

هک‌های Oracle

مؤلف: جان ویلی

مترجم: مرتضی کریمی

انتشارات
ناقص

Litchfield, David

سرشناسه : لیچفیلد، دیوید، ۱۹۷۵ - م.
عنوان و نام پدیدآور : هکهای Oracle / مؤلف جان ویلی؛ مترجم مرتضی کریمی.
مشخصات نشر : تهران: انتشارات ناقوس، ۱۳۸۹.
مشخصات ظاهری : ۱۷۶ ص: مصور، جدول.
شابک : ۹۷۸-۹۶۴-۳۷۷-۱۹۶-۶ : بها: ۵۰۰۰۰ ریال
وضعیت فهرست‌نویسی: فیبا
یادداشت : عنوان اصلی: Hacking and Defending Oracle.
موضوع : اوراکل (قابل کامپیوتر)
موضوع : پایگاه‌های اطلاعاتی - امنیت
شناسه افزوده : کریمی، مرتضی، ۱۳۶۴ -، مترجم
رده بندی کنگره : QAV۶/۹/۵۹ل۹ ۱۳۸۹ :
رده بندی دیویی : ۰۰۵/۸ :
شماره کتابشناسی ملی : ۲۱۴۹۴۳۵



www.naghoospress.ir

انتشارات
ناقوس

چاپ اول

نام کتاب : هکهای Oracle
ناشر : انتشارات ناقوس
ناشر همکار : انتشارات الیاس
مؤلف : جان ویلی
مترجم : مرتضی کریمی
چاپ اول : ۱۳۸۹
تیراژ : ۱۰۰۰ جلد
لینوگرافی : علامه
چاپ : علامه
صحافی : علامه
حروف‌نگار و صفحه‌آرا : مریم رضائی
قیمت : ۵۰۰۰۰ ریال
شابک : ۹۷۸-۹۶۴-۳۷۷-۱۹۶-۶
ISBN : 978-964-377-196-6

کلیه حقوق برای ناشر محفوظ است. تکثیر تمامی یا قسمتی از این اثر به‌صورت حروفچینی یا چاپ مجدد، چاپ افست، پلی‌کپی، فتوکپی و انواع دیگر چاپ ممنوع است و پیگرد قانونی دارد.

مراکز پخش:

- ۱- انتشارات ناقوس: میدان انقلاب، خیابان کارگر جنوبی، خیابان روانمهر، کوچه دولتشاهی، پلاک ۲
تلفن و فاکس: ۶۶۴۰۸۵۲۰ - ۶۶۴۰۱۷۹۸ - ۶۶۴۱۷۰۷۲ - ۶۶۴۶۶۷۹۳
- ۲- کتابفروشی الیاس: خیابان انقلاب، نیش فروردین تلفن: ۶۶۴۰۵۰۸۴

فهرست مطالب

۷	سر آغاز
۹	مقدمه
۱۰	مخاطبان
۱۰	نظرات، انتقادات و پیشنهادات
۱۱	فصل اول: نگاه کلی بر Oracle RDBMS
۱۱	معماری
۱۱	فرآیندها
۱۲	سیستم فایل
۱۸	شبکه
۱۹	شی‌های پایگاه داده
۱۹	کاربران و نقش‌ها
۱۹	امتیازات
۲۰	Oracle Patching
۲۱	نتیجه‌گیری
۲۲	فصل دوم: معماری شبکه‌ی Oracle
۲۳	خلاصه
۲۳	پروتکل TNS
۲۴	سرآیند TNS
۲۴	درون بسته‌ها
۲۶	بدست آوردن شماره نسخه Oracle
۲۷	شماره نسخه Listener و فرمان Status
۲۸	استفاده از شماره نسخه پروتکل TNS
۲۸	استفاده از شماره نسخه پایگاه داده XML
۲۹	استفاده از متن خطای TNS
۲۹	استفاده از تابع TTC ویرایش TNS
۳۰	استفاده بیشتر از مذاکرات (Negotiation) اختیاری شبکه
۳۰	نتیجه‌گیری
۳۱	فصل سوم: حمله به TNS Listener و توزیع‌کننده‌های امکانات (Dispatchers)
۳۹	حمله به TNS Listener
۳۹	گذشتن از محدودیت‌های Listener 10g
۴۰	

