Jared Kirkpatrick
Principle Consultant @ MMIBC
kirk1880@me.com

ABOUT ME

Principle Consultant @ MMIBC

Member of PASS since 1999

Presenter for several SQL Saturdays

5 X 140.6 Ironman Finisher | 21 X 70.3

12 Gran Fondo / 100 Mile Bike Race

recorded by moewalls.com

PUZZLES FOR TODAY

DBCatch

TIPS

Dynamic SQL
Number Tables

TRICKS

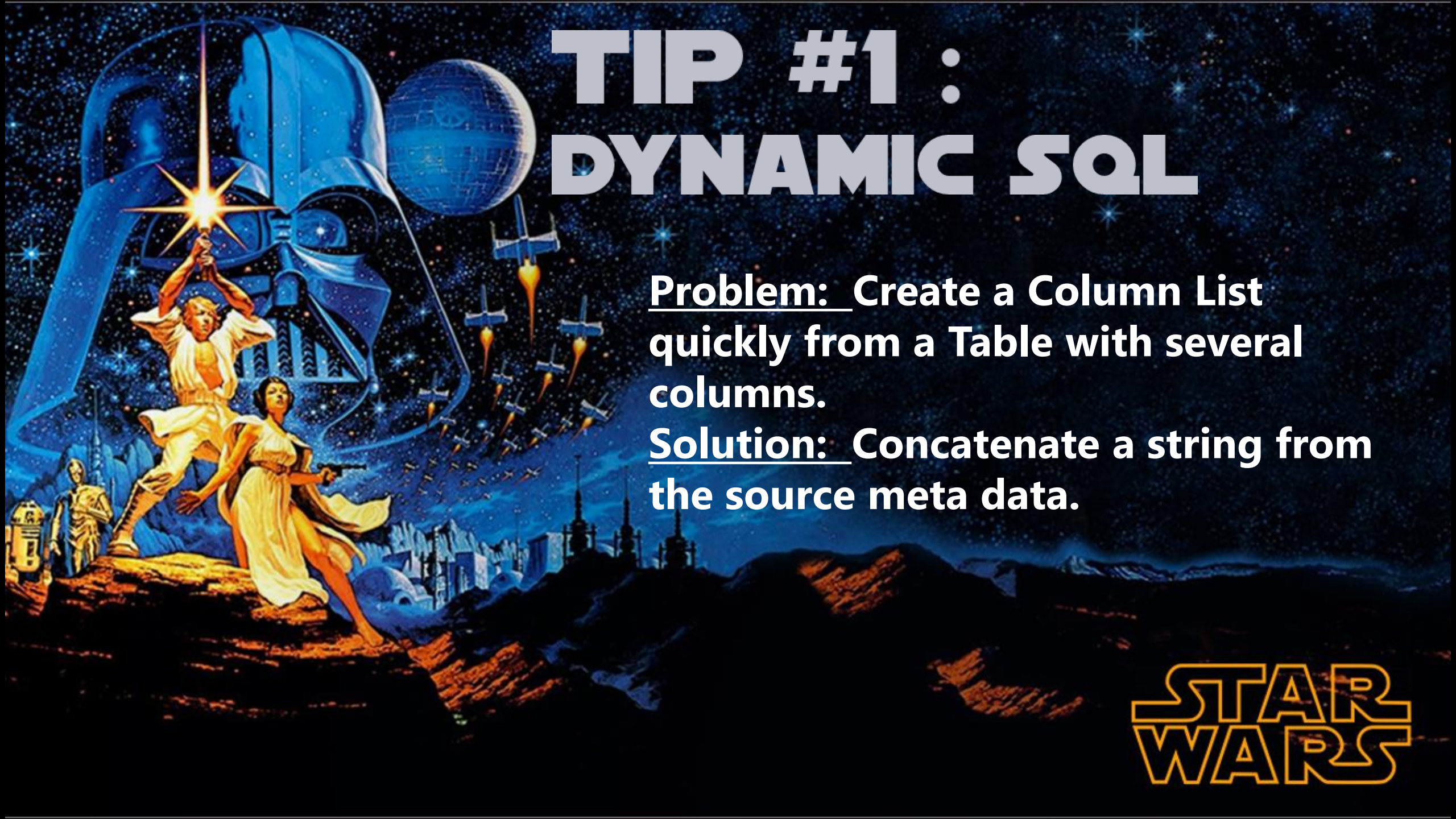
Randomization
Delimiter Splits

HACKS

Delete Dups
Sp_executeSQL

BACKDOORS

Read/Write to the Registry


TIP #1 :
DYNAMIC SQL
Problem: Create a Column List quickly from a Table with several columns.
Solution: Concatenate a string from the source meta data.
STAR WARS

```
DECLARE @v_SQL                  [NVARCHAR](MAX)                 = ''
