

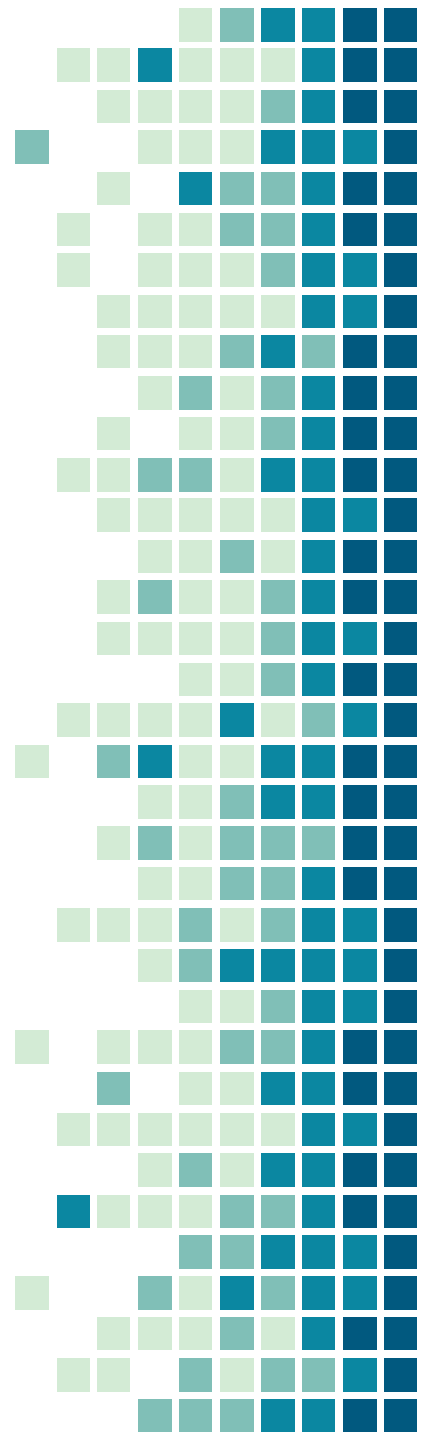
# Mastering Dynamic SQL

- Deborah Melkin
- She\Her
- Data Engineer



# About Me

- 20+ years as a DBA
- Co-Founder, WITspiration
- Speaker Idol Winner 2019
- Idera ACE, Class of 2020
- #Redgate100 (2022)
- Microsoft MVP – Data Platform



# About Me

- Longtime member of the Alto section
- 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.

