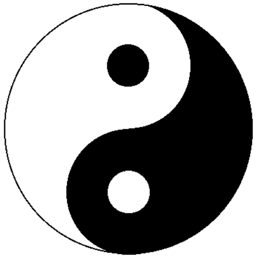
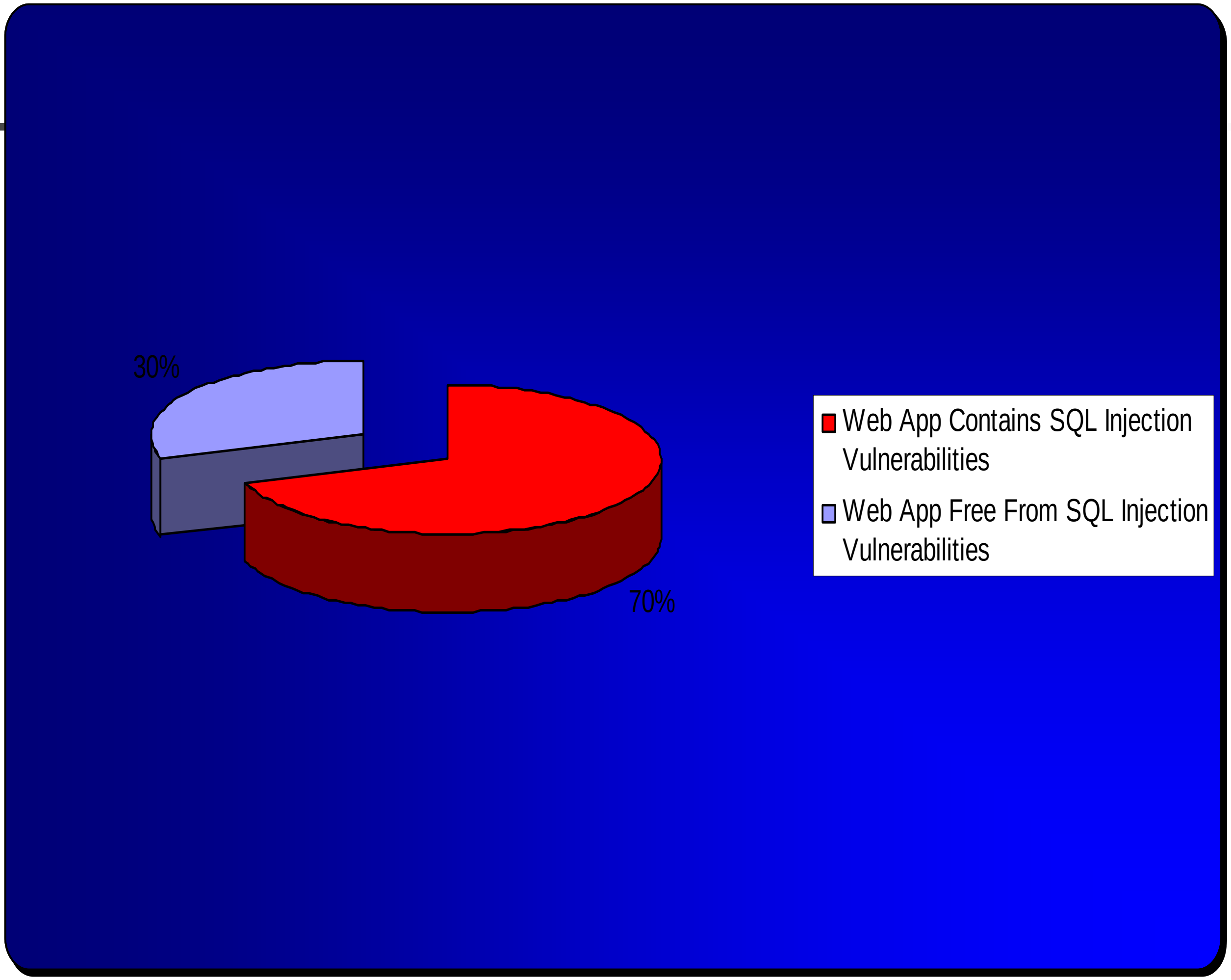


Improved Penetration Testing of Web Apps and Databases with MatriXay

Yuan Fan GCIH,GCIA,CISSP Frank@dbappsecurity.com
Xiao Rong CISSP,ITIL netxeyes@dbappsecurity.com

Background



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

What is The Presentation About

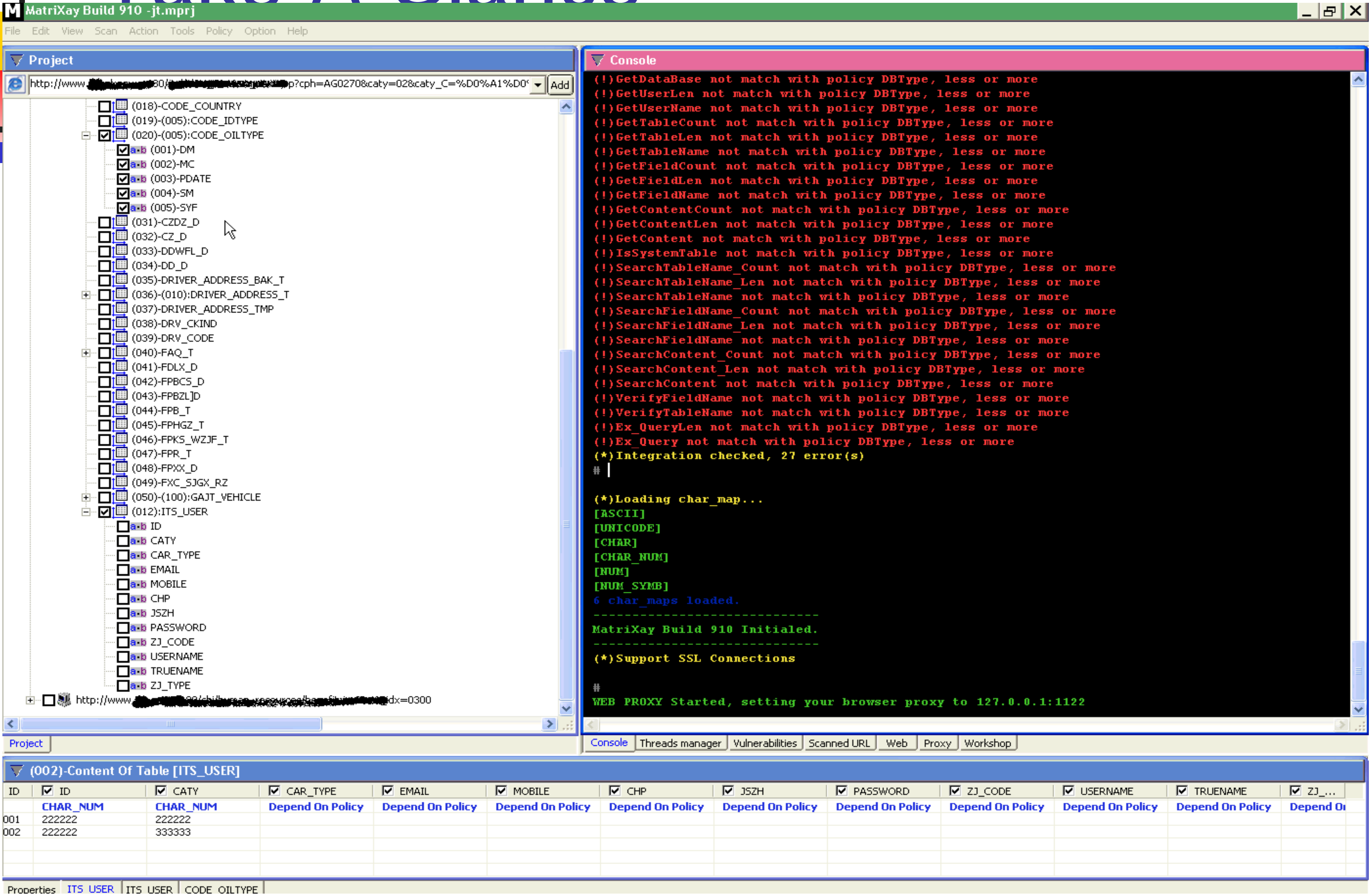
- It is a pen-test tool (sure with GUI ☺) first time revealed (and most time you only need a mouse to pen-test).

  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

Take A Glance


MatriXay Build 910 -jt.mprj
File Edit View Scan Action Tools Policy Option Help
Project
Add
Console

http://www.[redacted]30/[redacted]p?cph=AG0270&caty=02&caty_C=%D0%A1%D0'

