**Cahier des charges - Projet de détection des failles et des bugs en ligne**

**1.Introduction :** Le Projet consiste à concevoir et développer un site web qui contient

un outil à télécharger nommé ‘’ Cyber Armor ‘’.Cet outil doit scanner les vulnérabilités

d’un site web , les vulnérabilités de la base de données et les vulnérabilités du réseau.

**2.Objectifs du projet :**

* Développer un site web.
* Créer un outil de sécurité 'Cyber Armor'.
* Fournir un téléchargement facile de l'outil.
* Assurer la sécurité des utilisateurs.
* Fournir des rapports détaillés.

**3.Fonctionnalités principales :**

* Page d’accueil présentant une introduction sur notre outil détaillée de notre outil "Cyber Armor".
* Page ‘’Nos services’’ avec des informations complètes sur les services que nous offrons via l'outil, y compris des descriptions détaillées de chaque service.
* Page ‘’Téléchargement’’ offre un lien de téléchargement pour l'outil.
* **Analyse de sites web** : L’application doit être capable d’analyser un site web pour détecter les vulnérabilités potentielles.
* **Rapport de vulnérabilité** : L’application doit générer un rapport détaillé des vulnérabilités trouvées, y compris leur niveau de gravité.

**4. Contraintes techniques :**

* Développement du site en utilisant des technologies web modernes pour assurer une expérience utilisateur optimale. Les technologies recommandées incluent HTML5, CSS3, JavaScript.
* Développement de l'outil 'Cyber Armor' en Python, utilisation des bibliothèques spécialisées pour la détection des vulnérabilités, comme OWASP ZAP ou Wapiti.
* Le site web doit fournir un moyen sûr et facile de télécharger l'outil 'Cyber Armor'.

**5. Livrables attendus :**

* **Langages de programmatio**n : Le site web doit être développé en utilisant HTML, CSS, JavaScript pour le front-end et Python ou Java pour le back-end. L'outil de sécurité "Cyber Armor" doit être écrit en Python.
* **Sécurité** : Le site web et l'outil doivent respecter les normes de sécurité pour protéger les informations des utilisateurs et garantir la confidentialité des rapports de vulnérabilité.
* **Base de données :** L'outil "Cyber Armor" doit être capable de scanner les vulnérabilités dans différents types de bases de données. L’outil doit être capable de détecter les vulnérabilités courantes dans ces systèmes de gestion de bases de données, comme l'injection SQL, l'exposition de données sensibles, et les mauvaises configurations de sécurité.
* **Compatibilité** : L'outil "Cyber Armor" doit être compatible avec les systèmes d'exploitation les plus courants (Windows, MacOS, Linux).
* **Performance** : L'outil doit être capable de scanner et d'analyser les sites web rapidement et efficacement, sans causer de ralentissement notable du système de l'utilisateur.
* **Documentation** : Tous les codes sources doivent être bien documentés pour faciliter la maintenance et les futures améliorations.

**6. Calendrier de développement :**

* **Semaine 1-2 :** Collecte des informations et des données d'entraînement.
* **Semaine 3-4 :** Conception et implémentation des algorithmes nécessaires .
* **Semaine 5-7 :** Développement de l'interface utilisateur et intégration avec les algorithmes.
* **Semaine 8-9 :** Développement de l’application web.
* **Semaine 10-11 :** Tests d’outil.
* **Semaine 12 :** Finalisation de la documentation et préparation de la présentation finale.

**7. Validation et approbation :** Le cahier des charges doit être validé et approuvé par l'équipe enseignante ou les superviseurs du projet avant le début du développement. Tout au long du projet, des réunions régulières avec les superviseurs permettront de suivre l'avancement et de s'assurer que le projet respecte les spécifications établies.