APPLICATION SECURITY, INC.

ISACA Houston:

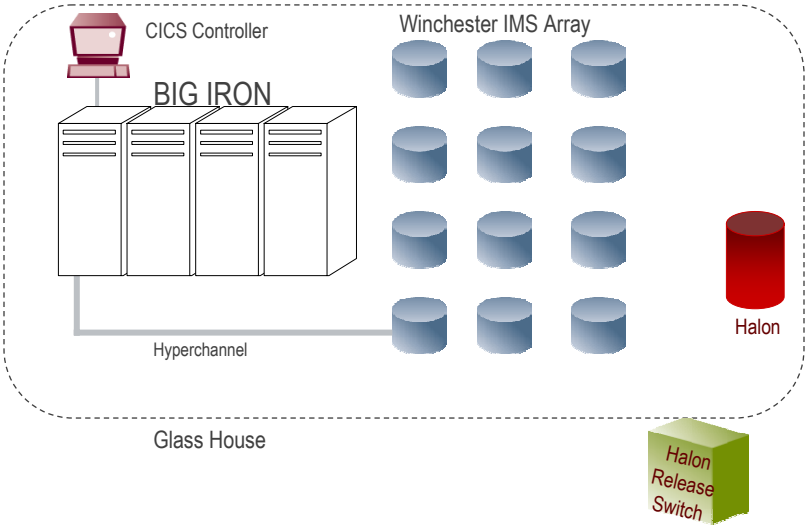
Anatomy of a Database Attack

Mark R. Trinidad
Product Manager
mtrinidad@appsecinc.com
March 19, 2009

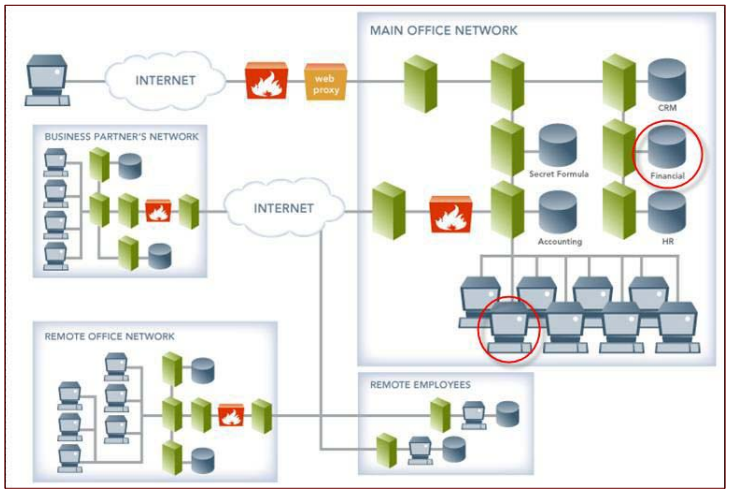
This Session's Agenda

- Introduction
  - Landscape
  - Database Vulnerabilities Are The New Front-Lines
- Attacking Where the Data Resides
  - Planning an Attack
  - Recreating Database Attacks
- Proactively Combating Database Attacks
  - Database Vulnerability Assessment / Activity Monitoring
  - Best Practices for Securing Your Databases
  - Resources for Further Advice and Research

Yesteryear's Data Processing Environment



Today's Data Processing Environment



Databases Are Under Attack

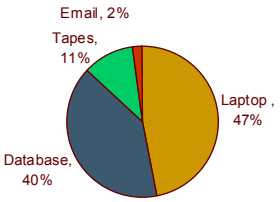
253,399,762

Total number of records compromised since April, 2005

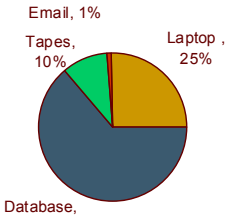
Hundreds of incidents

Virtually every industry

Source of Breach



Records Lost



Privacy Rights CLEARINGHOUSE

APPLICATION SECURITY, INC.

Database Vulnerabilities

Established Vulnerability Categories

- Most commonly known to apply to OS's and NOS's

	Operating Systems & Network Operating Systems (Microsoft Windows, Unix, and Linux)				
Default & Weak Passwords			✓		
Denial of Services & Buffer Overflows			✓		
Misconfigurations & Resource Privilege Management			✓		

Categories Also Apply to Databases!

- Databases are a separate attack vector!

	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	✓	✓	✓	✓	✓
Denial of Services & Buffer Overflows	✓	✓	✓	✓	✓
Misconfigurations & Resource Privilege Management	✓	✓	✓	✓	✓

Database Vulnerabilities: Default & Weak Passwords

- Databases have their own user accounts and passwords

	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	✓	✓	✓	✓	✓

Database Vulnerabilities: Default & Weak Passwords

- Oracle Defaults (hundreds of them)
  - User Account: internal / Password: oracle
  - User Account: system / Password: manager
  - User Account: sys / Password: change_on_install
  - User Account: dbsnmp / Password: dbsnmp
- MySQL Defaults
  - User Account: root / Password: null
  - User Account: admin / Password: admin
  - User Account: myusername / Password: mypassword
- Sybase Defaults
  - User Account: SA / Password: null
- Microsoft SQL Server Defaults
  - User Account: SA / Password: null

Database Vulnerabilities: Default & Weak Passwords

- It is important that you have all of the proper safeguards against password crackers because:
  - Not all databases have Account Lockout
  - Database Login activity is seldom monitored
  - Scripts and Tools for exploiting weak identification control mechanisms and default passwords are widely available

Database Vulnerabilities: Denial of Services (DoS) & Buffer Overflows

- Databases have their own DoS's & Buffer Overflows

	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	✓	✓	✓	✓	✓
Denial of Services & Buffer Overflows	✓	✓	✓	✓	✓

Denial of Services: Database have their own DoS Attacks

- Result in the **database crashing or failing to respond** to connect requests or SQL Queries.

- **Significant Database Denial of Services:**

  Oracle8i: NSPTCN data offset DoS

  Oracle9i: SNMP DoS

  Microsoft SQL Server: Resolution Service DoS

  IBM DB2: Date/Varchar DoS

Buffer Overflows: Database have their own Buffer Overflows

- Result in an **unauthorized user** causing the application to perform an action the application was not intended to perform.

