WEB-300 - Advanced Web Attacks and Exploitation (AWAE/OSWE)

Durée: 5 Jours **Réf de cours: GK840106** **Méthodes d'apprentissage: Intra-entreprise & sur-mesure**

Résumé:

OffSec's Advanced Web Attacks and Exploitation (WEB-300) course dives deep into the latest web application penetration testing methodologies and techniques. Learners gain extensive hands-on experience in an environment designed to elevate their skills in ethical hacking, vulnerability discovery, and exploit development.
Successful completion of the course and challenging exam earns the OffSec Web Expert (OSWE) certification. This web application security certification validates expertise in advanced web application security testing, including bypassing defenses and crafting custom exploits to address critical vulnerabilities, making certified professionals an asset for securing any organization against web-based threats.
Upd Apr2025

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

Public visé:

The WEB-300 course is ideal for experienced penetration testers and security professionals seeking to master advanced web application attacks and exploitation techniques, ultimately earning the OSWE certification.

Objectifs pédagogiques:

- Upon completing WEB-300 and successfully passing the OSWE exam, youll have mastered advanced web application security methodologies, including:
- In-depth vulnerability analysis and exploitation
- Custom exploit development
- Bypassing modern web application defenses
- Exploiting authentication and authorization flaws
- Attacking API endpoints and cloud-native applications

Pré-requis:

While there are no formal certification prerequisites, its strongly recommended that you have:

- Comfort reading and writing at least one coding language
- Familiarity with Linux
- Ability to write simple Python / Perl / PHP / Bash scripts
- Experience with web proxies
- General understanding of web app attack vectors, theory, and practice

Contenu:

Introduction

- About the AWAE Course
- Our Approach
- Obtaining Support
- Offensive Security AWAE Labs
- Reporting
- Backups
- About the OSWE Exam

Tools ; Methodologies

- Web Traffic Inspection
- Interacting with Web Listeners using Python
- Source Code Recovery
- Source Code Analysis Methodology
- Debugging

ATutor, Authentication, Bypass and RCE

- Initial Vulnerability Discovery
- A Brief Review of Blind SQL Injections
- Digging Deeper
- Data Exfiltration
- Subverting the ATutor Authentication
- Authentication Gone Bad
- Bypassing File Upload Restrictions
- Gaining Remote Code Execution

ATutor LMS Type, Juggling Vulnerability

- PHP Loose and Strict Comparisons
- PHP String Conversion to Number
- Vulnerability Discovery
- Attacking the Loose Comparison

ManageEngine, Applications Manager, AMUserResourcesSyn, cServlet SQL Injection, RCE

- Vulnerability Discovery
- How Houdini Escapes
- Blind Bats
- Accessing the File System
- PostgreSQL Extensions
- UDF Reverse Shell
- More Shells!!!

Bassmaster NodeJS, Arbitrary JavaScript, Injection Vulnerability

- The Bassmaster Plugin
- Vulnerability Discovery
- Triggering the Vulnerability
- Obtaining a Reverse Shell

DotNetNuke Cookie, Deserialization RCE

- Serialization Basics
- DotNetNuke Vulnerability Analysis
- Payload Options
- Putting It All Together

ERPNext, Authentication Bypass and Server Side Template Injection

- Introduction to MVC, Metadata-Driven Architecture, and HTTP Routing
- Authentication Bypass Discovery
- Authentication Bypass Exploitation
- SSTI Vulnerability Discovery
- SSTI Vulnerability Exploitation

openCRX, Authentication Bypass and Remote Code, Execution

- Password Reset Vulnerability Discovery
- XML External Entity Vulnerability Discovery
- Remote Code Execution

openITCOCKPIT XSS and OS Command Injection – Blackbox

- Black Box Testing in openITCOCKPIT
- Application Discovery
- Intro To DOM-based XSS
- XSS Hunting
- Advanced XSS Exploitation
- RCE Hunting

Concord, Authentication Bypass to RCE

- Authentication Bypass: Round One - CSRF and CORS
- Authentication Bypass: Round Two - Insecure Defaults

Server-Side Request, Forgery

- Introduction to Microservices
- API Discovery via Verb Tampering
- Introduction to Server-Side Request Forgery
- Render API Auth Bypass
- Exploiting Headless Chrome
- Remote Code Execution

Guacamole Lite, Prototype Pollution

- Introduction to JavaScript Prototype
- Prototype Pollution Exploitation
- EJS Handlebars

Conclusion

- The Journey So Far
- Exercises and Extra Miles
- The Road Goes Ever On

Méthodes pédagogiques :

Official course book provided to participants.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement