



راهنمای جامع امن سازی پایگاه داده SQL Server

گردآوری و ترجمه : مهندس حامد زندی



۱۳۹۳

سرشناسه	زندى، حامد، ۱۳۵۸ - گردآورنده، مترجم
عنوان و نام پدیدآور	راهنمای جامع امن سازی پایگاه داده SQL Server / گردآوری و ترجمه حامد زندی
مشخصات نشر	تهران: پایگاه دانش، ۱۳۹۳
مشخصات ظاهری	۲۵۴ ص.: مصور، جدول
شابک	۹۷۸-۶۰۰-۹۴۶۷۹-۰-۷
وضعیت فهرست نویسی	فیا
پادداشت	کتاب حاضر ترجمه از دو کتاب "Securing SQL server: protecting your database from attackers" اثر "تو دنی خری" و "Microsoft SQL server 2012 security cookbook" اثر تامس لاروک است
موضوع	سرویس، کیو. ال
موضوع	پایگاه‌های اطلاعاتی -- طراحی
موضوع	پایگاه‌های اطلاعاتی -- امنیت
شناسه افزوده	خری، دنی
شناسه افزوده	Cherry, Denny
شناسه افزوده	لاروک، تامس
شناسه افزوده	LaRock, Thomas
رده بندی کنگره	QA76/۹۷۱۳۹۳
رده بندی دیویی	۰۰۵/۷۵۴۵
شماره کتابشناسی ملی	۳۶۶۱۰۴۶

تماس با انتشارات : ۰۹۱۲۶۱۰۱۸۵۵ و ۰۲۱-۶۶۱۹۵۳۴۵

Email : payghadanesh@gmail.com



نام کتاب	راهنمای جامع امن سازی پایگاه داده SQL Server
گردآوری و ترجمه	حامد زندی
ناشر	پایگاه دانش
صفحه آرایى	واحد تولید انتشارات پایگاه دانش
نوبت چاپ	اول - ۱۳۹۳
شمارگان	۵۰۰ جلد
قیمت	۱۷۰۰۰ تومان
شابک	۹۷۸-۶۰۰-۹۴۶۷۹-۰-۷
ISBN	978-600-94679-0-7

کلیه حقوق این اثر برای ناشر محفوظ است.
هر گونه چاپ و تکثیر از محتویات اثر ممنوع
بوده و متخلفین تحت پیگرد قانونی قرار
می گیرند.

سخن نشر

با توجه به گسترش فناوری های نوین اطلاعاتی و افزایش خیل مشتاقان و دانش پژوهان حوزه فناوری اطلاعات و ارتباطات در صنایع و دانشگاههای کشور ، لزوم تولید آثار غنی و پربار علمی که نیازمندی جامعه دانشگاهی را پوشش دهد و همچنین آثار کاربردی که برآورنده نیاز صنایع بازار کار در کشور باشد ضروری به نظر می رسد .

انتشارات پایگاه دانش با بهره گیری از ظرفیت و توان اساتید ، دانش آموختگان و متخصصین و با هدف ارائه کتب دانشگاهی و کاربردی در زمینه های فناوری اطلاعات ، مدیریت و شاخه های مرتبط با آن کار خود را آغاز نموده است . با توجه به راهبرد انتشارات پایگاه دانش که همانا تولید آثار وزین ، پربار و جامع دانشگاهی و کاربردی است ، این انتشارات همواره تلاش خواهد نمود تا آثاری را به دست خواننده برساند که به لحاظ علمی ، محتوایی و نگارشی از سطح بالایی برخوردار باشد و بتواند رضایت خوانندگان را به خود جلب نماید .

امید داریم که راهکارها و پیشنهادات شما عزیزان ، اساتید و دانش پژوهان گرانقدر بتواند ما را پیشبرد اهداف عالیه و نشر آثار پربار علمی یاری دهد تا ان شاء الله شاهد ارتقای سطح دانشی دانش پژوهان ساعی و در پی آن افزایش رتبه علمی کشور عزیزمان باشیم . ضمن اینکه انتشارات پایگاه دانش، آمادگی لازم جهت همکاری با کلیه اساتید و مولفین عزیز جهت ارائه آثار ارزشمند علمی و تخصصی را دارد. خواهشمند است نظرات ، راهکارها و پیشنهادات خود را جهت پربارتر کردن آثار منتشر شده به آدرس paygahdanesh@gmail.com ارسال نمایید .

