A23 – Sécurité des applications - Travail pratique 6 (15%)

Objectifs du TP

Ce travail pratique (TP) vise à évaluer votre compréhension des notions vues en cours à savoir :

- Tests de pénétration avec OWASP ZAP;
- Audit de code avec SonarCloud;
- Modélisation des menaces avec MTMT.

Contexte

Ce travail doit être réalisé individuellement ou par groupe de deux étudiants. La remise est effectuée sur Léa et doit contenir :

- Un rapport au format Word ou PDF.

Date de remise

Votre travail doit être remis au plus tard le dimanche 25 février 2024 à 23h59.

Critères d'évaluation

Votre travail doit respecter l'ensemble des critères suivants :

- Le rapport contient tous les éléments attendus;
- -10 % par jour de retard;
- Note de 0 si le travail est remis après le retour à l'ensemble du groupe ou si le travail a été plagié en tout ou en partie.

Grille d'évaluation

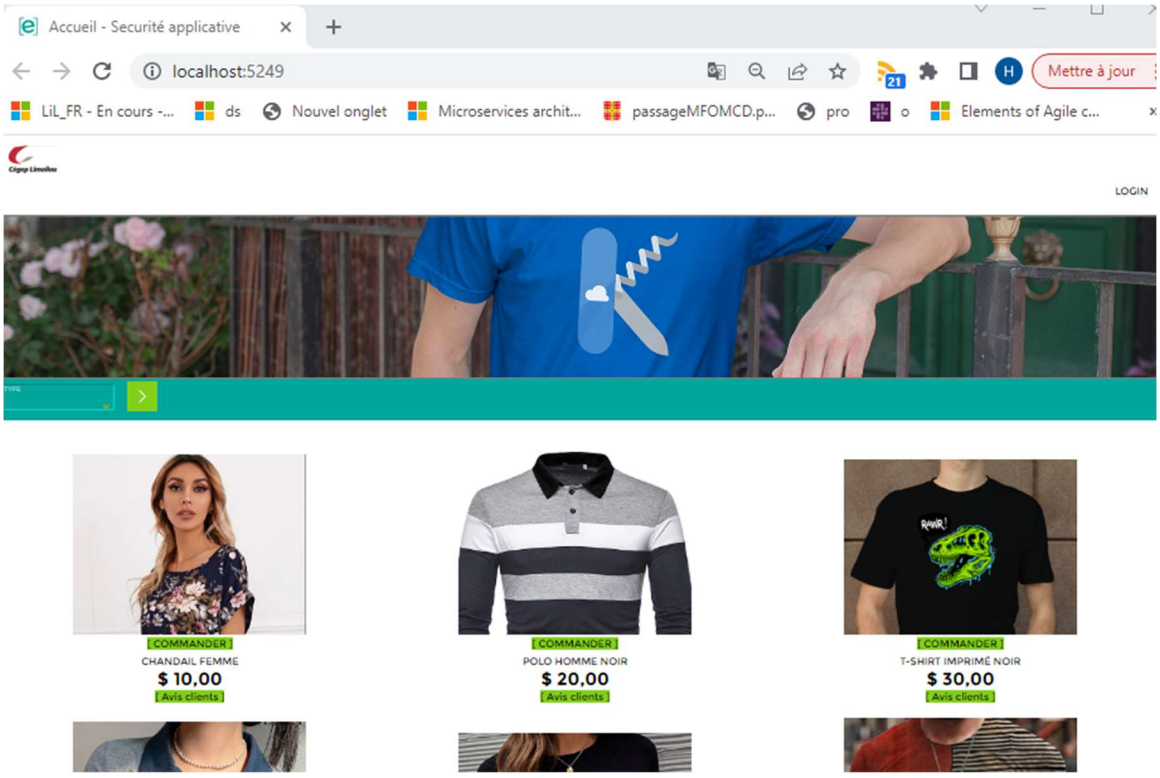
	Excellent	**Fonctionnel**	**Minimal**	**Insuffisant**
Capacité 1 : S'approprier les notions de sécurité informatique	• Les failles de sécurité sont parfaitement présentées; • Les conséquences d'un exploit sont parfaitement identifiées et décrites; • Les facteurs de risques sont parfaitement identifiés et décrits	• Les failles de sécurité sont bien présentées; • Les conséquences d'un exploit sont bien identifiées et décrites; • Les facteurs de risques sont bien identifiés et décrits	• Les failles de sécurité sont partiellement présentées; • Les conséquences d'un exploit sont partiellement identifiées et décrites; • Les facteurs de risques sont partiellement identifiés et décrits	• Les failles de sécurité sont peu détaillées; • Les conséquences d'un exploit sont peu décrites; • Les facteurs de risques sont peu identifiés et décrits
Capacité 2 : Sécuriser les applications	• Les failles dans le code ont été identifiées parfaitement; • Les correctifs à mettre en place ont été parfaitement définis; • La modélisation des menaces est correctement réalisée et documentée.	• Les failles dans le code ont été identifiées correctement; • Les correctifs à mettre en place ont été définis correctement; • La modélisation des menaces est presque correctement réalisée et documentée.	• Les failles dans le code ont été partiellement identifiées; • Les correctifs à mettre en place ont été partiellement définis; • La modélisation des menaces est partiellement réalisée et documentée.	• Les failles dans le code sont rarement identifiées; • Les correctifs à mettre en place sont rarement définis; • La modélisation des menaces est rarement réalisée et documentée.
Capacité 3 : Tester la sécurité des applications	• Identification de tous les éléments qui doivent être testés dans l'application; • Les tests de pénétration sont correctement réalisés et documentés; • L'analyse statique du code source est correctement réalisée et documentée.	• Identification de presque tous les éléments qui doivent être testés dans l'application; • Les tests de pénétration sont presque correctement réalisés et documentés; • L'analyse statique du code source est presque correctement réalisée et documentée.	• Identification partielle des éléments qui doivent être testés dans l'application; • Les tests de pénétration sont partiellement réalisés et documentés; • L'analyse statique du code source est partiellement réalisée et documentée.	• Identification insuffisante des éléments qui doivent être testés dans l'application; • Les tests de pénétration sont rarement réalisés et documentés; • L'analyse statique code source est rarement réalisée et documentée.