       ,@v_TBL                  [SYSNAME]                       = 'Dim_Server'
       ,@v_Max                  [INT];

SELECT @v_Max                   = MAX(ORDINAL_POSITION)
  FROM INFORMATION_SCHEMA.COLUMNS
 WHERE TABLE_NAME               = @v_TBL;

SELECT @v_SQL                   = @v_SQL + '[' + COLUMN_NAME + ']' +
    CASE WHEN ORDINAL_POSITION = @v_Max
         THEN ‘’
         ELSE ', ‘
          END
  FROM INFORMATION_SCHEMA.COLUMNS
 WHERE TABLE_NAME               = @v_TBL;
```

DBCatch
DEMO

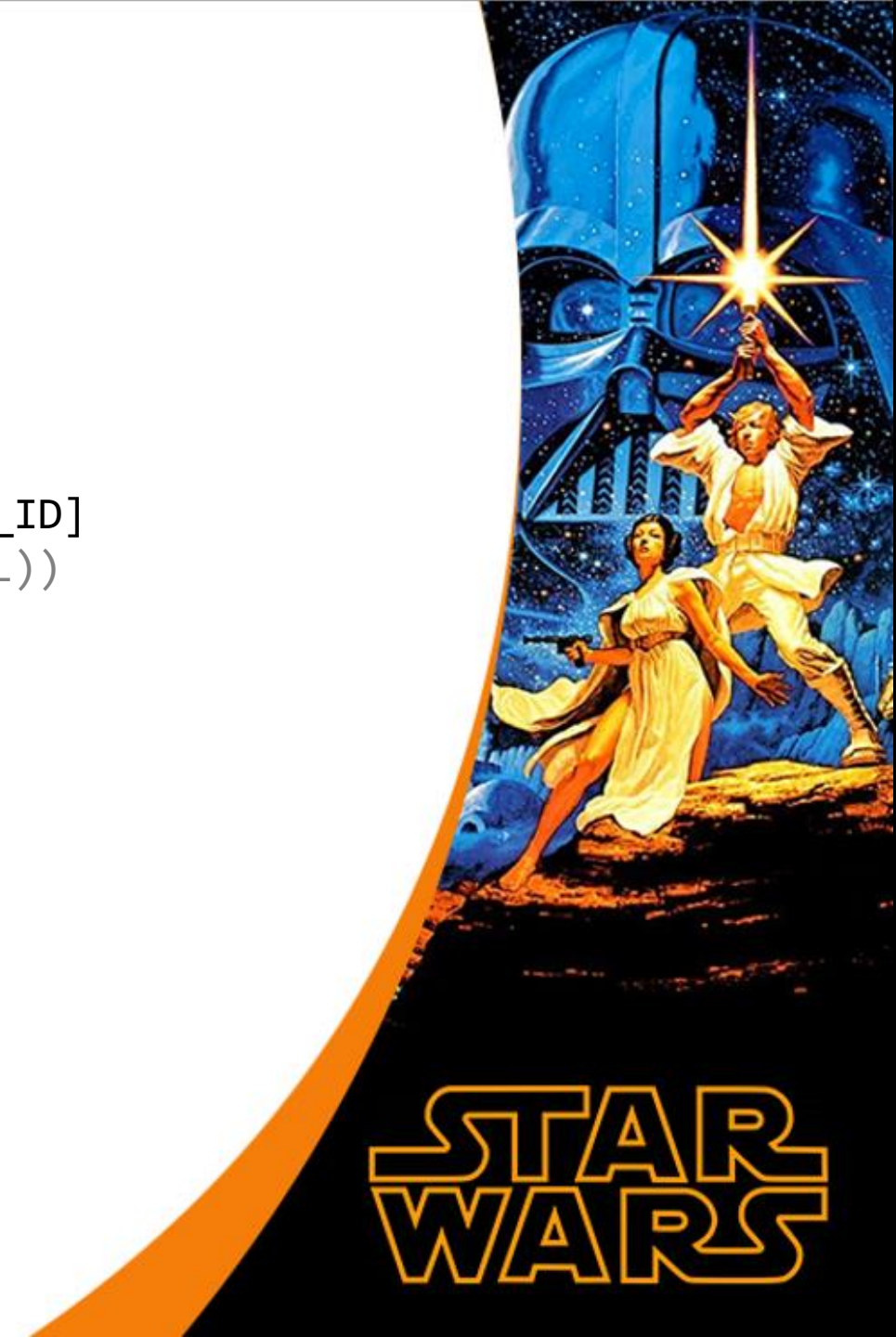
TRICK #1 :
RANDOMIZATION
Problem: Create a Random Data Set.
Solution: Manipulate the ORDER BY Clause.
STAR WARS

```sql
SELECT TOP 5 [Card]
  FROM [CardDeck]
 ORDER BY NEWID();
```

