

Re: SQL Injection Prevention

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.security/2004-09/0228.html>

From: Valery Pryamikov (Valery_at_nospam.harper.no)

Date: 09/28/04

Date: Tue, 28 Sep 2004 17:20:36 +0200

Common guys, what is it with you? I'm not bashing stored procedures, not at all. I'm just saying that when it concerns to SQL injection, then parameterized DML statement is more protected than parameterized call to stored procedure. That's it. I don't think you can prove opposite. But that doesn't mean anything about good programming practices what so ever. Do you read subject – SQL injection which only happens due to bad programming practices.

I'm not in any way going to fight beaten to death holy war about "are stored procedures better than SQL DMLs or not".

–Valery.

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

"Nigel Rivett" <sqlnr@hotmail.com> wrote in message
news:483195D1-E0AC-4765-8EDA-D0B76D923DED@microsoft.com...
> *You're comparing a well built parameterized sql statement against a badly
> built stored procedure so it's obvious which will win.*
>
> *Stored procedures are easier to review and so catch bad proctices and are
> usually the domain of people who have some experience in dealing with
> databases.*
>
>>> *for stored procedure to return the same cursor as select, this stored
>>> procedure has to execute the same select.*
>
> *Not true.*
>
>>> *if stored procedure implemented wrong way – ie it constructs sql by
>>> concatenating received parameter with sql string,*
>
> *I can't believe anyone would do that – if you would consider it then I
> suggest you stay away from databases altogether :).*
>
> *The stored procedure in your example would probably be*
>
> *create proc a*
> *@key int*

> as
> select somevalue from sometable where somekey = @key
> go
>
> You need to build a case that this is more vulnerable than the application
> code – bearing in mind that a person writing a stored proc is likely to
> have
> more database experience than the person writing the app code.
>
>>> in Oracle you have possibility to execute dynamic cursor from stored
>>> procedure. I.e. you construct whatever sql string inside stored procedure
>>> and open cursor on
> that string. I believe it must be similar functionality in SQL server
>
> Your belief is very wrong (and I hope you aren't trying to use that
> belief).
>
> p.s. I've have never written an explicit cursor in t-sql (except to "help"
> others and never will).
>
>
> "Valery Pryamikov" wrote:
>
>> Tibor,
>> we aren't talking about good programming practices when we discuss SQL
>> injection, aren't we :-).
>> as long as there is possibility to screw something, we have to account
>> for
>> it. Therefore my statement stays that parameterized SQL actually provides
>> better protection against SQL injection than parameterized call to stored
>> procedure.
>>
>> –Valery.
>> <http://www.harper.no/valery>
>>