



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



# CLUSIR-EST

# Sécurité des bases de données

**Louis Nyffenegger**  
<Louis.Nyffenegger@hsc.fr>

- Coeur du Système d'informations.
- Stockage de toutes les données importantes/métiers dans des bases :
  - données clients ;
  - données produits ;
  - gestion de la **paie** ;
  - **comptabilité** (notes de frais).
- Pas/peu d'interruption de services possibles :
  - ne pas prendre de risques avec des mises à jour ;
  - ne pas redémarrer le SGBD.

- Budgets sécurité :
  - vont d'abord à l'achat de système de sécurité (firewalls, IDS, ...)
  - à la formation
  - à la sécurisation des applications/des serveurs
- ☞ le SGBD est généralement un parent pauvre de la sécurité
- Complexité
  - Les SGBD sont une affaire de spécialistes :
    - au niveau de leur gestion : DBA,
    - au niveau de la programmation ;
  - peu ou mal enseigné en université ou école d'ingénieur ;
  - faire de l'Oracle deux fois par an n'est pas suffisant.

- Attaques frontales :
  - directement en ayant accès à la base de données ;
  - en passant par des applications fournies avec le SGBD.
- Attaques via le système d'exploitation :
  - compromission de la machine et rebond sur le SGBD.
- Attaques via une application utilisant la base de données :
  - défaut de conception d'une application cliente ;
  - injections SQL sur une application Web ou une application utilisant le SGBD.

# Attaques frontales : comptes par défaut

- Trop souvent (tout le temps), présence de comptes par défaut :
  - `scott/tiger`, `dbstmp/dbstmp`, ...
  - `sa/`
  - `root/` , `root/root`, ...
- Comptes par défaut avec mot de passe faible
- Attaques triviales donc dangereuses.
- Suppression par les fournisseurs de SGBD des comptes par défaut de plus en plus fréquente

- Vulnérabilité dans l'authentification de Mysql
  - 4.1.0 -> 4.1.2
  - 5.0
- Attaque du Listener oracle :
  - CVE-2002-0965 Long Service Name Buffer Overflow
  - CAN-2002-0509 TNS Remote Denial Service
  - CVE-2002-0567 Direct TNS Connection to ExtProc

- Élévation de privilèges :
  - dans les procédures sous Mysql 5 exécutées avec les droits du créateur de la procédure
  - dans les procédures fournies par défaut dans Oracle
- Rebond sur le système d'exploitation :

- lecture de fichiers sur le système :

```
Select load_file('/etc/passwd')
```

- écriture de fichiers sur le système :

```
Select * from users into outfile '/tmp/users'
```

- lancement de commandes sur le système :

```
xp_cmdshell 'dir c:\'
```

# Attaque via le système d'exploitation

- Compte par défaut sur le système :
  - oracle/oracle
  - mots de passe triviaux
- Vulnérabilités du système d'exploitation :
  - NT4
  - Solaris
- Possibilité de se connecter au SGBD :
  - sans accréditation ;
  - en récupérant celle-ci dans un fichier de configuration d'une application Web.
- Pas besoin de compte : présence de sauvegarde de la base de données en lecture pour tous sur le disque

# Attaque via une application : message d'erreurs

## Erreur SQL !

```
SELECT count(*) FROM ##### WHERE id###='000018'' and  
###='1'
```

**You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '1' at line 1**

```
java.lang.NullPointerException at  
sun.jdbc.odbc.JdbcOdbcDriver.initialize(JdbcOdbcDriver.java:436)  
  at sun.jdbc.odbc.JdbcOdbcDriver.getPropertyInfo(JdbcOdbcDriver.java:346)  
  at  
org.objectweb.rmijdbc.RJDriverServer.getPropertyInfo(RJDriverServer.java:158  
)  
  at sun.reflect.GeneratedMethodAccessor4.invoke(Unknown Source)  
  at  
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl  
.java:41)  
  at java.lang.reflect.Method.invoke(Method.java:386)  
  at sun.rmi.server.UnicastServerRef.dispatch(UnicastServerRef.java:278)  
[...]
```

# Attaque via une application : erreur de conception

- Programme coté client :
  - applet Java ;
  - animation flash ;
  - application sur le système d'exploitation (Java, C#, ... ).
- Accès direct à la base de données :
  - identifiant et mot de passe en clair dans l'application ;
  - identifiant et mot de passe un peu offusqué.
- Nécessité d'une compréhension de qui fait quoi et de la sécurité.

