Université de Sherbrooke

Centre de formation en technologie de l'information

INF 804 – Sécurité des logiciels

Plan d'activité pédagogique

Hiver 2026

Enseignants	Aboudoulaye Fofana	Émile Grenier St-Onge
Courriel :	aboudoulaye.fofana@usherbrooke.ca	emile.grenier.st-onge@usherbrooke.ca
Local :		
Téléphone :		
Disponibilités :	Par courriel	

Site web du cours : https ://moodle.usherbrooke.ca

Description officielle de l'activité pédagogique[1]

Cibles de formation :	Comprendre le cycle de vie de développement sécuritaire. Comprendre la sécurité applicative et les concepts de base qui s'y rapportent.
Contenu :	Programmation sécuritaire. Les tests de pénétration. Le contrôle des accès. La sécurité sur mobile : analyses d'applications iOS et Android.
Crédits	3
Organisation	3 heures d'exposé magistral par semaine 6 heures de travail personnel par semaine
Particularités	Aucune

[1] https ://www.usherbrooke.ca/admission/fiches-cours/inf804

1 Présentation

Cette section présente les cibles de formation spécifiques et le contenu détaillé de l'activité pédagogique. Cette section, non modifiable sans l'approbation du comité de programme du Centre de formation en technologie de l'information, constitue la version officielle.

1.1 Mise en contexte

Selon Statistique Canada, environ 20% des entreprises canadiennes ont été victimes d'incident de sécurité en 2021, et plus de 200 entreprises de toutes tailles ont déclaré des incidents de sécurité à la Commission des accès à l'information du Québec pour la période entre septembre 2022 et octobre 2023. En 2019, Desjardins a été victime d'une fuite colossale de données de ces 9 millions de clients au Québec et Canada résultant en une perte financière de plusieurs centaines de millions de dollars, perte de clients et atteinte importante à sa réputation et crédibilité.

L'objectif premier d'un pirate est de prendre le contrôle d'un logiciel (application, système) ou équipement informatique subtiliser les différentes données d'une organisation. Pour ce faire, plusieurs techniques ou approches d'intrusion sont mises à contribution – du simple courriel à l'exploitation des failles des composantes logicielles ou matérielles accessibles via le WEB public. Certains pirates le feront uniquement pour compter un exploit à son palmarès sans faire de dommage, alors que d'autres feront un commerce lucratif des données acquises illicitement.

La sécurité logicielle et la protection de l'information confidentielle deviennent un incontournable pour toutes les organisations qui offrent des services à leurs clients ou gèrent des données qui ont une quelconque valeur sur le marché « noir ».

1.2 Cibles de formation spécifiques

Cette activité pédagogique vise à développer chez l'étudiante ou l'étudiant la capacité de :

O1. Comprendre les différents concepts autour de la sécurité logicielle

O2. Reconnaître les enjeux et la complexité de la sécurité logicielle et la protection des données ;

O3. Différentes mécanismes et démarches pour assurer la sécurité logicielle.

Il est à noter que ce cours n'est pas une formation technique portant sur :

- détection de piratage ou faille de sécurité
- configuration des composantes de sécurité
- architecture de sécurité
- programmation sécure

1.3 Contenu détaillé

Thème	Contenu	Nbr. d'heures	Objectifs
1	Séance 1 : Introduction à la sécurité logicielle : concepts et enjeux : • Présentation du plan de cours • Introduction à la sécurité des logiciels • Présentation des types d'acteurs de la menace, enjeux liés à la sécurité logicielle • Équipes et assignation d'un sujet Présentation OWASP	3	
2	Séance 2 : Architecture des applications et sécurité : • Modèle d'architecture sécurisé (Microservices, service bus, API Gateway, Zero Trust) • Infrastructure as Code (IaC) • Sécurité des différents composants : Frontend, backend, base de données, API, etc. • Infonuagique et sécurité • IA et sécurité (assistant au codage, développement LLM, attaques basées sur IA)	3	

Table 1 :

