Titel: Google dorks

Auteur: Jasper Koehorst
Twitter: https://twitter.com/jaspkoehorst
Website/blog: http://jasperkoehorst.blog.com/

Waarschuwing: Deze informatie is ALEEN om te leren hoe dorks werken. Hacken is strafbaar en je kan gestraft worden als je deze informatie gebruikt om te hacken!

Inleiding:

Google is de meest gebruikte zoekmachine op het internet. Bijna alle websites zijn te vinden met google. Google is al sinds 1997 in de lucht. Google is genoemd naar het getal Googol. Larry Page, een van de oprichters, was gefascineerd door wiskunde en 'Googol'. De naam is uiteindelijk 'Google' geworden door een spelfout van Larry.
Maar google heeft ook een duistere kant: Google hacking (ook wel google dork genoemd). Dit zijn zoekopdrachten op maat. Officieel zijn dorks geen hacking, maar het wordt gretig gebruik door hackers.
Veel websites met een beveiligings lek kun je via google vinden. Stel de software joomla is lek (vaak gebeurt) dan hoef je alleen in te voeren: Powered by Joomla! En je hebt een lijst met websites die je kunt hacken.
Dit is met duizenden CMS software ook gebeurt en zal waarschijnlijk niet stoppen.
In deze PDF leg ik uit hoe google dorks in zijn werk gaat.

Admin panels vinden

Ook admin login panels zijn te vinden via google. Dit zijn wat dorks:
1:- ‘’filetype:asp admin login password inurl:admin’’
2:-‘’intitle:login filetype:php admin inurl:admin’’
Bug: veel admin panelen zijn te hacken via bypass.
Username: `' or '1'='1`
`Password ' or '1'='1`
`Zo heb je nog veel meer login bypass codes!`

Uitleg dork 1:

Nu leg ik uit wat dork 1 inhoudt (’filetype:asp admin login password inurl:admin’’)
Je ziet hier ’ filetype:’ dat betekent natuurlijk file.
En filetype:asp (Vindt je ASP bestanden)
Bij ‘INURL’: (in de url)
Als wij ASP veranderen in PHP krijg je alleen php bestanden.
Beveiligings fout: je kunt nu bestanden vinden, als je een lek in asp wilt vinden kun je dus alle ASP files vinden

Aanvallen op landen

Ook kunnen hackers een lijst krijgen met bijvoorbeeld Nederlandse sites. Dit is de dork: “Site:NL”(voor Nederland, je kunt het natuurlijk ook veranderen in BE (België) etc…
Nu kunnen wij deze dork maken: ”site:NL filetype:asp Inurl:admin intitle:login”
Met deze dork kun je dus Nederlandse inlog panelen vinden.

Website crawler

Via google is het ook mogelijk een lijst te krijgen van alle bestanden van een website (webcrawler)
Dit is een dork om een website te doorzoeken: “Site:www.tweedekamer.nl” (De link kun je natuurlijk ook veranderen)
Om bijvoorbeeld PDF bestanden te vinden doe je deze dork: site:tweedekamer.nl filetype:PDF
Om onbeschermde directories te vinden is deze dork vaak gebruikt: “intitle:index of /Icon Name Last modified Size Description”

PHP backdoor vinden via google

PHP Backdoors zijn php bestanden (C99shell bijvoorbeeld) die men toegang vershaft tot de beheer van een website, en soms zelfs de hele server. Deze bestanden worden door hackers geupload
Dit zijn wat dorks:
1 :- “safe-mode: off (not secure) drwxrwxrwx c99shell”
2:- “inurl:c99.php uid=0(root)”
3:-“ intitle:C99Shell v. 1.0 pre-release +uname”
4:- “webadmin.php copy, \, download, \, edit, \. File”
Foto: c99shell (Backdoor)

Wachtwoorden hash vinden:

“(username=* | username:* |) | (((password=* | password:*) | (passwd=* | passwd:”
Met deze dork kun je password hash vinden, je hebt online hash crackers (zie google) om het wachtwoord te ontcijferen.

XLS Wachtwoorden lijsten….

Deze dork: inurl:ftp "password" filetype:xls met deze dork kun je ook passwords vinden.

SQL-injectie targets vinden

Ook kun je natuurlijk met google websites vinden die gevoelig zijn voor SQL-injectie. Dit zijn de dorks:

“”inurl:index.php?id=””
“”inurl:trainers.php?id=””
“”inurl:buy.php?category=””
“”inurl:article.php?ID=””
“”inurllay_old.php?id=””
“”inurl:declaration_more.php?decl_id=””
(veel webwinkels zijn lek)

Gratis muziek

Ook kun je gratis muziek downloaden. Dit is een van de dorks:
intitle:index of / tiesto mp3 (tiesto kun je natuurlijk ook veranderen)

Upload formulieren (met bug)

Ook kunnen hackers een php backdoor uploaden via een foto upload formulier. Men noemt het bestand dan: “Backdoor.php.gif” (stiekem een php erin waardoor je php kunt uploaden, waar het eigenlijk niet mag)
Hier zijn de dorks:
“intitle:upload inurl:upload filetype:asp jpg gif”
“intitle:upload inurl:upload filetype:php jpg gif”
intitle:upload inurl:upload filetype:php jpg gif zip site:pl
En er zijn nog veel meer!

Preventie:

Je kunt voorkomen dat zoekmachines bestanden vinden door ‘robots.txt’ te uploaden naar je website, waarin je kan aangeven welke bestanden niet gevonden mogen worden.
Meer over Robots.txt vindt je op http://www.metatags.nl/sitebouw_tips_robotstxt