**Université Cheikh Anta Diop**

****

École Supérieure Polytechnique Département Génie Informatique

**Management Sécurité**

**Projet de programmation sécurisée**

*Partie 1 – Charte du projet (soumettre en PDF) [05 mars 2024, 23h59 (UTC)]*

| **Prénom** | **Nom** | **Classe** |
| --- | --- | --- |
| *Ibrahima Diagne* | *Seck* | *M2 GLSI* |
| *Oumou Hawa* | *Diallo* | *M2 GLSI* |
| *Ndeye Moussou* | *Sidibé* | *M2 SRT* |

# Partie 1 – Charte

* Le nom de travail de notre système est la gestion des stagiaires
* Dans ce projet, nous utiliserons comme langage de programmation : PHP.

Un langage que nous avons eu à étudier dans notre formation et que nous avons pu mettre en pratique que ce soit dans des projets d'école ou de stages, tel que l'application de gestion des classes et de l’emploi du temps.

* Le lien vers le dépôt de contrôle de version que nous utiliserons pour le développement du logiciel est le suivant :

<https://github.com/UCAD-ESP/projet-de-programmation-securisee>

* Notre équipe est constituée de :

| Membres | | Email | | GitHub |
| --- | --- | --- | --- | --- |
| Ibrahima Diagne | Seck | ibrahimadiagneseck@esp.sn | | [lien](https://github.com/ibrahimadiagneseck) |
| Oumou Hawa | Diallo | oumouhawadiallo@esp.sn | | [lien](https://github.com/oumouhawadiallo) |
| Ndeye Moussou | Sidibé | ndeyemoussousidibe@esp.sn | | [lien](https://github.com/Ndeyemoussou) |

* Notre plan pour une réunion de groupe hebdomadaire est le suivant :

Nous nous rencontrons tous les samedi soir, entre 20h et 22h, pour discuter de l'état d'avancement de votre projet.

# Proposition :

* L’objectif du projet est de mettre en place une plateforme qui permet de gérer les stages, de la demande à l’obtention du stage.
* Les principales caractéristiques du système seront de permettre de faire un suivi complet de ces stagiaires en implémentant :
* un module qui permettra la connexion des utilisateurs.
* un module qui permettra de gérer les rôles des utilisateurs.
* un module qui permettra d’enregistrer un grand nombre de demandes de stage.
* un module qui permettra la visualisation à ces stagiaires.
* un module qui permettra la survie de ces stagiaires.
* Pour notre système de gestion de stages, les éléments de sécurité essentiels à intégrer sont :
* **Autorisation :** Le système appliquera une politique d'autorisation appropriée pour contrôler l'accès des utilisateurs aux différentes fonctionnalités. Par exemple, un DAC pourrait être utilisé pour permettre aux administrateurs de gérer les demandes de stage.
* **Authentification :** Le système exigera une authentification des utilisateurs pour accéder à la plateforme avec l'utilisation de mots de passe pour le personnel ainsi que des clés d'accès pour les administrateurs.
* **Audit :** Le système enregistrera toutes les actions effectuées, telles que la soumission ou la modification des demandes de stage, afin d'établir la responsabilité en cas de besoin.
* **Confidentialité et intégrité :** Le système veillera à ce que les informations sensibles comme les données personnelles des stagiaires soient protégées contre tout accès non autorisé ou toute altération.
* La description narrative du système que nous voudrions concevoir :

Les difficultés rencontrées dans la prise en charge et le suivi des stagiaires, ainsi que le manque de visibilité sur leur progression et leur statut, soulignent la nécessité d'une solution centralisée et automatisée pour faciliter ces processus.

Nous envisagerons un système de gestion de stages entièrement automatisé, ce système fournira une plateforme centralisée et conviviale pour gérer l'ensemble du processus de stage, depuis l'inscription des stagiaires jusqu'à la fin de stage grâce aux fonctionnalités précédemment cités. Nous devrions aussi permettre au personnel administratif de suivre efficacement chaque étape du processus de stage. Cela garantira une meilleure prise en charge des stagiaires, en fournissant une visibilité accrue sur leur statut et leurs progrès.

En ce qui concerne la sécurité, le système intégrera des mécanismes robustes d'authentification et d'autorisation pour protéger les données sensibles des stagiaires. Les informations personnelles seront stockées de manière sécurisée et conformément aux réglementations sur la confidentialité des données grâce à des moyens tels que la cryptographie.