Thème	Contenu	Nbr. d'heures	Objectifs
3	Séance 3 : Comprendre les actifs informationnels et leur classification : • Classification des actifs informationnels • Cycle de vie des actifs informationnels et de leur gestion • Gouvernance de données • Protection des renseignements personnels au Québec (loi 25) et requis de sécurité • Bonnes pratiques pour atténuer le risque des données • Chiffrement • Anonymisation • Données de test • Gestion des accès • Infrastructure	3	
4	Séance 4 : Menace, Vulnérabilité et Risque : • Vulnérabilités (CWE, SANS Top 25), OWASP Top 10 • Techniques de modélisation des menaces (STRIDE, DREAD, etc.). • Renseignements sur les menaces (Threat intelligence) • Chasse aux menaces (Threat hunting) • Framework Mitre ATT&CK	3	
5	Séance 5 : Présentation des projets - sécurité des logiciels - OWASP (évaluée) : Présentation par les différentes équipes • OWASP Top 10 • OWASP Top 10 API • OWASP Top 10 CI/CD • OWASP Docker Top 10 • OWASP Mobile Top 10 • OWASP Top 10 for Large Language Model Applications • OWASP AI Security • OWASP Software Assurance Maturity Model (SAMM) • OWASP Dependency-Track • OWASP Top 10 Proactive Controls	3	
6	Séance 6 : Présentation des projets - sécurité des logiciels - OWASP (évaluée) : Suite de la présentation par les différentes équipes	3	
7	Séance 7 : Gouvernance et gestion de risque : • Cadre de sécurité NIST – un survol • Programme de sécurité et son application • Gestion de risques • Sécurité de la chaîne d'approvisionnement • Exigence de sécurité • Due diligence du tiers • Analyse de sécurité du logiciel tiers	3	
8	Séance 8 : Examen : Examen #1 – Bloc Fondamentaux de la sécurité des logiciels #1 à #7 (2 heures)	2	
9	Séance 9 : Sécurité dans le cycle de développement logiciel (SSDLC) : • Processus de développement logiciel (SDLC) • Principaux rôles d'une équipe de développement et sécurité • DevSecOps, CI/CD	3	

Table 1 :

Thème	Contenu	Nbr. d'heures	Objectifs
10	Séance 10 : Sécurité lors de la phase de planification et conception : • Architecture de la solution (applications traditionnelles et mobiles) • Exigences non fonctionnelles et cadre sécurité • Architecture spécifique d'une application mobile et ses contraintes • Considérations de sécurité précoces pour le mobile (principes MASVS niveau conception)	3	
11	Séance 11 : Sécurité lors de la phase de développement : • 8 principes du développement sécure • « Secure coding » (applications web et mobiles) • Implémentation des contrôles de sécurité • Focus sur les contrôles spécifiques aux applications mobiles (stockage sécurisé, validation des entrées) • Environnements de non-production • Passage à la phase de déploiement	3	
12	Séance 12 : Sécurité lors des phases de test, déploiement et post-déploiement : • Stratégie et plan de test de sécurité • Méthode commune de test • Essais de sécurité • Tests spécifiques pour applications mobiles (Guide MASTG) • Transition en production et configuration • Validation sécurité d'une application • Détection et réponses aux attaques • Les « app stores » Google et Apple pour le déploiement d'applications mobiles • Exigences de sécurité des « app stores »	3	
13	Séance 13 : Sécuriser les applications mobiles : • Gestion de la configuration et le changement • Gestion des vulnérabilités (applications web et mobiles) • Support aux opérations (Backup, Archivage, Rétention, Reprise après sinistre) • Synthèse : Cadre complet de sécurité des applications mobiles • Norme MASVS : consolidation des niveaux et exigences • Intégration MASDG et MASTG dans le cycle complet	3	
14	Séance 14 : Examen : Examen #2 – Bloc sécurité des applications séances #8 à #14 (2 heures)	2	

2 Organisation

Cette section propre à l'approche pédagogique de chaque enseignante ou enseignant présente la méthode pédagogique, le calendrier, le barème et la procédure d'évaluation ainsi que l'échéancier des travaux. Cette section doit être cohérente avec le contenu de la section précédente.

2.1 Méthode pédagogique

L'approche pédagogique privilégiée sera la tenue d'une formation classique à distance via TEAMS. La présentation sera disponible avant chaque séance et elle sera utilisée pour supporter les présentations et les discussions. Dans ce matériel, les différentes sources seront identifiées et des liens vers des lectures complémentaires ou obligatoires seront mentionnés. Il y aura aussi quelques documents pertinents dans le Moodle du cours.

