

Sicherheit von Web-Anwendungen aus Angreiferperspektive

Vermittlung von Angriffstechniken und Gegenmaßnahmen, um Web-Anwendungen nachhaltig schützen zu können

Schulungsveranstaltung | Ulm | März – November 2012



*“If you think technology can solve your security problems, then you don't understand the problems
and you don't understand the technology” - Bruce Schneier*

SCHUTZWERK

Die SCHUTZWERK GmbH ist ein unabhängiges und international tätiges Beratungsunternehmen.

Unsere Kernkompetenz liegt in der Prüfung sowie in der prozess- und konzeptbezogenen Optimierung der Bereiche IT-Sicherheit, Datenschutz und Unternehmenssicherheit.

Die ganzheitliche Stärkung technischer, organisatorischer und menschlicher Sicherheitsaspekte steht im Vordergrund unserer Dienstleistungen.

Thema der Schulung

- ▶ Sicherheit von Web-Anwendungen aus Angreiferperspektive.

Inhalt

- ▶ Erläuterung kritischer Sicherheitsmängel in Web-Anwendungen.
- ▶ Erläuterung der Vorgehensweise von Angreifern und deren Angriffstechniken innerhalb praktischer Übungen.
- ▶ Erläuterung direkter Gegenmaßnahmen sowie prozessgesteuerter Maßnahmen, innerhalb der Planungs- und Entwicklungsphase von Web-Anwendungen.

Ziel

- ▶ Vermittlung der Angreiferperspektive sowie Stärkung des Risikobewusstseins, um Web-Anwendungen nachhaltig schützen zu können.

Zielgruppe

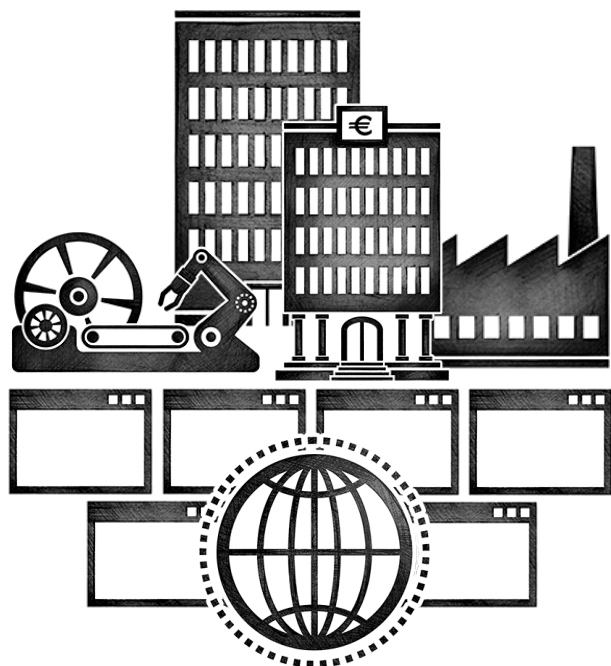
- ▶ Web-Entwickler
- ▶ Administratoren von Web-Umgebungen
- ▶ IT-Sicherheitsverantwortliche



Basierend auf den
OWASP-Vorgaben

In der modernen Geschäftswelt spielen Web-Anwendungen eine tragende Rolle. Daraus resultieren verschiedene unternehmenskritische Faktoren.

- ▶ Heutige Geschäftsprozesse sind ohne Web-Anwendungen kaum mehr denkbar. In vielen Fällen bilden diese sogar den eigentlichen Kern des Geschäftskonzepts. Aus dem hohen Stellenwert der Web-Anwendungen resultieren verschiedene unternehmenskritische Faktoren, wie z.B.:



