

GOOGLE DORKİNG(GOOGLE HACKİNG) VE KATANA DORK SCANNER

GOOGLE NEDİR?

Google, ilk olarak 4 Eylül 1998’de kuruldu, 19 Haziran 2004’de de halka arz edildi. Amerika Birleşik Devletleri merkezli olan Google dünya çapında hizmet vermektedir. Kuruluşundan itibaren hızlı bir şekilde büyümesi arama motoru dışında ürünler ve ortaklıklar elde etmesini sağladı. Gmail, Youtube, Google Drive ve Google Chrome Google’a ait olan ürünlerden bazılarıdır. En popüler arama motorlarında biri olan Google’ı veri, bilgi veya herhangi bir çevrimiçi kaynağı aramak için kullanılır.

GOOGLE DORKİNG (GOOGLE HACKİNG) NEDİR?

Savunmasız sitelere girmek veya genel arama sonuçlarında bulunmayan verileri aramak için Google Dorking kullanılır. Google Dorking (Google Hacking) basit aramalarda bulunamayan bilgileri bulmak için gelişmiş arama sorguları kullanmaktır. Google’un tam olarak ne demek istediğimizi anlamak için arama sınırlarını zorlama işlemidir. Google Hacking denmesini sebebi ise hackerların bilgi toplamak için kullanmasıdır. Ancak son zamanlarda reklamlar yüzünden aradığımızı rahat bir şekilde bulmak için Google Dork’u kullanabiliriz. Google arama sonuçlarını görseller, alışveriş, videolar, kitaplar, haritalar, haberler, uçuş aramaları ve finans olarak özelleştirebiliriz. Araçlar yardımı ile aramanın dilini, zamanını veya kelimesi kelimesine aramayı özelleştirebiliriz.

Google Dork’u ilk olarak bir kitabın pdfini bulmak istediğimde keşfettim. filetype:pdf sorgusu ile sadece pdf formatındaki aramaları görebileceğimi öğrendim.

Google Dork bir pasif bilgi toplama tekniği olduğu için yasaldir çünkü sadece halka açık hale getirilmiş şeylere erişiriz. Ancak dikkatli kullanmak gerekiyor, bu bilgileri kullanmaya kalktığımız zaman açık iznimiz olmadığı sürece bu yasadışı bir hal alır.

MANTIKSAL OPERATÖRLER VE SEMBOLLER

VE veya +	Dahillik anlamı katar.
DEĞİL veya -	Hariçlik anlamı katar.
VEYA veya	Veya anlamı katar yani anahtar kelimenin veya diğerinin eşleştiği sonuçları dahil eder.
Tilde (~)	Eşanlamlı veya benzer anlamı kelimeler için kullanılır.
Çift tırnak (“)	Birebir Çift tırnak içerisindeki sonucu dahil etmek için kullanılır.

Dönem (.)	Tek karakterlik joker karakterler eklemek için kullanılır.
yıldız işareti (*)	Tek kelimelik joker karakterleri eklemek için kullanılır.
parantez (())	Sorguları gruplamak için kullanılır.

GELİŞMİŞ ARAMA OPERATÖRLERİ

Başlıca gelişmiş arama operatörleri şunlardır:

info	info sorgusu ile belirtmiş olduğumuz web sitesi hakkında bilgilere erişim sağlayabiliriz.[info:www.medium.com]
link	link sorgusu ile web sayfasına bağlantı veren web sayfalarını görebiliriz.[link:www.linkedin.com]
cache	cache sorgusu ile web sayfasının önbellekteki halini yani en son kullanılan halini gösterecektir.[cache:www.google.com] Ancak sonunda bir kelime eklersek, önbellekteki içeriği o kelime vurgulanmış olarak gösterir.[cache:www.google.com web]
related	Bu sorgu ile belirtilen web sayfasına benzer web sayfalarını görürüz.
site	Aramamızın yanında bu sorguyu kullandığımız zaman sadece belirtmiş olduğumuz web sitesi ile sınırlı aramaları gösterecektir.[efekan acar site:www.linkedin.com]
inurl	Bu sorgu ile URL'sinde belirtmiş olduğum kelimelerden herhangi biri geçen sonuçları görebiliriz.[inurl:efekan acar]
allinurl	Bu sorgu ile URL'sinde belirtmiş olduğum kelimeleri bulunduran sonuçları görebiliriz.
inanchor	Bu sorgu ile belirtilen bağlantı metninin tamamının arama sonuçlarını görebiliriz.[inanchor:"siber güvenlik"]
intitle	Bu sorgu ile arama sonuçlarını başlığında belirtmiş olduğumuz kelime bulunan sitelerle sınırlar.
allintitle	Bu sorgu ile arama sonuçlarını başlığında belirtmiş olduğumuz kelimeler bulunan sitelerle sınırlar.
intext	Bu sorgu ile belirlemiş olduğumuz kelimenin metin içerisinde geçtiği sonuçları gösterir.
allintext	Bu sorgu ile belirlemiş olduğumuz kelimelerin metin içerisinde geçtiği sonuçları gösterir.
filetype/ext	Belirtilen dosya uzantılarını gösterir.