۴۱	Aurora GIOP Server
۴۶	XML Database
۴۹	نتیجه‌گیری
۵۱	فصل چهارم: حمله به سندیت فرآیندها
۵۱	سندیت چگونه کار می‌کند
۵۹	نام‌های کاربری و رمز عبورهای پیش‌فرض
۶۰	نگریستن در فایل‌ها برای رمز عبورها
۶۳	شمارش حساب کاربری و فاقد استدلال
۶۳	سرریز شدن‌های بافر در اثر نام کاربر طولانی
۶۴	یک نکته در Oracle روی Windows XP
۶۴	نتیجه‌گیری
۶۷	فصل پنجم: Oracle و PL/SQL
۶۷	PL/SQL چیست؟
۶۸	امتیازات اجرایی PL/SQL
۷۱	PL/SQL بسته‌بندی شده
۷۲	بسته‌بندی و باز کردن بسته در 10g
۷۲	بسته‌بندی و باز کردن بسته در ویرایش 9i و قبل از آن
۷۳	کار کردن بدون سورس
۷۴	تزریق PL/SQL
۷۶	ورود به دستورات SELECT برای بدست آوردن اطلاعات بیشتر
۷۷	ورود توابع
۷۸	ورود به بلاک‌های PL/SQL بی‌نام
۷۹	راه‌های برای ورود PL/SQL
۸۰	بررسی درزها
۸۴	درزهایی برای اجرای مستقیم SQL
۸۵	PL/SQL Race Condition
۸۶	بازرسی کد PL/SQL
۸۷	پکیج DBMS_ASSERT
۸۸	بعضی از مثال‌های واقعی
۸۹	بهره‌برداری از DBMS_CDC_IMPD
۹۰	بهره‌برداری از LT

۹۰	 بهره‌برداری از DBMS_CDC_SUBSCRIBE و DBMS_CDC_ISUBSCRIBE
۹۴	 Trigger ها و PL/SQL
۹۴	 نتیجه‌گیری
۹۵	 فصل ششم: Trigger ها
۹۵	 جذابیت Trigger: بهره‌برداری از Trigger برای سرگرمی و سود
۹۷	 مثالی از رفتار Trigger ها
۹۸	 Trigger MDSYS SDO_CMT_CBK_TRIG
۱۰۰	 Trigger SYS.CDC_DROP_CTABLE_BEFORE
۱۰۱	 Trigger MDSYS.SDO_DROP_USER_BEFORE
۱۰۱	 نتیجه‌گیری
۱۰۳	 فصل هفتم: افزایش امتیاز به طور غیرمستقیم
۱۰۳	 مراحل سه گانه: بدست آوردن امتیازات DBA به طور غیرمستقیم
۱۰۳	 بدست آوردن DBA از روی CREATE ANY TRIGGER
۱۰۳	 بدست آوردن DBA از CREATE ANY VIEW
۱۰۶	 بدست آوردن DBA از طریق EXECUTE ANY PROCEDURE
۱۰۸	 بدست آوردن DBA تنها از طریق CREATE PROCEDURE
۱۰۸	 نتیجه‌گیری
۱۰۹	 فصل هشتم: مغلوب ساختن VPD (Virtual Private Databases)
۱۱۱	 فریب دادن Oracle با حذف یک Policy
۱۱۱	 مغلوب ساختن VPD ها از طریق دسترسی به فایل ناقص
۱۱۵	 امتیازات عمومی
۱۱۷	 نتیجه‌گیری
۱۱۸	 فصل نهم: حمله به برنامه‌های وب PL/SQL از Oracle
۱۱۹	 معماری Oracle PL/SQL Gateway
۱۱۹	 شناخت Oracle PL/SQL Gateway
۱۱۹	 URL های PL/SQL Gateway
۱۲۰	 Oracle Portal
۱۲۱	 بررسی وجود Oracle PL/SQL Gateway
۱۲۲	 سرآیند پاسخ سرور HTTP سرور وب
۱۲۲	 امتحان NULL و سایر
۱۲۲	 تست امضاء (Signature Test)
۱۲۳	

