



BiltekCyber



# Google Dorking 101





# İçindekiler :::::

1-Google Dorks Nedir ?	3
2-Google Dorking Amacı	4
3-Google Hacking Senaryosu	5
4-Google Dorking Komutları	7
5-Advanced Google Dorking	15
6-Advanced Google Dorking Komutları	16
7-Exploit Database	26
8-Google Dorking'i Önleme	27
9-Robot.txt Nedir?	28
10-Google Dorking'i Önlemek için robots.txt Yapılandırmalarını Kullanma	29
11-Kaynakça	32



# Google Dorks Nedir?

Günümüzde çoğu kişinin arama motoru olarak kullandığı Google, internet üzerindeki bilgilerin her geçen gün artmasından dolayı yaptığımız aramalarla ilgili veya ilgisiz bir çok sonuç vermektedir.

Diğer bir adı Google hacking olan Google dorking yaptığımız bu aramalara belli komutlar üzerinden filtreleme yaparak bizim daha tutarlı sonuçlar elde etmemizi sağlar.



Google  
Dorks



# Google Dorking'in Amacı

Google dorking kişi veya kurum hakkında detaylı bilgi toplama konusunda bize yardımcı olması hackerlar için büyük bir avantaj sağlamaktadır. Bilgi elde etmek için harcanan zamanı azaltması ve başarı ihtimalini artırması araştırmanızda büyük fayda sağlayacaktır.







# Google Hacking Senaryosu

Örneğin ortalama (phishing) yapmak istiyorsunuz ve bir kurbanın dikkatini çekmek için mail kullanacaksınız. Kuruma ait "abc123@kurumdomaini.com" Google sorgusu ile filtreme yaparak aratacak olursak kurban hakkında daha fazla bilgi edinebiliriz.

Başka bir örnek olarak root parola kısmı boş bırakılmış phpmyadmin sayfalarını bulmak için bir kaç kelime komut yazmanız yetecektir.





