



ENI Service

référence
T44B-030

21h

Sécuriser les applications PHP

Mise à jour
17 juillet 2023

Formation
intra-entreprise
sur devis

 (Télé-)présentiel

 Formation certifiante

Sécuriser les applications PHP



Objectifs

- ✓ Décrire les vulnérabilités des applications Web.
- ✓ Identifier et mettre en oeuvre les contre-mesures appropriées pour se prémunir contre les attaques CSRF, XSS, SQL Injection, Remote Code Injection, ...
- ✓ Crypter les données applicatives sensibles.
- ✓ Décrire l'apport des frameworks et bibliothèques PHP, pour la sécurité.
- ✓ Sécuriser l'environnement d'exécution PHP pour la production.
- ✓ Sécuriser un serveur Web Apache exécutant des applications PHP.
- ✓ Sécuriser un serveur de base de données MySQL.

Pré-requis

- Connaître le langage PHP, ou idéalement avoir suivi la formation PHP Développer des applications Web [T44B-010].

Certification

Cette formation prépare en partie à la certification Développement de sites web dynamiques Option langage PHP

Suite à la formation, une mise en pratique approfondie de plusieurs mois est nécessaire pour garantir un bon résultat à l'examen.

Pour compléter la préparation à cet examen, il est possible de suivre les formations :

PHP Développer des applications Web

Développement de Services Web en PHP

Cette certification permet de prétendre aux métiers de :

Concepteur-Développeur

Intégrateur Web

Public

- Concepteurs/Développeurs
- Testeurs
- Architectes techniques
- Chefs de projets



 02 40 92 45 50

 formation@eni.fr

www.eni-service.fr

ENI Service - Centre de Formation

adresse postale : BP 80009 44801 Saint-Herblain CEDEX

SIRET : 403 303 423 00020 B403 303 423 RCS Nantes, SAS au capital de 864 880

1 / 3



ENI Service

référence
T44B-030

21h

Sécuriser les applications PHP

Mise à jour
17 juillet 2023

Formation
intra-entreprise
sur devis

 (Télé-)présentiel

 Formation certifiante

Programme de la formation



La sécurité informatique dans un contexte Web (3 heures)

- Les différentes attaques et vulnérabilités des applications et sites Web
 - > CSRF, XSS, SQL Injection, Remote Code Injection
- Présentation des attaques et des contremesures associées
 - > La théorie des techniques de contre-mesure
 - > L'apport des frameworks de développement PHP pour la sécurité
- Travaux pratiques :
 - > Importation d'un projet d'application PHP vulnérable
 - > Identification des failles dans l'application
 - > Définition de la stratégie de sécurisation

Sécurisation du code (12 heures)

- Les différents types d'attaques visant les failles du code PHP
- Sécuriser le contenu des paramètres des requêtes HTTP
 - > Paramètre `register_globals`
 - > Remote et Local File Include
- La gestion des sessions
 - > Par les cookies
 - > Par les en-têtes
 - > Renouvellement de l'identifiant de session
- La conception et traitement des formulaires
 - > XSS
 - > CSRF
 - > Les uploads
- La protection du code SQL
 - > Les requêtes paramétrées
- Le spam
- Se prémunir contre :
 - > Les authentifications en force brute
 - > Les attaques par déni de service avec les quotas
 - > Le Phishing
- Travaux pratiques :
 - > Applications des contre-mesures aux différentes fonctionnalités de l'application
 - > Utilisation des mécanismes de PHP pour la sécurisation des formulaires, de l'accès aux données et du transfert de fichiers

Sécurisation de la plateforme (4 heures)

- Sécurisation des éléments logiciels vis-à-vis de l'OS
 - > Les groupes d'utilisateurs
 - > Les permissions sur les fichiers
- Sécurisation du serveur Web
 - > Le cas du serveur Apache
- Les paramètres d'initialisation de PHP
 - > Les différentes directives du fichier `php.ini`
 - > Les localisations de définition des directives
 - > Utilisation des directives PHP dans la configuration d'Apache

