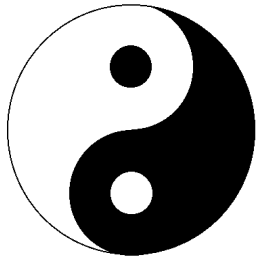


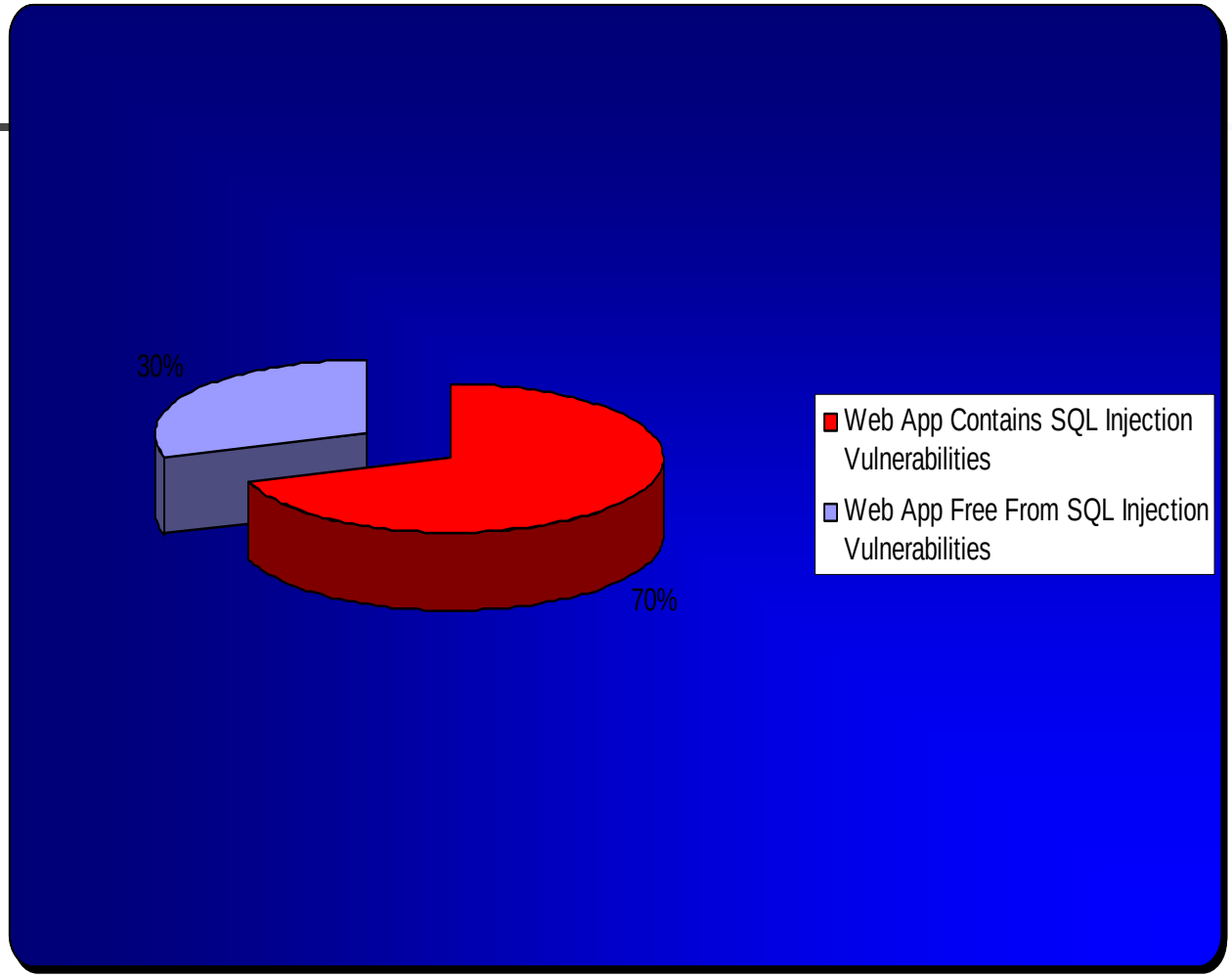
Improved Penetration Testing of Web Apps and Databases with MatriXay

Yuan Fan GCIH,GCIA,CISSP Frank@dbappsecurity.com

Xiao Rong CISSP,ITIL netxeyes@dbappsecurity.com

© Copyright 2005-2006 www.DBAppSecurity.com

Background



Disclaimer: Approximate percentages based on transitory marketing information. Actual data may vary.

