On adapte l'autoloader au système de namespace avec deux méthodes traductrices classe/Namespace.



```

 * (O) rien
 * (I) le string du namespace ou celui transmis par la méthode spl_autoload_register
 * @param string class string du nom de classe.
 */
public static function namespaceToClass(&$class){
    $class=preg_replace('/(.)*\\\\\\\'','',$class); //on enlève le namespace pour garder que le nom
de la classe
}
/**
 * (M) Méthode qui transforme les nom de classe en namespace. L'instanciation d'une classe par
l'utilisateur via la méthode des variables de string n'utilise pas le système de namespace. Cette
méthode résout ce problème
 * (O) rien
 * (I) le string de la classe à passer
 * @param string class string du nom de classe.
*/
public static function classToNamespace($controller){
    return '\\'.__NAMESPACE__.'\\'.$controller;
}

private function autoloadStyle(){
    $params=explode('/',$_GET['p']);
}

}

```

## B. Extrait de code de la classe Controller :

La méthode loadModel() sert à l'appel des classes models et la méthode render() prépare et réalise l'affichage finale en procédant à l'inclusion des views et des composants (elle réalise les require nécessaires en lui passant le nom de la view).

```

 /**
 * M permet d'initialiser les classe modèles choisies qui devra communiquer avec la bdd
 * O rien
 * I le string du nom du modèle ex: le model ;
 */
protected function loadModel(string ...$model){//créé une instance de models transmis pour
pouvoir faire appel à leurs méthodes

    foreach($model as $item){//sert uniquement à récupérer de la donnée
        $item=ucfirst($item); //On commence le nom de classe par une majuscule pour respecter le
nom de fichier qui correspond à celui utilisé pour l'appel de classe donc impérativement en majuscule
        $itemNamespace=Autoload::classToNamespace($item); // on récupère le namespace
correspondant
        $this->$item = new $itemNamespace(); // on instancie le model
    }
}

protected function getDatas($methode,string ...$data){

}

/**
 * M permet d'initialiser les classe modèles choisies qui devra communiquer avec la bdd
 * O rien
 * I le string du nom du modèle ex: le model ;
 */
protected function render(string $fichier,array $data = [],$class=null){// sert uniquement à
l'affichage en faisant les require des vues

    extract($data); //extrait les données d'un tableau associatif sous forme de variables. On
accède ainsi aux données unitaires recues de la bdd

```



```

        if($class==null){//si classe non défini on utilise la classe du contexte en cours ex:
Admin, Auth...
            $class=get_class($this);
        }
        Autoload::namespaceToClass($class);//on change les espaces de nom en classe pour les
require
try{
    self::loadComponent($this->theme);//charge les composants ou éléments html
headers... dans des constantes pour pouvoir les placer de façon structurer dans des layouts
}catch(Exception $e){
    self::loadComponent($this->defaultTheme); //charge le theme par défaut en cas d'erreur
}

ob_start();//enclenche la temporisation de sortie. Aucune donnée sauf les entêtes n'est
envoyé au navigateur
require_once(Sources::path('views').strtolower($class).'/'.{$fichier}.php');//commenter
pour changer de méthodes
//require_once(ROOT.'src/views/'.strtolower($class).'/'.{$fichier}.php);// decommenter
pour revenir à la méthode par défaut des require
$content=ob_get_clean();//les echos et require de la vue ont été placé dans une variable
qui est dans le layout
require_once(ROOT.'src/views/layouts/'.{$this->layout}.php');//une fois la variable
déclarée on importe le layout
}

```

### C. Extrait de code de la classe Model :

La plupart des méthodes des classes filles de Model utilisent pour les requêtes SQL les méthodes de Model à travers l'héritage. La connexion et ces méthodes sont encapsulées.

```

protected function updateBy($id,$valeur_id,$data,$isEncrypt=null,$key=self::ENCRYPT_SQL_KEY){

    $datas=array($id,$valeur_id,$data);
    $this->secure($datas);
    extract($datas);
    $i=0;
    $sql="UPDATE {$this->table} SET";
    foreach($data as $colonne => $valeur){
        $sql.=($isEncrypt!=null && !empty($key) && in_array($colonne,$isEncrypt))?' ' .{$colonne} .
= ' .{$this->enDecryptData('?', $key)} .': ' .{$colonne} .' = ? ,';
        $valeurs[$i]= $valeur;
        $i++;
    }
    $valeurs[$i]= $valeur_id;
    $sql=substr($sql,0,-1);
    $sql.=" WHERE $id = ?";
    $this->testSql($sql,$valeurs);

    $req=$this->connexion->prepare($sql);
    $this->setDataNull($valeurs);//[6] en param 2
    $req=$req->execute($valeurs);
    return $req;
}

```

### D. Extrait de la classe Article, fille de la classe Model et présentation des transactions par PDO

```

/**
 * (M) Méthode qui update un article
 * (O) rien
 * (I) 3 champs

```



```

 * @param string champ ou nom de colonne de l'id
 * @param string valeur du champs
 * @param array file facultatif contenant l'ensemble des propriétés du fichier image uploadé.
 */
public function updateOneArticle($id,$valeur_id,$file=null){
    $this->table='article';// on choisit la table article

    $this->setData(); // on configure les données à utiliser. Post non déclarés sont mis à vide et
    int on leur met une valeur 0

    ($file!=null)?$this-
>data['lien_image']=$file['filename'].$file['extendedName'].'.'.$file['type']:'';// on définit
l'adresse de l'image associée à l'article
    if($_POST['pu']>=0){// Sécurité sur le prix si le prix n'est pas correcte on refuse la mise à
jour
        (empty($this->data['active']))?$this->data['active']=0:'';
        $results= $this->updateBy($id,$valeur_id,$this->data); // on met à jour les données

        if(!$results){// Si on ne peut pas update
            try{
                $this->connexion->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION); // on met
le mode erreur de PDO en Exception pour qu'il retourne le message d'erreur
                $this->connexion->beginTransaction(); // on commence une transaction
                $this->insertOneArticle($this->data); // On insère la modification comme nouvel
article
                $tables=['approvisionnement','details_commande','details_reception','details_ut
ilisation']; // on définit les tables à modifier avec les nouvelles valeurs
                $lastId=$this->getLastId(); // on récupère l'id de la nouvelle ligne insérée

                foreach($tables as $table){ // pour chaque table à mettre à jour
                    $this->table=$table;
                    $this-
>updateBy('id_article',$_POST['validating_edit'],['id_article'=>$lastId]); // on met à jour les données
                }
                $this->table='article'; // on revient dans article
                $this->deleteBy($id,$valeur_id); // on supprime l'ancienne occurrence d'article
                $this->connexion->commit(); // on fait un commit
            }catch(Exception $e){ // si la transaction échoue
                $this->connexion->rollback(); // on fait un rollback
                $results=false; // on retourne un false pour échec
            }
        }
    }else{// si le prix est inférieur à 0
        $results=false; // on notifie un échec pour l'opération
    }
    return $results; // on retourne false ou true
}

```

#### E. Extrait de code de la classe model statistique montrant les appels de procédures :

```

public function fluxComCurrYearByUser($idUser){
    $sql= 'call flux_commande_current_year_by_user(?)';
    $req=$this->connexion->prepare($sql);
    $req->execute(array($idUser));
    return $req->fetchAll(); }

```

#### F. Extrait du code de la view Layout :

Il recueille les différentes views à travers la variable \$content ainsi que les différents composants d'une page (header, footer, sidebar, navbar...). Le layout permet de présenter les différentes views à travers des pages homogènes.

```

<!DOCTYPE html>
<html lang="en">

