WALL&KOLLEGEN

RECHTSANWÄLTE AVVOCATI BARRISTER-AT-LAW

MÜNCHEN **INNSBRUCK** **BOZEN**

Die 7 häufigsten Fehler im IT-Security-Management bei Webanwendungen

(nach OWASP)

München, 11.10.2011

DAV IT-RECHT
davit.de

c1

Apple's Worst Security Breach: 114,000 iPad Owners Exposed

Apple has suffered another embarrassment. A security breach has exposed iPad owners including dozens of CEOs, military officials, and top politicians. They—and every other buyer of the cellular-enabled tablet—could be vulnerable to spam marketing and malicious hacking.

Quelle: gawker.com 9.6.2010

c1 Ich habe die Grafik etwas zurechtgeschnitten.
computer; 09.10.2011

Fehler 1: Zugriffsrechte-Management

- **Mögliche Ursachen**

  versehentliches Löschen von Schutzmechanismen

  Unkenntnis der Sicherheitslage ("Security-by-Obscurity„)

  fehlende oder unklare Regeln, Zuständigkeiten und Rechte für die Publikation von Dokumenten oder Daten

- **Management-Fehler**

  Fehlerhaft konfigurierte Content-Management-Systeme (CMS)

  Fehlende Kontrollmechanismen bei Veröffentlichungen

  Keine/nicht ausreichende Sicherheitsrichtlinien

Fehler 2: Unzureichend abgesicherte Datenbanken

Datenbanken sind nicht ausreichend gegen Hackerangriffe gesichert, siehe Auszug aus OWASP Open Web Application Security Project (nächste Folie)

- **Management-Fehler**

  Nicht ausreichende Absicherung

  Weiterverarbeitung von externen Parametern ohne vorherige Validierung, z.B. SQL-Injection

LÖSUNG für Fehler 2

- **Risiko-Management-Prozess**

  Erfassung

  Analyse der Schwachstellen
  Risikobewertung (Eintrittswahrscheinlichkeit-Schaden)

  entsprechend der Risikobewertung:

  Steuerung

  Kontrolle

  Vgl. auch ISO 27005, BSI 100-3

Fehler 3: Unverschlüsselte oder unzureichend verschlüsselte Datenbankendaten

Insecure Cryptographic Storage

Daten, die nicht oder unzureichend verschlüsselt wurden, obwohl sie ohne/nur geringen für die Funktionalität der Anwendungen verschlüsselt werden könnten

Usability versus Sicherheit

Fehler 4: Unautorisierter direkter Zugriff auf Daten mittels Parameter-Manipulation

Insecure Direct Object Reference

Änderung von „Request-Parametern“, dadurch Zugriff auf personenbezogene Daten Dritter (Identitäts-Diebstahl)

Fehler 5: Fehlerhafte Authentifizierungs-Mechanismen

"Authentication and Session Management"

LÖSUNG für Fehler 5

IT Security -Management:

Ausreichende Authentifizierungsmaßnahmen

IT Security

Fehler 6: Email – Missmanagement

Fehler bei der Zustellung von eMails

- über Website-Formulare

- automatisierte Backend-Webapplikationen

-Newsletter-Systeme

LÖSUNG für Fehler 6

IT Security -Management:

Ausreichendes Emailzustellungssystem

Fehler 7: Unzureichender Schutz gegen Data-Mining

- Data-Mining: Erkennung von Mustern in komplexen Datenstrukturen

- Identifikation und Persönlichkeitsprofile einzelner Personen möglich (auch bei anonymen/pseudonymen Anwendungen)

LÖSUNG für Fehler 7

IT Security -Management:

Hackerschutzmaßnahmen

IT Security

IT Security Management bei kritischen Webanwendungen

➢**Wie finden Sie heraus, wie sicher Ihre Seite ist ??**

- Whitebox Testing

der Quellcode wird durch speziell geschulte IT Spezialisten analysiert.

- Blackbox Testing

der „legale" Hacker kennt keine Insider Informationen über sein Ziel.

Blackbox Testing machen professionelle Penetration Tester (sehr teuer).

Günstiger und umfassendere Tests durch viele „legale" Hacker über Hatforce.com.

IT Security

Heise Security
News-Meldung vom 06.10.2011 12:25

Apache-Lücke erlaubt Angreifern Zugriff auf interne Server
Die Sicherheitsexperten von Context haben eine **Lücke im Apache-Webserver** entdeckt, durch die Angreifer aus der Ferne auf interne Server zugreifen können. Die Rewrite-Engine mod_rewrite sorgt dafür, dass Anfragen anhand definierbarer Regeln auf verschiedene Server verteilt werden; … Diese Konfiguration bezeichnet man auch als Reverse Proxy. Unter bestimmten Umständen führt ein @-Zeichen in der Anfrage dazu, dass die Rewrite-Regeln zu einer falschen Umschreibung der URL führen und der Angreifer einen beliebigen Host angeben kann.

