



Design Bugs

**Alexios Fakos
Senior Security Consultant
n.runs AG
alexios.fakos@nruns.com**

OWASP

13.10.2009

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation
<http://www.owasp.org>

Agenda

- Einführung
- Wortdefinition
- Probleme und Beispiele
- Fazit

Agenda

Einführung

Einordnung in OWASP TOP 10 (2007)

- ▶ A1 - Cross Site Scripting (XSS)
- ▶ A2 - Injection Flaws
- ▶ A3 - Malicious File Execution
- ▶ A4 - Insecure Direct Object Reference
- ▶ A5 - Cross Site Request Forgery (CSRF)
- ▶ A6 - Information Leakage and
Improper Error Handling
- ▶ A7 - Broken Authentication and Session Management
- ▶ A8 - Insecure Cryptographic Storage
- ▶ A9 - Insecure Communications
- ▶ A10 - Failure to Restrict URL Access

Motivation für diesen Vortrag (1/2)

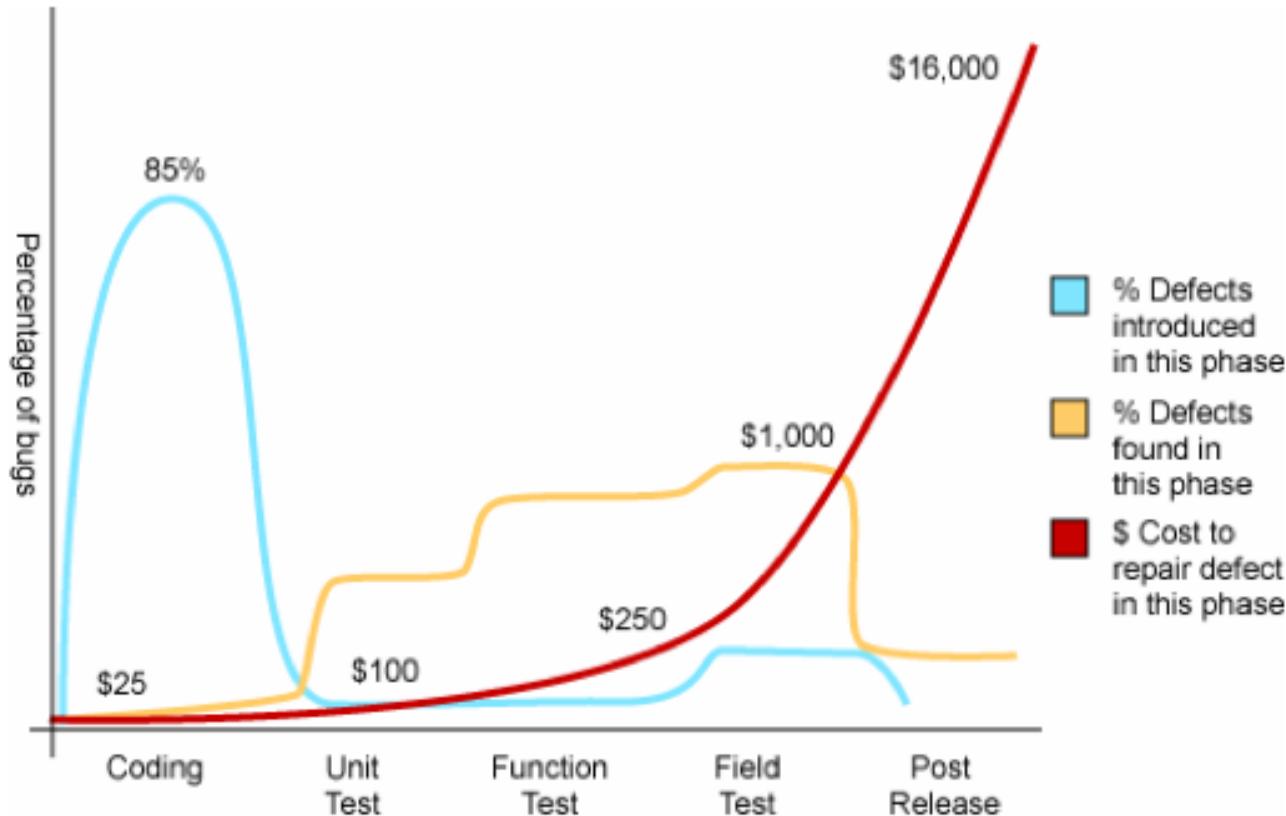
- ▶ Identifizierung von regelmäßigen Problemen bei Security Assessments
 - Oft Probleme, die Sie auch erkennen können !
 - ➔ selten technisches Know-How notwendig

Motivation für diesen Vortrag (2/2)

■ Probleme partiell zu beheben

→ i.d.R. zeit- und kostenintensiv !

