Université du Québec en Outaouais **Département d'informatique et d'ingénierie**

Sigle : CYB1123 Gr. 20
Titre : Sécurité de l'infonuagique et des services web
Session : Automne 2024 Horaire et local
Professeur : Caissy, David

1. Description du cours paraissant à l'annuaire :

Objectifs

Au terme de ce cours, l'étudiant.e sera familier.e avec les enjeux de la sécurité dans l'infonuagique et les services web, et sera capable de mettre en œuvre des solutions pour sécuriser les infrastructures infonuagiques et les services Web.

Contenu

Modèles de service (SAAS, PAAS, IAAS) et de déploiements (public, privé, communautaire, hybride) de l'infonuagique. Techniques et outils de virtualisation. Architecture d'une application Web. Éléments de base du langage SQL. Vulnérabilités, attaques et menaces dans le nuage et les services web (brute force, escalade de privilèges, XSS, injection de code, DDoS, etc.). Recommandations de l'OWASP (Open Web Application Security Project). Techniques de protection des données, des infrastructures et des applications dans le nuage (pare-feu, tests, etc.). Méthodologie d'évaluation de la sécurité applicative. Gestion des risques dans le nuage et aspects légaux de la sécurité dans le nuage et les applications Web. Ce cours comporte des séances obligatoires de travaux pratiques (TP).

Descriptif – Annuaire

2. Objectifs spécifiques du cours :

L'objectif de cette activité est que l'étudiante ou l'étudiant soit en mesure d'identifier les menaces et vulnérabilités de l'infonuagique, évaluer les méthodes d'attaque et gérer les risques de manière proactive. Il saura également sécuriser les applications infonuagiques et mettre en place la surveillance et l'automatisation de la sécurité, assurant ainsi une sécurité robuste et une conformité continue.

3. Stratégies pédagogiques :

Les séances de cours seront présentées sous forme magistrales, parsemées d'exercices de compréhension. Le matériel pédagogique est accessible à partir de la plateforme Moodle dédiée au cours. Un forum de discussion sera aussi disponible pour poser des questions liées à la matière enseignée.

Des travaux pratiques seront également réalisés afin de consolider les concepts présentés durant les séances de cours.

4. Heures de disponibilité ou modalités pour rendez-vous :

Communication par courriel (david.caissy@uqo.ca) et via le forum de discussion. Période de consultation flexible (lundi au vendredi) sur rendez-vous seulement (prévoir 48 heures d'avance pour la prise de rendez-vous).

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	**Chapitre 1 : Introduction** • Modèles de service (IaaS, PaaS, SaaS) • Modèle de responsabilité partagée • Techniques de virtualisation	9 sep. 2024

2	**Chapitre 2 : Gestion de l'identité** • Authentification unique (SSO) et multifacteur (MFA) • Gestion des identités et des accès (IAM) • Surveillance des comptes utilisateurs	16 sep. 2024
3	**Chapitre 3 : Rôles de sécurité** • Contrôle des accès • Gestion des privilèges (PAM) • Comptes utilisateurs spéciaux **Travail Pratique 1 :** Configuration des privilèges spéciaux	23 sep. 2024
4	**Chapitre 4 : Protection des données** • Identification et classification des données • Cryptage en transit et au repos • Gestion des clés de chiffrement **Travail Pratique 2 :** Élaboration des besoins en matière de sécurité	30 sep. 2024
5	**Chapitre 5 : Protection du réseau** • Protection du périmètre • Sécurité des points d'accès • Accès conditionnels	7 oct. 2024
6	**Semaine d'études**	14 oct. 2024
7	**Chapitre 6 : Connection service-à-service (S2S)** • Authentification des applications • Connection sécurisé aux systèmes externes • Gestion des clés API **Travail Pratique 3 :** Architecture de sécurité de connections externes	21 oct. 2024
8	**Examen de mi-session**	28 oct. 2024
9	**Chapitre 7 : Reprise après sinistre** • Planification d'urgence • Continuité des activités • Tests de reprise après sinistre	4 nov. 2024
10	**Chapitre 8 : Surveillance de la sécurité** • Journalisation et audits de sécurité • Systèmes de détection et de prévention d'intrusions (IDS et IPS) • Gestion des incidents de sécurité **Travail Pratique 4 :** Gestion d'incidents de sécurité	11 nov. 2024
11	**Chapitre 9 : Attaques des applications Web** • Attaques d'injection de code (SQLi, XSS, CSRF) • Déni de service distribué (DDOS) • Contrôle d'accès défectueux	18 nov. 2024

12	**Chapitre 10 : Identification et gestion des vulnérabilités** • Évaluation et autorisation de sécurité • Identification des menaces et des vulnérabilités • Calcul et gestion des risques • Recommandations **Travail Pratique 5 :** Classification et gestion des risques de sécurité	25 nov. 2024
13	**Chapitre 11 : Développement sécurisé d'applications infonuagiques** • Gestion de la configuration • DevSecOps pour la sécurité infonuagique • Recommendations de l'Open Web Application Security Project (OWASP) • Normes de vérification de la sécurité des applications (ASVS) **Travail Pratique 6 :** Sélection de contrôles de sécurité basés sur ASVS	2 déc. 2024
14	**Chapitre 12 : Conformité et considérations juridiques** • Aspects légaux • Protection de la vie privée • Conformité aux normes de l'industrie	9 déc. 2024
15	**Examen final**	16 déc. 2024

6. Évaluation du cours :

L'évaluation est l'appréciation du niveau d'apprentissage atteint par l'étudiant(e) par rapport aux objectifs des cours et des programmes. Dans le cas spécifique du cours **Sécurité de l'infonuagique et des services web**, l'attribution des notes se fera selon la répartition suivante :

- **Examen de mi-session : 30 %**
- **Examen final : 40 %**
- **6 travaux pratiques (5% chacun) : 30 %**

Une moyenne inférieure à 50 % aux examens est éliminatoire et conduit automatiquement à un échec.

7. Politiques départementales et institutionnelles :

- Politique du département d'informatique et d'ingénierie relative à la tenue des examens
- Note sur le plagiat et sur la fraude
- Politique relative à la qualité de l'expression française écrite chez les étudiants et les étudiantes de premier cycle à l'UQO
- Absence aux examens : cadre de gestion, demande de reprise d'examen (formulaire)

Tolérance ZÉRO en matière de violence à caractère sexuel.

Le Bureau d'intervention et de prévention en matière de harcèlement (BIPH) a pour mission d'accueillir, soutenir et guider toute personne vivant une situation de harcèlement, de discrimination ou de violence à caractère sexuel. Le BIPH oriente ses actions afin de prévenir les violences à caractère sexuel pour que nous puissions étudier, travailler et s'épanouir dans un milieu sain et sécuritaire.

Vous vivez ou êtes une personne témoin d'une situation de violence à caractère sexuel ? Vous êtes une personne membre de la communauté étudiante ou une personne membre du personnel, autant à Gatineau qu'à Ripon et St-Jérôme, l'équipe du BIPH est là pour vous, sans jugement et en toute confidentialité.

Ensemble, participons à une culture de respect.

Pour de plus amples renseignements consultez UQO.ca/biph ou écrivez-nous au Biph@uqo.ca

8. Principales références :

- Notes de cours disponibles sur Moodle
- **Sécurité dans le Cloud AWS** (https://aws.amazon.com/fr/security)
- **Documentation sur la sécurité Azure** (https://learn.microsoft.com/fr-ca/azure/security)
- **Mesures de protection du nuage du gouvernement du Canada** (www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=32787)

9. Page Web du cours :

https://moodle.uqo.ca