TECHWEAVER BLOG

TUTTO IL BELLO DELLA TECNOLOGIA

Guida veloce ai Google Hacks

OK

Introduzione

Questa mini guida è stata fatta per aiutare anche i meno esperti ad utilizzare Google per fare ricerche mirate e talvolta anche per divertirsi (si fa per dire) a cercare bug nei siti web ovviamente a scopo educativo e non malevolo. Quindi cercherò di esprimermi il più chiaramente possibile ed ovviamente le cose più difficili ma meno utili le salterò e probabilmente le metterò in una delle prossime guide più avanzate.

Cos'è il Google hacking e come metterlo in atto

Il Google hacking è un metodo che utilizza comandi specifici (dork) per effettuare ricerche più che mirate su uno dei più famosi motori di ricerca a livello mondiale, Google appunto.

Cosa sono le Dork e come utilizzarle

Le dork o meglio le Google dork sono delle parole che identificano comandi (es. allinurl:http://ww…… vedremo dopo cosa significa) che se ricercate sul motore di ricerca danno origine a risultati spesso nascosti o omessi. Questi comandi quindi se scritti rispettando certi criteri sono davvero utilissimi; alcuni esempi dei loro utilizzi sono cercare formati di file specifici (come canzoni in .mp3), navigare nella directory di un sito (mappa del sito) oppure divertirsi a cercare falle nei portali o documenti riservati ai quali è stata omessa una certa sicurezza web.

Lista delle Dork più comuni, più usate e più utili

Nella tabella qui sotto potete vedere tutte le dork più comuni con relativa "spiegazione" ed esempio.

Dork	Utilizzo	Esempio
site:	i risultati della ricerca saranno file e pagine presenti nel dominio scritto dopo la dork "site:"	site:http://html.it/
intitle:	i risultati della ricerca conterranno nel titolo la parola scritta dopo la dork "intitle:"	intitle:ciao
allintitle:	i risulati della ricerca conterranno nel titolo le parole scritte dopo la dork "allintitle:"	allintitle:ciao a tutti
inurl:	i risultati della ricerca conterranno nell' URL (indirizzo web) la parola scritta dopo la dork "inurl:"	Inurl:aereonautica
allinurl:	i risultati della ricerca conterranno nell' URL le parole scritte dopo la dork "allinurl:"	allinurl:aereonautica comunicazioni
filetype:	i risultati di ricerca saranno tutti file con l'estensione dichiarata dopo la dork "filetype:"	filetype:mp3
link:	Limita la ricerca ai siti che in almeno una delle loro pagine compare l'URL specificato dopo la dork "link:"	link:www.google.it

allintext:	i risultati della ricerca avranno nella descrizione il testo indicato dopo la dork “allintext:”	allintext:notizie web
related:	l’url dei risultati di ricerca saranno simili a quello che è scritto dopo la dork “related:”	related:html.it
cache:	i risultati di ricerca apparterranno al data center delle cache di Google ovvero pagine che vengono salvate ogni tot. tempo	cache:html.it
info:	i risultati di ricerca ci forniranno informazioni sul sito del quale metteremo l’URL dopo la dork “info:”	info:html.it

Quelle che avete appena visto sono le dork più utilizzate dette anche operatori avanzati, ma se ci sono gli avanzati ci saranno anche gli operatori base no?

Operatori base

Gli operatori base sono meno usati ed è per questo che li ho messi dopo gli operatori avanzati, ma vediamo comunque cosa sono e come funzionano.

AND è usato se vogliano cercare due parole insieme es. verde blu (verde and blu).

OR è usato se vogliamo cercare una parola o l’altra es. verde or blu.

- (meno) in questo modo google non cercherà la parola dopo il meno (es. -ciao)

+ (più) in questo modo google non include nella ricerca parole come congiunzioni articoli ecc. in modo da facilitarla notevolmente.

***(asterisco)** in questo modo google nei risultati metterà tutte le parole derivate da per esempio sal* che saranno sala, salutare, saluto ecc.