© Copyright 2005-2006 www.DBAppSecurity.com

What is The Presentation About

- It is a pen-test tool (sure with GUI ☺) first time revealed (and most time you only need a mouse to pen-test).

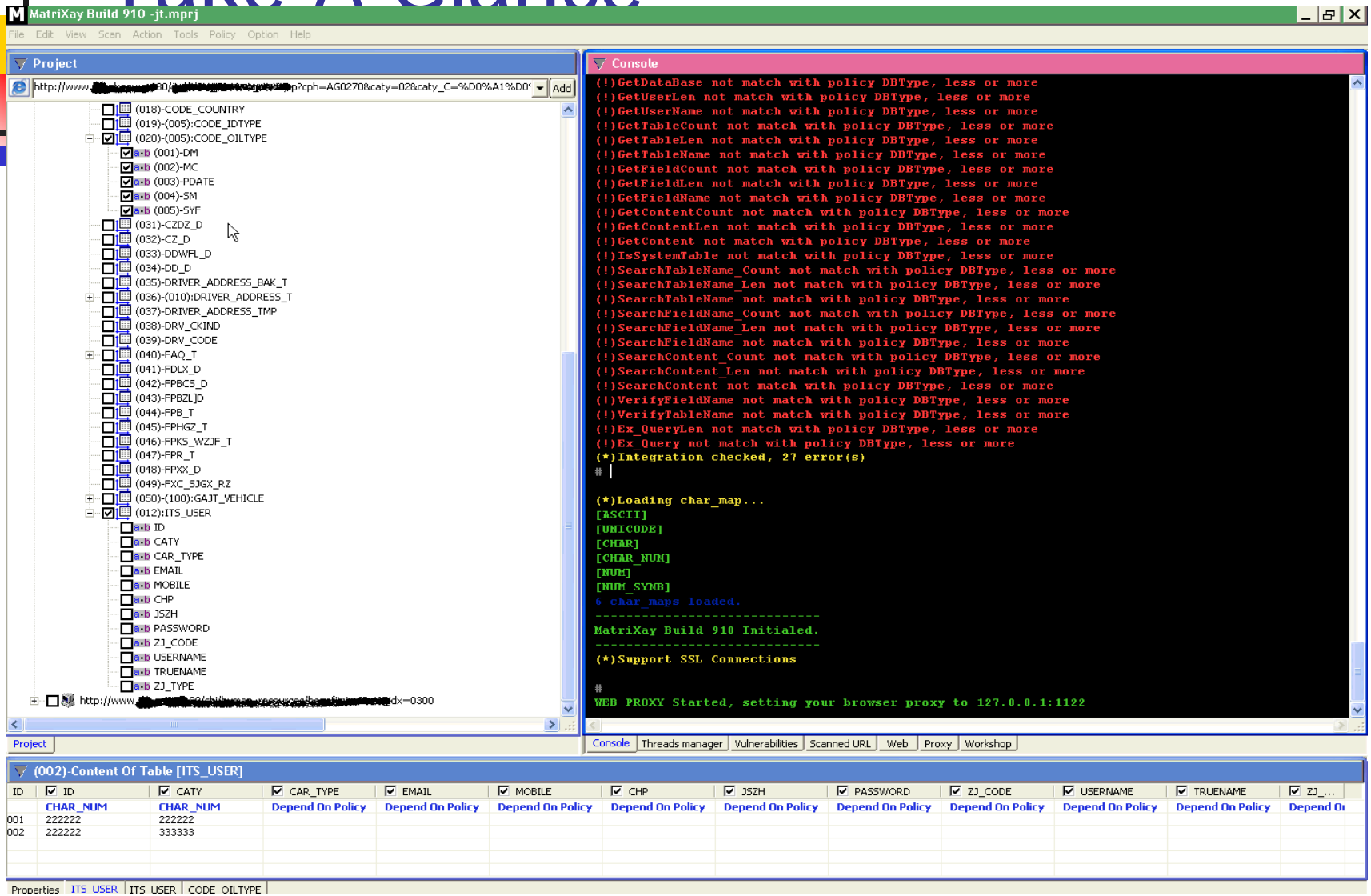
  Free Beta release for testing in same week (the week of July 31, 2006).

