ESER
ENES
SLAM2

PROJET AGORA SPRINT N°5:

CONTEXTE ET OBJECTIF :

L'association Agora souhaite disposer d'une interface pour gérer les comptes d'accès à l'application et demande de pouvoir donner des droits d'accès différents aux utilisateurs en fonction de leur rôle dans l'association.
L'association continue de confier cette mission à l'ESN Logma.
Le développement de l'application se fera dans un cadre de travail agile SCRUM.
L'administration des données de l'application ne sera bien sûr pas accessible à tous les utilisateurs.
Il convient de mettre en place un système d'authentification.
M. Sarment, responsable administratif de l'association et Product Owner de ce projet, a demandé la mise en place de l'authentification dans le sprint 5.
Il a défini 2 profils d'utilisateurs à gérer dans le back office :
- Administrateur : accès total -
Utilisateur : accès à tout sauf la gestion des utilisateurs

DESCRIPTION DE L'INCIDENT :

- **de qui émane-t-elle ?**

La demande provient de M. Sarment, responsable administratif de l'association Agora, qui agit en tant que Product Owner dans le cadre de ce projet agile.

- **À quel niveau d'habilitation ?**

- Administrateur : Accès à toutes les fonctionnalités du back office, y compris la gestion des utilisateurs.

- Utilisateur : Accès à toutes les fonctionnalités sauf celles concernant la gestion des utilisateurs.

- **Services potentiellement concernés**

  Gestion des utilisateurs : Création, modification, suppression des comptes d'accès et gestion des rôles.

  Sécurité de l'authentification : Mise en œuvre d'un système de connexion sécurisé (login/mot de passe, rôles).

  Back office : Interface d'administration pour l'association Agora.

ESER
ENES
SLAM2

- **Équipements concernés :**

  Serveur web hébergeant l'application Symfony.

  Bases de données (utilisées pour stocker les informations utilisateur).

  Infrastructure réseau (assurant la disponibilité du back office).

- **Niveau de service minimal attendu :**

  Garantir la sécurité de l'application pour tous les utilisateurs.

  Assurer une différenciation claire des droits d'accès entre les administrateurs et les utilisateurs.

  Respecter le délai fixé pour le sprint (Sprint 5).

- **Obligations du prestataire :**

  Proposer une solution conforme aux bonnes pratiques en matière de sécurité (hachage des mots de passe, gestion des sessions).

  Respecter le cadre de travail agile SCRUM.

  Documenter les fonctionnalités pour faciliter les évolutions futures.

- **Outil de gestion d'incident/demande :**

  Logiciel : VSCODE(éditeur de code), WampServer(base de données , hébergement local),

  Outil de communication : GitHub, Trello(SCRUM), Drive

Traitement de l'incident :

- **De quoi s'agit-il ?**

  Une demande d'évolution de service pour ajouter une fonctionnalité au back office.

  Cette évolution est une user story définie et priorisée dans le backlog du sprint 5.

- **Prise en charge et réponse :**

ESER
ENES
SLAM2

Analyse initiale :

- Vérification des besoins de l'association en matière de rôles et d'accès.
- Définition des permissions associées à chaque rôle.

Planification :

- Développement des composants nécessaires pour l'authentification et la gestion des rôles via Symfony (utilisation des composants Security et User Management).
- Mise en place de tests unitaires et fonctionnels pour valider la sécurité et le bon fonctionnement des nouvelles fonctionnalités.

L’incident est-il connu et documenté ?

Il s’agit d’une fonctionnalité standard dans Symfony, qui dispose d’une documentation complète.

Utilisation des composants Symfony Security et Doctrine pour le stockage des informations utilisateur.

- **Investigation :**

Analyse des fonctionnalités actuelles de l'application pour intégrer la gestion des utilisateurs.

Vérification de la sécurité et des performances des nouvelles fonctionnalités avant déploiement.