Vgl. <http://www.nist.gov/director/prog-ofc/report02-3.pdf>



Source: Applied Software Measurement, Capers Jones, 1996

Zielgruppe für den Vortrag

- ▶ Personenkreis, der Anforderungsdefinitionen schreibt

- Marketing
- Designer
- Software Architekten
- Anwendungsentwickler
- ...



- ▶ Personenkreis, das Problem evaluiert/entdeckt

- Support
- QA
- Security Consultants
- ...

Einführung

Ihnen sollte das als Kunde
nicht widerfahren

Einführung

Behebung einer

SQL Injection



als

Feature Enhancement

Feature Enhancement (1/3)

ENHANCEMENT REQUEST DESCRIPTION

ORACLE

=====

Apple used a commercial software IBM Rational AppScan 7.8.0.1 to test security vulnerability in [REDACTED] It presented these four areas as loopholes. Although none are considered as critical that require a hotfix, they may be considered as enhancement request if support/development considered it as a loophole. See attachment for report

Feature Enhancement (2/3)

[3 of 4] Authentication Bypass Using SQL Injection



Severity: High

Test Type: Application

Vulnerable URL:

a68a5d05a66b484c9cb0f6d3222ca59e48.e3aMc38KaxiNe38Kc3iTaNanOaNz

O (Parameter = currentPagination')

Remediation Tasks: Filter out hazardous characters from user input

Oracle consulting response for support/development: Need further analysis by support to verify if this is an enhancement request.

Feature Enhancement (3/3)

ORACLE

*** 07/23/09 12:40 pm DISCUSSION ***

*** 07/23/09 12:43 pm *** (CHG: Desirability-> 4 -> 2)

*** 07/23/09 09:08 pm *** (CHG: Asg->NEW OWNER)



Agenda

Wortdefinition

Design + Bug

Wortdefinition

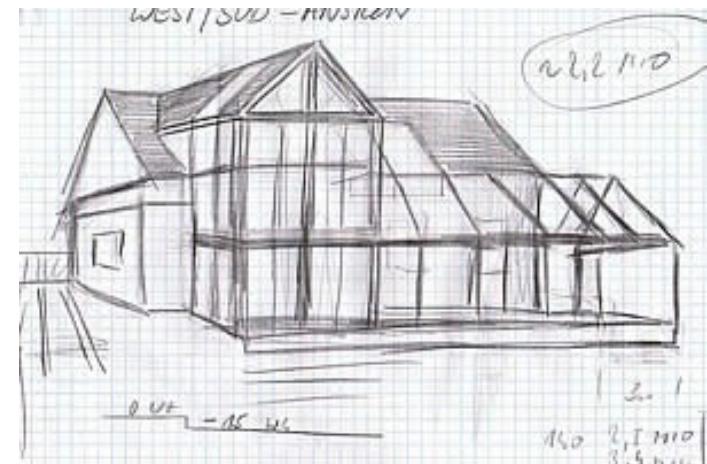
■ Design

► Übersetzt: Gestaltung

► „.... bedeutet meist Entwurf oder Formgebung“

► Erfüllt

- technisch-praktische / informative Funktionen
- ästhetische Funktionen



Wortdefinition

■ Design Entscheidungen

- ▶ Getrieben von Anforderungen

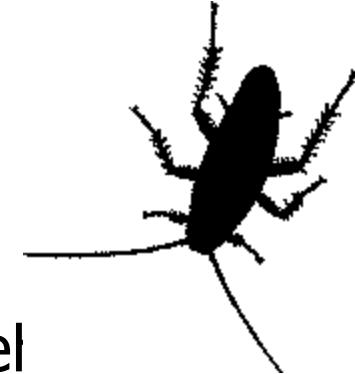
- Funktionale
 - Fachliche
- Nicht funktionale
 - Aussehen und Handhabung (Look and Feel)
 - Sicherheitsanforderungen (CIA Triade)
 - Korrektheit (Ergebnisse fehlerfrei)
 - Flexibilität (Unterstützung von Standards)
 - ...



Wortdefinition

■ Bug

► Übersetzt: Programmfehler oder Softwarefehler



► Auftreten des Fehlverhaltens

▪ Wenn ein bestimmter Zustand nicht berücksichtigt wird

- » Unvollständigkeit
- » Ungenauigkeiten
- » Mehrdeutigkeiten etc.
- ➔ in der Anforderungsdefinition



Wenn es mal schief läuft...

Wer ist Schuld ?