# Partie 2 – Document sur les exigences

Votre document sur les exigences fournit une proposition complète pour le système que votre équipe va développer. Il doit contenir les cinq sections suivantes :

## Objectif du système. En 3 ou 4 paragraphes, expliquez l'objectif de votre système. La base de cette explication doit être le résumé d'une page du système que vous avez rédigé dans la partie 1.

## Mettez ce résumé à jour si nécessaire, en fonction des exigences fonctionnelles et des objectifs de sécurité que vous développez dans ce document.

L’objectif du système est de permettre la gestion efficiente des stagiaires. Pour cela, nous allons mettre en place une plateforme qui permet de gérer ces stagiaires : de la demande de stage jusqu’à son obtention, en passant sa suivie.

Le système devra permettre en effet la traçabilité complète de ces stagiaires. Pour ce faire

* Le stagiaire devra pouvoir être enregistré dans le système avec leurs informations personnelles, ainsi que leur CV.
* Les administrateurs doivent pouvoir gérer les comptes des utilisateurs et leur rôle, attribuer des missions aux stagiaires, suivre leur progression, affecter les stagiaires un encadrant.
* Les stagiaires doivent pouvoir accéder à leur profil, consulter les missions qui leur sont assignées.

## Exigences fonctionnelles.

## Établissez une liste d'exigences fonctionnelles pour le système que vous concevez. Pour les besoins de ce projet, une exigence fonctionnelle comprend les données suivantes :

| **Exigences fonctionnelles** | **Type d'utilisateur** | **Actifs** | **Importance (MoSCoW)** | **User Story (INVEST)** |
| --- | --- | --- | --- | --- |
| Ajouter des utilisateurs | Administrateurs | Les coordonnées personnelles, les mots de passe, les rôles et autorisations de l’utilisateur | Essentielle: La capacité d'ajouter des utilisateurs dans le système est essentielle pour maintenir la base de données des utilisateurs à jour et permettre à de nouveaux utilisateurs d'accéder au système.  Devrait avoir: Cette fonctionnalité est importante pour assurer une gestion efficace des comptes utilisateur et faciliter l'intégration de nouveaux membres dans l'organisation.  Pourrait avoir: Des fonctionnalités supplémentaires telles que la définition de rôles et de permissions peuvent être envisagées pour une version future du système, mais ne sont pas indispensables pour l'ajout de base des utilisateurs.  Ne devrait pas avoir: Des fonctionnalités avancées, telles que la personnalisation des profils utilisateur ou la gestion avancée des autorisations, peuvent être considérées pour une version future, mais ne sont pas nécessaires pour la fonctionnalité de base d'ajout des utilisateurs par les administrateurs. | Pouvoir ajouter des utilisateurs dans le système. |
| Gérer les authentifications et autorisations | Administrateurs | Les mots de passe, les rôles et autorisations de l’utilisateur. | Essentiel: La gestion des accès au système est essentielle pour assurer la sécurité et la confidentialité des données.  Devrait avoir: Une gestion efficace des utilisateurs et de leurs accès améliore l'expérience utilisateur et la productivité.  Pourrait avoir: Un confort supplémentaire dans la gestion des comptes peut rendre l'utilisation du système plus conviviale, mais n'est pas indispensable pour sa fonctionnalité de base.  Ne devrait pas avoir: Les fonctionnalités avancées d'authentification et d'autorisation peuvent être envisagées pour une version future du système, mais ne sont pas critiques pour sa version actuelle. | Pouvoir attribuer des rôles et des autorisations aux utilisateurs. |
| Enregistrer les demandes de stage. | Administrateurs | Les documents et coordonnées du stagiaire. | Essentielle: L'enregistrement des stagiaires est essentiel pour suivre les ressources humaines et pour assurer la gestion efficace des effectifs.  Devrait avoir: La possibilité d'enregistrer de nouveaux stagiaires est importante pour maintenir à jour la base de données des ressources humaines et pour faciliter la communication et la collaboration avec les stagiaires.  Pourrait avoir: Les documents et coordonnées des stagiaires sont utiles pour faciliter leur intégration et leur suivi, mais ne sont pas indispensables pour l'enregistrement initial.  Ne devrait pas avoir: Les fonctionnalités avancées, telles que la gestion des tâches spécifiques des stagiaires, peuvent être envisagées pour une version future, mais ne sont pas critiques pour la fonctionnalité de base de l'enregistrement des stagiaires. | Pouvoir enregistrer un nouveau stagiaire. |
| Consulter son profil et ses missions | Stagiaires | Les missions | Essentielle: La possibilité pour les stagiaires de consulter leur profil et leurs missions est essentielle pour qu'ils puissent suivre leurs progrès et effectuer leurs tâches de manière efficace.  Devrait avoir: L'authentification pour accéder au profil et aux missions est importante pour garantir la sécurité des données personnelles et des informations sensibles liées aux missions.  Pourrait avoir: La consultation des missions permet aux stagiaires de mieux comprendre leurs responsabilités et leurs objectifs, mais peut être considérée comme une fonctionnalité supplémentaire par rapport à l'authentification et la consultation du profil.  Ne devrait pas avoir: Des fonctionnalités avancées de gestion des missions, telles que la modification en temps réel ou la collaboration avec d'autres utilisateurs, peuvent être envisagées pour une version future, mais ne sont pas indispensables pour la fonctionnalité de base de consultation du profil et des missions par les stagiaires. | Pouvoir s’authentifier et consulter ses missions |
| Ajouter des missions | Encadrant | Les missions | Essentielle: L'ajout de missions par les encadrants est essentiel pour définir les objectifs et les tâches à accomplir par les stagiaires, contribuant ainsi au bon déroulement des activités.  Devrait avoir: La capacité d'affecter des missions aux stagiaires est importante pour assurer une répartition équilibrée des tâches et une utilisation efficace des ressources humaines.  Pourrait avoir: La consultation des missions par les encadrants peut être utile pour suivre l'avancement des travaux et vérifier que les objectifs sont atteints, mais n'est pas aussi critique que l'ajout et l'affectation initiale des missions.  Ne devrait pas avoir: Des fonctionnalités avancées de gestion des missions, telles que la priorisation ou la planification détaillée, peuvent être envisagées pour une version future, mais ne sont pas indispensables pour la fonctionnalité de base d'ajout et d'affectation des missions par les encadrants. | Pouvoir affecter des missions aux stagiaires |
| Affecter des demandes de stages | Administrateur | Les données relatives aux stagiaires | Essentielle: La capacité d'affecter des stagiaires à des encadrants est essentielle pour organiser efficacement le travail au sein de l'organisation, en veillant à ce que chaque stagiaire soit supervisé et encadré adéquatement.  Devrait avoir: Cette fonctionnalité est importante pour garantir une répartition équilibrée des stagiaires entre les encadrants, optimisant ainsi l'utilisation des ressources humaines disponibles.  Pourrait avoir: La possibilité de consulter les affectations des stagiaires par les encadrants peut être utile pour suivre les tâches et les responsabilités de chacun, mais n'est pas aussi cruciale que la capacité d'affecter initialement les stagiaires.  Ne devrait pas avoir: Des fonctionnalités avancées, telles que la gestion détaillée des affectations ou la modification en temps réel, peuvent être envisagées pour une version future, mais ne sont pas indispensables pour la fonctionnalité de base d'affectation des stagiaires à des encadrants. | Pouvoir affecter un stagiaire à un encadrant. |
| Clôturer un stage | Encadrant | les informations sur le stage (date début et fin, appréciations) | Essentielle: La capacité de clôturer un stage en attribuant des appréciations est essentielle pour évaluer le travail accompli par le stagiaire et fournir des retours constructifs pour son développement professionnel.  Devrait avoir: Cette fonctionnalité est importante pour formaliser la fin du stage et documenter les performances du stagiaire, ce qui peut être utile pour les évaluations futures ou les références professionnelles.  Pourrait avoir: La possibilité de consulter les appréciations attribuées aux stagiaires peut être utile pour les encadrants et les administrateurs afin de suivre les progrès des stagiaires et d'identifier les domaines d'amélioration, mais n'est pas aussi cruciale que la capacité de clôturer le stage.  Ne devrait pas avoir: Des fonctionnalités avancées, telles que la gestion détaillée des appréciations ou la génération automatisée de rapports d'évaluation, peuvent être envisagées pour une version future, mais ne sont pas nécessaires pour la fonctionnalité de base de clôture du stage par les encadrants. | Pouvoir clôturer le stage en attribuant les informations du stage tel que la date de clôture et les appréciations, etc. |

## Analyse des menaces :

Identifiez les menaces qui pèsent sur votre système.

* **Attaques par force brute sur l'authentification :**

Tout système est assujetti aux attaques par brute-force, y compris la nôtre, celle du gestion des stages. Il y a une possibilité que les attaquants compromettent le compte des utilisateurs en essayant de deviner ou de brute-forcer les identifiants de connexion.

