

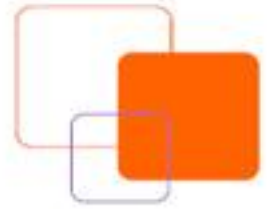


دانشگاه صنعتی شریف



آزمایشگاه و مرکز تخصصی آبا

در حوزه پایگاه داده ها

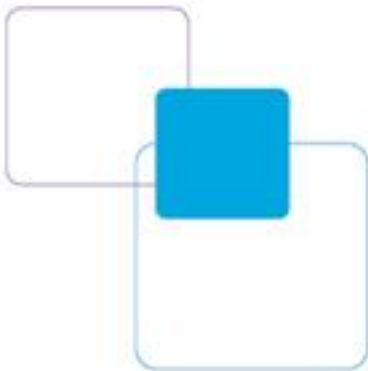


روش های کشف شناسه سیستم در  
پایگاه داده اوراکل ( قسمت سوم )

علی عباسی

[abbasi@ustmb.ac.ir](mailto:abbasi@ustmb.ac.ir)

فروردین ماه 1388

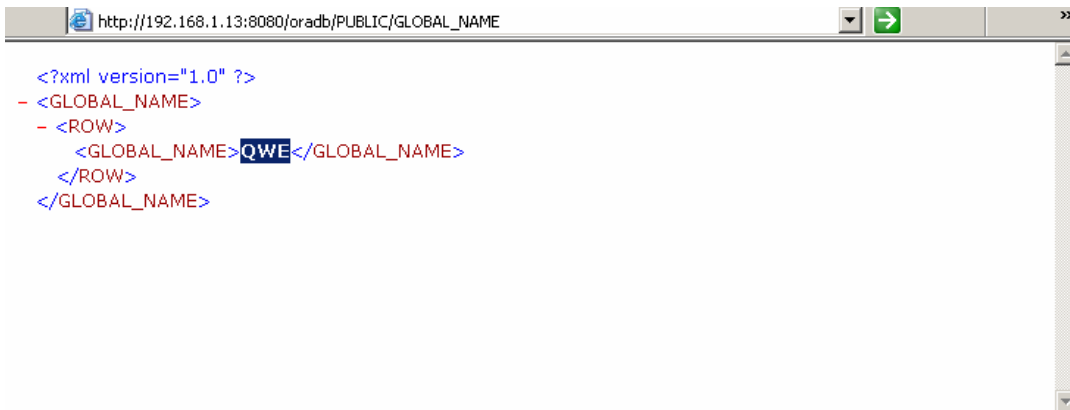


در قسمت های قبل ما به صورت ناتمام به بررسی روش های کشف شناسه سیستم در نرم افزار های ثالث پرداختیم. در این قسمت به ادامه بررسی روش های کشف شناسه سیستم در نرم افزار های ثالث خواهیم پرداخت و پس از آن روش های کشف شناسه سیستم را با استفاده از مجوز های اضافی در سیستم هدف مورد بررسی قرار خواهیم داد.

## : ORACLE XDB

در صورتی که ما دارای نام کاربری و کلمه عبور پایگاه داده باشیم اما موفق به کشف شناسه سیستم نشده ایم میتوانیم به وب سرویس Oracle XML DB Enterprise Edition (این مولفه به صورت پیش فرض در اوراکل نسخه های 9 و 10 نصب میشود) متصل شویم. برای بدست آوردن SERVICE\_NAME ما باید به آدرس زیر برویم :

[http://hostname:8080/oradb/PUBLIC/GLOBAL\\_NAME](http://hostname:8080/oradb/PUBLIC/GLOBAL_NAME).



```
<?xml version="1.0" ?>
- <GLOBAL_NAME>
- <ROW>
  <GLOBAL_NAME>QWE</GLOBAL_NAME>
</ROW>
</GLOBAL_NAME>
```

بدست آوردن SERVICE\_NAME با استفاده از Oracle XML DB

پس از بدست آوردن SERVICE\_NAME ما میتوانیم با استفاده از ابزار هایی مانند sqlplus به پایگاه داده متصل شویم.

## : SAP

بسیاری از شرکتها از پایگاه داده اوراکل به عنوان backend نرم افزار SAP/R3 استفاده میکنند. بر اساس تحقیقات صورت گرفته بر روی SAP در صورتی که SAP از پایگاه داده ی اوراکل به عنوان Backend استفاده

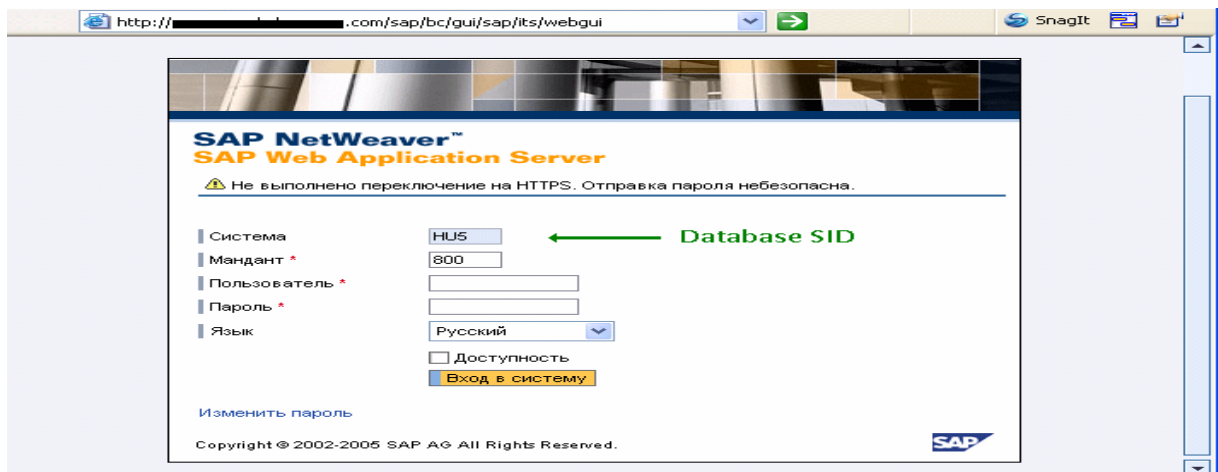
کند حداقل 4 راه برای بدست آوردن شناسه سیستم اوراکل وجود خواهد داشت . 2 راه برای کشف شناسه سیستم پایگاه داده از طریق SAP Application Server وجود دارد که به صورت پیش فرض بر روی پورت 8000 پروتکل TCP فعال است.

## 1 - صفحه پیش فرض مدیریت SAP Web Application Server :

همانطور که گفته شد دو راه برای کشف شناسه سیستم پایگاه داده در SAP Web Application Server وجود دارد که بر روی پورت 8000/TCP در انتظار برقراری ارتباط میماند. برای بدست آوردن شناسه سیستم پایگاه داده ما میتوانیم به راحتی به رابط تحت وب SAP در آدرس :

<http://hostname:8000/sap/bc/gui/sap/its/webgui>.

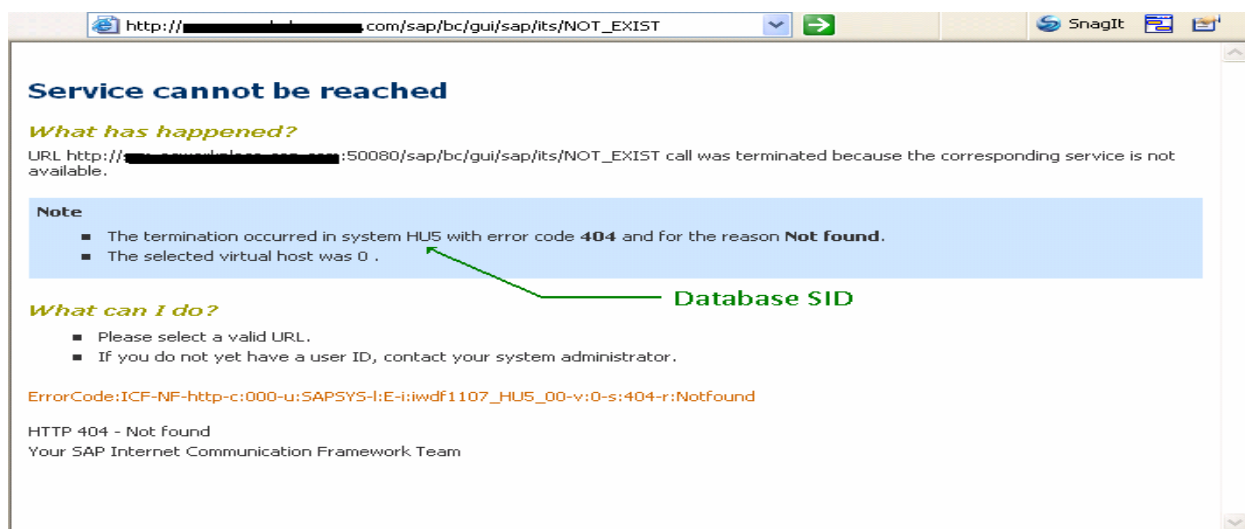
دسترسی یابیم. هنگامی که این صفحه را در مرورگر وب باز میکنیم ما صفحه ی خوش آمد گویی را میبینیم که حاوی فرم های نام کاربری و کلمه ی عبور و همچنین شامل مقدار شناسه سیستم پایگاه داده میباشد.