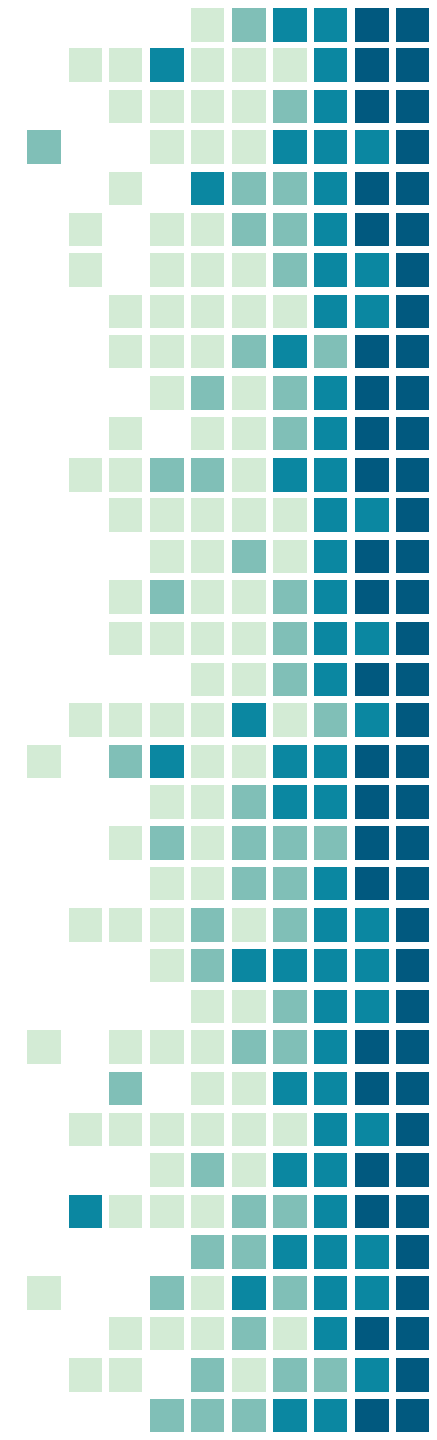


“ Q: *What is Dynamic SQL?*

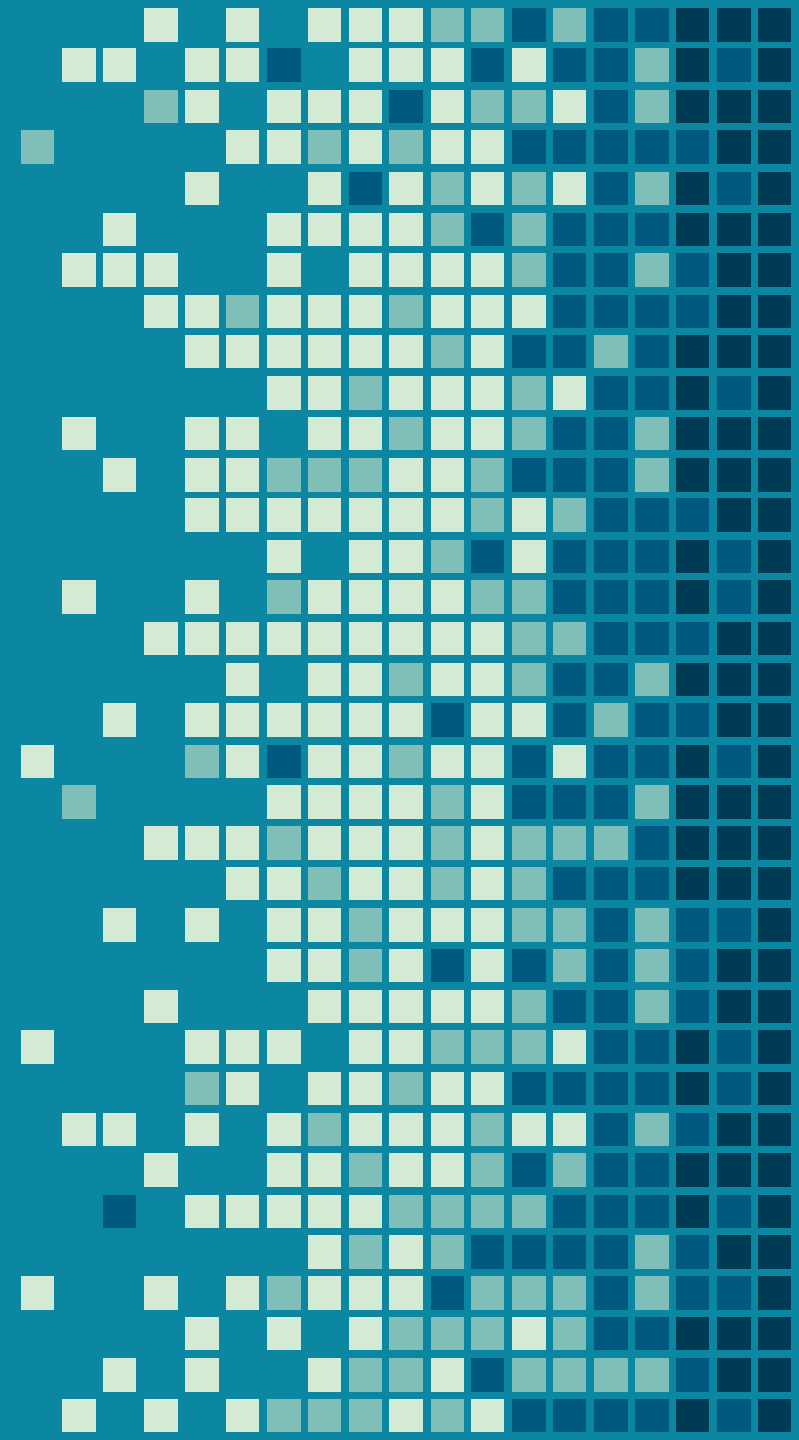
A: *SQL statements that are created ad hoc and executed.*

# Agenda

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

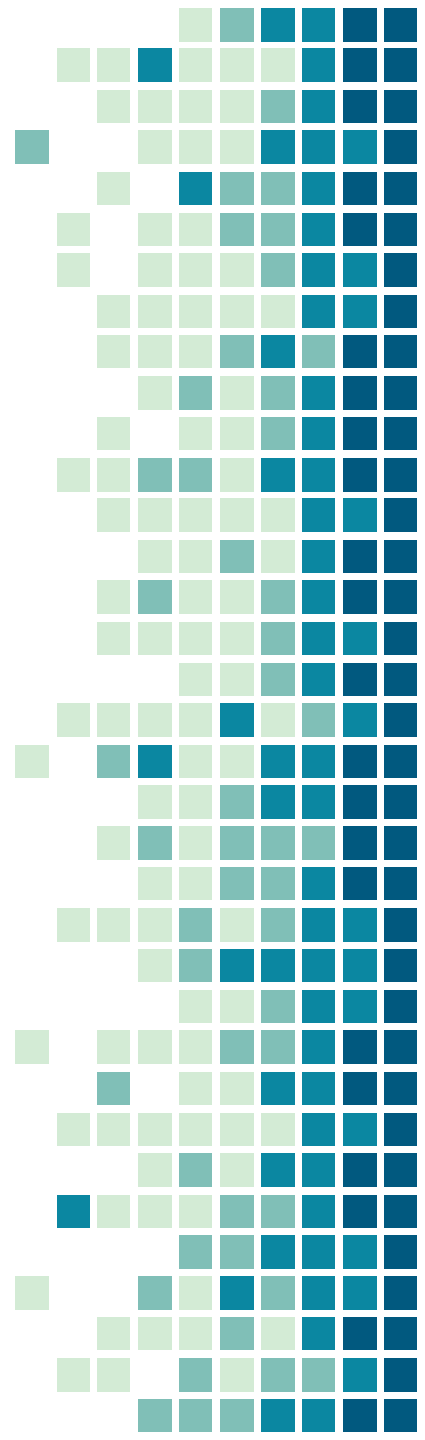