- Le cas de l'hébergement mutualisé
 - > Utilisation des directives PHP pour les hôtes virtuels
- Travaux pratiques :
 - > Création d'un hôte virtuel pour l'hébergement d'une application PHP
 - > Définition des paramètres de sécurisation des sessions, des fichiers transférés

Les bonnes pratiques (2 heures)

- Les patterns de programmation
- La gestion des mots de passe
 - > Fonctionnalités de cryptage disponible dans PHP
- Les frameworks
 - > La prise en charge des contre-mesures dans les librairies et frameworks PHP
- Travaux pratiques :
 - > Présentation de librairies et frameworks PHP et de leurs fonctionnalités natives pour la sécurisation des applications



02 40 92 45 50

formation@eni.fr

www.eni-service.fr

ENI Service - Centre de Formation

adresse postale : BP 80009 44801 Saint-Herblain CEDEX

SIRET : 403 303 423 00020 B403 303 423 RCS Nantes, SAS au capital de 864 880

2 / 3



ENI Service

référence
T44B-030

21h

Sécuriser les applications PHP

Mise à jour
17 juillet 2023

Formation
intra-entreprise
sur devis

 (Télé-)présentiel

 Formation certifiante



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

Formation avec un formateur, qui peut être suivie selon l'une des 3 modalités ci-dessous :

1 Dans la salle de cours en présence du formateur.

2 Dans l'une de nos salles de cours immersives, avec le formateur présent physiquement à distance. Les salles immersives sont équipées d'un système de visio-conférence HD et complétées par des outils pédagogiques qui garantissent le même niveau de qualité.

3 Depuis votre domicile ou votre entreprise. Vous rejoignez un environnement de formation en ligne, à l'aide de votre ordinateur, tout en étant éloigné physiquement du formateur et des autres participants. Vous êtes en totale immersion avec le groupe et participez à la formation dans les mêmes conditions que le présentiel. Pour plus d'informations : Le téléprésentiel notre solution de formation à distance.

Le nombre de stagiaires peut varier de 1 à 12 personnes (5 à 6 personnes en moyenne), ce qui facilite le suivi permanent et la proximité avec chaque stagiaire.

Chaque stagiaire dispose d'un poste de travail adapté aux besoins de la formation, d'un support de cours et/ou un manuel de référence au format numérique ou papier.

Pour une meilleure assimilation, le formateur alterne tout au long de la journée les exposés théoriques, les démonstrations et la mise en pratique au travers d'exercices et de cas concrets réalisés seul ou en groupe.

Modalités d'évaluation des acquis

En début et en fin de formation, les stagiaires réalisent une auto-évaluation de leurs connaissances et compétences en lien avec les objectifs de la formation. L'écart entre les deux évaluations permet ainsi de mesurer leurs acquis.

En complément, pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par un examen de certification.

Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification.

Pour certaines formations certifiantes (ex : ITIL, DPO, ...), le passage de l'examen de certification est inclus et réalisé en fin de formation. Les candidats sont alors préparés par le formateur au passage de l'examen tout au long de la 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 ENI.

Attestation de fin de formation, remise au stagiaire en main propre ou par courrier électronique.

Qualification du formateur

La formation est animée par un professionnel de l'informatique et de la pédagogie, dont les compétences techniques, professionnelles et pédagogiques ont été validées par des certifications et/ou testées et approuvées par les éditeurs et/ou notre équipe pédagogique.

Il est en veille technologique permanente et possède plusieurs années d'expérience sur les produits, technologies et méthodes enseignés.

Il est présent auprès des stagiaires pendant toute la durée de la formation.



02 40 92 45 50

formation@eni.fr

www.eni-service.fr

ENI Service - Centre de Formation

adresse postale : BP 80009 44801 Saint-Herblain CEDEX

SIRET : 403 303 423 00020 B403 303 423 RCS Nantes, SAS au capital de 864 880

3 / 3