- ☐ (018)-CODE_COUNTRY
- ☐ (019)-(005):CODE_IDTYPE
- ☑ (020)-(005):CODE_OILTYPE
  - ☑ a·b (001)-DM
  - ☑ a·b (002)-MC
  - ☑ a·b (003)-PDATE
  - ☑ a·b (004)-SM
  - ☑ a·b (005)-SYF
- ☐ (031)-CZDZ_D
- ☐ (032)-CZ_D
- ☐ (033)-DDWFL_D
- ☐ (034)-DD_D
- ☐ (035)-DRIVER_ADDRESS_BAK_T
- ☐ (036)-(010):DRIVER_ADDRESS_T
- ☐ (037)-DRIVER_ADDRESS_TMP
- ☐ (038)-DRV_CKIND
- ☐ (039)-DRV_CODE
- ☐ (040)-FAQ_T
- ☐ (041)-FDLX_D
- ☐ (042)-FPBCS_D
- ☐ (043)-FPBZLJD
- ☐ (044)-FPB_T
- ☐ (045)-FPHGZ_T
- ☐ (046)-FPKS_WZJF_T
- ☐ (047)-FPR_T
- ☐ (048)-FPXX_D
- ☐ (049)-FXC_SJGX_RZ
- ☐ (050)-(100):GAJT_VEHICLE
- ☑ (012):ITS_USER
  - ☐ a·b ID
  - ☐ a·b CATY
  - ☐ a·b CAR_TYPE
  - ☐ a·b EMAIL
  - ☐ a·b MOBILE
  - ☐ a·b CHP
  - ☐ a·b JSZH
  - ☐ a·b PASSWORD
  - ☐ a·b ZJ_CODE
  - ☐ a·b USERNAME
  - ☐ a·b TRUENAME
  - ☐ a·b ZJ_TYPE
- ☐ http://www.[redacted]dx=0300

```
(!)GetDataBase not match with policy DBType, less or more
(!)GetUserLen not match with policy DBType, less or more
(!)GetUserName not match with policy DBType, less or more
(!)GetTableCount not match with policy DBType, less or more
(!)GetTableLen not match with policy DBType, less or more
(!)GetTableName not match with policy DBType, less or more
(!)GetFieldCount not match with policy DBType, less or more
(!)GetFieldLen not match with policy DBType, less or more
(!)GetFieldName not match with policy DBType, less or more
(!)GetContentCount not match with policy DBType, less or more
(!)GetContentLen not match with policy DBType, less or more
(!)GetContent not match with policy DBType, less or more
(!)IsSystemTable not match with policy DBType, less or more
(!)SearchTableName_Count not match with policy DBType, less or more
(!)SearchTableName_Len not match with policy DBType, less or more
(!)SearchTableName not match with policy DBType, less or more
(!)SearchFieldName_Count not match with policy DBType, less or more
(!)SearchFieldName_Len not match with policy DBType, less or more
(!)SearchFieldName not match with policy DBType, less or more
(!)SearchContent_Count not match with policy DBType, less or more
(!)SearchContent_Len not match with policy DBType, less or more
(!)SearchContent not match with policy DBType, less or more
(!)VerifyFieldName not match with policy DBType, less or more
(!)VerifyTableName not match with policy DBType, less or more
(!)Ex_QueryLen not match with policy DBType, less or more
(!)Ex_Query not match with policy DBType, less or more
(*)Integration checked, 27 error(s)
#

(*)Loading char_map...
[ASCII]
[UNICODE]
[CHAR]
[CHAR_NUM]
[NUM]
[NUM_SYMB]
6 char_maps loaded.
-----------------------------
MatriXay Build 910 Initialed.
-----------------------------
(*)Support SSL Connections

#
WEB PROXY Started, setting your browser proxy to 127.0.0.1:1122
```

Project
Console | Threads manager | Vulnerabilities | Scanned URL | Web | Proxy | Workshop

(002)-Content Of Table [ITS_USER]

ID	☑ ID	☑ CATY	☑ CAR_TYPE	☑ EMAIL	☑ MOBILE	☑ CHP	☑ JSZH	☑ PASSWORD	☑ ZJ_CODE	☑ USERNAME	☑ TRUENAME	☑ ZJ_...
	CHAR_NUM	CHAR_NUM	Depend On Policy	Depend On Policy	Depend On Policy	Depend On Policy	Depend On Policy	Depend On Policy	Depend On Policy	Depend On Policy	Depend On Policy	Depend Oı
001	222222	222222										
002	222222	333333										

