

Re: SQL Injection Prevention

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.security/2004-09/0238.html>

From: Valery Pryamikov (Valery_at_nospam.harper.no)

Date: 09/28/04

Date: Tue, 28 Sep 2004 18:56:35 +0200

Aaron,

> *And if the stored procedure doesn't contain dynamic SQL? You seem to be
> under the impression that all stored procedures contain dynamic SQL.*

Please tell me what gives you such an impression? Can you please refer to any of my posts to that thread where I saying anything that could be interpreted that way?

Frankly, my impression is that you aren't even trying to read my arguments (that you apparently don't like) and you don't pay attention to what I'm saying. Can you please re-read my posts to that thread and try to understand my points.

fyi: during my work for Siemens (for the last 8.5 years) I was responsible for system development and architecting of large enterprise solution with more than ten thousands tables/views, more than 300000 lines in SQL stored procedures, more than 1.5 MLoC of Fortran code + more than 1.2 MLoC of C++ code (mostly my) + huge code base in VB 6.0 with about 1500 of inproc activeX document servers that are working against more than 200 DCOM servers. Believe me, I've seen a lot of code and I developed a lot of code (more than 1 MLoC of production code), so you don't need to teach me basics about SQL programming. Even so primarily I'm not database programmer, but I easily can account something like 200 KLoC of my code (production code) that directly works with database by means of plain ODBC API and plain OLEDB.

Valery Pryamikov. MCP, MCAD, MCSA, Windows Security MVP (former Windows SDK MVP).

<http://www.harper.no/valery>

"Aaron [SQL Server MVP]" <ten.xoc@dnartreb.noraa> wrote in message news:%23llwzZXpEHA.3800@TK2MSFTNGP14.phx.gbl...

>> *1. when you call parameterized stored procedure, it (the procedure) may
>> internally use dynamic sql (ie concatenate parameters to SQL string),*

>> *thus*

>> *introducing another SQL injection vulnerability.*

>

> *And if the stored procedure doesn't contain dynamic SQL? You seem to be
> under the impression that all stored procedures contain dynamic SQL. I*

> *can*

- > *assure you that this is not true.*
- >
- > *Stored procedures can be made just as safe as your method. (plus let's*
- > *not*
- > *forget all the other benefits of stored procedures over parameterized DML*
- > *statements).*
- >
- > *So I don't think it's fair to make a blanket statement. Everything*
- > *requires*
- > *caution to some degree... I really don't think it's worthwhile to throw*
- > *away*
- > *all the benefits of stored procedures to gain this slight edge in*
- > *security,*
- > *which is eliminated if your stored procedure doesn't contain dynamic SQL*
- > *and/or you properly validate input...*
- >
- > **A**
- >
- >