Agenda

Probleme

und (Parade) Beispiele



Probleme und Beispiele



Fehlermeldungen

A6 - Information Leakage and Improper Error Handling

Fehlermeldungen

Aus Sicht eines Designer(s) *

* in diesem Fall Designerin

Registrierung und Login –
Formulare und Prozesse
nutzerfreundlich und effektiv gestalten



Fehlermeldungen

Aus Sicht eines Designer(s) *

* in diesem Fall Designerin

Aus Fehlermeldungen positive Hinweise machen

Fehlermeldungen sollten deutlich mehr aussagen als der typische Satz „Es ist ein Fehler aufgetreten.“ Sind die betroffenen Felder markiert und eine freundlich formulierte Erläuterung direkt daneben platziert, kommt der Nutzer viel schneller zum Ziel.

Mit AJAX und JavaScript können die meisten Daten bereits während der Eingabe validiert werden. So zum Beispiel, ob der gewünschte Benutzername noch verfügbar ist, oder ob das E-Mail-Feld korrekt ausgefüllt ist. Damit erspart man dem Nutzer die Fehlermeldungen, wenn er glaubt, mit dem Klick auf „Absenden“ seine Registrierung abgeschlossen zu haben.

Fehlermeldungen – Registrierung



Fehlermeldungen – Registrierung



Fehlermeldungen – Registrierung



Fehlermeldungen – Registrierung

■ Folgen

- ▶ Enumerierung von gültigen
 - Benutzernamen
 - E-Mail Adressen
 - Benutzername + dazugehörige E-Mail Adresse

- ▶ Finden Sie auch bei
 - „Login“ Funktion
 - „Passwort vergessen“ Funktion

Fehlermeldungen – Registrierung

- heise News-Meldung vom 06.04.2009 17:21

Kunden-E-Mail-Adressen bei deutschen Providern leicht erratbar

"Das Datenleck sollte umgehend geschlossen werden", zeigte sich auch ein Sprecher des Landesdatenschutzbeauftragten von Rheinland-Pfalz besorgt gegenüber heise online. Die für den Telekommunikationsbereich zuständigen Stellen seien informiert worden.

<http://www.heise.de/security/meldung/Kunden-E-Mail-Adressen-bei-deutschen-Providern-leicht-erratbar-211766.html>

Probleme und Beispiele

Klartext
reden



A9 - Insecure Communications

Sicherer Transit

■ Wer kennt das nicht?

