

PHP-Sicherheit

Dozent: Peter Prochaska

Ablaufplan

Täglich von 9 bis 18 Uhr - Montag 10 bis 18 Uhr

Montag

Grundlegende Prinzipien und Einführung in die Materie

Was ist Sicherheit?

Diskussion: Sicherheitskonzepte im Vergleich

Warum ist Sicherheit notwendig (Beispiele bekannter Hacks etc.)?

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

Authentication und Authorization

Parametermanipulation & Autorisierung

Authentifizierung in PHP über Formulare sicher gestalten

nicht-algorithmische Attacks (Bruteforce, Social Engineering, Raten) verhindern

Authentifizierungsklassen in PEAR

Dienstag

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-Attacken

Mittwoch

Server-Konfiguration

Apache mit PHP konfigurieren und sichern

Hardened-PHP

mod_security: web-based intrusion detection and prevention

Eigene Applikationen werden zusammen penetriert.

Ende am Mittwoch nach Absprache gegen 15:30/16:00 Uhr.