Sécurité Technique

Préparation Offensive Security Web Expert (OSWE)

Vous allez apprendre à

La préparation à la certification Offensive Security Web Expert (OSWE) vous permettra de maîtriser les techniques avancées de test d'intrusion spécifiques aux applications web. Vous apprendrez à identifier et exploiter des vulnérabilités complexes dans des environnements web, en vous concentrant sur l'analyse du code source, l'exploitation des failles logiques et la manipulation des flux applicatifs. Cette formation mettra l'accent sur la compréhension approfondie des mécanismes internes des applications web, ainsi que sur la capacité à développer des exploits personnalisés pour démontrer la compromission. Vous développerez ainsi une expertise pointue pour sécuriser efficacement les applications web contre les attaques ciblées.

Public visé

- Testeurs d'intrusion expérimentés souhaitant approfondir l'audit de sécurité des applications web.
- Spécialistes en sécurité des applications web.
- Développeurs web souhaitant renforcer leurs compétences en sécurité.

Les objectifs de la formation

- Maîtriser les techniques avancées d'audit de sécurité des applications web en environnement « white-box ».
- Identifier et exploiter des vulnérabilités complexes via l'analyse de code source.
- Développer des scripts d'exploitation personnalisés pour des applications web.
- Préparer et réussir l'examen de certification OSWE.

Les prérequis de la formation

- Confort dans la lecture et l'écriture d'au moins un langage de programmation (PHP, Java, C#, JavaScript).
- Familiarité avec Linux.
- Capacité à écrire des scripts simples en Python, Perl, PHP ou Bash.
- Expérience avec des proxys web (ex. Burp Suite).
- Compréhension générale des vecteurs d'attaque des applications web.

Programme de la formation

Introduction et méthodologie

- Présentation du cours AWAE.
- Approche pédagogique et objectifs.
- Utilisation des laboratoires AWAE.

Outils et méthodologies

- Inspection du trafic web avec Burp Suite.
- Interaction avec des écouteurs web via Python.
- Récupération et analyse de code source.
- Méthodologie d'analyse de code source.
- Débogage et débogage à distance.

Études de cas pratiques

- ATutor : contournement d'authentification et exécution de code à distance.
- ATutor LMS : vulnérabilité de type juggling.
- ManageEngine Applications Manager : injection SQL et RCE.
- Bassmaster NodeJS : injection JavaScript arbitraire.
- DotNetNuke : désérialisation de cookies et RCE.
- ERPNext : contournement d'authentification et SSTI.
- openCRX : contournement d'authentification et exécution de code à distance.
- openITCOCKPIT : XSS et injection de commandes OS.
- Concord : contournement d'authentification vers RCE.
- Guacamole Lite : pollution de prototype JavaScript.