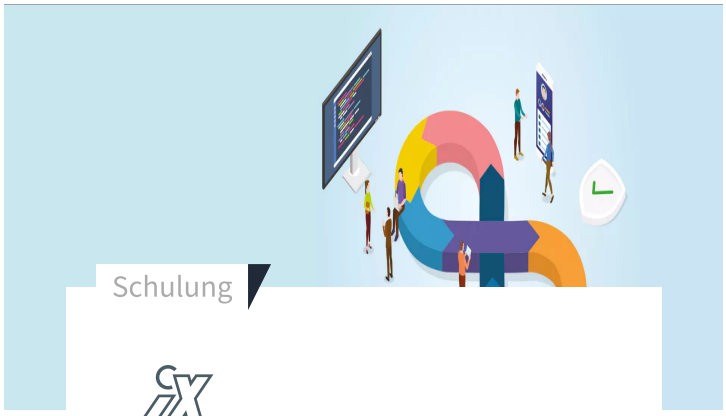
Sie suchen Ihre bereits erworbenen Lerninhalte? Dann geht es hier entlang:

Zum academy Campus

heise academy



Schulung

DevSecOps: Automatisierte Sicherheitstests für die Webentwicklung

Webentwicklung

19.02. – 20.02.2024

09:00 – 17:00 Uhr

1.650,^{00} €*

Ticket wählen

+ 2 weitere Optionen

Überblick

Zunächst machen Sie sich in dieser Schulung mit den Grundlagen der Sicherheit moderner Webanwendungen vertraut. Auf Basis vieler Beispiele lernen Sie anschließend in mehreren theoretischen und praktischen Teilen die einzelnen Themen theoretisch, aber auch praktisch kennen. Die Vertiefung und konkrete Anwendung der Tools

Sie lernen in einer Übungsumgebung in der Cloud, wie Sie (automatisierte) Sicherheitsprüfungen auf Anwendungsebene in den DevSecOps-Prozess integrieren. Vorgestellt werden Werkzeuge, die zur Überprüfung von Anwendungen und Systemen dienen können und Sie erfahren, wie sich diese in bestehende Jenkins-Pipelines integrieren lassen.

Mit Christian Biehler

Schulung

DevSecOps: Automatisierte Sicherheitstests für die

und Vorgehensweisen erfolgt in einer Demo-und-Übungsumgebung in der Public Cloud.

Zielgruppe

Interessenten aus den Bereichen Systemadministration/DevOps, Softwareentwicklung sowie IT-Sicherheit

Voraussetzungen

Zur Workshop-Durchführung wird Zoom verwendet mittels eines DSGVO-konformen On-Premise-Connectors. Wir bitten Sie, ein Mikrofon oder Headset sowie einen aktuellen Browser zu nutzen.

Unterlagen

- Sie erhalten die Schulungsunterlagen während der Schulung in Präsentationsform in

deutscher Sprache als PDF-Dokument. (Es gibt keine ausgedruckten Schulungsunterlagen)

- Die während des Workshops gezeigten Scriptlets und Commandline-Parameter können Sie über das GIT-Repository von bi-sec herunterladen und verwenden

Inhalte

1. Einführung in gängige Standards zur Web-Sicherheit, z. B.

- OWASP Top 10, OWASP ASVS und SANS CWE Top 25
- Vor- und Nachteile der individuellen Standards

2. Einführung in Kali-Linux und gängige Prüfwerkzeuge für (Web-) Anwendungen

- Verbindungssicherheit / TLS
  Header

4. Schwachstellen auf System- und Dienstebene erkennen und beheben

- Nutzung automatisierter Werkzeuge
- Härtung und Absicherung von Diensten wie Tomcat auf Linux

5. Einführung DevSecOps mit Beispielen aus der Praxis

- Was gehört zur CI-/CD-Pipeline mit Fokus auf Sec
- Wie machen es andere Firmen?

- Abgrenzung der Möglichkeiten und Grenzen von automatisierten „Scannern“, manuellen Pentests und Quellcode-Prüfungen
- Einführung in die Sicht eines Hackers auf Webanwendungen und Pentest-Proxies

3. Kennenlernen und verstehen typischer Angriffsvektoren von Webanwendungen:

- SQL-Injections, Command-Injections und co.
- Authentifizierung und Autorisierung
- Cross-Site-Scripting
- HTML5: Tags und Browserspeicher
- JavaScript / client-seitige Eingabevalidierung
- WebSockets
- Cross-Origin-Resource-Sharing