- **Can allow arbitrary commands to be executed**
  - No matter how strongly you've set passwords and other authentication features.

- **Significant Database Buffer Overflows:**
  - Oracle9i: TZ_OFFSET buffer overflow
  - Microsoft: pwdencrypt buffer overflow / Resolution Stack Overflow
  - Sybase: xp_freedll buffer overflow

Misconfigurations & Resource Privilege Management Issues

- Misconfigurations can make a database vulnerable

	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	✓	✓	✓	✓	✓
Denial of Services & Buffer Overflows	✓	✓	✓	✓	✓
Misconfigurations & Resource Privilege Management	✓	✓	✓	✓	✓

Misconfigurations & Resource Privileges can make Databases Vulnerable

Oracle
- External Procedure Service
- Default HTTP Applications
- Privilege to Execute UTL_FILE

Microsoft SQL Server
- Standard SQL Server Authentication Allowed
- Permissions granted on xp_cmdshell

Sybase
- Permission granted on xp_cmdshell

IBM DB2
- CREATE_NOT_FENCED privilege granted (allows logins to create SPs)

MySQL
- Permissions on User Table (mysql.user)

Database Vulnerabilities Wrap-up

	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	✓	✓	✓	✓	✓
Denial of Services & Buffer Overflows	✓	✓	✓	✓	✓
Misconfigurations & Resource Privilege Management	✓	✓	✓	✓	✓

Emerging Database Threats

- Sophisticated attacks that exploit un-patched vulnerabilities
- Cyber espionage efforts by well resourced organizations looking to extract large amounts of data
- Insider attacks
- Insider mistakes
- Advanced identity theft via database rootkits
- Increasingly sophisticated social engineering leading to full-blown database disclosures
- Weak or non-existent audit controls
- Powerful self-propagating attacks distributed via “infection kits” on legitimate websites

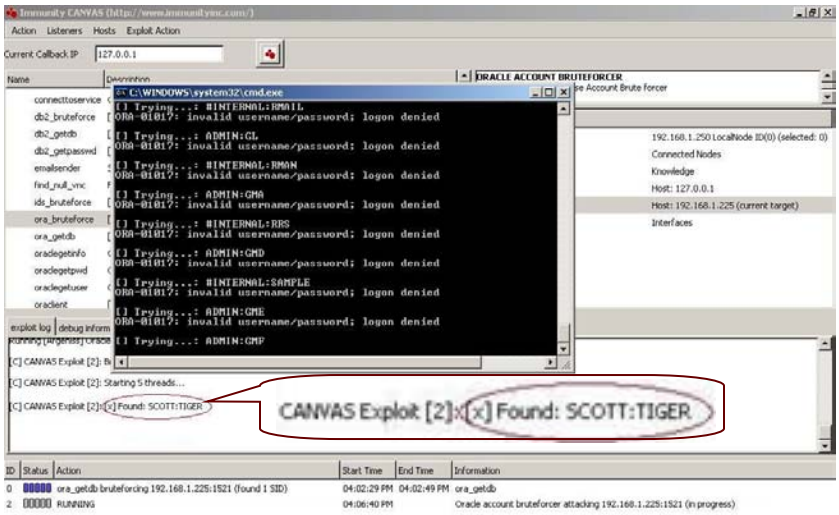
APPLICATION SECURITY, INC.

Database Attack Illustrations

Directly Attacking A Database: *Oracle Password Cracking*

- Attack Target: Oracle
- Privilege Level: Network Connection to Target
- Scenario:
  - Illustration of an Attacker Using Various Tools to Crack Oracle Passwords
- Vulnerabilities Exploited:
  - Default & Weak User Account Passwords
  - Misconfigurations & Privilege Resource Management

Directly Attacking A Database: *Oracle Password Cracking*



Directly Attacking A Database: *Oracle Password Cracking*

Google "oracle password cracker" Search Advanced Search Preferences

Results 1 - 10 of about 1,790 for "oracle password cracker".

Oracle Password Cracker (Checker)
Checkpwd - **Oracle password cracker**.
www.red-database-security.com/software/checkpwd.html -

Oracle Passwords
Oracle Password Cracker Checkpwd 2.00 by Red-Database-Security GmbH (fast, pw/sec, C-based, 7-11g); **Oracle Password Cracker** Benchmark Benchmark for ...
www.red-database-security.com/whitepaper/oracle_passwords.html - 17k -
Cached - Similar pages
More results from www.red-database-security.com »

Pete Finnigan's Oracle security weblog
This cracker is the fastest **Oracle password cracker** that i know of - and I know ... It is also probably the best featured **Oracle password cracker** available. ...
www.petefinnigan.com/weblog/archives/00000535.htm - 32k - Cached - Similar pages

Pete Finnigan - Oracle and Oracle security information
This is a very useful tool for performing Oracle database security audits as it is the first publicly available stand alone **Oracle password cracker** written ...
www.petefinnigan.com/tools.htm - 100k - Cached - Similar pages
More results from www.petefinnigan.com »

oracle password cracker orabf version 0.7
www.toolcrypt.org/tools/orabf/index.html - Similar pages

Oracle password best practices
Figure 7.1 **Oracle Password Cracker**. You don't make it to the front page on a list of nearly 2 million search entries without a lot of clicks. ...
searchoracle.techtarget.com/tip/0,289483,sid41_gci1281026,00.html - 57k -
Cached - Similar pages

Penetration Testing: **Oracle password cracker**
Oracle password cracker. This message : [Message body] [More options]; Related messages : [Next message] [Previous message] [Next in thread ...
seclists.org/pen-test/2008/Jan/0199.html - Similar pages

Directly Attacking A Database Recap: *Oracle Password Cracking*

- Outcome:
  - Compromised an Oracle User Account!
- Vulnerabilities Exploited:
  - Weak Password
  - Misconfigurations & Resource Privilege Management
- How did we do it?
  - Freely Available Exploit Code!
  - Google: **Oracle Password Cracker**

Attacking Databases Over the Internet : *Exploiting Search Engines (Google)*

- Attack Target: Oracle
- Privilege Level: Anyone with Access to the Web and a Search Engine
- Outcome: Complete Administrative Control
- Vulnerabilities Exploited:
  - Misconfigurations & Resource Privilege Management

