Présentiel/distanciel

NOUVEAUTÉ

Programmation avancée en Python et JS pour la conception et la sécurité fullstack

Objectifs pédagogiques

- Approfondir la maîtrise des concepts avancés en Python et JavaScript, en mettant l'accent sur la performance et la sécurité.
- Mettre en oeuvre des pratiques de développement sécurisées pour concevoir des applications robustes et protégées.
- Intégrer des mécanismes avancés d'authentification et de gestion des accès (OAuth2, JWT, SAML).
- Exploiter les outils de test et d'analyse de vulnérabilités pour détecter et corriger les failles de sécurité.
- Développer et sécuriser des API en utilisant REST et GraphQL.
- Découvrir l'automatisation du déploiement et la sécurisation d'applications fullstack en environnement cloud.

Prérequis

Maîtriser les fondamentaux de Python et de JavaScript et connaître les bases du développement web.

Public concerné

Développeurs fullstack souhaitant approfondir Python et javaScript pour concevoir des applications robustes et sécurisées.

Programme détaillé

Programmation avancée en Python et JavaScript (10h20)

- **Python avancé :**
  - Programmation fonctionnelle et orientée objet avancée
  - Générateurs, coroutines et programmation asynchrone (async/await)
  - Gestion avancée des erreurs et logging
- **JavaScript avancé :**
  - Closures, prototypes, et manipulation avancée des objets
  - Programmation asynchrone avec Promises et Async/Await
  - Modules et importation dynamique
- **Optimisation et Debugging :**
  - Profiling et optimisation du code
  - Outils de debugging avancés (Chrome DevTools, PyCharm Debugger)
  - Introduction aux WebAssembly pour optimiser JavaScript

Développement et sécurisation d'API REST et GraphQL (7h00)

- **Conception d'API REST et GraphQL :**
  - Structuration et bonnes pratiques
  - Gestion des versions d'API
  - GraphQL vs REST : avantages et inconvénients
- **Sécurisation des API :**
  - Protection contre l'injection SQL, XSS, CSRF et autres vulnérabilités OWASP
  - Gestion des CORS et validation des entrées
  - Implémentation de rate-limiting et de logging sécurisé
- **Authentification et Autorisation :**
  - OAuth2, JWT et gestion des sessions
  - RBAC et ABAC pour la gestion des permissions
  - Sécurisation des identités avec OpenID Connect

DevSecOps et Sécurité Applicative (10h20)

- **Automatisation des tests de sécurité :**
  - Introduction à DevSecOps.
  - Utilisation de SonarQube, OWASP ZAP, Burp Suite
  - Intégration des tests dans le CI/CD
- **Sécurisation du Backend et du Frontend :**
  - Gestion des clés et données sensibles (HashiCorp Vault, AWS Secrets Manager)
  - Protection contre l'exfiltration de données et l'élévation de privilèges
  - Implémentation de CSP, HSTS et autres en-têtes de sécurité

Orchestration et Sécurisation des Déploiements (7h00)

- **Mise en place d'un pipeline CI/CD sécurisé :**
  - Automatisation des tests et déploiements
  - Scan de vulnérabilités dans le CI/CD
  - Hardening des conteneurs et des images Docker
- **Gestion des permissions et surveillance des applications :**
  - IAM et gestion des rôles (AWS IAM, Azure RBAC)
  - Monitoring et audit de logs avec Prometheus et Grafana
  - Sécurité des microservices et isolation des workloads

Délais d'accès à la formation

Les inscriptions sont possibles jusqu'à 48 heures avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ENI Service est tenu de respecter un délai minimum obligatoire de 11 jours ouvrés entre la date d'envoi de sa proposition et la date de début de la formation.

Modalités et moyens pédagogiques, techniques et d'encadrement

La formation peut être suivie uniquement en présentiel dans l'un des campus de l'ENI Ecole Informatique (Nantes, Rennes, Niort, Quimper). Le stagiaire intègre une promotion de l'ENI Ecole Informatique d'environ 25 à 28 stagiaires max par session.
Chaque stagiaire dispose d'un poste de travail adapté aux besoins de la formation et des supports de cours au format numérique.
Il alterne apports théoriques, démonstrations et mise en pratique au travers d'exercices, de travaux pratiques et de cas concrets, réalisés individuellement ou en groupe.

Modalités d'évaluation des acquis

Une évaluation des acquis du stagiaire est réalisée en fin de formation.

Moyens de suivi d'exécution et appréciation des résultats

Feuille de présence, émargée par demi-journée par chaque stagiaire et le formateur.
Évaluation qualitative de fin de formation, qui est ensuite analysée par l'équipe pédagogique de l'ENI Ecole Informatique.
Attestation de fin de formation remise au stagiaire.

Qualification du formateur

La formation est animée par un professionnel de l'informatique et de la pédagogie, recruté sur la base de son expérience professionnelle dans le domaine enseigné.
Nos formateurs sont pour la plupart ENI Certified Trainers. Ils assurent une veille technologique permanente.

Accessibilité de la formation

ENI Service s'engage en faveur de l'accessibilité pour les personnes en situation de handicap (PSH). Toutes nos formations sont ainsi accessibles aux PSH. Pour en savoir plus, nous vous invitons à consulter la page "Accueil des personnes en situation de handicap" de notre site internet.