

SECURITÉ

CODE : UE3-7

Catégorie : ÉCONOMIQUE	
Section : INFORMATIQUE DE GESTION	Sous-section / Finalité / Option : Sans objet
Implantation : Campus Jupiter , Avenue Jupiter, 201 – 1190 Bruxelles Téléphone secrétariat : 02 / 340 16 70	
Cycle : <input type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 Bloc d'études : 2 Situation dans la formation : <input checked="" type="checkbox"/> 1 ^{er} quadrimestre <input type="checkbox"/> 2 ^{ème} quadrimestre Niveau du cadre européen des certifications : <input type="checkbox"/> Niveau 6 <input type="checkbox"/> Niveau 7	Unité d'enseignement pré-requise : Néant Unité d'enseignement co-requise : Néant Volume horaire : 39h Nombre de crédits ECTS : 3 Obligatoire / Optionnelle Langue d'enseignement : français Langue d'évaluation : français
Responsable de l'UE : Monsieur Fabrice MEDOL	<u>Titulaire des activités d'apprentissage :</u> Monsieur Fabrice MEDOL (<i>Programmation sécurisée, Sécurité (réseaux, internet)</i>)
CONTRIBUTION AU PROFIL D'ENSEIGNEMENT :	
En regard de l'ensemble du programme de formation, l'UE contribue au développement des compétences et capacités suivantes :	
Compétences :	
C3 : Mobiliser les savoirs et les savoir-faire propres à l'informatique de gestion C4 : Analyser les données utiles à la réalisation de sa mission en adoptant une démarche systémique.	
Capacités :	
C3 <ul style="list-style-type: none"> • Concevoir, implémenter et maintenir des algorithmes répondant aux spécifications et fonctionnalités fournies • Choisir et mettre en œuvre un standard défini ou une technologie spécifique (méthodologie, environnement, langage, Framework, librairies, ...) C4 <ul style="list-style-type: none"> • Prendre en compte la problématique de sécurité des applications. 	

ACQUIS D'APPRENTISSAGE SPÉCIFIQUES

De manière générale pour l'unité d'enseignement :

Au terme de cette unité d'enseignement, l'apprenant sera capable :

- d'identifier et d'analyser les attaques sur un système informatique,
- d'exploiter et de définir la portée ainsi que l'impact d'une vulnérabilité,
- de sécuriser un réseau et d'y intégrer les outils de détection et de protection adéquats.

Par activité d'apprentissage :

En Programmation sécurisée:

Au terme de l'activité d'apprentissage, l'étudiant sera capable de reconnaître les principales techniques de cryptographie mises en œuvre pour sécuriser l'information, et de réaliser des applications Web sécurisées et des applications de bureau sécurisées.

En Sécurité (réseaux et internet):

Au terme de l'activité d'apprentissage, l'étudiant sera capable de reconnaître les principales vulnérabilités réseau, d'en sécuriser l'accès et de protéger efficacement les services qui y résident.

CONTENU SYNTHÉTIQUE

En Programmation sécurisée:

- Analyse des risques d'une application
- Modélisation des menaces
- Types de failles (le débordement de mémoire tampon, etc.)
- Problèmes liés aux saisies dans les bases de données
- Problèmes liés aux saisies sur le Web
- Niveau de protection des langages
- Pièges de la cryptographie (générateurs de nombres aléatoires, taille et réutilisation de clés, ...)
- Bonnes pratiques générales

En Sécurité (réseaux et internet):

- Introduction et rappels sur les aspects juridiques
- Se protéger avec la bonne cryptographie : principes et mise en œuvre
- Élaborer une politique d'authentification
- Protéger l'accès au réseau
- Concevoir une interconnexion sécurisée
- Sécuriser les accès distants
- Administrer de façon sécurisée
- Sécuriser la navigation internet
- Protéger ses serveurs applicatifs et Web
- Virtualisation et sécurité

MÉTHODES D'APPRENTISSAGE

Présentations PowerPoint accompagnées d'exercices pratiques

SUPPORTS DE COURS

	Obligatoire	En ligne
Programmation sécurisée	Non	Oui
Sécurité (réseaux, internet)	Non	Oui

MODALITÉS D'ÉVALUATION

Type d'évaluation :

En Programmation sécurisée:

Examen écrit (100%) en janvier, remédiable (à 100%) en seconde session

En Sécurité (réseaux et internet):

Examen écrit (100%) en janvier, remédiable (à 100%) en seconde session

Calcul de la note de l'UE :

Évaluation des activités d'apprentissage avec pondération :

- **Programmation sécurisée:** 67%
- **Sécurité (réseaux et internet):** 33%

Si toutes les activités d'apprentissage au sein d'une Unité d'enseignement ont une note égale ou supérieure à 10, la note de l'Unité d'enseignement est la moyenne arithmétique pondérée des notes des activités d'apprentissage. Dans les autres cas, la note de l'Unité d'enseignement est celle de l'activité d'apprentissage qui a la note la plus basse.

SOURCES DOCUMENTAIRES

Utilisées par l'enseignant :

ACISSI (M.), *Sécurité informatique - Ethical Hacking*, 4è ed., France, Eni, 2015

DUBERTRET (G.). *Initiation à la cryptographie : cours & exercices corrigés*, Paris : Vuibert, 2012

GHERNAOUTI (S.). *Sécurité informatique et réseaux : cours avec plus de 100 exercices corrigés*. 4e édition, Paris, Dunod, 2013

Proposées à l'appui du travail personnel de l'étudiant :

DUBERTRET (G.). *Initiation à la cryptographie : cours & exercices corrigés*, Paris : Vuibert, 2012

GHERNAOUTI (S.). *Sécurité informatique et réseaux : cours avec plus de 100 exercices corrigés*. 4e édition, Paris, Dunod, 2013

Supports de cours et autres :

<https://ecampus.helb-prigogine.be>