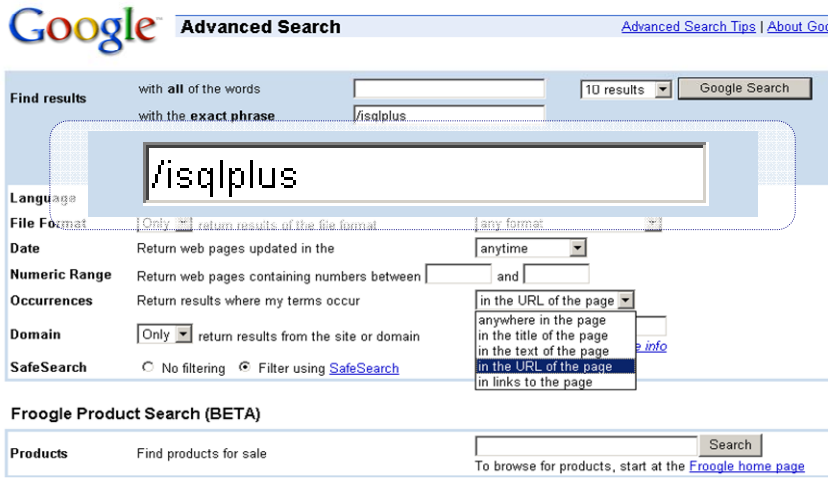
How is Google used for attacks?

- First thing an attacker needs is information
  - Where to attack
  - What a site is vulnerable to
- Google is a large repository of information
  - Every web page in your application
  - Every domain on the Internet
- Google provides 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**

Example – looking for iSQL*Plus

- Oracle HTTP Servers
  - Execute queries on database using an HTTP form
  - Accessed using the URL **/isqlplus**
  - By default runs on any Oracle HTTP server installed with:
    - Oracle Applications Server
    - Oracle Database Server
- Search can be performed on Google
  - looking for **Oracle HTTP servers**
  - Using the “allinurl” advanced search feature

Using Google Advanced Search



Results of Google Advanced Search

iSQL*Plus Release 9.2.0.5.0 Production: Anmelden - [Translate this page]
Anmelden. Benutzername: Kennwort: Connect-String: ueb.
holle.db.informatik.uni-kassel.de/**isqlplus** - 3k - Cached - Similar pages

iSQL*Plus Release 9.2.0.4.0 Production: Logowanie
Logowanie. Nazwa użytkownika: Hasło: Identyfikator połączenia:
dblab.cs.put.poznan.pl/**isqlplus** - 4k - Cached - Similar pages

iSQL*Plus Release 9.2.0.1.0 Production: Anmelden - [Translate this page]
Anmelden. Benutzername: Kennwort: Connect-String:
lwis02.inf.fh-koeln.de:7778/**isqlplus** - 3k - Cached - Similar pages

[DOC] Table des matières
File Format: Microsoft Word 2000 - View as HTML
... Middle Tier □ Serveur Oracle HTTP. Pour installer **iSQLPlus** : Unziper la distribution **iSQLPlus** en .zip dans un répertoire temporaire. ...
www.isnetne.ch/lbd/SGBD/oracle/ documents/**isqlplus**/Inst_**isqlplus**817.doc - Similar pages

iSQL*Plus Release 9.2.0.1.0 Production: Login
Login. Username: Password: Connection Identifier: oracle.unc.edu.
https://oraclient.unc.edu/**isqlplus** - 3k - Cached - Similar pages

Gooooogle
Result Page: Previous 1 2 3 4 Next

allinurl: "/isqlplus" Search

Search within results | Language Tools | Search Tips

Yahoo! Advanced Search Works Too…..

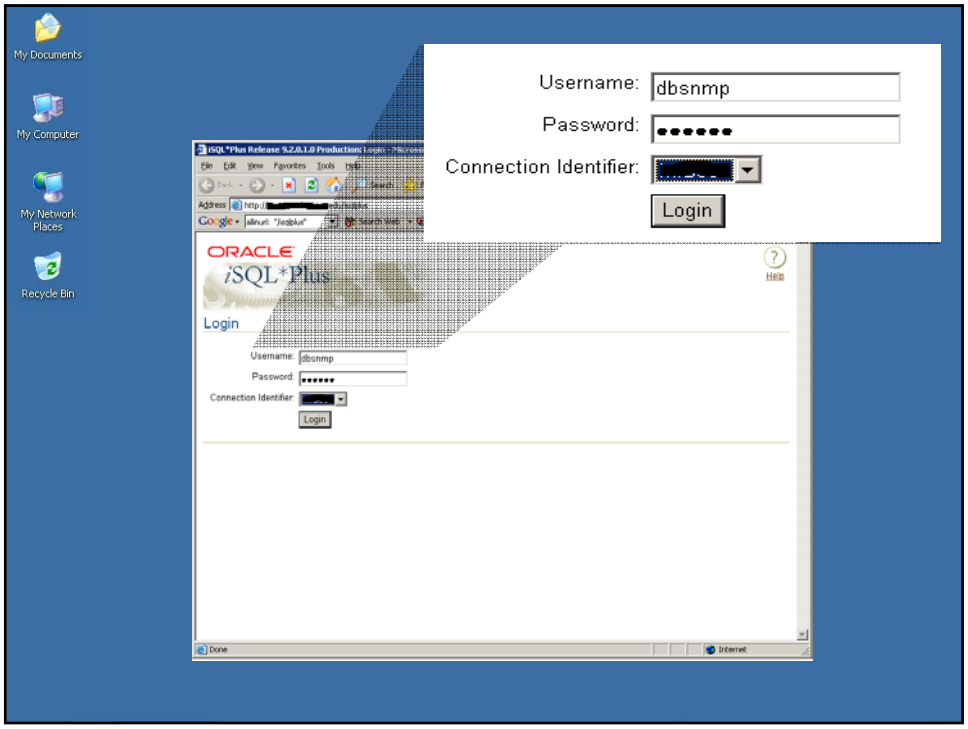
YAHOO! search | Web | Images | Directory | Local NEW! | News | Products

