



### 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 Intégré	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 boîte 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

Capacité d'identification et d'exploitation des vulnérabilités Web. Capacité de faire des recommandations de correction et de remédiation sur les vulnérabilités Web.

Capacité de réaliser des développements sécurisés.

## 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