ÖN BİLGİ

Bir makale internetten bulunup şu adreste yedeklenmiştir.

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Google%20Dork%20Queries(ghdb).pdf

Bu belge ise yedeklenen bu makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Bilgisayar korsanları önemli bilgiler içeren web uygulamalarına arama motorları sayesinde kolayca erişebilmektedirler. Hedeflenen anahtar kelimeler ile web sitelerinden önemli bir bilgiyi almak saniyeler sürmektedir. Arama motoruna girilecek anahtar kelimeler ile dizin listelemeye açık dizinlere sahip web siteleri, belirtilen hata mesajlarını üreten web siteleri, çeşitli veritabanı dosya uzantılı dosyaları erişilebilir bırakmış web siteleri tespit edilebilmektedir ve bu bilgiler kötü yönde kullanılabilmektedir.

(Page 1)

2)

■ site: operatörü ile google'a sadece belirtilen domain'e sahip sonuçları döndür demiş oluruz.

> site:karabuk.edu.tr

■ filetype: operatörü ile google'a sadece belirtilen dosya uzantısına sahip linkleri döndür demiş oluruz.

> filetype:pdf

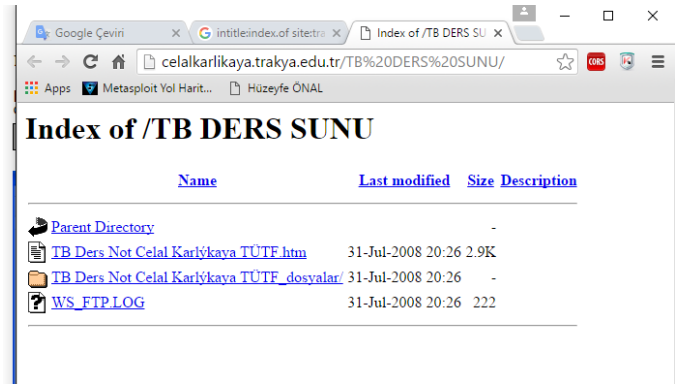
NOT:

Operatörler ardarda da kullanılabilmektedir. Mesela aşağıdaki örnekte google'ın pdf uzantılı ve karabuk.edu.tr domain'li linkleri döndürmesi sağlanmıştır.

> *filetype:pdf site:karabuk.edu.tr*

■ intitle: operatörü ile google'a sadece listelemeye açık sitelerin linklerini döndür demiş oluruz.

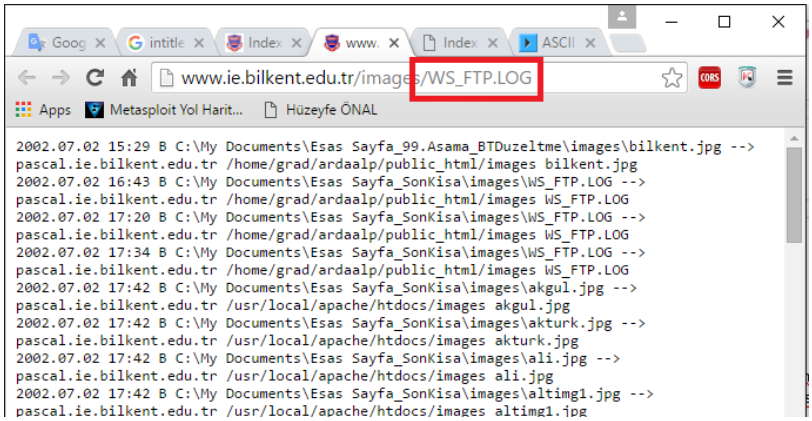
> intitle:index.of site:trakya.edu.tr



• Eğer belirli bir dosyayı barındıran listelemeye açık websitelerini görmek istiyorsak intitle:index.of ifadesi sonrası istenilen dosyanın ismi yazılır.