مقدمه مؤلف

روند رو به رشد فناوری اطلاعات در کشور و توسعه روز افزون برنامه های کاربردی و سرویس های وب و سایت های اینترنتی سبب می شود تا امن سازی اطلاعات و داده های انباشته شده در مراکز داده یا در حال انتقال در شبکه بیش از پیش ضرورت پیدا کند .

به دلیل اینکه اغلب سرویس های وب بر بستر اینترنت به کاربران ارائه می شوند و مستعد حملات مختلف از سوی کاربران بد اندیش هستند لذا امن سازی شبکه و پایگاه داده قبل از انتشار برنامه کاربردی در اینترنت باید مد نظر قرار گیرد .

کتاب پیش روی جزو معدود کتبی است که به بحث تخصصی پیرامون موضوع امنیت پایگاه داده SQL Server می پردازد . علت انتخاب این DBMS این است که حجم وسیعی از عملیات پایگاه داده بر روی این ابزار پیاده سازی شده و طیف وسیعی از برنامه نویسان و راهبران پایگاه داده و مدیران امنیت با این محصول ماکروسافتی مانوس هستند اگر چه اکثر مطالب ارائه شده قابلیت استفاده در سایر DBMS ها را داراست و موضوعات به نحوی در کتاب سازماندهی شده که بطور کلی قابلیت استفاده در سایر محصولات را نیز دارد .

با توجه به اینکه هر اثری خالی از ایراد و اشکال نبوده و قطعاً خوانندگان فهیم می توانند به نحو مطلوبی ما را در ارائه آثار پربارتر یاری کنند . از این رو خواهشمند است نظرات ، انتقادات و پیشنهادات اصلاحی خود را درخصوص این اثر به آدرس zandi_hamed@yahoo.com ارسال نمایید .

فهرست مطالب

فصل اول ◀ امنیت شبکه	۱۳
امن سازی شبکه	۱۴
فایروال های شبکه	۱۴
فایروال های سرور	۲۱
IP عمومی و IP خصوصی	۲۵
دسترسی به SQL Server از منزل	۲۷
امنیت فیزیکی	۲۹
پورت های باز در شبکه	۳۰
ایستگاه های کاری قفل شده	۳۱
مهندسی اجتماعی	۳۳
یافتن نمونه های SQL نصب شده	۳۴
تست امنیت شبکه	۳۶
فصل دوم ◀ رمز گذاری پایگاه داده	۳۹
رمز گذاری پایگاه داده	۴۰
درهم سازی در مقابل رمز گذاری	۴۰
در هم سازی	۴۲
رمز گذاری داده های جدول	۴۴
رمز گذاری در SQL Server	۴۵
رمز گذاری داده های جانبی	۵۵
رمز گذاری داده های در حال انتقال	۶۰
استفاده از SQL Server بر روی SSL	۶۱

۶۳	SQL Server 2000 و قبل از آن
۶۵	SQL Server 2005 و بالاتر
۶۷	مخفی کردن نمونه SQL Server
۶۸	IPSec
۷۵	رمزگذاری داده‌ها با درایورهای MPIO
۷۶	رمزگذاری Powerpath با نیازمندی‌های RSA
۸۹	رمزگذاری داده‌ها از طریق HBA
۹۱	فصل سوم - امنیت کلمه عبور در SQL Server
۹۲	امنیت کلمه عبور در SQL Server
۹۴	Extended Protection
۹۹	رمزهای عبور پیچیده
۱۰۴	رمزگذاری رشته اتصال کلاینت
۱۰۵	سرویس‌های گزارش‌گیری SQL
۱۰۵	نقش‌های برنامه کاربردی
۱۱۰	استفاده از پالسی برای اعمال طول کلمه عبور
۱۱۳	پالسی‌های گروهی احراز هویت ویندوز
۱۱۶	نیازمندی‌های استفاده از پالسی‌ها در مدیریت لاگین‌های SQL
۱۱۹	فصل چهارم - امن سازی نمونه SQL
۱۲۰	چه اجزایی از SQL Server را باید نصب کرد؟
۱۲۲	احراز هویت SQL و احراز هویت ویندوز
۱۲۵	ویرایش فایل Master.mdf
۱۲۵	استفاده از یک دیباگر برای کلمه عبور

