بسم الله الرحمن الرحیم

آموزشگاه تحلیل داده

تخصصی ترین مرکز برنامه نویسی و دیتابیس در ایران

سناریوهای مختلف امنیتی برنامه های کاربردی در SQL Server

مدرس : مهندس افشین رفوآ

دوره آموزش SQL Server Administration

سناریوهای مختلف امنیتی برنامه های کاربردی در SQL Server

در راستای ساخت یک برنامه ی امن سمت سرویس گیرنده SQL Server روش های مختلف صحیحی وجود دارد که می توان از آن ها بهره برد، بدین معنا که هر برنامه در شرایط موردنیاز، محیط نصب و تعداد کاربران آن از دیگر برنامه ها کاملا متفاوت بوده و منحصر بفرد می باشد. یک برنامه ای که در ابتدای نصب آن کاملا ایمن بوده ممکن است به مرور زمان دیگر از آن امنیت اولیه برخوردار نباشد. نمی توان با هیچ قطعیتی تمامی خطرات احتمالی که در آینده ممکن است برنامه را تهدید کند، پیشبینی نمود.

SQL Server به عنوان یک محصول، به تدریج (و طی ویرایش های متعدد) تکامل یافته و تمامی ویژگی ها و امکانات جدید امنیتی را که قابلیت ایجاد برنامه های پایگاه داده ایمن را به برنامه سازان می دهد، در خود گنجانده. با این حال تامین امنیت یک برنامه امری ساده نبوده و نیازمند نظارت و بروز رسانی پیوسته می باشد.

تهدید های امنیتی معمول

برنامه نویسان باید با خطرات امنیتی آشنا بوده، ابزار مقابله با آن را بشناسد و نیز نحوه ی اجتناب از حفره های امنیتی که به موجب عدم بررسی جامع توسعه دهنده خود در برنامه ایجاد می کند را درک کند. بهترین دید نسبت به امنیت در تصور کردن آن به عنوان یک زنجیر خلاصه می شود که وجود یک شکستکی در فقط یکی از حلقه های آن ممکن است استحکام کل مجموعه را به خطر بیاندازد. در زیر به هریک از تهدیدات امنیتی معمول می پردازیم.

SQL Injection

فرایندی است که طی آن یک کاربر مخرب بجای وارد کردن input معتبر و مجاز، دستورات Transact-SQL را وارد می نماید. چنانچه ورودی به طور مستقیم و بدون اینکه مورد اعتبارسنجی قرار گیرد به سرویس دهنده ارسال گردد و همچنین برنامه به صورت تصادفی کد تزریق شده را اجرا نماید، در آن صورت حمله ی انجام شده می تواند داده ها را تخریب کرده و یا کملا نابود سازد.

می توان حملات SQL Server injection را با بهره گیری از stored procedure ها و دستورات پارامتری (parameterized command)، اجتناب از SQL پویا (dynamic) و همچنین محدودسازی مجوزها برای کلیه ی کاربران، کاملا خنثی نمود.

بالا بردن سطح مجوزها

این نوع حمله زمانی رخ می دهد که کاربری بتواند به سطح دسترسی یک حساب کاربری قابل اطمینان و مورد اعتماد (trusted account) نظیر یک مالک یا مدیر دست یابد. به این خاطر پیشنهاد می کنیم تا حد امکان از حساب های کاربری با کمترین سطح دسترسی بهره گرفته و تنها مجوزهای لازم را به کاربران تخصیص دهید و از بکار بردن حساب های مدیریتی یا مربوط به مالک به منظور اجرای کدهای خود اجتناب ورزید. با این کار از میزان خساراتی که ممکن است حین رخداد موفقیت آمیز حمله به داده ها وارد گردد، کاسته می شود. به هنگام اجرای تسک هایی که به مجوزهای بیشتری نیاز دارند، توصیه می کنیم از امضای پروسیجر (procedure signing) یا جعل هویت (impersonation) تنها در مدت زمان اجرای تسک استفاده کنید. می توان stored procedure ها را با گواهینامه امضا کرده و یا با بهره وری از impersonation به طور موقت مجوز تخصیص داد.

مراقبت هوشمند و محافظت در برابر حملات کاوشی

یک حمله ی کاوشی با بهره گیری از پیغام های خطا که توسط یک برنامه تولید می شود، آسیپ پذیری ها و شکاف های امنیتی را شناسایی می کند. با پیاده سازی مدیریت خطا (error handling) در کد های پروسیجر خود مانع از بازگردانی اطلاعات خطاهای SQL Server به کاربر شوید.

احراز هویت (اعتبارسنجی)

یک حمله ی connection string injection در صورتی رخ می دهد که connection string مبتنی بر ورودی کاربر درست در زمان اجرا ساخته شده و ما از لاگین SQL Server استفاده کنیم. چنانچه connection string به منظور یافتن جفت های کلیدواژه معتبر مورد بررسی قرار نگیرد، در آن صورت attacker (مخرب) می تواند کاراکترهای اضافی بر سازمان درج کرده و به اطلاعات حساس یا دیگر منابع مستقر بر روی سرور دسترسی پیدا کند. لذا توصیه می کنیم تا حد امکان از اعتبارسنجی ویندوز (Windows authentication) استفاده کنید. در صورت لزوم استفاده از لاگین SQL Server، پیشنهاد می کنیم از SqlConnectionStringBuilder برای ایجاد و اعتبارسنجی connection string ها در زمان اجرا استفاده کنید.

گذرواژه ها

بسیاری از حملات موثر به این خاطر است که شخص مخرب توانسته به گذرواژه ی حساب کاربری با سطح دسترسی بالا (privileged user) دست یافته و یا آن را حدس بزند. هویدا است که گذرواژه ها اولین خط دفاعی شما در برابر حملات محسوب می شوند، از این رو انتخاب گذرواژه های قوی و کارامد برای حفظ امنیت سیستم ضروری می باشد. برای اعتبارسنجی ترکیبی (mixed mode) بایستی سیاست های رمزگذاری تعریف کرده و به اجرا درآورد.

همیشه یک گذرواژه ی منحصر بفرد،قدرتمند و بهینه از لحاظ ایمنی به حساب کاربری sa تخصیص دهید، حتی در شرایطی که از اعتبارسنجی ویندوز استفاده می کنید.