

Die 20 beliebtesten Versäumnisse hinsichtlich Sicherheit in der Softwareentwicklung

EUROSEC GmbH Chiffriertechnik & Sicherheit

Tel: 06173 / 60850, www.eurosec.com

© EUROSEC GmbH Chiffriertechnik & Sicherheit, 2005

Die 20 beliebtesten Versäumnisse

- ungenügende (Security-) Anforderungsspezifikation
- ungenügende (Security-) Designspezifikation
- kein Abgleich zwischen Anforderungs- und Designspezifikation
- keine Richtlinien zur sicheren Softwareentwicklung
- Security Reviews wahlweise gar nicht, oder nur vor oder nur nach dem Erstellungsprozess
- Implementierung eigener (i.d.R. zu schwacher) Schutzmechanismen und Kryptofunktionen

Parameterprüfung

- DAS Problem Nr. 1 in Web-Anwendungen
- Resultat mangelhafter Überprüfung der Eingaben:
 - Cross-Site Scripting
 - SQL-Injection
 - Directory Traversal
 - Command Injection
 - Code Injection
 - Cookie Poisoning
 - Buffer Overflows
 - Format String Attacken

Die 20 beliebtesten Versäumnisse

- Unkenntnis der Entwickler bzgl. der häufigsten Hackermethoden (z.B. SQL Injection, Cross-Site Scripting, u.v.m.)
- zu generische Anforderungskataloge, die vom Entwickler erst mühsam interpretiert werden müssten
- ungenügende Prüfung auf Einhaltung existierender Sicherheitsvorgaben, bestenfalls Selbstauskunft durch Entwicklungsverantwortliche
- keine Schwachstellenanalyse des Prototyps durch unabhängige Spezialisten

Die 20 beliebtesten Versäumnisse

- allmächtiger technischer Benutzer für Datenzugriffe
- „Schützen durch bloßes Verstecken“ (z.B. von Funktionsaufrufen, URLs, Parametern, etc.)
- Ungenügender Schreib-/Leseschutz von Programmdateien
- Keine Input-Validierung / Filterung von User Input
- fehlende Planung zum Schutz der Backendsysteme, insbesondere für Datenbanken
- keine adäquate Protokollierung

Die 20 beliebtesten Versäumnisse

- Benutzer- und Rechteverwaltung schlecht konzipiert, zu seltener Gebrauch vorhandener (externer) Funktionalität
- mangelhafte Dokumentation vorhandener Sicherheitsmechanismen und erforderlicher Konfigurationsanpassungen
- Unkenntnis oder mangelnde Berücksichtigung von Kundenanforderungen
- später erforderliche Nachbesserungen scheitern an zu vielen Abwärtskompatibilitätsanforderungen, die häufig durch bessere Planung hätten vermieden werden können

Weitere beliebte Schwächen in Anwendungsservern

- Alte Softwareversionen installiert (auch Betriebssystem etc.)
- Konfigurationsfehler auf allen Ebenen
- Standardinhalte, Beispielanwendungen wurden nicht entfernt
- Dateisystemberechtigungen nicht restriktiv genug
- Administrationsbenutzer = Laufzeitbenutzer

- Betreffen meist alle installierten Web-Anwendungen und oft das Server-Betriebssystem
- Resultat: Zugriff auf Server hinter der Firewall

Warum dieser Vortrag von uns?

- Unsere Erfahrung:

- mehrere Personenjahre in Forschungsprojekten zur sicheren Softwareentwicklung; derzeit gemeinsam mit Partnern wie SAP, Commerzbank, Universitäten, ...
- zahlreiche Schwachstellenanalysen für Softwarehersteller, nebst intensiver Feedbackzyklen mit den Entwicklern
- Erstellung von Anforderungs- und Designspezifikationen in mehreren großen Entwicklungsprojekten
- Erstellung von Guidelines zur sicheren Softwareentwicklung, mit Schwerpunkten Banking & Finance, sowie Webapplikationen
- Reverse Engineering und Gutachten von Sicherheitsfunktionen und Kryptomechanismen
- Implementierung von Sicherheitsfunktionen im Auftrag

Abschlussbemerkung

- die vorliegende Dokumentation wurde von EUROSEC erstellt im Rahmen des secologic Forschungsprojekts, Laufzeit 2005 und 2006, nähere Informationen unter www.secologic.org
- wir bedanken uns beim Bundesministerium für Wirtschaft für die Förderung dieses Projektes
- Anregungen und Feedback sind jederzeit willkommen, ebenso Anfragen zu Sicherheitsaspekten, die hier nicht behandelt werden konnten.

Copyright Hinweis

- Diese Folien wurden von EUROSEC erstellt und dienen der Durchführung von Schulungen oder Seminaren zum Thema Sichere Anwendungsentwicklung, mit Fokus Webapplikationen.
- Wir haben diese Folien veröffentlicht, um die Entwicklung besserer Softwareprodukte zu unterstützen.
- Die Folien dürfen gerne von Ihnen für eigene Zwecke im eigenen Unternehmen verwendet werden, unter Beibehaltung eines Herkunfts-Hinweises auf EUROSEC.
- Eine kommerzielle Verwertung, insbesondere durch Schulungs- oder Beratungsunternehmen, wie beispielsweise Verkauf an Dritte oder ähnliches ist jedoch nicht gestattet.