

# Webapplikationssicherheit (inkl. Livehack) TUGA 15

Advisor for your Information Security



**SEC Consult**

<b>Version:</b>	<b>1.0</b>
<b>Autor:</b>	<b>Thomas Kerbl</b>
<b>Verantwortlich:</b>	<b>Thomas Kerbl</b>
<b>Datum:</b>	<b>05. Dezember 2008</b>
<b>Vertraulichkeitsstufe:</b>	<b>Öffentlich</b>

# Der Vortragende

- Name: Thomas Kerbl
- Senior Security Consultant bei SEC Consult
- Spezialisiert auf Webapplikations-Sicherheit
- Akkreditierter Auditor für ONR 17700
  
- Projekterfahrung im Security Umfeld:
  - Blackbox- / Whitebox-Audits (intern & extern)
  - Sourcecode Reviews
  - Entwicklung von Security Policies
  - Projekte für sichere Softwareentwicklung
  
- Branchenspezialisierung:
  - Öffentlicher Sektor
  - Finanzdienstleister und Versicherungen
  - Logistik- und Infrastrukturdienstleister
  - Telekommunikationsprovider



# SEC Consult – Advisor for your information security

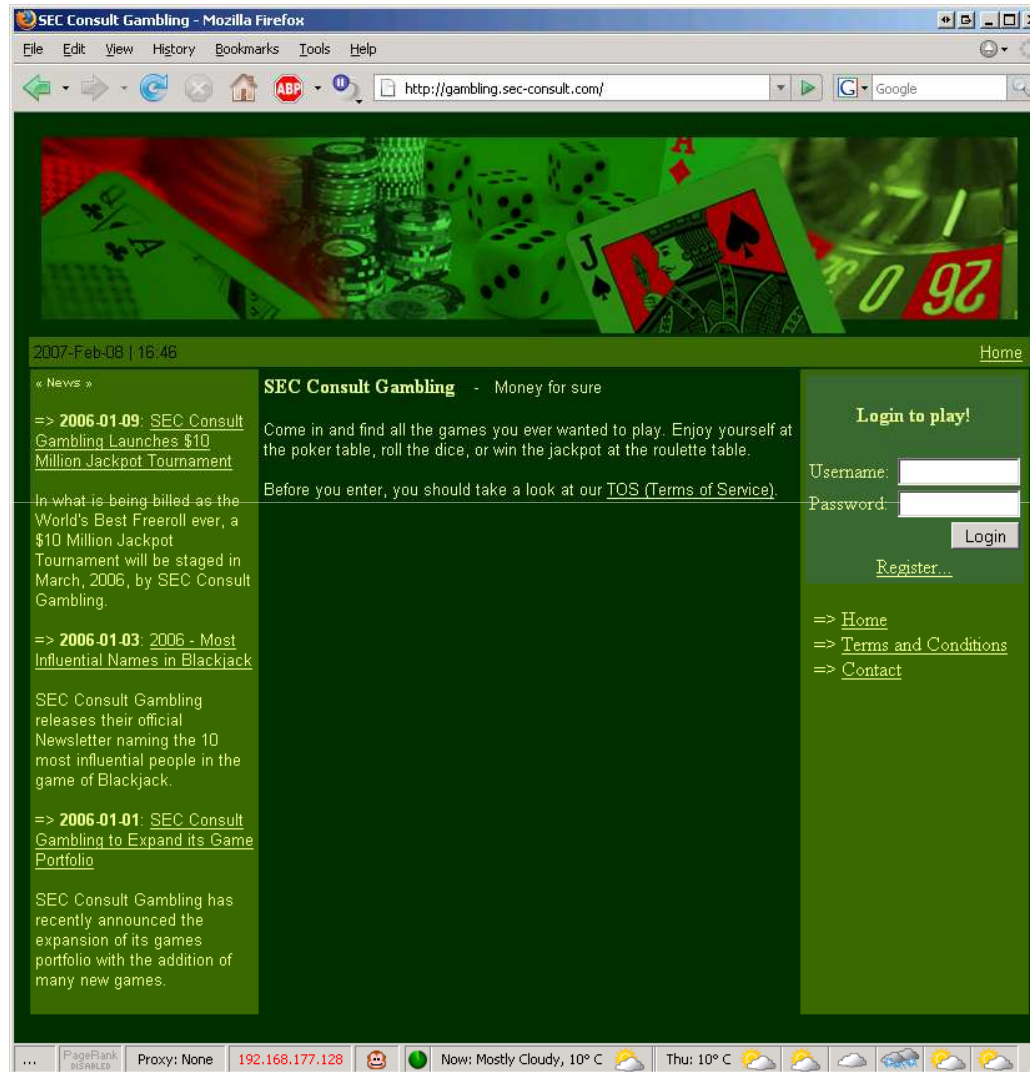


- **Berater für Information Security**
- **Experte** für die **Einführung** von **Sicherheitsprozessen** und **Policies** (ISO 27001, BS 25999, GSHB)
- **Führend** bei **technischen Sicherheits-Audits** und bei der **Umsetzung**
- **Spezialist** für Webapplikationssicherheit auf Basis A7700
- **Unabhängigkeit** von Produktherstellern
- **Behörden, Banken, Versicherungen, börsennotierte Unternehmen** in **Zentraleuropa** als Kunden
