

Ön Söz

Bilgisayar korsanları, önemli bilgiler içeren web uygulamalarına arama motorları sayesinde kolayca erişebiliyorlar. Hedeflenen anahtar kelimeler ile web sitelerinden önemli bilgiyi almak saniyeler sürüyor.

Dizin listelemeye açık dizinler, hata mesajları, yönetici veya kullanıcı bilgileri/dosyaları, çeşitli veritabanı dosyaları veya önemli veri içeren dosyalar, sunucular hedeflenerek önemli bilgiler elde edilir.

Örneğin ; Hedef bir firma hakkında genel iletişim bilgileri , telefon numaraları, e-postaları, şirket yapısı gibi gibi bilgiler, güvenlik zaafiyeti olan uygulamaya sahip adresler, web server bilgileri arama motorları sayesinde kolayca elde edilebilmekte.

Belge mümkün olduğu kadar kısa ve basit tutulmuş ve saldırganların hacking yaparken Google arama motorunu nasıl etkili şekilde kullandıkları somut örneklerle anlatılmıştır.

Google Hacking

Google en iyi ve en geniş içeriğe sahip kendini kanıtlamış bir arama motorudur. Google örümcekleri sıklıkla sitelerini ziyaret eder ve içeriğini (sayfalar , klasörler ,dizinler vb.) indeksleyerek veritabanına kaydeder.

Arama sonuçlarında belirli kriterlere göre sıralar.

Temel kullanım bilgilerini aşağıdaki adresten öğrenebilirsiniz;

<http://www.google.com/help/basics.html>

Gelişmiş Google Operatörleri

Google, kendisi için özel anlama sahip sorgu kelimeleri olan çeşitli gelişmiş operatörleri destekler. Tipik olarak bu operatörler arama işlemini etkilemekte ve hatta Google'a farklı türde arama yapmasını söylemektedirler.

Google gelişmiş operator listesine aşağıdaki adresten ulaşabilirsiniz;

<http://www.google.com/help/operators.html>

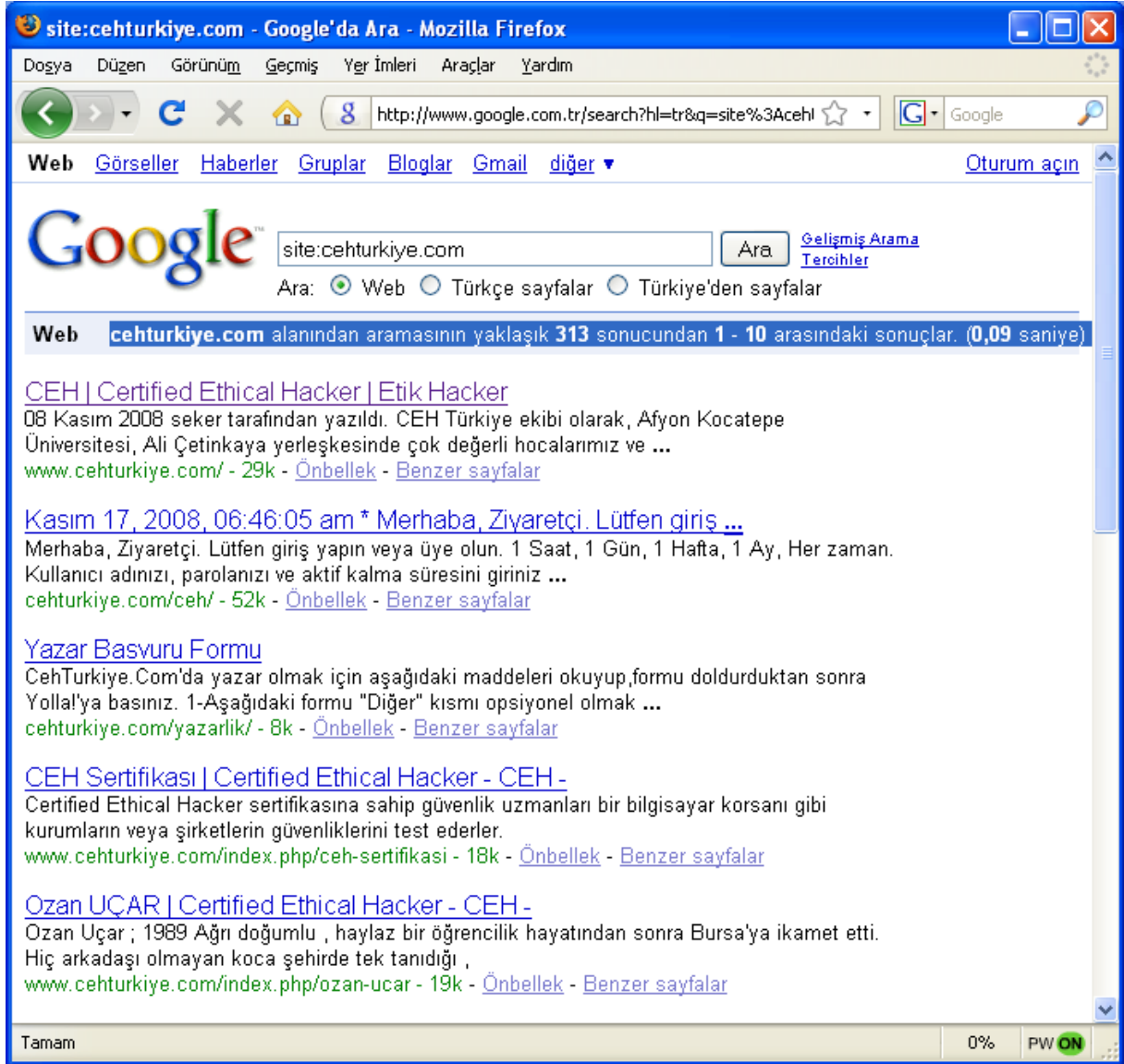
Bir Domain İçin Arama

[site:] operatörü ile arama yapılarak Google sonuçları, istenilen alan adındaki web siteleriyle sınırlandırılabilir.

Bir örnek ile inceleyelim :

Örnek #1 :

site:cehturkiye.com



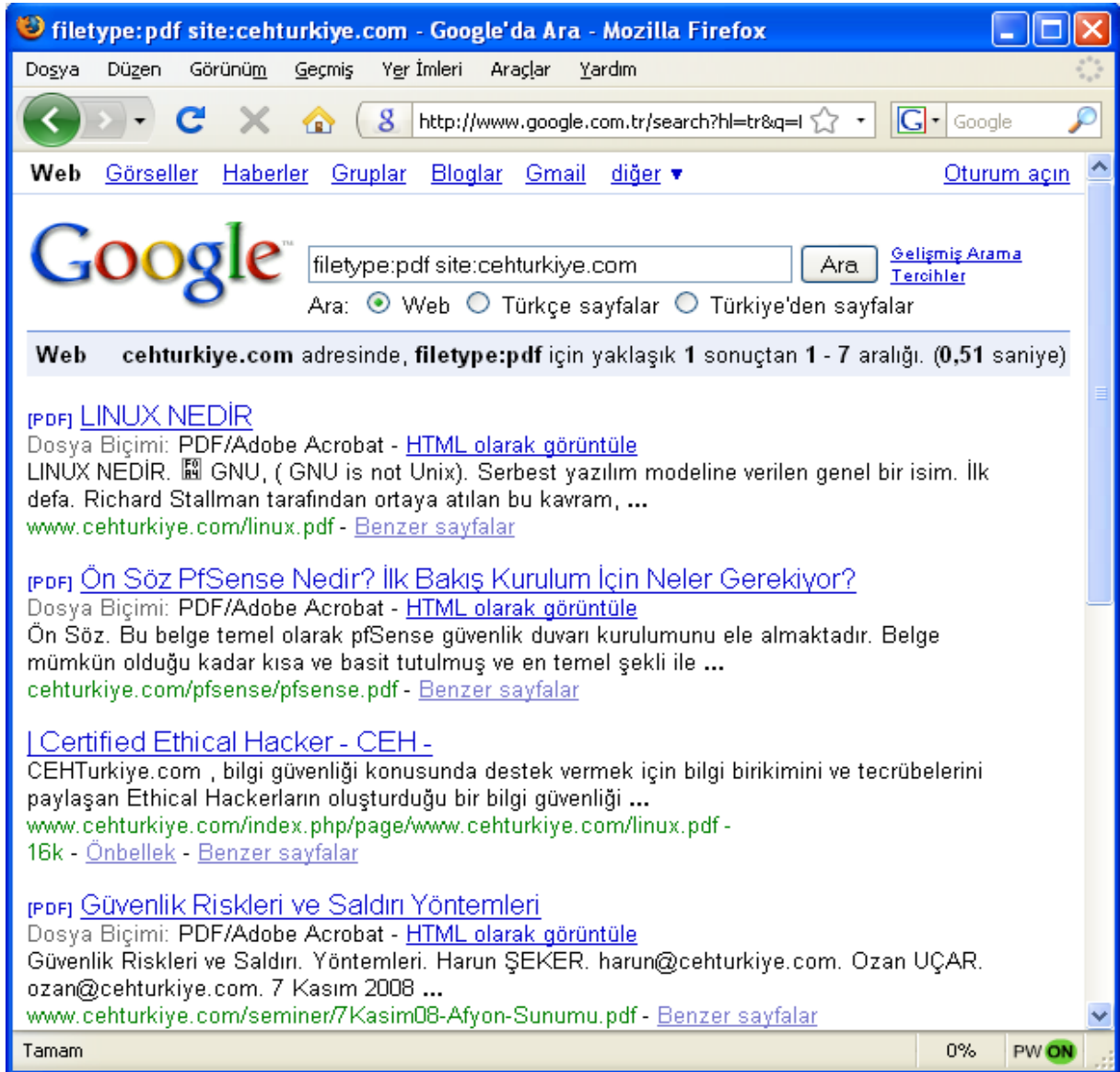
Yukarıdaki resimde de görüldüğü gibi google , daha önce farklı zamanlarda hedef site (cehturkiye.com) ile ilgili gezip keşfettiği ve veritabanına kaydettiği tüm içeriği sundu.

Özel Dosya Arama

[Filetype:] operatörü ile evrensel olarak google ön belleğinde olan siteler üzerinde veya hedef bir site üzerinde istenilen dosya türü listelenebilir ;
Örnek #2:

filetype:pdf site:cehturkiye.com

cehturkiye.com da bulunan .pdf uzantılı dosyaları listeleyebiliriz.
Bu arama tekniği örneklerle çoğaltılabilir.Saldırganların hedef site üzerinde bulmak istedikleri uzantıları aramakta sıklıkla kullanırlar.