- Not so blind SQL Injection tool

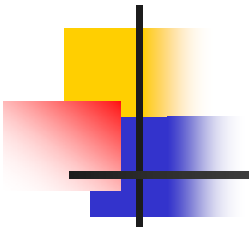
- An automated/powerful Web App SQL injector and backend DB pen-tester

© Copyright 2005-2006 www.DBAppSecurity.com

Take A Glance



© Copyright 2005-2006 www.DBAppSecurity.com



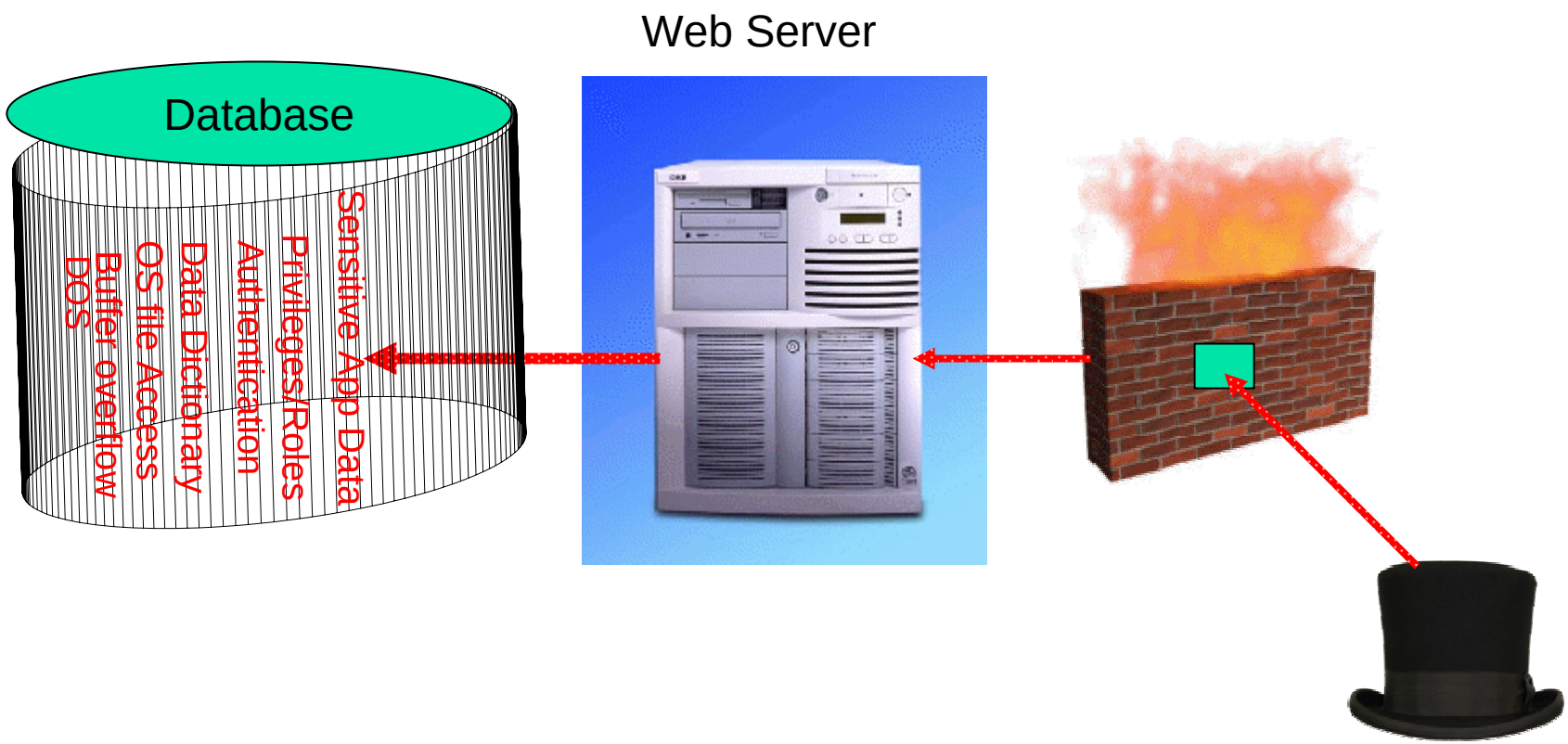
In Short

- A systematic/automatic way to inject Webapp and then audit backend DB
- Cross Database support (Current support Oracle, SQL Server, DB2, and Access. More than 20 websites have been Pen-Tested using this tool with permission)

