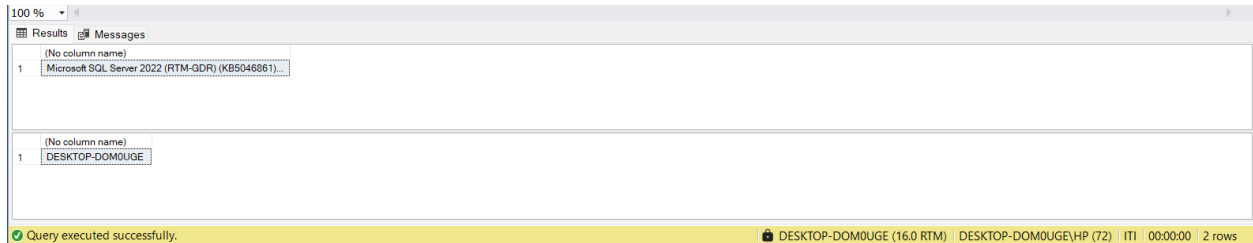


Display results of the following two statements and explain what is the meaning of @@AnyExpression

```
select @@VERSION  
select @@SERVERNAME
```



The screenshot shows the SQL Server Enterprise Manager interface. The top bar indicates 100% zoom. Below the toolbar, there are two tabs: 'Results' and 'Messages'. The 'Results' tab is active, displaying two query results. The first query, 'select @@VERSION', returns a single row with the value 'Microsoft SQL Server 2022 (RTM-GDR) (KB5046861)'. The second query, 'select @@SERVERNAME', returns a single row with the value 'DESKTOP-DOM0UGE'. The status bar at the bottom indicates 'Query executed successfully.' and '2 rows'.

	(No column name)
1	Microsoft SQL Server 2022 (RTM-GDR) (KB5046861)

	(No column name)
1	DESKTOP-DOM0UGE

Query executed successfully. | DESKTOP-DOM0UGE (16.0 RTM) | DESKTOP-DOM0UGE\HP (72) | ITI | 00:00:00 | 2 rows

- 1- اول حاجة ال version بيعرض الإصدار اللي شغال عليه دلوقتي على الجهاز انه مثلا Microsoft sql server 2022
- 2- ثاني حاجة ال server اللي مشبك عليه دلوقتي من الجهاز نفسه يعني الجهاز نفسه شغال ع أي سيرفر حاليا

Report

1- ايه هو الClass Digram

ويستخدم في تصميم UML (Unified Modeling Language) هو نوع من أنواع مخططات **Class Diagram** الـ (OOP - خاصة في البرمجة الكائنية) البرامج.

تعريف بسيط

Class Diagram (attributes) في النظام، ويوضح العلاقات بينها، والخصائص (classes) هو رسم يبين الكلاسات (methods) والوظائف التي جوا كل كلاس.

بيتكون من ايه؟

بيتعرض كـ "صندوق" فيه 3 أقسام **Class** كل

scss
CopyEdit

الاسم (Class Name)	الكلاس
الخصائص (Attributes)	
الدوال (Methods/Operations)	

مثال بسيط

Class: student

pgsql
CopyEdit

Student
- id: int - name: string - age: int
+ register() + login()

- **private** يعني الخاصة -
- **public** يعني الوظيفة +

أنواع العلاقات بين الكلاسات

العلاقة	معناها	مثال
Association	علاقة عامة	طالب يدرس في جامعة
Aggregation	جزء من - لكن مش مملوك	قسم يحتوي على طلاب
Composition	جسم الإنسان يحتوي على قلب جزء من - ومملوك	
Inheritance	كلاس يرث من كلاس ثاني (وراثه)	User يرث من Admin

بيستخدم إمتى؟

- وانت بتصمم نظام كبير قبل ما تكتب كود
- لو بتعمل تحليل أو توثيق لنظام مبرمج بـ OOP زي (Java, C#, Python OOP)
- في المشاريع الجامعية والتقارير الفنية

أدوات ترسم بيها Class Diagram

- draw.io
- StarUML
- Lucidchart
- Visual Paradigm

2- ايه هو ال build in stored presedure

SQL Server في Built-in Stored Procedure يعني ايه

SQL جاهزة ومعمولة مسبقاً من قبل (stored procedures) هي إجراءات مخزنة Built-in Stored Procedures نفسها، وموجودة جوه النظام Server.

يعني بدل ما تكتب كود من الصفر، تقدر تستخدم واحدة من دول علشان تتفقد أو تستعلم أو تتحكم في حاجة في الداتا بيز.

