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. Dovoluji si tvrdit, ze autor je mistrem ve svem oboru...

Predstavovanim googlu a jeho potencionalniho vyuziti by bylo asi nosenim drivi do lesa. Urcite vsichni vite, co vsechno google ve svem nitru schovava a co vse indexuje za stranky. Stranky pro nej sbiraji a indexuji roboti - skripty, mozna i samostatne pocitace, jenz hledaji webove servery, prolezaji zdrojove kody stranek a logicky zarazuji tyto stranky do databaze google. Ovsem sem tam naleznou i nejaky ten soubor, jenz by normalne nemel byt uzivateli pristupny. Stava se to v pripadech, kdy tvurce (webmaster) spatne stranky vytvoril - napriklad se ve zdrojovem kodu nachazi odkaz na soubor s hesly. Tim jsem vas seznamil s problematikou google a ukoncil bych tak uvod. Nasleduje prelozeny clanek:

Hackovani pomoci google je bezvadna vec. Pouzitim spravne upravenych vyhledavacich retezcu muzeme leckdy nalezt spoustu zajimavych informaci. Muzeme najit napriklad: Cisla kreditnich karet, hesla, software, pisnicky (MP3)... (a dalsi)
Texty uvedene nize jsou pouze zajimavymi priklady, jenz muzeme poslat googlu a z vysledku ziskat informace o nekterych lidech, z kterych by urcite oni sami nebyli moc nadseni... Pokud mate chut, zkuste svoje vlastni upravene vyhledavaci retezce pro ziskani uzitecnych informaci.

Zkuste par nasledujicich prikladu:

```
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: 300000000000000..399999999999999
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 (zlomitelnych) hesel, uzivatelskych jmen a e-mailovych adres pro DCForum a DCShop.

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

Ukaze stranky pouzivajici soubor config.php, ktery (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. Vyhneme 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, ktere 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 nedbalych 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 [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