۱۲۶	پالسی‌های تغییر کلمه عبور
۱۲۷	ردگیری لاگین‌های ناموفق
۱۳۰	تغییر نام حساب SA
۱۳۱	غیر فعال کردن حساب SA
۱۳۳	امنیت نقاط پایانی
۱۳۴	رویه‌های ذخیره شده به عنوان یک معیار امنیتی
۱۳۵	عدم نیاز دسترسی به جداول پایه
۱۳۷	حداقل مجوزهای ممکن
۱۳۸	سرورهای پیوندی
۱۳۹	مشکلات NCLM Double Hop
۱۴۰	استفاده از پالسی برای امن سازی نمونه
۱۴۶	تنظیمات خاص SQL Azure
۱۴۸	نمونه‌هایی از پایگاه داده که از سازمان خارج می‌شوند
۱۵۱	فصل پنجم ◀ امنیت پایگاه داده‌های در معرض اینترنت
۱۵۲	SQL CLR
۱۵۶	رویه‌های ذخیره شده توسعه یافته
۱۵۷	محافظت از رشته اتصال
۱۵۸	قاپروال‌های پایگاه داده
۱۵۹	پاک کردن Pagefile حافظه مجازی
۱۶۴	(UAC) User Access Control
۱۶۶	تنظیم سایر پالسی‌های دامنه
۱۶۷	سرویس‌های گزارش گیری

۱۶۸		احراز هویت بدون نام
۱۷۰		احراز هویت فرم ها
۱۷۱		امنیت در Reporting Services
۱۷۳		فصل ششم ◀ مقابله با حملات تزریق SQL
۱۷۴		حمله تزریق SQL چیست؟
۱۷۷		امن سازی در چند لایه
۱۷۸		دلیل موفق بودن حملات تزریق SQL
۱۷۹		محافظت در مقابل حملات تزریق SQL
۱۸۴		محافظت کد SQL بویا از حمله تزریق از طریق رویه ذخیره شده
۱۸۶		حذف برخی رویه های ذخیره شده سیستمی
۱۸۷		استفاده از منطق درست کد نویسی
۱۸۸		خطاهای نمایش یافته برای کاربر
۱۹۰		پاکسازی پایگاه داده پس از حمله تزریق SQL
۱۹۳		فصل هفتم ◀ امنیت پشتیبان گیری از پایگاه داده
۱۹۵		بازنویسی نسخه های پشتیبان
۱۹۷		حذف نسخه های پشتیبان قدیمی
۲۰۲		کلمه عبور برای Media Set و Backup Set
۲۰۳		رمزگذاری نسخه پشتیبان
۲۰۴		ابزار LiteSpeed for SQL Server
۲۰۵		ابزار Red Gate SQL HyperBac
۲۰۵		ابزار Red Gate SQL Backup
۲۰۷		رمز گذاری داده ها بصورت نابدا

۲۰۸	فشرده سازی و رمز گذاری
۲۰۸	انتقال نسخه پشتیبان به محل دیگر
۲۱۱	فصل هشتم ◀ ممیزی امنیت
۲۱۲	استفاده از Profiler برای ممیزی دسترسی‌ها
۲۱۹	ممیزی ورود به SQL Server
۲۱۹	ممیزی ورود در SQL Server 2005 و قبل از آن
۲۲۱	ممیزی ورود در SQL Server 2008 و بعد از آن
۲۲۶	ممیزی تغییرات داده
۲۲۶	بیکربندی CDC
۲۲۸	ممیزی پرس و جو گیری داده‌ها
۲۳۱	ممیزی تغییر در ساختار شماها
۲۳۲	استفاده از پالسی برای ممیزی
۲۳۴	ممیزی C2
۲۳۷	فصل نهم ◀ مجوزهای سرور
۲۳۸	مجوزهای مورد نیاز OS جهت سرویس SQL Server
۲۳۸	مجوزهای سیستمی ویندوز
۲۳۹	مجوزهای NTFS در SQL Server
۲۴۰	مجوزهای مورد نیاز سیستم عامل جهت DBA
۲۴۱	حساب کاربری دوگانه
۲۴۱	حقوق دسترسی مورد نیاز برای نصب سرویس بک
۲۴۲	حق دسترسی مورد نیاز OS برای اتصال راه دور به SSIS
۲۴۴	دسترسی‌های پیش فرض Sysadmin

۲۴۴ Sysadmin نقش کاربردی و نقش

۲۴۵ پیوست ◀ چک لیست امنیت شبکه و پایگاه داده

www.ketab.ir