► Anmeldung via Klartext Protokolle

- HTTP
- SMTP / POP3
- FTP
- Telnet

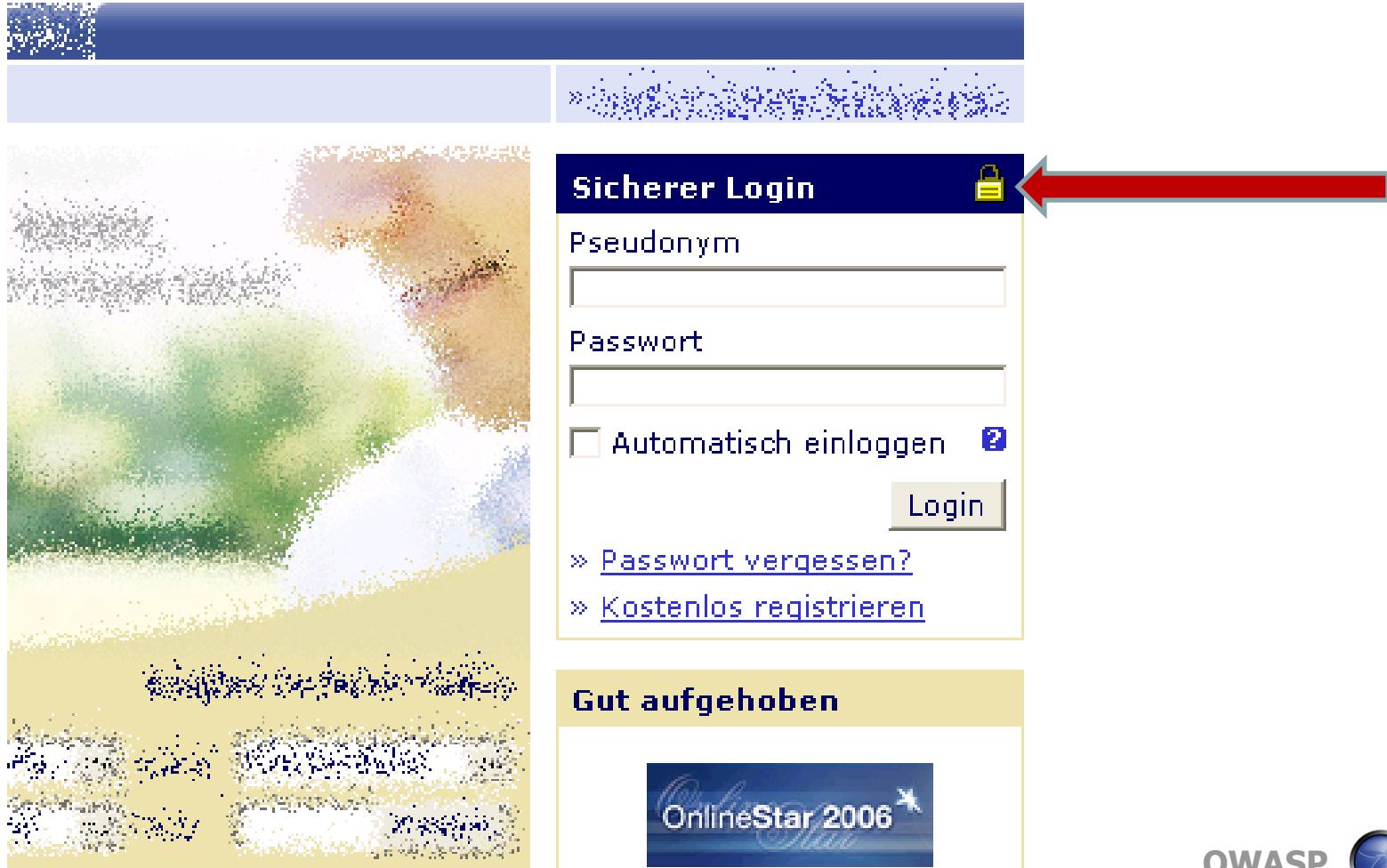
Sicherer Transit

■ Der sichere Login – Umfrage



Sicherer Transit

■ Der sichere Login



Sicherer Transit

■ Der sichere Login

Studie (2007)

- ▶ An evaluation of website authentication and the effect of role playing on usability studies <http://www.usablesecurity.org/emperor/>

Sicherer Transit

■ Der sichere Login

97 % der Probanden sagten:

Login ist sicher



Sicherer Transit

■ Der sichere Login

3 % der Probanden:

Verweigerten die Eingabe



Sicherer Transit

■ Der sichere Login – Auflösung

The screenshot shows a web browser window with the following details:

- Address Bar:** Address http://www.**REDACTED**.de/
- Page Title:** Sicherer Login
- Form Elements:** Two FORM elements are visible:
 - FORM name=SearchBoxRight action=/searchboxright.html
 - FORM name=login action=/login.html
- SSL Indicator:** A green bar at the bottom of the page indicates an SSL-encrypted connection, with the text ".right" title="SSL verschlüsselt" height=15 SSL verschlüsselt".
- Content Area:** The main content area displays a "Sicherer Login" form with fields for Pseudonym and Passwort, and checkboxes for Automatisch einloggen and Remember me.
- Buttons:** A "Login" button and links for "Passwort vergessen?" and "Kostenlos registrieren".
- Bottom Navigation:** A yellow bar with the text "Gut aufgehoben" and a logo for "OnlineStar 2006".

Sicherer Transit

- Da war doch was ...
 - ▶ Abwrackprämie online

Am heutigen Gründonnerstag teilte die Behörde gegenüber heise online mit, dass an der Verschlüsselung weiterhin "mit Hochdruck gearbeitet" werde, derzeit werde das erforderliche Zertifikat erstellt. Auch will das BAFA an dem in die Kritik geratenen

Passwortversand

■ Geschäftsmodelle



Passwortversand

- E-Mail Empfang nach
 - ▶ Registrierung
 - ▶ „Passwort vergessen“

Ihr neues Passwort Inbox | X

star bot@ to me

Sehr geehrte(r) 

ihr Passwort wurde auf Ihre Anfrage hin zurückgesetzt.

Ab sofort ist für Sie ein neues Passwort eingerichtet.

