درس ۱۱ :

SQL Server Security

بحث امنیت همواره یکی از مهمترین شاخه های مهندسی نرم افزار و به تبع آن، یکی از حساسترین وظایف مدیران سیستم به خصوص مدیران شبکه و یا مدیران بانکهای اطلاعاتی است. با تنظیم سطوح دسترسی برای کاربران شبکه یا بانکهای اطلاعاتی شبکه، امنیت اطلاعات یا به عبارتی عدم دسترسی افراد فاقد صلاحیت به اطلاعات، تضمین میگردد. هر سیستم عامل، پلتفرم یا بانک اطلاعاتی، شیوه های خاصی را برای برقراری قواعد امنیتی به کاربران معرفی مینماید. در SQL Server هم روشهای خاصی برای این مقوله وجود دارد . SQL server سطوح مختلف امنیتی را برای دسترسی به بانک اطلاعاتی فراهم می کند.

سطح اول : تائید هویت برای اتصال به سرور

درسطح اول کاربران برای اتصال به SQL Server باید با یکی از دو روش زیر تایید هویت شوند:

۱. **Windows Authentication**
۲. **SQL server Authentication**

در روش اول کاربران برای اتصال به سرویس دهنده SQL باید توسط ویندوز شناسایی شوند در نتیجه کاربرانی که با موفقیت وارد ویندوز شده اند می توانند به سرور متصل شوند کاربرانی که از طریق شبکه قصد اتصال به سرور را دارند باید نام کاربری و رمز عبور در سیستم داشته باشند.

در روش دوم کاربرانی می توانند به سرور متصل شوند که نام کاربری و کلمه ی عبور معتبر در SQL server داشته باشند. هنگام نصب SQL server به طور پیش فرض یک کاربر به نام sa ایجاد می شود.

سطح دوم : نقش های از پیش تعریف شده سرویس دهنده (Server Roles)

نقش های سرویس دهنده برای آن هستند تا برخی از کارهای مدیریتی سرویس دهنده را به اشخاص دیگر واگذار کنید.

Sysadmin (System Admin) : اعضای این نقش می توانند هر عملی را در سرویس دهنده انجام دهند.

Serveradmin : اعضای این نقش می توانند پیکربندی مشخصات سرویس دهنده را انجام دهند.

Setupadmin : اعضای این نقش مجازند پیوندهای سرویس دهنده ها را حذف یا اضافه کنند. همچنین ، روالهای ذخیره شده را اجرا و مدیریت کنند.

Securityadmin : اعضای این نقش میتوانند کاربران را مدیریت کنند.

processadmin: اعضای این گروه می توانند هر فرآیندی را که درSQL اجرا می شود را مدیریت کنند.

Dbcreator : این گروه مجوز ایجاد بانکهای اطلاعاتی در سرویس دهنده را دارد.

Diskadmin : این گروه مجوز ایجاد و مدیریت فایل ها در دیسک را دارد.

Bulkadmin (Bulk Insert Administrators) : این نقش امکان واردات داده ها (Import) از فایل های دیگر را فراهم می کند.

- **مشاهده مجوز های هر رل SqlServer**

```
Sp_srvrolepermission  'sysadmin'
```

تمامی امکانات دسترسی یک عضو Sysadmin را نمایش می دهد.

سطح سوم : تعیین کاربران مربوط به یک بانک اطلاعاتی

هر کدام از کاربران Sqlserver می توانند به عنوان کاربر یک یا چند بانک اطلاعاتی تعیین شوند و در هر بانک اطلاعاتی دارای یک یا چند نقش باشند(**Database Roles**)، که با بر عهده گرفتن هر نقش مجموعه ای از اختیارات را در مورد آن بانک به دست می آورند. برای تعیین کردن یک login به عنوان کاربر بانک اطلاعاتی و دادن نقش ها به آن از صفحه ی user mapping در کادر مشخصات login استفاده می کنیم و با انتخاب کردن یک بانک اطلاعاتی می توان از پایین کادر نقش های مربوط به آن را انتخاب کرد این نقش ها عبارتند:

db-accessadmin

کاربران تعریف شده در این نقش قادر خواهند بود، سطوح دسترسی و امنیتی کلیه کاربران و نقشها را در قسمتهای مختلف پایگاه تعریف کنند.

db-backupoperator

این نقش مسؤول ایجاد نسخههای پشتیبان از سیستم و اطلاعات درون آن است.

db-datareader

این نقش قادر است کلیه اطلاعات تمام جداول بانک اطلاعاتی موجود در سیستم را بخواند .مگر آنکه اطلاعات خاصی توسط مکانیسم Deny از دسترس او دور نگاه داشته شود.