# “ Use Cases



## When to Use

- “Catch All” Queries
- End User 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.

```
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)
```



# End User Customized Queries

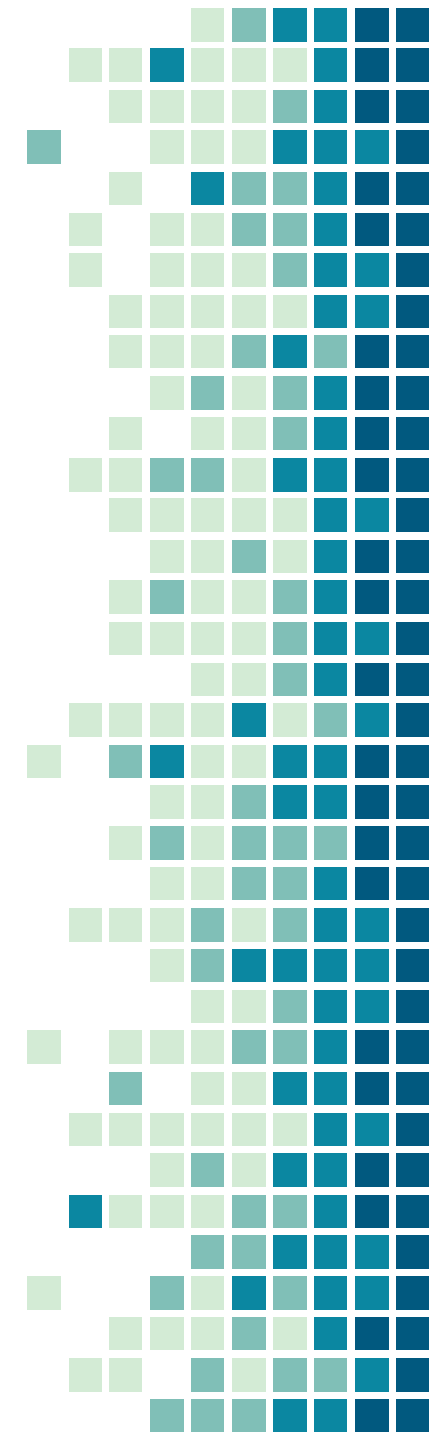
Application has screens that display data based on what clients choose.