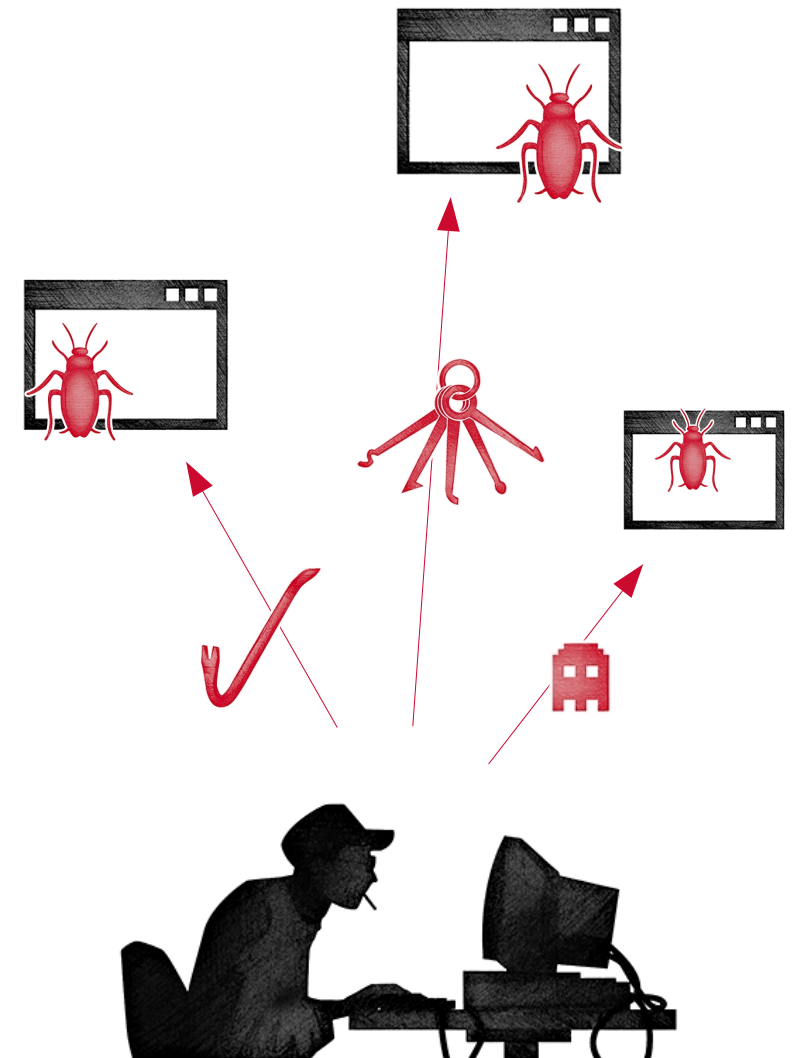
- > Der Geschäftserfolg ist direkt oder indirekt von der Funktionstüchtigkeit der Web-Anwendung abhängig.
- > Die mit der Web-Anwendung verarbeiteten Daten sind oftmals sensibel und von großem Wert.
- > Durch die Vernetzung mit anderen Systemen bilden die Web-Anwendungen ein potentiell Einfallstor zum internen Netzwerk.

Diese Faktoren machen Web-Anwendungen für Angreifer besonders interessant. Die Praxis zeigt jedoch, dass das Sicherheitsniveau häufig nicht den daraus resultierenden Anforderungen entspricht.

- ▶ An die Sicherheit von Web-Anwendungen werden hohe Anforderungen gestellt, da diese aufgrund der genannten Faktoren für potentielle Angreifer von besonderem Interesse sind. Die exponierte Stellung der Systeme sowie deren teilweise hohe Komplexität und Dynamik verschärft die Situation zusätzlich.
- ▶ Zahlreiche Sicherheitsvorfälle der jüngsten Zeit zeigen deutlich, dass viele Web-Umgebungen gezielten Angriffen nicht stand halten.

Nur wer seine Gegenspieler und deren Möglichkeiten kennt, kann sich angemessen schützen.

- ▶ Web-Entwickler, Administratoren und Sicherheitsverantwortliche müssen sich diesen Herausforderungen stellen. Dazu ist es von großem Vorteil, die Angriffsmethoden und Werkzeuge der Angreifer zu kennen. Dieses Wissen bildet die Basis für eine nachhaltige Optimierung der Sicherheitskonzepte.



Vorrangiges Ziel der Schulung ist es, den Teilnehmern die Perspektive der Angreifer zu vermitteln.

- ▶ Grundlage der Schulung bildet die detaillierte Erläuterung kritischer Sicherheitsmängel (in Architektur, Software und Konfiguration).
- ▶ In zahlreichen praktischen Übungen erhalten die Teilnehmer die Möglichkeit, Sicherheitsmängel aufzuspüren und mittels entsprechender Werkzeuge selbst Angriffe auf Web-Anwendungen durchzuführen.