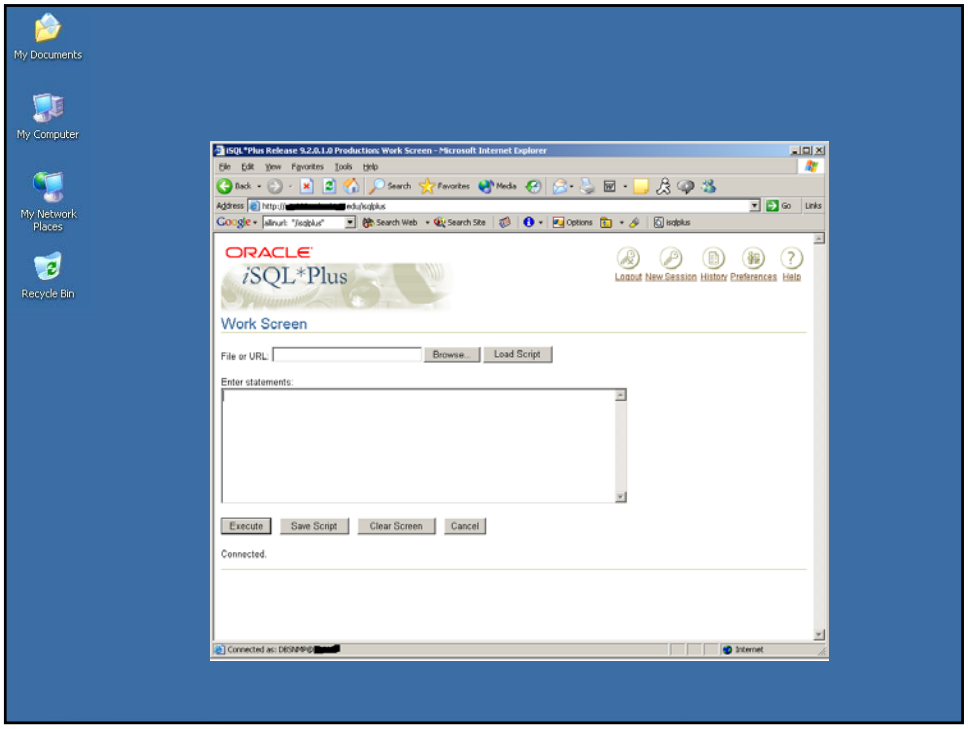
"iSQL*Plus Release" Search

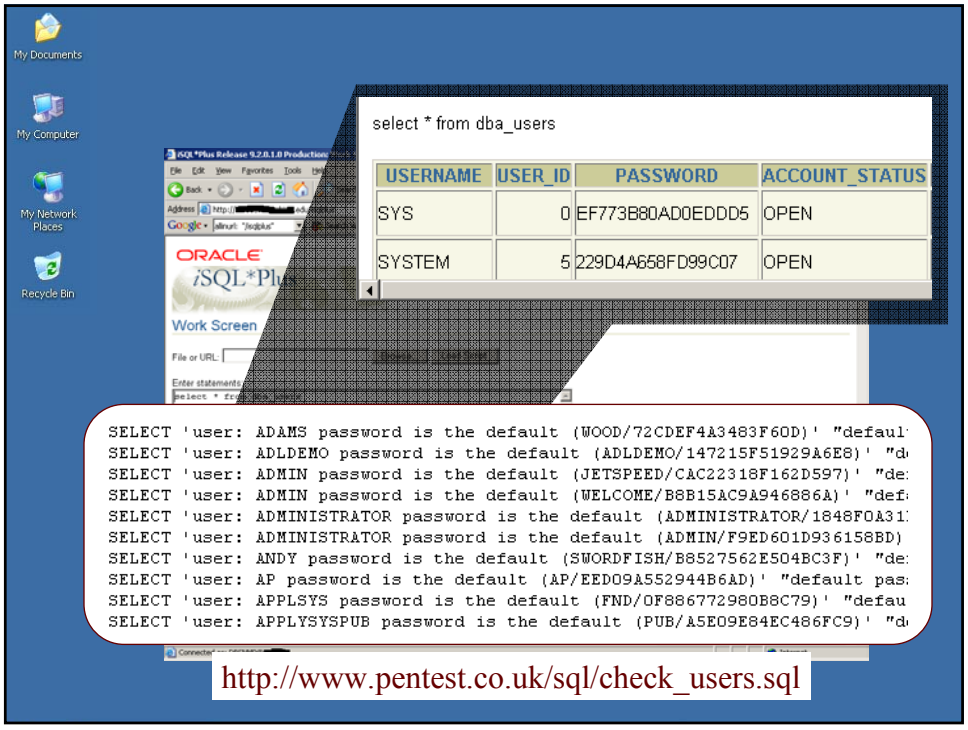
Shortcuts Advanced

Search Results Results **1** - **10** of about **79** for **"iSQL*Plus Release"** - 0.23

1. iSQL*Plus Release 9.2.0.1.0 Production: Login
   Help. Login. Username: Password: Connection Identifier:
   gettysburg.wccnet.edu:7777/**isqlplus** - 3k - Cached - More from this site
2. iSQL*Plus Release 9.0.1
   Script Location: Enter statements:
   student.cob.ohiou.edu/jb250299/ sqlweb.htm - 20k - Cached - More from this site
3. iSQL*Plus Release 9.0.1
   Script Location: Enter statements:
   student.cob.ohiou.edu/jb250299/ sarasql.htm - 23k - Cached - More from this site
4. iSQL*Plus Release 9.2.0.5.0 Production: Login
   Help. Login. Username: Password: Connection Identifier:
   isqlplus.it.swin.edu.au:7777/ **isqlplus** - 3k - Cached - More from this site
5. What's New in SQL*Plus?
   … Any user customizations can be manually merged into the default **iSQL*Plus Release** 9.2 configuration file … There are several new parameters for sizing and tuning **iSQL*Plus Release** 9.2 …
   cs.utah.edu/classes/cs6530/oracle/**…** /server.920/a90842/whatsnew.htm - 30k - Cached - More from this site
6. iSQL*Plus Release 10.1.0.2
   * Indicates required field. Username. Password. Connect Identifier. Help. Copyright © 2003, Oracle. All rights reserved.
   www.onlinecreation.com:5560/ **isqlplus** - 9k - Cached - More from this site