**Motivations :**

Les attaquants pourraient utiliser des techniques d'usurpation d'identité pour se faire passer pour des utilisateurs légitimes du système, leur permettant ainsi d'accéder à des informations sensibles ou d'effectuer des actions malveillantes au nom de ces utilisateurs.

Les attaquants peuvent être motivés par le vol d'informations sensibles, le sabotage ou la perturbation des opérations d'une organisation.

**Ressources et capacités :**

Les attaquants peuvent utiliser des outils automatisés pour effectuer des attaques par force brute ou exploitant des listes de mots de passe courants ou des dictionnaires. Ils peuvent également déployer des réseaux de zombies (botnets) pour augmenter leur capacité de traitement et échapper à la détection.

* **Altération ou suppression de données :**

Notre système de gestion de stage court aussi le risque qu’une personne pourrait modifier ou supprimer des données stockées dans le système de manière accidentel ou non, entraînant ainsi des perturbations importantes dans les opérations de l'organisation ou compromettant l'intégrité des informations.

**Motivations :**

Les personnes malveillantes peuvent être motivées par des intentions malveillantes, telles que la vengeance, le sabotage ou la fraude.

**Ressources et capacités :**

Les personnes ayant un accès légitime aux systèmes peuvent être impliquées dans de telles attaques, et elles peuvent exploiter leur connaissance du système pour manipuler les données de manière subtile et difficile à détecter.

* **Attaques par déni de service (DDoS) :**

Des attaquants pourraient lancer des attaques par déni de service dans le but de perturber ou de bloquer l'accès de notre système pour les utilisateurs légitimes.

**Motivations :**

Les attaquants peuvent être motivés par des raisons idéologiques, financières ou simplement pour perturber les opérations du système ou pour entraîner une interruption des services, une perte de productivité ou des dommages à la légitimité.

**Ressources et capacités :**

Les attaquants peuvent louer des services de botnet sur le dark web ou compromettre des milliers d'appareils connectés pour mener des attaques DDoS massives. Ils peuvent également exploiter des vulnérabilités dans les protocoles réseau pour amplifier leurs attaques.

* **Injections SQL :**

Les attaquants pourraient exploiter les vulnérabilités des formulaires de saisie de données de notre système pour injecter des commandes SQL malveillantes.

**Motivations :**

Les attaquants peuvent chercher à voler des données sensibles, à modifier des informations ou à compromettre l'intégrité du système, ce qui leur permettrait de voler des données sensibles stockées dans le système, telles que les CV des stagiaires, les évaluations des stages ou d'autres informations confidentielles. Ces données pourraient être utilisées à des fins de fraude, de chantage ou de compromission de la vie privée des utilisateurs.

**Ressources et capacités :**

Les attaquants peuvent utiliser des outils automatisés pour identifier et exploiter des vulnérabilités SQL, en utilisation de frameworks d'attaque automatisés qui peuvent automatiser le processus d'exploitation des vulnérabilités SQL, tels que SQLMap, Havij, ou Burp Suite, pour élaborer des requêtes SQL malveillantes spécifiques qui exploitent les vulnérabilités trouvées dans les applications ou les systèmes cibles. ainsi que des techniques d'ingénierie sociale pour inciter les utilisateurs à divulguer des informations sensibles.

* **Exploitation des messages d'erreurs :**

Les attaquants peuvent exploiter les messages d'erreurs générés par notre système pour obtenir des informations sensibles sur sa configuration ou sur les données manipulées.

**Motivations :**

Pour affiner les attaques ultérieures, telles que l'injection SQL ou le piratage des sessions. Les attaquants peuvent également utiliser ces messages pour profiler le système et identifier des failles de sécurité potentielles.

**Ressources et capacités :**

Les attaquants peuvent utiliser des outils d'analyse automatisés pour examiner les messages d'erreurs et identifier des failles de sécurité potentielles.

* **Injections de fichiers malveillants :**

Les attaquants peuvent tenter d'insérer des fichiers malveillants dans la base de données en exploitant des vulnérabilités dans nos formulaires de téléchargement (CV) ou nos champs de saisie de données.

**Motivations :**

Ces fichiers peuvent contenir des logiciels malveillants tels que des virus, des chevaux de Troie ou des ransomwares, et peuvent être utilisés pour compromettre le système ou voler des données sensibles.