```



```

<head>
    <?=HEAD?>
    <link rel="stylesheet" href="=BASE_URI?&gt;src/assets/css/backend-style.css"&gt;
&lt;/head&gt;

&lt;body&gt;

    &lt;?=($POST['mail']) &amp;&amp; !empty(MAIL)? MAIL:""?&gt;

    &lt;header&gt;
        &lt;?=NAVBAR?&gt;
    &lt;/header&gt;
    &lt;?=SIDEBAR?&gt;
    &lt;main&gt;
        &lt;section&gt;
            &lt;div class="home_content"&gt;
                &lt;div class="text top_title"&gt;
                    &lt;h1&gt;
                        Page des &lt;?=PAGE?&gt;
                    &lt;/h1&gt;
                &lt;/div&gt;
                &lt;div class="content"&gt;
                    &lt;div class="container"&gt;
                        &lt;?=$content?&gt;
                    &lt;/div&gt;
                &lt;/div&gt;
            &lt;/section&gt;
        &lt;/main&gt;
    &lt;?=(!empty(MODAL) &amp;&amp; !empty($_SESSION['message']))?MODAL:"";?&gt;
    &lt;?=($POST['upload_file']) &amp;&amp; !empty(FILE)? FILE:""?&gt;
    &lt;script src="<?=BASE_URI?&gt;node_modules/chart.js/dist/chart.min.js"&gt;&lt;/script&gt;
    &lt;script src="<?=BASE_URI?&gt;src/assets/Js/script.js"&gt;&lt;/script&gt;
    &lt;?=FOOTER?&gt;
&lt;/body&gt;
&lt;/html&gt;
</pre

```

## G. Méthode qui génère les notifications

```

/**
 * M méthode qui adresse les messages
 * O Rien
 * I Rien
 */
protected function message($message,$id_message=1){
    if(!empty($_SESSION['message'][0])){
        unset($_SESSION['message'][0]);
    }
    ($isset($_SESSION['message'][$id_message]))?$_SESSION['message'][$id_message]=$message
    :$_SESSION['message'][$id_message]=$message;
}

```

## H. Extrait de code de la classe Admin :

- *Page d'accueil des formateurs :*

```

public function index(){//pour aller au menu de back-end
    define('PAGE','espaces membres');// on indique le nom de la page d'accueil admin comme
"parametres"

    if($_SESSION['login']=='logged'){//si on est loggé on affiche le menu
        (!$this->checkUserContenuPermission('INDEX',[ 'LECTURE']))?$this-
        >redirection('pages/blocked'):';// on continue si on a les permissions ou on est redirigé

```



```

        $this->loadModel('Statistique');
        if(!empty($idUser=$_SESSION['id'])){
            $commandesCurrentYear=$this->Statistique->fluxComCurrYearByUser($idUser);
            $comUserGrpByArt=$this->Statistique->fluxComCurrYearByUserGrpByArticle($idUser);
            $sortieCurrMonthUser= $this->Statistique->sortieCurMonthByUser($idUser);
            $comMonthUser = $this->Statistique-> comCurrentMonthByUser($idUser);
            $comMonthUserGrpByArt = $this->Statistique->
comCurrentMonthByUserGrpByArticle($idUser);
            $fluxMensuel = $this->Statistique->fluxUtilisationMensuelleUser($idUser);
            (!empty($preferredArticle = $this->Statistique-
>preferedArticleByUser($idUser)))?$_POST['preferedArticle']=$preferredArticle:$_POST['preferedArticle']=
[];
        }
        //var_dump($preferredArticle );die();
        $this-
>render('espaceperso',compact('fluxMensuel','preferredArticle','commandesCurrentYear','comUserGrpByArt',
'sortieCurrMonthUser','comMonthUser','comMonthUserGrpByArt'),'admin');
    }else{//sinon réaffiche la page de login
        $this->redirection('auth/login');
    }
}

```

- *Extrait de la méthode centres de la classe Admin*

```

public function centres(){//méthode qui gère les groupes

    define('PAGE', __FUNCTION__);// definit le nom de la page

    if($_SESSION['login']=='logged'){
        (!$this->checkUserContenuPermission(PAGE,['LECTURE']))?$this-
>redirection('pages/blocked'):'';// on continue si on a les permissions ou on est redirigé

        $this->loadModel("Formation");//on charge les modèles utilisés par la méthode groupes

        if(!empty($_POST['delete'])){ //si on valide la suppression du groupe
            (!$this->checkUserContenuPermission(PAGE,['SUPPRESSION']))?$this-
>redirection('pages/blocked'):'';// on continue si on a les permissions ou on est redirigé

            if($this->Formation->deleteOneCentre('id_centre',$_POST['delete'])){ //si la suppression
réussit
                $this->message("Le centre a bien été supprimé",__FUNCTION__); //on envoie une
notification de succès
                $this->redirection('admin/'.__FUNCTION__); // on redirige vers la page d'accueil des
centres
            } else{
                $this->message("Erreur lors de la suppression",__FUNCTION__); //on envoie une
notification de succès
            }
        }elseif(isset($_POST['create'])&&!empty($_POST['id_centre'])&&
!empty($_POST['nom_centre'])){//si on valide la création d'une centre non vide
            (!$this->checkUserContenuPermission(PAGE,['CREATION']))?$this-
>redirection('pages/blocked'):'';// on continue si on a les permissions ou on est redirigé

            if($this->Formation->insertOneCentre()){// si le rajout du nouveau centre réussit
                $this->message("La centre a été créé",__FUNCTION__); // on envoie une notification
de succès
                $this->redirection('admin/'.__FUNCTION__);
            }else{
                $this->message("La centre n'a pas été créé",__FUNCTION__); // on envoie une
notification de succès
            }
        }elseif(!empty($_POST['validating_edit'])){ //si on valide l'édition d'un centre
    }
}

```



```

(!$this->checkUserContenuPermission(PAGE,['MODIFICATION']))?$this-
>redirection('pages/blocked'):';// on continue si on a les permissions ou on est redirigé
$centres=$this->Formation->getAllcentres();// on récupère les informations sur les
centres

$data=[// on récupère les informations mises à jour du centre venant du formulaire
'id_centre' =>$_POST['id_centre'].$_POST['validating_edit'],
'nom_centre' =>$_POST['nom_centre'].$_POST['validating_edit']]
];
if($this->Formation->updateOneCentre('id_centre',$_POST['validating_edit'],$data)){//si la mise à jour réussit
    $this->message('Le centre '.$data['nom_centre'].' a été mis à jour",__FUNCTION__);
// on envoie une notification de succès
    $this->redirection('admin/'.$__FUNCTION__); // on redirige vers l'accueil du centre
}else{
    $this->message('Le centre '.$data['nom_centre'].' n\'a pas été mis à
jour',__FUNCTION__); // on envoie une notification de succès
}

}
}else{//si on n'est pas loggé
    $this->redirection('utilisateurs/login');// on est renvoyé à la page de login
}
$this->setPagination('Formation','countCentres',$search,$limit,$numberOfPage);
$datas=$this->Formation->getAllCentres($search,$limit); // on récupère les infos actualisées des
centres
$this->render('centres',compact('datas','numberOfPage'));// on affiche d'accueil des
groupes avec les liste des groupes
}