db-datawriter

افراد تعریف شده در این نقش قادرند تا کلیه اطلاعات موجود در کلیه جداول بانک را با استفاده از دستورات سه گانه Delete ، UPdate ، Insert تغییر دهند .مگر آن که جدول یا فیلد خاصی توسط مکانیسم Deny از دسترسشان دور نگه داشته شود.

db-ddladmin

کاربران دارای این نقش می‌توانند ساختار جداول، viewها، روتین‌ها و توابعی که بانک اطلاعاتی را با استفاده از دستورات سه‌گانه Create ، alter ، Drop بسازند، تغییر دهند یا از بین ببرند.

db-denydatareader

این نقش قادر به خواندن هیچ اطلاعاتی از جداول یا سایر قسمتهای بانک نیست.

db-denydatawriter

این نقش قادر به تغییر دادن هیچ یک از قسمتهای بانک اطلاعاتی نیست.

db-owner

این نقش قادر به انجام هر عملی در بانک اطلاعاتی میباشد و بالاترین سطح موجود در یک بانک است.

db-securityadmin

مسئول تعریف و تنظیم نقشها، کاربران و سطوح دسترسی در یک بانک است.

public

کاربران این نقش قادرند تمام جداول، دیدها و سایر قسمتهایی که توسط خودشان یا توسط کاربران متعلق به نقش dbowner ساخته شده را بخوانند و بنویسند.

- **مشاهده مجوز های هر رل Database**

برای اینکه بدانید هر نقش چه مجوزی دارد می توان از روال سیستمی زیر استفاده نمود.

sp_dbfixedrolepermission 'db_owner'

سطح چهارم :تعیین مجوزها برای هر کدام از اشیا

هر کدام از کاربران بانک اطلاعاتی می توانند به هر جدول یا اجزای دیگر آن دسترسی محدود داشته باشند به عنوان مثال می توان تعیین کرد که کاربر خاصی از بانک اطلاعاتی مجوز درج، حذف، اصلاح و....داشته باشد یا نداشته باشد. برای تعیین این مجوز ها از صفحه ی permissions در کادر مشخصات جدول استفاده می کنیم.

- ***راست کلیک روی جدول سپس Propertice و بعد روی سربرگ Permissions کلیک نمایید.***

دستور کار: ۱ - خروجی هر یک از مثال های زیر را مشاهده و در گزارش خود بنویسید.

۲ – تمرین ها را انجام داده و خروجی آن را مشاهده و در گزارش خود بنویسید.

تعریف کاربر جدید:

۱- ایجاد کاربر Amin بارمز عبور ۷۷

```
Sp_addlogin   'Amin','77'
```

نکته : *فقط مدیر سیستم می تواند این روال را اجرا نماید .*

۲ - تغییر رمز عبور(با اجرای این روال رمز عبور برای Amin به '123' تغییر می کند.)

```
Sp_password  '77'  , '123' , 'Amin'
```

نکته : *هرکاربر می تواند رمز خود را تغییر دهد. مدیر سیستم می تواند رمز همه کاربران را تغییر دهد.*

۳- اتصال کاربر به پایگاه داده

نکته : *ابتدا پایگاه داده خود را Use کنید.*

```
Use Employee
Go
Sp_grantdbaccess   'Amin'
```

نکته: *در SqlServer هر پایگاه داده به صورت پیش فرض دارای دو کد کاربری dbo و guest می باشد .*

۴ - قطع دسترسی یک کاربر به پایگاه داده

```
Sp_revokedbaccess   'Amin'
```

۵ - حذف کاربر

```
Sp_droplogin   'Amin'
```

(در صورت حذف کاربر Amin مجددا آنرا اضافه نموده و به پایگاه داده خود متصل نمایید.)

اتصال یک کاربر و یا گروه کاربران Windows به Sqlserver و پایگاه داده

می توانیم کاربران ویندوز را به سرور و پایگاه داده متصل کنیم و برای آن ها سطح دسترسی تعریف کنیم.

Sp_grantlogin 'نام کاربر\اسم کامپیوتر'

قطع ارتباط یک کاربر و یا گروه کاربران Windows با SqlServer

Sp_denylogin ' نام کاربر\ اسم کامپیوتر'

تمرین۱:

- کاربر Dbuser2 را به کاربران Windows اضافه نمایید.
- کاربر Dbuser2 را به کاربران SqlServer اضافه نمایید.
- کاربر Dbuser2 را به پایگاه داده خود متصل نمایید.
- دسترسی کاربر Dbuser2 را به پایگاه داده خود قطع نمایید.
- دسترسی کاربر Dbuser2 را به SqlServer قطع نمایید.

