

## 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 určité oni sami nebyli moc nadšení... Pokud máte chuť, zkuste svoje vlastní upravené vyhledávací řetězce pro získání užitečných informací.

### Zkuste par nasledujících příkladu:

```
intitle:"Index of" passwords modified
allinurl:auth_user_file.txt
"access denied for user" "using password"
"A syntax error has occurred" filetype:html
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, že jsem pouze změnil název rodičovského adresáře. Změnou na cokoliv jiného/zajímavého, můžete sehnat spoustu užitečných věcí.

## METODA 2

hodte do googlu tento řetězec:

`?intitle:index.of? mp3`

Tedy staci, aby jste přidali jméno skladby/skupiny/zpěváka.

Například:

`?intitle:index.of? mp3 jackson`

## METODA 3

ted zkuste tento řetězec:

`inurl:microsoft filetype:iso`

Můžete změnit řetězec na něco jiného, například microsoft na adobe, iso na zip, atd... (pozn. překladatel: Fantazii se meze nekladou:))

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

Frontpage hesla... pěkně čisté a přehledné výsledky !!

`"AutoCreate=TRUE password=*"`

Toto bude vyhledávat heslo pro "Website Access Analyzer", japonský software pro tvorbu webových statistik. Pro ty, jenž umí japonsky, koukněte se na stránku autora tohoto softwaru

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

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

Tímto požadavkem získáte hesla z vyhledávacích engineů (ale ne z google). Místo domainname musíte napsat název domény bez koncovky (.cz, .sk, ...)

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

Take můžete napsat:

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

`"sets mode: +k"`

Tento požadavek odhalí klíče (hesla) z logů z kanálu IRC.

`allinurl: admin mdb`

Ne všechny stránky, které google po tomto vrátí, obsahují uživatelská jména, hesla nebo ostatní citlivé údaje, ale některá ano!

`allinurl:auth_user_file.txt`

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

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

Ukaze stránky používající soubor config.php, který (většinou) obsahuje uživatelské jméno a heslo pro připojení k SQL databázi. Hodně sajtu používá fora bezíci na PHP. Tento soubor vám dá plný přístup (administratorský účet) do databáze.

```
eggdrop filetype:user user
```

Konfigurační soubor eggdropa. Vyhnete se rozsáhlým diskuzím o eggdropovi a vůbec IRC botech. Je možné, že soubor bude obsahovat uživatelská jména a hesla IRC uživatele.

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

Google vám s tímto dotazem vyhledá "etc" adresare, kde se nachází spousta typu souboru s hesly. Tento odkaz není spolehlivý, ale prolezání "etc" adresaru může být vážně sranda!

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

Pro vyhledávání záloh (souboru \*.bak). Tyto zálohy vytváří některé editory nebo někdy i samotní administrátoři.

Zkusme předstírat, že potřebujeme seriové číslo pro Windows XP Professional.

Do vyhledávací kolonky Google napíšeme něco takového - "Windows XP Professional" 94FBR

klic 94FBR je kódem... ten je přidán k mnoha kopiím MS Office. Velmi vám pomůže zredukovat množství "podvodných" porno stránek, které vás chtějí zmást. Jestliže hledáte seriový kód pro Winzip 8.1 - "Winzip 8.1" 94FBR

Poděkování a další informace na: <http://johnny.ihackstuff.com> [5]

## Zaver

Zaverem se musím přiznat, že po pěti minutách hledání a zkoušení různých retezcu na Googlu jsem se až zalekl toho, jaké informace se dají získat. Článek každopádně nemá vybudit zbesilou honbu za těmito informacemi, ale má poukázat na nesikovnost...někdy až ignoranci nedbalých webmasterů! Chtěl jsem spíše poukázat na to, jak se dá daný dotaz více specifikovat a najít tak rychleji to, co potřebujete.

Odkaz na originální 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 neděste se, já udělal volný překlad, ale význam je stejný :)

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

### Odkazy:

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

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

[3] <https://www.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)