```

## I. Description de la méthode principale qui gère les permissions dans la classe Security

```

/**Description : fonction qui gère la vérification des permissions des users par page
 * @param string nomPage string du nom de page
 * @param array permString de string de nom des permissions nécessaires ex :
 *      ['LECTURE',
 *       'CREATION',
 *       'MODIFICATION',
 *       'SUPPRESSION']
 * @param boolean egaliteStrict facultatif si on veut définir des permissions strictes par
exemple seul création est autorisé.Si une personne a un score supérieure elle sera quand même refusée.
 * peut servir à affiner les permissions sur des pages ou l'affichage ou non de blocs html
 * @return boolean true si le score de permission de l'utilisateur est supérieure à celle
demandée
 */
protected function checkUserContenuPermission($nomPage,$permString,$egaliteStrict=false){

$allowedScore=0;// on met un score autorisé de 0
foreach($permString as $perm){// pour chaque string de permission entré
    if($this->translatePermStringToValue($perm)>=0){//on traduit le string en score et s'il
est bon et >=0
        $allowedScore=$allowedScore+$this->translatePermStringToValue($perm);// on le
rajoute au score autorisé
    }
}
$idPage=$this-
>translatePermStringToValue(strtoupper($nomPage),Security::PERMISSION_CONTENU);//on récupère l'id de
page à partir du nom

$results=false;
$roleFromDb = new Role();// on initie une instance de role
if(!empty($_SESSION['role'])){//si la session n'est pas vide
    $roles= explode(',',$_SESSION['role']); // on obtient tous les roles enrgistrés dans la
session
}

```



```

foreach($roles as $role){// pour chaque role
    $score=0;// on définit un score de départ de 0
    $userRole=$roleFromDb->getOneRole('code_role',$role);// puis on récupère les infos
du role

    $userPermission=@json_decode($userRole["permission"]);//on récupère plus
précisememnt l'ensemble des permissions du role sous forme d'objet
    if(gettype($userPermission)=='array'){
        foreach($userPermission as $permission){//pour chaque permission de page

            ($permission->id == $idPage && $permission->permissions
>=$score)?$score=$permission->permissions:'';// si l'id de page correspond et si son score de
permission est supérieure au score en cours on l'enregistre et obtient le niveau de permission accordé
le plus élevé
        }
    }

    if($egaliteStrict==true){// si on souhaite une valeur de permission égale
        $results = $score==$allowedScore;// si le score de l'utilisateur est strictement
égale à celui demandé on retourne true
    }else{// si on ne souhaite pas d'égalité stricte

        $results = ($score>=$allowedScore);// si le score de l'utilisateur est suffisant on
retourne true
    }
}
return $results;
}

```

- *Fonction qui masque le nom des classes par des alias dans l'url. Elle peut être étendue aux méthodes.*

```

/**(M) Fonction qui à partir d'un alias redonne le nom de classe telle que défini dans
Security::CLASS_ALIAS. La fonction sert à masquer le nom des classes dans les url en utilisant des
alias. Le mode est personnalisable par Security::USE_STRICT_CLASS_ALIAS qui à false autorise les alias
et nom de classe
 * (O) String du nom de classe correspondant à l'alias
 * (I) prends 1 parametre 1 string de l'alias
 * @param string alias nomde l'alias
 */
public static function classAlias($alias){
    return @self::alias($alias,self::CLASS_ALIAS,self::USE_STRICT_CLASS_ALIAS);
}

```

- *Méthode qui sécurise les données utilisateurs au travers de la fonction HtmlEntities(). D'autres fonctions peuvent être ajoutées.*

```

/**(M) Méthode qui applique des méthodes pour sécuriser les variables Post et SESSION
 * (O) rien
 * (I) rien
 */
private static function sanitizePostAndSession(){
    @self::methodsToArrayValues($_POST,self::SECURITY_METHOD);
    @self::methodsToArrayValues($_SESSION,self::SECURITY_METHOD);
}
/**(M) Méthode qui applique des méthodes pour sécuriser un array ou un string
 * (O) rien
 * (I) prends 1 parametre le string ou l'array de valeur à sécuriser
 * @param string string ou array des valeurs à sécuriser
 */
public static function sanitizeUserData($data){
    @self::methodsToArrayValues($data,Security::SECURITY_METHOD);
}

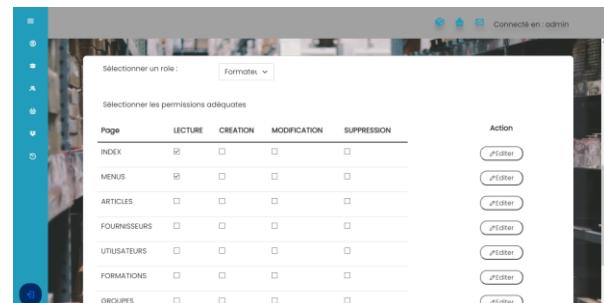
```



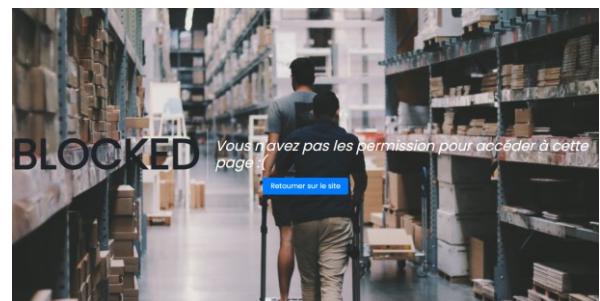
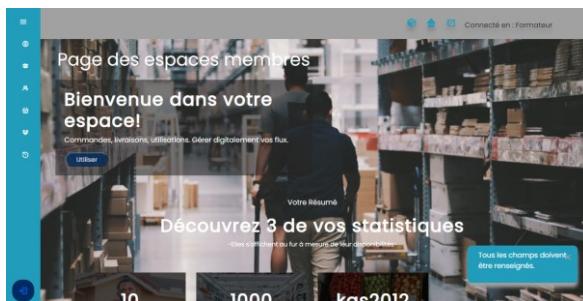
# CHAPITRE 6 – PRÉSENTATION DU JEU D'ESSAI

## I. GESTION DES PERMISSIONS :

On est connecté en admin et on donne les permissions de lecture de la page index et menus au rôle formateur et lui refuse les autres permissions.



On est connecté sous le rôle formateur. Nous avons bien accès à la page index et non aux pages d'administration telle que la page de gestion des utilisateurs. A la tentative de connexion on est renvoyé vers une page d'erreur.



## II. NOUVELLE SORTIE DE MARCHANDISES

On valide une sortie de 5 articles tapis sur le bon 12.

ID	Référence	Libelle	Prix	Qte	Montant TTC
3	tapis	tapis	10.00	5	50.00

On retrouve bien nos 5 tapis en sortie par l'utilisateur test qui est un formateur.



# CHAPITRE 7 – VEILLE SUR LES VULNÉRABILITÉS DE SÉCURITÉ

## I. LES INJECTIONS SQL

### Réalisation

Les injections sql consistent à insérer du code dans les requêtes SQL au travers des inputs de formulaires pour en modifier les comportements et les faire exécuter côté serveur. Elles sont utilisées ainsi pour exécuter des LMD non voulus et voler des données de la BDD.

**Un premier correctif consiste à utiliser les requêtes paramétrées** soit en SQL dur avec « SET @variable = » ou par l'intermédiaire des requêtes préparées de PDO qui utilise cette technique.

La solution a été portée par PDO.

