



HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

JSSI Rouen 2008

Sécurité des applications

Louis Nyffenegger
<Louis.Nyffenegger@hsc.fr>

- Un sujet vaste
- La sécurité des applications :
 - Développement
 - Déploiement de l'application
 - Vie de l'application (vulnérabilités, mises-à-jour)
- Les applications
 - Application « éditeur »
 - Application libre
 - Application « maison »
- Quelques exemples

- Injection SQL :
 - Changement de la sémantique d'une requête

∅ Démo !

<http://monsiteweb/product.php?id=1>

```
select nom from articles where id=1 ;
+-----+
| nom    |
+-----+
| chaise longue |
+-----+
```

<http://monsiteweb/product.php?id=1> union select login from users;

```
select nom from articles where id=1 union select login from users;
+-----+
| nom    |
+-----+
| chaise longue |
| admin  |
| user   |
+-----+
```

- Traversée de répertoires (« *directory traversal* ») :

<http://monsiteweb/file.php?file=fichier.pdf>

<http://monsiteweb/file.php?file=../../../../../../../../etc/passwd>

- Erreur algorithmique/de logique :
 - Achat en quantité négative
 - Realvnc 4.1
- Injection de code :
 - Reprise d'une données utilisateurs sans filtrage
<http://monsiteweb/sync.sh?dir=images ; cat /etc/passwd>
- Erreur d'architecture
 - application lourde accédant directement à la base de données
- ...

- Les interfaces d'administration (Tomcat & Jboss)
 - Possibilité de déployer à distance des applications
 - Prise de contrôle triviale du serveur
 - Rebond
- Les comptes par défaut :
 - Existence de liste sur internet pour la majorité des applications (et des équipements réseaux)
 - Exemple avec Oracle :
 - dbsnmp/dbsnmp
 - sys/sys
 - sys/change_on_install
 - system/system
 - outln/outln
 - oe/oe
 - hr/hr
 - dip/dip
 - **Démo !**
 - ...

- 32 vulnérabilités cette nuit

National Vulnerability Database

Paramètres de flux...

Texte complet

Titres

Afficher : [0 nouvel élément](#) - [tous les éléments](#)

[Tout marquer comme lu](#)

[Actualiser](#)

[afficher les détails](#)

☆ CVE-2008-4638 (veritas_file_system) »

22 oct. 2008 (hier)

qioadmin in the Quick I/O for Database feature in Symantec Veritas File System (VxFS) on HP-UX, and before 5.0 MP3 on Solaris, Linux, and AIX, allows local users to read arbitrary files by causing qioadmin to write a file's content to standard error.

☆ Activer le suivi [Partager](#) [Partager avec une note](#) [E-mail](#) [Ajouter des tags](#)

☆ CVE-2008-4637 (cpcommerce) »

22 oct. 2008 (hier)

Cross-site scripting (XSS) vulnerability in cpCommerce before 1.2.4 allows remote attackers to inject arbitrary web script or HTML via unknown vectors in the advanced search feature. NOTE: this is probably a variant of CVE-2008-4121.

☆ Activer le suivi [Partager](#) [Partager avec une note](#) [E-mail](#) [Ajouter des tags](#)

☆ CVE-2008-4121 (cpcommerce) »

22 oct. 2008 (hier)

Multiple cross-site scripting (XSS) vulnerabilities in cpCommerce before 1.2.4 allow remote attackers to inject arbitrary web script or HTML via (1) the search parameter in a search.quick action to search.php and (2) the name parameter in a sendtofriend action to sendtofriend.php.

☆ Activer le suivi [Partager](#) [Partager avec une note](#) [E-mail](#) [Ajouter des tags](#)

☆ CVE-2008-3248 (veritas_file_system) »

22 oct. 2008 (hier)

qiomkfile in the Quick I/O for Database feature in Symantec Veritas File System (VxFS) on HP-UX, and before 5.0 MP3 on Solaris, Linux, and AIX, does not initialize filesystem blocks during creation of a file, which allows local users to obtain sensitive information by creating and then reading files.

☆ Activer le suivi [Partager](#) [Partager avec une note](#) [E-mail](#) [Ajouter des tags](#)

- Importance de la vulnérabilités
- Produits impactés

- Problématique des mises à jour :
 - Avoir le temps
 - Pouvoir stopper le service
- De plus en plus d'applications se mettent à jour automatiquement
- Nécessité d'un suivi des listes de sécurité
- Nécessité d'un échantillonnage

- Bonnes pratiques lors du développement :
 - Ne jamais faire confiance au client de l'application
 - Toujours partir du principe que le code source est public
- Importance du durcissement des applications avant leur mise en production
 - Comptes par défaut
 - Minimisation (« *Secure by default* » ou pas...)
- Importance de la mise à jour des applications :
 - Veille : mailing-list (sécurité, développement), « 2ème mardi », ...
 - Déploiement « intelligent » des mises à jour (échantillon)

Questions ?

Louis.Nyffenegger@hsc.fr

www.hsc.fr