۱۲۲	چگونه Oracle PL/SQL Gateway با سرور پایگاه داده ارتباط برقرار می‌کند.....
۱۲۴	حمله به PL/SQL Gateway.....
۱۲۵	لیست ممانعت PL/SQL.....
۱۳۱	نتیجه‌گیری.....
۱۳۳	فصل دهم: اجرای فرمان‌های سیستم عامل.....
۱۳۳	اجرای فرمان‌های OS از طریق PL/SQL.....
۱۳۴	اجرای فرمان‌های OS از طریق Java.....
۱۳۵	اجرای فرمان‌های OS با استفاده از DBMS_SCHEDULER.....
۱۳۶	اجرای مستقیم فرمان‌های OS با زمانبند Job (Job Scheduler).....
۱۳۷	اجرای فرمان‌های OS با استفاده از ALTER SYSTEM.....
۱۳۷	نتیجه‌گیری.....
۱۳۹	فصل یازدهم: دسترسی به سیستم فایل.....
۱۳۹	دسترسی به سیستم فایل با استفاده از پکیج UTL_FILE.....
۱۴۰	دسترسی به سیستم فایل با استفاده از Java.....
۱۴۱	دسترسی به فایل‌های باینری.....
۱۴۴	کاوش در متغیرهای محیطی سیستم عامل.....
۱۴۵	نتیجه‌گیری.....
۱۴۷	فصل دوازدهم: دسترسی به شبکه.....
۱۴۷	داده پالایشی.....
۱۴۸	استفاده از UTL_TCP.....
۱۴۹	استفاده از UTL_HTTP.....
۱۴۹	استفاده از Query های DNS و UTL_INADDR.....
۱۵۰	رمزنگاری داده قبل از پالایش.....
۱۵۱	حمله به دیگر سیستم‌های روی شبکه.....
۱۵۲	Java و شبکه.....
۱۵۳	لینک‌های پایگاه داده.....
۱۵۴	نتیجه‌گیری.....
۱۵۵	ضمیمه الف.....
۱۵۵	نام‌های کاربری و رمزهای عبور پیش‌فرض.....

سرآغاز



از زمان تولید اولین کامپیوترها تاکنون مدت زیادی نمی‌گذرد و شاید انتظار نمی‌رفت که اینگونه کامپیوترها، جهان پیرامون انسان را احاطه کنند. امروزه جهان بدون کامپیوتر قابل تصور نیست و روز به روز این علم نوپا رو به پیشرفت است و بقیه علوم هم از این علم در حیطه کاری خود استفاده می‌کنند. یکی از رکن‌های اصلی در این علم ذخیره اطلاعات می‌باشد. در گذشته انسان مجبور بود اطلاعات مهم خود را روی کاغذ بنویسد و با آمدن کامپیوتر بشر به این فکر افتاد که از کامپیوتر به جای کاغذ استفاده کند. اما سوال این بود که

نگونه باید این کار را انجام می‌داد؟ به همین منظور نرم‌افزارهای پایگاه داده ایجاد شدند. در این نرم‌افزارها کاربر می‌توانست اطلاعات خود را در جداولی منظم قرار دهد و از آنها استفاده نماید. کم‌کم نرم‌افزارها توسعه پیدا کردند و توانستند در دیگر عرصه‌های کاربرد کامپیوتر نیز به کار روند. یکی از این نرم‌افزارها Oracle می‌باشد که از لحاظ امنیت از بقیه نرم‌افزارهای موجود در رتبه بالاتری قرار دارد. در این کتاب، مشکلات امنیتی این نرم‌افزار بیان شده است و یک مدیر پایگاه داده می‌تواند با شناخت آنها از آشکار شدن اطلاعات خود در مقابل مهاجمان جلوگیری نماید. هر چند از این مشکلات می‌توان به‌عکس نیز استفاده و از آنها برای حمله به پایگاه داده استفاده کرد اما هدف اصلی این کتاب رفی روش‌های لازم جهت ممانعت از انجام چنین اعمالیست. امیدوارم این کتاب راهنمای مناسبی برای اندنگان عزیز بوده و بدین ترتیب توانسته باشم گامی هر چند کوچک در تعالی و پیشرفت این مرز و م داشته باشم.