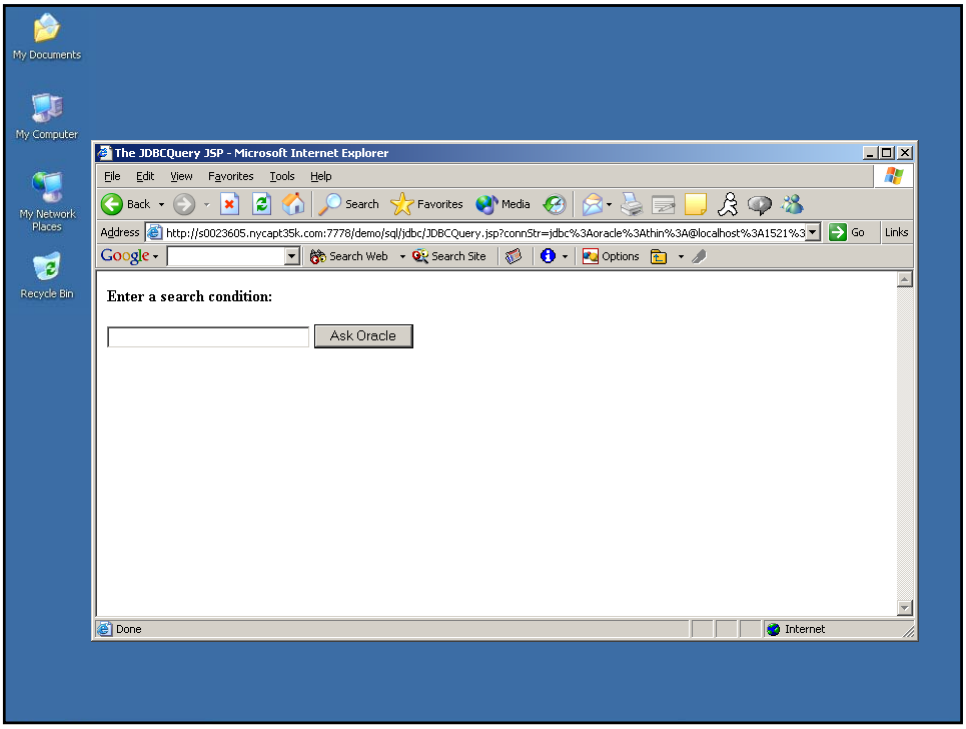
http://www.pentest.co.uk/sql/check_users.sql

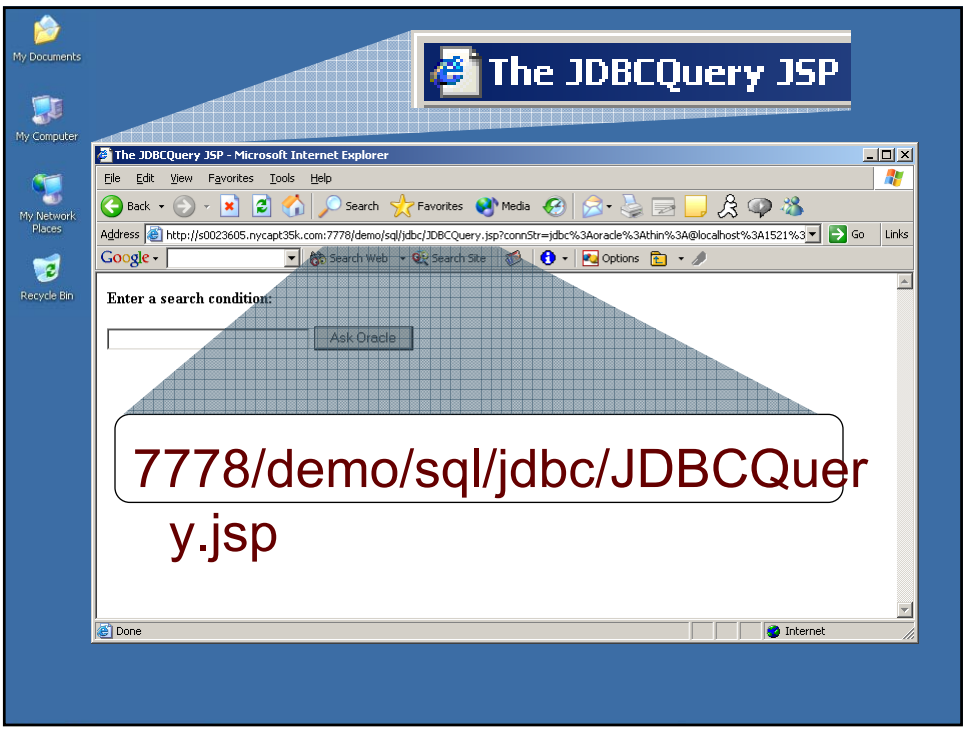
Attacking Databases Over the Internet: *Exploiting Search Engines (Google)*

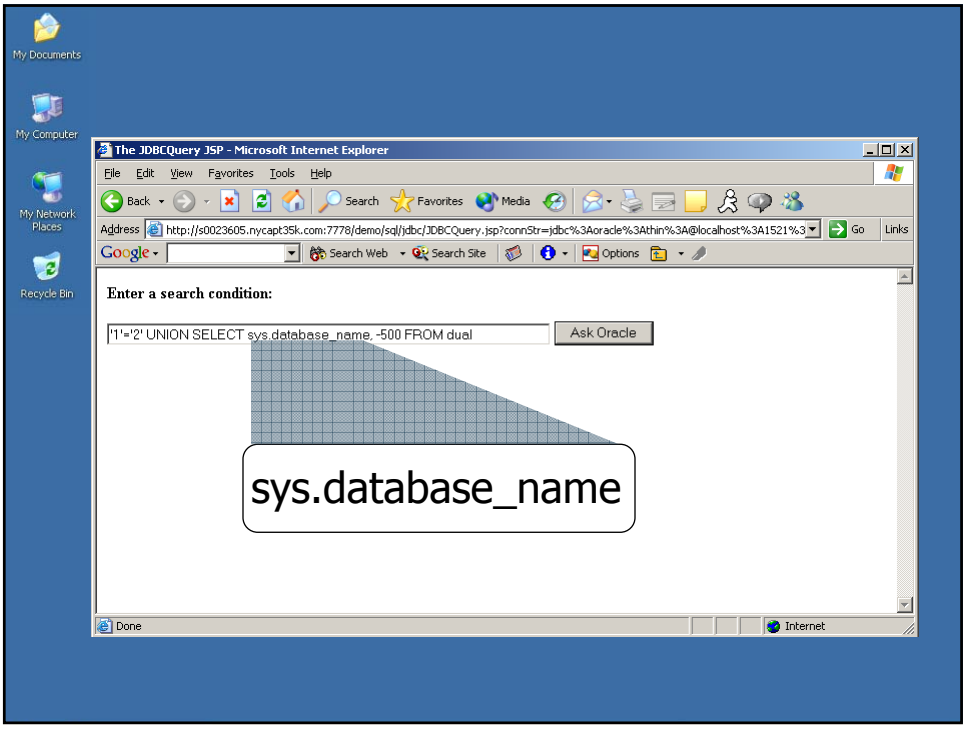
- Outcome: First step towards administrative control!
- Vulnerabilities Exploited:
  - Misconfigurations & Resource Privilege Management
- How did we do it?
  - "Googled" for "isql" and took advantage of poor security practices!