after/before	Bir süre önce veya sonra oluşturulan sayfaları gösterir.
define	Bu sorgu ile belirtmiş olduğumuz hatanın ne olduğu hakkında sonuçları görebiliriz.[define:”sql syntax error”

Google search results for "hayvan çiftliği filetype:pdf". The search results show a list of PDF files, including "Hayvan Çiftliği - Origo" by George Orwell. The right sidebar provides a detailed overview of the book "Hayvan Çiftliği" (Animal Farm) by George Orwell, including its publication date (1945), author (George Orwell), and a brief description of the plot.

Burada hayvan çiftliği aramamın yanına dosya uzantısını pdf olarak belirtmek için filetype sorgusunu kullandım. Bu sayede sadece pdf olan sonuçları listelemiş oldum.

Google search results for "site:linkedin.com intitle:developer". The search results show a list of job listings for developers on LinkedIn. The right sidebar provides a detailed overview of the search results, including the number of results (5,210,000) and a list of job titles such as "Türkiye konumunda 2.000 Developer iş ilanları (247 yeni)".

Bu şekilde iki sorguyu birlikte de kullanabiliriz.www.linkedin.com sitesinde developer geçen web sayfalarını listelemesini istedim.

GOOGLE GELİŞMİŞ ARAMA

Google'un https://www.google.com/advanced_search sitesinden ayarlamış olduğumuz özelleştirmeler ile gelişmiş aramalar yapabiliriz.

Google



Gelişmiş Arama

Şu sayfaları bul...

Şu kelimelerin tümünü içeren:

siber

Aynı şü kelimeyi veya kelimeleri içeren:

güvenlik

Şu kelimelerden herhangi birini içeren:

frat

Şu kelimelerden hiçbirini içermeyen:

eğitim

Şu sayıdan:

bu sayıya kadar:

Bu işlemi arama kutusunda yapmak için:

Önemli kelimeleri yazın: boz renkli tarla faresi

Kelimelerin tamamını tınak içine alın: "boz tarla faresi"

İstediğiniz tüm kelimelerin arasına OR yazın: sınıyatur OR standart

İstemediğiniz kelimelerin hemen önüne bir eksi işareti koyun: -kemingen, -"Jack Russell"

Sayılar arasına iki tane nokta koyun, sonuna da bir ölçü birimi ekleyin: 10..35 kg, \$100..\$500, 2010..2011

Sonuçları daha da filtrelemek istiyorsanız...

Dil:

herhangi bir dil

Seçtiğiniz dildeki sayfaları bulun.

Bölge:

Türkiye

Belirli bir bölgede yayınlanan sayfaları bulun.

Son güncelleme tarihi:

herhangi bir zaman

Belirlediğiniz süre içinde güncellenmiş sayfaları bulun.

Site veya alan adı:

.com

Aramayı bir site içinde yapın (wikipedia.org gibi) ya da sonuçları .edu, .org veya .gov gibi bir alan adıyla sınırlandırın.

Terimlerin görüldüğü yer:

sayfanın herhangi bir yerinde

Terimleri tüm sayfada, sayfa başlığında veya web adresinde ya da aradığınız sayfaya verilen bağlantılarda arayın.

Güvenli Arama:

Uygunsuz sonuçları göster

Müşahadenizi güvenli filtre uygulanıp uygulanmayacağını Güvenli Arama seçeneği belirler.

Dosya türü:

Adobe Acrobat PDF (.pdf)

İstediğiniz türdeki sayfaları bulun.

Kullanım hakları:

lisansla filtrelenmemiş

Kullanmanıza izin verilen sayfaları bulun.

Gelişmiş Arama

Yaptığımız aramaya göre "siber", "güvenlik" ve "frat" kelimeleri geçen; "eğitim" kelimesi geçmeyen ; herhangibir dildeki, Türkiye bölgesindeki, her hangi bir zamandaki, ".com" alan adına sahip, terimlerin sayfanın herhangi bir yerinde olduğu uygunsuz sonuçları da gösteren, ".pdf " dosya türüne sahip olan, lisansla filtrelenmemiş aramaları bize gösterecek.



siber fırat "güvenlik" -eğitim site:.com filetype:pdf



Tümü

Görseller

Haberler

Alışveriş

Haritalar

Daha fazla

Araçlar

Herhangi bir dil

Herhangi bir zaman

Tüm sonuçlar

Temizle

Reklam · <https://www.turkcell.com.tr/>

Siber Tehditlere Karşı Savunma - Siber Güvenlik Danışmanlığı

Stratejilerinizi Oluşturmak ve Yönetmek İçin **Siber Güvenlik** Çözümlerimizle Tanışın. **Siber Güvenlik** Tecrübemizi **Güvenlik** Operasyon Merkezi İle Müşterilerimize Aktarıyoruz.