### Description

```
$articleid = $_GET['article'];
$query = "SELECT * FROM articles WHERE articleid = '$articleid';"
```

Un attaquant peut envoyer une requête qui sera exécutée avec la requête, comme ci-dessous:

```
'union+select+1,version(),3'
```

La requête ci-dessus modifiera le code comme suit:

```
$query = "SELECT * FROM articles WHERE articleid = '1'+union+select+1,version(),3'"
```

## II. SCRIPTS INTERSITES OU FAILLES XSS

### Réalisation

Les failles XSS consistent à insérer un script étranger dans la page côté client afin de le faire exécuter par le système de l'utilisateur. Elles sont utilisées pour voler des informations d'identification ou le contenu des cookies.

**Comme premier correctif on a appliqué la méthode htmlEntities().**

### Description

L'extrait de code vulnérable suivant peut être exploité pour lancer une attaque XSS:

```
String s = request.getParameter("string");
String strng;
```

Lorsque l'attaquant passe des codes tels que <script> alert ('XSS'); </script> à cette page Web, il sera exécuté et affichera «XSS». Cela montre comment des codes malveillants externes peuvent être injectés et exécutés pour causer des dommages.

Vous pouvez empêcher de telles attaques en suivant les étapes ci-dessous:

- Filtrer toutes les données externes: si vous filtrez toutes les données entrantes et sortantes de votre site Web, vous pouvez arrêter la plupart des attaques XSS
- Fonctions existantes: PHP a quelques fonctions que vous pouvez utiliser telles que `htmlentities()`, `utf8_decode()` et `strip_tags()`. L'utilisation de ces fonctions vous fera gagner du temps et, comme elles sont intégrées, elles auront moins de vulnérabilité



## I. LA FIXATION DE SESSION

Elle consiste pour l'attaquant à créer une session et à envoyer son id de session à sa victime qui lorsqu'elle se connectera se connectera sous cet id et validera la session. Une recommandation pour pouvoir authentifier les sessions valides implique l'usage parallèle de cookies afin d'identifier la machine locale. Cela demandera à l'attaquant un effort supplémentaire . **Comme premier correctif utilisé, à chaque connexion on détruit systématiquement la session** en générant une nouvelle.

## II. FAILLE INCLUDE

### Réalisation

**Comme correctif :** aucun appel de fichier n'utilise de variables fournies par l'utilisateur.  
**Nous utilisons une classe Autoload** avec des méthodes et propriétés privées pour l'inclusion de fichiers. Les noms de classes sont fournis par la méthode `spl_autoload_register` et seul les classes des dossiers spécifiés sont appelées.

**Un système d'alias et un routeur ont également été mis en place** afin de masquer les noms de classes et dossiers.

### Description

Dans cette attaque, on peut afficher ou exécuter des fichiers et des dossiers cruciaux qui devraient être inaccessibles à tout le monde sauf aux administrateurs. Ces fichiers peuvent résider en dehors des dossier racine et avec des autorisations de fichier incorrectes ou une erreur de codage, ces fichiers peuvent être vulnérables à un accès non autorisé.

L'exemple de code ci-dessous permettra les requêtes qui peuvent accéder aux fichiers:

```
$file = $_GET['file'];
include($file);
```

## III. FALSIFICATION DE DEMANDES INTERSITES OU FAILLES CSRF

### Réalisation

**Comme correctif : on a privilégié l'utilisation de POST** à la place des GET dans le formulaire, l'utilisation d'un triple token (SESSION, cookies,URL) obtenue à partir d'un token généré et sauvegardé en BDD par session est également en phase de développement, ainsi que le cryptage aléatoire par sessions des noms de variables POST.

### Description

Il s'agit de faire exécuter à l'internaute des actions non désirées en profitant des priviléges utilisateurs dont il bénéficie. Cette pratique peut prendre la forme de GET envoyés via une url qui sera adressée et cliquée par l'utilisateur.

L'utilisation de HTTPS comme protocole pour le tunnel de transmission de données a également été recommandée.



## IV. ATTAQUES PAR FORCE BRUTE

### Réalisation

Comme correctif ultérieur le nombre de tentative peut être enregistré en bdd pour chaque compte pour pouvoir les limiter à 3.

### Description

On teste chaque combinaison possible d'un mot de passe/identifiant donné afin de se connecter au service ciblé.

## V. CRYPTAGE DE MOTS DE PASSE ET RECOMMANDATIONS DE SECURITE

**Pour l'instant le procédé de cryptage utilise la méthode de cryptage AES() proposée par MySQL où il est stocké en donnée de type VARBINARY(). Le rajout de password\_hash() est prévu.**

password\_hash() génère un hachage de soixante caractères basé sur BCRYPT (algorithme CRYPT\_BLOWFISH). Il prend 3 paramètres : le mot de passe, l'algorithme de hashage et le

coût. Le mot de passe crypté ne peut plus être retrouvé mais vérifié via password\_verify().

```
$hash = \password_hash($password, PASSWORD_DEFAULT);

if (\password_verify($password, $hash)) {
    // Authenticated.
    if (\password_needs_rehash($hash, PASSWORD_DEFAULT)) {
        // Rehash, update database.
    }
}
```

## VI. LE DETOURNEMENT OU VOL DE SESSION

Le pirate réussit à obtenir les identifiants de session de l'utilisateur et les utilise pour tromper le site afin d'obtenir l'accès aux priviléges utilisateurs de la session piratée.

**Comme premier correctif, une vérification des variables d'environnement telle que l'adresse IP, l'user-agent... sera apportée. Les variables en cours seront comparées à celles utilisées par la dernière session utilisateur qui auront été préalablement sauvegardées en BDD afin de les authentifier.**



# CHAPITRE 8 – SITUATIONS DE TRAVAIL AYANT NÉCESSITÉ UNE RECHERCHE

## I. DEFAUT DE REWRITE-ENGINE SUR LE SERVEUR LINUX :

[https://ubiq.co/tech-blog/how-to-enable-mod\\_rewrite-in-xampp-wamp/](https://ubiq.co/tech-blog/how-to-enable-mod_rewrite-in-xampp-wamp/)

L’application et le pattern MVC se base sur l’utilisation du module de réécriture d’URL d’Apache afin de fixer un seul point d’entrée qui est le fichier index.php. Ce module est un composant essentiel de l’application. Cependant sur le serveur local sur lequel devait être installé l’application, le module de réécriture n’était pas activé.

**J’ai pu obtenir les commandes cli sur bash et les instructions de configuration de apache pour pouvoir activer le module rewrite :**

By default, Apache prohibits using an .htaccess file to apply rewrite rules, so first you need to allow changes to the file. Open the default Apache configuration file using nano or your favorite text editor:

```
$ sudo nano /etc/apache2/sites-available/000-default.conf
```

Inside that file, you will find a <VirtualHost \*:80> block starting on the first line. Inside of that block, add the following new block so your configuration file looks like the following. Make sure that all blocks are properly indented:

```
/etc/apache2/sites-available/000-default.conf

<VirtualHost *:80>
    <Directory /var/www/html>
        Options Indexes FollowSymlinks
        AllowOverride All
        Require all granted
    </Directory>
    ...
</VirtualHost>
```

```
#cd mods-enabled  
#sudo a2enmod rewrite
```

## II. DEFAUT DE ROLLBACK DE PDO EN CAS D’ECHEC D’UNE TRANSACTION :

<https://stackoverflow.com/questions/23851360/pdocommit-success-or-failure>

Certains use-cases nécessitent la manipulation de deux tables ayant une relation cif. Pour respecter les contraintes d’intégrité fonctionnelle plusieurs requêtes SQL doivent être exécutées. Par exemple la mise à jour d’un rôle dont la clé primaire est absorbée par la table groupe nécessite de faire un insert dans role, un update dans groupe puis role et un delete dans role pour respecter les contraintes d’intégrité fonctionnelle à moins de désactiver la vérification des clés étrangères avec « SET FOREIGN\_KEY\_CHECKS =



0; ». L'utilisation d'une transaction est devenue nécessaire afin de s'assurer de la cohérence des données selon les propriétés ACID.