- 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.

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

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

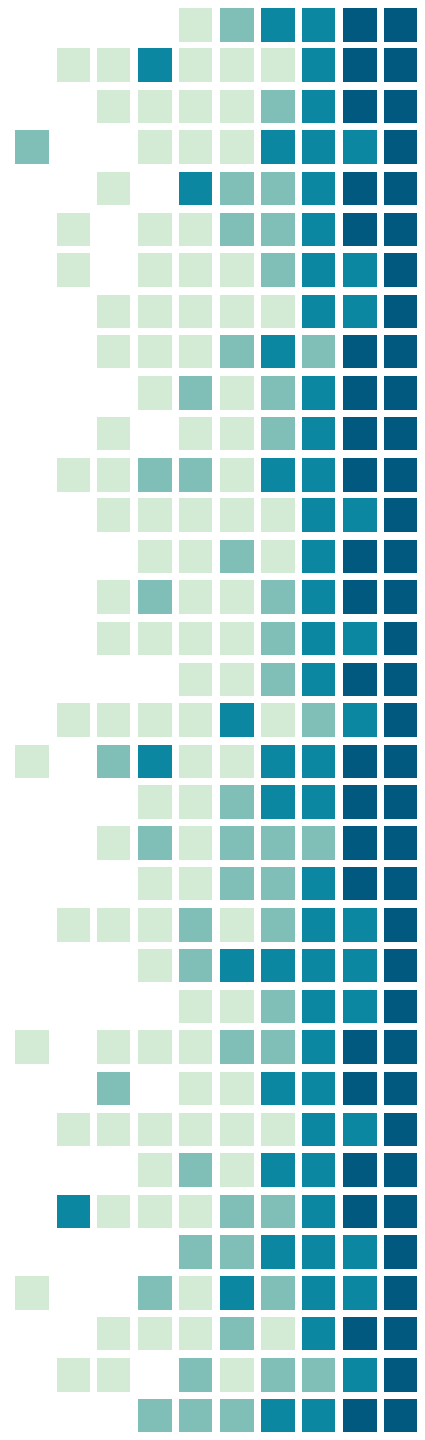
```
SELECT @sql = 'SELECT *  
FROM ' + quotename(@database) + '.dbo.Inventory'
```

# Delay Parsing

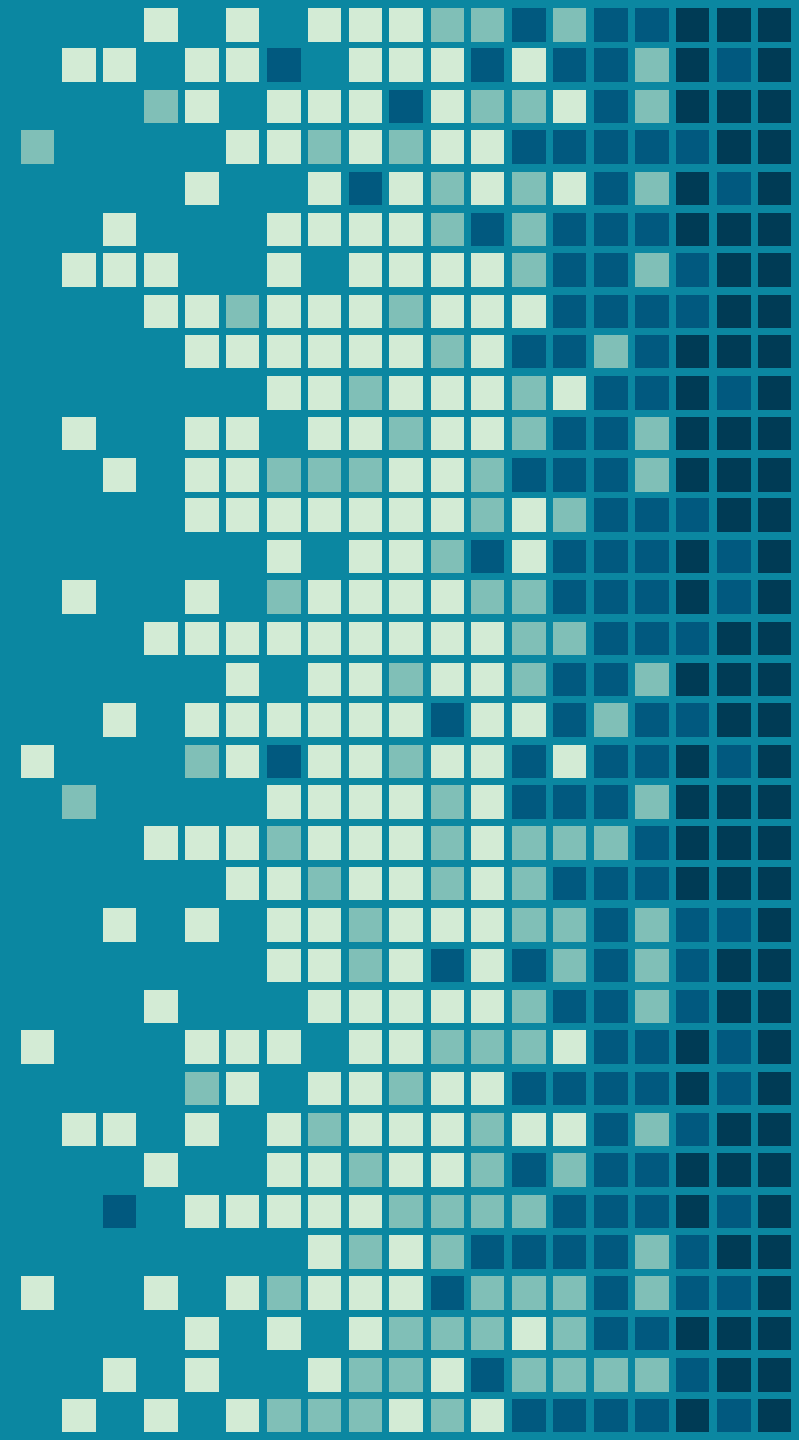
- Moves the parsing of the query to run-time execution to avoid errors or allow for better error handling.