Dijitalleşen Sektörler

Maliyetlerinizi Düşürecek, Gelirlerinizi Arttıracak Çözümler

Dijital İş Servisleri

İşinizi Uzaktan Yönetmeniz için Çözümlerimiz ile Yanınızdayız

Turkcell İş Ortaklığı

Kurumsal Müşterilere Uçtan Uca Teknoloji Çözümleri Sunuyoruz


Turkcell İşte İletişim

Turkcell Kalitesinde Uygun Tarifeler ve Kampanyalar

Bu sayede rahatlıkla Google dork oluşturabiliriz.

GOOGLE HACKING DATABASE

Google hacking Database’de bir çok hassas ve önemli bilgilere erişim sağlayan arama sorguları yer almaktadır. Hackerlar veya siber güvenlik uzmanları buralara önemli gördüğü sorguları yüklemektedir. <https://www.exploit-db.com/google-hacking-database> adresinden ulaşabilirsiniz.



EXPLOIT
DATABASE

Google Hacking Veritabanı

Göstermek120

Hızlı arama

filtrelerHepsini sıfırla

Ekleme Tarihi	İP	Kategori	Yazar
2022-01-12	site:vps-*vps.ovh.net	Web Sunucusu Algılama	zincir butiği
2022-01-12	inurl:adminpanel sitesi:gov.*	ayaklıklar	Asheet Turkey
2021-11-19	site:gov.*intitle:"index of"*.csv	Sulu Bilgi İçeren Dosyalar	Midhun Mohanan
2021-11-19	Google'dan wordpress'e geçiş	Sulu Bilgi İçeren Dosyalar	Aitor Herrero
2021-11-19	Fwd: intitle:"/" dizini intext:"resource/"	Sulu Bilgi İçeren Dosyalar	Mugdha Bansode
2021-11-19	site:papaly.com + anahtar kelime	Sulu Bilgi İçeren Dosyalar	Gabriel Tarsia
2021-11-19	Fwd: intitle:"tavsiye - yeni nesil"	Sulu Bilgi İçeren Dosyalar	Mugdha Bansode
2021-11-18	site:pastebin.com başlık:"cpanel"	Sulu Bilgi İçeren Dosyalar	İşhani Dhar
2021-11-18	inurl:/wp-content/uploads/inurl:"robots.txt" "İzin verme:" filetype:txt	Sulu Bilgi İçeren Dosyalar	ritwick baba
2021-11-18	inurl:admin dosya türü:xls	Sulu Bilgi İçeren Dosyalar	ritwick baba
2021-11-18	intitle: settings.py dizini	Sulu Bilgi İçeren Dosyalar	Amit Adhikari
2021-11-18	inurl:admin dosya türü:xlsx site:gov.*	Sulu Bilgi İçeren Dosyalar	Krishna Agarwal
2021-11-18	db_password dosya türü:env	Sulu Bilgi İçeren Dosyalar	Thiru kumaran
2021-11-18	inurl:/intranet/login.php	Giriş Portalları İçeren Sayfalar	Diego Bardalez Plaza
2021-11-18	inurl:"*admin oturum aç" inurl:.php .asp	Giriş Portalları İçeren Sayfalar	Krishna Agarwal
2021-11-18	site:postman.com + anahtar kelime	Sulu Bilgi İçeren Dosyalar	Gabriel Tarsia

KATANA DORK SCANNER

Katana Dork Scanner Google Dorking'i otomatikleştiren basit bir python aracıdır. Google, Scada, Tor ve Proxy modları mevcuttur. Basit ve yararlı bir araçtır.

KURULUM

Aracımızı kurmadan önce python3 ve toru yüklüyoruz. Sonra githubdan gerekli kodları indiriyoruz.
git clone <https://github.com/adnane-X-tebbaa/Katana.git>

```
root@kali:~/Desktop/Google Dork# git clone https://github.com/adnane-X-tebbaa/Katana.git
Cloning into 'Katana'...
remote: Enumerating objects: 579, done.
remote: Counting objects: 100% (63/63), done.
remote: Compressing objects: 100% (57/57), done.
remote: Total 579 (delta 35), reused 11 (delta 5), pack-reused 516
Receiving objects: 100% (579/579), 2.53 MiB | 814.00 KiB/s, done.
Resolving deltas: 100% (289/289), done.
```

Daha sonra yüklenen "cd" komutu ile yüklenen Katana klasörünün içine giriyoruz ve "ls" komutu ile içeriğini listeliyoruz ihtiyacımız olan dosyalar indiğine göre gerekli olan diğer indirmeleri de yapıyoruz.

python3 -m pip install -r requirements.txt