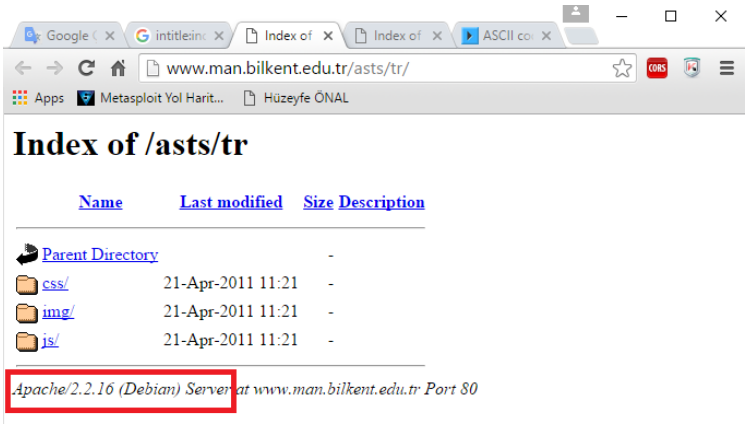
> intitle:index.of ws_ftp.log

ws_ftp.log dosyası ftp olaylarının log'landığı dosyadır. Bu dosya ftp ile ilgili özel bilgiler içerebilir.



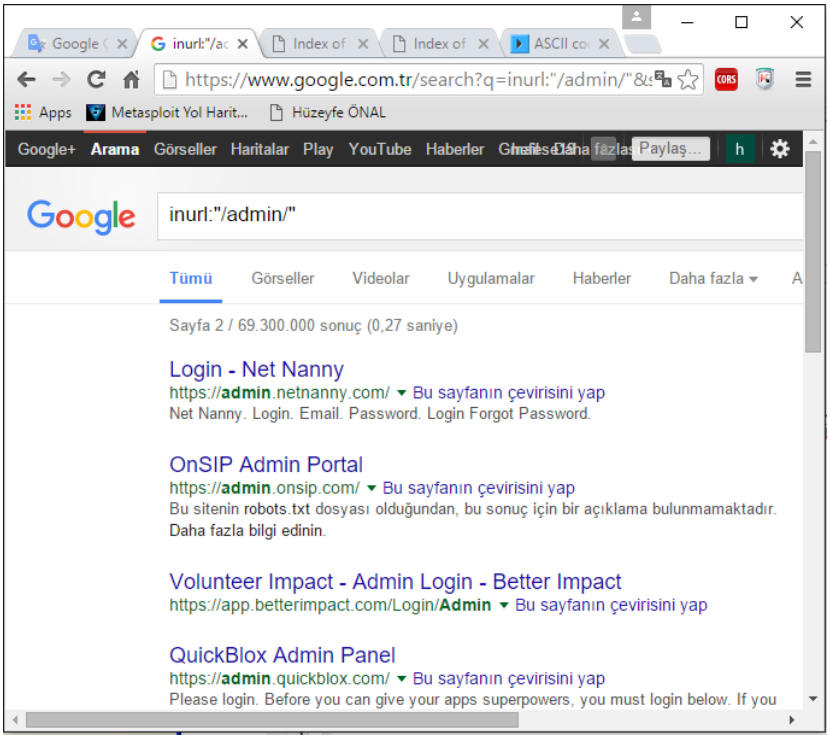
• Listelemeye açık siteleri veren intitle:index.of operatörü sonrası "server at" anahtar kelimesi kullanılırsa sitelerin sunucu yazılımı ve versiyonunu öğrenebiliriz.

> intitle:index.of "server at"   site:bilkent.edu.tr



■ inurl: operatörü ile arama yapılarak google'a sadece belirtilen dizini içeren linkleri döndür demiş oluruz. Mesela aşağıdaki örnek ile url'sinde admin kelimesi geçen siteleri google'a sıralatmış oluruz.

> inurl:"/admin/"



• admin dizini olan listelemeye açık siteleri görüntülemek için aşağıdaki dork kullanılabilir:

> intitle:index.of inurl:"/admin/"

(Page 3-7)

3)

Geniş bir kesim tarafından kullanılan phpBB (Popular Open Source Forum Software) forum scriptinde güvenlik zafiyeti bulan saldırgan ilgili exploit'i denemek için phpBB kullanan web sitelerini topluca bulan bir dork kullanabilir.

> "Powered by phpBB" inurl:"index.php?s" OR inurl:"index.php?style"

Böylece bulduğu exploit'i (http://www.milw0rm.com/exploits/1469) google'da listelenen sitelerden birine uygulayarak hedefine ulaşabilir.

Not: Bahsedilen örnekte "Powered by phpBB" ile bu yazıyı sayfalarında içeren web siteleri aranmıştır. Bunun gibi daha birçok string girilebilir ve arzulanan servisi kullanan web sitelerini google'a listelettirebiliriz.

