



mit jahrelanger Application Developer Erfahrung in den Bereichen PHP, Java und C++ war er Teamleiter GMX Applications Services und für die Absicherung des gesamten GMX Webaustritts zuständig.

“nur wer den Blickwinkel des Angreifers kennt hat die Möglichkeit eigene Applikationen auf Schwachstellen zu überprüfen, und diese effektiv zu beseitigen.”

Jan Röseler studierte an der Universität Passau Informatik mit Vertiefungsgebiet Informationssysteme / Wissensbasierte Systeme.

**HACKATTACK® IT SECURITY GmbH**

> **kostenlose Infoline**  
0800 20 60 900

training@hackattack.com  
www.hackattack.com



**secure web  
applications**

www.hackattack.com

**HACKATTACK®**  
we hack to protect you

## [secure web applications]

- > **OWASP Top 10** basierend  
die OWASP Top 10 stellen die offizielle Hitliste der kritischsten Web Sicherheitsrisiken dar
- > Welchen Gefahren ist mein System ausgesetzt?
- > Wie erkennen Sie Sicherheitslücken der eigenen Applikation?
- > Wie können Schwachstellen beseitigt werden?

## [Praxis Seminar]

### Anhand eines konkreten Web Community Projekts

lernen Sie die zehn gefährlichsten Schwachstellen kennen die von Angreifern ausgenutzt werden.

... notwendige Theorie ...  
... noch mehr Praxis ...

## [Vorkenntnisse]

Dieses Seminar richtet sich an Webentwickler Inter-, Intra- und Extranet. Grundkenntnisse PHP, Java und MySQL werden vorausgesetzt. Kenntnisse über das Zend Framework sind hilfreich, aber nicht erforderlich.

## [Inhalte]

### [tag 1]

- > **Sichere Programmierung** Die 10 Prinzipien
- > **Bedrohungen** Bestimmen und Bewerten
- > **Was sind die OWASP Top 10?**
- > **Hackertools für Entwickler**  
WebScarab, Firefox, ...
- > **Daten ausspähen und einschleusen**  
LDAP Injection, SQL Injection, Command Injection
- > **User ausspähen und manipulieren**  
Cross Site Scripting (HTML, CSS, DOM, Javascript)

### [tag 2]

- > **Sicherheitsanforderungen** und Tests entwickeln
- > **Automatisierte Tests für Entwickler**  
mittels Selenium
- > **Den eigenen Sicherheitsstandard**  
bewerten und verbessern
- > **Fallbeispiel** mittels des erworbenen Wissens  
hacken Sie selbstständig ein System und lernen so die Schwachstellen zu beheben
- > **Abschluss mit Zertifikat**

### [tag 3]

- > **Authentifizierungs- und Session Management**
- > **laufende Angriffe erkennen u. abwehren**  
User-Tracking, Logfiles uvm.
- > **Server übernehmen** Command execution,  
Privilege escalation, offene Ports,  
ungenutzte Dienste, Frameworks
- > **Weit verbreitet kaum bekannt**  
Cross Site Request Forgery
- > **Ungeschützt trotz Verschlüsselung**  
SSL, md5, DES, SHA, Rainbow Tables
- > **Öffentlich zugängliche Schwachstellen**  
Google Hacks, Frameworks, Social Networks