- **Branchenspezifische Ausrichtung** (Defense, Public, Finance, Industry)

# Übersicht

- Livehack
- Verbreitete Sicherheitsprobleme bei Webapplikationen
- Normen und Standards für die Sicherheit von Webapplikationen

# Livehack



# Übersicht

- Livehack
- Verbreitete Sicherheitsprobleme bei Webapplikationen
- Normen und Standards für die Sicherheit von Webapplikationen

# Auszug der Fehlerklassen im Bereich Webapplikationen (1)

Schwachstellen	Angriffsvektoren
Konfigurationsfehler	<ul style="list-style-type: none"><li>• Enumeration von Server-Inhalten</li><li>• Ausnutzung von Default-Accounts</li><li>• Enumeration von Benutzer-Accounts</li><li>• Ausnutzung gefährlicher Protokollfeatures</li><li>• Ausnutzung nicht ausreichend gesetzter Berechtigungen</li><li>• Ausnutzung von ungeschützter Funktionalität</li><li>• Enumeration von Server-internen Informationen</li><li>• Erraten von Passwörtern</li><li>• Mitlesen unverschlüsselter, sensibler Daten</li></ul>
Fehler in Authentisierung oder Autorisierung	<ul style="list-style-type: none"><li>• Umgehen der Authentisierung</li><li>• Zugriff auf geschützte Funktionalität</li><li>• Zugriff auf geschützte Ressourcen</li></ul>
State- / Session-Management-Fehler	<ul style="list-style-type: none"><li>• a. Ermittlung von Session-Identifikatoren</li><li>• b. Ausnutzung von Problemen im State-Management</li></ul>

