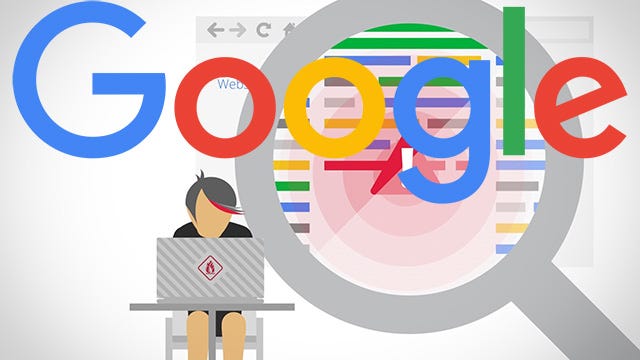
**GOOGLE NEDİR?**

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 yasaldır 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 anlamlı 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**

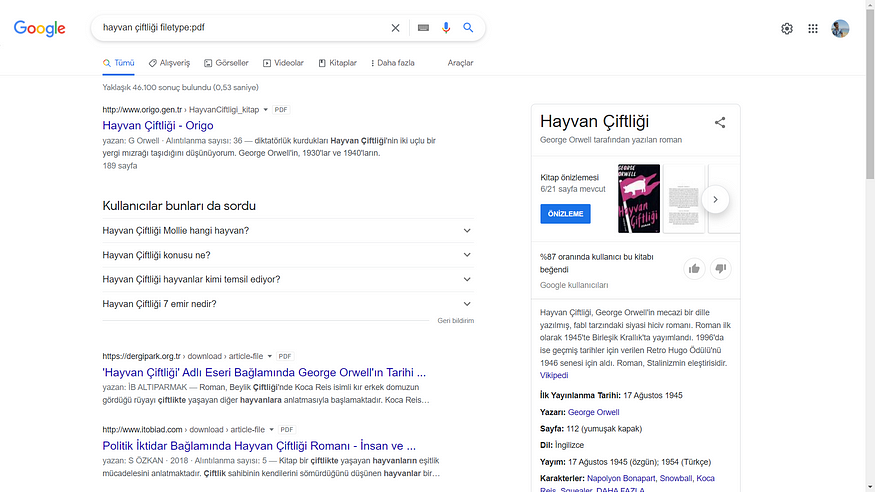
Belirtilen dosya uzantılarını gösterir.

**after/before**

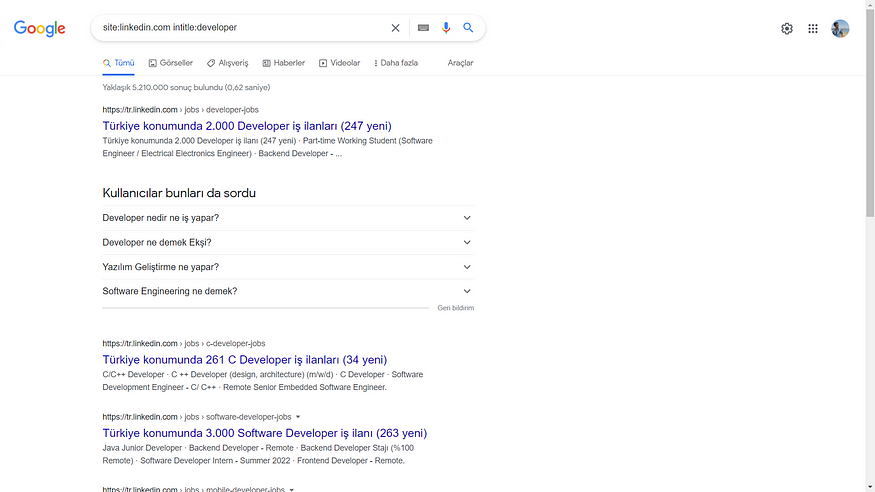
Bir süre önce veya sonra oluşturulan sayfaları gösterir.