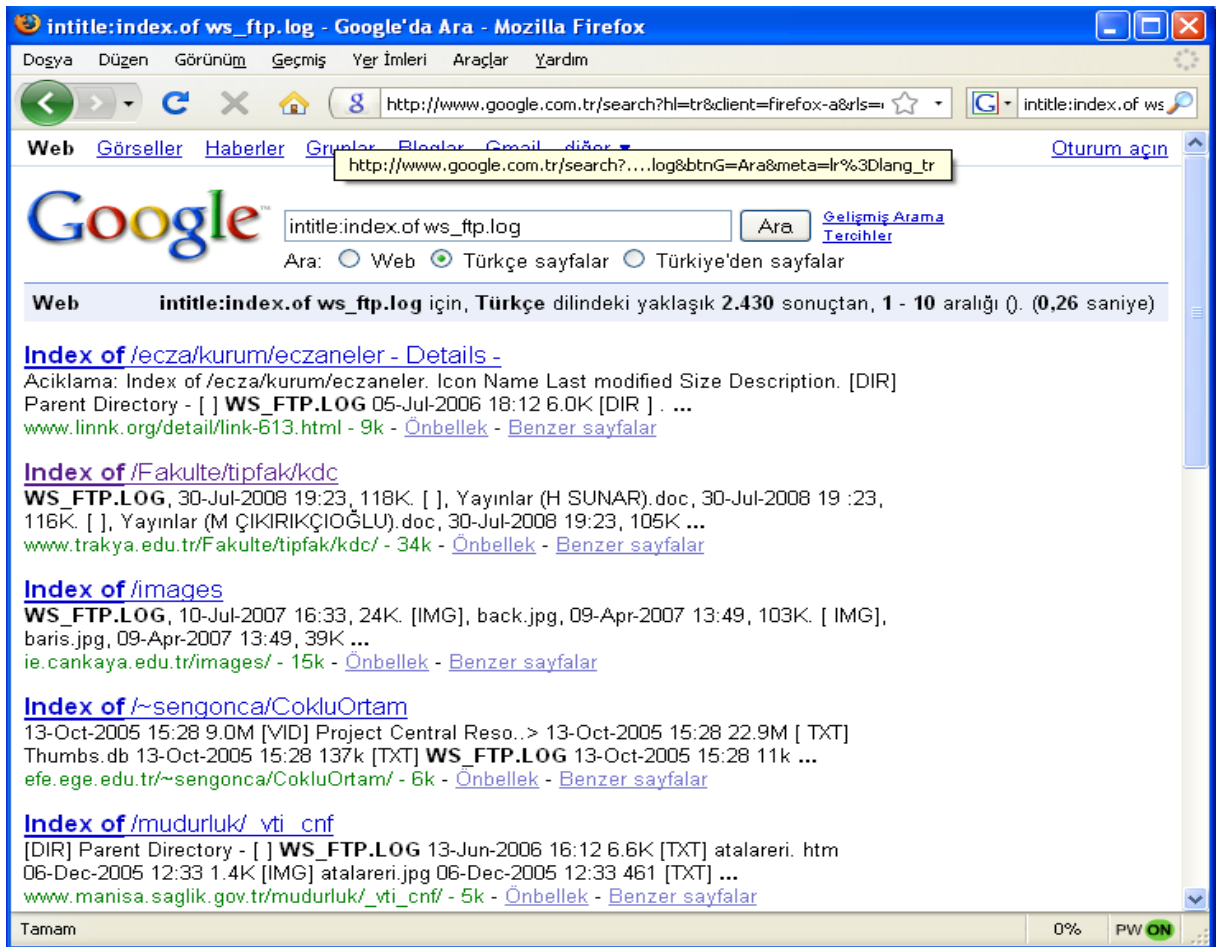
The screenshot shows a Mozilla Firefox browser window with the title "filetype:pdf site:cehturkiye.com - Google'da Ara - Mozilla Firefox". The address bar contains the search query "http://www.google.com.tr/search?hl=tr&q=I". The search results page displays the Google logo and the search query "filetype:pdf site:cehturkiye.com". Below the search bar, there are radio buttons for "Web", "Türkçe sayfalar", and "Türkiye'den sayfalar". The search results section shows "Web cehturkiye.com adresinde, filetype:pdf için yaklaşık 1 sonuçtan 1 - 7 aralığı. (0,51 saniye)". The first result is "[PDF] LINUX NEDİR" with a description: "Dosya Biçimi: PDF/Adobe Acrobat - HTML olarak görüntüle LINUX NEDİR. GNU, (GNU is not Unix). Serbest yazılım modeline verilen genel bir isim. İlk defa. Richard Stallman tarafından ortaya atılan bu kavram, ... www.cehturkiye.com/linux.pdf - Benzer sayfalar". The second result is "[PDF] Ön Söz PfSense Nedir? İlk Bakış Kurulum İçin Neler Gerekliyor?" with a description: "Dosya Biçimi: PDF/Adobe Acrobat - HTML olarak görüntüle Ön Söz. Bu belge temel olarak pfsense güvenlik duvarı kurulumunu ele almaktadır. Belge mümkün olduğu kadar kısa ve basit tutulmuş ve en temel şekli ile ... cehturkiye.com/pfsense/pfsense.pdf - Benzer sayfalar". The third result is "[Certified Ethical Hacker - CEH -" with a description: "CEHTurkiye.com , bilgi güvenliği konusunda destek vermek için bilgi birikimini ve tecrübelerini paylaşan Ethical Hackerların oluşturduğu bir bilgi güvenliği ... www.cehturkiye.com/index.php/page/www.cehturkiye.com/linux.pdf - 16k - Önbellek - Benzer sayfalar". The fourth result is "[PDF] Güvenlik Riskleri ve Saldırı Yöntemleri" with a description: "Dosya Biçimi: PDF/Adobe Acrobat - HTML olarak görüntüle Güvenlik Riskleri ve Saldırı Yöntemleri. Harun ŞEKER. harun@cehturkiye.com. Ozan UÇAR. ozan@cehturkiye.com. 7 Kasım 2008 ... www.cehturkiye.com/seminer/7Kasim08-Afyon-Sunumu.pdf - Benzer sayfalar". The browser status bar at the bottom shows "Tamam", "0%", and "PW ON".

Dizin Listeleme

[intitle:] operatörü kullanılarak **intitle:index.of** ile dizinler listelenebilir.

Örnek #3 :

intitle:index.of ws_ftp.log



ws_ftp.log anahtar kelimesini ekleyerek ws_ftp.log dosyasının olduğu dizinleri listeleyebiliriz. ws_ftp.log dosyası ; ftp olaylarının kayıt edildiği dosyadır bulunduğu adresdeki ftp olayları ile ilgili özel bilgiler görüntülenebilir.

Örnek;