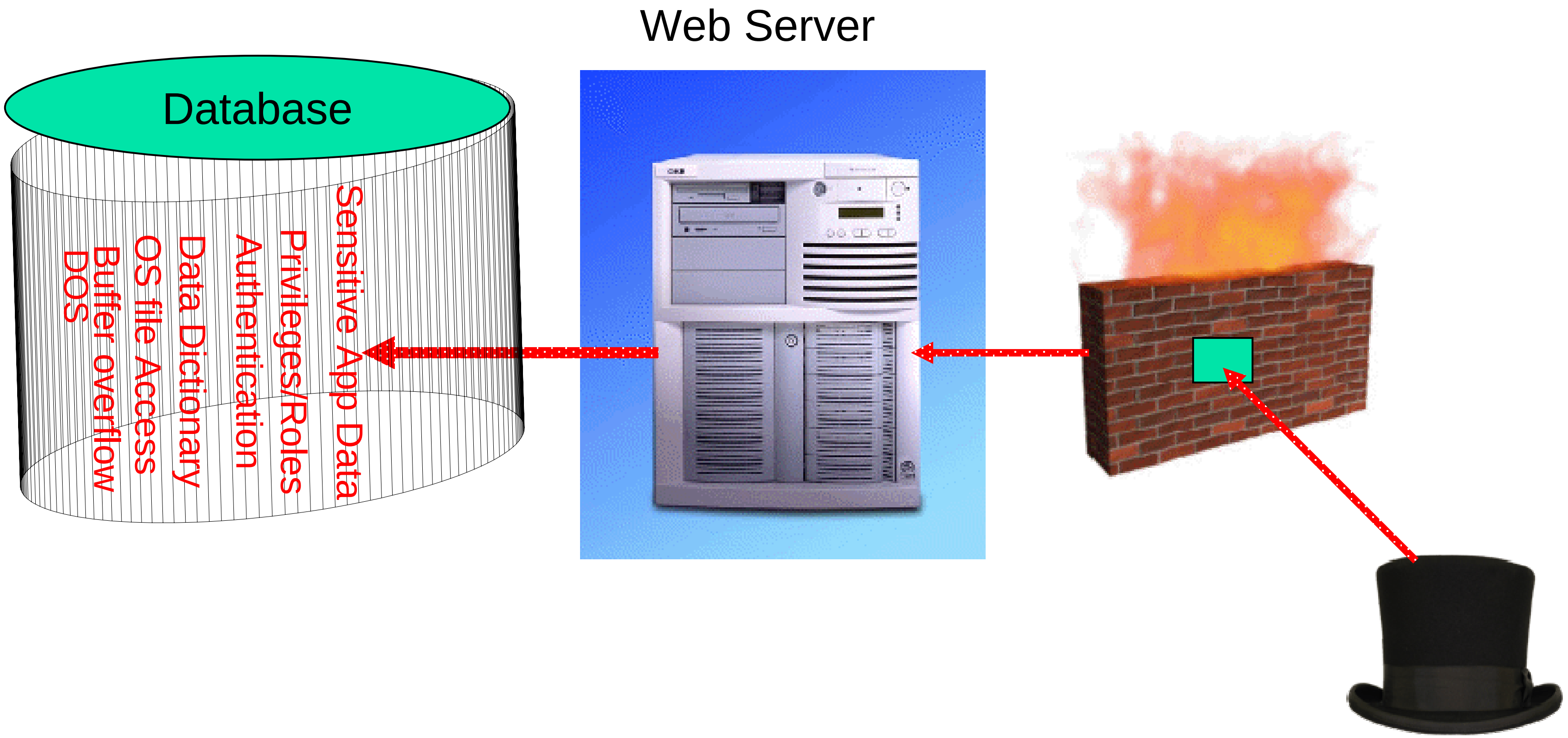
In Short

- 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)

Yeah, we know you had a firewall

But see following, not to mention insiders



Web Server

Database

Sensitive App Data
Privileges/Roles
Authentication
Data Dictionary
OS file Access
Buffer overflow
DOS