Built-in Stored Procedures: أمثلة مشهورة على ✂

وظيفته	الإجراء
يعرض معلومات عن جدول أو فيو أو كائن معين	sp_help
في جدول معين (columns) يعرض معلومات الأعمدة	sp_columns
يعرض كود الإجراء المخزن أو الفانكشن	sp_helptext
يغير اسم جدول أو عمود	sp_rename
يعرض أسماء قواعد البيانات	sp_databases
يعرض كل الجداول في قاعدة البيانات	sp_tables
يعرض معلومات عن المستخدمين المتصلين	sp_who
locks يعرض معلومات عن الـ	sp_lock
يعرض الكائنات اللي بتعتمد على كائن معين	sp_depends

✂ مثال عملي:

1. sp_help

```
sql
CopyEdit
EXEC sp_help Employees;
```

Employees. يعرض كل المعلومات عن جدول

2. sp_rename

```
sql
CopyEdit
```

```
EXEC sp_rename 'Employees.Address', 'EmpAddress', 'COLUMN';
```

EmpAddress إلى Employees في جدول Address بـ تغيير اسم العمود

3. sp_helptext

GetEmployees اسمها stored procedure لو عندك

```
sql
CopyEdit
EXEC sp_helptext 'GetEmployees';
```

دي procedure يعرض كود الـ

💡 Built-in procedures? ليه نستخدم الـ

- توفر وقت
 - تريحك من كتابة استعلامات معقدة
 - بتسهل إدارة قواعد البيانات
-

⚠️ ملحوظة:

sp_ بيبدأوا بـ built-in stored procedures كل الـ

SQL Injection؟ يعني إيه

وَيَدْخُلُ فِيهِ بَيَانَاتُ مِنَ الْمُسْتَعْمَلِ مِنَ SQL بِتَحْصُلِ لَمَّا الْمَبْرَمَجُ يَكْتُبُ كُودَ (vulnerability) هِيَ ثَغْرَةٌ SQL Injection. جُوهُ الْبَيَانَاتِ SQL كُودَ (inject) غَيْرِ مَا يَحْمِيهَا، فَالْمَخْتَرَقُ يَقْدَرُ يَحْقِنَ.

يَكْسِرُ الْقَاعِدَةَ أَوْ يَسْرِبُ بَيَانَاتِ SQL يَعْنِي بَدَلَ مَا الْمُسْتَعْمَلُ يَدْخُلُ اسْمَ، يَدْخُلُ كُودَ.

□ مثال واقعي:

تُخِيلُ إِنَّكَ عَامِلُ صَفْحَةٍ تَسْجِيلِ دُخُولِ، وَالْكَودُ دِهْ هُوَ الَّذِي بِيَشْتَغَلُ وَرَا الْكُوَالِيْسَ:

```
sql
CopyEdit
SELECT * FROM Users WHERE username = 'userInput' AND password = 'passInput';
```

(أَوْ غَيْرُهُ PHP أَوْ C# فِي) وَإِنْتَ بَتَنْقُذَ الْكَودَ دِهْ كَدِهْ:

```
sql
CopyEdit
string query = "SELECT * FROM Users WHERE username = '" + username + "' AND password = '" + password + "'";
```

لَوِ الْهَآكِرُ كَتَبَ بَدَلَ الْإِسْمِ:

```
sql
CopyEdit
' OR '1'='1
```

يَبْقَى الْكَودُ الْنَهَائِي بَقِيَ كَدِهْ:

```
sql
CopyEdit
SELECT * FROM Users WHERE username = '' OR '1'='1' AND password = ''
```

🔒 والنّتيّة؟: هِيَعْدِي الدُّخُولَ حَتَّى لَوْ مَشَّ عَارَفَ الْبَاسُورْدَ ✓

🔒 SQL Injection: أخطر ما في

- يَقْدَرُ يَعْدِي دُخُولَ مِنْ غَيْرِ كَلِمَةٍ سِرِّ
- يَقْدَرُ يَمْسَحُ جَدَاوِلَ

- يقدر ياخذ نسخة من كل الداتا (سرقة بيانات)
- يقدر يوقف النظام بالكامل

🛡️ □ إزاي نحمي نفسنا؟

1. ✔️ **parameterized queries** استخدم
 - في Java PreparedStatement أو في C# مع SqlCommand زي
2. ✔️ **ORM** استخدم زي Entity Framework
3. ✔️ **Sanitization** فلتر البيانات المدخلة من المستخدم
4. ✔️ **SQL** اقلل صلاحيات حساب الـ

✔️ C#: مثال حماية باستخدام

```
csharp
CopyEdit
SqlCommand cmd = new SqlCommand("SELECT * FROM Users WHERE username =
@username AND password = @password", connection);
cmd.Parameters.AddWithValue("@username", usernameInput.Text);
cmd.Parameters.AddWithValue("@password", passwordInput.Text);
```

كده حتى لو حد كتب كود خبيث، هيتعامل كأنه نص عادي مش كود.

🚀 الخلاصة:

🌟 SQL Injection

🛡️ □ الحل

parameterized queries استخدم ثغرة بسبب دمج البيانات مع الكود مباشرة
فلتر البيانات وتقليل الصلاحيات بتسمح للمهاجم يعدل أو يسرّب أو يمسح بيانات