## Auszug der Fehlerklassen im Bereich Webapplikationen (2)

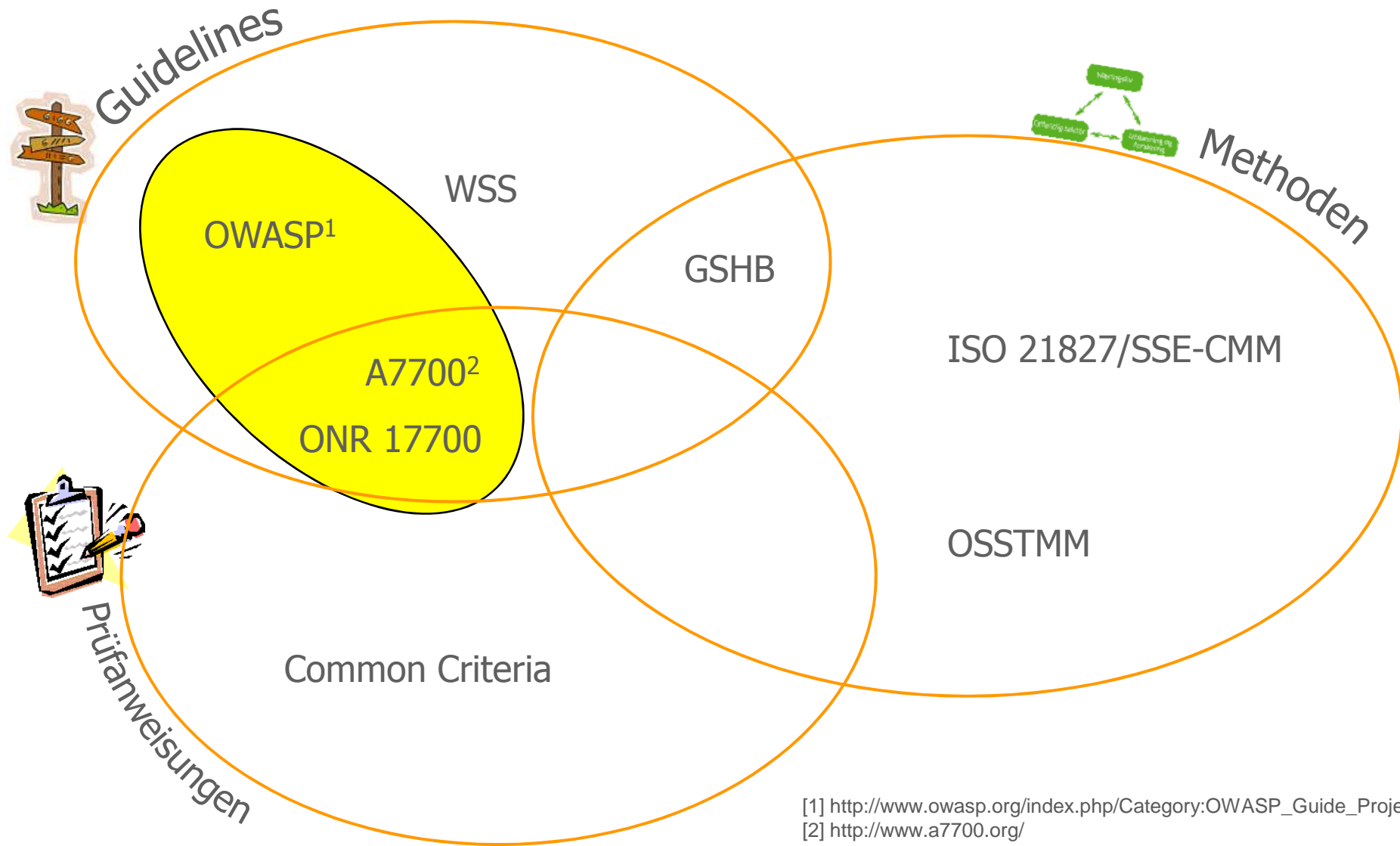
Schwachstellen	Angriffsvektoren
Interpreter Injection Schwachstellen	<ul style="list-style-type: none"><li>• Zugriff auf das Dateisystem</li><li>• Code Injection</li><li>• Command Injection</li><li>• Format String Injection</li><li>• IMAP/SMTP Injection</li><li>• LDAP Injection</li><li>• Overflowing Character Buffers</li><li>• Path Traversal</li><li>• SQL Injection</li></ul>
Verwundbarkeit gegenüber client-seitigen Attacken (Web Browser)	<ul style="list-style-type: none"><li>• Cross Site Request Forgery (XSRF)</li><li>• HTML Injection / Cross Site Scripting (XSS)</li><li>• HTTP Response Splitting / header injection</li></ul>

Derzeit sind im Bereich der Webapplikationen **über 40 Angriffsvektoren** bekannt

# Übersicht

- Livehack
- Verbreitete Sicherheitsprobleme bei Webapplikationen
- Normen und Standards für die Sicherheit von Webapplikationen

# Relevante Guidelines und Standards



[1] [http://www.owasp.org/index.php/Category:OWASP\\_Guide\\_Project](http://www.owasp.org/index.php/Category:OWASP_Guide_Project)

[2] <http://www.a7700.org/>

# Die Historie der ONR 17700



- Die **ONR 17700** legte als **erste Norm im EU-Raum** für die Sicherheit von Webanwendungen das Fundament für die ÖNORM A7700
- **ONR 17700** wurde **2004/05** von **Österreichischem Normungsinstitut, SEC Consult, Großbanken, Großversicherungen, Behörden, etc.** entwickelt. Unter anderem:

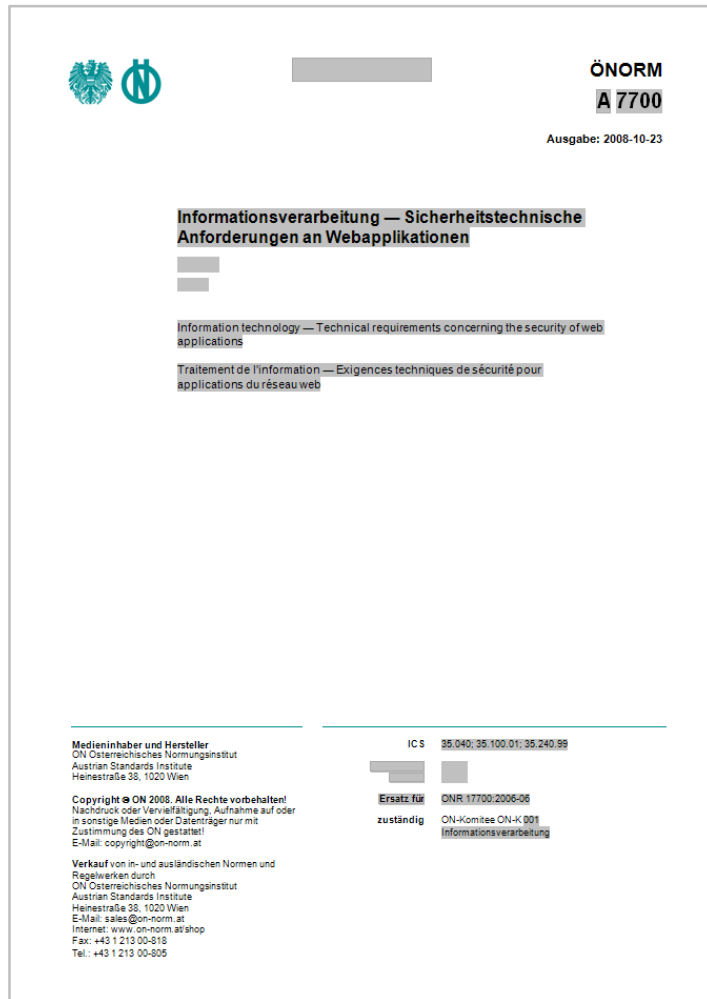


- Unternehmen mit **ONR 17700** zertifizierten Web-Applikationen<sup>1</sup>:



[1] Quelle: <http://www.on-norm.at/publish/2040.html>

# ÖNORM A7700 – Sicherheitstechnische Anforderungen an Webapplikationen



- Die **A7700** stellt eine **überarbeitete und aktualisierte Version der ONR 17700** dar und wurde **2007/2008** entwickelt.

- **Offizieller Standard** zur Definition des **Stand der Technik** im Bereich der Sicherheit von Web-Applikationen

- Release Datum: **01. Dezember 2008**

## Ziele der A7700:

- **Vollständige Abdeckung** des **Sicherheitsbereichs** in Webapplikationen und Webservices (die von anderen Normen z.B. ISO 27001 nur gestreift werden)
- Gewährleistung eines **hohen Sicherheitsniveaus durch mehrstufiges** vollständiges Source-Code Audit

## A7700 – Der Standard zum globalen OWASP Guide

- Definition der Anforderungen betreffend (1/2):
- Kapitel 3 – Architektur der Webapplikation
- Kapitel 4 – Datenspeicherung und Datentransport
- Kapitel 5 – Konfigurationsdaten
- Kapitel 6 – Authentifizierung, Autorisierung und Sitzungen
- Kapitel 6.1 – Allgemeines
- Kapitel 6.2 – Authentifizierung
- Kapitel 6.2.1 – Authentifizierungsmethoden
- Kapitel 6.2.2 – Passwörter
- Kapitel 6.3 – Autorisierung
- Kapitel 6.4 – Sitzungen
- Kapitel 6.4.1 – Separierung durch Sitzungen
- Kapitel 6.4.2 – Qualitätskriterien für Sitzungen

14 Controls gemäß  
ISO 27001:2005, z.B.:

- Electronic commerce
- On-Line Transactions
- Publicly available information

PCI-DSS Requirements

- Req. 4.1: Use strong cryptography
- Req. 6.5: Develop web applications based on secure coding guidelines
- Req. 6.6: Protect all web-facing applications (source code review)

## A7700 – Der Standard zum globalen OWASP Guide

- Definition der Anforderungen betreffend (2/2):
- Kapitel 7 – Behandlung von Benutzereingaben
- Kapitel 7.1 – Anforderungen
- Kapitel 7.2 – Dateigenerierung
- Kapitel 7.3 – Speichermanagement
- Kapitel 7.4 – Einbinden von Ressourcen
- Kapitel 8 – Behandlung von Datenausgaben
- Kapitel 9 – Hintergrundsysteme
- Kapitel 10 – System- und Fehlermeldungen
- Kapitel 11 – Kryptographie

14 Controls gemäß  
ISO 27001:2005, z.B.:

- Electronic commerce
- On-Line Transactions
- Publicly available information

PCI-DSS Requirements

- Req. 4.1: Use strong cryptography
- Req. 6.5: Develop web applications based on secure coding guidelines
- Req. 6.6: Protect all web-facing applications (source code review)

# Wie erreichen Sie SEC Consult?

## SEC Consult Unternehmensberatung GmbH

Mooslackengasse 17,

A-1190 Wien

Tel: +43 / 1 8903043 0

Fax: +43 / 1 8903043 15

Email: [office@sec-consult.com](mailto:office@sec-consult.com)

<http://www.sec-consult.com>

Bezug und weiterführende Informationen zur A7700:

<http://www.a7700.org/>