- Atomicité : une transaction se fait au complet
- Cohérence : l'état des données avant et après doivent être valides selon l'ensemble des règles définies(logique métier, cif...)
- Isolation : une transaction est indépendante d'une autre transaction
- Durabilité : une fois une transaction exécutée elle est enregistrée dans la BDD

Bien que la transaction puisse être écrite en dure dans le SQL , PDO propose des méthodes pour le faire qui constituent un choix valide. Cependant, l'absence de rollback par PDO lors d'erreurs mettait à mal les principes des propriétés ACID et donc la validité des données. **J'ai pu trouver la solution à ce problème en mettant PDO en mode ERRMODE\_EXCEPTION.** En effet pour que PDO déclenche le rollback en cas d'erreur, ses méthodes doivent pouvoir retourner une erreur.

### III. DEFAUT DE PERMISSION POUR L'UTILISATION DE PROCEDURES STOCKEES UTILISANT DU LMD :

<https://stackoverflow.com/questions/26015160/deterministic-no-sql-or-reads-sql-data-in-its-declaration-and-binary-logging-i>

L'application utilise des triggers mais aussi des procédures et fonctions stockées dans sa conception. Cependant MySQL me renvoyait ce message d'erreur lors de leurs insertions en base de données :

```
1418 (HY000) at line 10185: This function has none of DETERMINISTIC, NO SQL, or READS SQL  
DATA in its declaration and binary logging is enabled (you *might* want to use the less safe  
log_bin_trust_function_creators variable)
```

Cette solution a été proposée sur le site Stackoverflow pour la résolution du problème:

```
SET GLOBAL log_bin_trust_function_creators = 1;
```



# CHAPITRE 9 – EXTRAITS DES SITES ANGLOPHONES UTILISÉS DANS LA RECHERCHE

Défaut de rewrite-engine sur le serveur linux : [https://ubiq.co/tech-blog/how-to-enable-mod\\_rewrite-in-xampp-wamp/](https://ubiq.co/tech-blog/how-to-enable-mod_rewrite-in-xampp-wamp/)

## Traduction

### 1.Autoriser le mod\_rewrite

Pour permettre à Apache de gérer les rewrite rules, nous devons activer le mod\_rewrite. Il est déjà installé par défaut mais désactivé. Utiliser la commande a2enmod pour autoriser le module.

Cela va activer le module ou vous prévenir qu'il est déjà activé. Redémarrer apache pour rendre les modifications effectives.

Par défaut Apache interdit l'usage du .htaccess pour appliquer des règles de réécriture, nous allons devoir autoriser ces modifications. Ouvrez le fichier de configuration d'apache en utilisant nano ou votre éditeur de texte préféré. Dans le fichier, vous trouverez un bloc commençant par <VirtualHost \*:80> . Dans ce bloc rajoutez le bloc ci-dessous afin qu'il ressemble à ceci. Assurer que chaque bloc soit correctement indenté.

## Original

### Step 1 – Enabling mod\_rewrite

In order for Apache to understand rewrite rules, we first need to activate mod\_rewrite. It's already installed, but it's disabled on a default Apache installation. Use the a2enmod command to enable the module:

```
$ sudo a2enmod rewrite
```

Copy

This will activate the module or alert you that the module is already enabled. To put these changes into effect, restart Apache:

```
$ sudo systemctl restart apache2
```

Copy

By default, Apache prohibits using an .htaccess file to apply rewrite rules, so first you need to allow changes to the file. Open the default Apache configuration file using nano or your favorite text editor:

```
$ sudo nano /etc/apache2/sites-available/000-default.conf
```

Copy

Inside that file, you will find a <VirtualHost \*:80> block starting on the first line. Inside of that block, add the following new block so your configuration file looks like the following. Make sure that all blocks are properly indented:

```
</VirtualHost>
<Directory /var/www/html>
    Options Indexes FollowSymlinks
    AllowOverride All
    Require all granted
</Directory>
```

...

</VirtualHost>

AllowOverride None

and change them to

AllowOverride All

Also read : How to Change Default Timezone in Apache/PHP

Now, create an .htaccess file in the web root:

```
$ sudo nano /var/www/html/.htaccess
```

Copy

Add this line at the top of the new file to activate the rewrite engine.

```
/var/www/html/.htaccess
```

RewriteEngine on



## Défaut de rollback de PDO en cas d'échec d'une transaction :

<https://stackoverflow.com/questions/23851360/pdocommit-success-or-failure>

### Traduction

La documentation PHP sur PDO ::commit() indique que la méthode retourne vraie en cas de succès et faux en cas d'échec. Est-il question de succès ou d'échec de l'exécution des requêtes entre beginTransaction() et commit() ?

La solution réside essentiellement dans le fait de mettre PDO en mode exception, tandis que l'utilisation d'un try -catch n'est pas nécessaire. Cependant ton code est correcte, il y a nul besoin de le changer si ton objectif est simplement de faire un rollback(retour à l'état antérieur) en cas d'échec tant que tu auras cette ligne d'inscrite.

`$dbh->setAttribute( PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION )`

Dans le cas d'un échec, le script s'arrête, la connexion se ferme et mysql sera heureux d'annuler pour toi la transaction.

Dans le cas où ton besoin est de réaliser le rollback de façon manuelle, tu devrais le faire correctement, pas comme ce qui est indiqué dans les autres réponses données.

Veille à bien :

- Capturer Exception et non PDOException, tant que la nature de l'exception à l'origine de l'interruption n'importe pas.
- Rejeter une exception après le rollback pour être notifié du problème.
- T'assurer que le moteur de ta base de données supporte les transactions (ex : pour MySQL le moteur devrait être InnoDB et non MyISAM)

La liste à cocher provient de mon article que tu pourras trouver utile sur bien des aspects.

### Original

#### PDO::commit() success or failure

Asked 7 years, 11 months ago Modified 4 years, 5 months ago Viewed 10k times

The PHP PDO::commit() documentation states that the method returns TRUE on success or FALSE on failure. Does this refer to the success or failure of the statement executions between beginTransaction() and commit()?

For example, from the documentation:

```
$dbh->beginTransaction();
$stmt = "INSERT INTO fruit (name, colour, calories) VALUES (?, ?, ?)";
$stmt->prepare($sql);

foreach ($fruits as $fruit) {
    $stmt->execute([
        $fruit->name,
        $fruit->colour,
        $fruit->calories,
    ]);
}

$dbh->commit();
```

If any of the above executions fail, will the commit() method return false due to the "all-or-nothing basis" of atomic transactions?

The key part is to set PDO in exception mode, while having try-catch only to do a rollback is unnecessary. Thus, your code is all right, no need to change it if all you want is rollback on failure, as long as you have this line somewhere:

```
$dbh->setAttribute( PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION );
```

In case of failure the script will be terminated, connection closed and mysql will be happy to roll back the transaction for you.

In case you still want to rollback manually, you should be doing it properly, not like it is said in the other answers. Make sure that

- you are catching `Exception`, not `PDOException`, as it doesn't matter what particular exception aborted the execution
- you are re-throwing an exception after rollback, to be notified of the problem
- also that a table engine supports transactions (i.e. for Mysqli it should be InnoDB, not MyISAM).