DBCatch
DEMO

HACK #1 :
DELETE DUPLICATES
Problem: We have a table with no Unique Key and currently 4 identical duplicate records and we need to remove 3.
Solution: Delete through a CTE.
STAR WARS

```
WITH CTE_delete AS
(
    SELECT RN = ROW_NUMBER() OVER(PARTITION BY [Dim_Server_ID]
                                  ORDER BY (SELECT NULL))
    FROM [dbo].[DemoServer]
)
DELETE FROM CTE_delete
WHERE RN > 1;
```



DBCatch
DEMO

BACK DOOR #1: READ FROM THE WINDOWS REGISTRY

Problem: We need to programmatically get the "True" Domain of the SQL Server Instance we are currently logged into.

Extended Problem: We think the company is using aliases.

Solution: Grab the "True" Domain name from the Windows Registry (Since we cannot use xp_cmdshell).

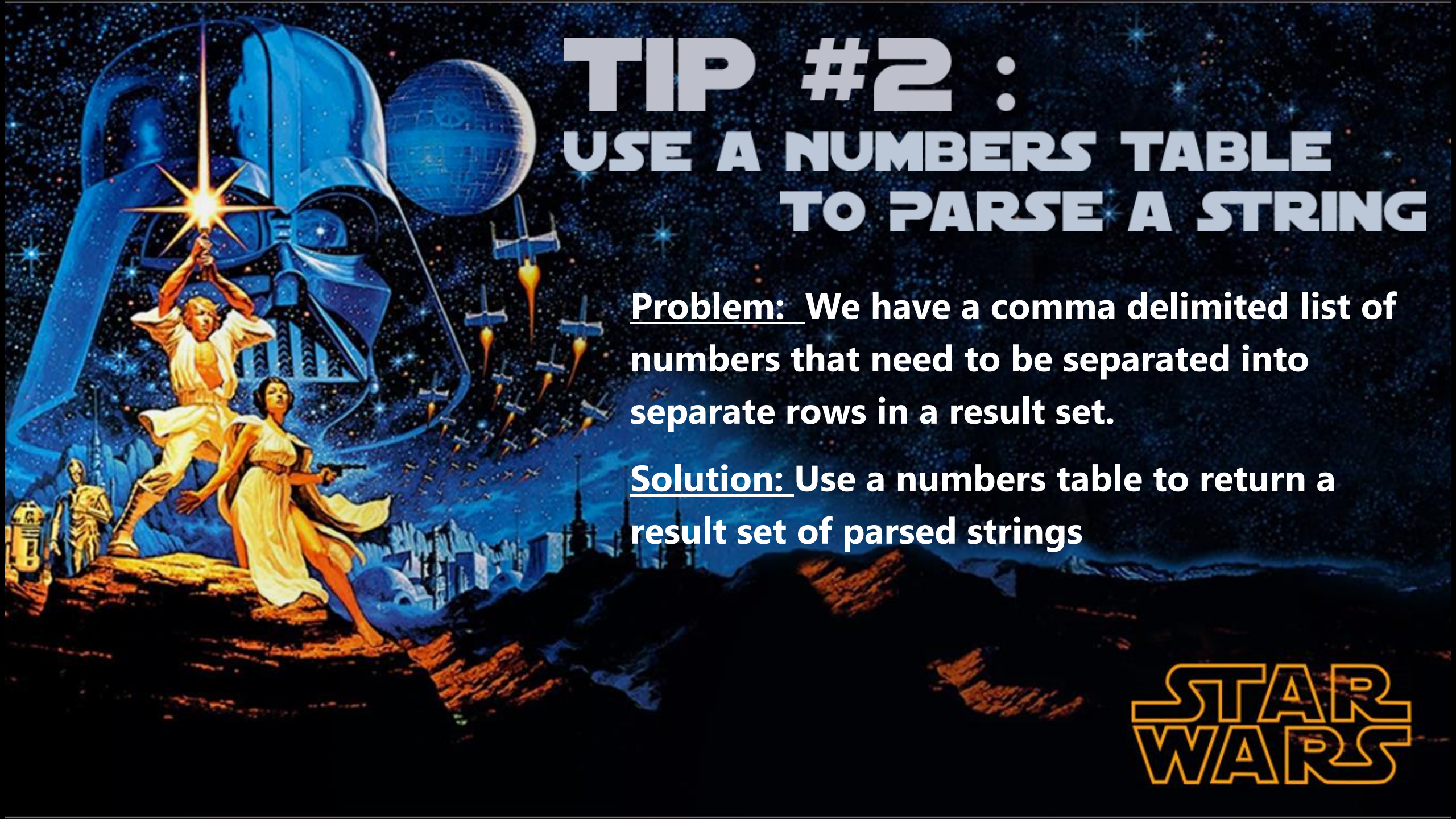
STAR WARS

```
DECLARE @v_Domain [NVARCHAR](100);

EXEC [master].[dbo].[xp_regread]
     @rootkey                    = 'HKEY_LOCAL_MACHINE'
    ,@key                        = 'SYSTEM\ControlSet001\Services\Tcpip\Parameters\'
    ,@value_name                 = 'Domain'
    ,@value                      = @v_Domain OUTPUT;

SELECT @v_Domain                 AS [@Domain];
```