Ihre neuen Daten lauten:

Ihr Benutzername lautet: .com

Ihr Passwort lautet: 

Bitte klicken Sie auf folgenden Link um sich am System anzumelden:

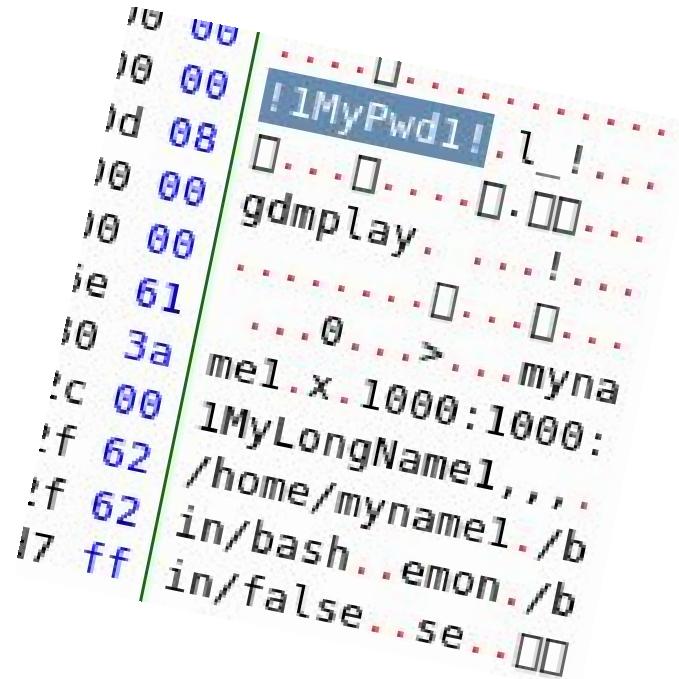
[Systemanmeldung](#)

Passwortversand

Wenn das letzte verwendete Passwort
mitgeschickt wird, dann ...



Probleme und Beispiele



```
!1MyPwd1! l_!
gdmplay. !
myna
mel.x.1000:1000:
1MyLongName1...
/home/mynamel...
in/bash...emon./b
in/false...se...ff
```

Datenhaltung

A8 - Insecure Cryptographic Storage

Datenhaltung

■ Passwörter in Klartext ablegen

- ▶ Datenbank
- ▶ Binäre Dateien
 - Applet / ActiveX
 - Flash
- ▶ Klientseitig
 - Konfigurationsdateien
 - Browser Cookie
 - Flash / Silverlight Cookie
 - HTML
 - Hidden Fields
 - Serialisierte Werte
 - Kommentare

Datenhaltung

■ Flash Login Datei

Only for
Staff

Username:

Password:

Go

**Please enter your
username and password**

Datenhaltung

■ Dissamblierte Flash Datei

```
Label1:  
push 'g';  
push 'user'  
getVariable  
stringEq  
push 'web'  
push 'pass'  
getVariable  
stringEq  
and  
not  
branchIfTrue Label2  
gotoFrame 2  
branch Label21
```

Datenhaltung

■ Passwörter in Klartext ablegen

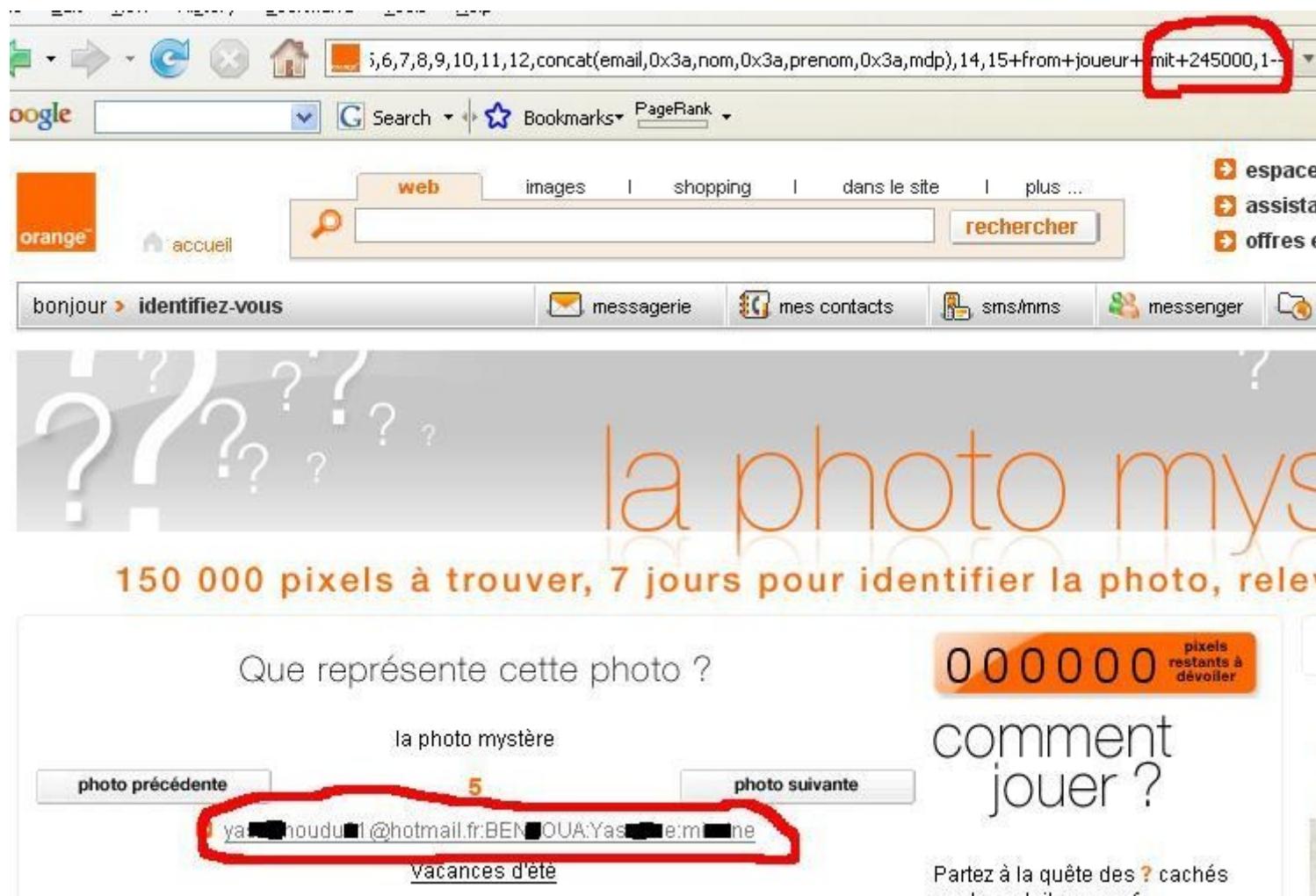
- ▶ Nicht nur in "historisch gewachsenen" Applikationen