http://www.trakya.edu.tr/Fakulte/tipfak/kdc/WS_FTP.LOG

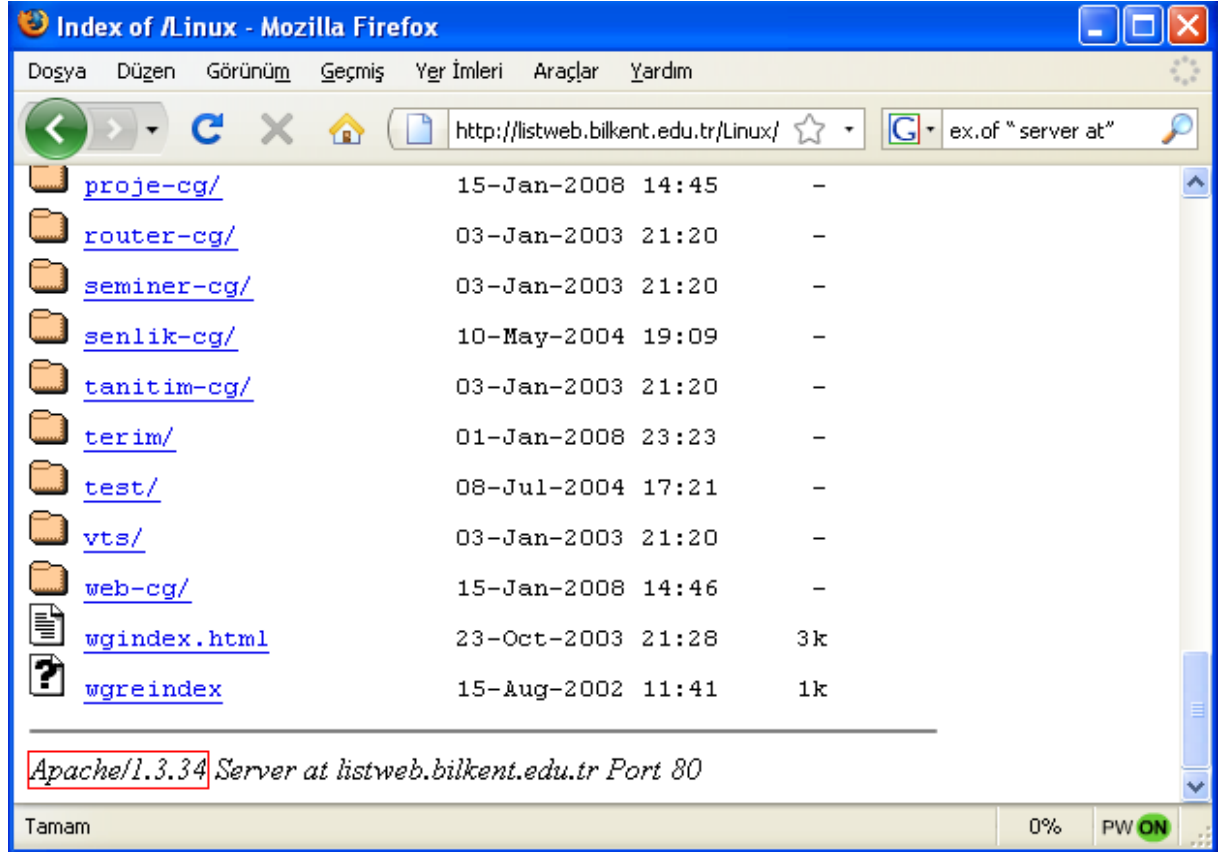
104.12.31 16:18 B

e:\DocumentsandSettings\umid\MyDocuments\wwwroot_31_05_2004\Fakulte\tipfak\kdc\Hasta_Bilgilendirme_kitabi.pdf --> 193.255.140.21 /var/www/html/a1/kdc Hasta_Bilgilendirme_kitabi.pdf

Örnek #4 :

intitle:index.of "server at"

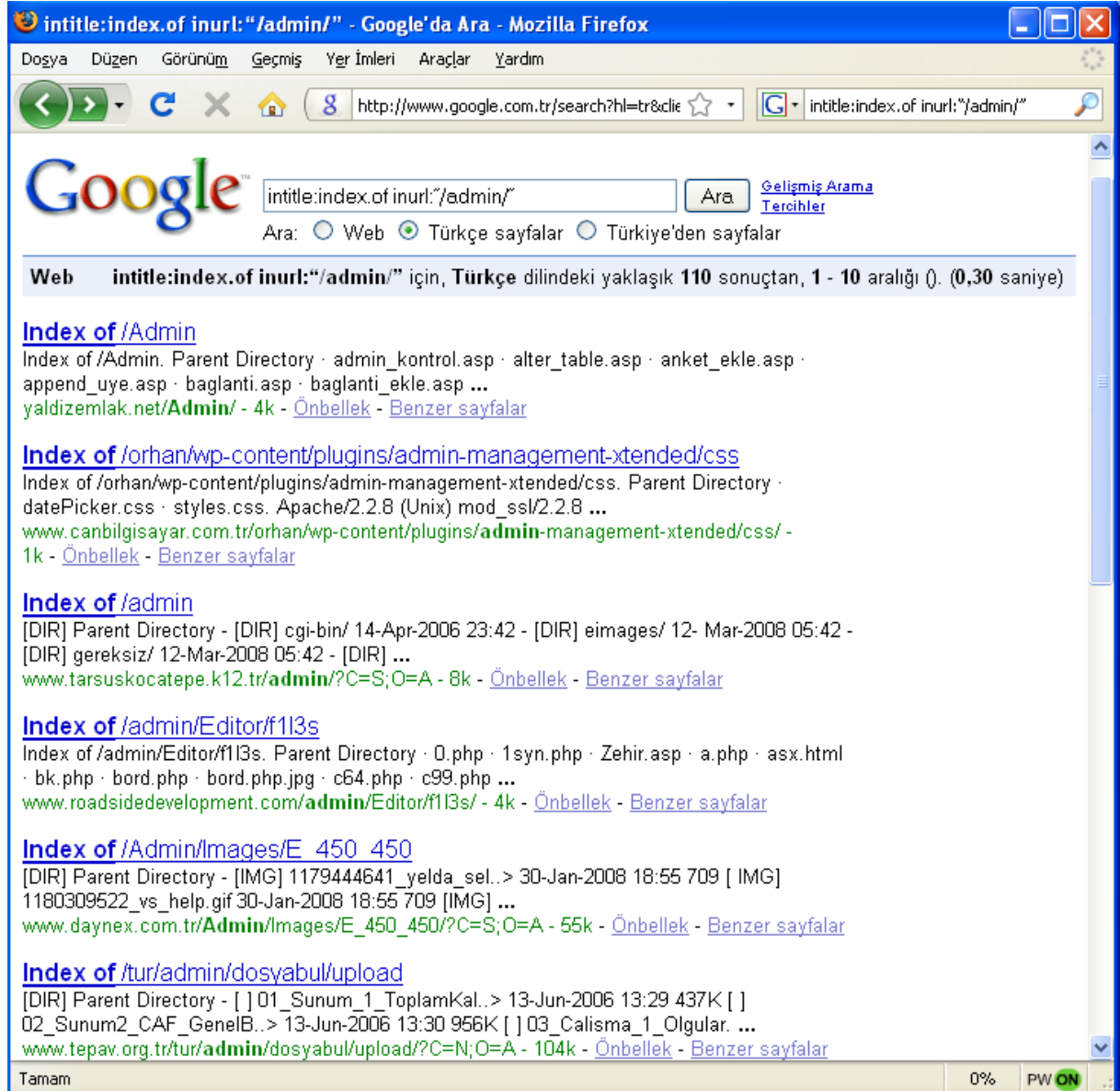
Özel dizinleri listelerken "server at" anahtar kelimesini ekleyerek sitelerin sunucu bilgisini öğrenebiliriz. Bu örnekler çoğaltılabilir ve amaca göre farklı aramalar gerçekleştirilebilir.



