



CYBERHOUSE
INTERACTIVE COMMUNICATIONS

CYBERdays_

Sicherheit von Content-Management- Systemen

Wien, 16.3.2010





Übersicht_

Übersicht

- › Einleitung
 - › Erklärung der Angriffsmöglichkeiten mit Beispielen
 - › Statistik
 - › Sicherheit von Content-Management-Systemen
 - › Was kann man dagegen tun?
 - › Fazit
-



Einleitung_

Über mich

- › Georg Ringer
 - › seit 2008 bei CYBERhouse als Entwickler (TYPO3, Magento)
 - › seit Ende 2009 Mitglied im TYPO3 Security Team
 - › Verbesserung der Sicherheit des TYPO3 Core
 - › Zusammenarbeit mit Extension-Entwicklern
 - › Bewusstsein für sicheres Programmieren schaffen
-



Einleitung_

Sicherheitslücken

- › senken nachhaltig das Vertrauen
- › sorgen nachhaltig für schlechte Publicity
- › sind direkt geschäftsschädigend

Sicherheitslücken entstehen durch

- › Unwissenheit
 - › Zeitmangel
 - › Unachtsamkeit
-



SQL Injections

› Manipulation einer Datenbankabfrage

› Benötigte Kenntnisse

- Vorwissen über das eingesetzte System
- Vorwissen über die eingesetzte Datenbank

› Auswirkungen

- Auslesen beliebiger Datenbank-Tabellen (Bestellungen, Produkten, Zugangsdaten, ...)
- kompromittiertes System

› Aufwand zur Vermeidung gering



SQL Injections II

Tabelle mit Content

Id	title	text
3	Willkommen	Willkommen auf meiner Seite
5	Gästebuch	Tragen Sie sich in mein Gästebuch ein
14	Neuigkeiten	News von der Firma

Tabelle mit Administratorzugängen

Id	Benutzername	Email	Passwort
1	max.mustermann	max@gmail.com	geheimesspasswort
7	ulrike	ulrike@firma.at	test123



SQL Injections III

Tabelle mit Content, kombiniert mit den Administratorzugängen

Id	title	text
3	Willkommen	Willkommen auf meiner Seite
5	Gästebuch	Tragen Sie sich in mein Gästebuch ein
14	Neuigkeiten	News von der Firma
1	max.mustermann	geheimesspasswort
7	ulrike	test123



Cross-Site Scripting (XSS)

› Manipulation der Ausgabe

› Benötigte Kenntnisse

- HTML
- JavaScript (DOM, Ajax, ...)

