

# Google ашиглан Hack хийх

<http://www.tuguldur.tk>

Та Google хайлтын хуудасыг мэдэх байх. Google-г ашиглан хэрхэн Hack хийж болдогыг харуулая! <http://www.google.com/>  
Одоо та эдгээрийг өгөөд хайлгаад үз

```
allintitle:"index of/root"
allintitle:"index of/admin"
inurl:"wwwroot/*."
filetype:htpasswd htpasswd
intitle:"Index of" ".htpasswd" -intitle:"dist" -apache -htpasswd.c
index.of.private (algo privado)
intitle:index.of master.passwd
inurl:passlist.txt (para encontrar listas de passwords)
intitle:"Index of..etc" passwd
intitle:admin intitle:login
"Incorrect syntax near" (SQL script error)
intitle:"the page cannot be found" inetmgr (debilidad en IIS4)
intitle:index.of ws_ftp.ini
"Supplied arguments is not a valid PostgreSQL result" (possible debilidad SQL)
_vti_pvt password intitle:index.of (Frontpage)
inurl:backup intitle:index.of inurl:admin
"Index of /backup"
index.of.password
index.of.winnt
inurl:"auth_user_file.txt"
"Index of /admin"
"Index of /password"
"Index of /mail"
"Index of /" +passwd
Index of /" +.htaccess
Index of ftp +.mdb allinurl:/cgi-bin/ +mailto
allintitle: "index of/admin"
allintitle: "index of/root"
allintitle: sensitive filetype:doc
allintitle: restricted filetype :mail
allintitle: restricted filetype:doc site:gov
administrator.pwd.index
authors.pwd.index
service.pwd.index
filetype:config web
gobal.asax index
inurl:passwd filetype:txt
inurl:admin filetype:db
inurl:iisadmin
inurl:"auth_user_file.txt"
inurl:"wwwroot/*."
allinurl: winnt/system32/ (get cmd.exe)
allinurl:/bash_history
intitle:"Index of" .sh_history
intitle:"Index of" .bash_history
intitle:"Index of" passwd
intitle:"Index of" people.1st
intitle:"Index of" pwd.db
intitle:"Index of" etc/shadow
intitle:"Index of" spwd
intitle:"Index of" master.passwd
intitle:"Index of" htpasswd
intitle:"Index of" members OR accounts
```

intitle:"Index of" user\_carts OR user\_cart  
\_vti\_inf.html  
service.pwd  
users.pwd  
authors.pwd  
administrators.pwd  
test-cgi  
wwwboard.pl  
www-sql  
pwd.dat  
ws\_ftp.log

Жишээ 1:

allintitle:"index of/root" гэж хайхад

<http://www.google.com/search?q=allintitle%3A%22index+of%2Froot%22+&sourceid=mozilla-search&start=0&start=0&ie=utf-8&oe=utf-8&client=firefox-a&rls=org.mozilla:de-DE:official>

=====

Жишээ 2:

inurl:"auth\_user\_file.txt" гэж хайхад

[http://64.233.183.104/search?q=cache:E5z\\_9X\\_1FUQJ:www.soirjewellers.com/members/Data/auth\\_user\\_file.txt+inurl:%22auth\\_user\\_file.txt%22+&hl=en&client=firefox-a](http://64.233.183.104/search?q=cache:E5z_9X_1FUQJ:www.soirjewellers.com/members/Data/auth_user_file.txt+inurl:%22auth_user_file.txt%22+&hl=en&client=firefox-a)

txUKhXYi4xeFs|master|admin|Worasi|Junsawang|xxx@xxx|on  
qk6GaDj9iBfNg|tomjang||Bug|Tom|xxx@xxx|on

Хараж байн уу Hash нууцлагдсан түлхүүр үг байна. Одоо тэгээд john the ripper ашиглан тайлаад л боллоо.

