Travail Pratique 3

Par:

Francis Lussier

Mathew Lemonde

Marc-André Landry

Travail remis à:

Hugo St-Louis

Enseignant

Dans le cadre du cours : 420-5GE-HY

Développement d'applications E-Commerce

Gr : 00001

Cégep de Saint-Hyacinthe

15/12/2014

Table des matières

[Sécurité 3](#_Toc406073901)

# Sécurité

#1 : Hashage de password pour ne pas garder des données sensible dans la base de donnée.  
Tout d’abord, nous avons décidé de sécuriser nos comptes clients en « Hashant » leur mot de passe. Ceci à pour but d’empêcher des pirates de voir les mot de passe en clair s’ils accèdent à la base de donnée pour une raison inconnue…

#2 : Authorize et Role pour s’assure qu’il n’y ai pas de manque de contrôle d’accès au niveau fonctionnel  
En plus, les pages webs de notre site web ne sont pas toutes visibles aux clients. Il y a des pages pour les administrateurs, et ils sont les seuls à pouvoir y accédé.

#3 : Protection contre l’injection SQL et autre dans les textbox  
Aussi, notre site web de commerce est très protégé contre les attaques d’injection SQL grâce à MVC5 qui les valide toutes les entrées d’utilisateurs pour nous.

#4 : Capcha pour empecher les robots de spammer.  
Comme la plupart des sites, nous demandons aux utilisateurs de remplir un « Capcha » pour être certain que l’utilisateur est un humain et non pas un robot. Ceci à pour but d’enlever un peu de poids sur le serveur et d’avoir moins d’utilisateurs bidons dans la base de données.

#5 : Serveur qui bloque les ping pour empêcher ddos.