DBCatch
DEMO


TIP #2 :
USE A NUMBERS TABLE
TO PARSE A STRING
Problem: We have a comma delimited list of numbers that need to be separated into separate rows in a result set.
Solution: Use a numbers table to return a result set of parsed strings
STAR WARS

```
DECLARE @v_a                    [NVARCHAR](255);

SELECT @v_a                     = '1,3,5,7,9,14,36,395';

SELECT [Number]
  FROM [dbo].[Numbers]
 WHERE CHARINDEX(',' + CONVERT([NVARCHAR](12), [Number]) + ',',
       ',' + @v_a + ',') > 0
 ORDER BY [Number];
```

DBCatch
DEMO

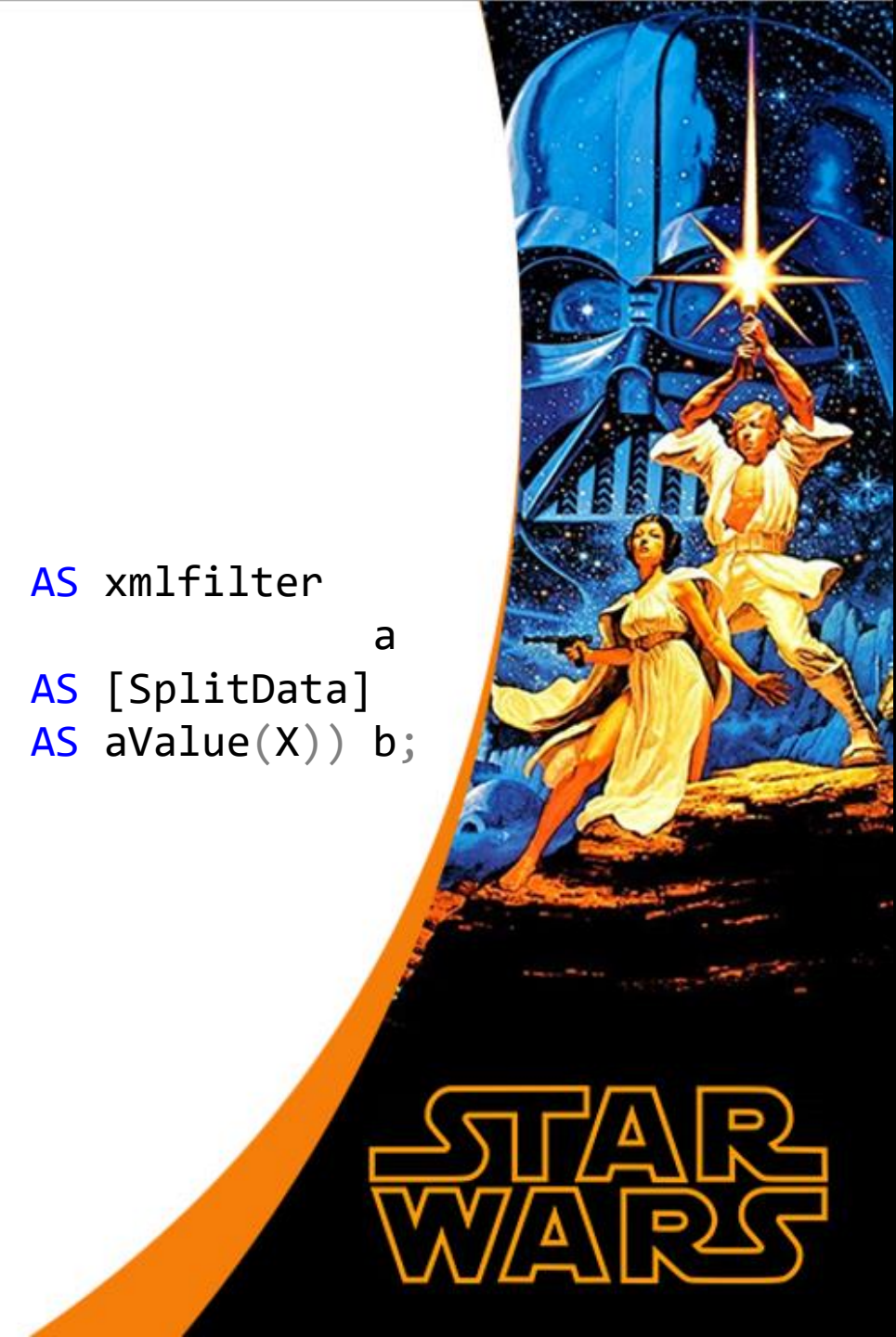
TRICK #2 : FOR XML CROSS APPLY TO RETURN A DELIMITED RESULT SET

Problem: We have strings in our data that need to be rolled out so that we can have non-overloaded data in our result sets.

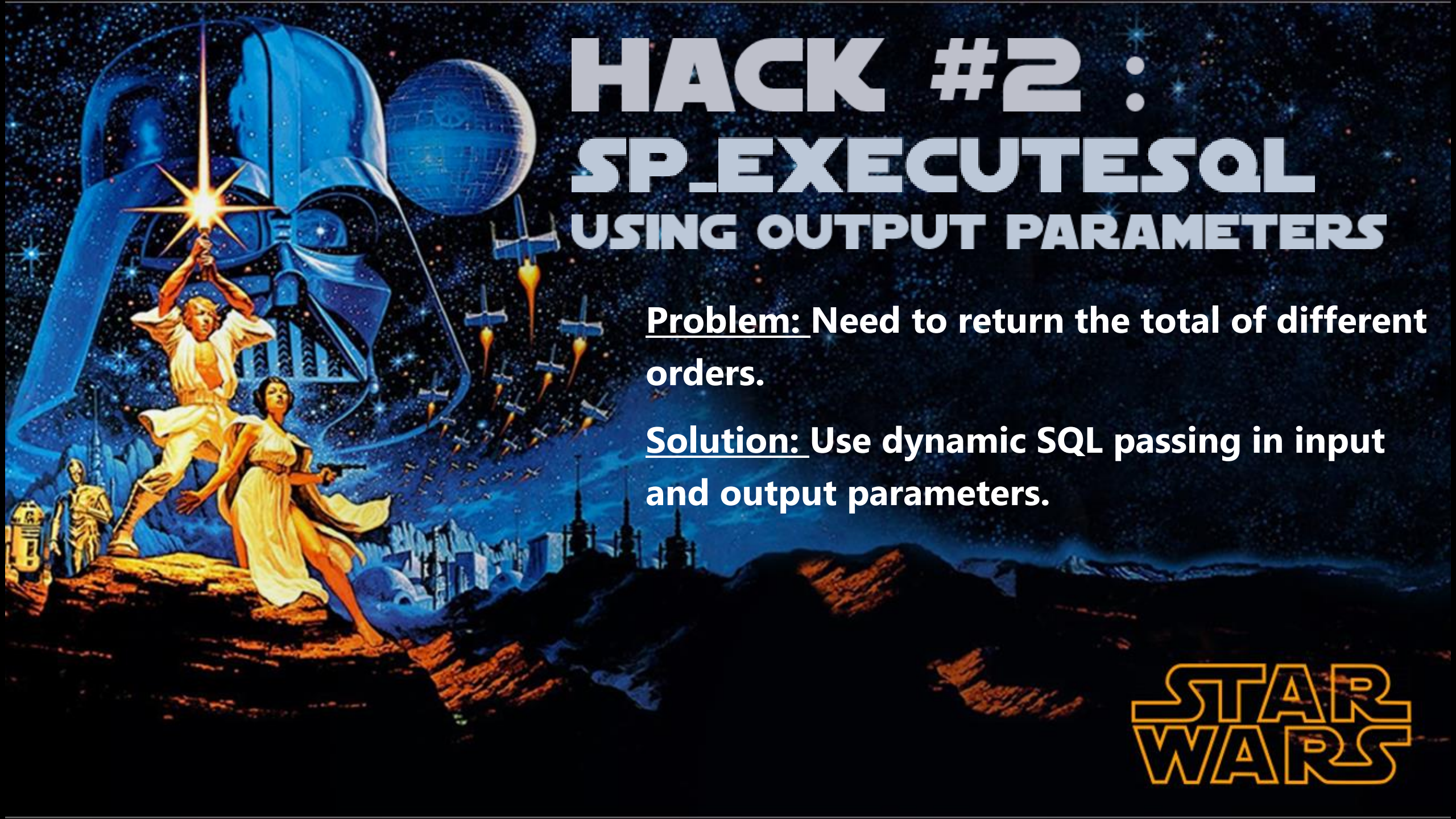
Solution: Use for XML with a cross apply to return a non overloaded data result set.

