



SySS-Workshop: Sicherheit bei Web-Applikationen (2 Tage)

Für Hacker sind Web-Applikationen heutzutage das Einfallstor Nummer 1. Oftmals finden sie Schwachstellen, die ihnen ermöglichen, sensible Daten zu entwenden und weiter in das System bis hin zum Unternehmensnetzwerk vorzudringen.

Dieser zweitägige Workshop richtet sich an Web-Developer und Mitarbeiter im IT-Bereich, die Web-Applikationen programmieren, bzw. zu betreuen haben. Im Rahmen der Fortbildungsmaßnahme lernen die Teilnehmer, wie Hacker in Web-Applikationen einbrechen und welchen Gefahren so manche Anwendungen ausgesetzt sind.

Der Workshop stellt die gängigsten Angriffe zunächst in der Theorie dar und geht anschließend mit Übungen darauf ein, wie sie in der Praxis umgesetzt werden können. Ziel des Workshops ist es, dass die Teilnehmer am Ende des zweiten Schultages selbst Angriffe auf eine eigens für den Workshop erstellte Web-Applikation durchführen können.

Der Workshop wird die folgenden Hauptthemen detailliert behandeln:

- **Cross-Site Scripting (XSS)** Angriffe auf Sitzungsinformationen, Phishing und Defacing
- **Cross-Site Request Forgery (XSRF)** Wie Angreifer Applikationsnutzer dazu bringen, das zu tun, was sie wollen
- **SQL-Injection** Unberechtigtes Auslesen von Daten aus einer Datenbank
- **OS Command Injection** Einschleusen von eigenen Betriebssystem-Kommandos in eine Web-Applikation
- **Local/Remote File Inclusion (LFI/RFI)** Wie Hacker eigenen Programmcode auf dem angegriffenen Server ausführen können
- **Session-Hijacking** Übernahme fremder Sitzungen mit Hilfe von Cross-Site Scripting-Angriffen
- **Cookies** Was bei der Generierung und Verwendung von (Session-)Cookies zu beachten ist

Grundkenntnisse in HTML, HTTP und SQL werden vorausgesetzt.