A23 – Sécurité des applications - Travail pratique 2 (15%)

Objectifs du TP

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

- Les failles par injection;
- La protection des données;
- L'exploitation des failles par injection;
- La mise en place des contremesures.

Contexte

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

- Une vidéo explicative d'exploitation des failles par injection;
- Un rapport au format Word ou PDF;
- Le code source de l'application corrigée.

Date de remise

Votre travail doit être remis au plus tard le mardi 12 décembre à 23h59.

Critères d'évaluation

Votre travail doit respecter l'ensemble des critères suivants :

- Le code source est optimal et sans erreur;
- Le rapport contient tous les éléments attendus;
- La vidéo de démonstration est fluide, optimale et tous les membres de l'équipe ont participé et sont visibles;
- -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

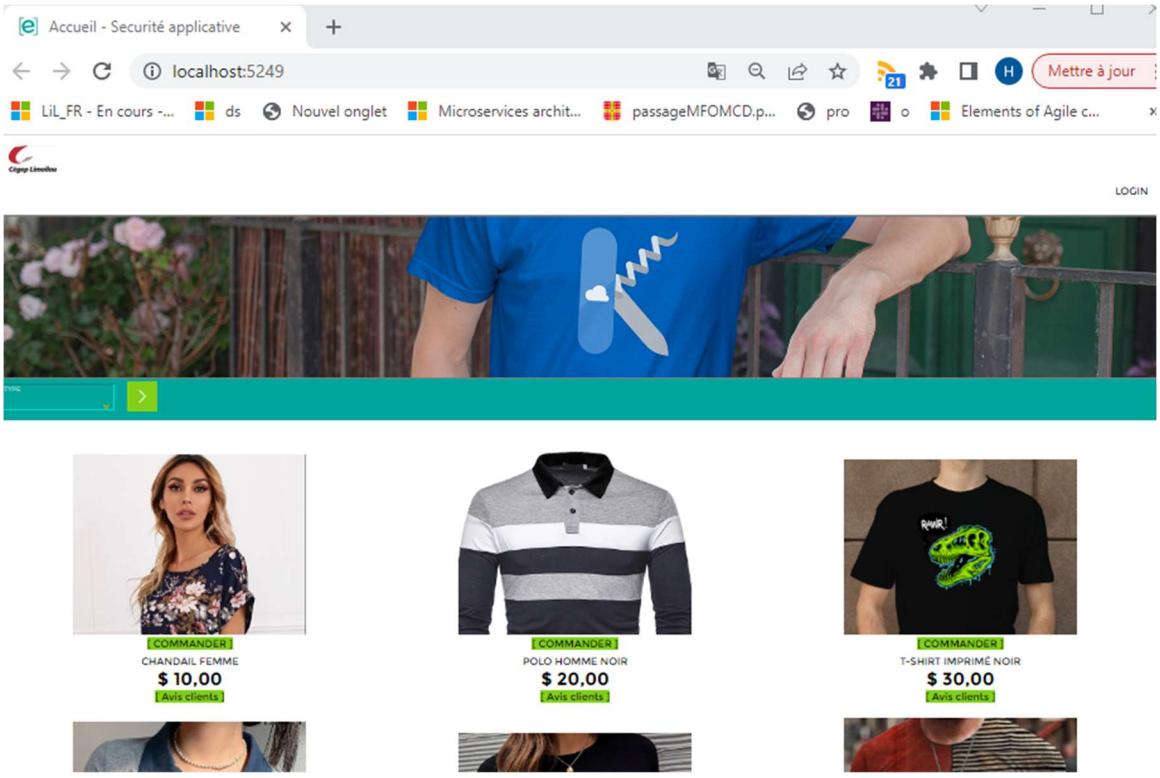
	Excellent	**Fonctionnel**	**Minimal**	**Insuffisant**
Capacité 1 : S'approprier les notions de sécurité informatique	• Les failles de sécurité sont parfaitement présentées; • Les conséquences d'un exploit sont parfaitement identifiées et décrites; • Les facteurs de risques sont parfaitement identifiés 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; • Les modifications apportées au code sont optimales.	• Les failles dans le code ont été identifiées correctement; • Les correctifs à mettre en place ont été définis correctement; • Les modifications apportées au code sont presque optimales.	• Les failles dans le code ont été partiellement identifiées; • Les correctifs à mettre en place ont été partiellement définis; • Les modifications apportées au code sont partiellement optimales.	• Les failles dans le code sont rarement identifiées; • Les correctifs à mettre en place sont rarement définis; • Les modifications apportées au code ne sont pas optimales.
Capacité 3 : Tester la sécurité des applications	• La démonstration de l'exploitation d'une faille de sécurité est optimale; • Identification de tous les éléments qui doivent être testés dans l'application; • La revue du code source est correctement réalisée.	• La démonstration l'exploitation d'une faille de sécurité est correcte; • Identification de presque tous les éléments qui doivent être testés dans l'application; • La revue du code source est presque correctement réalisée.	• La démonstration de l'exploitation d'une faille de sécurité est partiellement correcte; • Identification partielle des éléments qui doivent être testés dans l'application; • La revue du code source est partiellement réalisée.	• La démonstration de l'exploitation d'une faille de sécurité est insuffisante; • Identification insuffisante des éléments qui doivent être testés dans l'application; • La revue du code source est rarement réalisée.