STAR WARS

```
/* Select the data out using XML CROSS APPLY */
SELECT a.[xmldemo_id]
      ,a.[Value]
      ,b.[SplitData]
  FROM (SELECT *
              ,CAST('<X>' + REPLACE([Value],
                    ',','</X><X>') + '</X>' AS XML)          AS xmlfilter
  FROM #xmldemo)                                                    a
  CROSS APPLY (SELECT aValue.X.value('.','VARCHAR(50)')      AS [SplitData]
                 FROM a.[xmlfilter].nodes('X')               AS aValue(X)) b;
```

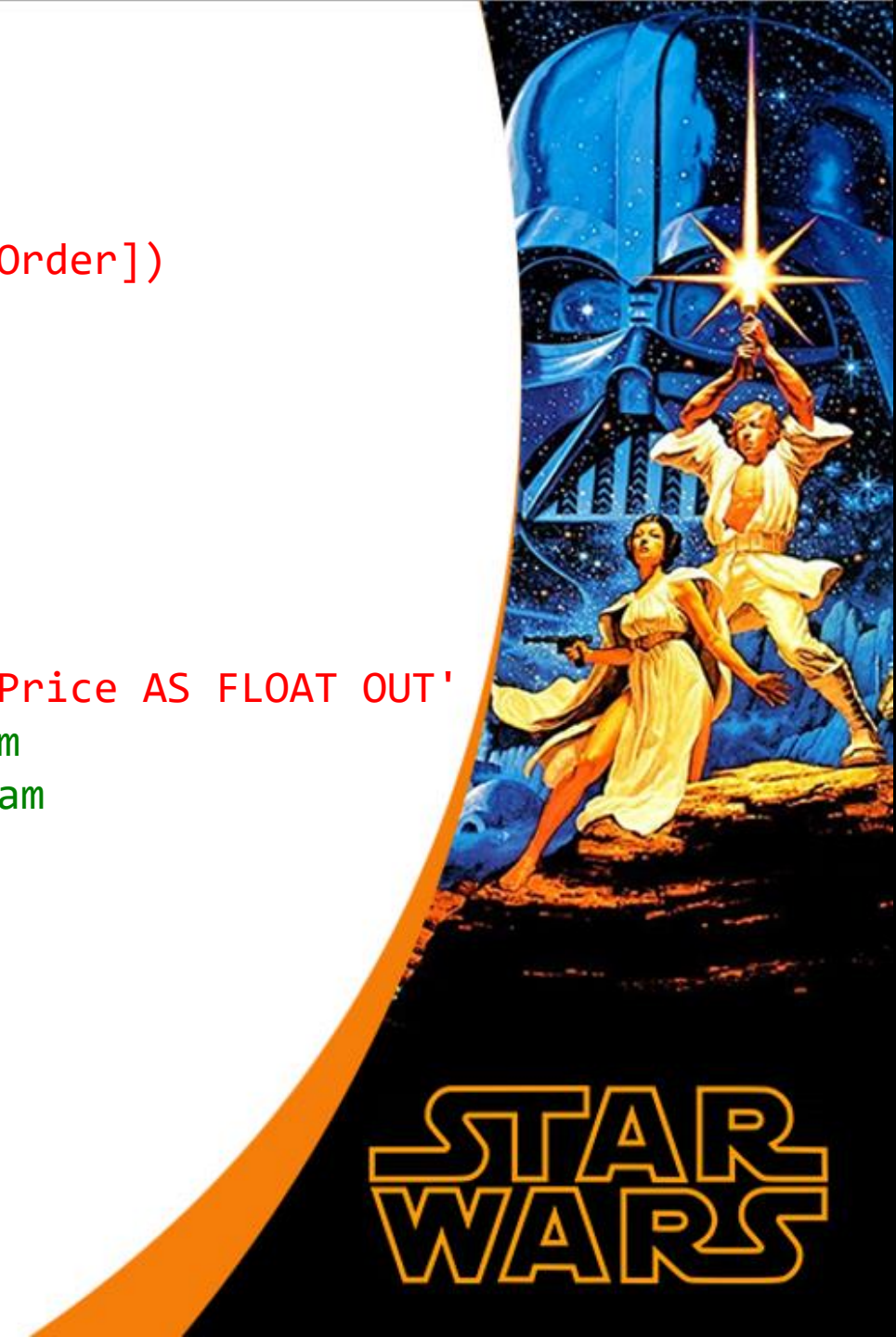


DBCatch
DEMO

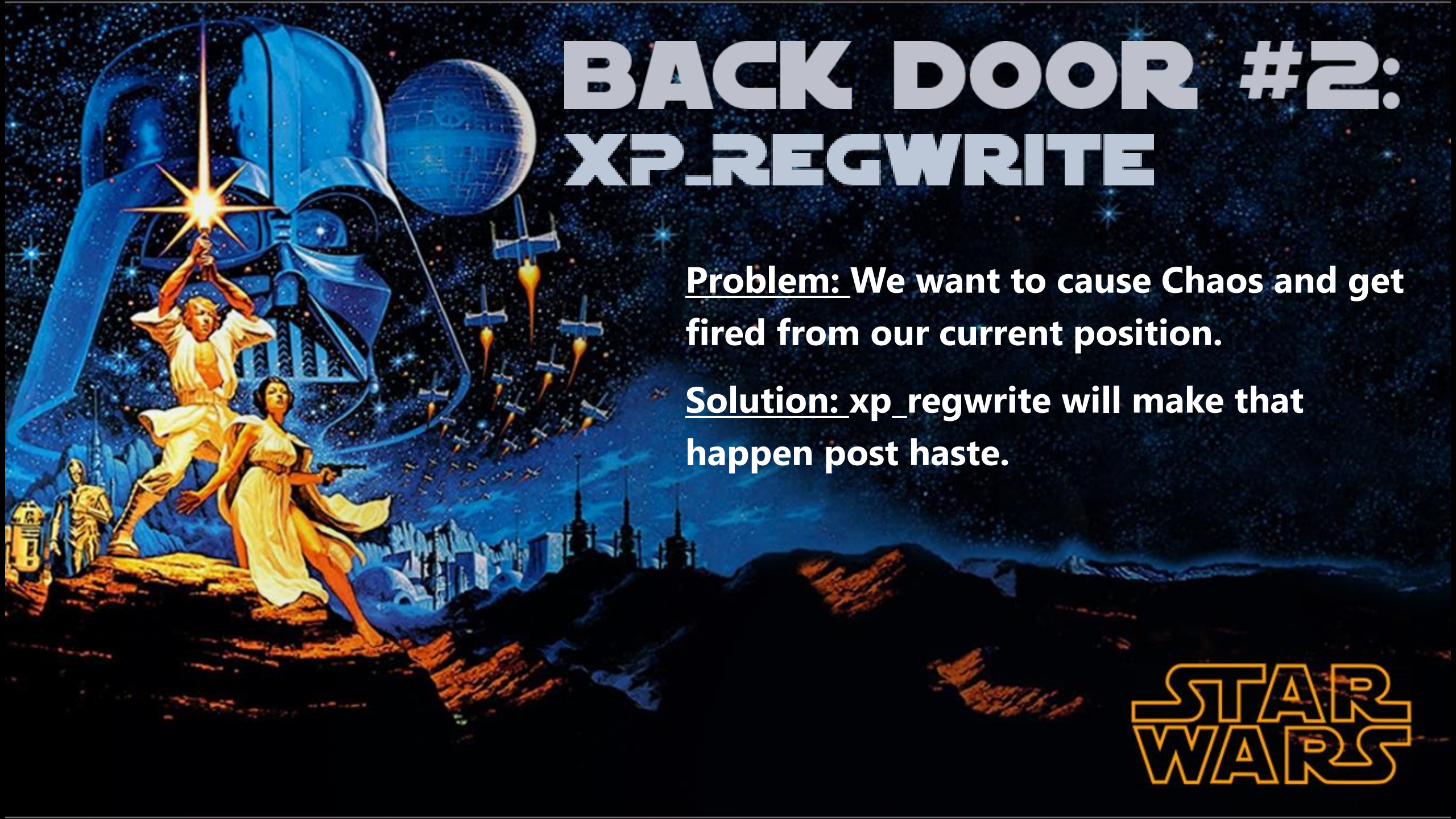

HACK #2 :
SP_EXECUTESQL
USING OUTPUT PARAMETERS
Problem: Need to return the total of different orders.
Solution: Use dynamic SQL passing in input and output parameters.
STAR WARS

```
SELECT @v_SQL           = N'
  SELECT @d_TotalPrice = SUM([Cost]) OVER(PARTITION BY [Order])
    FROM [OrderItems]
   WHERE [Order]        = @d_Order
   ORDER BY [Order]
  OFFSET 0 ROWS FETCH FIRST 1 ROW ONLY;';

EXEC sp_executesql
  @stmt                 = @v_SQL
 ,@params               = N'@d_Order AS SYSNAME, @d_TotalPrice AS FLOAT OUT'
 ,@d_Order              = @v_Order          -- Input param
 ,@d_TotalPrice         = @v_Total OUTPUT;  -- output param
```