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

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

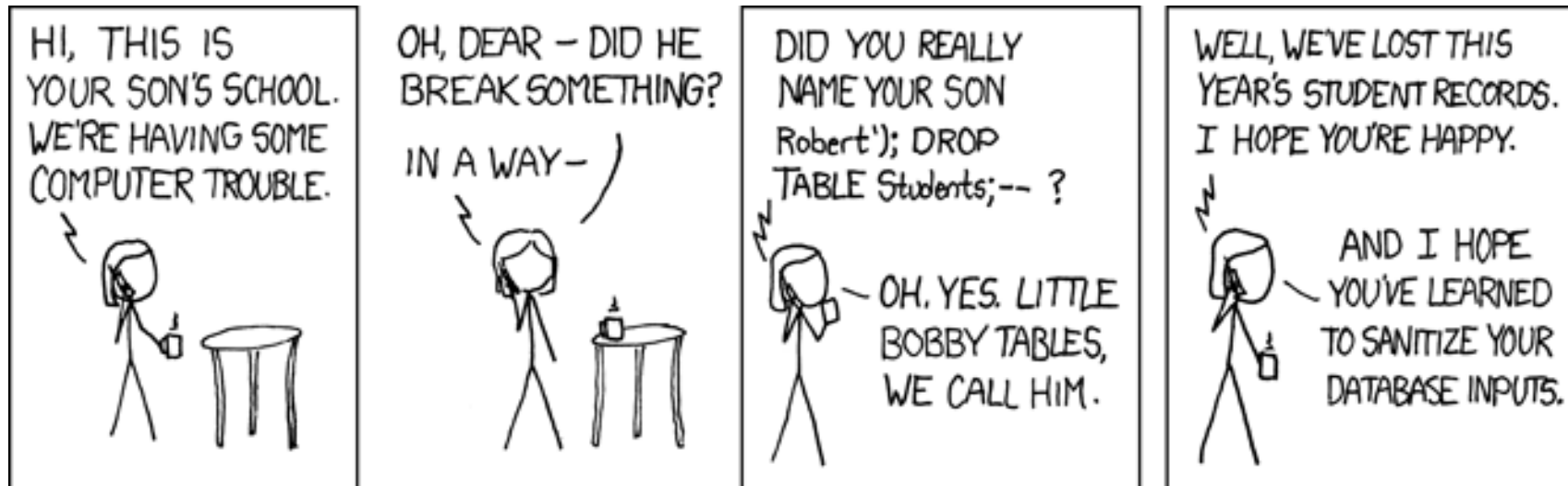


# “ Security & Vulnerabilities

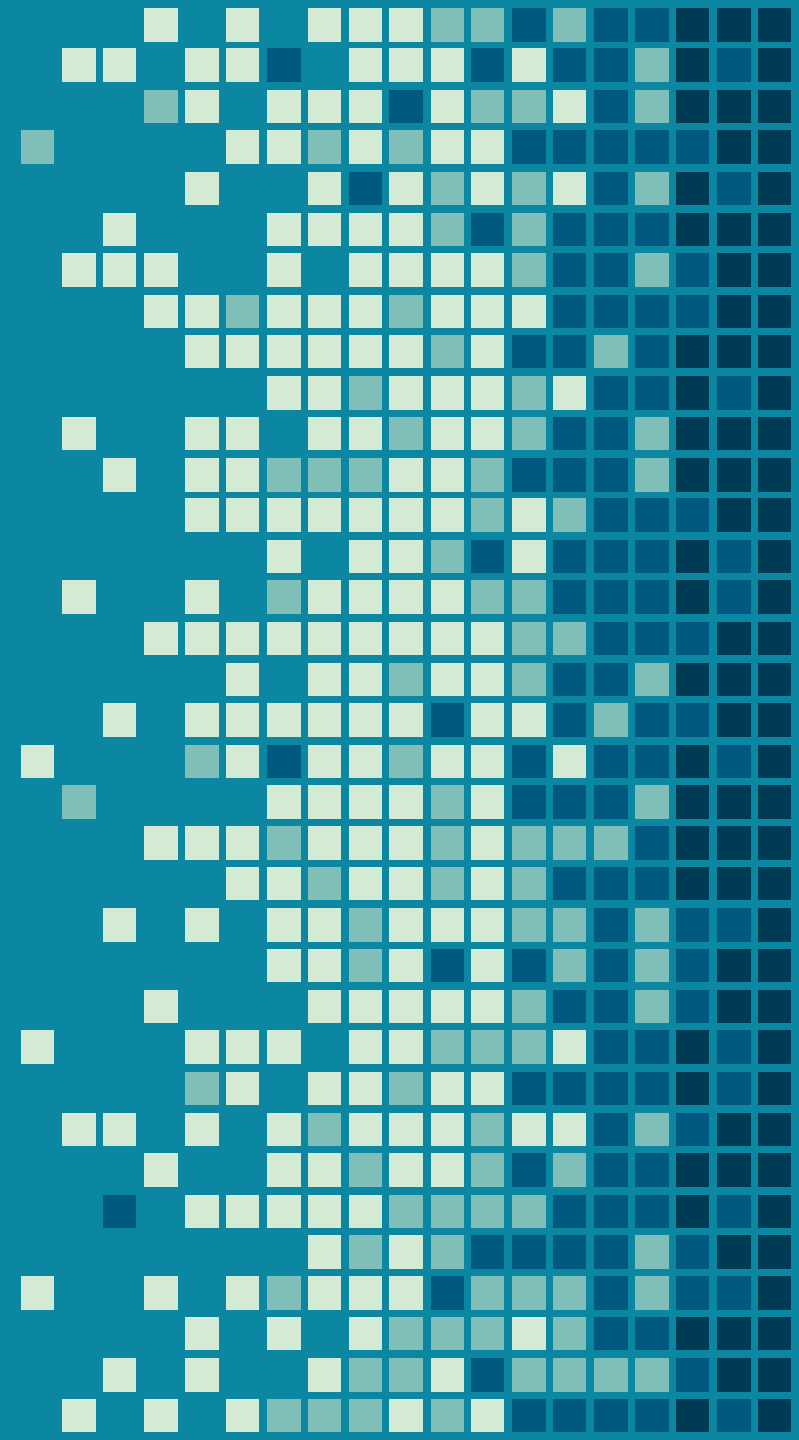


# Protect Against SQL Injection

- Dynamic SQL can be vulnerable to SQL Injection if you don't code against it.
- [xkcd.com](http://xkcd.com): "[Little Bobby Tables](http://xkcd.com/326/)"

