


DESCRIPTION D'UNE MISSION BTS SIO			
Prénom – Nom	Quentin Coqueran	N° mission	2
Option	SLAM		
Situation		Formation	
Lieu de réalisation	Campus Montsouris 2 Rue Lacaze – 75014 PARIS		
Période de réalisation	Décembre 2019		
Modalité de réalisation	VÉCUE		

Intitulé de la mission	Titre de la mission
	Mission de sécurisation de l'application RAPID
Description du contexte de la mission	Description en 2 à 3 lignes maxi
	Le but de cette mission est la sécurisation de deux éléments de L'application Registre d'Accueil du Public Informatisé de la DSPAP

Ressources et Outils utilisés	Liste des ressources disponibles et outils utilisés (Documentations, Matériels et Logiciels)
	<ul style="list-style-type: none"> - Visual Studio 2019 - Docker - Git - Ubuntu 18
Résultat attendu	Résultat attendu avec la réalisation de cette mission
	Sécurisation du mot de passe d'accès et de la récupération du mail UGO de contact
Contraintes	Contraintes : techniques budgétaires temps O.S. ou outils imposés...
	<ul style="list-style-type: none"> - Modification des prérequis de mot de passe lors de la première connexion. - Modification de la récupération du mail UGO dans le formulaire de contact. - Ajouter des mentions légales concernant la possible surveillance du site.

	Liste des intitulés du tableau de compétences (avec les références)
Compétences associées <i>(Voir tableau)</i>	A1.1.1 : Analyse du cahier des charges d'un service à produire A1.1.2 : Étude des exigences liées à la qualité attendue d'un service A1.3.2 : Accompagnement de la mise en place d'un nouveau service A2.1.1 : Accompagnement des utilisateurs dans la prise en main d'un service A3.1.1 Proposition d'une solution d'architecture A3.1.2 Prise en compte du niveau de sécurité nécessaire à une infrastructure A4.1.3 Conception ou adaptation d'une base de données A4.1.4 Gestion d'environnements de développement et de test A4.1.5 Développement, utilisation ou adaptation de composants logiciels A4.1.6 Réalisation de tests nécessaires à la validation d'éléments adaptés ou développés A5.1.1 : Recueil d'informations sur une configuration et ses éléments A5.2.1 Recueil d'informations sur une configuration et ses éléments 5.2.3 Etude d'une technologie, d'un composant, d'un outil ou d'une méthode

Description simplifiée des différentes étapes de réalisation de la mission en mettant en évidence la démarche suivie, les méthodes et les techniques utilisées
<p><u>Chapitre 1 : Prise en main et découverte du projet</u></p> <p><u>Etape :</u></p> <p>RAPID est une application web qui sert à l'enregistrement de l'accueil du public dans les différents commissariats de l'agglomération parisienne. Il est possible d'en tirer des statistiques sur la raison de la visite ou le temps d'attente.</p> <p>1.1/ Tout d'abord je clone le dossier du projet sur Gitlab avec la commande : "git clone lien_du_projet".</p> <p>1.2/ Ensuite il faut lancer les différents containers qui servent à faire fonctionner le projet dans les mêmes conditions qu'en production. Pour cela il faut se placer dans le dossier où se trouve notre fichier docker-compose.yml qui sert à configurer nos containers.</p>

```
quentin@IU19657:~/Projets/rapid/docker/debian9$ ls
config docker-compose.yml sql_dumps web
quentin@IU19657:~/Projets/rapid/docker/debian9$ docker-compose up --build
```

1.3/ Nous devons taper la commande "docker-compose up - -build" qui permet de démarrer la construction et le lancement de nos containers.

Si tout se passe bien les containers sont maintenant actifs et on peut donc consulter notre application Web via notre navigateur.

Résultat :

Le projet est prêt à être utilisé et testé

Chapitre 2 : Modification des prérequis de mot de passe

Etape :

2.1/ Les nouveaux prérequis de mot de passe à la première connexion sont :

- Une majuscule
- Une minuscule
- Un chiffre
- Minimum 8 caractères
- Maximum 25 caractères

Pour les appliquer j'ai modifié la regex existante :

```
if (preg_match('#^(?=.*[a-z])(?=.*[A-Z])(?=.*[0-9]).{8,}$#', $Mdp))
if (preg_match('#^(?=.*[a-z])(?=.*[A-Z])(?=.*[0-9]).{8,25}$#', $pass))
```

L'ancienne regex est en rouge la nouvelle en vert.

2.2/ Il ne suffit pas seulement de le modifier dans le code. J'ai dû gérer les différents affichages et le formulaire afin d'accompagner au mieux l'utilisateur dans cette démarche.

```
9      ?> <div text-align="center" style="margin-top:80px"> <?php echo("La modification a
      échoué, le mot de passe doit comprendre une minuscule, une majuscule et un 1 chiffre, et faire au minimum 8
      caractères"); ?> </div>
0 +    <div text-align="center" style="margin-top:100px"> <a
      href="nouveau_mdp.php?user_ni=<?php echo $matricule; ?>"> Réessayer </a> </div>
```

Résultat :

Le nouvel utilisateur devra renseigner un nouveau mot de passe maintenant plus sécuriser.

Chapitre 3 : Sécurisation de la récupération du mail UGO dans le formulaire de contact

Etape :

3.1/ Les réglementations de sécurité internes à la préfecture de police nous imposent d'être très minutieux sur la sécurité. Ce qui nous a amené à découvrir que le mail de contact de l'Unité de Gestion Opérationnelle (un service d'administration) était transmis en \$_POST.

C'est une faille de sécurité car un utilisateur malveillant peut injecter du SQL dans l'URL et modifier ou accéder à des données.

3.2/J'ai donc modifié le type de stockage de cette information pour la mettre en \$_SESSION car les données sont stockées côté serveur et sont donc moins sensibles que sur le client.

```
$To = htmlspecialchars($_SESSION['mail_ugo']);
```

Résultat :

La donnée sensible du mail UGO est donc maintenant plus sécurisée.

Chapitre 4 : Mentions légales et Tests

Etape :

4.1/ La suite de la mission qui m'a été confiée est de faire apparaître la mention légale qui stipule que le site internet est surveillé en permanence et que les actions des utilisateurs sont enregistrées.

"Attention ceci est un site surveillé, les traces de vos interventions sont enregistrées pendant votre connexion."

4.2/ La prochaine étape consiste à tester le processus du nouveau mot de passe. Il faut aussi vérifier le bon affichage des mentions légales et des indications de mot de passe.

4.3/ Il ne reste plus qu'à effectuer la commande git push qui va envoyer notre version locale sur le serveur GitLab.

Conclusion

Familiarisation avec un projet en production.
Meilleure compréhension de Docker et ses commandes
Utilisation de Git pour le versionning.

Productions associées	Liste des documents produits et description