■ Einige Beispiele (aus dem Jahr 2009)

- ▶ Orange (.fr, .co.uk)
- ▶ BNP Paribas (.fr)
- ▶ PwC (.de)



Orange



BNP Paribas

The screenshot shows a browser window with the URL <http://unu1234567.baywords.com/2009/10/01/bnp-paribas-expose-sensitive-datesql-injection-with-shell-upload-possibility/>. The page displays the BNP Paribas logo and slogan "La banque d'un monde qui change". The main heading "Bienvenue au cœur de la banque en action" is present. A large banner features the text "le Cercle des Actionnaires". On the left, a sidebar titled "Ma région" lists regions: Nord Est, Nord Ouest, Sud Est, Sud Ouest, Grand Est, Grand Ouest, Bassin Parisien, and Deric. Below the sidebar, there's a section titled "Vidéos" with thumbnails for various video clips, including "Le code a changé", "Jacques Vidal interview", "Jacques Vidal concert", "Christophe Wallemme", "Tigran Hamasyan", and "BNP Paribas dans le monde". The status bar at the bottom of the browser shows the full URL.

Datenhaltung

■ Was kann “Bösewicht” den tun, mit ...

- ▶ Benutzername
- ▶ E-Mail Adresse
- ▶ Passwort
- ▶ Vor- und Nachname
- ▶ ...