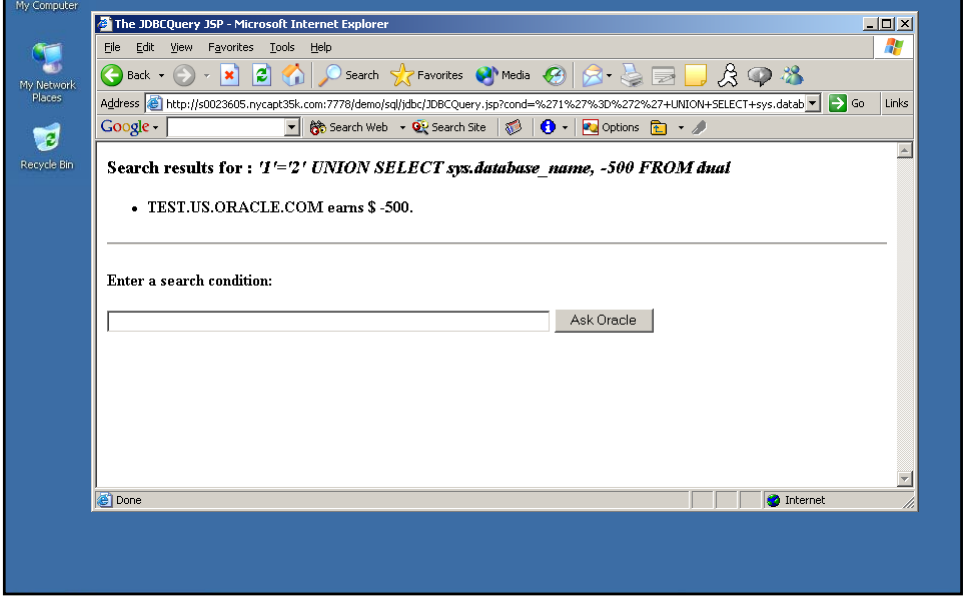
Attacking through a Web Application: *Oracle JDBC Query Sample*

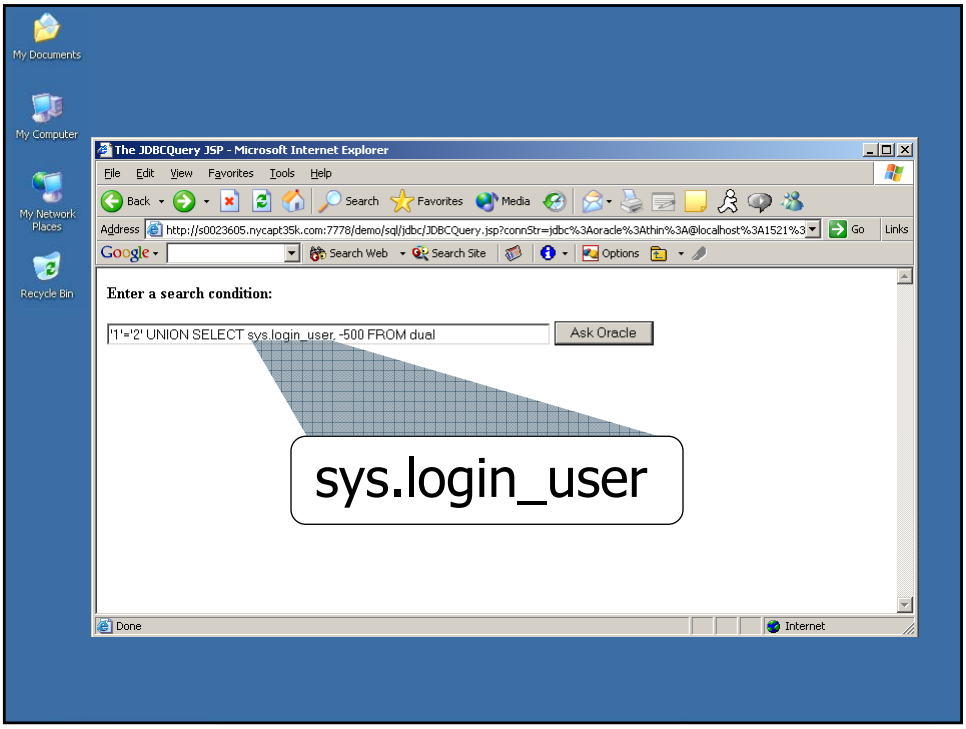
- Attack Target: All Versions of Oracle
- Privilege Level: Anyone with Internet Access
- Scenario:
  - Illustration of an Attacker using SQL Injection to run commands on a database via a vulnerable web application
- Vulnerabilities Exploited:
  - SQL Injection
  - Denial of Services & Buffer Overflows
  - Misconfigurations & Resource Management Issues