Ausgehend von den Sicherheitsmängeln und Angriffsvektoren werden Gegenmaßnahmen aufgezeigt.

- ▶ Auf Basis des erlangten Verständnisses bezüglich der Sicherheitsmängel und Angriffsvektoren werden den Teilnehmern die verschiedenen Gegenmaßnahmen erläutert.
- ▶ Darüber hinaus wird der Weg aufgezeigt, alle relevanten Sicherheitsaspekte prozessgesteuert bereits in die Planungs- und Entwicklungsphase zu integrieren.



Die Inhalte der Schulung im Überblick:

- ▶ Einführung
- ▶ Technische Grundlagen
- ▶ Sicherheitsmängel und jeweilige Angriffsmethoden
(Vorgehensweisen, Techniken und Gegenmaßnahmen)
 - > Enumeration
 - > Manipulation von clientseitigen Daten
 - > Authentisierung und Autorisierung
 - > Session Management
 - > Path Traversal
 - > Code Injection
 - > Client Side Attacks
- ▶ Sicherheitsaspekte in der Planungs- und Entwicklungsphase

Die Inhalte der Schulung basieren auf den Vorgaben der verschiedenen Teilprojekte des Open Web Application Security Projects – OWASP.

- ▶ OWASP Development Guide
- ▶ OWASP Testing Guide
- ▶ OWASP Top Ten
- ▶ Etc



Weitere Informationen unter <http://www.owasp.org>

Die Schulungsveranstaltung richtet sich an folgende Zielgruppen:

- ▶ Web-Entwickler
- ▶ Administratoren von Web-Umgebungen
- ▶ IT-Sicherheitsverantwortliche

Teilnahmevoraussetzungen

- ▶ Grundkenntnisse in HTML, Web-Server-Administration und Web-Entwicklung



Termine 2012

- ▶ 12 - 13. März
- ▶ 07 - 08. Mai
- ▶ 02 - 03. Juli
- ▶ 24 - 25. September
- ▶ 26 - 27. November

Ort

- ▶ Ulm / Pfarrer-Weiß-Weg 12
- ▶ SCHUTZWERK Schulungszentrum

Dauer

- ▶ Tag 1 - von 09.00 bis 17.00 Uhr
- ▶ Tag 2 - von 08.30 bis 17.00 Uhr

Teilnahmegebühr

- ▶ 1.350,- EUR zzgl. MwSt.
- ▶ 15% Frühbucherrabatt (bei Anmeldung bis 4 Wochen vor Beginn der jeweiligen Veranstaltung)

Rahmenbedingungen

- ▶ Die Teilnahmegebühr umfasst Mittagessen und Getränke.
- ▶ Alle notwendigen IT-Systeme (Notebooks, Testumgebung etc.) werden gestellt.
- ▶ Die Teilnehmer erhalten detaillierte Schulungsmaterialien.
- ▶ Detailinformationen zum Veranstaltungsort und zu Übernachtungsmöglichkeiten finden Sie in der Anlage des Anmeldeformulars.

Jochen Hämmerle

Ihr Referent



jhaemmerle@schutzwerk.com
+49 731 977 191 0

Jochen Hämmerle ist seit 1997 beruflich in der Informatik und im Bereich IT-Sicherheit tätig. Seither realisierte er zahlreiche IT-Projekte mit den Schwerpunkten Software-Entwicklung, verteilte Systeme, Kommunikationssicherheit und sichere Zugriffsverfahren.

In unserem Hause ist Herr Hämmerle verantwortlich für den Bereich der Web Application Security Audits. Durch seine langjährige Erfahrung in der Software-Entwicklung und Administration kennt er die Problemstellungen, durch welche die Applikations- und Systemverantwortlichen täglich herausgefordert werden. Dies erlaubt ihm, das Thema Web-Hacking von Seiten der Angreifer wie auch der Verteidiger zu beleuchten und die Brücke zwischen den beiden Welten zu schlagen.

SCHUTZWERK

SCHUTZWERK GmbH

Parkstraße 2

89231 Neu-Ulm

Phone +49 731 977 191 0

Fax +49 731 977 191 99

www.schutzwerk.com

info@schutzwerk.com

Für Fragen stehen wir Ihnen gerne zur Verfügung