2.2 Calendrier

Date	Thème
2026-01-05	1
2026-01-08	2
2026-01-12	3
2026-01-15	4
2026-01-19	5
2026-01-22	6
2026-01-26	7
2026-01-29	8
2026-02-02	9
2026-02-05	10
2026-02-09	11
2026-02-12	12
2026-02-16	13
2026-02-19	14

2.3 Évaluation

Modalités d'évaluation	**%**
1 Présentation projet OWASP notée (pair 30% et enseignant 70%)	30 %
1 examen récapitulatif par bloc (2 examens au total)	40 %
1 thème à explorer	30 %

2.3.1 Qualité de la langue et de la présentation

Conformément à l'article 17 du Règlement facultaire d'évaluations des apprentissages[2] l'enseignante ou l'enseignant peut retourner à l'étudiante ou à l'étudiant tout travail non conforme aux exigences quant à la qualité de la langue et aux normes de présentation.

2.3.2 Plagiat

Le plagiat consiste à utiliser des résultats obtenus par d'autres personnes afin de les faire passer pour sien et dans le dessein de tromper l'enseignante ou l'enseignant. Vous trouverez en annexe un document d'information relatif à l'intégrité intellectuelle qui fait état de l'article 9.4.1 du Règlement des études[3]. Lors de la correction de tout travail individuel ou de groupe une attention spéciale sera portée au plagiat. Si une preuve de plagiat est attestée, elle sera traitée en conformité, entre autres, avec l'article 9.4.1 du Règlement des études de l'Université de Sherbrooke. L'étudiante ou l'étudiant peut s'exposer à de graves sanctions qui peuvent être soit l'attribution de la note E ou de la note zéro (0) pour un travail, un examen ou une activité évaluée, soit de reprendre un travail, un examen ou une activité pédagogique. Tout travail suspecté de plagiat sera transmis au Secrétaire de la Faculté des sciences. Ceci n'indique pas que vous n'ayez pas le droit de coopérer entre deux équipes, tant que la rédaction finale des documents et la création du programme restent le fait de votre équipe. En cas de doute de plagiat, l'enseignante ou l'enseignant peut demander à l'équipe d'expliquer les notions ou le fonctionnement du code qu'elle ou qu'il considère comme étant plagié. En cas d'incertitude, ne pas hésiter à demander conseil et assistance à l'enseignante ou l'enseignant afin d'éviter toute situation délicate par la suite.

2.4 Échéancier des travaux

Les dates de remise des travaux seront indiquées sur les énoncés.

2.5 Utilisation d'appareils électroniques et du courriel

Selon le règlement complémentaire des études, section 4.2.3 [4], l'utilisation d'ordinateurs, de cellulaires ou de tablettes pendant une prestation est interdite à condition que leur usage soit explicitement permise dans le plan de cours.

Dans ce cours, l'usage de téléphones cellulaires, de tablettes ou d'ordinateurs est autorisé. Cette permission peut être retirée en tout temps si leur usage entraîne des abus.

Tel qu'indiqué dans le règlement universitaire des études, section 4.2.3[5], toute utilisation d'appareils de captation de la voix ou de l'image exige la permission de la personne enseignante.

Note : Je réponds aux questions posées par courriel à l'extérieur des périodes de cours.

3 Matériel nécessaire pour l'activité pédagogique

Voir le site MOODLE

[2] https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/documents/Etudiants_actuels/Informations_academiques_et_reglements/2017-10-27_Reglement_facultaire_-_evaluation_des_apprentissages.pdf

[3] https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/

[4] https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/documents/Etudiants_actuels/Informations_academiques_et_reglements/Sciences_Reglement_complementaire.pdf

[5] https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/

Faculté des sciences UdS

Délits relatifs aux études

Extrait du règlement des études (Règlement 2575-009)

Sont notamment considérés comme un délit relatif aux études les faits suivants :

a) commettre un plagiat, soit faire passer ou tenter de faire passer pour sien, dans une production évaluée, le travail d'une autre personne, des passages ou idées tirés de l'œuvre d'autrui ou du contenu, de toute forme, généré par un système d'intelligence artificielle (ce qui inclut notamment le fait de ne pas indiquer la source et la référence adéquate);
b) commettre un autoplagiat, soit soumettre, sans autorisation préalable, une même production, en tout ou en partie, à plus d'une activité pédagogique ou dans une même activité pédagogique (notamment en cas de reprise);
c) usurper l'identité d'une autre personne ou procéder à une substitution de personne lors d'une production évaluée ou de toute autre prestation obligatoire;
d) fournir ou obtenir toute forme d'aide non autorisée, qu'elle soit collective ou individuelle (incluant l'assistance provenant d'un système d'intelligence artificielle), pour une production faisant l'objet d'une évaluation;
e) obtenir par vol ou toute autre manœuvre frauduleuse, posséder ou utiliser du matériel non autorisé de toute forme (incluant le matériel numérique et celui généré par un système d'intelligence artificielle) avant ou pendant une production faisant l'objet d'une évaluation;
f) copier, contrefaire ou falsifier un document pour l'évaluation d'une activité pédagogique;
k) posséder ou avoir à sa portée un appareil électronique ou numérique interdit durant une activité d'évaluation;