Örnek #5 :

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

intitle:index.of ile birlikte **inurl:"/admin/"** yazarak admin dizini olan listelemeye açık siteleri görüntüleyebiliriz.



The screenshot shows a Mozilla Firefox browser window with the title "intitle:index.of inurl:\"/admin/\" - Google'da Ara". The address bar contains "http://www.google.com.tr/search?hl=tr&clie". The search bar contains the query "intitle:index.of inurl:\"/admin/\"". The search results are displayed in Turkish, showing several links to directories and websites. The first result is "Index of /Admin" with a description of a parent directory containing files like "admin_kontrol.asp" and "alter_table.asp". The second result is "Index of /orhan/wp-content/plugins/admin-management-xtended/css" with a description of a parent directory containing files like "datePicker.css" and "styles.css". The third result is "Index of /admin" with a description of a parent directory containing files like "cgi-bin/" and "eimages/". The fourth result is "Index of /admin/Editor/f113s" with a description of a parent directory containing files like "0.php" and "1syn.php". The fifth result is "Index of /Admin/Images/E_450_450" with a description of a parent directory containing files like "1179444641_yelda_sel.." and "1180309522_vs_help.gif". The sixth result is "Index of /tur/admin/dosyabul/upload" with a description of a parent directory containing files like "01_Sunum_1_ToplamKal.." and "02_Sunum2_CAF_GenelB..". The status bar at the bottom shows "Tamam", "0%", and "PW ON".

Güvenlik Zaafiyeti Olan Web Uygulamalarının Tespiti

Saldırganlar ve kötü niyetli hackerlar güvenlik zaafiyetini keşfettikleri uygulamalara sahip siteleri bulmak için arama motorlarını sıkca kullanırlar.

Örnek web açıklıkları ve google arama yöntemleri

Query	Vulnerability
"Powered by A-CART"	A-CART 2.x vulnerable to cross-site scripting
<i>inurl:"dispatch.php?atknodetype" inurl:*.atknodateattribute.js.php</i>	Achievo .8.x could allow remote code execution
<i>intitle:guestbook "advanced guestbook 2.2 powered"</i>	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
<i>inurl:changepassword.cgi --cvs</i>	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 by: 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
<i>inurl:/site/articles.asp?idcategory=</i>	Dwc_Articles 1.6 has multiple input validation problems
<i>inurl:custva.asp</i>	EarlyImpact Productcart v1.5 contains multiple vulnerabilities
<i>inurl:"ibecomunity/community/index.php?pageurl="</i>	E-market prior to 1.4.0 contains various vulnerabilities
<i>intitle:"EMUMAIL - Login" "Powered by EMU Webmail"</i>	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
<i>intitle:gallery inurl:setup "Gallery configuration"</i>	Gallery default configuration files allow gallery modification
<i>inurl:"messageboard/Forum.asp?"</i>	GoSmart Message Board (specific versions) are susceptible to SQL injection attack and cross-site scripting attack
<i>intitle:welcome.to.horde</i>	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
<i>inurl:wikiMediaWiki</i>	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"	mnoGoSearch 3.1.20 and 3.2.10 contain a buffer overflow vulnerability

Örnek #6 :

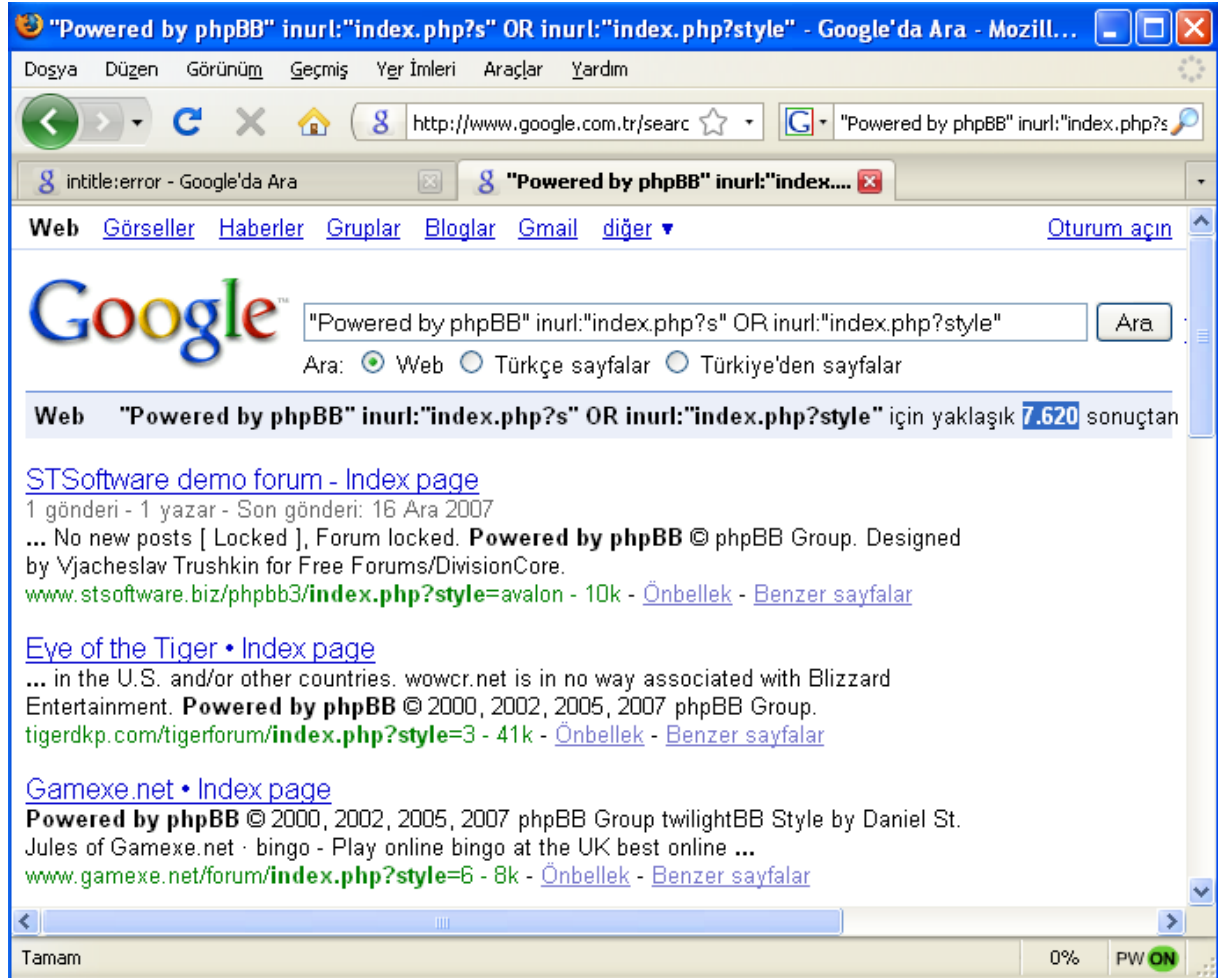
Geniş bir kesim tarafından kullanılan phpBB (popular open source forum software) forum scriptinde güvenlik zaafiyeti bulan saldırgan phpBB kullanan web sitelerini topluca bulmak isteyecektir. Bunun için google.com da küçük bir arama ile hızlıca google önbelleğinde ki tüm phpBB kullanan siteleri tespit edebilir.