This checklist is taken from [my article](#) which you may find useful in this or many other aspects as well.

## Défaut de permission pour l'utilisation de procédures stockées utilisant du LMD :

<https://stackoverflow.com/questions/26015160/deterministic-no-sql-or-reads-sql-data-in-its-declaration-and-binary-logging-i>

### Traduction

Il y a deux solutions pour régler ce problème

1. Exécute le code suivant dans la console MySQL
2. Ajoute cette ligne dans le fichier de configuration mysql.ini

Ces réglages soustrait la vérification des fonctions non-déterministes. Les fonctions non déterministes sont des fonctions qui modifient les données (ex : les requêtes d'Update, d'Insert ou de Delete).

NB : Si la journalisation binaire n'est pas activée, ces réglages ne s'appliqueront pas.

### Original

While importing the database in mysql, I have got following error:

```
1418 (HY000) at line 10185: This function has none of DETERMINISTIC, NO SQL, or READS SQL DATA in its declaration and binary logging is enabled (you *might* want to use the less safe log_bin_trust_function_creators variable)
```

I don't know which things i need to change. Can any one help me how to resolve this?

There are two ways to fix this:

- 356 1. Execute the following in the MySQL console:  
`SET GLOBAL log_bin_trust_function_creators = 1;`
2. Add the following to the mysql.ini configuration file:  
`log_bin_trust_function_creators = 1;`

The setting relaxes the checking for non-deterministic functions. Non-deterministic functions are functions that modify data (i.e. have update, insert or delete statement(s)). For more info, see [here](#).

Please note, if binary logging is NOT enabled, this setting does not apply.

[Binary Logging of Stored Programs](#)

If binary logging is not enabled, `log_bin_trust_function_creators` does not apply.

`log_bin_trust_function_creators`

This variable applies when binary logging is enabled.



# ANNEXES

- ❖ Questionnaire de spécification
- ❖ Cartographie des triggers, fonctions et procédures stockées
- ❖ Présentation client
- ❖ Mentions légales



# Questionnaire de spécification

---

1. Quels sont les objectifs de l'application ? //cette partie sert à lister les fonctionnalités de base ou de départ objet de l'application
  - a. Quelles sont les avantages/fonctionnalités voulues ?
2. Qui utilisera l'application et comment ? //cette partie sert à faire ressortir les fonctionnalités ou caractéristiques qui peuvent apparaître à l'usage
  - a. Qui saisit les données ?
  - b. Qui les consultent ?
  - c. les traitent ?
  - d. sous quels formats ?
  - e. Comment sont saisies les données ?
  - f. Comment sont-elles utilisées ?
  - g. Lister les exemples d'usages courant :
    - a. Cas 1 :
    - b. Cas 2 :
    - c. ...
  - h. Lister les exemples d'usages particuliers :
    - a. Cas particulier 1 :
    - b. Cas particulier 2 :
    - c. ...
3. Quelle est la qualité des données //cette partie sert à définir le dictionnaire des données point de départ du MCD
  - a. (types ex : « texte », natures ex : « référence », longueur...) qui sont saisies ?
  - b. A quels critères de validité (restrictions) doivent-elles se conformer ?
  - c. Quelles données doivent être présentées ?
  - d. Comment doivent-elles être présentées ?

Que doit proposer l'application en dehors de son usage ? //fonctionnalités en dehors de l'usage même de l'application.



# CARTOGRAPHIE DES TRIGGERS, FONCTIONS ET PROCÉDURES STOCKÉES

## Fonctions

Procédures stockées				
Nom	Action	Type	Retourne	
check_mail_f	Éditer Exécuter Exporter Supprimer	FUNCTION	int(11)	
flux_by_article	Éditer Exécuter Exporter Supprimer	FUNCTION	int(11)	
getUserByRole	Éditer Exécuter Exporter Supprimer	FUNCTION	json	
qte_com_from_one_recep_and_art	Éditer Exécuter Exporter Supprimer	FUNCTION	int(11)	
qte_recep_from_one_com_and_art	Éditer Exécuter Exporter Supprimer	FUNCTION	int(11)	
stock_by_article	Éditer Exécuter Exporter Supprimer	FUNCTION	int(11)	
stock_by_article_by_centre	Éditer Exécuter Exporter Supprimer	FUNCTION	int(11)	
sum_entree_by_article	Éditer Exécuter Exporter Supprimer	FUNCTION	int(11)	
sum_entree_by_article_by_centre	Éditer Exécuter Exporter Supprimer	FUNCTION	int(11)	
sum_entree_by_centre	Éditer Exécuter Exporter Supprimer	FUNCTION	int(11)	
sum_livraison_by_article	Éditer Exécuter Exporter Supprimer	FUNCTION	int(11)	
sum_livraison_by_article_by_centre	Éditer Exécuter Exporter Supprimer	FUNCTION	int(11)	
sum_livraison_by_articleby_centre	Éditer Exécuter Exporter Supprimer	FUNCTION	int(11)	
sum_sortie_by_article	Éditer Exécuter Exporter Supprimer	FUNCTION	int(11)	
sum_sortie_by_article_by_centre	Éditer Exécuter Exporter Supprimer	FUNCTION	int(11)	
total_entree_by_article	Éditer Exécuter Exporter Supprimer	FUNCTION	int(11)	
total_entree_by_article_by_centre	Éditer Exécuter Exporter Supprimer	FUNCTION	int(11)	

Déclencheurs				
Nom	Table	Action	Temps	Événement
check_mail	user	Éditer Exporter Supprimer	BEFORE INSERT	
no_del_com_livr	détails_commande	Éditer Exporter Supprimer	BEFORE DELETE	
no_del_com_over_livr	détails_commande	Éditer Exporter Supprimer	BEFORE DELETE	
no_del_livr	détails_reception	Éditer Exporter Supprimer	BEFORE DELETE	
no_insert_com_over_livr	commande	Éditer Exporter Supprimer	BEFORE INSERT	
no_insert_livr_sup_com	détails_reception	Éditer Exporter Supprimer	AFTER INSERT	
no_upd_com_over_livr	détails_commande	Éditer Exporter Supprimer	BEFORE UPDATE	
no_update_livr_sup_com	détails_reception	Éditer Exporter Supprimer	AFTER UPDATE	

