RÉFÉRENTIEL DE COURS

Numéro du programme :	420.B0	
Nom du programme :	Techniques de l'informatique	
Discipline :	Informatique	
Département :	Informatique	
Numéro et titre du cours :	420-5D3-JR	*Sécurité des données*
	No du cours	**Titre du cours**
Durée et pondération :	45 heures	1-2-1
	Durée du cours	**Pondération du cours**
Session :	Session 5	
Préalable(s) :	420-3D4-JR – *Technologies Web*	
Cours corequis :	Aucun	

Ce référentiel contient les informations suivantes :

1. Présentation du cours
2. Description de la cible du cours
3. Compétence(s) développée(s) dans le cours et contenus essentiels prescrits
4. Description générale de l'évaluation synthèse du cours
5. Attitudes professionnelles
6. Références
7. Remarques

Le comité de programme recommande l'approbation de ce référentiel de cours le :	**Cliquez ici pour entrer une date.**

La Direction des études approuve ce référentiel de cours.

	Cliquez ici pour entrer une date.
Signature de la Direction des études	**Date**

1. PRÉSENTATION DU COURS

Famille : Transversale

Au terme de ce cours, l'étudiant sera en mesure d'utiliser les notions avancées en base de données relationnelle : requêtes complexes, déclencheurs, procédures stockées ainsi que le rôle stratégique de l'administrateur de la base de données. Par ailleurs, l'étudiant devra appliquer des techniques de programmation sécurisées (hachage, chiffrement, …) pour protéger les données.

2. DESCRIPTION DE LA CIBLE DU COURS

À la fin de ce cours, l'étudiant aura une vue d'ensemble sur les concepts de la sécurité des données et sera en mesure de déterminer et d'utiliser des techniques de programmation sécurisées.

3. COMPÉTENCE(S) DÉVELOPPÉE(S) DANS LE COURS ET CONTENUS ESSENTIELS PRESCRITS

Code compétence :	00Q7	**Nombre d'heures total dans le programme**	90
Énoncé de la compétence :	Exploiter un système de gestion de base de données		

Cours contribuant au développement de la compétence :

Numéro du cours	Titre du cours	Session	Heures dédiées
420-2C4-JR	*Base de données relationnelle*	2	60
420-5D3-JR	*Sécurité des données*	5	30

Éléments de la compétence prescrits dans le devis ministériel	Contenus essentiels prescrits devant faire l'objet d'activités d'enseignement et d'apprentissage
1. Créer la base de données. 2. Formuler des requêtes de lecture, d'insertion, de modification et de suppression de données. 3. Assurer la confidentialité et la cohérence des données. 4. Programmer des traitements de données automatisés. *Cet élément de compétence sera traité dans un autre cours* 5. Sauvegarder et restaurer la base de données.	– Rappels sur les notions de SQL – Administration des bases de données – SQL o Gestion des utilisateurs et des privilèges ▪ Création et suppression d'utilisateurs ▪ Octroi et suppression de privilèges ▪ Validation du fonctionnement des privilèges o Notion de jeux de caractères (Ex : UTF8) o Notion de collation (Ex : Case sensitive, Case insensitive) – Fonctions de cryptographie : Exemples : `SHA2, AES_Encrypt, AES_Decrypt` – Automatisation des traitements des données – SQL o Transactions ▪ Start Transaction ▪ SavePoint ▪ Commit ▪ Rollback o Procédures stockées en PL/SQL (`DECLARE, BEGIN, END, LOOP, END LOOP, CURSOR, IF, etc.`) ▪ Création : `PROCEDURE` ou `FUNCTION` ▪ Modification : `REPLACE` ▪ Suppression : `DROP` ▪ Exécution : `CALL` o Déclencheurs ▪ Création: `TRIGGER, CREATE, BEFORE, AFTER` ▪ Modification: `REPLACE` ▪ Suppression: `DROP` ▪ Pseudo-enregistrements: `OLD, NEW` ▪ Exemples d'utilisation: • Validation de données • Transformation et conversion de données

	• Ajout de colonnes d'audit dans une table avec un timestamp et un ID de l'utilisateur pour connaître la date de la dernière modification o Vues (View) : Création, utilisation, modification et suppression

Code compétence :	00Q8	**Nombre d'heures total dans le programme**	30
Énoncé de la compétence :	Effectuer des opérations de prévention en matière de sécurité de l'information		

Cours contribuant au développement de la compétence :

Numéro du cours	Titre du cours	Session	Heures dédiées
420-2C5-JR	Réseau local et sécurité	2	15
420-5D3-JR	Sécurité des données	5	15