Güvenlik zaafiyetinin duyurusuna ve exploit kodlarına aşağıdaki adresten erişebilirsiniz:

<http://www.milw0rm.com/exploits/1469>

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

Yapılan arama için yaklaşık 7.620 kayıt bulundu :)



The screenshot shows a Mozilla browser window with the title "Powered by phpBB" inurl:"index.php?s" OR inurl:"index.php?style" - Google'da Ara - Mozill... The address bar shows the search URL. The search results are displayed in a list format with the following entries:

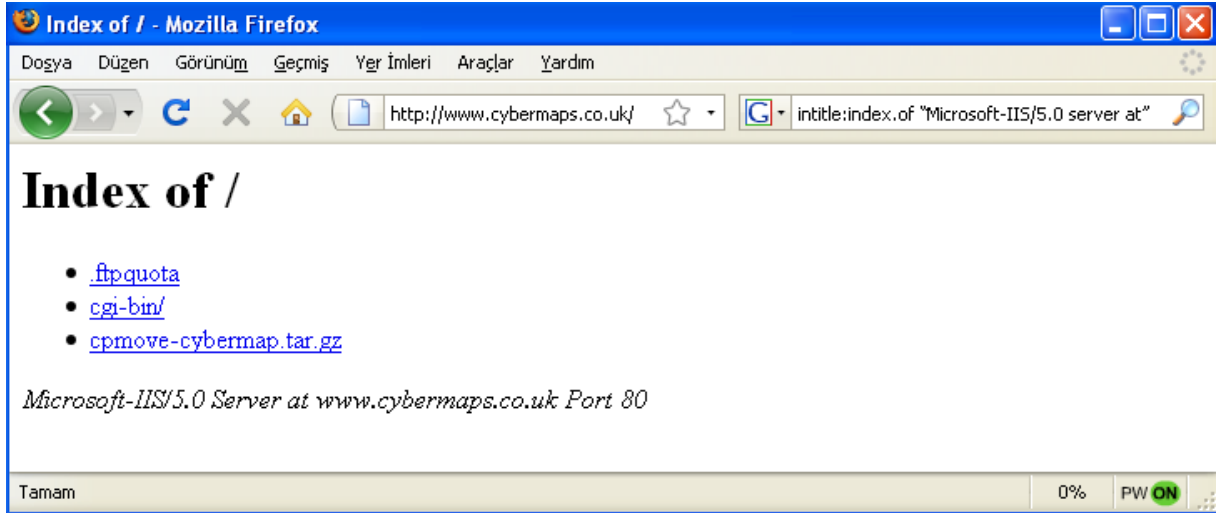
- Web** [STSoftware demo forum - Index page](#)
1 gönderi - 1 yazar - Son gönderi: 16 Ara 2007
... No new posts [Locked], Forum locked. **Powered by phpBB** © phpBB Group. Designed by Vjacheslav Trushkin for Free Forums/DivisionCore.
[www.stsoftware.biz/phpbb3/index.php?style=avalon](#) - 10k - [Önbellek](#) - [Benzer sayfalar](#)
- Web** [Eye of the Tiger • Index page](#)
... in the U.S. and/or other countries. wowcr.net is in no way associated with Blizzard Entertainment. **Powered by phpBB** © 2000, 2002, 2005, 2007 phpBB Group.
[tigerdkp.com/tigerforum/index.php?style=3](#) - 41k - [Önbellek](#) - [Benzer sayfalar](#)
- Web** [Gamexe.net • Index page](#)
Powered by phpBB © 2000, 2002, 2005, 2007 phpBB Group twilightBB Style by Daniel St. Jules of Gamexe.net · bingo - Play online bingo at the UK best online ...
[www.gamexe.net/forum/index.php?style=6](#) - 8k - [Önbellek](#) - [Benzer sayfalar](#)

The browser status bar at the bottom shows "Tamam", "0%", and "PW ON".

Web Serverlerin Tespiti

“Microsoft-IIS/5.0 server at”

Microsoft-IIS/5.0 web serverları tespit etmek için “Microsoft-IIS/5.0 server at” sorgusu kullanılabilir.



“Apache/1.3.27 Server at”

Apache web serverları tespit etmek için “Apache/1.3.27 Server at” sorgusu kullanılabilir.