## Procédures

Procédures stockées				
Nom	Action	Type	Retourne	
checkMails	Éditer Exécuter Exporter Supprimer	PROCEDURE		
create_database	Éditer Exécuter Exporter Supprimer	PROCEDURE		
create_tables1	Éditer Exécuter Exporter Supprimer	PROCEDURE		
drop_table	Éditer Exécuter Exporter Supprimer	PROCEDURE		
flux_Commande_current_month_by_user	Éditer Exécuter Exporter Supprimer	PROCEDURE		
flux_Commande_current_month_by_user_by_article	Éditer Exécuter Exporter Supprimer	PROCEDURE		
flux_Commande_current_year	Éditer Exécuter Exporter Supprimer	PROCEDURE		
flux_Commande_current_year_by_user	Éditer Exécuter Exporter Supprimer	PROCEDURE		
flux_Commande_current_year_by_user_by_article	Éditer Exécuter Exporter Supprimer	PROCEDURE		
flux_Commande_par_centre_date	Éditer Exécuter Exporter Supprimer	PROCEDURE		
flux_reception	Éditer Exécuter Exporter Supprimer	PROCEDURE		
flux_reception_current_year	Éditer Exécuter Exporter Supprimer	PROCEDURE		
flux_reception_par_centre_date	Éditer Exécuter Exporter Supprimer	PROCEDURE		
flux_sortie_current_month_by_user	Éditer Exécuter Exporter Supprimer	PROCEDURE		
flux_utilisation_month_user	Éditer Exécuter Exporter Supprimer	PROCEDURE		
flux_utilisation_par_centre_date	Éditer Exécuter Exporter Supprimer	PROCEDURE		
flux_utilisation_par_centre_date_par_mouvement	Éditer Exécuter Exporter Supprimer	PROCEDURE		
flux_utilisation_par_centre_date_par_utilisateur	Éditer Exécuter Exporter Supprimer	PROCEDURE		
getUserByRole	Éditer Exécuter Exporter Supprimer	PROCEDURE		
get_centre	Éditer Exécuter Exporter Supprimer	PROCEDURE		
jeu_dessai_1	Éditer Exécuter Exporter Supprimer	PROCEDURE		
pero_entre_sur_sortie_user_par_centre	Éditer Exécuter Exporter Supprimer	PROCEDURE		
preferred_article_month_user	Éditer Exécuter Exporter Supprimer	PROCEDURE		
statut_des_articles	Éditer Exécuter Exporter Supprimer	PROCEDURE		
statut_des_articles_par_id	Éditer Exécuter Exporter Supprimer	PROCEDURE		
truncate_table	Éditer Exécuter Exporter Supprimer	PROCEDURE		



AATTI

## APPLICATION DE GESTION DE STOCK



AUTEUR :  
Christian  
Marais

Stagiaire AFPAR  
DWWM 21-22

Ce document contient des éléments graphiques et de design créés et édités soumis aux droits d'auteurs. Toutes modifications, reproductions partielles ou complètes sont interdites sans autorisation expresse de l'auteur. Seul, est autorisée la consultation par les destinataires du document ou les personnes directement impliquées dans le projet à savoir : le personnel de l'AATI et l'AFPAR.

Le document contient également des éléments graphiques soumis à des licences (photos, typographies, iconographies ..) auprès des tiers sous-nommé freepik.com et canva.com et des éléments graphiques et de contenu soumis aux droits d'auteurs auprès de l'AATI (logo, screenshot de site web) et l'AFPAR (logo) autorisés ici seulement dans le cadre de cette utilisation et aux fins de la mission qui a été confiée. Les renseignements concernant les licences sont disponibles sur les sites indiqués.

AUTEUR :

Christian  
Marais

Stagiaire AFPAR  
DWWM 21-22

# Sommaire

- 
- 04 Équipe
  - 05 Objectifs
  - 06 Cahier des charges
  - 07 .Fonctionnalités
  - 08 .Spécifications techniques
  - 09-10 .Charte graphique
  - 11 L'application Web
  - 12 .Le login
  - 13 .La gestion des utilisateurs
  - 14 .La gestion des produits
  - 15 Remerciements



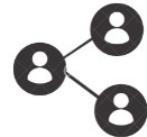
# L'Équipe



**Chan-Kui Liam**  
Responsable technique



**Christian Marais**  
Développeur



**Beta-testeur**

AUTEUR :  
**Christian  
Marais**

Stagiaire AFPAR  
DWWM 21-22

# Les Objectifs



## AMELIORER L'EXPÉRIENCE

Augmenter le confort pédagogique

Disponibilité des données

Facilité et instantanéité des demandes de fournitures

## ASSURER LA FIABILITÉ ET L'INTÉGRITÉ DES DONNÉES

Améliorer la confiance dans les données

Eliminer les erreurs

Eviter les pertes de registres

Contrôler l'historique des registres

## DIGITALISATION DE LA GESTION DE STOCK

Pousser davantage l'accessibilité

Consultation accessible à tous les acteurs

Evolution vers un système centralisé de gestion de stock pour les différents sites

AUTEUR :  
Christian  
Marais

Stagiaire AFPAR  
DWWM 21-22

# CAHIER DES CHARGES



AUTEUR :  
Christian  
Marais

Stagiaire AFFPAR  
DWWM 21-22



# Fonctionnalités

## LISTE DETAILLÉE

- 1.Créer et gérer des formations.
- 2.1Créer et gérer des comptes utilisateurs
- 2.2 Gérer des permissions à travers les rôles :
  1. Super-Admin,
  2. Responsable de l'organisme,
  3. Formateurs,
  4. Responsable logistique
- 3.Créer et gérer des groupes.
- 4.Créer et gérer des domaines de formation
- 5.Ajouter des éléments dans le stock
- 6.Retirer des éléments du stock.
- 7.Consulter l'historique du stock
- 8.Avoir des statistiques du stock
- 9.Envoie un mail au responsable de l'organisme pour lui indiquer qu'on a besoin d'un certain nombre de produit.

AUTEUR :  
Christian  
Marais

Stagiaire AFPAR  
DWWM 21-22

PAGE | 10

# Spécifications techniques

## MOYENS EXISTANTS

Moyens matériels : Infrastructure local	Disponible
Plateforme d'hébergement : Serveur local	Disponible
Logiciels disponibles:	Non-imposé

## TECHNOLOGIES APPROCHÉES

Les technologies : Sql, Php8,HTML5,CSS3, Javascript	Inclus
L'architecture : MVC, procédurale.	Inclus
Les plateformes de développement : LARAGON (Mysql).	Inclus
Les logiciels : Visual Studio Code, PhpMyAdmin	Inclus



AUTEUR :  
Christian  
Marais

Stagiaire AFPAR  
DWWM 21-22

PAGE | 24

# Charte graphique



Accueil

Nos Formations

Offres d'emploi

Le Centre

Contact



NOS  
**FORMATIONS SELON LES  
FILIÈRES ICI :**

- [Service à la personne](#) ▾
- [Agricole](#) ▾
- [Mediation Socioculturelle](#) ▾
- [Sécurité et Hygiène](#) ▾
- [Restauration](#) ▾
- [Education](#) ▾
- [Gestion commerciale et administrative](#) ▾



## LE CENTRE

**FORMATEURS  
EXPERTS DANS  
PLUSIEURS  
DOMAINES**

**8 FILIÈRES.**

**11 FORMATIONS.**

**EN INITIAL OU EN  
ALTERNANCE !**

[En savoir plus](#)

AUTEUR :

Christian  
Marais

Stagiaire AFPAR  
DWWM 21-22

**TAUX DE  
RÉUSSITE  
ÉLEVÉ.**



[En savoir plus](#)

**UN CENTRE  
CERTIFIÉ.**

**Qualiopi** ➔  
processus certifié



**BUREAU  
VERITAS**

[En savoir plus](#)



# Charte graphique

## Identité visuel

### Inspiration

La direction artistique sera harmonisée sur la charte graphique disponible et celle utilisée pour le site internet. Elle aura une direction intuitive et minimaliste.

The screenshot shows the AATI website's header with the logo 'AATI' and links for Accueil, Nos Formations, Offres d'emploi, Le Centre, and Contact. Below the header, there's a menu for 'NOS FORMATIONS SELON LES FILIÈRES ICI:' with options like Service à la personne, Agricole, Mediation Socioculturelle, Sécurité et Hygiène, Restauration, Education, and Gestion commerciale et administrative. To the right is a cartoon illustration of a person working on a laptop. The main content area is titled 'LE CENTRE' and contains three boxes: one about trainers being experts in multiple fields, another showing a 93% success rate, and one about being certified, featuring the Qualiopi logo and Bureau Veritas certification.

### Les polices

Les polices respectent les polices et la pâte de la typographie du site.

#### Web

Titre - Monserrat 700  
Texte - Monserrat 400

Les typographies sont repries selon les usages du site.