› Auswirkungen

- Defacement
- Auslesen von Benutzerdaten & Übernahme von Benutzersessions

› Aufwand zur Vermeidung gering



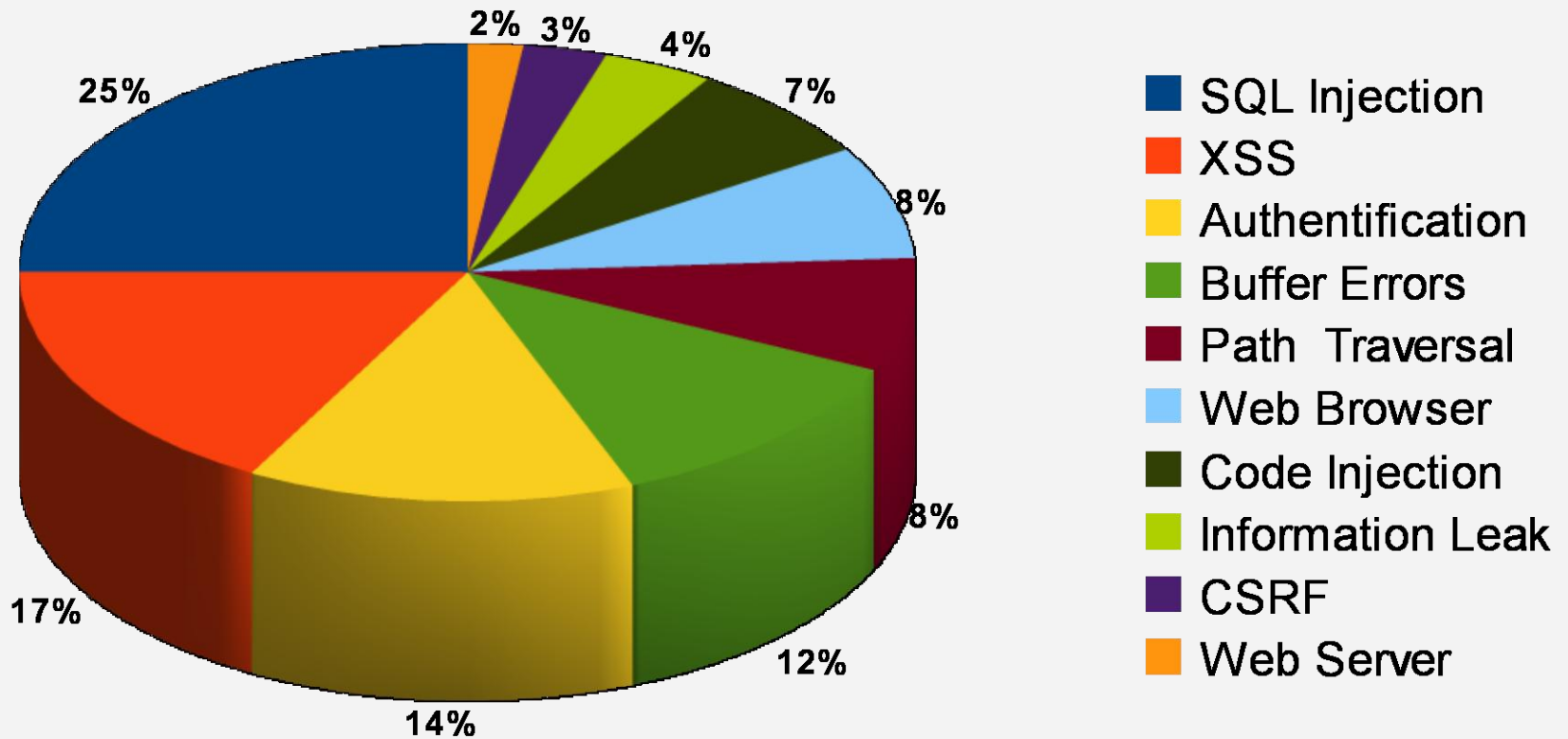
Sonstige Lücken_

Sonstige Lücken

- › Fehlende/Falsche Authentifizierung
 - › Information disclosure
 - › Security Bypass: Captcha lässt sich überspringen
-



Häufigkeit der Lücken





Sicherheitslücken_

Wie werden Lücken entdeckt

- › Persönliche Neugier
- › Suchmaschinen
- › automatisierte Bots

Wieviele Websites mit Lücken
findet man in ~ **8** Stunden?

Quelle: insbesondere www.oewa.at



CMS_

Sicherheit von Content-Management-Systemen

- › Individualprogrammierung vs. Standardsoftware
 - › Proprietär vs. Open-Source
 - › **Unterscheidung zwischen:**
 - › System
 - › Erweiterungen (Plugins)
-



Was tun?_

Sicherheit erhöhen & Probleme vermeiden

- › Sicherheit als Merkmal bei der Wahl des CMS / Auftraggebers
- › Immer die aktuellste Version benutzen (Website des CMS, Wartungsvertrag, ...)
- › Security-Reviews
- › Awareness fördern

Aus Sicht des Anwenders

- › Sichere Passwörter
 - › Nicht jedem Link vertrauen, insbesondere URL-Verkürzungsdiensten
<http://bit.ly/cJLUSh> = http://5z8.info/hack-outlook_d8q9a_warez = ???
-



Ich bedanke mich
für Ihre Aufmerksamkeit!