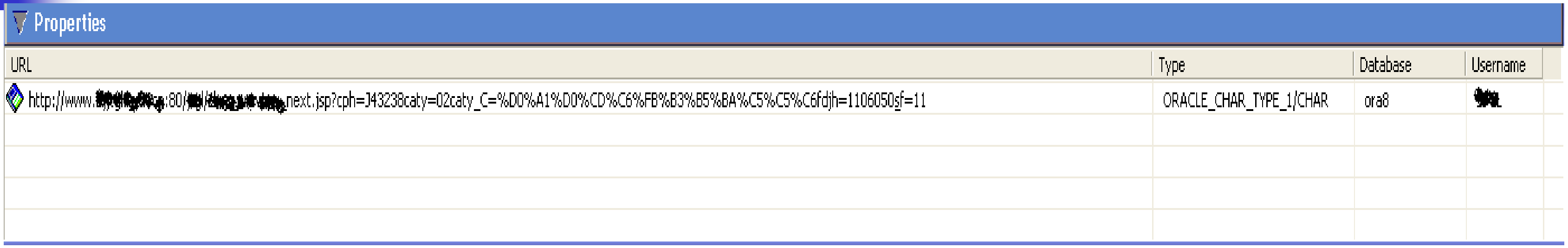
Essential Fact/Theory Based

- 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

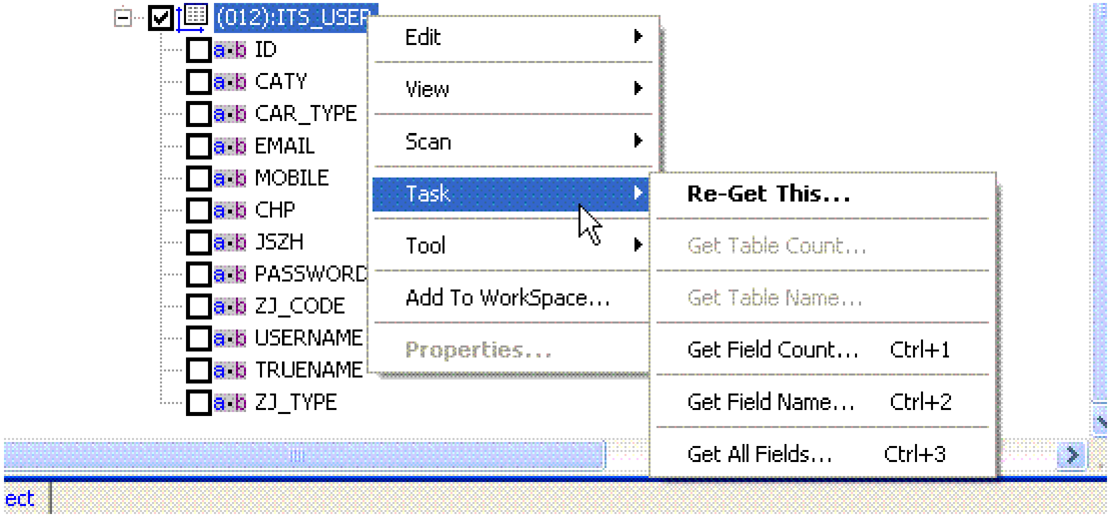
Popular Database in Common

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

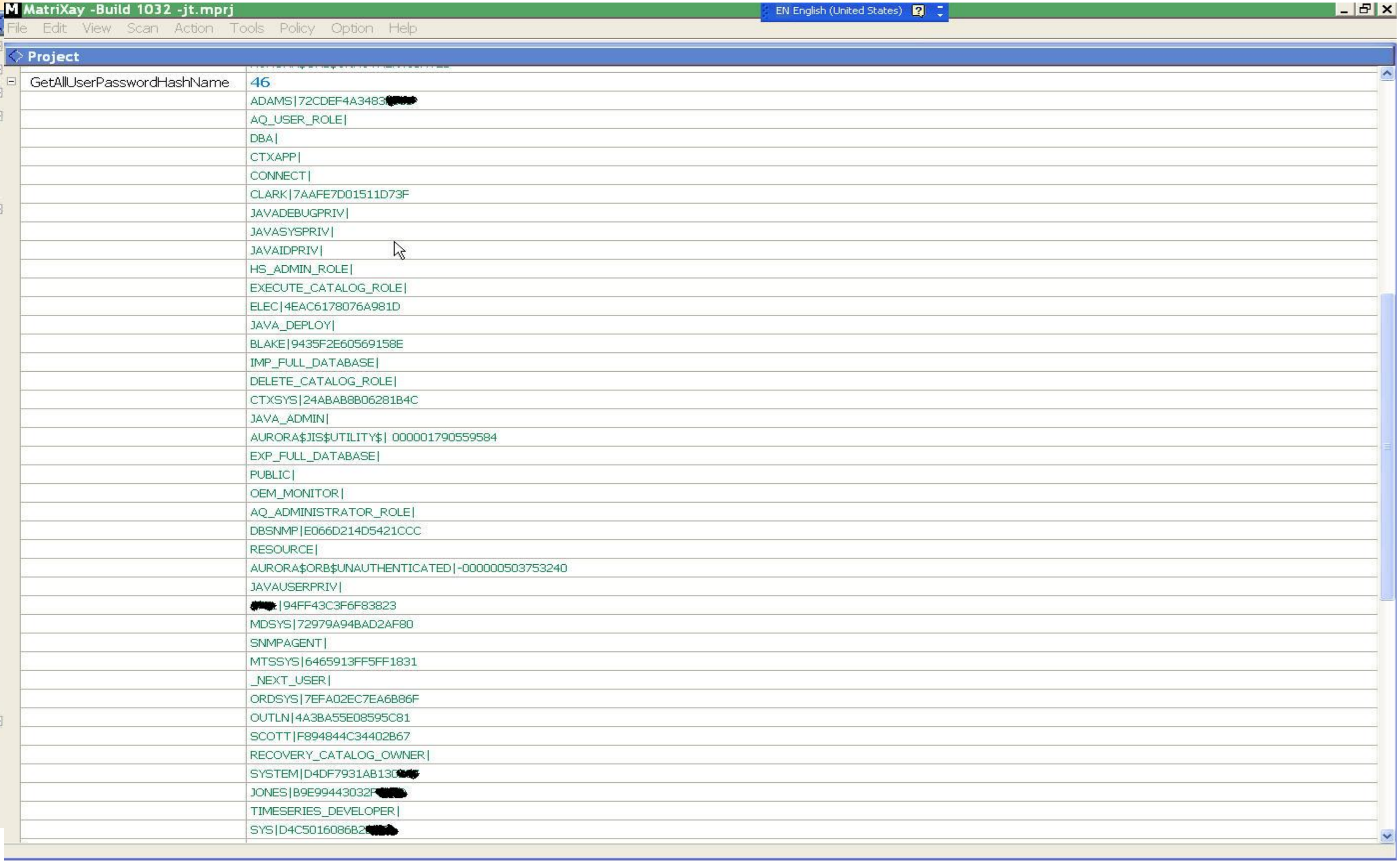
Snap Shots



URL	Type	Database	Username
http://www.[redacted]:80/[redacted]/[redacted]next.jsp?cph=J43238caty=02caty_C=%D0%A1%D0%CD%C6%FB%B3%B5%BA%C5%C5%C6fdjh=1106050sf=11	ORACLE_CHAR_TYPE_1/CHAR	ora8	[redacted]



Auditing



```
GetAllUserPasswordHashName   46
                             ADAMS|72CDEF4A3483[redacted]
                             AQ_USER_ROLE|
                             DBA|
                             CTXAPP|
                             CONNECT|
                             CLARK|7AAFE7D01511D73F
                             JAVADEBUGPRIV|
                             JAVASYSPRIV|
                             JAVAIDPRIV|
                             HS_ADMIN_ROLE|
                             EXECUTE_CATALOG_ROLE|
                             ELEC|4EAC6178076A981D
                             JAVA_DEPLOY|
                             BLAKE|9435F2E60569158E
                             IMP_FULL_DATABASE|
                             DELETE_CATALOG_ROLE|
                             CTXSYS|24ABAB8B06281B4C
                             JAVA_ADMIN|
                             AURORA$JIS$UTILITY$| 000001790559584
                             EXP_FULL_DATABASE|
                             PUBLIC|
                             OEM_MONITOR|
                             AQ_ADMINISTRATOR_ROLE|
                             DBSNMP|E066D214D5421CCC
                             RESOURCE|
                             AURORA$ORB$UNAUTHENTICATED|-000000503753240
                             JAVAUSERPRIV|
                             [redacted]|94FF43C3F6F83823
                             MDSYS|72979A94BAD2AF80
                             SNMPAGENT|
                             MTSSYS|6465913FF5FF1831
                             _NEXT_USER|
                             ORDSYS|7EFA02EC7EA6B86F
                             OUTLN|4A3BA55E08595C81
                             SCOTT|F894844C34402B67
                             RECOVERY_CATALOG_OWNER|
                             SYSTEM|D4DF7931AB130[redacted]
                             JONES|B9E99443032F[redacted]
                             TIMESERIES_DEVELOPER|
                             SYS|D4C5016086B2[redacted]
```