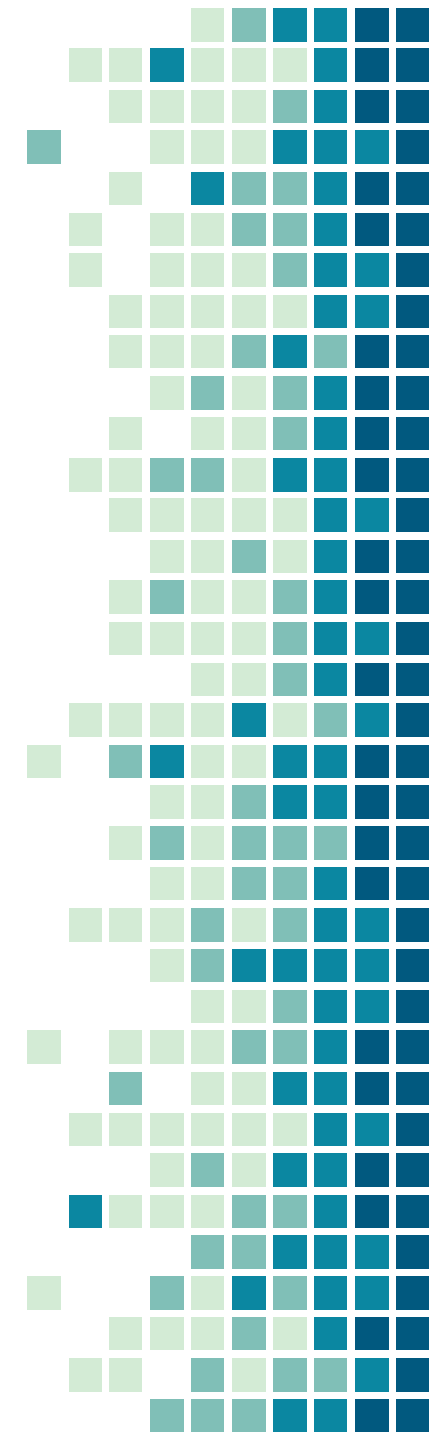


“ *Syntax*



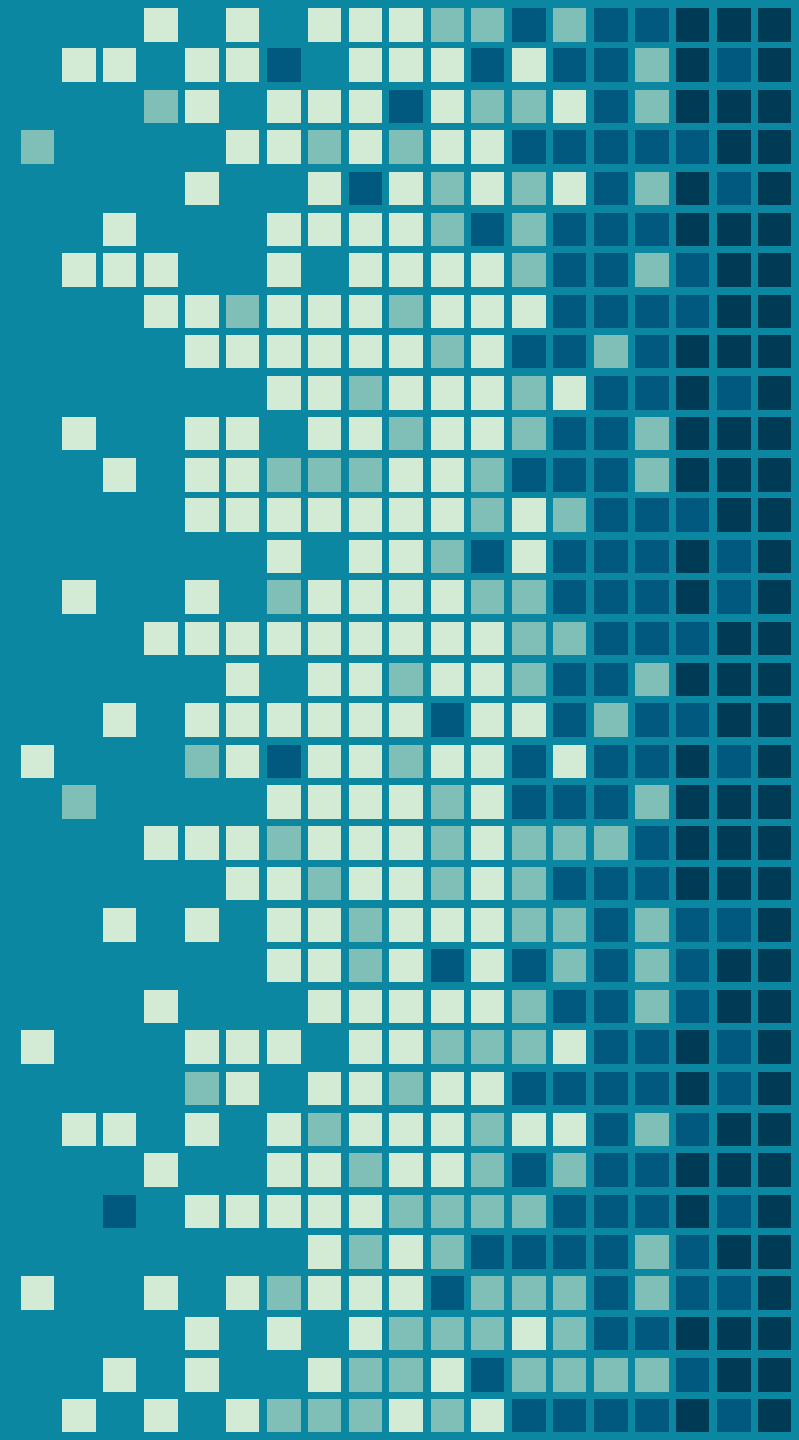
# Ways to Write Dynamic SQL

- 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



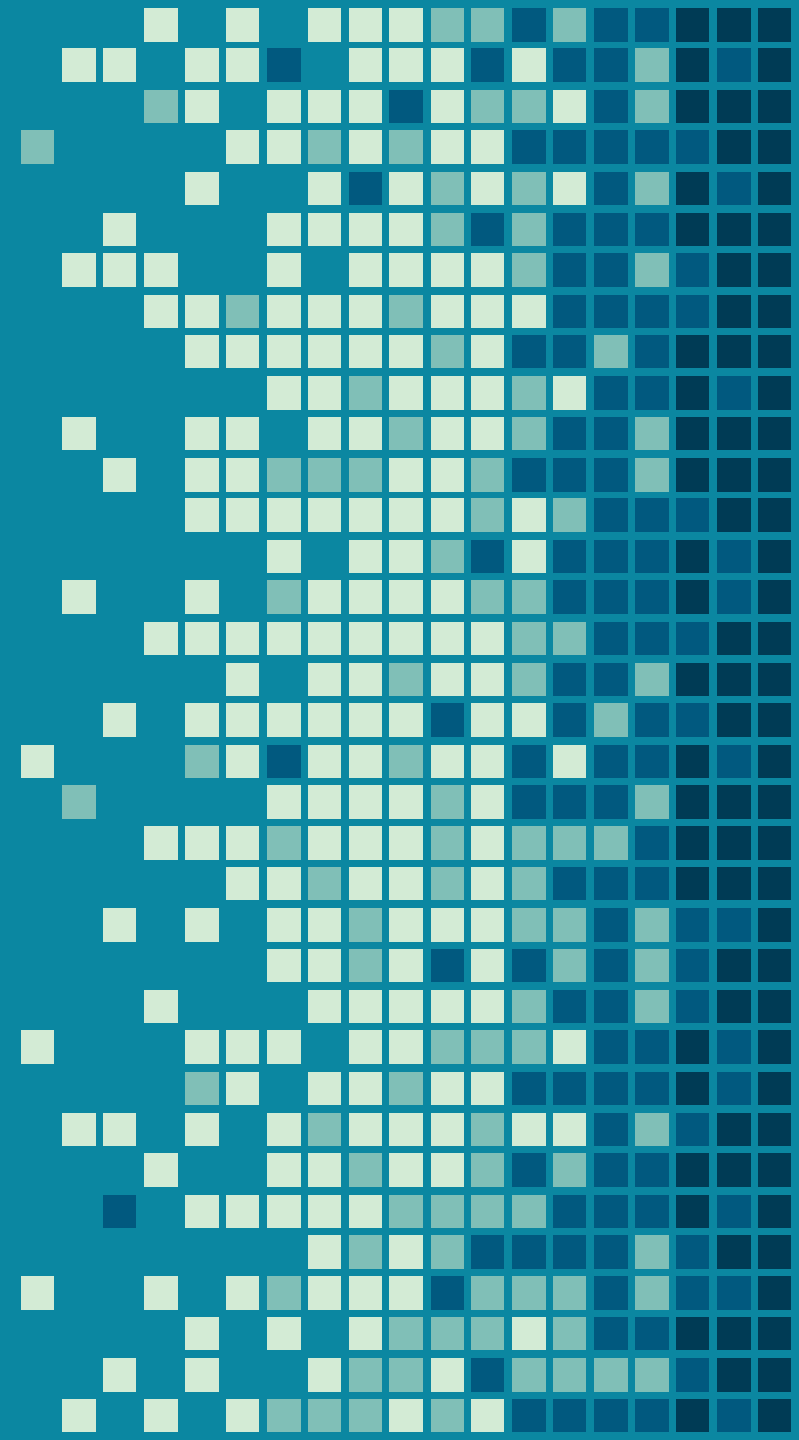
“ *At this point, I could talk  
about it or show you....*