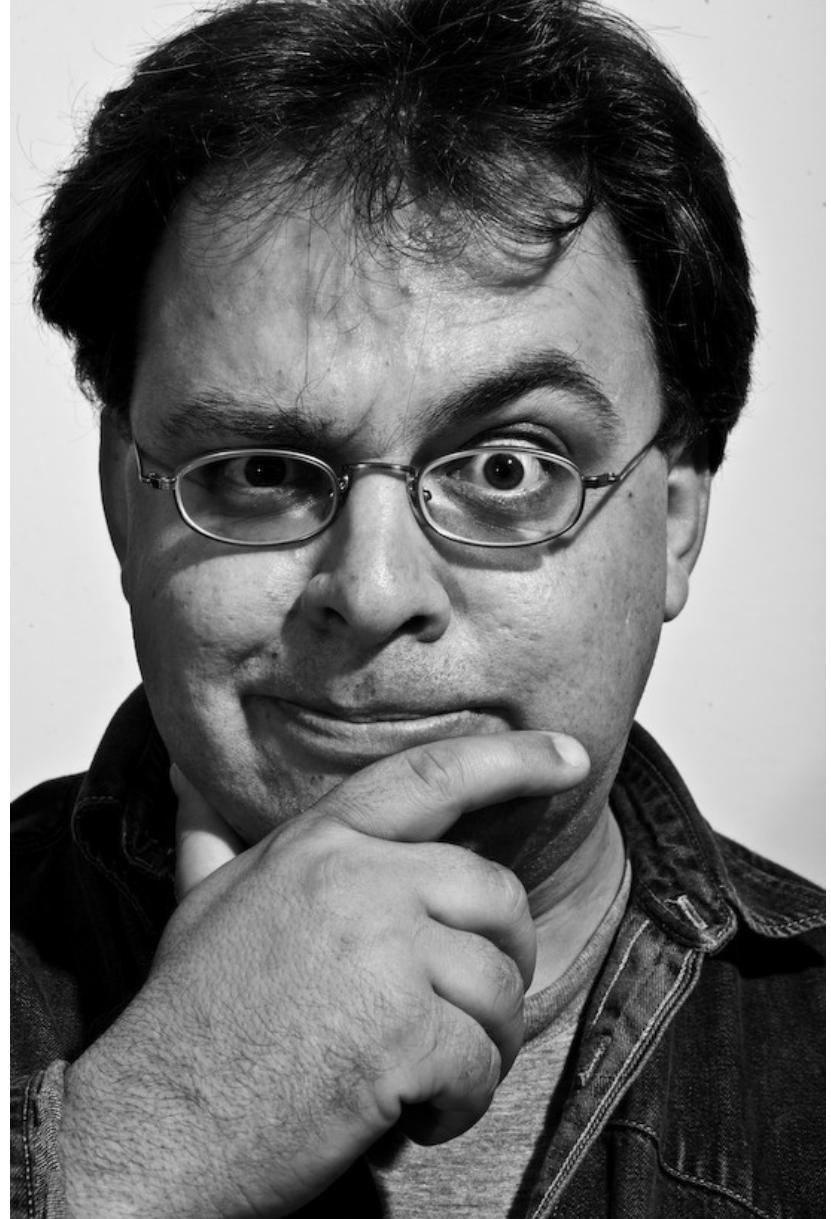
Fauxpas hat weitere Konsequenzen

- Gleiche Anmeldedaten werden oft wieder verwendet
 - ▶ Interessantes Ergebnis aus einer Studie (2008)

Studie

61 % verwenden
nur **EIN** Passwort

für Ihre Online-Aktivitäten



Fauxpas hat weitere Konsequenzen

■ PwC Daten wurden bei Online-Bezahldiensten missbraucht

- ▶ Moneybookers
- ▶ Click&Buy
 - gmx: 13.000 Adressen
 - web.de: 12.000 Adressen
 - Hotmail: 3300 Adressen
 - Yahoo: 2700 Adressen
 - T-Online: 2200 Adressen

Probleme und Beispiele



Bitte erinnere mich was ich
letzten Sommer getan habe

A7 - Broken Authentication and Session Management

Erinnerung – „Passwort vergessen“

If You Forget Your Password...

* Security question:

[Select a Question]

* Your answer:

[Select a Question]

* Birthday:

What is your pet's name?

* ZIP/Postal code:

What was the name of your first school?

Alternate Email:

Who was your childhood hero?

Customizing Yahoo!

* Birthday:

What is your favorite pastime?

ZIP/Postal code:

What is your all-time favorite sports team?

Alternate Email:

What is your father's middle name?

Customizing Yahoo!

What was your high school mascot?

Customizing Yahoo!

What make was your first car or bike?

Customizing Yahoo!

Where did you first meet your spouse?



Erinnerung – „Passwort vergessen“



Erinnerung – „Passwort vergessen“

How Paris Hilton Got Hacked? Bad Password Protection from the *tinkerbell* dept

This morning, in [Good Morning Silicon Valley](#), John Paczkowski joked (I think) that he'd bet "\$5 and a Swarovski-encrusted dunce cap says her password was Tinkerbell." He might be right. While T-Mobile still says they're trying to figure out how Paris Hilton's T-Mobile account got hacked, Brian McWilliams has it all figured out. Her password might not have been [Tinkerbell](#) (the well known name of her dog), but the [secret question to get her password reset was: "What is your favorite pet's name?"](#) Yup. It wasn't necessarily social engineering or a security hole or even real hacking (though, in some sense, it was a combination of all three). It was good, old fashioned, stupidity -- leaving the keys under the front door matt with a big sign that says "keys under the matt" next to it.

Erinnerung – „Passwort vergessen“

- Paris Hilton Hack (2005)
- Sarah Palin Hack (2009)

► „Erinnerungsfragen“ können oft ermittelt werden



Hintertüren ???