Бусад өөр хайх аргууд:

=====

"Index of /admin"  
"Index of /password"  
"Index of /mail"  
"Index of /" +passwd  
"Index of /" +password.txt  
"Index of /" +.htaccess  
index of ftp +.mdb allinurl:/cgi-bin/ +mailto

administrators.pwd.index  
authors.pwd.index  
service.pwd.index  
filetype:config web  
gobal.asax index

allintitle: "index of/admin"  
allintitle: "index of/root"  
allintitle: sensitive filetype:doc  
allintitle: restricted filetype :mail  
allintitle: restricted filetype:doc site:gov

inurl:passwd filetype:txt  
inurl:admin filetype:db  
inurl:iisadmin  
inurl:"auth\_user\_file.txt"  
inurl:"wwwroot/\*."

top secret site:mil  
confidential site:mil

allinurl: winnt/system32/ (get cmd.exe)  
allinurl:/bash\_history

intitle:"Index of" .sh\_history  
intitle:"Index of" .bash\_history  
intitle:"index of" passwd  
intitle:"index of" people.lst  
intitle:"index of" pwd.db  
intitle:"index of" etc/shadow  
intitle:"index of" spwd  
intitle:"index of" master.passwd  
intitle:"index of" htpasswd  
intitle:"index of" members OR accounts  
intitle:"index of" user\_carts OR user\_cart

default.asp  
showcode.asp  
sendmail.cfm  
wwwboard.pl  
www-sql  
view-source  
campas  
aglimpse  
glimpse  
man.sh  
AT-admin.cgi  
AT-generate.cgi  
default.asp  
dvwssr.dll  
cart32.exe  
add.exe  
index.jsp  
SessionServlet  
shtml.dll  
index.cfm  
page.cfm  
shtml.exe  
web\_store.cgi  
shop.cgi  
upload.asp  
default.asp  
pbserver.dll  
phf  
test-cgi  
finger  
Count.cgi  
jj  
ssi  
php.cgi  
php  
nph-test-cgi

handler  
webdist.cgi  
getFile.cfm  
imagemap.exe  
admin  
cgiwrap  
edit.pl  
perl  
names.nsf  
webgais  
dumpenv.pl  
test.cgi  
submit.cgi  
guestbook.cgi  
guestbook.pl  
cachemgr.cgi  
responder.cgi  
perlshop.cgi  
query  
w3-msql  
plusmail  
htsearch  
infosrch.cgi  
publisher  
ultraboard.cgi  
htgrep  
wais.pl  
amadmin.pl  
subscribe.pl  
news.cgi  
auctionweaver.pl  
ad.cgi  
WSFTP.LOG  
index.html~  
forums.html~  
index.html.bak  
test.bat  
msadcs.dll  
htimage.exe  
counter.exe  
browser.inc  
\_vti\_inf.html  
service.pwd  
users.pwd  
authors.pwd  
administrators.pwd  
shtml.dll  
shtml.exe  
fpcount.exe  
hello.bat  
websendmail  
faxsurvey  
htmlscript  
perl.exe  
webgais  
filemail.pl  
maillist.pl  
info2www  
files.pl  
bnbform.cgi  
survey.cgi  
classifieds.cgi

wrap  
db.cgi  
formmail.cgi  
allmanage.pl  
adpassword.txt  
redirect.cgi  
cvsweb.cgi  
login.jsp  
dbconnect.inc  
forums.html.bak  
print.cgi  
register.cgi  
webdriver  
bbs\_forum.cgi  
mysql.class  
sendmail.inc  
CrazyWWWBoard.cgi  
search.pl  
way-board.cgi  
webpage.cgi  
pwd.dat  
adcycle  
post-query  
help.cgi  
.htpasswd  
acid\_main.php  
access.log  
log.htm  
log.html  
log.txt  
logfile  
logfile.htm  
logfile.html  
logfile.txt  
logger.html  
stat.htm  
stats.htm  
stats.html  
stats.txt  
webaccess.htm  
wwwstats.html  
source.asp  
perl  
mailto.cgi  
YaBB.pl  
mailform.pl  
cached\_feed.cgi  
global.cgi  
Search.pl  
build.cgi  
common.php  
show  
global.inc

Өөр маш олон арга бий сэтгээд сайн бод  
Үүнийг үз дээ  
allinurl:winn/system32/

**Bibo**

<http://www.tuguldur.tk>