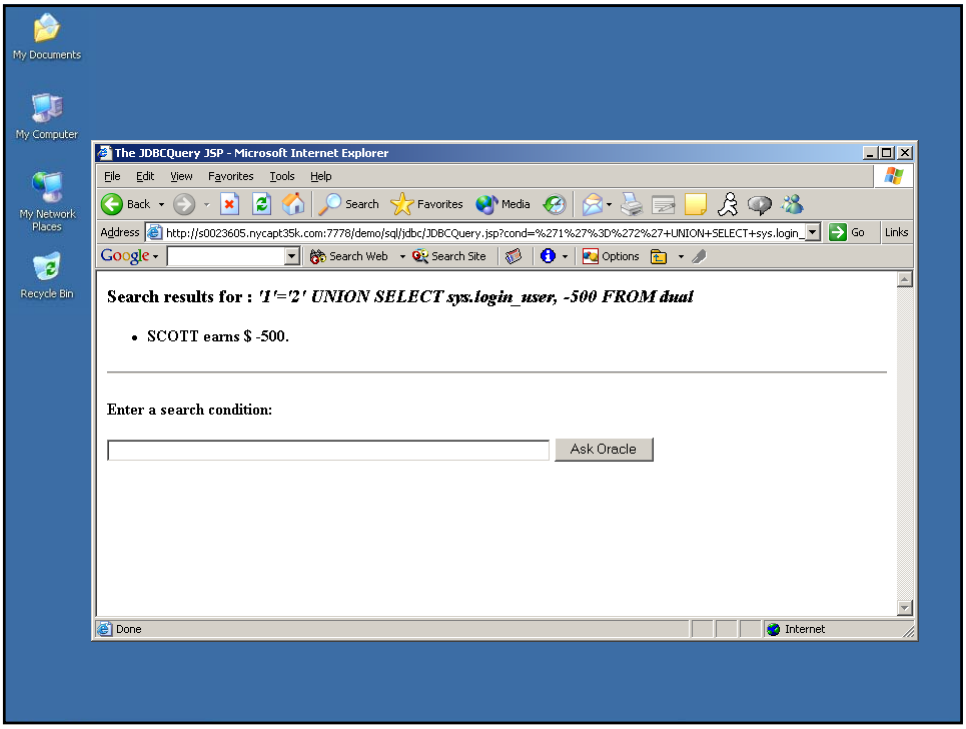

My Documents
My Computer
My Network Places
Recycle Bin
The JDBCQuery JSP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?connStr=jdbc%3Aoracle%3Athin%3A@localhost%3A1521%3
Go Links
Google Search Web Search Site Options
Enter a search condition:
Ask Oracle
Done
Internet

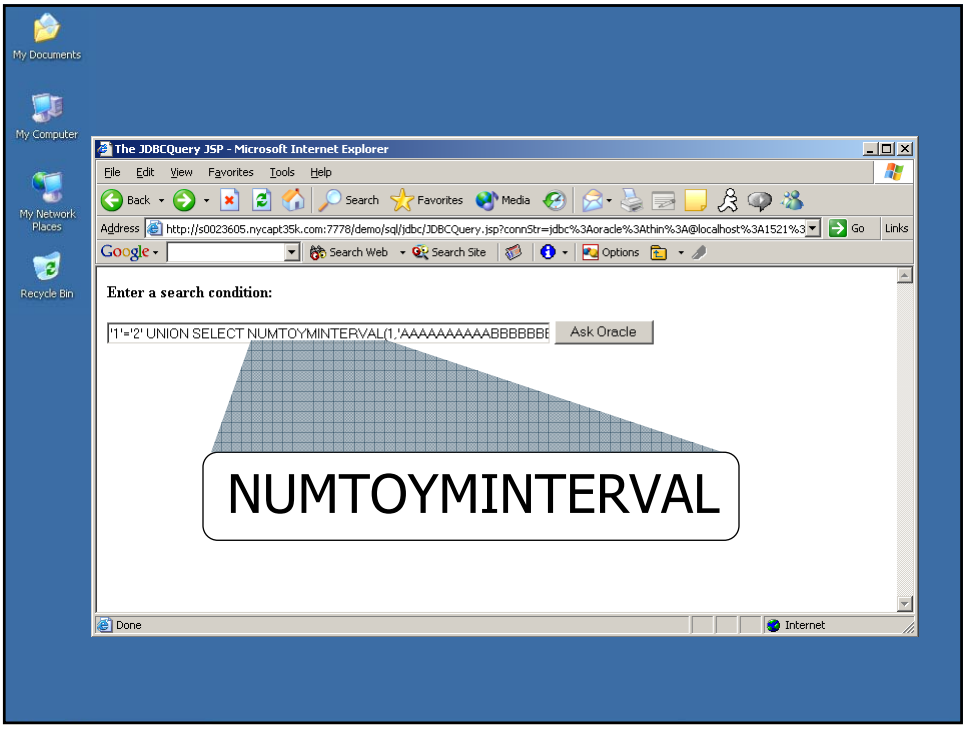

My Documents
My Computer
My Network Places
Recycle Bin
The JDBCQuery JSP
The JDBCQuery JSP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?connStr=jdbc%3Aoracle%3Athin%3A@localhost%3A1521%3
Go Links
Google Search Web Search Site Options
Enter a search condition:
Ask Oracle
7778/demo/sql/jdbc/JDBCQuery.jsp
Done
Internet