[...]

Un guide sur l'intégrité intellectuelle vous est rendu disponible par le service des bibliothèques et des archives de l'Université de Sherbrooke, afin de bien comprendre les différents délits et ainsi éviter d'être aux prises avec un dossier disciplinaire et une ou des sanctions.

Les mesures pouvant être imposées à titre de sanctions disciplinaires sont les suivantes :

a) la réprimande simple ou sévère consignée au dossier étudiant pour la période fixée par l'autorité disciplinaire ou à défaut, définitivement. En cas de réprimande fixée pour une période déterminée, la décision rendue demeure au dossier de la personne aux seules fins d'attester de l'existence du délit en cas de récidive;
b) l'obligation de reprendre une production ou une activité pédagogique, dont la note pourra être établie en tenant compte du délit survenu antérieurement;
c) la diminution de la note ou l'attribution de la note E ou 0;

[...]

UDS Faculté des sciences

Balises d'utilisation des outils d'intelligence artificielle générative

Autorisés ou pas dans les situations d'apprentissage et d'évaluation ?

NIVEAU 0	NIVEAU 1	NIVEAU 2	NIVEAU 3	NIVEAU 4
L'utilisation des outils d'intelligence artificielle générative (IAg) est limitée, voire complètement interdite parce que la personne enseignante considère que l'usage de ces outils nuit au développement de compétences essentielles. Ces compétences peuvent être disciplinaires, comme elles peuvent être d'ordre méthodologique, rédactionnel ou informationnel. Considérant que l'utilisation des IAg requiert un esprit critique, il peut s'agir d'une situation d'apprentissage ou d'évaluation sans IAg qui vise à développer celui-ci. Dans ces situations, **la personne étudiante produit le travail**.			L'utilisation prononcée des IAg est permise parce que la personne enseignante considère que les personnes étudiantes sont en mesure d'exercer un esprit critique et sont capables de juger de la qualité des contenus produits par les IAg. Ou encore, l'utilisation est encouragée parce que la situation d'apprentissage ou d'évaluation proposée contribue à développer leur esprit critique. Dans ces situations, l'IAg produit le travail préliminaire, alors que **la personne étudiante s'assure de sa qualité en l'améliorant**.	
				
Utilisation interdite	**Utilisation limitée**	**Utilisation guidée**	**Utilisation balisée**	**Utilisation libre**
Le **NIVEAU 0** signifie que l'**utilisation est interdite**. Ceci signifie que si la personne enseignante a un motif de croire qu'il y a eu l'utilisation d'une IAg dans une situation d'évaluation, elle doit dénoncer les faits auprès de la personne responsable des dossiers disciplinaires universitaires. Il s'agit d'un délit relatif aux études tel que stipulé dans le Règlement des études.	Le **NIVEAU 1 D'UTILISATION** signifie que l'**utilisation est autorisée uniquement pour assister l'apprentissage dans le domaine disciplinaire ou des langues**. Dans ce contexte, la personne étudiante **est tenue de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation peut être considérée comme un délit. Par exemple : Domaine disciplinaire : - S'inspirer - Générer des idées - Explorer un sujet pour mieux le comprendre - Générer du matériel pour apprendre Domaine des langues : - Identifier ses erreurs et se les faire expliquer - Reformuler un texte - Générer un plan pour aider à structurer un texte - Traduire un texte	Le **NIVEAU 2 D'UTILISATION** signifie que l'**utilisation est autorisée pour améliorer un travail produit par la personne étudiante**. Dans ce contexte, la personne étudiante **est tenue de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation est considérée comme un délit. Par exemple : - Analyser des contenus - Obtenir une rétroaction - Évaluer la qualité de son travail à partir de critères - Demander à être confronté relativement à ses idées, à sa démarche - Diriger les processus de résolution de problèmes	Le **NIVEAU 3 D'UTILISATION** signifie que l'**utilisation est autorisée pour produire un travail qui sera amélioré.** Dans ce contexte, la personne étudiante **est tenue de citer selon les normes[1] le contenu généré par l'IAg** ou **de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation est considérée comme un délit. Par exemple : - Résumer ou rédiger des parties d'un texte - Générer un texte ou un modèle d'une production et l'adapter - Réaliser des calculs mathématiques - Produire du code informatique - Résoudre des problèmes complexes - Répondre à une question - Générer des images, ou autres contenus multimédias	Le **NIVEAU 4 D'UTILISATION** signifie qu'**aucune restriction spécifique n'est imposée**. Dans ce contexte, la personne étudiante **est tenue de citer selon les normes[1] le contenu généré par l'IAg** ou **de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation est considérée comme un délit. Ce niveau inclut tout ce qui précède, de l'exploration à la production, ainsi que toute autre tâche particulière jugée complexe.