Travail à faire

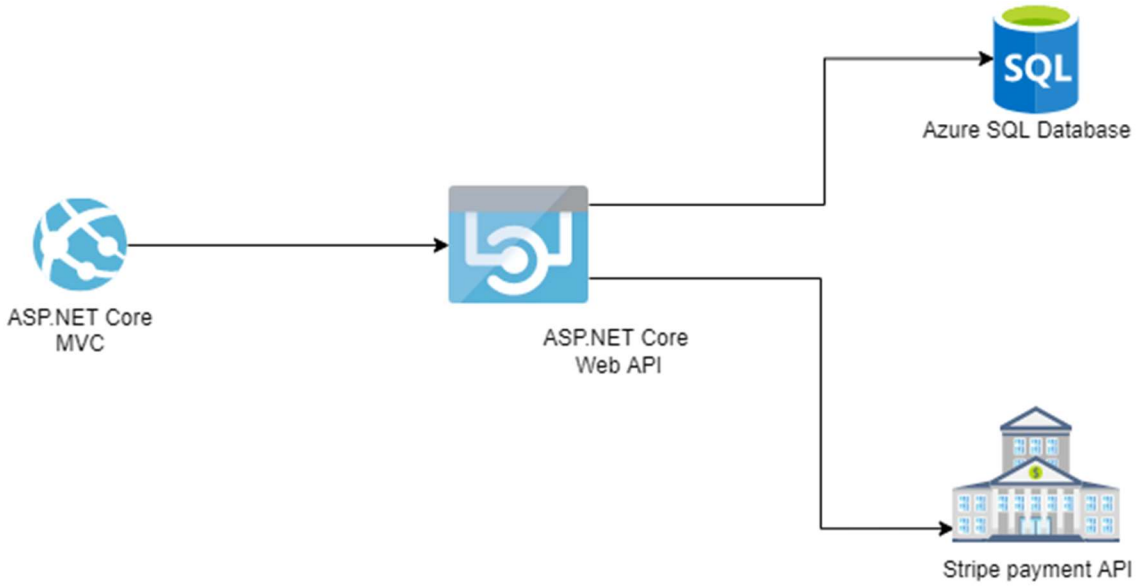
Vous avez été recruté par une entreprise commerciale qui est sur le point de lancer son site de commerce en ligne. Votre mission est d'auditer le code source de l'application en accordant une attention particulière à la sécurité. Vous devez apporter les corrections nécessaires à l'application avant que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

Il est préférable d'utiliser votre propre instance de base de données pour exécuter 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 :



Partie 1 : Injection

L'application dispose de plusieurs failles de types Injection. Votre première mission est donc d'effectuer un audit pour détecter ces failles. Il peut s'agir des failles d'injection SQL ou d'injection de script XSS.

1. Produire une capsule vidéo pour démontrer l'exploitation des failles de type injection dans l'application (au moins une faille d'injection SQL et une faille XSS). Chaque étudiant du groupe doit démontrer une faille.
2. Produire un rapport d'audit de code pour les failles d'injection de l'application. Le rapport doit contenir :
    a. Une description des failles;
    b. Les possibilités d'exploitation de ces failles;
    c. Les conséquences que ces failles peuvent avoir sur l'application;
    d. Les méthodes vulnérables de l'application et la faille identifiée pour ces méthodes;
    e. Les mesures pouvant être mises en place pour corriger la faille/mitiger les possibilités d'attaques.
3. Apporter les ajustements nécessaires à l'application pour corriger les failles d'injection que vous avez identifiées. Vous ne devez pas utiliser d'expression LINQ.

Partie 2 : protection des données

L'application manipule des données sensibles qui ne sont pas protégées. Ces données peuvent être sécurisées en utilisant le chiffrement ou le hachage. Après avoir effectué l'audit de code de l'application en vous concentrant sur la portion protection des données, vous devez :

1. Produire un rapport dans lequel :
    a. Vous spécifiez les données sensibles qui doivent être protégées et pourquoi.
    b. Vous présentez les approches qui peuvent être utilisées pour protéger les données (entre le chiffrement et le hachage) et pourquoi.
    c. Vous présentez les algorithmes et leur implémentation en .NET que vous allez utiliser pour remédier au problème et pourquoi vous avez fait le choix de ceux-ci.
2. Apportez les ajustements nécessaires à l'application pour assurer la protection des données sensibles.

Bon travail!