بدست آوردن شناسه سیستم به وسیله ی SAP Web Application Server

## 2 - خطای عدم وجود صفحه مورد نظر در SAP Web Application Server :

یکی از راه های دیگر برای بدست آوردن شناسه سیستم پایگاه داده ، درخواست یک صفحه ی نامرتبط و نا موجود در SAP Web Application Server است. سرور در جواب درخواست ما یک خطا با شماره 404 میدهد که حاوی اطلاعات اشکال زدایی بسیار زیادی است که شامل شناسه سیستم پایگاه داده نیز میشود.



بدست آوردن شناسه سیستم بوسیله ی خطای 404 در SAP Web Application Server

## : SAP RFC

یک راه دیگر برای بدست آوردن شناسه سیستم پایگاه داده Oracle و همچنین اطلاعات مفید دیگر ابزار rfcping است که برای تست رابط SAP RFC استفاده میشود. در صورتی که رابط RFC فعال نباشد این روش قابلیت استفاده نخواهد داشت .

```
./rfcping ashost=172.16.1.13 sysnr=00
```

SAP System Information

```
-----
Destination          test2_NSP_00
Host                  test2
System ID             NSP
Database              NSP
DB host               test2
DB system             ORACLE
SAP release           700
```

SAP kernel releas	700
RFC Protokoll	011
Characters	1100 (NON UNICODE PCS=1)
Integers	LIT
Floating P.	IE3
SAP machine id	560

همانطور که در این مثال مشاهده میکنید پایگاه داده اوراکل بوده و شناسه سیستم ( System ID ) نیز برابر مقدار "NSP" میباشد.

### اجرای حمله جستجوی تمام حالات بر روی SAP برای بدست آوردن شناسه سیستم :

هنگامی که شناسه سیستم را در SAP ایجاد میکنیم هیچ محدودیتی در آن وجود ندارد . شناسه سیستم شامل حروف و اعداد انگلیسی و باید دارای 3 کاراکتر و یا کمتر باشد ! این بدین معناست که ما میتوانیم شناسه سیستم را به راحتی با یک حمله جستجوی تمام حالات بدست آوریم ( که برای بدست آوردن آن تنها 10 دقیقه زمان لازم است ). ما از این متد در صورتی که هر یک از روش های ذکر شده ( به عنوان مثال دسترسی به SAP Web Application Server و یا رابط کاربری RFC محدود شده باشد ) میتوانیم استفاده کنیم.

### بدست آوردن شناسه سیستم بوسیله ی برنامه های تحت وب آسیب پذیر:

در صورتی که وب سرور بر روی همان سرور پایگاه داده اوراکل نصب شده باشد و شامل یک برنامه ی تحت وب آسیب پذیر به حملات پیمایش شاخه ( Directory Traversal ) باشد ، بدست آوردن شناسه سیستم و یا SERVICE\_NAME با درخواست فایل حاوی تنظیمات اوراکل به اسم tnsnames.ora از طریق آن آسیب پذیری ممکن خواهد بود. این فایل به صورت پیش فرض در شاخه ORACLE-home/NETWORK/admin قرار دارد .

Close Help Window

Notice: Undefined variable: CONFIG in y:\home\non-existent-host\help.php on line 46  
[Aáááá: ñèàcàòü âîü:eiob îðe+eîó îoéáèè]

Notice: Undefined variable: \_SESSION in y:\home\non-existent-host\help.php on line 46  
# tnsnames.ora Network Configuration File: E:\oracle\product\10.2.0\db\_1\network\admin\tnsnames.ora # Generated by Oracle configuration tools.  
ORCL102 = (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.40.14)(PORT = 1521)) (CONNECT\_DATA = (SERVER = DEDICATED) (SERVICE\_NAME = orcl102))) EXTPROC\_CONNECTION\_DATA = (DESCRIPTION = (ADDRESS\_LIST = (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1))) (CONNECT\_DATA = (SID = PLSExtProc) (PRESENTATION = RO)))

Close Help Window

### بدست آوردن شناسه سیستم بوسیله دسترسی های بیشتر در سیستم هدف :

خوب تا اینجا ما میدانیم چگونه شناسه سیستم را از نرم افزار هایی که از پایگاه داده استفاده میکنند بدون داشتن هیچ اطلاعاتی برای احراز هویت بدست آوریم.