Éléments de la compétence prescrits dans le devis ministériel	Contenus essentiels prescrits devant faire l'objet d'activités d'enseignement et d'apprentissage
1. Analyser des risques en matière de sécurité de l'information. 2. Appliquer des mesures de sécurité reconnues pour protéger le réseau. 3. Appliquer des mesures de sécurité reconnues pour protéger une application.	– Hachage et protection des mots de passe o Concepts généraux o Algorithmes de hachage (Ex : MD5, SHA1, SHA2, etc.) ▪ Propriétés des fonctions de hachage : unidirectionnelle, résistance aux collisions, rapidité d'exécution. ▪ Évaluation et comparaison d'algorithmes de hachage ▪ Concept d'obsolescence o Algorithmes de protection des mots de passe (Ex : Argon, pbkdf2, scrypt, bcrypt) ▪ Paramètres : Salt, Pepper ▪ Types d'attaques : Dictionnaires basés sur des sites compromis, attaque force brute, attaque basée sur une *rainbow table* – Chiffrement symétrique o Concepts généraux o Exemples d'implémentation : ROT13, code césar, Énigma machine, DES, AES o Exemple de code avec l'algorithme AES – Chiffrement asymétrique o Concepts généraux ▪ Clés privées et clés publiques ▪ Signatures numériques o Exemples d'implémentation : RSA, Elliptic Curve o Exemple de code avec l'algorithme RSA – Protocole HTTPS o Concepts généraux et fonctionnement o Algorithmes d'échange de clés o Notion et validation d'un certificat o Expérimentation avec le logiciel Wireshark – Vulnérabilités des applications Web o Injection en base de données (SQL, noSQL) o Injection XSS o Broken Access Control ▪ Cross-site request forgery (csrf) o Etc. – Mécanisme d'authentification o Technique désuète : Captcha et Recaptcha o Authentification à deux facteurs o Réinitialisation de mot de passe o Authentification sans mot de passe via un lien dans un courriel o Etc. – Blockchain o Concepts généraux

	○ Preuve de travail (Proof of work) ○ Preuve de participation (Proof of stake) ○ Utilisation : Cryptomonnaie, document, NFT (Non-Fungible token) – Expressions régulières

4. DESCRIPTION GÉNÉRALE DE L'ÉVALUATION SYNTHÈSE DU COURS	**Pondération :**	**40 %**	**de la note finale**
Objets d'évaluation			
La capacité de l'étudiant à expliquer les concepts de la sécurité des données et à déterminer les contextes pertinents où les appliquer.			
Contexte de réalisation			
Volet A	**Pondération :**	**40/40**	
Tâche exigée de l'élève :	Examen individuel		
Durée :	3 périodes ou 3 heures		
Matériel permis lors de l'évaluation :	Toute documentation permise excluant Internet		

Critères d'évaluation :	**Pondération suggérée**
Détermination correcte des conséquences sur la sécurité	s.o.
Choix approprié des mesures de sécurité à appliquer	s.o.
Utilisation appropriée des bibliothèques de cryptographie	s.o.
Détermination judicieuse des traitements de données à automatiser	s.o.

5. ATTITUDES PROFESSIONNELLES

Rigueur	S'assurer de la pertinence des techniques de sécurisation des données mises en place
Adaptabilité	Changement continu des techniques et concepts de sécurisation des données
Coopération	Attitude non évaluée dans ce cours

6. REFERENCES

Références pour l'enseignant(e)

Environnement laboratoire de OWASP : https://owasp.org/www-project-juice-shop/

Collation : https://docs.microsoft.com/en-us/sql/relational-databases/collations/collation-and-unicode-support?view=sql-server-ver15

csrf : https://portswigger.net/web-security/csrf

Références obligatoires pour l'élève

Aucune

7. REMARQUES

Équipe de réalisation :	Alain Martel, Yannick Charron et Houssem Aloulou
Version	1.0.0 – Avril 2022

Contenus essentiels

Pour la section des privilèges, il est suggéré d'utiliser un outil graphique (Ex : MySQL Workbench, Heidi, PhpMyAdmin).

Les expressions régulières peuvent être abordées dans les deux contextes (BD et Web) du cours.

Organisation du cours

Il est fortement recommandé d'avoir un TP sur les procédures, les triggers et les vues SQL

Pour la section des vulnérabilités Web, il est suggéré d'utiliser l'environnement laboratoire de OWASP : https://owasp.org/www-project-juice-shop/

Épreuve synthèse

Advenant le cas où plusieurs enseignants donnent le cours, il est fortement recommandé que les enseignants s'entendent sur la durée de l'évaluation synthèse (Voir article 5.12 de la PIEA).