© Copyright 2005-2006 www.DBAppSecurity.com

Yeah, we know you had a firewall

- But see following, not to mention insiders



© Copyright 2005-2006 www.DBAppSecurity.com

Essential Fact/Theory Based

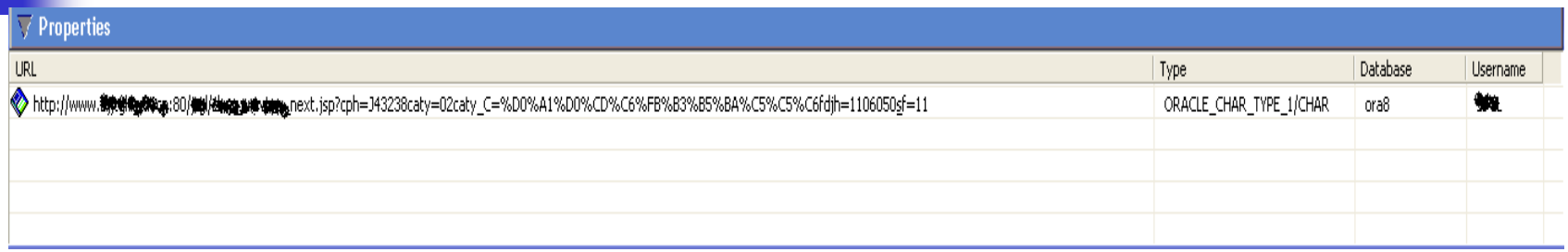
- Perimeter defense usually do too little to help with web/database security
- Databases are all different, but has things in common such as data dictionary
- Database has to maintain lots of information such as from session to performance data and even user credential
- Harden a Database (fully) is not so easy

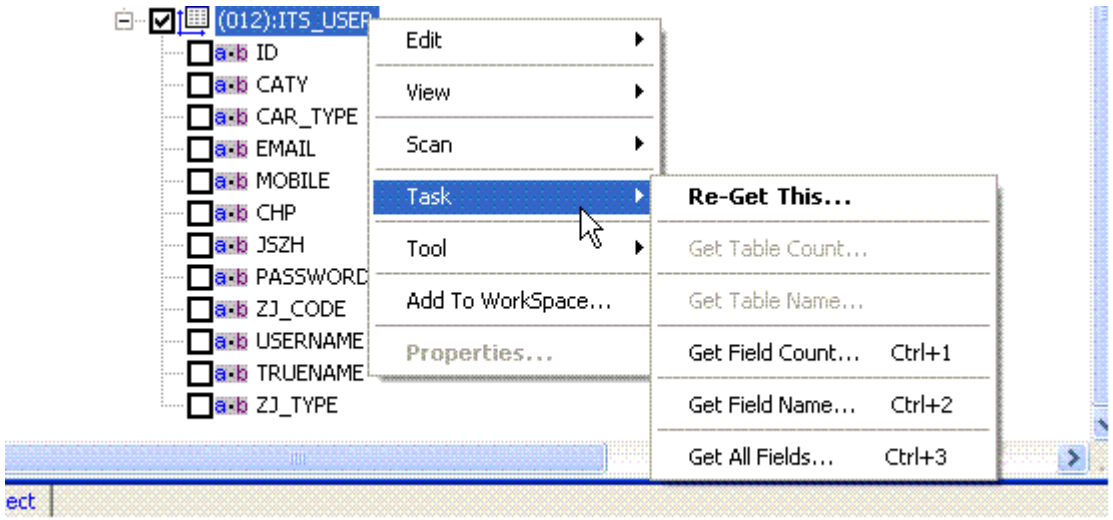
© Copyright 2005-2006 www.DBAppSecurity.com

Popular Database in Common

Data Dictionary	Oracle	SQL Server	DB2
Versions, Tables, Columns, Users	V$version User_tables, cols, All_users,dba_users, sys.user$...	@@version Information_schema.Tables, Information_schema.columns, sysobjects	Sysproc.env_get_inst_info(), SYSCAT.TABLES, SYSCAT.columns, ... SQLCA
Default user/password	sys/change_on_install, system/manager, dbsnmp/dbsnmp ...	sa/<blank>	db2admin/db2admin db2inst1/ibmdb2