■ Nicht dokumentierte Funktionen

■ Passwort Varianten

► "default password"

- Sollten vom Benutzer geändert werden → erfolgt oft nicht
- Zum Teil unbekannte Benutzer
 - Beispiel:
Oracle: OUTLN (ausgestattet mir DBA Rechte)

► "hardcoded password"

- "Wartungszugang"
- Zum Debugging



Einige Beispiele

- Cisco - IP Phone Default Administrative Password

CVE-2002-0881



Einige Beispiele

- ▶ Cisco - WLSE and HSE devices contain hardcoded username and password CVE-2004-0391



Einige Beispiele

- ▶ Cisco - IP/VC 3500 Series Hard-Coded SNMP Community Strings CVE-2005-0612



Einige Beispiele

- ▶ Cisco - Unified IP Conference Stations and IP Phones Default Account, Administrative Bypass and Privilege Escalation CVE-2007-1062 – CVE-2007-1072



Einige Beispiele

► Aruba Networks - Unauthorized Administrative and WLAN Access through Guest Account

CVE-2007-0932, n.runs-SA-2007.001

Regulatory and Safety Compliance

FCC part 15 Class A CE

Industry Canada Class A

VCCI Class A (Japan)

EN 55022 Class A (CISPR 22 Class A), EN 61000-3

EN 61000-4-2, EN 61000-4-3, EN 61000-4-4

EN 61000-4-5, EN 61000-4-6, EN 61000-4-8

EN 61000-4-11, EN 55024, AS/NZS 3548

UL 60950, EN60950

CAN/CSA 22.2 #60950

CE mark, cTUVus, GS, CB, C-tick, Anatel, NOM, MIC, IQC

Aruba Networks, Sunnyvale, Calif., the Mobile Edge company, is delivering the only Wireless LAN (WLAN) system that meets all requirements of the U.S. Department of Defense's (DoD's) recent mandate on secure wireless access and Intrusion Detection Systems (IDS). DoD Directive (DoDD) 8100.2, which was released on June 2, 2006, provides additional guidance on the requirements for any wireless device that is connected to the DoD Global Information Grid and specifies that all such systems should be capable of delivering integrated IDS in addition to other security measures.



Einige Beispiele

- Aruba Networks - Unauthorized Administrative and WLAN Access through Guest Account

CVE-2007-0932, n.runs-SA-2007.001



Agenda



Fazit

Fazit (1/2)

- Verwenden Sie generische Fehlermeldungen
- Verwenden Sie keine Klartextprotokolle
- Speichern Sie sensible Daten nur server-seitig ab
- Wenden Sie kryptografisch unbedenkliche Algorithmen an
- Vorsicht bei „Passwort vergessen“ Funktionen

- Verzichten Sie auf „Features“
 - ▶ „Standard Benutzer/Passwörter“ sind tabu

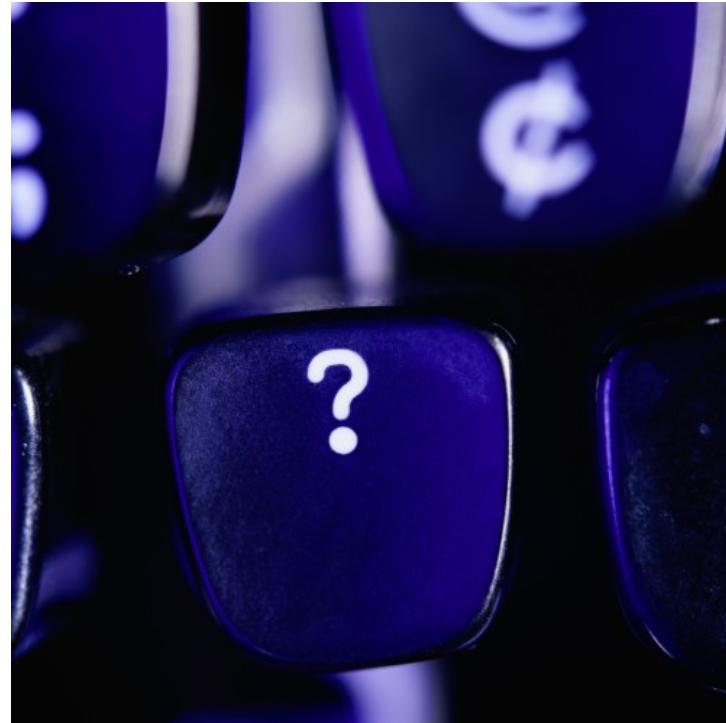
Fazit (2/2)

■ Design Bugs
sabotieren
die Sicherheit der Gesamtlösung
von Beginn an



- ▶ Selbst bei sicherer Implementierung kann das Endprodukt nicht sicher sein

Vielen Dank für Ihre Aufmerksamkeit !



Fragen ?!