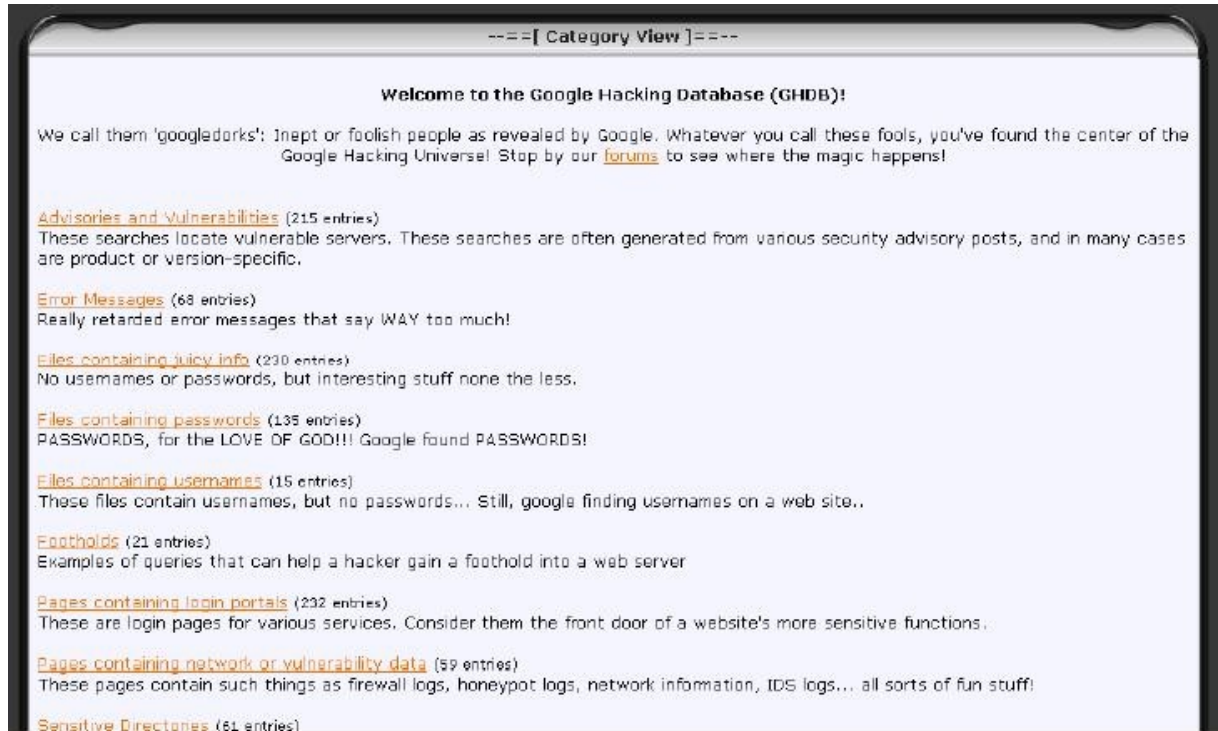


Google Hacking Araçları

Google Hacking Database (GHDB)

Hassas ve önemli bilgilere erişmek için google arama sorgularını içerir. Daha fazlası için aşağıdaki adresi ziyaret edebilirsiniz;

<http://johnny.ihackstuff.com>



--=[Category View]=--

Welcome to the Google Hacking Database (GHDB)!

We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe! Stop by our [forums](#) to see where the magic happens!

[Advisories and Vulnerabilities](#) (215 entries)
These searches locate vulnerable servers. These searches are often generated from various security advisory posts, and in many cases are product or version-specific.

[Error Messages](#) (68 entries)
Really retarded error messages that say WAY too much!

[Files containing juicy info](#) (230 entries)
No usernames or passwords, but interesting stuff none the less.

[Files containing passwords](#) (135 entries)
PASSWORDS, for the LOVE OF GOD!!! Google found PASSWORDS!

[Files containing usernames](#) (15 entries)
These files contain usernames, but no passwords... Still, google finding usernames on a web site..

[Footholds](#) (21 entries)
Examples of queries that can help a hacker gain a foothold into a web server

[Pages containing login portals](#) (232 entries)
These are login pages for various services. Consider them the front door of a website's more sensitive functions.

[Pages containing network or vulnerability data](#) (59 entries)
These pages contain such things as firewall logs, honeypot logs, network information, IDS logs... all sorts of fun stuff!

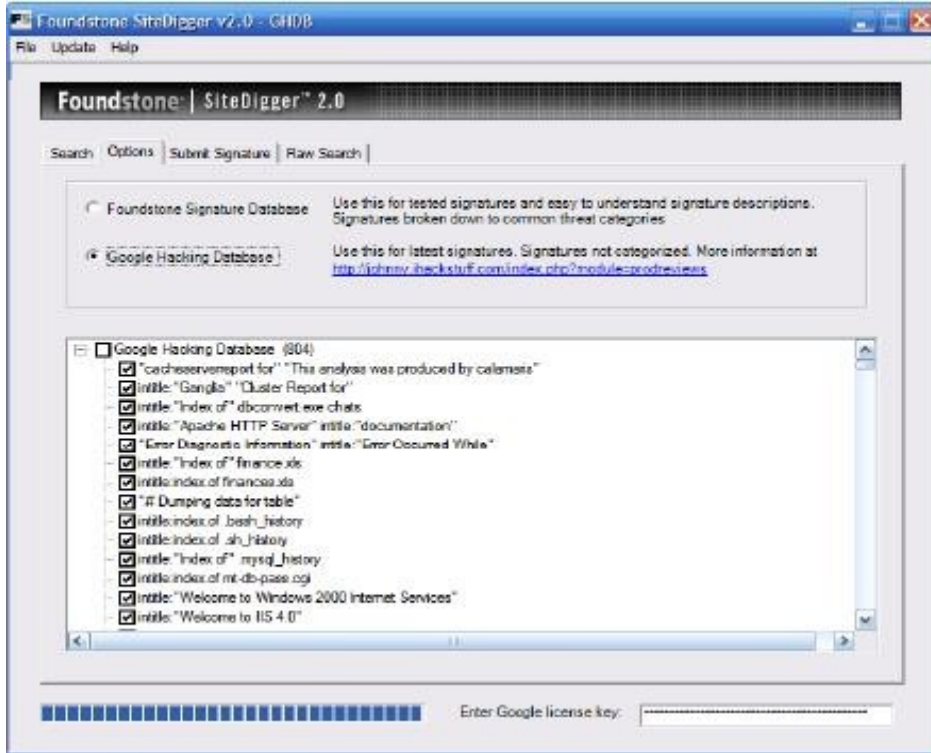
[Sensitive Directories](#) (61 entries)

SiteDigger Tool

Google önbelleğinde değişik güvenlik zaafiyetleri, hataları, yanlış konfigürasyonu olan siteleri bulmak için kullanılan güzel bir araçtır.