مشاهده اطلاعات مربوط به کاربران در پایگاه داده

Sp_helpuser

اختصاص Role به کاربران SqlServer

برای انجام مثال های زیر چنانچه کاربر Amin را حذف نموده اید مجددا آن را ایجاد نمایید.

۱- اختصاص رل Sysadmin به کاربر Amin

Sp_addsrvrolemember 'Amin' , 'sysadmin'

نکته : *برای مشاهده اعضای Sysadmin روی رل Sysadmin دو بار کلیک نمایید. مشاهده می کنید که با اجرای این روال کاربر Amin به رل Sysadmin اضافه شد.*

نکته: *روی کاربر Amin دو بار کلیک نمایید در سربرگ Server Roles رل اختصاص داده شده به کاربر Amin را مشاهده می کنید.*

۲ - قطع یک نقش یا رل از کاربر

Sp_dropsrvrolemember 'Amin', 'sysadmin'

تمرین۲:

- رل Dbcreator را به کاربر Amin اختصاص دهید.
- رل sysadmin را از کاربر Amin بگیرید.

مجوز های کاربر روی پایگاه داده

۱- تعیین سطح دسترسی روی پایگاه داده

با استفاده از دستور**Grant** میتوان برای کاربران مجوز های پایگاه داده را تعریف نمود و با استفاده از دستور **Deny** مجوزها از کاربران گرفته می شود.

Grant create table , backup database , create procedure to Amin

نکته : *روی پایگاه داده خود راست کلیک نمایید سپس Propertice و بعد روی سربرگ Permissions کلیک نمایید. مجوز هایی که هر کاربرمی تواندروی پایگاه داده داشته باشد را ملاحظه می کنید.*

تمرین ۳ : مجوز ایجاد Procedure را از کاربر *Amin* بگیرید.

۲- تعیین سطح دسترسی روی جدول

با استفاده از دستور**Grant** میتوان برای کاربران مجوز هایی روی جداول پایگاه داده را تعریف نمود.

Grant Select , insert on spec to Amin with Grant option

نکته : *عبارت with Grant option وقتی استفاده می شود که به کاربر مجوزی داده شود و کاربر بتواند آن دسترسی را به دیگر کاربران موجود در این پایگاه داده واگذار نماید.*

نکته : *روی جدول spec راست کلیک نمایید گزینه Propertice و سپس روی سربرگ Permission کلیک نمایید، تمامی مجوزهایی که هر کاربر ممکن است روی جدول داشته باشد را مشاهده می کنید.*

تمرین ۴ : به کاربر Amin مجوز اجرای پروسیجر addprice بدهید.

- اعطای این مجوز را در کدام قسمت مشاهده نماییم؟

۳- تعیین سطح دسترسی روی ستون ها

با استفاده از دستور**Grant** میتوان برای کاربران مجوز هایی روی ستون های جداول پایگاه داده را تعریف نمود.

Grant Update on project(price) to Amin

نکته : *روی جدول Project راست کلیک نمایید گزینه Propertice و سپس دکمه Permission را کلیک نمایید و سپس دکمه Columns را کلیک نمایید ، تمامی مجوزهایی که هر کاربر ممکن است روی ستون های جدول داشته باشد را مشاهده می کنید.*

نکته : *تمامی روال های استفاده شده Store Procedure می باشند که در پوشه System Store Procedure ذخیره شده اند.*

تمرین ۵ : تمرین زیر را روی دیتابیس کتابخانه انجام دهید.

۱) کاربر Hamed و Hamid را ایجاد نمایید .

۲) کاربر Hamed و Hamid را به پایگاه داده **LIbrary** متصل نمایید.

۳) به کاربران Hamed و Hamid مجوزهای ایجاد Table و ایجاد Procedure بدهید.

۴) به کاربران Hamed و Hamid مجوزهای Update و Delete روی جدول Member بدهید.

۵) به کاربر Hamid امکان Update روی ستونهای Borrowed_From و Borrowed_To از جدول Borrower بدهید.

۶) از کاربر Hamed امکان Update روی ستون Book_Title از جدول Book را بگیرید.

کار روی پروژه:

۱- در فرم اول پروژه ترتیبی اتخاذ نمایید که از یک کاربر sql استفاده شود وبا ورود نام کاربر و رمز عبور صحیح فرم دوم باز شود.

۲- در قسمت امکانات گزینه های " اضافه نمودن کاربر جدید" و "تغییر رمز کاربران" اضافه شود.