**define**

Bu sorgu ile belirtmiş olduğumuz hatanın ne olduğu hakkında sonuçları görebiliriz.[define:“sql syntax error”



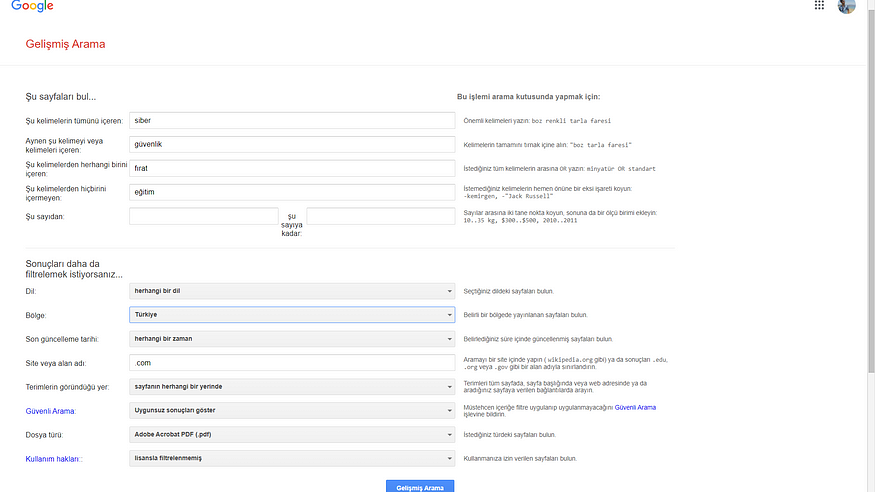
Burada hayvan çiftliği aramamın yanına dosya uzantısını pdf olarak belirtmek için filetype sorgusunu kullandım. Bu sayede sadece pdf olan sonuçları listelemiş oldum.



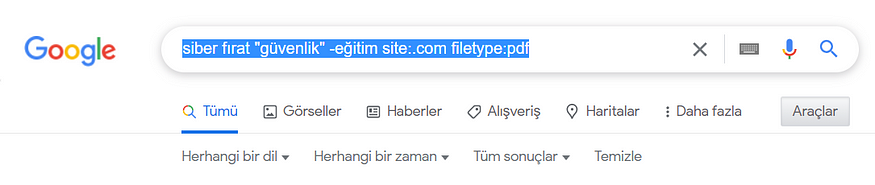
Bu şekilde iki sorguyu birlikte de kullanabiliriz.[www.linkedin.com](http://www.linkedin.com/) sitesinde developer geçen web sayfalarını listelemesini istedim.

**GOOGLE GELİŞMİŞ ARAMA**

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



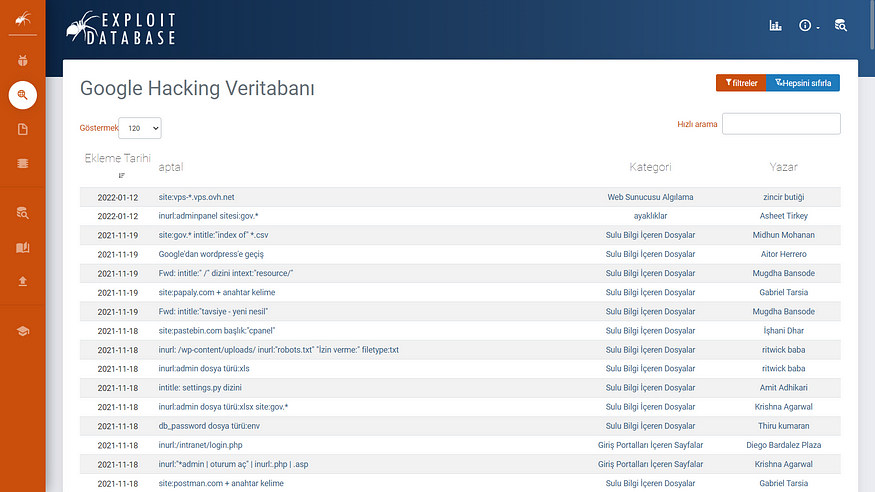
Yaptığımız aramaya göre “siber”, “güvenlik” ve “fırat” kelimeleri geçen; “eğitim” kelimesi geçmeyen ; herhangi bir dildeki, Türkiye bölgesindeki, her hangi bir zamandaki, “.com” alan adına sahip, terimlerin sayfanın herhangi bir yerinde olduğu uygunsuz sonuçları da gösteren, “.pdf “ dosya türüne sahip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



Bu sayede rahatlıkla Google dork oluşturabiliriz.