**Ressources et capacités :**

Les attaquants peuvent utiliser des techniques d'ingénierie sociale pour inciter les utilisateurs à télécharger des fichiers malveillants, ainsi que des outils d'automatisation pour scanner et exploiter des vulnérabilités dans les formulaires de téléchargement de fichiers.

## Objectifs de sécurité :

| **Actif** | **Parties Prenantes** | **Valeur pour les Parties Prenantes** | **Analyse des Préjudices** | **Objectif de Sécurité** | **Caractéristiques de l’objectif** | **Analyse des faisabilités** |
| --- | --- | --- | --- | --- | --- | --- |
| Coordonnées personnelles des utilisateurs | Administrateurs, Encadrants, Stagiaires | Pour les Administrateurs:  \* Assurer une authentification sécurisée des utilisateurs.  \* Maintenir la confidentialité et l'intégrité des données personnelles dans le système.  Pour les Encadrants:  \* Permettre de s’authentifier et un suivi efficace des stagiaires.  Pour les Stagiaires:  \* Permettre de s’authentifier et de consulter ses missions qui lui sont attribuées. | Accès non autorisé, Modification, ajout ou suppression non autorisée | Le système doit empêcher l'accès non autorisé aux données et la modification, ajout ou suppression non autorisée des données. | Confidentialité, Intégrité | Réalisable |
| Mots de passe | Administrateurs, Encadrants, Stagiaires | Garantir un mécanisme d'authentification sécurisé pour tous les utilisateurs, assurant ainsi la confidentialité des données d'identification et la protection contre les attaques par force brute et la divulgation non autorisée des mots de passe. | Attaque par force brute, Divulgation non autorisée | Le système doit empêcher les attaques par force brute et la divulgation non autorisée des mots de passe. | Confidentialité | Réalisable |
| Rôles et autorisations | Administrateurs | Assurer un contrôle d'accès efficace et une séparation appropriée des tâches pour les administrateurs, garantissant ainsi la confidentialité et l'intégrité des données en empêchant l'accès non autorisé aux fonctionnalités et l'élévation non autorisée des privilèges. | Accès non autorisé, Élévation de privilèges | Le système doit empêcher l'accès non autorisé aux fonctionnalités et l'élévation non autorisée des privilèges. | Confidentialité, Intégrité | Réalisable |
| Documents et coordonnées des stagiaires | Administrateurs, Encadrants | Faciliter le suivi des stagiaires et la communication entre les administrateurs et les encadrants en assurant l'intégrité des documents et des coordonnées des stagiaires. Cela garantit que les informations sont fiables et exactes, tout en empêchant toute altération ou destruction non autorisée de ces données. | Altération, Destruction | Le système doit empêcher l'altération et la destruction non autorisées des documents et des coordonnées. | Intégrité, Confidentialité | Réalisable |
| Missions | Encadrants, Stagiaires | Permettre la planification efficace des stages et le suivi des progrès en assurant l'intégrité des missions. Cela garantit que les objectifs et les tâches assignés aux stagiaires restent intacts et non altérés, tout en empêchant toute suppression non autorisée des missions, ce qui contribue à la fiabilité et à la cohérence des informations. | Altération, Suppression | Le système doit empêcher l'altération et la suppression non autorisées des missions. | Intégrité | Réalisable |
| Informations sur les stages (date début/fin, appréciations) | Encadrants, Stagiaires | Assurer un suivi précis des stages et des évaluations des stagiaires pour les encadrants et les stagiaires en garantissant la confidentialité et l'intégrité des informations sur les stages. Cela permet de protéger les données sensibles contre l'accès non autorisé et la modification non autorisée, assurant ainsi la fiabilité et la précision des évaluations et des informations sur les stages. | Accès non autorisé, Modification non autorisée | Le système doit empêcher l'accès non autorisé aux informations et la modification non autorisée des informations. | Confidentialité, Intégrité | Réalisable |
| Les données relatives aux stagiaires | Encadrants, Stagiaires | Encadrants Suivi précis des progrès des stagiaires pour évaluer leurs performances pendant le stage.  Stagiaires Consultation facile des missions attribuées et des évaluations pour suivre leur progression. | Risque d'accès non autorisé aux données personnelles des stagiaires.<br> Risque de modification ou de suppression non autorisée des informations sur les stages et les évaluations. Risque de divulgation non autorisée des données sensibles des stagiaires. | Garantir la confidentialité, l'intégrité et la disponibilité des données relatives aux stagiaires. | Confidentialité, Intégrité | Réalisable |