6. Security im agilen Entwicklungsumfeld

- Sicherheit der Entwicklungslandschaft
- Sicherheit der entwickelten Anwendung
- Sicherheit von Dritt-Bibliotheken und co.
- Absicherung der Konfiguration der Anwendungssysteme

7. Vorstellung möglicher Sec-Anteile in der CI-/CD-Pipeline

- Sec-Tools für eine CI-/CD-Pipeline
- Diskussion bisher verwendeter Tools in der aktuellen Pipeline des Kunden
- Integration von automatisierten Security-Tools in Jenkins („as Code" vs. „Plugin)
- Umgang mit False-Positives bei automatisierten Sicherheitsüberprüfungen

Demos und Übungen

1. Im Rahmen unserer Übungen und Demos behandeln wir in diesem Workshop folgende Themen:

- Spidern und automatisierte Schwachstellenscans auf Anwendungsebene
- Passive Suche nach Schwachstellen in Webanwendungen
- Erkennen und automatisiert prüfen von typischen Webschwachstellen:
  - SQL-Injection
  - Local file inclusion
  - OS-Command-Injection
  - Cross-Site-Scripting
  - Cross-Site-Request-Forgery
  - HTML5- und WebSocket
- Tool-basierte Basisabsicherung von Tomcat aus Linux
- Umgang mit API-Keys und GIT-Repositories
- Einbau von Security-Tools in die Jenkins Pipeline
- Exemplarische Auswertung der Tool-Ausgaben
- Umgang mit False-Positives in der Build-

In unserer Demo- und Übungsumgebungen verwenden wir u.a. Java und PHP. Die Bearbeitung der Tool-Ausgaben richtet sich oft nach den Tools selbst, findet typischerweise aber in Python statt. Neben selbst entwickelten Labs sind beispielsweise noch der OWASP Juice Shop und die DVWA in die Lab-Umgebung eingebunden.

Werkzeuge und Tools

1. In den Übungen und Demos kommen unter anderem folgende Werkzeuge und Tools zum Einsatz. Den Großteil davon werden Sie im Workshop auch selbst anwenden:

- OWASP ZAP
- Burp Suite
- sqlmap
- nikto
- SSLScan
- nmap
- hydra
- tesseract
- OWASP ZAP (Automatisierung per API)
- OpenVAS (& Nessus)
- OWASP Dependency Checker
- CodePulse
- SonarCube
- RIPS
- DeepDive

Leistungen Ihres Workshoptickets

- Workshopunterlagen
- Teilnahmebescheinigung

Durchführung

Ist die Durchführung der Veranstaltung aufgrund höherer Gewalt, wegen Verhinderung eines Referenten, wegen Störungen am Veranstaltungsort oder aufgrund zu geringer Teilnehmerzahl (weniger als 50%) nicht möglich, werden die Teilnehmer spätestens 7 Tage vorher informiert.

Die Teilnehmerzahl ist auf max. 20 Personen begrenzt.

Christian Biehler

IT-Berater und Geschäftsführer | bi-sec GmbH

Zum Profil

Schulung

DevSecOps: Automatisierte Sicherheitstests für die Webentwicklung

19.02. – 20.02.2024

09:00 – 17:00 Uhr

1.650,^{00} €*

Ticket buchen

10% Frühbucherrabatt bis zum 28. Mai 2024

26.06. – 27.06.2024

09:00 – 17:00 Uhr

1.650,^{00} €* **1.485,^{00} €***

Ticket buchen

10% Frühbucherrabatt bis zum 9. Sep. 2024

08.10. – 09.10.2024

09:00 – 17:00 Uhr

1.650,^{00} €* **1.485,^{00} €***

Ticket buchen

Haben Sie Fragen zu unseren Schulungen? Wir helfen Ihnen gern weiter.

Füllen Sie ganz einfach und bequem das Kontaktformular aus und wir werden Ihnen Ihre Fragen schnellstmöglich beantworten.

Team Schulungen

workshops@heise-academy.de

+49 511 5352 8604

Telefonisch erreichbar: Mo – Fr | 09:00 – 17:00 Uhr

Unsere Antworten auf die häufigsten Fragen

Kontaktformular

Anrede

Bitte wählen

Vorname

Nachname

Unternehmen

Position (optional)

Telefon

E-Mail

Ihre Anfrage

Bei Betätigen des Absenden-Buttons verarbeiten wir die von Ihnen angegebenen personenbezogenen Daten ausschließlich für den Zweck Ihrer Anfrage. Weitere Informationen zum Datenschutz finden Sie in unserer Datenschutzerklärung.

Absenden

Unsere Marken

*Alle Preise verstehen sich inklusive der gesetzlichen MwSt. und ggf. zzgl. Versandkosten.