Sécurité des Applications

TEM1011-NAIN_

Domaine : **Sciences** Grade académique : **Master en architecture des systèmes informatiques - Namur**
Niveau de certification : **7** Cycle : **Deuxième cycle** Année académique : **2026-2027** (Q2)

CRÉDITS ECTS	VOLUME HORAIRE
5	**60 h**
PRÉREQUIS	**CO-REQUIS**
Aucun	*Aucun*

IMPLANTATION	DIRECTEUR DE DÉPARTEMENT DU DOMAINE	RESPONSABLE DE L'UE	ENSEIGNANTS INTERVENANTS
Département technique de Namur	Willem Kuypers	Romain Absil	Romain Absil Florentin Rochet

PROGRAMME D'ÉTUDES

Programme	Bloc	Caractère
IE-Master en architecture des systèmes informatiques	1	Obligatoire

Partie 1 Contribution de l'UE au profil d'enseignement du programme et acquis d'apprentissage spécifiques (AAS) sanctionnés par l'évaluation

CONTEXTUALISATION

UE prérequise : aucune

Cette UE contribue à l'atteinte des acquis d'apprentissage terminaux suivants :

• Agir de façon réflexive et autonome, en équipe, en partenariat

– Organiser son temps, respecter les délais

– Acquérir une capacité d'autocritique

– Actualiser ses connaissances et compétences

– Collaborer activement avec d'autres

– Animer et accompagner une équipe

– Assumer les responsabilités associées aux actes posés

• Innover, concevoir ou optimiser un système

– Intégrer l'ensemble des composantes d'un système à partir des résultats d'analyse

– Concevoir un cahier des charges et/ou ses spécifications

– Concevoir des procédures et des dispositifs

– Modéliser, dimensionner et optimiser des systèmes

• Utiliser des procédures et des outils

– Exploiter les outils appropriés afin de résoudre une tâche spécifique

– Effectuer des tests, des contrôles et des mesures

– Effectuer des paramétrages, des réglages

ACQUIS D'APPRENTISSAGE SPÉCIFIQUES (AAS)

Au terme de l'activité, l'étudiant sera capable de :

• Identifier les failles de sécurité courantes dans les applications et services web

• Expliquer les principes de fonctionnement de ces failles

• Mettre en oeuvre des pratiques de sécurité prévenant l'exploitation de ces failles

OBJECTIFS DE DÉVELOPPEMENT DURABLE

Document annexe à la fiche UE accessible via un lien explicitant en quoi le programme d'études s'inscrit dans une politique de développement durable. Une ou plusieurs UE spécifique(s) pourraient être ciblée(s) dans cette annexe.

Partie 2 Description de l'unité d'enseignement

OBJECTIFS

Faire prendre conscience des risques informatiques les plus fréquents et apprendre à maitriser les outils et les bonnes pratiques de programmation permettant de les éviter. Familiariser avec le vocabulaire et les notions fondamentales nécessaires à la compréhension des problèmes de sécurité auxquels un informaticien fait face durant sa carrière.

CONTENU

Théorie

• Introduction

• Access control

• Side channel and remanence attacks

• Set-uid programs

• Buffer overflow

• Race condition attacks

Laboratoires

• Exercices pratiques portant sur les points vus au cours théorique

SOURCES ET RÉFÉRENCES

Théorie

• https://gitlab.com/rabsil/ssd (repository public)

• Wenliang Du - Computer Security: A hands-on approach, CreateSpace Independent Publishing Platform: 2nd edition (May 1, 2019)

• OWASP Foundation - OWASP Top 10, https://owasp.org/www-project-top-ten/ (Last accessed on February 3, 2022)

• Christof Paar and Jan Pelzl - Understanding Cryptography: A Textbook for Students and Practitioners, Springer (November 8, 2014)

SUPPORTS DE COURS

Activité d'apprentissage	Support
AAIN1011-A — Théorie	*À définir*
AAIN1011-B — Laboratoires	*À définir*

Partie 3 Méthodologie mise en œuvre et éventuel découpage de l'UE

DESCRIPTION DES ACTIVITÉS D'APPRENTISSAGE (AA) AU REGARD DE LEUR STATUT

Activité d'apprentissage	Heures	Langue d'enseignement	Langue d'évaluation
AAIN1011-A — Théorie	30 h	Français	Français
AAIN1011-B — Laboratoires	30 h	Français	Français

MÉTHODES D'ENSEIGNEMENT ET D'APPRENTISSAGE

Activité d'apprentissage	Méthodes d'enseignement et d'apprentissage
AAIN1011-A — Théorie	*À définir*
AAIN1011-B — Laboratoires	*À définir*

DÉTERMINATION DE LA COHÉRENCE PÉDAGOGIQUE EN CAS DE REGROUPEMENT D'AA FAISANT L'OBJET D'UNE ÉVALUATION DISTINCTE

Sans objet

Partie 4 Évaluation de l'unité d'enseignement

STRUCTURE DU DISPOSITIF GÉNÉRAL D'ÉVALUATION (EN LIEN AVEC LE PROGRAMME D'ÉTUDES)

Évaluation intégrée : oui

UE remédiable.

Évaluation : session de juin (Q2) et seconde session (Q3).

MÉTHODOLOGIE DE CONSTRUCTION DE LA NOTE FINALE DE L'UE

Première session

• Travaux dirigés en laboratoire, évaluation continue - pondération : 35 %

• Examens : Défense orale du projet - pondération : 65 %

Deuxième session

• Examens : Défense orale du projet amendé - pondération : 100 %

Des questions théoriques sont posées lors de la défense du projet.

LA PONDÉRATION DE L'ÉVALUATION DE L'UE À DES FINS DE DÉLIBÉRATION LORS DU CALCUL DE LA MOYENNE

Au sein du programme d'études, lors du calcul de la moyenne, la pondération de l'évaluation de l'unité d'enseignement est effectuée sur base des crédits affectés à cette unité d'enseignement et évalués

MODALITÉS D'ÉVALUATION PAR ACTIVITÉ D'APPRENTISSAGE

Activité d'apprentissage	Modalités d'évaluation
AAIN1011-A — Théorie	*À définir*
AAIN1011-B — Laboratoires	*À définir*

MODALITÉS CONCRÈTES D'ÉVALUATION

Une mention sur la fiche informera les étudiants du fait que les précisions sur les épreuves seront disponibles sur Moodle au plus tard 6 semaines avant l'évaluation.