آزمایشگاه و مرکز تخصصی آپا

در حوزه پایگاه داده ها

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

علی عباسی

abbasi@ustmb.ac.ir

فروردین ماه 1388

آزمایشگاه و مرکز تخصصی آپا در حوزه پایگاه داده ها- مقاله سفید

در قسمت قبل ما به بررسی روش های بدست آوردن شناسه سیستم با استفاده از شناسه های سیستمی پیش فرض و عمومی اقدام کردیم. در این قسمت ، روش های حدس شناسه سیستم با استفاده از حمله واژه نامه و جستجوی تمامی حالات را مورد بررسی قرار خواهیم داد. سپس به بررسی روش های شناسایی شناسه سیستم در نرم افزار های ثالث خواهیم پرداخت.

حدس شناسه سیستم با استفاده از حمله واژه نامه :

اگر شناسه سیستم پایگاه داده در لیست پیش فرض و یا جزو شناسه سیستم های عمومی نبود ، ما میتوانیم برای حدس زدن شناسه سیستم از حمله واژه نامه استفاده کنیم . ابزار ها و اسکریپت هایی برای اتوماتیک کردن این پروسه وجود دارند . پر استفاده ترین این ابزار ها در جدول زیر قابل مشاهده است :

نام ابزار	نویسنده	آدرس دریافت :
CsidGuess.py from Inguma	Joxean Koret	http://sourceforge.net/projects/inguma
ora-getsid, ora-brutesid from OAK	David Litchfield	http://www.vulnerabilityassessment.co.uk/oak.htm
oscanner	Patrik Karlsson	http://www.cqure.net/tools/oscanner_bin_1_0_6.zip
sidguess	Red database Security	http://www.red-database-security.com/software/sidguess.zip
sidguesser	Patrik Karlsson	http://inguma.sourceforge.net/index.php

هنگامی که از این ابزار ها استفاده میکنیم مهمترین پارامتر سرعت است . جهت سنجش سرعت این ابزار ها ما تصمیم به انجام 2 آزمایش گرفتیم .

- ✓ تست اول برای سنجش زمان انجام کار با لیست استاندارد شناسه سیستم ها شامل 600 کلمه
- ✓ تست دوم برای سنجش زمان حدس شناسه سیستم پیش فرض "ORCL" با استفاده از حملات جستجوی تمام حالات بود. نتیجه ی این تست را نیز میتوانید در جدول زیر مشاهده کنید:

سرعت تست :

نام ابزار	سرعت حمله جستجوی تمام حالات	زمان صرف شده برای تست تمامی مقادیر پیش فرض (600 مورد)	زمان صرف شده برای حدس شناسه سیستم پیش فرض "ORCL" به روش جستجوی تمام حالات
Ora-brutesid	SID 90 در ثانیه	پیاده سازی نشد	114 دقیقه
Ora-getsid	SID 88 در ثانیه	7 ثانیه	پیاده سازی نشد
Oscanner	SID 80 در ثانیه	8 ثانیه	پیاده سازی نشد
Sidguesser	SID 71 در ثانیه	10 ثانیه	پیاده سازی نشد
Sidguess	SID 11 در ثانیه	58 ثانیه	این ابزار نتوانست کار را به پایان برساند

همانطور که مشاهده میکنید ابزار Ora-getsid بیشترین سرعت را برای حدس شناسه سیستم به روش حمله واژه نامه دارا بوده است.

حمله ی جستجوی تمام حالات :