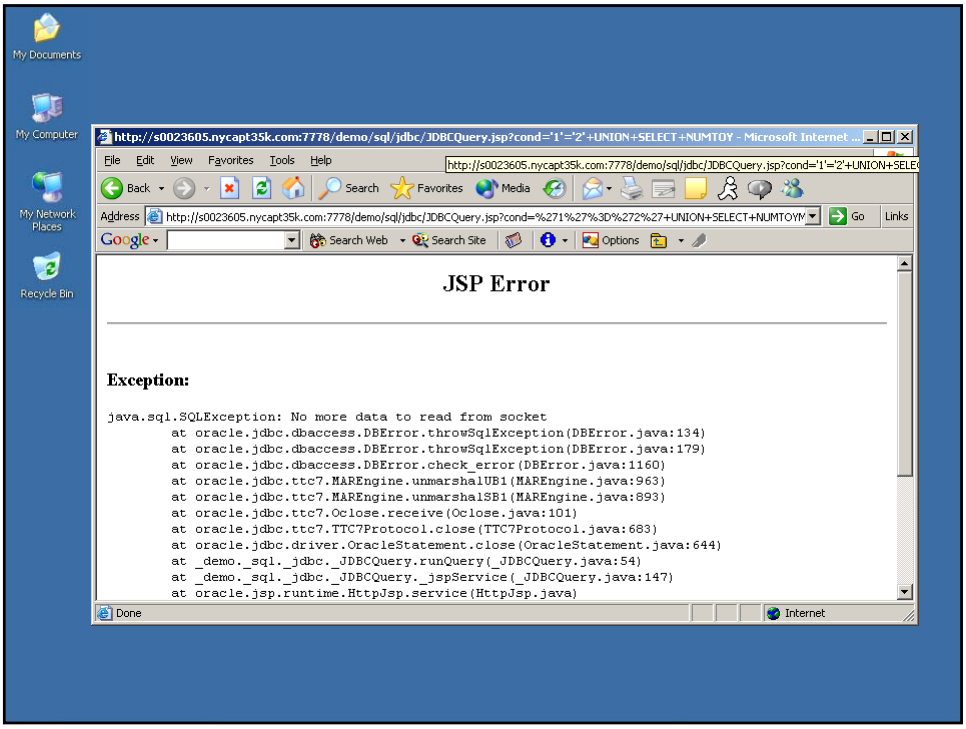

My Documents
My Computer
My Network Places
Recycle Bin
The JDBCQuery JSP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?connStr=jdbc%3Aoracle%3Athin%3A@localhost%3A1521%3
Go Links
Google Search Web Search Site Options
Enter a search condition:
'1'='2' UNION SELECT sys.database_name, -500 FROM dual
Ask Oracle
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 Search Favorites Media
Address http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?cond=%271%27%3D%272%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:
Ask Oracle
Done
Internet


My Documents
My Computer
My Network Places
Recycle Bin
The JDBCQuery JSP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
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:
'1'='2' UNION SELECT sys.login_user, -500 FROM dual
Ask Oracle
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 Search Favorites Media
Address http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?cond=%271%27%3D%272%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:
Ask Oracle
Done
Internet


My Documents
My Computer
My Network Places
Recycle Bin
The JDBCQuery JSP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
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:
'1'='2' UNION SELECT NUMTOYMINTERVAL(1,'AAAAAAAAAABBBBBBB
Ask Oracle
NUMTOYMINTERVAL
Done
Internet


My Documents
My Computer
My Network Places
Recycle Bin
http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?cond='1'='2'+UNION+SELECT+NUMTOY - Microsoft Internet ...
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://s0023605.nycapt35k.com:7778/demo/sql/jdbc/JDBCQuery.jsp?cond=%271%27%3D%272%27+UNION+SELECT+NUMTOYM
Go Links
Google Search Web Search Site Options
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.Oclose.receive(Oclose.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

APPLICATION SECURITY, INC.

Proactively Combating Database Attacks

Preventing the Password Attack

Database Vulnerability Assessment (DVA)

- Find and Change Default Passwords
  - Remove SCOTT/TIGER
- Implement Password Controls
  - Account Lockout
  - Minimum Password Length
  - Password Expiration
  - Password Complexity

Database Activity Monitoring (DAM)

- Monitor Database Login Attempts
  - Log all failed and successful logins
  - Alerts on repeated failed logins

Preventing the Privilege Escalation Attack

Database Vulnerability Assessment (DVA)

- Identify Missing Security Patches
  - Apply the latest:
    - CPU
    - PatchSet
    - ServicePack
    - HotFix

Database Activity Monitoring (DAM)

- Monitor Attempts to Exploit Known Vulnerabilities
  - Real Time Alerts on Privilege Escalation Attempts

Addressing Database Vulnerabilities

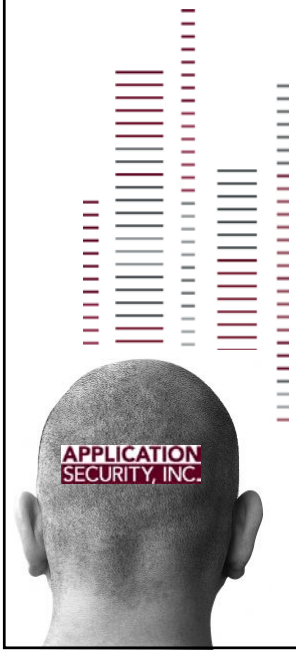
- Start with a Secure Configuration
- Stay Patched
  - Stay on top of all the security alerts and bulletins
- Defense in Depth / Multiple Levels of Security
  - Regularly scan your databases for vulnerabilities
    - Fix the problems reported!
  - Regularly run user entitlement reviews
    - Revoke access not needed for business!
  - Implement database activity monitoring…
  - …and database intrusion detection
    - Especially if you can't stay patched!
  - Encryption of data-in-motion / data-at-rest

Best Practices by Database Vendors & Notable Third Parties

- Oracle
  - Oracle9i Security Checklist
    otn.oracle.com/deploy/security/oracle9i/index.html
  - Oracle Project Lockdown
    www.oracle.com/technology/pub/articles/project_lockdown/index.html
  - Oracle Security Checklist
    www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf
- SANS Institute (SysAdmin, Audit, Network, Security)
  - Oracle Database Checklist
    www.sans.org/score/checklists/Oracle_Database_Checklist.doc
- Microsoft
  - 10 Steps to Secure SQL Server
    www.microsoft.com/sql/techinfo/administration/2000/security/securingsqlserver.asp
- SQLSecurity.com
  - SQLSecurity Checklist
    www.SQLSecurity.com

Database Security Info from AppSecInc

- White Papers
  - http://www.appsecinc.com/techdocs/whitepapers/research.shtml
    - Database Activity Monitoring
    - Search Engines Used to Attack Databases
    - Introduction to Database and Application Worms
    - Hunting Flaws in Microsoft SQL Server
- Presentations
  - http://www.appsecinc.com/techdocs/presentations.shtml
    - Protecting Databases
    - Hack-Proofing MySQL, IBM DB2, Oracle9iAS
    - Writing Secure Code in Oracle
- Security Alerts
  - www.appsecinc.com/resources/mailinglist.html



APPLICATION SECURITY, INC.

Thank you!

Questions?

Application Security, Inc.
1-866-9APPSEC (1-866-927-7732)
asktheexpert@appsecinc.com