

3IF5220 - Développement et sécurité web

Responsables : **Pierre-François GIMENEZ**

Langues d'enseignement : **FRANCAIS**

Campus où le cours est proposé : **CAMPUS DE RENNES**

Nombre d'heures d'études élèves (HEE) : **60**

Nombre d'heures présentielles d'enseignement (HPE) : **24**

Année académique : **2024-2025**

Niveau avancé : **non**

Présentation, objectifs généraux du cours :

Les applications web sont devenues un paradigme de développement et de programmation majeur, gagnant souvent une place centrale dans les systèmes d'information modernes. Du point de vue de la sécurité informatique, elles constituent également la plus grande source de vulnérabilités et le point d'entrée le plus courant pour un attaquant. Ce module a pour objectif de fournir des compétences de base en développement web, une vision synthétique des principes de fonctionnement et d'architecture des applications web modernes et un aperçu de quelques technologies de développement parmi les plus utilisées. Sur ces fondations, les problématiques de sécurité spécifiques aux applications web sont introduites, d'une façon à la fois théorique et expérimentale, de manière à acquérir les outils et compétences nécessaires à l'évaluation de la sécurité d'une application web. Un projet de développement significatif, dans une technologie au choix, permet aux étudiants de se mesurer au problème de la conception d'une application web sécurisée.

Période(s) du cours (n° de séquence ou hors séquence) :

SM11

Prérequis :

Enseignements de première année :

- Réseaux et Sécurité.

Enseignements de troisième année :

- Ateliers de programmation et outils de développement ;
- Introduction à la Sécurité ;
- Cryptographie 1.

Plan détaillé du cours (contenu) :

- Cours 1 (3h) : Introduction, architectures modernes pour les applications web
- Cours 2 (3h) : JavaScript
- TP 1 (3h) : Frameworks JavaScript (Angular, Node.js)
- Cours 3 (3h) : React

- Cours 4 (3h) : Un framework de développement Python côté serveur : Flask
- TP 2 (3h) : Flask + React
- Cours 5 (3h) : Sécurité des applications web
- Cours 6 (3h) : Sécurité - vulnérabilités logiques
- Cours 7 (3h) : Sécurité - vulnérabilités côté client
- Cours 8 (3h) : Sécurité - vulnérabilités côté serveur
- Cours 9 (3h) : Sécurité - vulnérabilités chaînées
- TP 3 (3h) : Projet de développement
- TP 4 (3h) : Projet de développement
- TP 5 (3h) : Projet de développement

Déroulement, organisation du cours :

Cours magistraux : 27h
Travaux pratiques : 15h

Organisation de l'évaluation :

Évaluation d'un projet de développement d'une application web sécurisée.

Moyens :

Outils logiciels :

- Environnements courants de développement web ;
- Burp Suite Community Edition ;
- Plate-forme de challenges de sécurité dédiée mise à disposition pour les travaux pratiques.

Acquis d'apprentissage visés dans le cours :

À la fin de cet enseignement, l'étudiant sera capable de :

- Concevoir et développer une application web moderne incluant des traitements côté serveur comme côté client ;
- Anticiper les risques de sécurité lors de la conception d'une application web ;
- Évaluer la sécurité d'une application web en utilisant les outils et méthodologies appropriés ;
- Mener des activités de tests d'intrusion en environnement web ;
- Conseiller architectes et développeurs web sur l'amélioration de la sécurité de leurs produits.

Description des compétences acquises à l'issue du cours

:

-
- C4.2 Propose one or more solutions that answer the question reformulated in terms of value creation and complete by taking into account the impact on the other stakeholders and by taking into account the other dimensions. Quantify the value created by these solutions.
Arbitrate between possible solutions
- C7.1 Substance: Structure ideas and arguments, summarise (hypotheses, objectives, expected results, approach and value created).
- C8.1 Build a team to work as a team