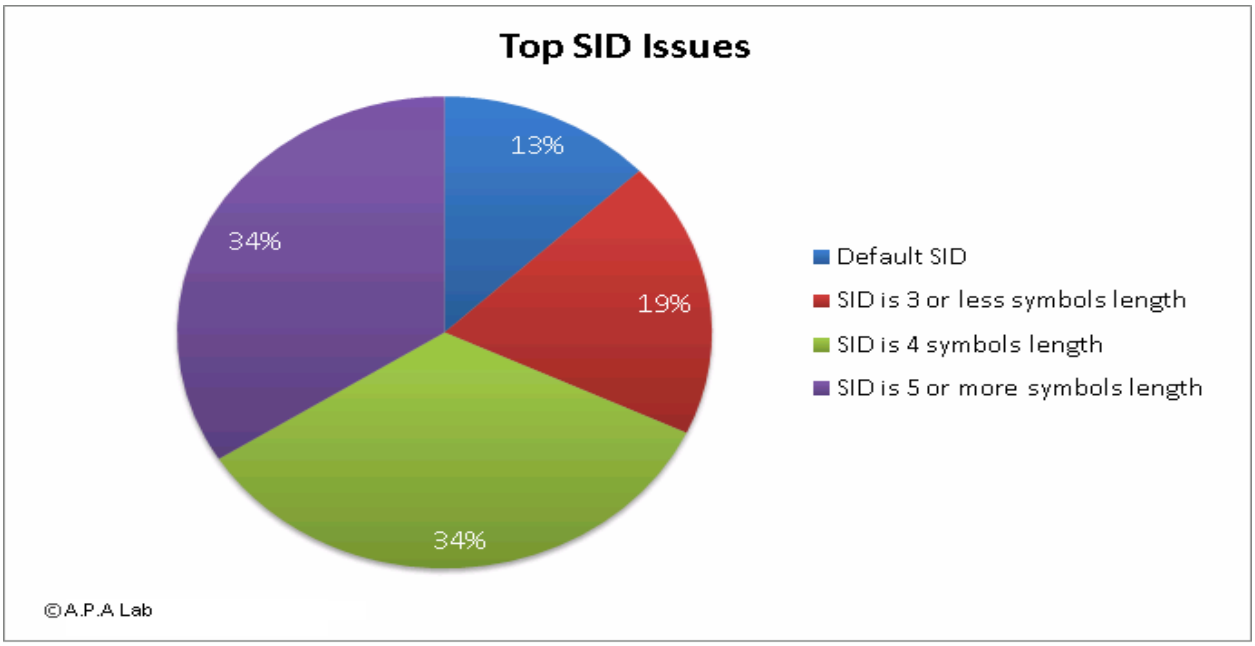
پس از اجرای حمله به وسیله حمله واژه نامه در صورتی که موفق به کشف شناسه سیستم نشدیم ، آخرین شانس ممکن اجرای حمله جستجوی تمام حالات بر روی شناسه سیستم میباشد. بهترین وسیله برای حمله جستجوی تمام حالات بر روی شناسه سیستم، ابزار ora-brutesid میباشد (به جدول قبل دقت کنید). با استفاده از ora-brutesid ما میتوانیم تمام شناسه سیستم های 4 کاراکتری ممکن را در زمان تقریبی 3 ساعت امتحان کنیم.

در صورتی که شناسه سیستم شامل 5 کارکتر باشد برای کشف شناسه سیستم 3 روز زمان لازم است . صرف این زمان نیز همچنان یک زمان نرمال برای اجرای حمله جستجوی تمام حالات میباشد . برای

آزمایشگاه و مرکز تخصصی آپا در حوزه پایگاه داده ها- مقاله سفید

افزایش سرعت کار ما میتوانیم چندین پروسه ی brutesid را برای حدس شناسه سیستم ها در پایگاه داده های متفاوت به طور همزمان اجرا کنیم که این زمان انجام کار را کاهش خواهد داد.

بر اساس نتایج گزارش های تست نفوذ پذیری گروه DSG در شرکت های بزرگ 13 درصد پایگاه داده ها از شناسه سیستم پیش فرض استفاده کرده اند. 19 درصد آنان از شناسه سیستم با حداکثر 3 کاراکتر استفاده نموده اند و 34 درصد آنان تعداد کاراکتر های شناسه سیستم آنان 4 بوده است.



بر اساس آمار های بالا احتمال کشف موفقیت آمیز شناسه سیستم در زمان تقریبی 3 ساعت در حدود 66 درصد میباشد (66% ≅ 34% + 19% + 13%) .

جستجوی شناسه سیستم و SERVICE_NAME در نرم افزارهای ثالث:

استفاده از حملات جستجوی تمام حالات و یا حمله واژه نامه همیشه موفقیت آمیز نیست. همچنین اجرای حمله جستجوی تمام حالات به دلیل ایجاد ترافیک و هشدارهای زیاد در فایل های رویداد نامه Listener توجه زیادی را جلب کرده و به راحتی قابل تشخیص است.

