integrata Cegos Group | inspire qualify change

WEB HACKING

Angriffe gegen Webserver und -anwendungen erkennen und vorbeugen

Dauer: 3 Tage

Durchführungsart: Präsenztraining

Zielgruppe: Dieser Web Hacking Kurs ist insbesondere für Webentwickler, Webprogrammierer, Webadministratoren, Webverantwortliche, IT-Sicherheitsbeauftragte geeignet.

Voraussetzungen: Kenntnisse in den Bereichen Webtechniken, Webentwicklung, Netzwerke und Datenbanken sind von Vorteil, aber keine Voraussetzung.

Nr.: 5213
Preis: 1.590€ netto / 1.892,10 € inkl. 19 % MwSt.

Schulungsmethode: Unsere praxiserfahrenen Trainer erläutern Ihnen die theoretischen Grundlagen von Web Hacking und demonstrieren anhand von Beispielen die wesentlichen Elemente von Hacker Angriffen auf Webapplikationen. Das vermittelte Wissen wenden Sie anhand von praktischen Übungen direkt an und haben die Möglichkeit mit anderen Teilnehmern ihr Wissen auszutauschen.

Die Kenntnis der Angriffstechniken gegen Webserver und -anwendungen ist die Grundvoraussetzung für die erfolgreiche Abwehr von Hackern. Das Seminar Web Hacking ist so ausgelegt, dass es jedem, auch nicht technisch versierten, einen möglichst einfachen Einstieg in die Hacking Thematik bietet. Anhand vieler praktischer Beispiele und Erfahrungsberichte wird das notwendige Know-how vermittelt und notwendige Tools vorgestellt, um Vorgehensweisen von Hackern zu verstehen und direkt erste Sicherheitskonzepte umsetzen zu können.
Das Seminar geht dabei auf alle wesentlichen Komponenten ein, die im Zusammenspiel mit Webanwendungen verbunden sind (Netzwerk-, System-/Server- und Anwendungssicherheit).

Programm

Hacking Grundlagen:

- Erkennung der Angriffsziele und Bedrohungen
- Vorgehensweisen bei einem Angriff
- Protokolle im Web
- SSL (Un)Sicherheit

Hacking auf System- / Dienstebene:

- Informationsgewinnung
- Kennenlernen des Angriffsziels
- Untersuchung des Zielsystems
- Mögliche Security Schwachstellen
- Geläufige Webserver Architekturen
- Angriffe auf Datenbanksysteme
- Grundlagen für den sicheren Serverbetrieb
- Schutz des Serversystems

Anwendungsebene:

- Aktuelle Zahlen und Fakten
- Lebenszyklus einer Webanwendung: Sicherheit und Kosten
- Angriffe auf Authentifizierung und Autorisierung im Web
- Session Management und die Gefahren
- Tücken der Ein- und Ausgabe Validierung

- Setzen von Vertrauensgrenzen
- Grundlegende, neue/unbekanntere und zukünftige Cross-Site-Scripting (XSS) Angriffstechniken
- SQL Injections
- LDAP Injections
- Cross-Site-Request-Forgery (CSRF)
- Web 2.0 und HTML5: neue Techniken und deren Gefahren
- Maßnahmen zur Abwehr
- Codebeispiele

Web hacking Testwerkzeuge:

- Portscanner
- Web Application Scanner
- Exploiting Frameworks
- Intercepting Proxies
- SSL Proxies
- Password Bruteforcer
- Sniffer/Man-in-the-Middle Tools
- Browser Plugins
- Code Audit Tools
- Blackbox Testing
- Session Vorhersageprüfung
- übungs- und Testsysteme zur Festigung des Gelernten

Mitigating Controls:

- Web Application Firewalls
- Aktive, programmatische überwachung
- Reverse Proxys
- Aspektorientierte Programmierung
- AppArmor und SELinux

Extras:

- Ausführliche Sicherheitscheckliste für die tägliche Arbeit
- Praktische übungen
- Erfahrungsberichte über Angriffe

Termine und Orte – Nr.: 5213

München

29 Jul - 31 Jul 2019

Hamburg

18 Nov - 20 Nov 2019