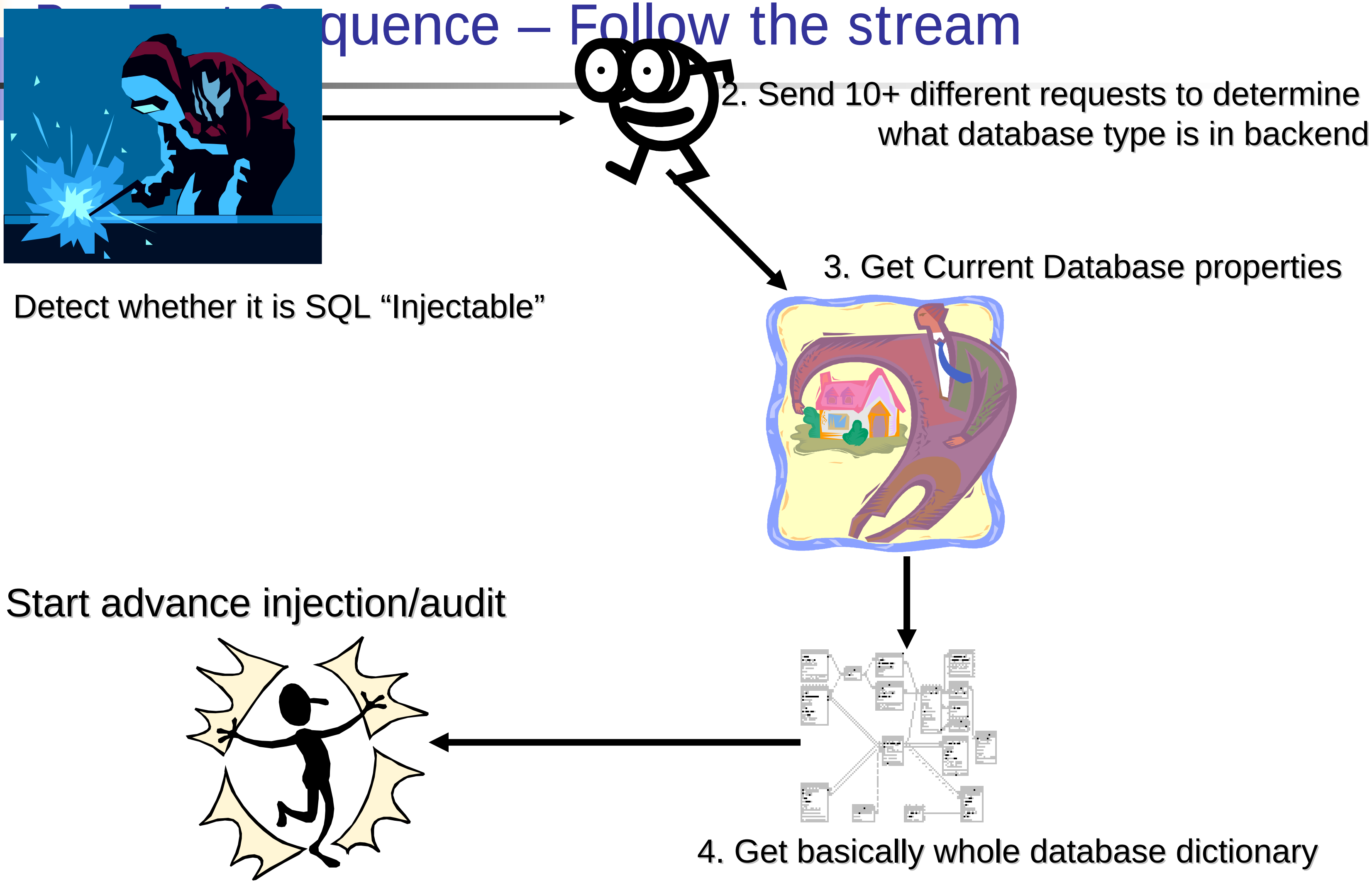
Special Spots for Databases

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

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

Pen Test Sequence – 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

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

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.

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 !!