در اینجا ما راه حل دیگری را برای شناسایی شناسه سیستم بررسی خواهیم کرد.

آزمایشگاه و مرکز تخصصی آپا در حوزه پایگاه داده ها- مقاله سفید

در بسیاری از شرکت های بزرگ از پایگاه داده اوراکل به همراه نرم افزارهای مختلفی استفاده میشود مانند Oracle Application Server و یا Oracle SOA Suite و یا نرم افزار های دیگری مانند SAP R/3 (SAP R/3 یکی از نرم افزار های موجود برای پیاده سازی سیستم های ERP است).

اگر ما به نرم افزارهایی که به پایگاه داده اوراکل متصل بوده و با آن کار میکنند دسترسی داشته باشیم میتوانیم برای به دست آوردن شناسه سیستم و یا SERVICE_NAME حتی در صورت غیر فعال بودن فرامین Remote Listener یا ناموفق بودن حملات جستجوی تمام حالات اقدام کنیم . در لیست زیر ما رایج ترین نرم افزار هایی که میتواند برای شناسایی شناسه سیستم بدون داشتن سطوح دسترسی اضافی به کار روند را معرفی کرده ایم :

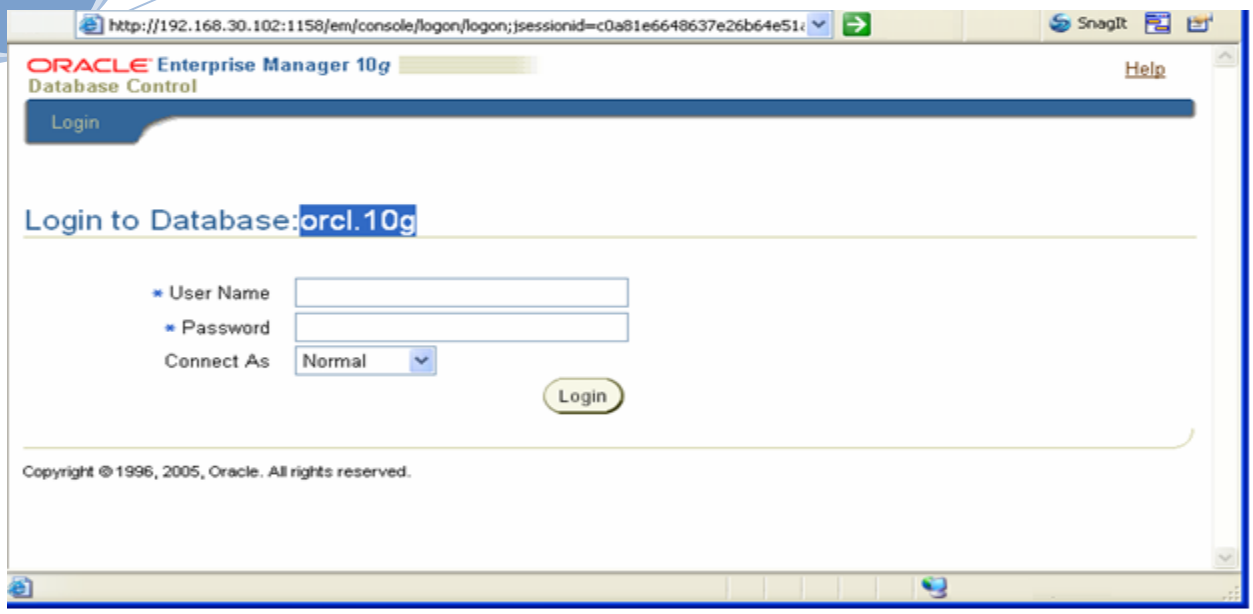
1- Oracle Enterprise Manager Control
2- Oracle Application Server
3- Oracle XDB
4- SAP Web Application Server
5- نرم افزار های تحت وب دارای آسیب پذیری

نرم افزار Oracle Enterprise Manager Control :