Query	Vulnerability
"Powered by A-CART"	A-CART 2.x vulnerable to cross-site scripting
inurl:"dispatch.php?atknodetype" | inurl:class.atkdateattribute.js.php	Achievo .8.x could allow remote code execution
intitle:guestbook "advanced guestbook 2.2 powered"	Advanced Guestbook v2.2 has an SQL injection problem that allows unauthorized access
"Powered by AJ-Fork v.167"	AJ-Fork, a fork based on the CuteNews 1.3.1 core, is susceptible to multiple vulnerabilities
"BlackBoard 1.5.1-f | ¬© 2003-4 by Yves Goergen"	BlackBoard 1.5.1 has a remote file inclusion vulnerability
"BosDates Calendar System " "powered by BosDates v3.2 by BosDev"	BosDates 3.2 is vulnerable to SQL injection
inurl:changepassword.cgi —cvs	changepassword.cgi allows for unlimited repeated failed login attempts
"Copyright ¬© 2002 Agustin Dondo Scripts"	CoolPHP 1.0 has multiple vulnerabilities
"Powered by CubeCart 2.0.1"	CubeCart 2.0.1 has an SQL injection vulnerability
*"Powered *: newtelligence" ("dasBlog 1.6"| "dasBlog 1.5"| "dasBlog 1.4"|"dasBlog 1.3")*	DasBlog versions 1.3–1.6 are susceptible to an HTML injection vulnerability in their request log
"Powered by DCP-Portal v5.5"	DCP-Portal version 5.5 is vulnerable to SQL injection
"2003 DUware All Rights Reserved"	DUForum 3.0 may allow a remote attacker to carry out SQL injection and HTML injection attacks
"inurl:/site/articles.asp?idcategory="	Dwc_Articles 1.6 has multiple input validation problems
inurl:custva.asp	EarlyImpact Productcart v1.5 contains multiple vulnerabilities
inurl:"/becommunity/community/index.php?pageurl="	E-market prior to 1.4.0 contains various vulnerabilities
intitle:"EMUMAIL - Login" "Powered by EMU Webmail"	EMU Webmail 5.6 messaging product is susceptible to a cross-site scripting vulnerability
"Powered by FUDforum"	FUDforum 2.0.2 allows manipulation of arbitrary server files
"1999-2004 FuseTalk Inc" -site:fusetalk.com	FuseTalk forums (v4) are susceptible to cross-site scripting attacks
"Powered by My Blog" intext: "FuzzyMonkey.org"	FuzzyMonkey 2.11 has an SQL injection vulnerability
"Powered by Gallery v1.4.4"	Gallery 1.4.4 allows remote code execution
intitle:gallery inurl:setup "Gallery configuration"	Gallery default configuration files allow gallery modification
inurl:"messageboard/Forum.asp?"	GoSmart Message Board (specific versions) are susceptible to SQL injection attack and cross-site scripting attack
intitle:welcome.to.horde	Horde Mail prior to 2.2 has had several reported vulnerabilities
"Powered by IceWarp Software" inurl:mail	IceWarp Web Mail (versions prior to 5.2.8) is reported prone to multiple input validation vulnerabilities
"Ideal BB Version: 0.1" -idealbb.com	Ideal BB 0.1 is susceptible to multiple vulnerabilities
"Powered by Ikonboard 3.1.1"	IkonBoard 3.1.1 allows cross-site scripting
*"Powered by Invision Power Board(U) v1.3 Final ¬© *"*	Invision Power Board v1.3 is vulnerable to SQL injection
inurl:wiki/MediaWiki	MediaWiki 1.3.5 has a cross-site scripting vulnerability
*"Powered by Megabook *" inurl:guestbook.cgi*	MegaBook 2.0 is prone to multiple HTML injection vulnerabilities
"Powered by mnoGoSearch - free Web search engine software"	mnGoSearch 3.1.20 and 3.2.10 contain a buffer overflow vulnerability

4)

Microsoft-IIS/5.0 web sunucu yazılımını kullanan server’ları tespit etmek için arama motoruna aşağıdaki sorgu girilebilir:

> "Microsoft-IIS/5.0 server at"

Veyahut apache versiyon 1.3.27 kullanan server’ları google’a listeletmek için aşağıdaki sorgu girilebilir:

> "Apache/1.3.27 server at"