در صورتی که تمامی متد های معرفی شده برای بدست آوردن شناسه سیستم با شکست مواجه شد میتوانید با بدست آوردن مجوز های دسترسی بیشتر در سرور هدف و یا منابع دیگر در سیستم اطلاعاتی شناسه سیستم را بدست آورید.

در ادامه فرض خواهیم کرد که ما دارای دسترسی بیشتری به سرور هدف و یا برنامه های نصب شده بر روی آن هستیم.

### بدست آوردن شناسه سیستم به وسیله دسترسی به سرور هدف :

1- بدست آوردن شناسه سیستم به وسیله دسترسی به System Account سیستم عامل در سرور

2- بدست آوردن شناسه سیستم به وسیله یک حساب قرارداد انتقال فایل در سرور

3- بدست آوردن شناسه سیستم به وسیله یک حساب MSSQL در سرور هدف.

بدست آوردن شناسه سیستم بوسیله حساب سیستم عامل در سرور:

به سادگی قابل تصور است در صورتی که نفوذگر به شاخه `$ORACLE_HOME/NETWORK/admin` دسترسی داشته باشد میتواند شناسه سیستم را از فایل تنظیمات پایگاه داده با نام `tnsnames.ora` بخواند و یا با استفاده از فرمان `"Isnrctl status"` آن را بدست آورد.

### بدست آوردن شناسه سیستم بوسیله یک حساب قرار داد انتقال فایل در سرور هدف:

در صورتی که ما دارای یک حساب قرارداد انتقال فایل در سرور هدف بوده و دارای سطح دسترسی `Read` در شاخه `$ORACLE_HOME` باشیم میتوانیم باز هم شناسه سیستم را بدست آوریم.

این کار به سادگی با خواندن فایل `tnsnames.ora` قابل انجام است. در صورتی که کاربر دارای هیچ نوع دسترسی `Read` نباشد او میتواند شناسه سیستم را با استفاده از بدست آوردن نام دایکتوری ها هم بدست آورد. در ویرایش های متفاوت پایگاه داده ، مکان های مختلفی برای شاخه ای وجود دارد که هم نام با شناسه سیستم پایگاه داده باشد. به عنوان مثال بیابید نگاهی به `Oracle 10g R2` بیاندازیم. اولین راه لیست کردن شاخه های موجود در مسیر `ORACLE_HOME\..\admin` میباشد.

```
C:\oracle\product\10.2.0\oradata >dir
Volume on the device C has no label.
The serial number of volumes: 8CFF-37FC
The contents of the folder C: \ oracle \ product \ 10.2.0 \ admin
08.04.2009 12:55 <DIR> .
08.04.2009 12:55 <DIR> ..
08.04.2009 12:55 <DIR> ORCL102
```

دایکتوری با نام `ORCL102` برابر شناسه سیستم پایگاه داده میباشد.

راه دوم لیست کردن شاخه های موجود در مسیر `$ORACLE_HOME\..\oradata` میباشد:

```
C: \ oracle \ product \ 10.2.0 \ oradata > dir
Volume on the device C has no label.
The serial number of volumes: 8CFF-37FB
The contents of the folder C: \ oracle \ product \ 10.2.0 \ oradata
08.04.2009 12:55 <DIR> .
08.04.2009 12:55 <DIR> ..
```

08.09.2009 12:55 <DIR> ORCL102

دایکتوری با نام ORCL102 مقدار شناسه سیستم پایگاه داده میباشد.

راه سوم لیست کردن نام شاخه های موجود در مسیر \$ORACLE\_HOME میباشد.

The contents of the folder E: \ oracle \ product \ 10.2.0 \ db\_1

04.04.2009 18:07 <DIR> .

04.04.2009 18:07 <DIR> ..

04.04.2009 18:07 <DIR> 192.168.40.14\_orcl102

04.04.2009 17:30 <DIR> admin

04.04.2009 17:30 <DIR> assistants

04.04.2009 16:53 <DIR> BIN

دایکتوری با اسم 192.168.40.14\_ORCL102 مشاهده میشود که مقدار ORCL102 برابر شناسه سیستم پایگاه

داده میباشد.

ادامه دارد.....