*Demo Time!*



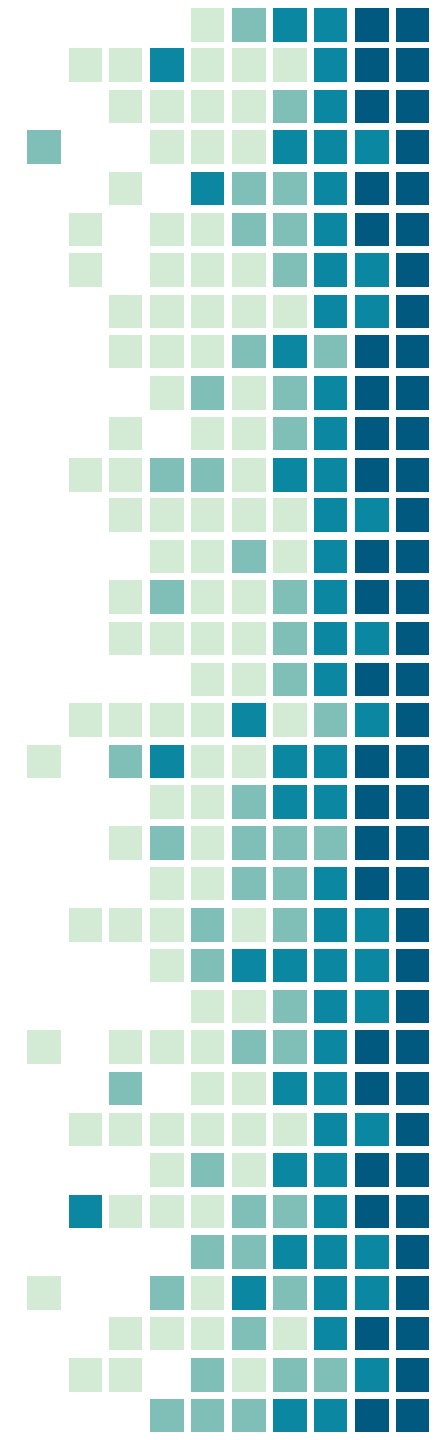


# “ Tips & Tricks



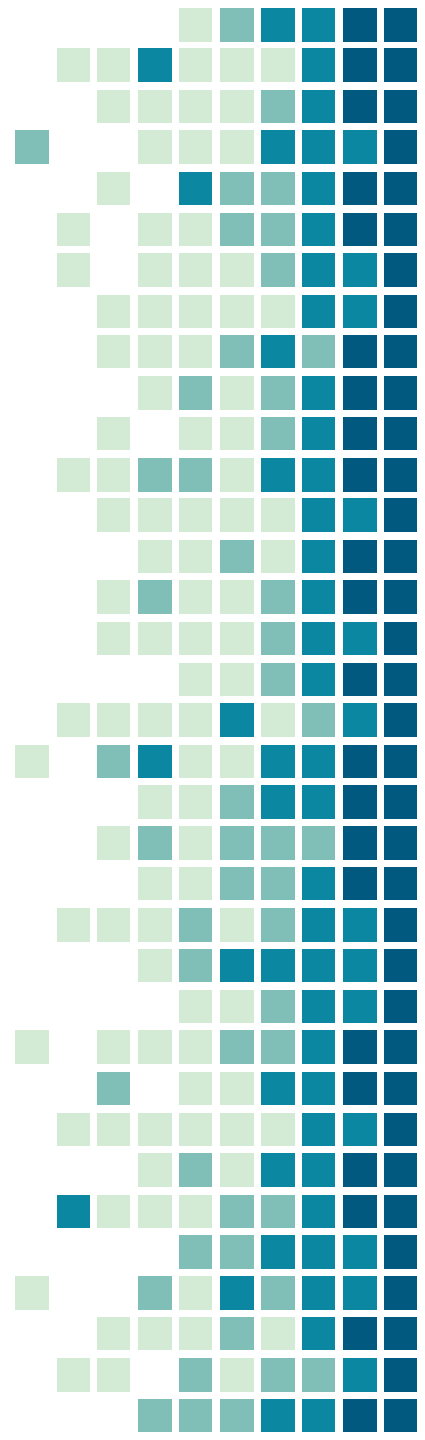
# Tips & Tricks

- Add `@debug bit` to your procs
- Validate your parameters
- Use `QUOTENAME` for your objects
- Add error handling



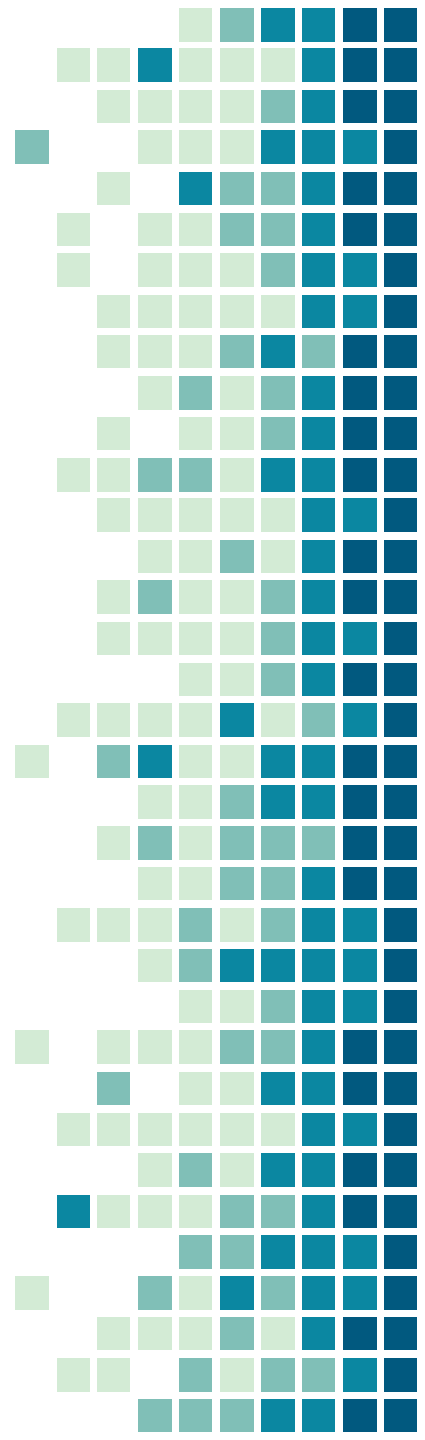
## Tips & Tricks (cont'd)

- 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.