Mise en contexte

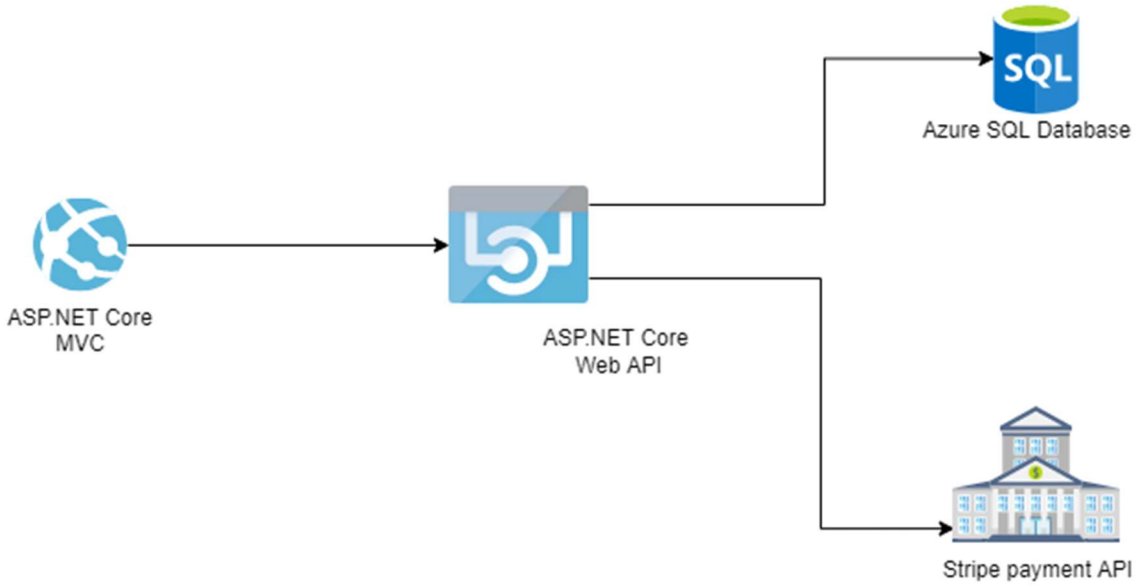
Vous avez été recruté par une entreprise commerciale qui est sur le point de lancer son site de commerce en ligne. Votre mission est d'auditer le code source de l'application en accordant une attention particulière à la sécurité. Vous devez apporter les corrections nécessaires à l'application avant que cette dernière ne soit déployée.

Il est préférable d'utiliser votre propre instance de base de données pour exécuter à l'application. Pour cela, vous devez :

- Créer une base de données Azure SQL Database;
- Modifier le fichier appsettings.json de l'API pour ajouter la chaine de connexion;
- Exécuter le script de migration (Update-Database);
- Définir les deux applications comme projets de démarrage;
- Exécuter.



L'image ci-dessous vous donne une idée de la structure de la solution :



Travail à faire

Vous devez utiliser comme projet de départ la solution initiale mise à votre disposition, sans aucune modification. Elle est jointe à ce document.

Vous devez utiliser un ensemble d'outils de sécurité pour analyser le code source de la solution (application MVC et API) et produire un document qui contient :

- Le rapport des tests de pénétration avec OWASP ZAP. Le rapport doit contenir tous les éléments d'un livrable de tests de pénétration. (4 points)
- Le rapport de sécurité (concentrez-vous uniquement sur la portion sécurité) d'analyse de SonarQube. Vous devez commenter ce rapport en mentionnant par exemple les risques auxquels l'application s'exposer et donner au moins une recommandation de correctif pouvant être mis en place; (4 points)
- Le diagramme de modélisation des menaces avec MTMT et le rapport de détection. Le Rapport doit être documenté. Vous devez vous appuyer sur l'image de la solution ci-dessus pour réaliser le travail demandé (5 points)
- En guise de conclusion, vos avis personnels sur les trois outils utilisés et la pertinence de ceux-ci dans l'amélioration de la sécurité des applications (2 points).

Bon travail!