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

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]
```

General features overview Cont'd – Raw SQL Auditing

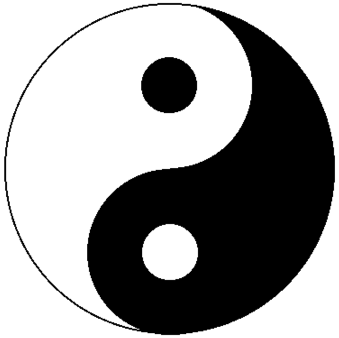
The important thing besides real injection is pinpoint more places where potentially vulnerable (Currently support for Oracle only)

- 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)

General features overview Cont'd – 2 modes



- Ying Mode

  Passive listen and detection. It is Proxy mode.

- Yang Mode

  Direct targeting to web.

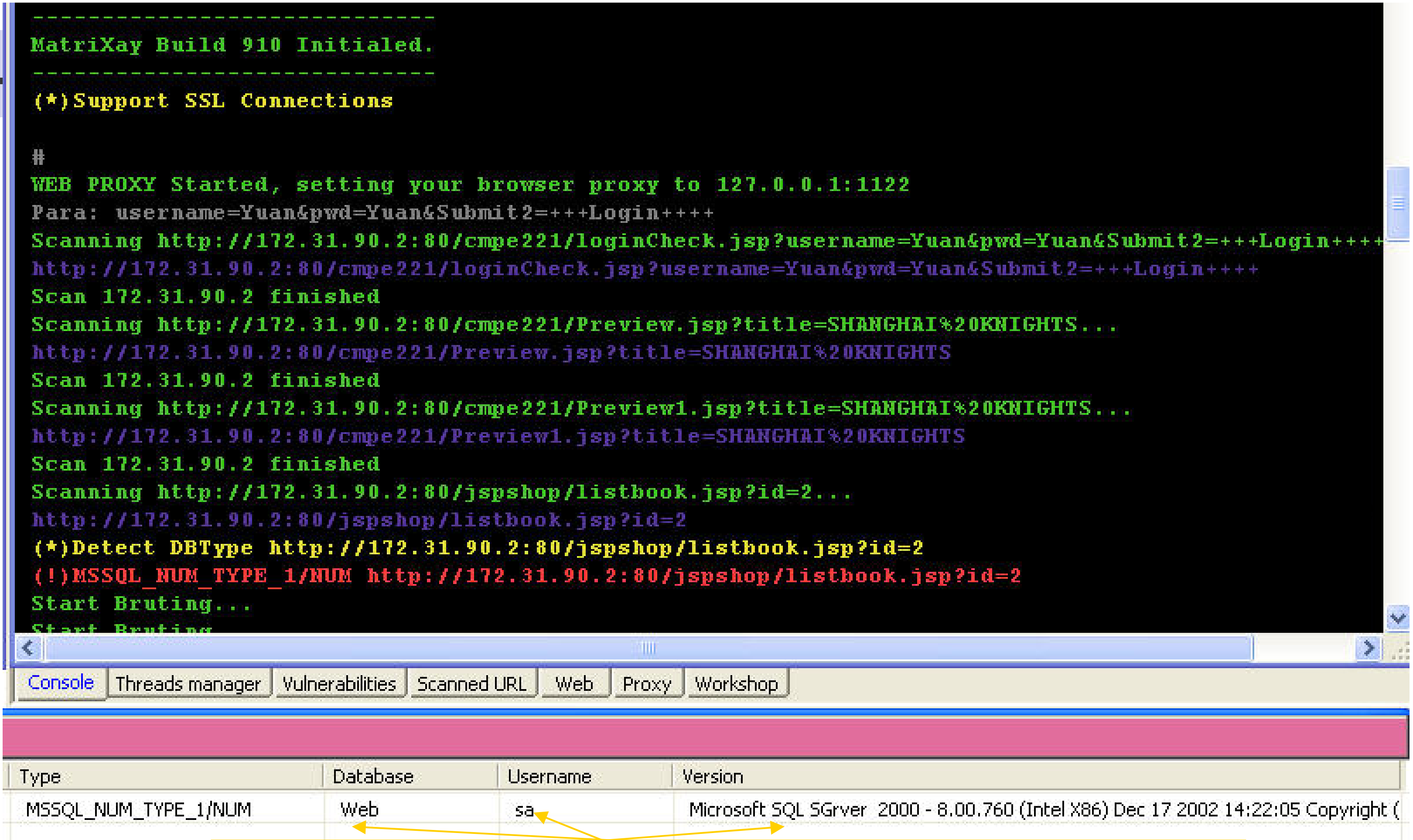
General features overview Cont’d – Ying Mode

- 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).

Ying Mode Cont’d



```
--------------------------------
MatriXay Build 910 Initialed.
--------------------------------
(*)Support SSL Connections

#
WEB PROXY Started, setting your browser proxy to 127.0.0.1:1122
Para: username=Yuan&pwd=Yuan&Submit2=+++Login++++
Scanning http://172.31.90.2:80/cmpe221/loginCheck.jsp?username=Yuan&pwd=Yuan&Submit2=+++Login+++
http://172.31.90.2:80/cmpe221/loginCheck.jsp?username=Yuan&pwd=Yuan&Submit2=+++Login++++
Scan 172.31.90.2 finished
Scanning http://172.31.90.2:80/cmpe221/Preview.jsp?title=SHANGHAI%20KNIGHTS...
http://172.31.90.2:80/cmpe221/Preview.jsp?title=SHANGHAI%20KNIGHTS
Scan 172.31.90.2 finished
Scanning http://172.31.90.2:80/cmpe221/Preview1.jsp?title=SHANGHAI%20KNIGHTS...
http://172.31.90.2:80/cmpe221/Preview1.jsp?title=SHANGHAI%20KNIGHTS
Scan 172.31.90.2 finished
Scanning http://172.31.90.2:80/jspshop/listbook.jsp?id=2...
http://172.31.90.2:80/jspshop/listbook.jsp?id=2
(*)Detect DBType http://172.31.90.2:80/jspshop/listbook.jsp?id=2
(!)MSSQL_NUM_TYPE_1/NUM http://172.31.90.2:80/jspshop/listbook.jsp?id=2
Start Bruting...
Start Bruting
```

Type	Database	Username	Version
MSSQL_NUM_TYPE_1/NUM	Web	sa	Microsoft SQL SGrver 2000 - 8.00.760 (Intel X86) Dec 17 2002 14:22:05 Copyright (

Database name, username and version auto detected

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.

Advanced Feature overview - Privilege escalation

- How if we don’t have enough privilege?

- Oracle 9i Examples:

```
SELECT
SYS.DBMS_METADATA.GET_DDL('''||theuser.EVIL_FUNC()||''','') FROM dual;
```

- Oracle 10g Privilege Escalation

DBMS_ADVISOR

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!

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

Similar tool in market comparison

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

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 ☺

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

Demo, Demo, Demo

- Nothing is better than Real Demo

- Future roadmap/enhancement overview

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

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