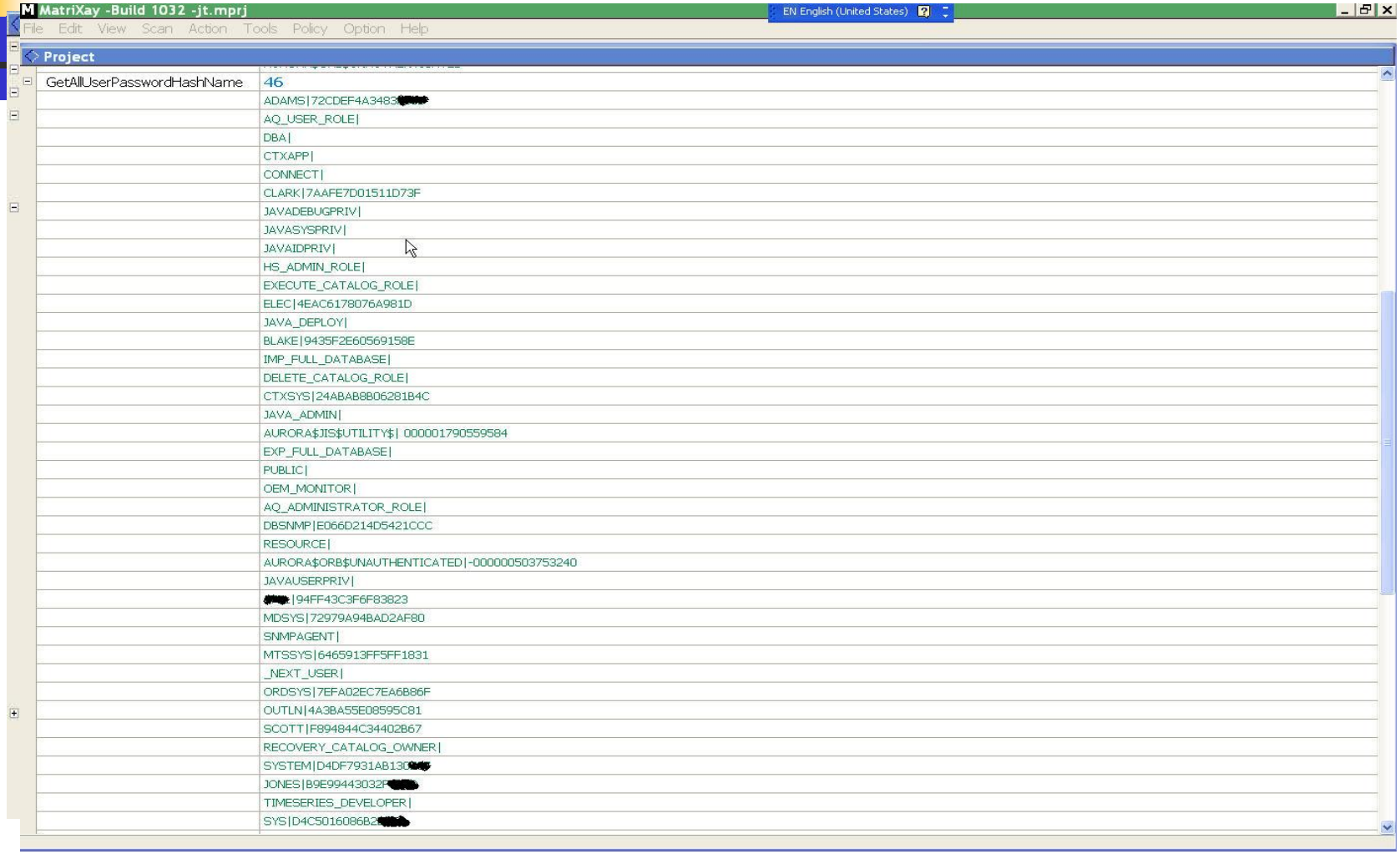
Snap Shots





© Copyright 2005-2006 www.DBAppSecurity.com

Auditing



© Copyright 2005-2006 www.DBAppSecurity.com

Special Spots for Databases

Spots	Oracle	SQL Server	DB2
Password management	Weak password hash algorithm exposed years ago and still did not change. No Salt!	Stored In Sysxlogins, Pwdencrypt()	Os level, SYSADM_GRP, SYSCTRL_GRP
Ports	1521 widely open unless you edit the sqlnet.ora to lock the IP connects in.	1433 TCP 1434 UDP	50000
"Evil" procedure	DBMS_SCHEDULER, UTL_HTTP, UTL_TCP UTL_SMTP,	Sp_OACreate Xp_cmdshell, Xp_regread, Xp_regwrite, Xp_logininfo, Xp_grantlogin Xp_xxxxx	>Create table Load from file. >Easy to create precedure to exec os cmd