UDS Faculté des sciences

À considérer avant l'utilisation d'outils d'intelligence artificielles génératives

Si, en tant que personne étudiante envisagez d'utiliser un outil d'intelligence artificielle générative (IAG) lorsque l'évaluation autorise les niveaux 1 à 4 d'utilisation mentionnés précédemment.

Dans ce cas, gardez à l'esprit les éléments clés suivants.

- Vous assumez la responsabilité de tout le contenu produit, avec ou sans IAG, et intégré à votre production.
- Les produits des outils d'IAG peuvent très souvent comporter **des erreurs ou des faussetés** (hallucinations) : on doit donc impérativement valider tout contenu généré par ces outils.
- Dans l'état actuel de la Loi sur le droit d'auteur du Canada, les **productions faites par l'IAG sont du domaine public,** puisque les outils d'IAG ne sont pas reconnus comme des auteurs au sens de la Loi et que les contenus générés ne répondent pas aux critères d'une œuvre protégée, notamment aux critères d'originalité.
- L'entreprise qui fournit le service pourrait émettre certaines exigences dans ses conditions d'utilisation. Comme l'algorithme et le code informatique appartiennent à l'entreprise qui les a développés, nous devons tenir compte de ces conditions. Celles-ci pourraient également fournir des précisions relatives à la **réutilisation des données soumises (confidentialité)**.

Comment déclarer l'utilisation d'outils d'intelligence artificielle générative

Dans l'esprit d'une conduite intègre et responsable, vous devez TOUJOURS mentionner de façon explicite toute utilisation de l'intelligence artificielle, conformément au Règlement des études (9.4.1 Délits relatifs aux études). De plus, à des fins pédagogiques, il est recommandé de toujours intégrer à la production les requêtes, de même que les réponses intégrales générées par les outils d'IAG. Celles-ci pourront être intégrées directement dans le corps du texte ou en note de bas de page. Les réponses longues pourraient être insérées en annexe de votre document ou dans des documents supplémentaires, selon les directives de la personne enseignante.

L'utilisation de ces deux documents s'avèrera utile, ils se trouvent sous licence libre, donc vous pouvez utiliser les tableaux et les adapter selon votre besoin:

1. Modèle de citation : Ce formulaire, à remplir par l'enseignant, donne un exemple aux étudiants de citation de l'IAg dans la réalisation d'un travail évalué ou non.
2. Déclaration d'usage : Ce formulaire, à remplir par les étudiants, doit être remis avec une réalisation afin de déclarer l'usage de l'IAg dans la réalisation, qu'elle soit évaluée ou non.

Référence

La Faculté des sciences tient à remercier le SSF pour la production des documents.

- Cabana, M. et Côté, J.-A. (2024). Balises d'utilisation des outils d'intelligence artificielle générative. Service de soutien à la formation, Université de Sherbrooke. Sous licence CC BY 4.0.
- Cabana, M. et Beaudet, M. (2024). Directives de déclaration de l'utilisation de l'intelligence artificielle générative dans une production étudiante. Service de soutien à la formation, Université de Sherbrooke. Sous licence CC BY 4.0.
- Cabana, M. (2024). Formulaire de déclaration de l'utilisation de l'intelligence artificielle générative dans une production étudiante. Service de soutien à la formation, Université de Sherbrooke. Sous licence CC BY 4.0.