

## Google hacking... (profesionalne)

Vložil/a [clusk](#) [1], 14 Prosinec, 2004 - 06:14

- [Hacking](#) [2]
- [Hacking method](#) [3]

Clanek je pouze prekladem dokumentu "Google hacking". Autorem originalu je administrator serveru i-hacked.com a johnny.ihackstuff.com. Dovolují si tvrdit, že autor je mistrem ve svém oboru...

Představováním googlu a jeho potencialního využití by bylo asi nosením dříví do lesa. Urcíte vsichni vite, co všechno google ve svém nitru schovává a co vše indexuje za stránky. Stránky pro něj sbírají a indexují roboti - skripty, možná i samostatné počítače, jenž hledají webové servery, prolezají zdrojové kódy stránek a logicky zarazují tyto stránky do databáze google. Ovšem sem tam naleznou i nějaký ten soubor, jenž by normálně neměl být uživateli přístupný. Stává se to v případech, kdy tvůrce (webmaster) špatně stránky vytvořil - například se ve zdrojovém kódu nachází odkaz na soubor s hesly. Tím jsem vás seznámil s problematikou google a ukončil bych tak úvod. Následuje přeložený článek:

Hackování pomocí google je bezvadná věc. Použitím správně upravených vyhledávacích řetězců můžeme leckdy nalézt spoustu zajímavých informací. Můžeme najít například: čísla kreditních karet, hesla, software, písničky (MP3)... (a další)

Texty uvedené níže jsou pouze zajímavými příklady, jenž můžeme poslat googlu a z výsledku získat informace o některých lidech, z kterých by urcíte oni sami nebyli moc nadšeni... Pokud máte chuť, zkuste svoje vlastní upravené vyhledávací řetězce pro získání užitečných informací.

### Zkuste pár následujících příkladů:

```
intitle:"Index of" passwords modified
allinurl:auth_user_file.txt
"access denied for user" "using password"
"A syntax error has occurred" filetype:ihtml
allinurl: admin mdb
"ORA-00921: unexpected end of SQL command"
inurl:passlist.txt
"Index of /backup"
"Chatologica MetaSearch" "stack tracking:"
```

```
Amex Numbers: 3000000000000000..3999999999999999
MC Numbers: 5178000000000000..5178000000000000
Visa 4356000000000000..4356000000000000
```

```
"parent directory " /appz/ -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
```

```
"parent directory " DVDRip -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
```

```
"parent directory " Xvid -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
```

```
"parent directory " Gamez -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
```

```
"parent directory " MP3 -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
```

```
"parent directory " Name of Singer or album -xxx -html -htm -php -shtml -opendivx
```

`-md5 -md5sums`

Vsimnete si, ze jsem pouze zmenil nazev rodicovskeho adresare. Zmenou na cokoliv jineho/zajimave, muzete sehnat spoustu uzitecnych veci.

## METODA 2

hodte do googlu tento retezec:

`?intitle:index.of? mp3`

Ted staci, aby jste pridali jmeno skladby/skupiny/zpevaka.

Napriklad:

`?intitle:index.of? mp3 jackson`

## METODA 3

ted zkuste tento retezec:

`inurl:microsoft filetype:iso`

Muzete zmenit retezec na neco jineho, napriklad microsoft na adobe, iso na zip, atd... (pozn. prekladatele: Fantazii se meze nekladou:))

`"# -Frontpage-" inurl:service.pwd`

Frontpage hesla... pekne ciste a prehledne vysledky !!

`"AutoCreate=TRUE password=*"`

Toto bude vyhledavat heslo pro "Website Access Analyzer", japonsky software pro tvorbu webovych statistik. Pro ty, jenz umi japonsky, kouknete se na stranku autora tohoto softwaru

<http://www.coara.or.jp/~passy/> [4]

`"http://*:*@www" domainname`

Timto pozadavkem ziskate hesla z vyhledavacich enginu (ale ne z google). Misto domainname musite napsat nazev domeny bez koncovky (.cz, .sk, ...)

`"http://*:*@www" bangbus` nebo `"http://*:*@www"bangbus`

Take muzete napsat:

`"http://bob:bob@www"`

`"sets mode: +k"`

Tento pozadavek odhali klice (hesla) z logu z kanalu IRC.

`allinurl: admin mdb`

Ne vsechny stranky, ktere google po tomto vrati, obsahuji uzivatelska jmena, hesla nebo ostatni citlive udaje, ale nektera ano!

`allinurl:auth_user_file.txt`

Soubor s hesly od DCFora. Soubor obsahuje seznam (zlomitelných) hesel, uzivatelských jmen a e-mailových adres pro DCForum a DCShop.

```
intitle:"Index of" config.php
```

Ukaze stranky pouzivajici soubor config.php, který (vetsinou) obsahuje uzivatelske jmeno a heslo pro pripojeni k SQL databazi. Hodne sajtu pouziva fora bezici na PHP. Tento soubor vam da plny pristup (administratorsky ucet) do databaze.

```
eggdrop filetype:user user
```

Konfiguracni soubor eggdropa. Vyhname se rozsahlym diskuzim o eggdropovi a vubec IRC botech. Je mozne, ze soubor bude obsahovat uzivatelska jmena a hesla IRC uzivatelu.

```
intitle:index.of.etc
```

Google vam s timto dotazem vyhleda "etc" adresare, kde se nachazi spousta typu souboru s hesly. Tento odkaz neni spolehlivy, ale prolezani "etc" adresaru muze byt vazne sranda!

```
filetype:bak inurl:"htaccess|passwd|shadow|htusers"
```

Pro vyhledavani zaloh (souboru \*.bak). Tyto zalohy vytvari nektere editory nebo nekdy i samotni administratori.

Zkusme predstirat, ze potrebujeme seriove cislo pro windows xp professional.

Do vyhledavaci kolonky google napiseme neco takoveho - "Windows XP Professional" 94FBR

klic 94FBR je kodem... ten je prikladan k mnoha kopiim MS Office. Velmi vam pomuze zredukovat mnozstvi "podvodnych" porno stranek, které vas chteji zmast. Jestlize hledate seriovy kod pro winzip 8.1 - "Winzip 8.1" 94FBR

Podekovani a dalsi informace na: <http://johnny.ihackstuff.com> [5]

## Zaver

Zaverem se musim priznat, ze po peti minutach hledani a zkouseni ruznych retezcu na googlu jsem se az zalekl toho, jake informace se daji ziskat. Clanek kazdopadne nema vybudit zbesilou honbu za temito informacemi, ale ma poukazat na nesikovnost...nekdy az ignoranci nedbalých webmasteru! Chtel jsem spise poukazat na to, jak se da dany dotaz vice specifikovat a najit tak rychleji to, co potrebujete.

Odkaz na originalni dokument je zde: [www.i-hacked.com/index2.php?option=com\\_content&do\\_pdf=1&id=23](http://www.i-hacked.com/index2.php?option=com_content&do_pdf=1&id=23) [6] a nedeste se, ja udelal volny preklad, ale vyznam je stejny :)

**URL článku:** <https://security-portal.cz/clanky/google-hacking-profesionalne>

## Odkazy:

[1] <https://security-portal.cz/users/clusk>

[2] <https://security-portal.cz/category/tagy/hacking>

[3] <https://security-portal.cz/category/tagy/hacking-method>

[4] <http://www.coara.or.jp/~passy/>

[5] <http://johnny.ihackstuff.com>

[6] [http://www.i-hacked.com/index2.php?option=com\\_content&do\\_pdf=1&id=23](http://www.i-hacked.com/index2.php?option=com_content&do_pdf=1&id=23)