

EC-Council - Web Application Hacking and Security (WAHS)

EC-Council's Web Application Hacking and Security ist eine Spezialisierungszertifizierung, die es den Cybersecurity-Mitarbeitern ermöglicht, Webanwendungen zu erlernen, zu hacken, zu testen und vor bestehenden und aufkommenden Sicherheitsbedrohungen in den verschiedenen Branchen zu schützen. Web Application Hacking and Security ist wie ein Capture-The-Flag (CTF)-Wettbewerb, um Ihre Hacking-Fähigkeiten zu testen. Aber Sie können es so lange versuchen, bis Sie das Ziel erreicht haben. Testen Sie Ihre Fähigkeiten und arbeiten Sie alleine, um komplexe Probleme zu lösen, oder folgen Sie dem Ausbilder, der Ihnen mit Hilfe eines Walkthroughs hilft, Web Application Hacking and Security zu lernen.

Zielgruppe:

Wenn Ihre Aufgabe darin besteht, Webanwendungen zu implementieren, zu verwalten oder zu schützen, dann ist dieser Kurs genau das Richtige für Sie. Wenn Sie ein Cyber- oder Technikprofi sind, der daran interessiert ist, Methoden zur Bewältigung einer Vielzahl von Web-Sicherheitsproblemen zu erlernen oder zu empfehlen und ein rein praxisorientiertes Programm wünschen, dann ist dies der Kurs, auf den Sie gewartet haben.

Der Kurs wird in Zusammenarbeit mit dem akkreditierten TrainingCenter EDC-Business Computing GmbH durchgeführt.

Seminar- bzw. Schulungsinhalte

- Advanced Web Application Penetration Testing
- Advanced SQL Injection (SQLi)
- Reflected, Stored and DOM-based Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF) GET and POST Methods
- Server-Side Request Forgery (SSRF)
- Security Misconfigurations
- Directory Browsing/Bruteforcing
- CMS Vulnerability Scanning
- Network Scanning
- Auth Bypass
- Web App Enumeration
- Dictionary Attack
- Insecure Direct Object Reference Prevention (IDOR)
- Broken Access Control
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- Arbitrary File Download
- Arbitrary File Upload
- Using Components with Known Vulnerabilities
- Command Injection
- Remote Code Execution
- File Tampering
- Privilege Escalation
- Log Poisoning

- Weak SSL Ciphers
- Cookie Modification
- Source Code Analysis
- HTTP Header modification
- Session Fixation
- Clickjacking

Seminar- bzw. Schulungsvoraussetzungen

Keine Angaben

Seminarart

Dieses Seminar können Sie als **Präsenzseminar** oder als **Live-Online-Training** (virtuelles Präsenzseminar) buchen.

Dauer

3 Tage von 09:00 bis 18:30 Uhr

Preise

Die Teilnahmegebühr beträgt 2.950,00 € (3.510,50 € inkl. 19% MwSt.)

Im Preis enthalten sind Kursmaterial, Pausenverpflegung, Getränke und Schulungszertifikat.

Anmeldung

Bitte **online** anmelden oder per **Fax**.

Termine

Die aktuellen Termine und Standorte für EC-Council - Web Application Hacking and Security (WAHS) finden Sie **online**.

Weitere Seminare

Alle Seminare finden Sie in unserer **Seminarübersicht**.

Gerne unterbreiten wir Ihnen auch ein individuelles Angebot entsprechend Ihrer Wünsche und Vorstellungen. Senden Sie hierfür Ihre Anfrage einfach an **training@pc-college.de**.

Erstellt am 27.04.2024

Viele Partner für ein Ziel: Beste Leistung und Rundum-Service

Live-Online-Training

Berlin
Bremen
Dortmund
Dresden
Düsseldorf
Erfurt
Essen
Frankfurt
Freiburg
Hamburg
Hannover
Jena
Karlsruhe
Kassel
Koblenz
Köln
Krefeld
Leipzig
Mannheim
München
Münster
Nürnberg
Paderborn
Regensburg
Saarbrücken
Siegen
Stuttgart
A-Wien
CH-Basel
CH-Bern
CH-Zürich



PC-COLLEGE Zentrale Berlin

Stresemannstraße 78 (Nähe Potsdamer Platz) | D-10963 Berlin
Telefon: 0800 5777 333 / +49 (0)30 235 0000 | Fax: +49 30 2142988 | E-Mail: training@pc-college.de
Ansprechpartner*in: Stefanie Wendt und Kollegen*innen

Alle Informationen und Aktionsangebote finden Sie unter www.pc-college.de