

Formation Sécurité Web

La sécurité web regroupe l'ensemble des mesures et techniques permettant de protéger les systèmes informatiques, ainsi que les données des utilisateurs et des entreprises, contre les cyberattaques et les menaces en ligne. Elle englobe la sécurité des serveurs web, des bases de données, des réseaux et des applications, tout comme la protection des données sensibles (mots de passe, informations de paiement). Pour contrer ces menaces, plusieurs leviers sont essentiels, notamment l'utilisation de pare-feu, de logiciels antivirus et le chiffrement des données. Il est également crucial d'adopter les bonnes pratiques en ligne, telles que l'authentification à deux facteurs, et de rester informé des dernières vulnérabilités. En tant que développeur web, il est indispensable d'intégrer la sécurité dès la conception d'un site ou d'une application afin de garantir la protection des données et l'intégrité du système.

PROGRAMME

JOUR 1

Tour de table

1/ Introduction

- Mythes et réalités
- Architecture d'une application Web typique : client, serveur, proxies
- Le top 10 : 2025 (8eme édition, janv 2026) des vulnérabilités selon OWASP, CWE et CVE
- Profils des attaquants : attaques externes et internes - Les étapes d'une attaque
- Arsenal des attaquants

2/ La place de la sécurité dans le cycle de développement

- Malentendus récurrents
- Biais envers la production
- Gouvernance, politique de sécurité
- L'affaire de tous et toutes
- Législation

3/ Activités internes liées à sécurité

- (In)compatibilité avec les approches dites "Agile" ? - Le mouvement DevSecOps
- Inventaire et shadow IT
- Tests : unitaires, intégration, bout en bout
- Revues de code
- Analyse statique
- Analyse dynamique
- Outils de sécurité compatible avec le CI/CD

4/ La sécurité vue de l'extérieur

- Audits de sécurité
- Politique de divulgation responsable
- Programme de prime au bug (bug bounty)

5/ Rappels de cryptographie

- La crypto en deux mots
- Chiffrement
- Hachage

MAJ : 07.08.26

Numéro de déclaration d'activité

11922694792

Durée : 3 jours -
21 heures

Code : SEW1

Prix inter : 2300 euros HT

Horaires

09:30 – 13:00 / 14:00 – 17:30

Objectifs

- Se mettre à jour au sujet de failles plus obscures mais tout aussi redoutables
- Apprendre comment mettre en place des protections efficaces
- Connaître les bonnes pratiques de développement sécurisé
- Se familiariser avec les outils de sécurité qui comptent
- Savoir mettre en place une politique de divulgation responsable

Prérequis

- Expérience en développement Web
- Une certaine expérience avec SQL

Public concerné

- Signature numérique
- Algorithmes modernes et caduques

6/ Un tour d'horizon des protocoles et langages importants

- Adresses IP et DNS
- Subdomain takeover : mécanismes et risques
- Rappels sur le protocole HTTP
- HTTPS
- TLS
- HTML/CSS/JavaScript

7/ Fuite d'informations sensibles

- Identifiants numériques séquentiels
- Messages d'erreurs verbeux
- Capture de données sensibles dans les logs
- Secrets stockés côté client
- Dépôts publics de développeurs
- Historique Git

Tour de table de régulation

JOUR 2

Tour de table

8/ Authentication & vulnerabilities

- Méthodes d'authentification
- Énumération d'utilisateurs
- Single Sign On (SSO) : OAuth 2, OpenID Connect, SAML - Contournement du rate limiting
- Questions de sécurité
- Authentification à facteurs multiples

9/ Mots de passe

- Politique de robustesse
- Mots de passe ayant fuité, haveibeenpwned
- Gestionnaire de mots de passe
- Salage et hachage
- Stockage
- Réinitialisation de mot de passe

10/ Gestion de sessions

- Cookies
- Fixation de sessions
- Vol/détournement de sessions
- Cross-site request forgery
- Clickjacking
- Cross-site script inclusion
- Contre-mesures
- JSON Web Tokens (JWTs)

11/ Autorisation / contrôle d'accès

- Distinction entre authentification et autorisation
- Rôles and permissions
- Insecure direct object reference (IDOR)
- Missing function-level access control

- Développeurs
- Chefs de projets

Dates Interentreprises

délai d'entrée : sans – Paris et à distance :
07/12/2026 - 04/01/2027 - 05/04/2027 -
05/07/2027 - 04/10/2027

Modalité d'évaluations

- L'évaluation des acquis se fait tout au long de la formation au travers d'exercices à réaliser, de mises en situation et de QCM. Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Certificat de stage

- Un certificat de fin stage est remis au participant

Compétences du formateur

- Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque formation qu'ils animent. Ils ont majoritairement cinq à dix années d'expérience dans leur domaine de compétences et ont une grande pratique en entreprise

Moyens pédagogiques et techniques

- 50% pratique et 50% théorique
- Exposés théoriques
 - Exercices individuels et collectifs

Les supports pédagogiques sont remis au format électronique aux participants. Ce support est projeté via un vidéo projecteur afin d'animer la formation. Des exercices d'application ou études de cas sont prévus afin de valider les acquis des stagiaires.

Accès handicap

- Oui, consultez notre référent interne hoully@reboot-training.fr

Modalités de suivi de l'exécution

12/ Contrôle des entrées utilisateur

- Côté client, côté serveur, ou les deux ?
- Cross-site scripting (XSS)
- Les différentes formes de XSS
- Défenses contre le XSS
- Autres formes d'injection
- Déni de service dû à l'utilisation d'expression régulières inefficaces (ReDoS)

13/ URLs

- Anatomie d'une URL
- Des disparités inquiétantes entre parseurs
- Open redirects
- Server-side request forgery
- Bonnes pratiques

Tour de table de régulation

JOUR 3

Tour de table

14/ Cross-Origin Resource Sharing (CORS)

- Les concepts d'origine Web et de site
- Same-origin policy
- Les alternatives à CORS
- Cross-Origin Resource Sharing (CORS)
- Bonnes et mauvaises configurations de CORS et risques associés
- Private Network Access

15/ Bases de données

- Principe du moindre privilège
- Injection SQL
- L'outil sqlmap
- Injection NoSQL
- Transactions et situations de compétitions

16/ Décodage

- Mass assignment
- XML : attaques de type XXE et billion laughs
- Attaques de désérialisation (Java, Python, PHP)

17/ Fichiers

- Chargement (upload)
- Path traversal
- Local-File Inclusion
- Remote-File Inclusion

18/ Risques liés aux dépendances

- Frameworks et bibliothèques
- Téléchargement sécurisé des dépendances
- Politique de mise à jour
- Software Component Analysis (SCA)
- Cas d'étude : log4shell
- Attaques de la supply chain et dependency confusion
- Vérification d'intégrité des dépendances
- Content-Management Systems (CMS)

- Contrôle systématique des présences par demi-journée
- Attestation de présence remis à chaque participant

Moyens d'accompagnement

- 10 personnes maximum, formation animée par un formateur expert sur le sujet.
- Mise en situation : Pédagogie active et participative.
- Apport théorique et méthodologique.
- Etude de cas.

Nature des travaux demandés au stagiaire

- Un exercice est réalisé par le participant à la fin de chaque chapitre. Le participant dispose de 20 min avant de passer à la correction avec le formateur.

Modalités techniques en cas de problèmes

- Les connexions et installations d'outil peuvent être testées en amont de la formation avec le formateur et les stagiaires ou le donneur d'ordre.
- Ce test permet d'éviter tout accident technique lié aux outils de connexion à distance.
- Le formateur prend la main sur le poste du participant en cas de difficulté durant la formation.
- Dans le cadre d'une formation à distance, le lien de connexion est envoyé 2 semaines avant le début de la formation
- Pour avoir une assistance, contacter nous : houliv@reboot-training.fr - 0614928564 (réponse en moins de 24 heures)

NOUS CONTACTER

Dulytech

35 rue Pierre Brossolette

92130 Issy-les-Moulineaux

Tel : 06 14 92 85 64

www.reboot-training.fr