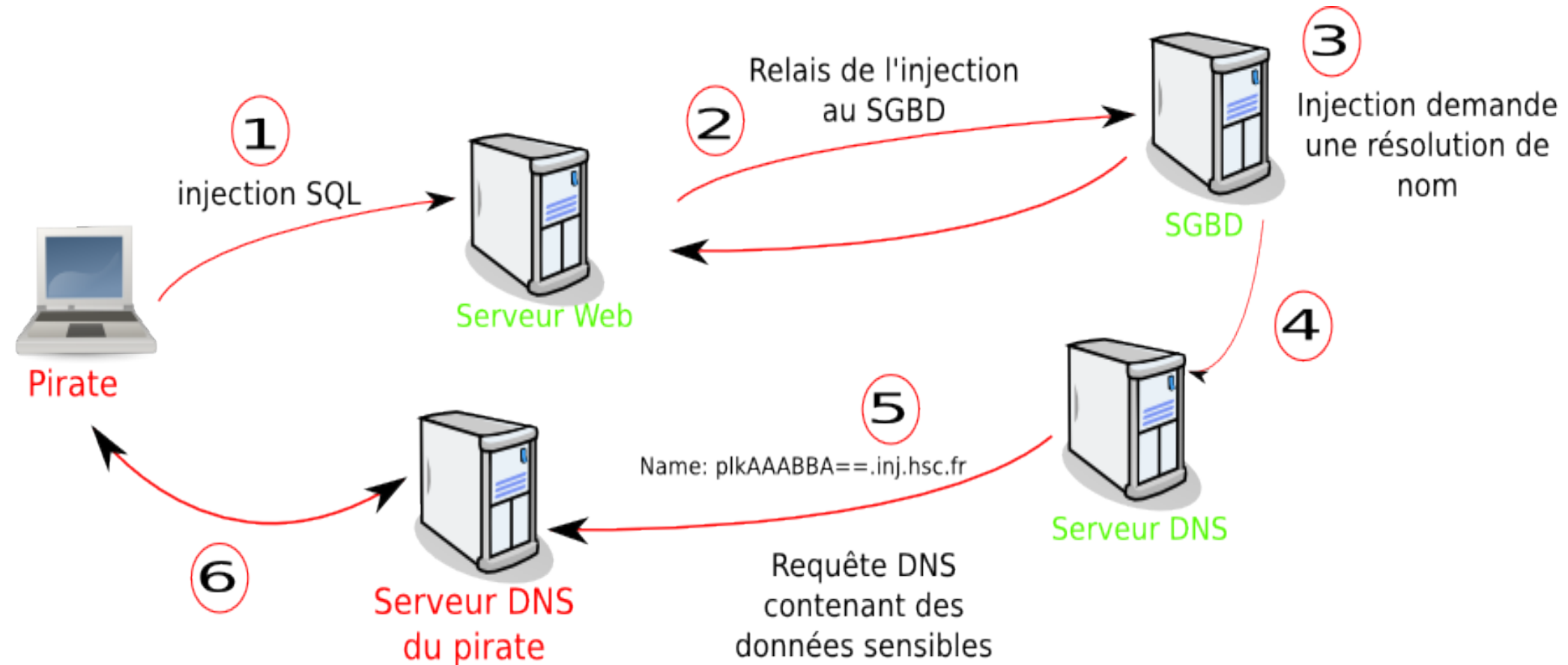
- Mauvais filtrage des données par une application
- Possibilité de modifier arbitrairement le contenu de la requête SQL :

```
$sql = 'SELECT nom from articles where id = $_GET['id'];
```

