Seminarangebot WEBAPP-SEC

Sicherheit für Webanwendungen

Stand 2026-06

Die Mehrheit aller Web-Anwendungen hat ernste Sicherheitslücken. Die Mehrheit der Nutzer ahnt nichts davon. Und – Hand aufs Herz – die meisten Entwickler:innen auch nicht. Genau hier setzt dieses Seminar an.

In diesem intensiven, praxisorientierten Seminar schlüpfst du selbst in die Rolle des Angreifenden: An einer bewusst verwundbaren Beispiel-Anwendung spürst du die kritischsten Sicherheitslücken systematisch auf, exploitest sie live – und schließt sie anschließend Schritt für Schritt. Du erlebst hautnah, wie verblüffend einfach ein Angriff sein kann und wie wenig es oft braucht, um gravierende Fehler von vornherein zu vermeiden.

Wir arbeiten uns entlang der OWASP Top 10 (Version 2025) durch alle relevanten Angriffsklassen: von SQL- und Command-Injection über Cross-Site-Scripting, XXE, SSRF und CSRF bis hin zu Broken Access Control. Du lernst, wie Authentifizierung wirklich sicher umgesetzt wird – mit modernem Passwort-Hashing, MFA und Passkeys –, wie HTTP-Security-Header (CSP, CORS, HSTS & Co.) deine Anwendung härten und warum die gefährlichste Schwachstelle manchmal vor dem Bildschirm sitzt (Social Engineering).

Brandaktuell: Wir sezieren echte Software-Supply-Chain-Angriffe wie den Shai-Hulud-npm-Wurm – und zeigen, warum dein nächstes `npm install` ein Sicherheitsvorfall sein kann.

Software Security
Hannes Molsen
Wieselgang 7 | 23683 Scharbeutz
mail@sosec.de | 0162/7160342
Steuernummer 25/077/04553

KI IST ÜBERALL – WIR NUTZEN SIE OFFENSIV UND DEFENSIV

Künstliche Intelligenz zieht sich als roter Faden durch das ganze Seminar – vom Finden bis zum Fixen der Lücken:

- Du nutzt LLMs, um Schwachstellen aufzuspüren, Exploits zu bauen und Fixes zu generieren.
- Du verstehst die neue Angriffsfläche, die KI selbst mitbringt: Prompt Injection, Prompt Leaking, Jailbreaking und die Tücken von RAG.
- Im Highlight binden wir den Security-Scanner ZAP (zaproxy) so an, dass er sich per LLM steuern lässt – Pentesting in natürlicher Sprache, live demonstriert.

TECHNOLOGIEUNABHÄNGIG UND SOFORT ANWENDBAR

Die vermittelten Konzepte sind unabhängig von konkreten Sprachen und Frameworks. Output-Escaping zeigen wir exemplarisch quer durch den Stack (ASP.NET, PHP, JSP, JSF, React & Co.), damit du das Gelernte direkt in dein eigenes Projekt übertragen kannst – egal, womit du arbeitest.

FÜR WEN?

Dieses Seminar richtet sich an Softwareentwickler:innen sowie Software-Architekt:innen, die ihre Web-Anwendungen wirksam gegen die häufigsten und gefährlichsten Angriffe schützen wollen – und die verstehen möchten, wie Sicherheit und KI zusammenspielen.

INHALT

- OWASP-Einführung (OWASP Top 10 2025, Cheat Sheets, Werkzeuge)
- Software-Supply-Chain-Sicherheit (npm-Security, Dependency-Management, SBOM, SCA)
- Injektionsangriffe (SQL Injection, Command Injection, uvm.)
- KI- & LLM-Sicherheit (Prompt Injection, Prompt Leaking, Jailbreaking, RAG)
- Authentifizierung & sichere Passwörter (Hashing, Salting, MFA, Passkeys, OAuth)
- XML External Entities (XXE) & „Billion Laughs“
- Server-Side Request Forgery (SSRF)
- Cross-Site-Scripting (DOM-based, Reflected, Stored)
- Session Hijacking & Cookie-Flags
- Cross-Site Request Forgery (CSRF) – Tokens, SameSite, Fetch-Metadata
- Input Validation / Output Escaping (Sanitization)
- HTTP-Security-Header (CSP, SOP, CORS, HSTS, Clickjacking-Schutz, uvm.)

- Social Engineering & menschliche Faktoren
- Access Control (Path Traversal, Privilege Escalation, IDOR)
- Dynamic Application Security Testing mit KI (ZAP ❤️ Claude Code)

VORAUSSETZUNGEN

Du bist erfahren mit mindestens einer Programmiersprache und kennst Grundlagen der Webentwicklung, d.h. Begriffe wie: HTTP, HTML, Browser, Service. Hilfreich aber nicht zwingend erforderlich sind Basis-Kenntnisse in SQL und JavaScript. Die Übungen finden in Java statt, Sie benötigen aber keine Java-Kenntnisse.

TEILNEHMERINNENZAHL

Das Seminar kann für 2-10 Personen angeboten werden.

RAHMENBEDINGUNGEN

Die Schulung findet an 3 aufeinanderfolgenden Tagen statt und kann sowohl als Präsenzveranstaltung wie auch remote als Live Online Seminar durchgeführt werden.

Tag 1:	9:00 – 17:00
Tag 2:	9:00 – 17:00
Tag 3:	9:00 – 16:00

Das Seminar findet zu einem großen Teil als praktischer Teil in einer virtuellen Maschine statt. Informationen zur Rechnervorbereitung findest du auf

https://vulnerads.de

Statt deinen Rechner vorzubereiten können die praktischen Übungen auch ganz komfortabel in einer Cloud-Umgebung durchgeführt werden – dann braucht nichts vorbereitet werden. Ein Browser und ein Internetzugang genügen!

LIVE ONLINE SEMINAR

Online-Seminare finden über Zoom statt. Die Einwahldaten werden ca. eine Woche vor dem Seminar übermittelt.

Ich empfehle, dass du dich im Vorfeld mit der Plattform Zoom vertraut machst. Damit auch alle benötigten Zoom-Features zur Verfügung stehen, muss eine App ausgeführt werden. Vor dem Seminar solltest Du testen, ob alles funktioniert: https://zoom.us/test.

Apps gibt es für PC, Mac, iOS oder Android. Für die Bildschirmfreigabe empfiehlt sich aber eine Teilnahme vom Rechner (PC, Mac): https://zoom.us/download.

Bitte schalte während des Seminars deine Kamera ein. Das visuelle Feedback ist für ein interessantes und den Teilnehmenden angepasstes Seminar unerlässlich.