“”(virgolette) con le virgolette possiamo cercare un intera frase che ritroveremo per intero nei risultati.

Esempi pratici utili

Adesso che conosciamo tutti i comandi per farci far vedere da Google quello che vogliamo noi e non quello che vuole lui possiamo iniziare a divertirci componendo le dork fra loro e trovando risultati che pochi conoscono.

1. Cercare brani online in vari formati musicali

Mettiamo che vogliamo sentire una canzone o scaricarla e non riusciamo a trovarla, come fare? Semplice su Google basta usare la dork filetype: più il nome della canzone. Ecco un esempio:

party rock filetype:mp3

2. Cercare file riservati come password

Il Google hacking spesso è anche usato per testare la sicurezza di un sito, ma dato che il motore di ricerca lo possiamo usare tutti perché non provare? Ecco come fare:

per cercare file di password in un sito italiano:

site:it filetype:pwd

per cercare file come scannerizzazioni, liste dei dipendenti di un azienda e documenti riservati possiamo utilizzare una dork del tipo:

allintitle:lista filetype:doc

Questi sono solo alcuni esempi, ma se volete provare vi consiglio di sbizzarrire la vostra fantasia per combinare operatori semplici e avanzati insieme. Se la ricerca alcune volte non dovesse avere risultati state tranquilli, vi posso assicurare che c'è molto molto materiale online.

Trucchetti e parole utili se vogliamo provare a testare la sicurezza dei siti

Sono sicuro che molti di voi si sono chiesti almeno una volta come facciano gli hacker a penetrare siti, modificare loro dati e grafica. Bene, premetto che questi non sono metodi che gli hacker usano nella maggior parte dei casi (infatti sono quasi banali visto che non tutti i siti per fortuna hanno falle così ben visibili da un motore di ricerca), ma sono comunque metodi buoni per provare a capire come funziona a grandi linee l'informatica.

Ecco qui di seguito un elenco di dork relative a web server e server vulnerabili, come potete notare sono tutte parole derivate da l'unione di dork specifiche.

Apache 1.3.0 intitle:index.of "Apache/1.3.0 Server at"
Apache 2.0 Intitle:Simple.page.for.Apache Apache.Hook.Functions

Apache SSL/TLS Intitle:test.page “Hey, it worked !” “SSL/TLS-aware”
Iss “Microsoft-IIS/* server at” intitle:index.of
Iss 4.0 “Microsoft-IIS/4.0” intitle:index.of
Iss 5.0 “Microsoft-IIS/5.0 server at”
Iss 6.0 “Microsoft-IIS/6.0” intitle:index.of
Matrix Appliance “Welcome to your domain web page” matrix
Kwiki “Congratulations! You’ve created a new Kwiki website.”
HP appliance sa1* intitle:”default domain page” “congratulations” “hp web”
Intel Netstructure “congratulations on choosing” intel netstructure
Generic Appliance “default web page” congratulations “hosting appliance”
iPlanet / Many intitle:”web server, enterprise edition”
Debian Apache intitle:”Welcome to Your New Home Page!” debian
J2EE / Many intitle:”default j2ee home page”
Resin / Many allintitle:Resin-Enterprise Default Home Page
Resin / Enterprise allintitle:default home page java web server
Jigsaw / 2.2.3 intitle:”jigsaw overview” “this is your”
XAMPP XAMPP “inurl:xampp/index”
Windows 2000 intitle:”Welcome to Windows 2000 Internet Services”
OpenBSD “powered by openbsd” +”powered by apache”
Red Hat Unix Administration intitle:”Page rev */*/*” inurl:”admin

Con questo conclude la mia guida e vi consiglio che se doveste trovare ad esempio bug nei siti di contattare sempre l’amministratore e di non utilizzare la falla per improvvisarvi hacker perchè sono sicuro che vi beccherebbero subito. Quindi io per questo non me ne assumo nessuna responsabilità. In ogni caso spero di essere stati chiaro e utile. Vi ricordo che il mio blog è il seguente:
http://techweaver11.altervista.org/