SETC Training Corporate Logo

Formation sécurité TI : Sécuriser les applications web (PROSECPFR, 4 jours)

Description

Ce cours de formation en sécurité informatique offre aux participants une exploration complète de la sécurité des applications Web. Les participants sont tout d'abord initiés aux concepts essentiels du renseignement de source ouverte et de l'ingénierie sociale, tout en commençant à comprendre l'état d'esprit du pirate informatique. Vient ensuite une dissection complète de l'infrastructure qui soutient les opérations des applications Web. La formation entre ensuite dans les détails du top 10 de l'OWASP, tandis que les participants apprennent à réaliser des attaques web complexes telles que l'injection SQL, le cross site scripting, le verb tempering, les attaques XXE et bien d'autres encore. Enfin, les participants apprennent à analyser JavaScript et à écrire du code sécurisé à l'appui des applications d'entreprise. Le cours se termine par une discussion à plusieurs volets sur la configuration de la sécurité et la surveillance d'un environnement d'entreprise, y compris la sécurité de Linux et d'Active Directory.

Tarifs

- Tarification: $3,750/person
- Rabais de 10% lorsque vous inscrivez 3 personnes.

Plan de cours

Introduction

- Un mot sur l'importance de l'ingénierie sociale
- Un mot sur l'importance du renseignement de source ouverte
- Comprendre l'état d'esprit des pirates informatiques
- L'importance cruciale de l'éducation des utilisateurs

Architecture des applications web

- Comprendre la dynamique client-serveur : De la demande à la réponse
- Du nom d'hôte au payload: DNS, protocoles et serveurs Web
- Le rôle et la position du serveur de base de données
- Le rôle et la position du serveur Web
- Exploration des zones et des enregistrements DNS
- Le rôle des certificats et du protocole TLS
- Disséquer le trafic Web : Ports et protocoles
- À propos du renseignement sur les menaces, de la gestion des risques et de l'évaluation des vulnérabilités
- Utilisation de Metasploit, nmap et d'autres outils pour établir le profil d'une cible
- La topologie des vulnérabilités du Web : Où chercher ?

Aperçu du top 10 2021 de l'owasp

- Numéro 10 : Falsification de requête côté serveur
- Numéro 9 : Défaillances en matière de journalisation et de surveillance de la sécurité
- Numéro 8 : Défauts d'intégrité des logiciels et des données
- Numéro 7 : Défaillances en matière d'identification et d'authentification
- Numéro 6 : Composants vulnérables et obsolètes
- Numéro 5 : Mauvaise configuration de la sécurité
- Numéro 4 : Conception non sécurisée
- Numéro 3 : Injection
- Numéro 2 : Défaillances cryptographiques
- Numéro 1 : Contrôle d'accès défaillant
- Un plan d'action pour la sécurité du Web

Outils et techniques d'analyse

Analyse du code JavaScript
Décompression de plusieurs couches de code JavaScript emballé
Détection et suppression du code mort injecté
Rétro-ingénierie des méthodes avancées d'obscurcissement de JavaScript
Analyse statique et dynamique de JavaScript : Utilisation des outils du métier

Exploitation des sites web - injection et cross-site scripting

Qu'est-ce que l'injection et qu'est-ce qui la rend possible ?
Réalisation d'une attaque par injection - Partie I
Réalisation d'une attaque par injection - Partie II
Utilisation de mapsql pour identifier les vulnérabilités d'injection
Qu'est-ce que le Cross-Site Scripting et qu'est-ce qui le rend possible ?
Réalisation d'une attaque XSS - Partie I
Réalisation d'une attaque XSS - Partie II
Utilisation de nikto pour rechercher des vulnérabilités Web

Exploitation des sites web - modification des verbes

Exploration des VERBES HTTP
À propos de la modification des verbes HTTP
Détecter et exploiter les vulnérabilités liées à la modification des verbes HTTP
Configuration des serveurs sécurisés : Prévention des vulnérabilités liées à la modification des verbes HTTP

Exploitation des sites web - iodr

Que sont les vulnérabilités IDOR et comment se produisent-elles ?
Exemples de code vulnérable à IDOR
Différents types de vulnérabilités IDOR
Comment détecter les vulnérabilités IDOR
Différentes méthodes d'exploitation des vulnérabilités IDOR
Prévention des vulnérabilités IDOR

Exploitation des sites web - xxe

Que sont les vulnérabilités XXE, et comment se produisent-elles ?
Exemples de code vulnérable au XXE
Identification et exploitation des vulnérabilités XXE
Techniques de prévention XXE

Codage sécurisé

Identification des problèmes de sécurité courants dans le code JavaScript
Identification d'une vulnérabilité d'injection de commande dans les codes JavaScript
Identification d'une vulnérabilité avancée de type XSS (Cross-Site Scripting)
Vérification de l'existence de la vulnérabilité
Corrections des erreurs et des vulnérabilités identifiées

Gestion de la sécurité

Lignes directrices du NIST pour les mots de passe
Conception de processus de gestion de la sécurité
Sécurisation d'Active Directory et des machines Linux
Planification du stockage sécurisé des mots de passe
Un mot sur les autres services : IPMI, DNS, SMTP et autres
Assurer des configurations sécurisées
Assurer la surveillance