

microsoft.public.sqlserver.programming: Re: IN Clause – Stuck on an easy query :-(

Re: IN Clause – Stuck on an easy query :-(

Source:

<http://www.tech-archive.net/Archive/SQL-Server/microsoft.public.sqlserver.programming/2004-09/0450.html>

From: Steve Kass (*skass_at_drew.edu*)

Date: 09/01/04

Date: Wed, 01 Sep 2004 16:24:16 -0400

Joe Celko wrote:

>>>> *From Yukon (abridged) BOL -- SQL Injection 'You must therefore
>>>
>>>
> validate all user input on the client side, and force server-side type
> checking by calling parameterized stored procedures.'* <<
>
> *This has nothing to do with SQL Injection; it is ****basic**** Software
> Engineering: Never trust the front end in a tiered architecture to
> validate or verify the data. The database is the repository and trusted
> data source, not some unknown program to be written by an unknown
> programmer in an unknown language at some unknown time in the future.
>
> Parameterized stored procedures are also a bad idea. They will not port
> (which is what MS wants as part of its fight against Open Source). Most
> of the validations can be easily done with CHECK(), DEFAULT and
> REFERENCES. The CHECK() constraints and REFERENCES also provide extra
> predicates for the optimizer.
>
You have to be joking. Are all the examples of parameterized stored
procedures you've posted yourself (such as in the 317 results of
<http://groups.google.com/groups?q=celko+%22create+procedure%22>) "bad
idea[s]"?*

I'll give you credit for the novel concept: check user input by
inserting it into a user-input-verification-table as-is, and reject it
if a CHECK constraint is violated?

Have you implemented any real-world database projects in the last 5
years or so using no stored procedures (or only parameterless ones)?
Using what RDBMS (if you used one)? Assuming those projects had any
users, how did you incorporate the user input into queries, with dynamic
SQL? Not to mention questions of security, testing, code management, or
a whole host of other important issues.

Re: IN Clause – Stuck on an easy query :-(

microsoft.public.sqlserver.programming: Re: IN Clause – Stuck on an easy query :-(

Steve Kass
Drew University

>
>
>--*CELKO*--
>=====

> *Please post DDL, so that people do not have to guess what the keys,*
> *constraints, Declarative Referential Integrity, datatypes, etc. in your*
> *schema are.*

>
>*** Sent via Developersdex <http://www.developersdex.com> ***
>Don't just participate in USENET...get rewarded for it!

>
>

Re: IN Clause – Stuck on an easy query :-(