© Copyright 2005-2006 www.DBAppSecurity.com

Roles&Privilege Auditing

Oracle	SQL Server	DB2
session_privs System_privilege_map All_tab_privs_made User_tab_privs_made	**IS_MEMBER** **IS_SRVROLEMEMBER**	SYSCAT.PASSTHRUAuth SYSCAT.SCHEMAAuth SYSCAT.DBAuth SYSCAT.TabAuth SYSCAT.COLAuth

© Copyright 2005-2006 www.DBAppSecurity.com

quence – Follow the stream

1. Detect whether it is SQL “Injectable”

2. Send 10+ different requests to determine what database type is in backend

3. Get Current Database properties

4. Get basically whole database dictionary

5. Start advance injection/audit

© Copyright 2005-2006 www.DBAppSecurity.com

Search Specific Spot

- Search specific table name or field name

  For example %passw% %user%

- Search for any unrelated but sensitive content through the vulnerable URL

© Copyright 2005-2006 www.DBAppSecurity.com

General features overview Cont'd – Authentication

- Get current user privileges
- Default password check.
- Get system user table/view (sys.user$ or dba_users in Oracle), then crack password hash locally.

Note for Oracle: sys/system/dbsnmp's password hash can be pre-generated so it is "rainbow-like" fast crack.

© Copyright 2005-2006 www.DBAppSecurity.com

Authentication Cont'd – Huge Leak in Oracle 10g

- You can get oracle default user - dbsnmp's clear password through a query. (Oh, my…)
- More importantly, with default Oracle 10g installation, SYS, System and dbsnmp share same password !!

© Copyright 2005-2006 www.DBAppSecurity.com

Database Configuration Auditing

Oracle	▪ Init Parameters 07_DICTIONARY_ACCESSIBILITY, Audit_trail, Audit_sys_operations,Remote_os_authentication, UTL_FILE_DIR etc. ▪ Database link password ▪ Patch info
SQL Server	▪ Allow_updates, Remote Access etc ▪ Audit_mode(C2, normal, none) ▪ Sp_trace_create file output ▪ All extended procedures ▪ Patch info
DB2	▪ Catalog_noauth, Datalinks, Trust_allclnts etc ▪ Audit info ▪ Patch info

© Copyright 2005-2006 www.DBAppSecurity.com

General features overview Cont'd – Configuration Auditing

- [START]

- Task[0].name=getSQL92Para
- Task[0].description=Check SQL92_SECURITY parameter
- Task[0].resultType=Integer
- [RESULT]
- [0]
- Task[0].severity=medium
- Task[0].msg=Parameter SQL92_SECURITY is set to FALSE. This feature disables the SQL92 security.
- [/0]

- [1]
- Task[0].severity=none
- Task[0].msg=Parameter SQL92_SECURITY is set to true. This feature enable the SQL92 security.
- [/1]

- [every_result_else]
- Task[0].msg=this is impossible
- [/every_result_else]
- [/RESULT]

- [/START]

© Copyright 2005-2006 www.DBAppSecurity.com

General features overview Cont'd – Raw SQL Auditing

The important thing besides real injection is pinpoint more places where potentially vulnerable (Currently support for Oracle only)

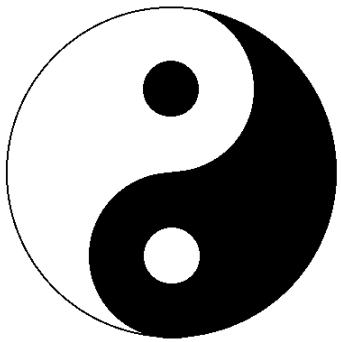
- Get the SQL being used in the current session by web user

  Now you got idea to know what is really going on in backend.