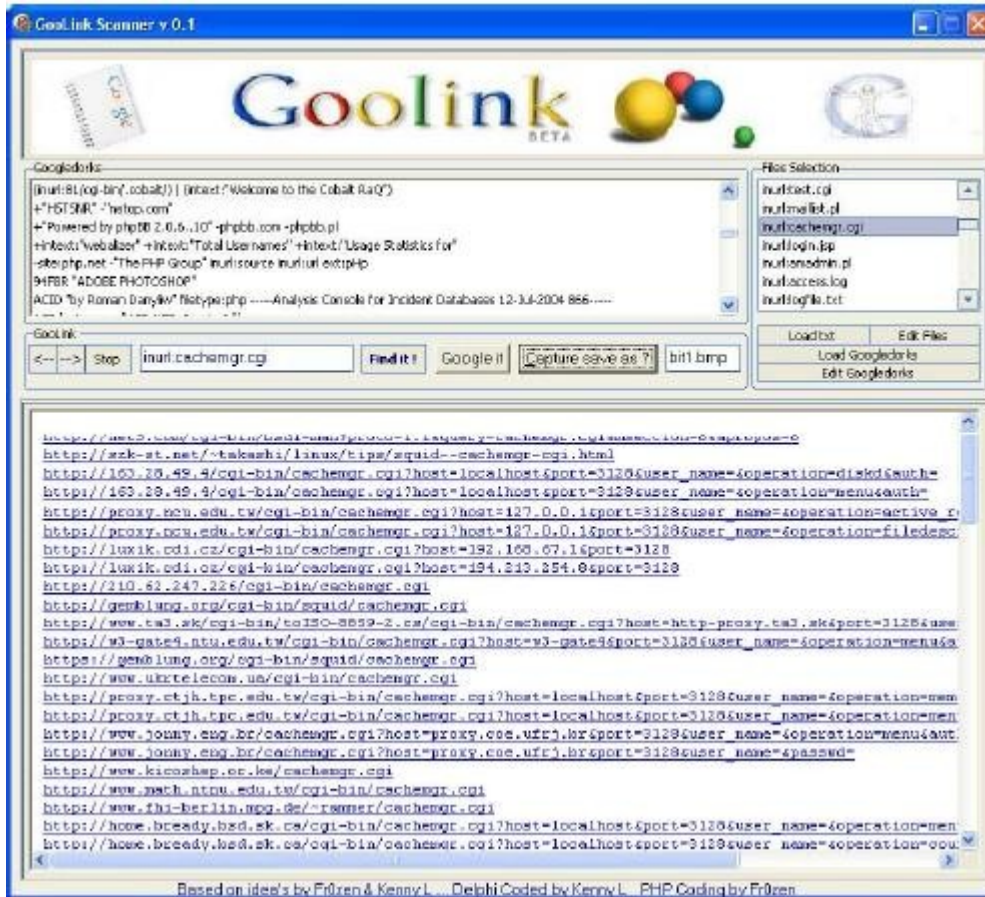
SiteDigger için aşağıdaki adresi ziyaret edebilirsiniz;

<http://www.foundstone.com/us/resources/proddesc/sitedigger.htm>



Goolink Scanner

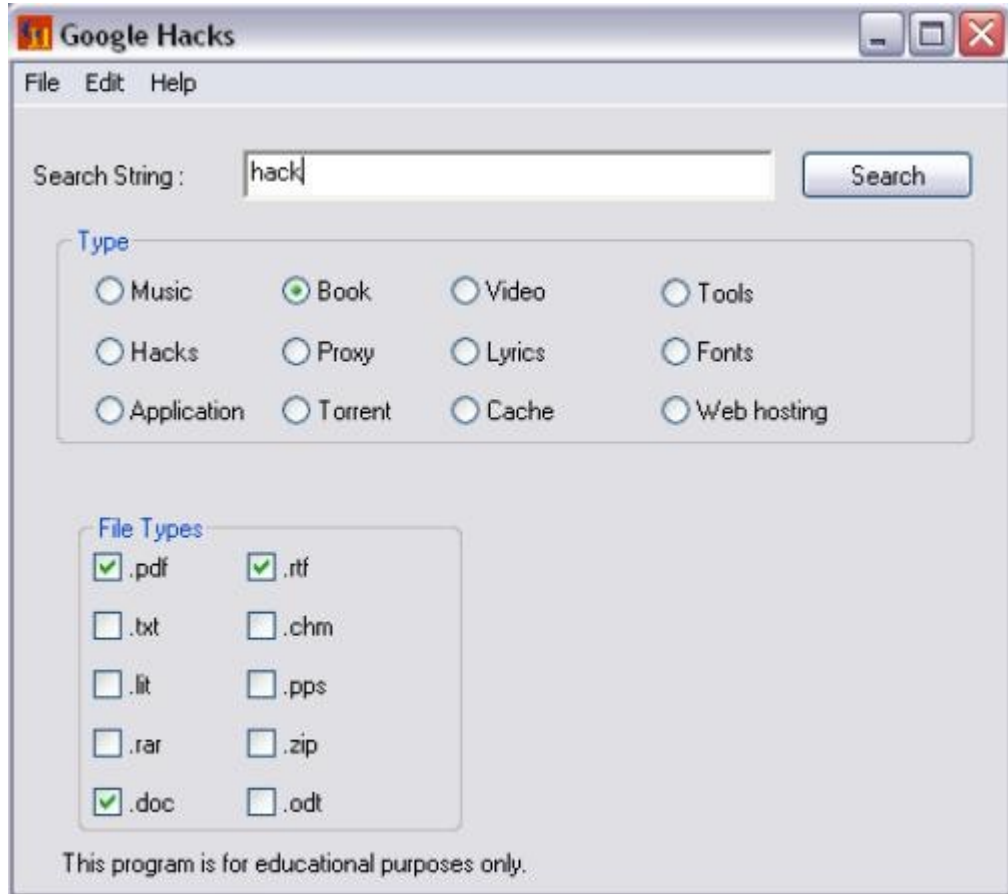
SiteDigger Tool ile benzer görevi yapan pratik bir araç.



Google Hacks

(code.google.com/p/googlehacks/)

Belirttiğiniz dosya ve dosya uzantılarına göre google önbelleğinde arama yapar. Müzik , kitap, video, araç vs. aramak için ideal bir araç.



Belge Ozan UÇAR tarafından yazılmıştır ve yazarın ismine sadık kalmak kaydı ile belge izin alınmaksızın her şekilde paylaşılabilir ve dağıtılabilir.

Referanslar

www.google.com

www.cehturkiye.com

johnny.ihackstuff.com

www.milw0rm.com