ENSEIRB-MATMECA

# Module 3 : Intrusion sur les applications Web

École / Prépa
ENSEIRB-MATMECA

## En bref

- **Langue(s) d'enseignement:** Français
- **Ouvert aux étudiants en échange:** Non

# Présentation

**Code interne :** EC9IT313

## Objectifs

Ce module s'adresse à des personnes disposants de connaissances techniques et souhaitant parfaire leurs connaissances des vulnérabilités sévères modernes. Le module a pour but de présenter, en s'appuyant sur de nombreux cas pratiques, les différentes réflexions et observations permettant de guider l'expert dans sa découverte de vulnérabilités.

## Heures d'enseignement

| | | |
|---|---|---|
| CI | Cours Intégrés | 24h |

## Syllabus

- Introduction (déroulement d'une intrusion, méthodologie et concepts généraux, démarches et ressources)
- BurpSuite (utilisation de BurpSuite dans le cadre d'une intrusion en boite noire, possibilités et limites de BurpSuite, raccourcis et mécanismes d'automatisation, Extensions)
- Reconnaissance (surface d'attaque, outillage)
- Méthodologies et démarche (caractère itératif du processus, vulnérabilités logiques, gestion de mécanismes communs : authentification, contrôle d'accès, entrées utilisateurs, identification des technologies côté client et côté serveur)
- Etude et exploitation des vulnérabilités avancées (Tour d'horizon des vulnérabilités applicatives : XXE, SSRF, injections, SSTI, Prototype, pollution, attaques cryptographiques, attaques des mécanismes d'authentification, GraphQL, vulnérabilités spécifiques au cloud)

- Etude et exploitation de vulnérabilités spécifiques (Java, PHP, Python/Django, Perl)

## Compétences visées

**Ce module appartient au bloc de compétences de l'Activité A2 : Audit de sécurité technique**

Tâche 1 (A2T1) : Réaliser des audits de sécurité technique, incluant des tests d'intrusion, pour évaluer la sécurité des applications Web, des systèmes d'exploitation (Linux, Windows) et des protocoles réseau.

· A2T1C1 : Identifier, analyser et documenter les vulnérabilités dans les applications, systèmes et réseaux à l'aide d'outils spécifiques.

· A2T1C2 : Exécuter des tests d'intrusion dans des environnements variés (Web, Linux, Windows) tout en respectant les normes et la réglementation en vigueur.

· A2T1C3 : Synthétiser les résultats des audits et tests d'intrusion dans un rapport clair et détaillé, incluant des recommandations pour améliorer la cybersécurité.

Tâche 2 (A2T2) : Participer à la mise en œuvre et au suivi des mesures correctives identifiées lors des audits de sécurité technique.

· A2T2C1 : Prioriser les vulnérabilités et proposer des solutions adaptées en collaboration avec les équipes techniques.

· A2T2C2 : Superviser le déploiement des correctifs et s'assurer de la conformité des systèmes aux standards de sécurité.

· A2T2C3 : Valider l'efficacité des mesures correctives mises en place et communiquer les résultats aux parties prenantes.

Tâche 3 (A2T3) : Concevoir et tester des scénarios d'attaque simulés pour évaluer la résilience des systèmes en conditions réalistes.

· A2T3C1 : Développer des scénarios de simulation réalistes en s'appuyant sur les tactiques, techniques et procédures (TTP) des attaquants.

· A2T3C2 : Simuler des attaques dans des environnements variés et évaluer la capacité de défense de l'infrastructure numérique.

· A2T3C3 : Documenter les résultats des simulations et fournir des recommandations stratégiques pour améliorer la résilience des systèmes.

Tâche 4 (A2T4) : Développer et animer des programmes de formation en cybersécurité

· A2T4C1 : Concevoir des supports pédagogiques adaptés aux différents publics (utilisateurs finaux, équipes techniques, dirigeants).

- A2T4C2 : Animer des sessions de sensibilisation et former les collaborateurs.
- A2T4C3 : Actualiser les contenus de formation grâce à la veille sur les menaces émergentes.

# Modalités de contrôle des connaissances

## Évaluation initiale / Session principale - Épreuves

| Type d'évaluation | Nature de l'épreuve | Durée (en minutes) | Nombre d'épreuves | Coefficient de l'épreuve | Note éliminatoire de l'épreuve | Remarques |
|---|---|---|---|---|---|---|
| Contrôle Continu | Contrôle Continu | | | 1 | | |

## Seconde chance / Session de rattrapage - Épreuves

| Type d'évaluation | Nature de l'épreuve | Durée (en minutes) | Nombre d'épreuves | Coefficient de l'épreuve | Note éliminatoire de l'épreuve | Remarques |
|---|---|---|---|---|---|---|
| Epreuve terminale | Oral | 30 | | 1 | | sans document |