یکی از رایج ترین روش ها برای بدست آوردن SERVICE_NAME استفاده از رابط تحت وب Enterprise Manager Control است. وقتی پایگاه داده Oracle 10g R2 را نصب میکنیم Enterprise Manager Control به صورت پیش فرض نصب گردیده و بر روی پورت 1158 در انتظار ارتباط خواهد ماند. در صورتی که ما با استفاده از یک مرورگر وب، آدرس

http://hostname:1158/em/console

را وارد کنیم . صفحه خوش آمد گویی را خواهیم دید که از کاربر درخواست نام کاربری و کلمه عبور را میکند. جالبتر از همه اینکه این صفحه شامل مقدار SERVICE_NAME پایگاه داده نیز میشود.به تصویر زیر دقت کنید:

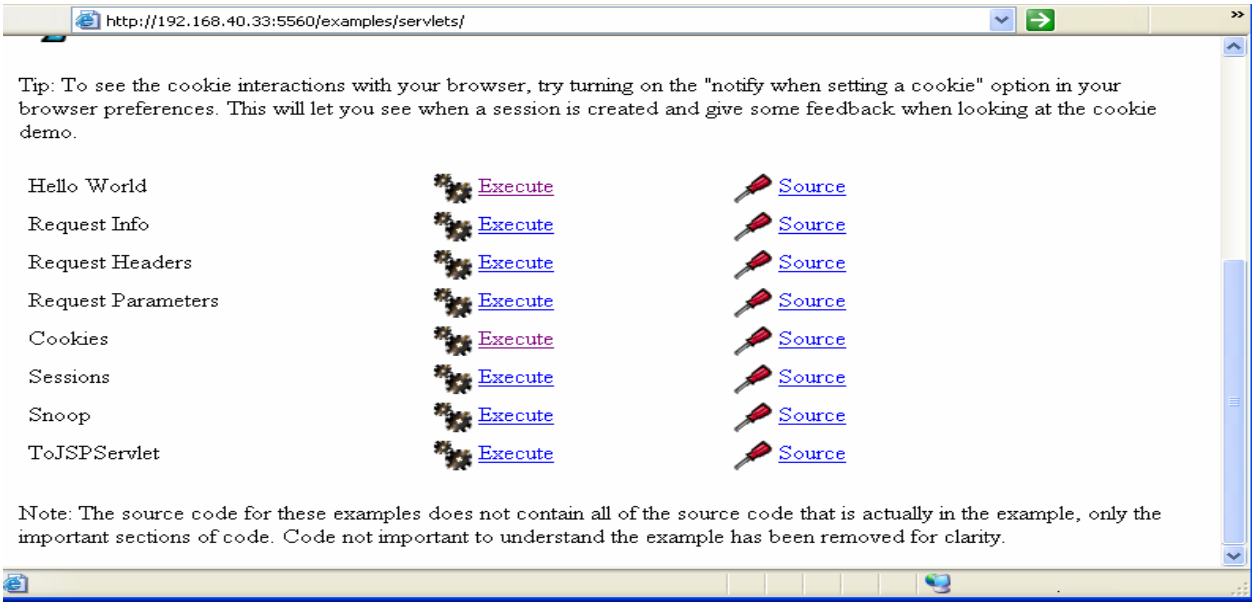


شناسایی مقدار SERVICE_NAME با استفاده از Enterprise Manager Database Control

نرم افزار Oracle Application Server

هنگامی که پایگاه داده ی Oracle 10g را نصب میکنیم شامل مولفه ای به نام Oracle Application Server میباشد (Oracle Application Server شامل Oracle Container For J2EE (OC4J) و Containers for J2EE و Oracle HTTP Server است) . Oracle Application Server شامل چند ابزار دیگر هم میباشد که به همراه آن نصب شده اند. ما میتوانیم این ابزار ها را در آدرسی شبیه به این مشاهده کنیم :

http://hostname:5560/examples/servlets.



آزمایشگاه و مرکز تخصصی آپا در حوزه پایگاه داده ها- مقاله سفید

ابزار های دیگری هم به همراه Oracle Application Server نصب شده اند که در اینجا دیده نمیشوند. نام یکی از آنها "Spy" میباشد. ما میتوانیم از این ابزار برای بدست آوردن SERVICE_NAME پایگاه داده استفاده کنیم. برای اینکار ما باید به آدرس زیر برویم:

http://hostname:5560/servlets/Spy.

ادامه دارد.....