**GOOGLE HACKİNG 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.



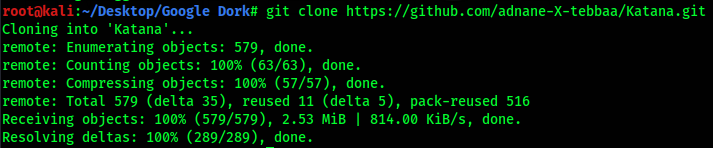
**KATANA DORK SCANNER**

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

**KURULUM**

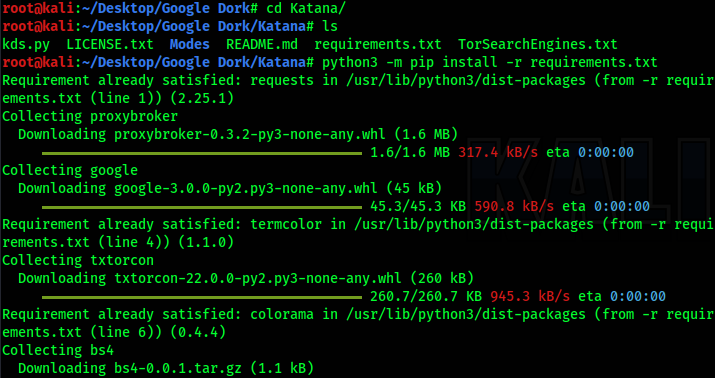
Aracımızı kurmadan önce python3 ve toru yüklüyoruz. Sonra githubdan gerekli kodları indiriyoruz.

***git clone https://github.com/adnane-X-tebbaa/Katana.git***



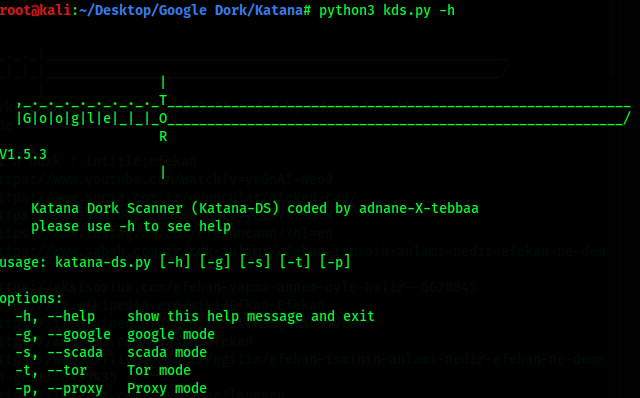
Daha sonra yüklenen “cd” komutu ile yüklenen Katana klasörünün içine giriyoruz ve “ls” komutu ile içeriğini listeliyoruz ihtiyacımız olan dosyalar indiğine göre gerekli olan diğer indirmeleri de yapıyoruz.

***python3 -m pip install -r requirements.txt***



Bir hata almadan bu indirmeleri de yaptığımıza göre aracımızın nasıl çalıştığını görmek için çalıştırıyoruz.

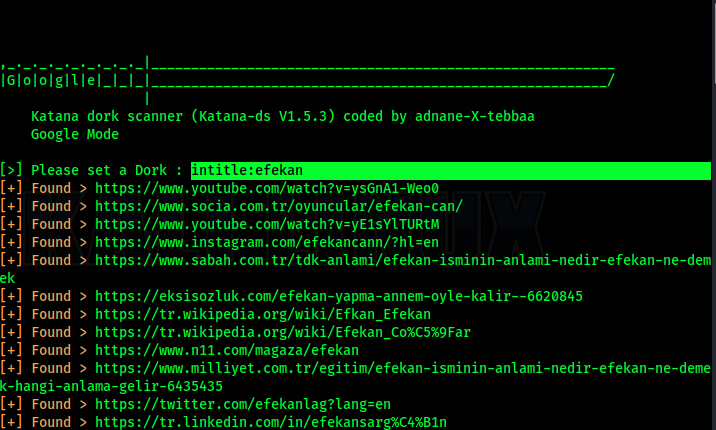
***python3 kds.py –h***



**KULLANIM**

Gördüğümüz gibi –h, -g, -s, -t ve –p parametrelerini kullanabiliriz. Ben –g parametresini yani Google modunu kullanacağım. Gerekli kodu yazdıktan sonra benden dork yazmamı istiyor. Yazdıktan sonra arama sonuçlarını linkler halinde görmemizi sağlıyor.

***python3 kds.py –g***



Googlehack, Goolink Scanner, Site Digger Tool gibi araçlar da Katana Dork Scanner gibi Google Dorking’i özelleştiren araçlardan başlıcalarıdır.

**KAYNAKLAR**

<https://www.hackthebox.com/blog/What-Is-Google-Dorking>

<https://www.acunetix.com/websitesecurity/google-hacking/>

<https://www.google.com.tr/intl/tr/help/operators.html#:~:text=Bu%20operat%C3%B6rler%20aras%C4%B1nda%20OR%20(veya,ise%20Geli%C5%9Fmi%C5%9F%20Arama%20sayfas%C4%B1ndan%20eri%C5%9Filebilir>.

<https://www.berkeunal.com.tr/katana-dork-scanner-kurulumu-ve-kullanimi/>