### Les couleurs



#219ebc

#f9c315

#161a42

1. PRIMAIRE : # 219 EBC
2. SECONDAIRE : # F9C315
3. TERTIAIRE : # 161A42

La couleur primaire sera la couleur dominante reprise pour les titres et les différents composants :

- barre de navigation
- Boutons
- Titres

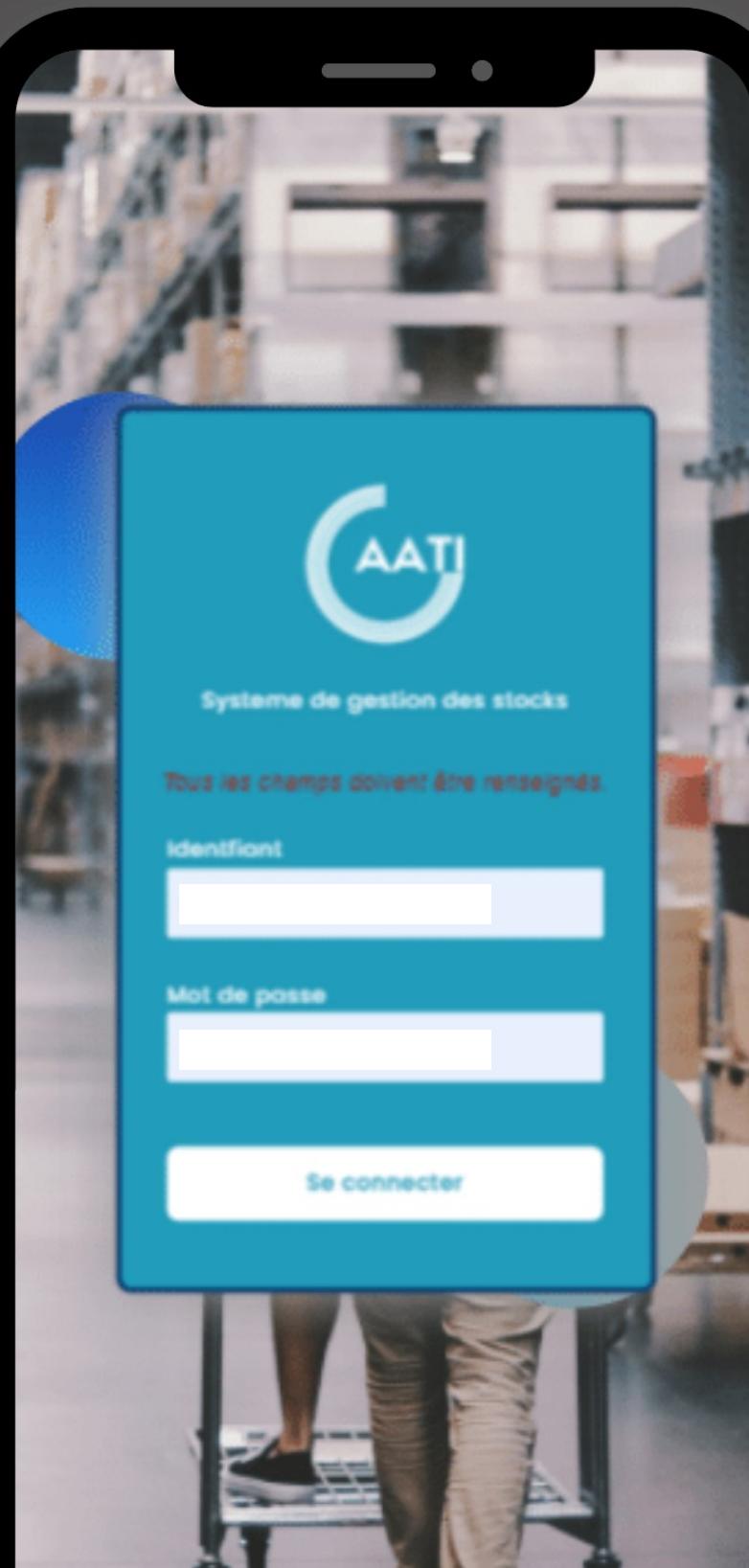
### Le logo



AUTEUR :  
Christian  
Marais

Stagiaire AFPAR  
DWWM 21-22

# Web Mobile-Desktop



# Login

Deux types d'accès :

Accès administrateurs privilégiés

Accès utilisateurs



\*Design indicatif ne reflétant pas le produit fini

## Fonctionnalités

- MENTIONS CGU
- GESTION UTILISATEUR
- GESTION DES GROUPES ET DES FORMATIONS
- CONSULTATION D'HISTORIQUE ET DE STATISTIQUES DES STOCKS
- GESTION DES FOURNITURES

- MENTIONS CGU
- RETRAIT QUANTITE FOURNITURES
- EMAILING DES DEMANDES FOURNITURES

# GESTION DES PRODUITS

La gestion des produits est divisée en deux :

Retrait des produits sur la quantité disponible du stock par les formateurs

Ajout et suppression de produits par l'administrateur;



## Fonctionnalités

**CONSULTER LES PRODUITS  
AJOUTER UNE QUANTITE  
RETRAIT DE QUANTITE  
CONSULTATION DES STOCKS**

AUTEUR :  
**Christian Marais**  
Stagiaire AFPAR  
DWWM 21-22

# GESTION DES UTILISATEURS

L'administrateur aura la possibilité de gérer et supprimer des comptes utilisateurs

## ATTRIBUTION DE RÔLE & GROUPE

### ÉDITION D'UTILISATEURS

### CONSULTATION DE L'HISTORIQUE DES ACTIONS UTILISATEURS



## Fonctionnalités

- AJOUT & SUPPRESSION  
D'UTILISATEURS  
- ÉDITION DE RÔLES

CRÉATION DE GROUPE  
AJOUT ET SUPPRESSION DE  
FORMATIONS

- CONSULTATION DES RETRAITS  
DE QUANTITE EN STOCK POUR UN  
GROUPE OU D'UN UTILISATEUR

# CALENDRIER PREVISIONNEL



AUTEUR :

Christian  
Marais

Stagiaire AFPAR  
DWWM 21-22

Points de rendez-vous :

D-0 : Livrable

D-2 semaines: Début phase de test et de correction de bug

D-2 semaines :

Livrable application fonctionnelle

D-8 semaines : phase de développement

D-9 semaines : courant de la semaine  
démarrage de la phase de conception

D-9 semaines : fin de la phase de  
spécifications et étude de faisabilité

D-10 semaines : Phase de spécifications

# MERCI À VOUS



AUTEUR :  
Christian  
Marais  
Stagiaire AFPAR  
DWWM 21-22

## MENTIONS LEGALES

---

Ce document contient des éléments graphiques et de design créés et édités soumis aux droits d'auteurs. Toutes modifications, reproductions partielles ou complètes sont interdites sans autorisation expresse de l'auteur. Seul, est autorisée la consultation par les destinataires du document ou les personnes directement impliquées dans le projet à savoir : le personnel de l'AATI et l'AFPAR.

Le document contient également des éléments graphiques soumis à des licences (photos, typographies, iconographies ..) auprès des tiers sous-nommés freepik.com et canva.com et des éléments graphiques et de contenu soumis aux droits d'auteurs auprès de l'AATI (logo, Screenshot de site web) et de l'AFPAR (logo) autorisés ici seulement dans le cadre de cette utilisation et aux fins de la mission qui a été confiée. Les renseignements concernant les licences sont disponibles sur les sites indiqués.