- Procedure source. (for example user_source in Oracle)

© Copyright 2005-2006 www.DBAppSecurity.com

General features overview Cont'd – 2 modes



- Ying Mode

  Passive listen and detection. It is Proxy mode.

- Yang Mode

  Direct targeting to web.

© Copyright 2005-2006 www.DBAppSecurity.com

General features overview Cont'd – Ying Mode

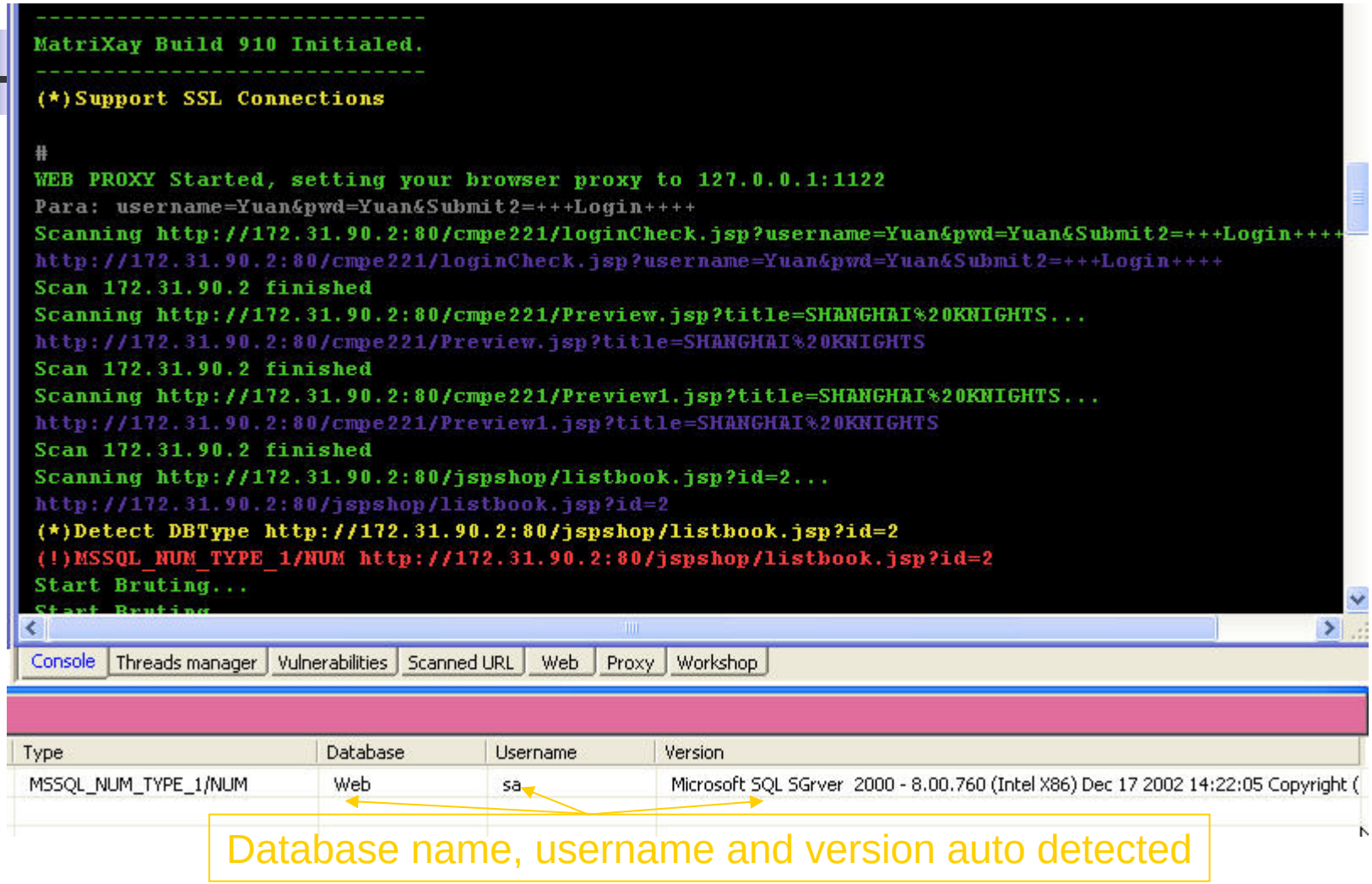
- Proxy mode

  As long as the browser point to the local proxy port which MatriXay starts.