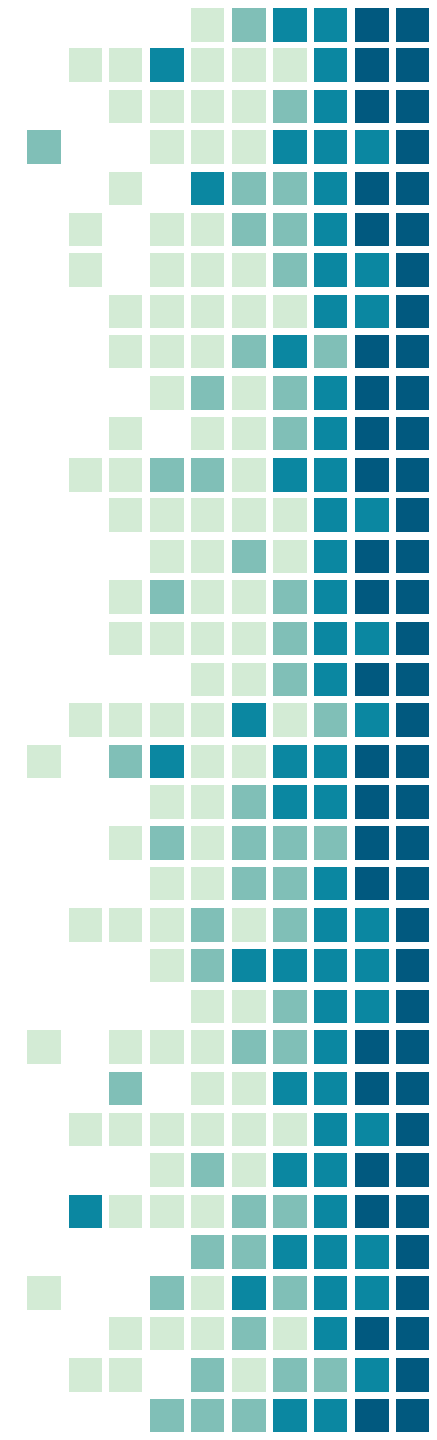
# Resources

- 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](#)



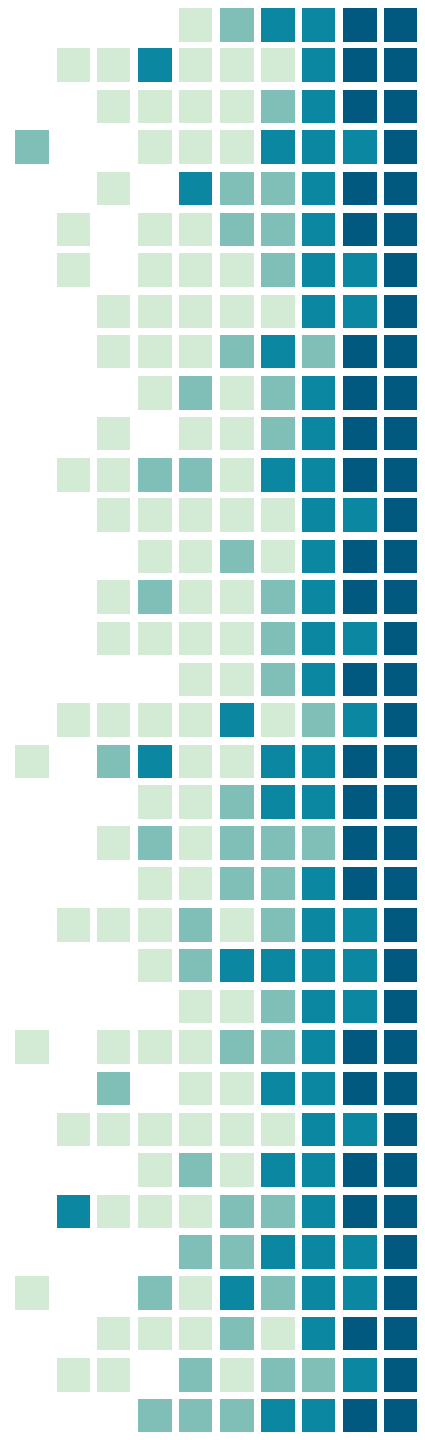
## Resources (cont'd)

- Erland Sommarskog –
  - [The Curse and Blessings of Dynamic SQL](#)
  - [Error and Transaction Handling Part 2](#)
- Kenneth Fisher - [Demystifying Dynamic SQL](#)



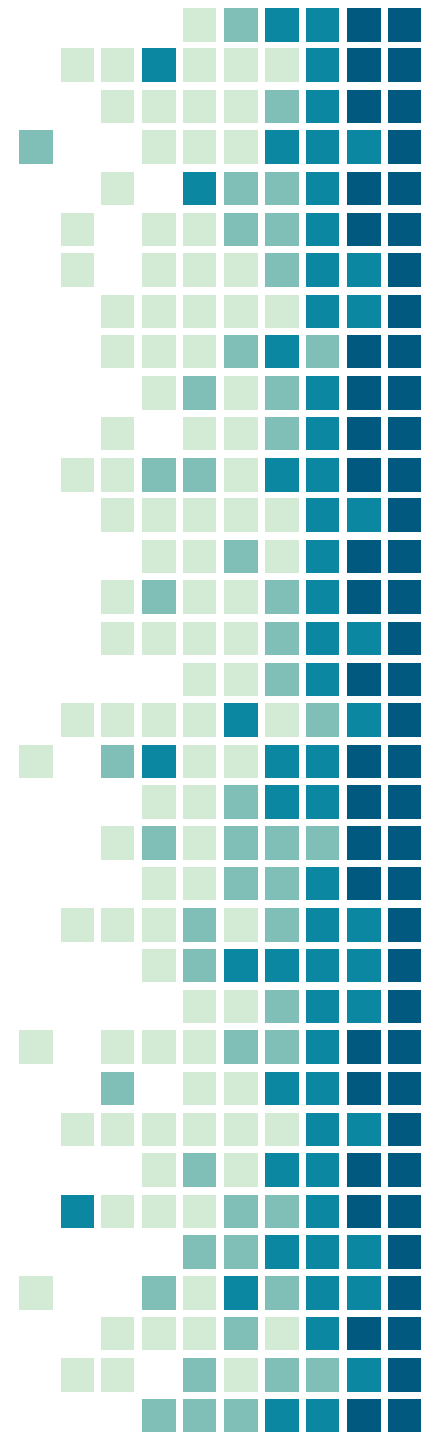
## Resources (cont'd)

- Deborah Melkin –
  - [Dynamic SQL, Sessions, and Execution](#)
  - [Openrowset Dynamic SQL Error Handling](#)
- Microsoft documentation: [sp\\_executesql](#)



# Have more Qs?

- **Email:** [dgmelkin@gmail.com](mailto:dgmelkin@gmail.com)
- **Blog:** [DebtheDBA.wordpress.com](http://DebtheDBA.wordpress.com)
- **Socials:** @dgmelkin (@dataplatfrom.social) (.bsky.social)
- **Github:** <https://github.com/DebtheDBA/MasteringDynamicSQL>



Thanks for coming!

