

# PHP- / Webserverversicherheit

## Dozent

**Richard Temme**

Der Dozent Richard Temme arbeitet seit mehreren Jahren als PHP-Entwickler und Trainer bei der Firma Peter Prochaska Softwareentwicklung. Er ist Zend Certified Engineer und hat bereits mehrere Schulungen in den Bereichen Zend Framework und PHP-Security gehalten.

## Ablauf

### Grundlegende Prinzipien und Einführung in die Materie

- Was ist Sicherheit?
- Diskussion: Sicherheitskonzepte im Vergleich
- Warum ist Sicherheit notwendig (Beispiele bekannter Hacks etc.)?

### Grundlegende Prinzipien und Einführung in die Materie

- Facetten der Sicherheit als Teilaspekte eines tragfähigen Sicherheitskonzepts
- *Kenne Deinen Feind* - wie Angreifer ein Zielsystem auskundschaften

### Parametermanipulation & Autorisierung

- Manipulation an GET-Parametern (?include=/etc/passwd et al.)
- Welche weiteren Parameter kann man manipulieren (Header-Manipulation, POST, etc.)
- Auswirkungen solcher Manipulationen
- Warum `register_globals` böse ist
- Eigene Skripte säubern, Parametermanipulation verhindern
- Abgrenzung der AAA: Authentication, Authorization, Accounting

### Parametermanipulation & Autorisierung

- Authentifizierung in PHP über Formulare oder Apache-Auth sicher gestalten
- Common Pitfalls
- nicht-algorithmische Attacken (Bruteforce, Social Engineering, Raten) verhindern
- Authentifizierungsklassen in PEAR

## SQL-Probleme

- SQL-Datenbanken sinnvoll konfigurieren (Netzwerk, Zugriffskontrolle etc.)
- SQL-Injection: Typen (First Order, Second Order)
- Prominente Opfer von SQL-Injection
- First-Order SQL Injection: Beispiele
- First-Order SQL-Injection: Vermeidungsstrategien
- Second-Order SQL Injection: Beispiele
- Second-Order SQL-Injection: Vermeidungsstrategien
- Übungen und Vertiefung

## XSS, Sessions, Exploits in PHP

- Was ist XSS?
- Was kann XSS?
- Wie verhindere ich XSS? (übungen)
- Sessions: Wo liegen die Gefahren?
- Sessions in eigenen Applikationen sicher einsetzen
- Sessions in Shared-User Environments
- Session Fixation/Session-Attacken