Beispiel:
So bildet mod_rewrite aus der HTTP-Anfrage
GET @InternalNotAccessibleServer/console HTTP/1.0
die URL http://internalserver:80@InternalNotAccessibleServer/console

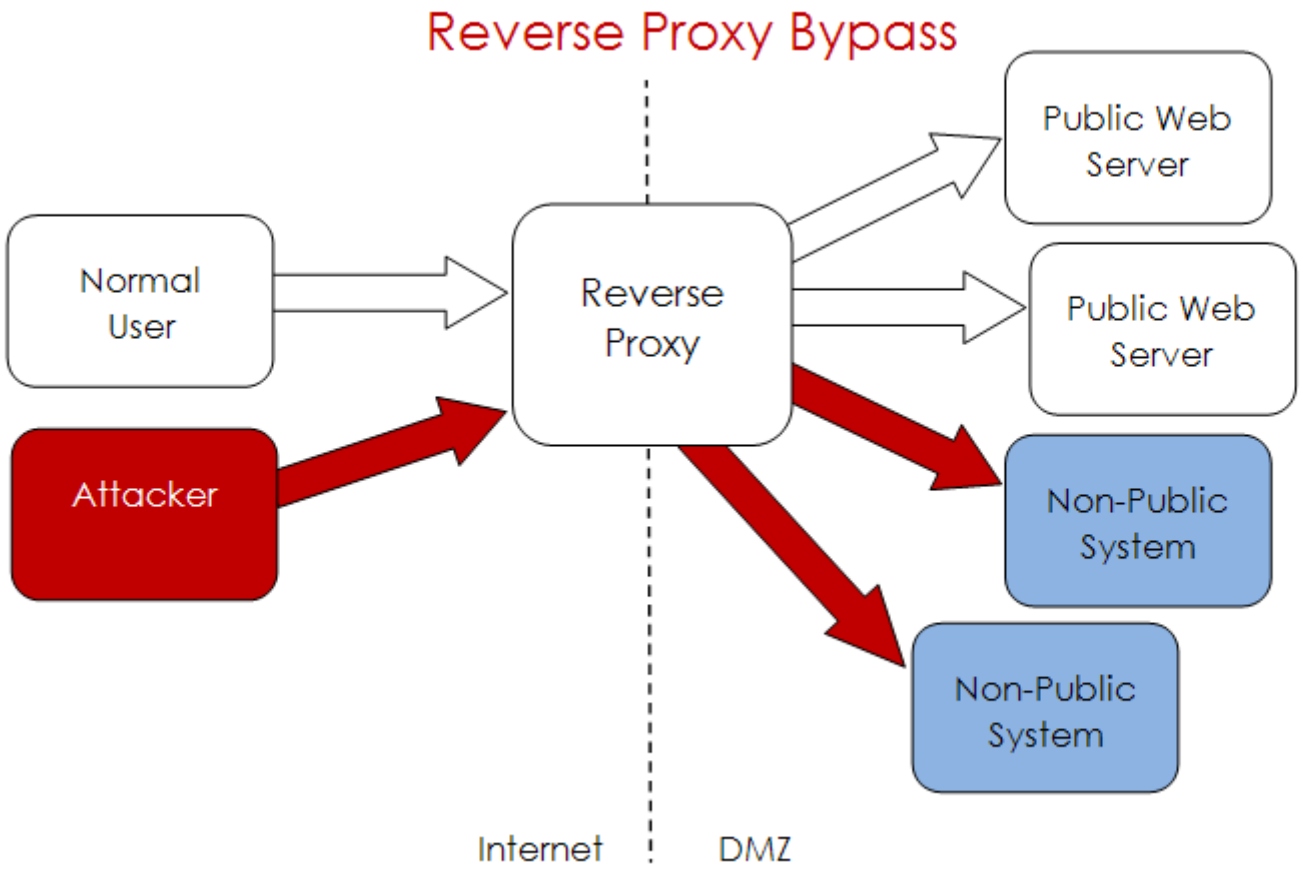
Durch das @ wird der Part mit dem eigentlichen Host als HTTP-Authentification interpretiert und die Anfrage auf einen vom Angreifer wählbaren Server (NotAccessibleServer) umgeleitet, der sich im lokalen Netz des Apache-Servers befinden kann.

Einzige Voraussetzung ist, dass der Angreifer den lokalen Hostnamen oder die lokale IP des Servers kennt, auf den er zugreifen will. An diese Information kann er jedoch etwa mittels Brute Force gelangen.

Betroffen sind Apache 1.3 und der 2er-Versionszweig bis 2.2.20. Die Apache Foundation hat bereits einen **Patch** auf Version 2.2.21 veröffentlicht, der dieses Problem beseitigt.

URL dieses Artikels:
http://www.heise.de/security/meldung/Apache-Luecke-erlaubt-Angreifern-Zugriff-auf-interne-Server-1355778.html

IT Security



Resultat der Lücke: Zugriff auf Server, die eigentlich nicht angesprochen werden sollten.

IT Security

Natalie Wall

Fachanwältin für
Informationstechnologierecht

www.wall-legal.de

Rechtsanwältin

Natalie Wall

Karlsplatz 7
80335 München

FON 089 30 90 589-0
FAX 089 30 90 589-11

MOB 0173-3582228

wall@wall-legal.de
www.wall-legal.de