Mastering Dynamic SQL

Deborah Melkin
(she\her)
SQL Saturday NYC
May 6, 2023

SQL Saturday New York City 2023

A BIG Thank You to our Sponsors

Platinum

Exelegent

Microsoft

solarwinds

SIOS

Gold

Quest

Bronze

QAssociates
EST. 1992

redgate

About Me

MVP

FEATURED IN THE redgate 100 MOST INFLUENTIAL IN THE DATABASE COMMUNITY 2022 redgate

- 20+ years as a DBA
- NESQL Board Member
- Azure Data Community Advisory Council
- Co-Founder, WITspiration
- Speaker Idol Winner 2019
- Idera ACE, Class of 2020
- #Redgate100
- Microsoft MVP – Data Platform

About Me

- Alto section leader in my choir.
- Pick at bluegrass jams regularly.
- Learning guitar and neglecting mandolin.
- Musical theater geek.
- My husband and I take pictures of our dog doing geeky things.

MVP

FEATURED IN THE
redgate
100
MOST INFLUENTIAL
IN THE DATABASE
COMMUNITY 2022
redgate

“ Q: What is Dynamic SQL?

A: SQL batches that are created ad hoc and executed.

Agenda

- Use Cases
- Security
- Syntax
- Demos
- Tips & Tricks

“ Use Cases

When to Use

- “Catch All” Queries
- Client Customized Queries
- Variables for server, database, or object names
- Delay parsing of query

“Catch-All” Queries

- A single query that tries to account for all options available.
- Sample syntax:

```
WHERE (VIN = @vin OR @vin IS NULL)
AND (BaseModelID = @BaseModelID OR
@BaseModelID IS NULL)
AND (PackageID = @PackageID OR
@PackageID IS NULL)
AND (TrueCost = @TrueCost OR @TrueCost
IS NULL)
AND (InvoicePrice = @InvoicePrice OR
@InvoicePrice IS NULL)
```

Client Customized Queries

- Application has screens that display data based on what clients choose.
- Example:
  - Dealership A wants
    - VIN
    - True Cost
    - Invoice Price
  - Dealership B wants
    - VIN
    - Base Model Name
    - Package Name
    - MSRP

Variables for Static Info

- Allows variables to be used to specify parts of the query that can't otherwise accept variables
- Example:

```
SELECT *
FROM @database.dbo.Inventory
```

```
DECLARE @database sysname =
'AutoDealershipDemo',
@sql nvarchar(max)
```

```
SELECT @sql = 'SELECT *
FROM ' + quotename(@database) +
'.dbo.Inventory'
```

Delay Parsing

- Moves the parsing of the query to run-time execution to avoid errors or allow for better error handling.
- Example:

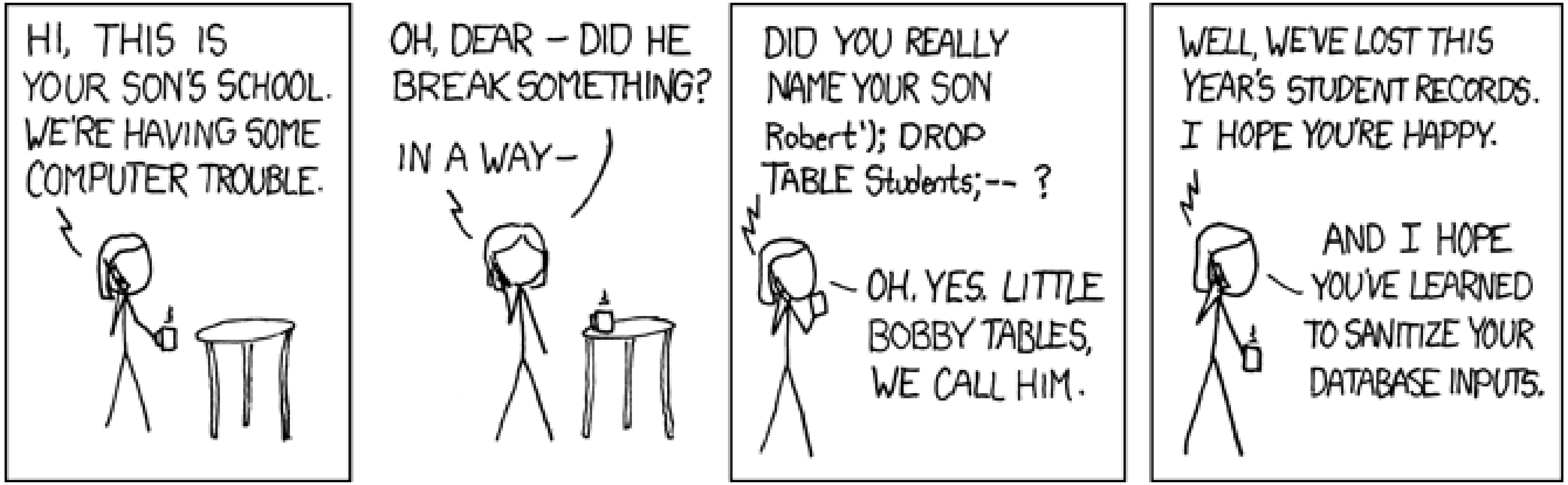
```
SELECT UpgradeTestID, StaticColumn,
DropThisColumn
FROM DynamicSQL.UpgradeTestTable

ALTER TABLE DynamicSQL.UpgradeTestTable
DROP COLUMN DropThisColumn
GO 2
```

“ Security & Vulnerabilities

Protect Against SQL Injection

- Dynamic SQL can be vulnerable to SQL Injection if you don’t code against it.
- xkcd.com: "Little Bobby Tables"


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

“ Syntax

Ways to Write Dynamic SQL

- EXEC (@sql)

- EXEC sp_executesql @sql
  - ★ Allows for parameters to be passed in and out of the statement

- EXEC sp_MSforeachdb @sql
  - Not documented or officially supported

> “ **At this point, I could talk about it or show you….**

Demo Time!

“ Tips & Tricks

Tips & Tricks

- Add `@debug bit = 1` to your procs
- Validate your parameters
- Use quotename for your objects
- Add error handling
- Performance tune the created statement like you would any other SQL in your codebase
    - You are just creating the different versions of the SQL to run.

Resources

- Tara Kizer – EXEC vs sp_executesql
- Tim Ford - Run same command on all SQL Server databases without cursors
- Eitan Blumin - Simplest Alternative To sp_msforeachdb
- Aaron Bertrand - Making a More Reliable and Flexible sp_MSforeachdb

Resources (cont’d)

- Deborah Melkin –
  - Dynamic SQL, Sessions, and Execution
  - Openrowset Dynamic SQL Error Handling
- From Microsoft documentation:
  - sp_executesql

Have more Qs?

- **Email:** dgmelkin@gmail.com
- **Twitter:** @dgmelkin
- **Mastodon:** dataplatform.social/@dgmelkin
- **Blog:** DebtheDBA.wordpress.com
- **Github:** https://github.com/DebtheDBA/MasteringDynamicSQL

“ Thanks for coming!