  Automatically detect the vulnerable URL while you surfing internet – before you even notice (see next slide).

© Copyright 2005-2006 www.DBAppSecurity.com

Ying Mode Cont'd



© Copyright 2005-2006 www.DBAppSecurity.com

Yang Mode

- Direct scan mode, and Yes: Https supported
- Options to configure Get/Post, thread pool number etc.
- Options to configure the session
- Tools -> “get proxy list” to get a list of proxies from all over the world to hide your real IP Address.

© Copyright 2005-2006 www.DBAppSecurity.com

Advanced Feature overview - Privilege escalation

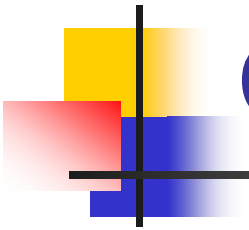
- How if we don't have enough privilege?
- Oracle 9i Examples:

```
SELECT
SYS.DBMS_METADATA.GET_DDL('"||theuser.EVI
L_FUNC()||'",") FROM dual;
```

- Oracle 10g Privilege Escalation

  DBMS_ADVISOR

© Copyright 2005-2006 www.DBAppSecurity.com



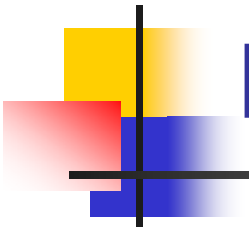
Oracle specific vulnerability check

- Oracle mod-plsql vulnerabilities

- www.xxx.xx/pls/portal/<<label>>SYS.OWA_UTIL.CELLSPRINT?P_THEQUERY=select+*+from+xxx

Works with all mod_plsql apps without the april 2006 patch!

© Copyright 2005-2006 www.DBAppSecurity.com



Pen-Test Plug-in Capability

- Often we found new vulnerabilities
- A configuration file with simple grammar
- Add new pen-test capability without the need to changes the code

© Copyright 2005-2006 www.DBAppSecurity.com

Similar tool in market comparison

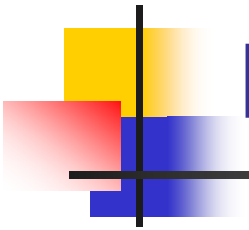
- Paros
- Absinthe
- SQL Injector from SpyDynamics
- Watchfire AppScan

© Copyright 2005-2006 www.DBAppSecurity.com

Evasion Techniques

- Instead of 1=1 or ‘1’=‘1 using dynamically generated values. Such as 2000=2000
- Make use of functions such as soundex (e.g. soundex(‘FAN’) = ‘F500’
- Random sleep range for multi threading to avoid detection as an automated attack tool.
- Distribute different http request through different free proxy so it looks more like normal traffic ☺

© Copyright 2005-2006 www.DBAppSecurity.com

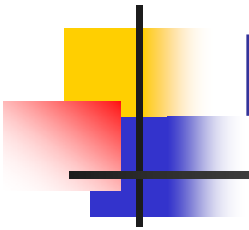


Defense Techniques At a Glance

- Default installation/configuration is very lame
- Dictionary protection
- Least privilege and make use of roles

  Most Latest example: “select privilege only user can modify data in oracle (unless you grant through roles), no patch yet.” [Ref#1]
- Pen-test and continues monitoring

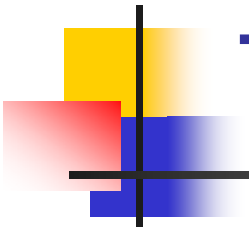
© Copyright 2005-2006 www.DBAppSecurity.com



Demo, Demo, Demo

- Nothing is better than Real Demo
- Future roadmap/enhancement overview

© Copyright 2005-2006 www.DBAppSecurity.com



Thanks for listening

- Have to mention my partner XiaoRong
- Special Thanks to Alexander Kornbrust for great comments
- Your feedback is most valuable to us, and we will incorporate into next release.

  Send comments/suggestions to info@dbappsecurity.com

© Copyright 2005-2006 www.DBAppSecurity.com

Reference

- www.dbappsecurity.com
  (Main website for MatriXay release and Status update)
- www.red-database-security.com
- www.petefinnigan.com
- www.ngssoftware.com
- www.oracle.com/technology/deploy/security
- www.securityfocus.com
- www.sqlsecurity.com
- www.owasp.org

© Copyright 2005-2006 www.DBAppSecurity.com