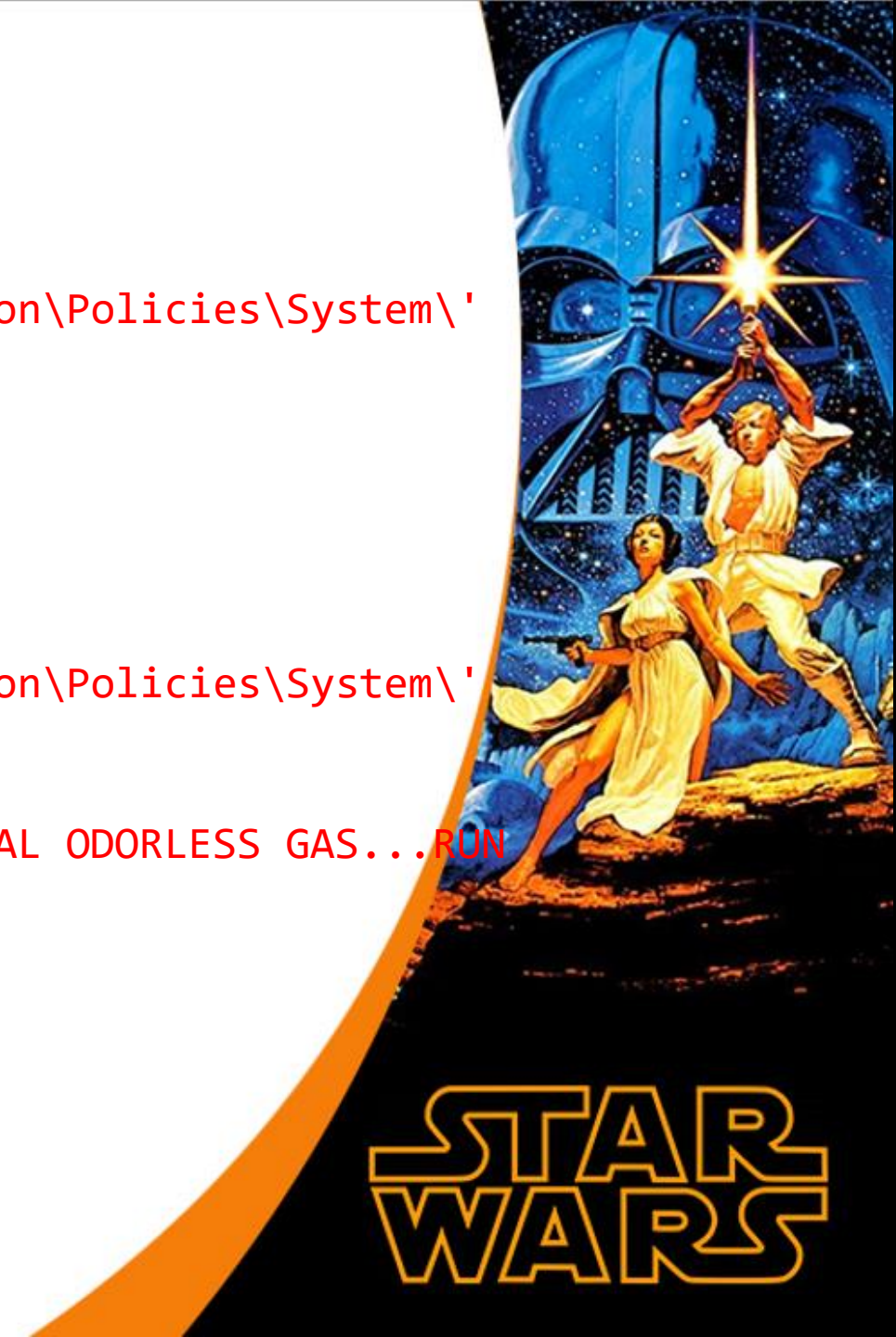


DBCatch
DEMO


BACK DOOR #2:
XP_REGWRITE
Problem: We want to cause Chaos and get fired from our current position.
Solution: xp_regwrite will make that happen post haste.
STAR WARS

```
EXEC [master].[dbo].[xp_regWrite]
     @rootkey     = 'HKEY_LOCAL_MACHINE'
    ,@key         = 'SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\'
    ,@value_name = 'legalnoticecaption’
    ,@type        = 'REG_SZ'
    ,@value       = 'WARNING!!!';

EXEC [master].[dbo].[xp_regWrite]
     @rootkey     = 'HKEY_LOCAL_MACHINE'
    ,@key         = 'SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\'
    ,@value_name = 'legalnoticetext’
    ,@type        = 'REG_SZ’
    ,@value       = 'You are about to release the CLEAR LETHAL ODORLESS GAS...RUN
AWAY!!!!!!';
```



DBCatch
DEMO

WARNING!!!
You are about to release the CLEAN LETHAL ODORLESS GAS...RUN AWAY!!!!!!!
OK

We swim with sharks

DBCatch