پایان این کتاب را به پدر و مادر عزیزم تقدیم کرده و از زحمات تمامی کسانی که مرا در نگارش این یاری نموده‌اند تشکر می‌نمایم.

مرتضی کریمی

مقدمه

امنیت نرم افزار همیشه یکی از مسائل مهم برای تولیدکنندگان و استفاده کنندگان آن به شمار می آید. در پایگاه داده این فاکتور از دیگر مسائل مهم تر است و همیشه بر آن تاکید می شود. امنیت نرم افزار تا به حال، هیچگاه به طور کامل برای تولیدکنندگان و استفاده کنندگان بدست نیامده و Oracle نیز که در جهان امروز یکی از بهترین نرم افزارهای پایگاه داده بشمار می آید خالی از این نقیصه نیست. در این کتاب سعی شده است حفره های امنیتی Oracle برای شما عزیزان بازگو شود و با مثال ها و کدهایی که در آن ارائه شده است آن را به شما نشان دهد. حفره هایی که در این کتاب آمده است معمولاً برای نسخه های Oracle 10g Release 2, Oracle 10g Release 9i و ویرایش های قبل تر از آن کاربرد دارد.

در فصل اول این کتاب، ابتدا نگاهی اجمالی بر معماری Oracle داریم و بعد از آن به فرآیندها، سیستم فایل و Patching در Oracle خواهیم پرداخت.

در فصل دوم به معماری شبکه Oracle و مسائل پیرامون آن می پردازیم.

در فصل سوم نحوه حمله به TNS Listener و Dispatcher ها را بررسی می کنیم.

در فصل چهارم چگونگی حمله به سندیت فرآیندها و همچنین چگونگی استفاده از نام های کاربری و رمزهای عبوری که به طور پیش فرض در Oracle وجود دارد را بررسی می کنیم.

در فصل های پنجم و ششم به ترتیب PL/SQL و Trigger ها را بررسی می کنیم. همچنین چگونگی وارد شدن SQL در Oracle، معرفی Trigger ها و نحوه استفاده از آنها را نیز تشریح خواهیم کرد.

در فصل هفتم با تکیه بر مطالب فصل های پنجم و ششم به چگونگی افزایش امتیازات از طریق Trigger ها می پردازیم.

فصل هشتم به VPD یا (Virtual Private Databases) خواهیم پرداخت.

فصل نهم به چگونگی بهره برداری از برنامه های وب PL/SQL می پردازیم.

فصل دهم به چگونگی اجرای فرمان های OS اشاره می کنیم.

فصل یازدهم به چگونگی دسترسی به سیستم فایل خواهیم پرداخت.

فصل دوازدهم نحوه دسترسی به شبکه را بررسی می کنیم.

در فصل آخر کتاب به ترکیب PL/SQL و Java را اشاره کرده و با تکیه بر این دو فاکتور نحوه نفوذ Oracle را بررسی می کنیم.

ضمیمه کتاب نیز تمامی نام های کاربری و رمزهای عبور پیش فرض در Oracle 10g ارائه شده است و تمامی شما دوستان عزیز توصیه می کنم از این ضمیمه براحتی نگذشته و حتماً آن را مطالعه فرمایید

زیرا یکی از رکن‌های اساسی نفوذ در Oracle بر چگونگی استفاده از این نام‌های کاربری و رمزهای عبور تکیه دارد. بدیهی است این کتاب فقط به مسائل پایه می‌پردازد و برای تسلط بیشتر در این زمینه، شما دوستان عزیز باید زمان و انرژی بیشتری را صرف نمایید.

مخاطبان

این کتاب برای مخاطبان در سطح متوسط و پیشرفته می‌باشد و برای استفاده هر چه بهتر از آن لازم است کاربران عزیز، آشنایی لازم با محیط Oracle و زبان‌های C، SQL و Java را داشته باشند.

نظرات، انتقادات و پیشنهادات

تمامی خوانندگان عزیز می‌توانند نظرات، انتقادات و پیشنهادات خود را به پست الکترونیکی Morteza_karimi_64@yahoo.com ارسال نمایند.