- `$_GET['id'] = 1`    ➔ l'article 1 est affiché
- `$_GET['id'] = 1'`    ➔ **message d'erreur**
- `$_GET['id'] = 1 and 1=0 /*`    ➔ aucun article n'est affiché
- `$_GET['id'] = 1 union select password from users LIMIT 2,1 /*`    ➔ mot de passe ?

## Démonstration

- Dans les mauvais cas, pas de retour de données dans l'application :
  - soit rien ne se passe : affichage classique de la page ;
  - soit un message d'erreur est généré.
- Possibilité de brute forcer à partir de cette état en testant des égalités
- Possibilité d'utiliser des canaux de sorties différents :
  - HTTP
  - TCP
  - DNS



- Modification de vues de la base de données :
  - v\$session,
  - gv\_\$session,
  - flow\_sessions,
  - v\_\$process.
- Ajout d'une condition :

```
WHERE username != 'INTRUS'
```

[http://www.red-database-security.com/wp/oracle\\_rootkits\\_2.0.pdf](http://www.red-database-security.com/wp/oracle_rootkits_2.0.pdf)

- Sujet en plein développement depuis cet été (BlackHat) :
  - les bases de données sont victimes d'attaques comme tout système
  - des analyses post-incident sont nécessaires
- Peu d'outils pour l'instant :
  - un outil en cours de développement par David Litchfield : FEDS
- Conférences sur le sujets :
  - <http://databasesecurity.com/database-forensics.htm>
  - <https://www.blackhat.com/presentations/bh-usa-07/Fowler/Presentation/bh-usa-07-fowler.pdf>

- Minimiser/durcir le SGBD :
  - supprimer les comptes par défaut/changer les mots de passe ;
  - suppression des packages non nécessaires et les applications périphériques ;
  - minimisation des accès vers le SGBD ;
  - minimisation des accès depuis le SGBD.
- Minimiser les interactions entre l'OS et le SGBD en terme d'accréditations.
- Mettre à jour le SGBD régulièrement.
- Augmenter la taille des journaux.

Former les développeurs au développement sécurisé.

- Databases security :
  - <http://www.databasesecurity.com/>
- Site Pete Finnigan :
  - <http://www.petefinnigan.com/orasec.htm>
  - <http://www.petefinnigan.com/tools.htm>
- SQL Zoo :
  - <http://sqlzoo.net/>

- Des informations sensibles en jeu.
- Peu de sécurité actuellement :  
**« Le SGBD n'est accessible qu'en interne »**
- Les SGBD : une affaire de spécialiste.
- La sécurité des SGBD ne peut pas être mise de côté.
- un chance pour les administrateurs : l'intrusion dans un SGBD demande aussi des connaissances pointues.

- **Tutoriel au Salon de la Sécurité : Sécurité de la voix sur IP le 21 novembre 2007**
  - [http://www.hsc.fr/conferences/reed2007\\_securite\\_voip.html.fr](http://www.hsc.fr/conferences/reed2007_securite_voip.html.fr)
- **Tutoriel au Salon de la Sécurité : Sécurité des Webservices le 22 novembre 2007**
  - [http://www.hsc.fr/conferences/reed2007\\_securite\\_webservices.html.fr](http://www.hsc.fr/conferences/reed2007_securite_webservices.html.fr)
- **Réalisation pratique des Tests d'Intrusion Paris du 21 au 25 janvier 2008**
  - [http://www.hsc.fr/services/formations/formations\\_ti.html.fr](http://www.hsc.fr/services/formations/formations_ti.html.fr)

## Questions ?

Louis.Nyffenegger@hsc.fr  
www.hsc.fr