BiltekCyber

# KOMUTLAR 101

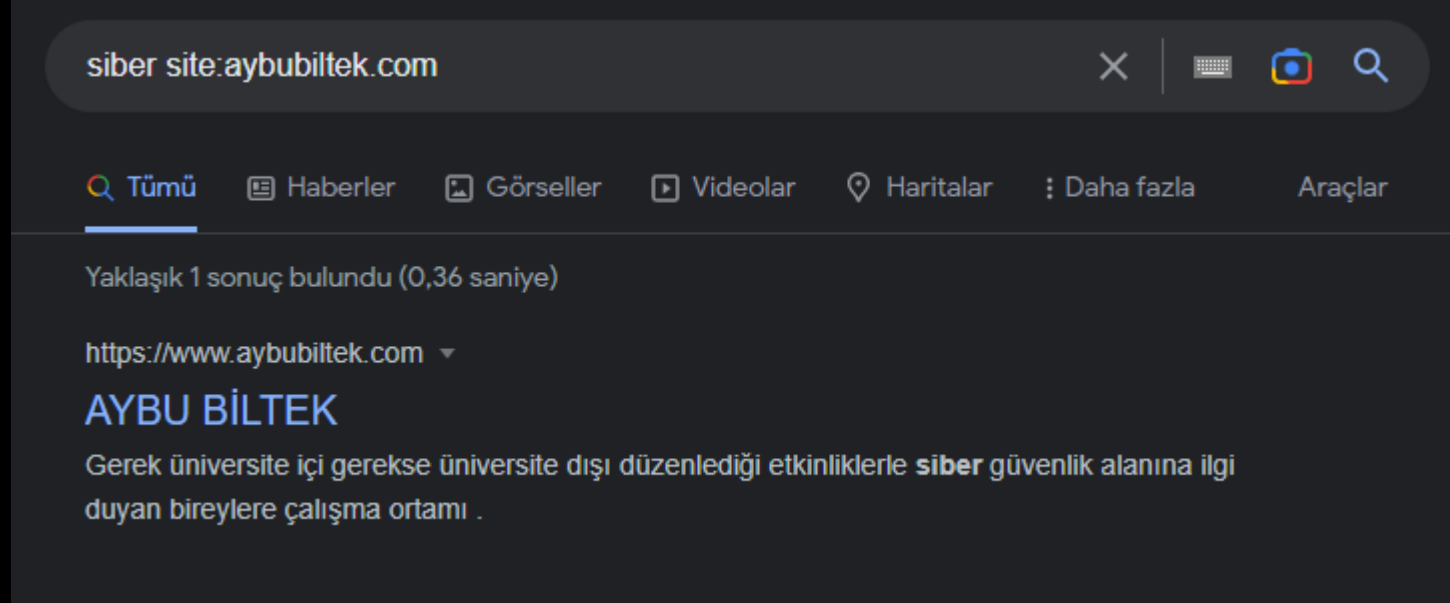




# Google Dorking Komutları Nelerdir?

## site

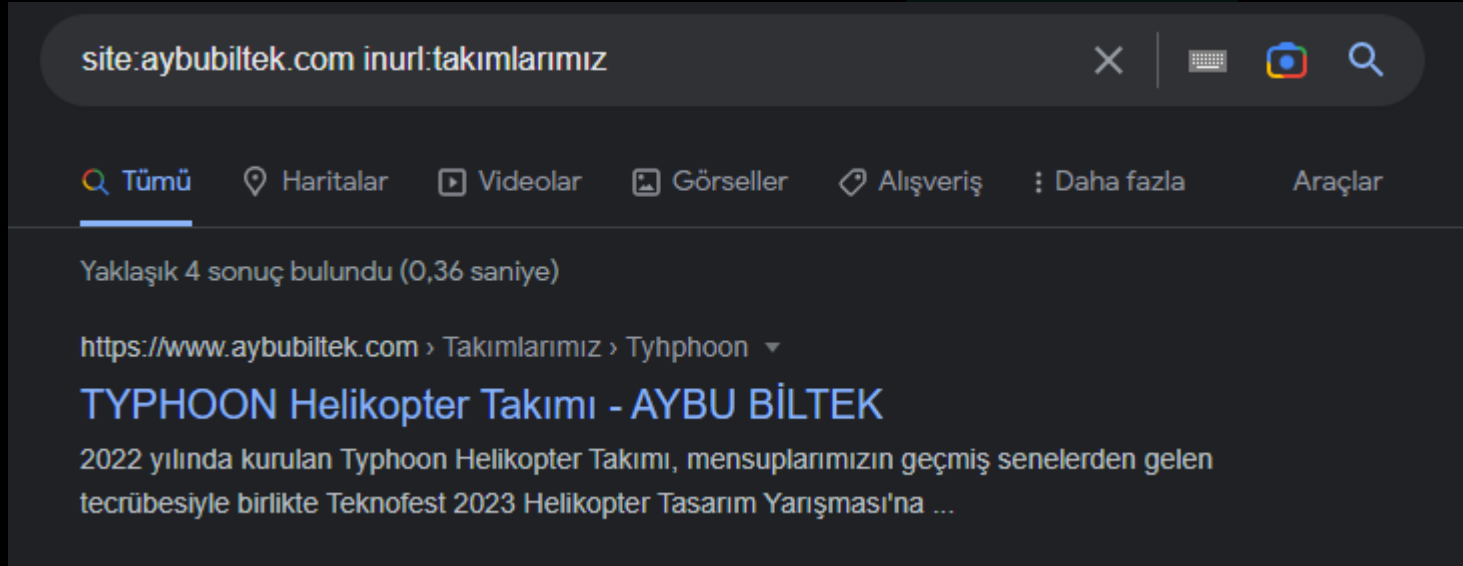
**Siber** ile ilgili bir içerik arıyoruz ama bu içeriğin **aybubiltek.com** sitesinde olmasını istiyoruz. Bunu arama motoruna "siber site:aybubiltek" ifadesiyle belirtebiliyoruz.





## inurl

inurl dorku ise, verdiğimiz parametreyi **url adresi** içerisinde arar. site:aybubiltek.com inurl:takımlarımız url adresinde “takımlarımız” ifadesi olan internet sitelerini listeler.



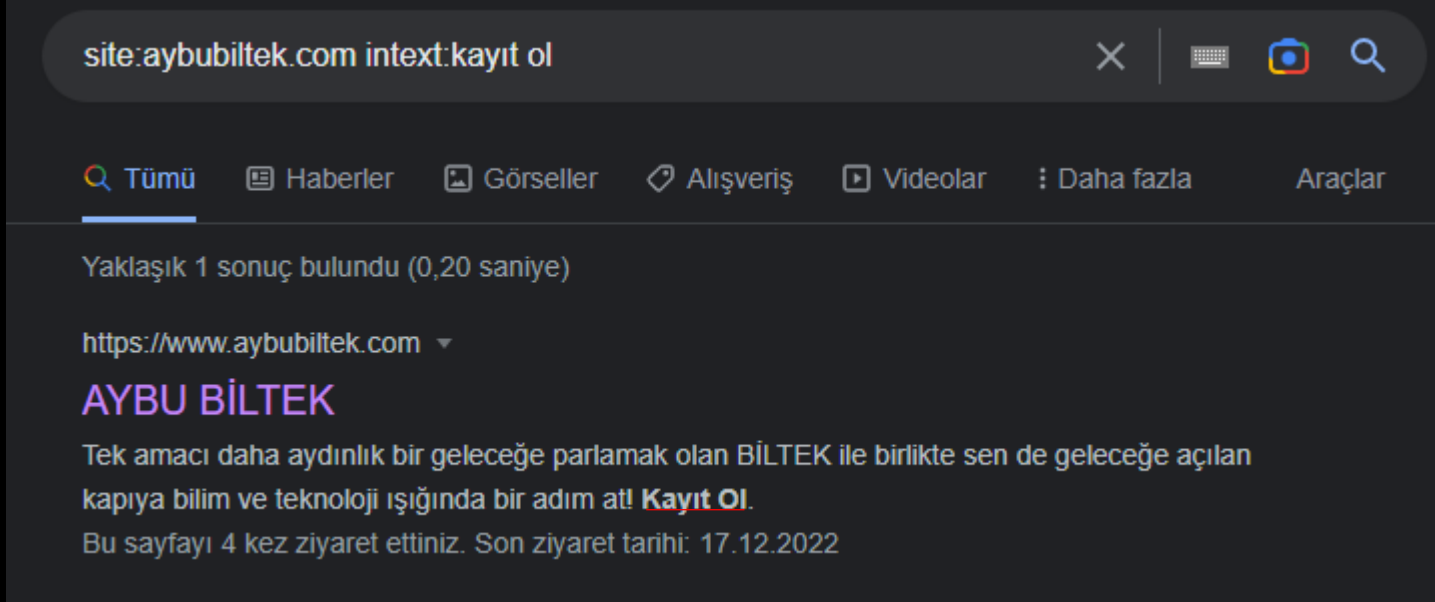




BiltekCyber

## intext

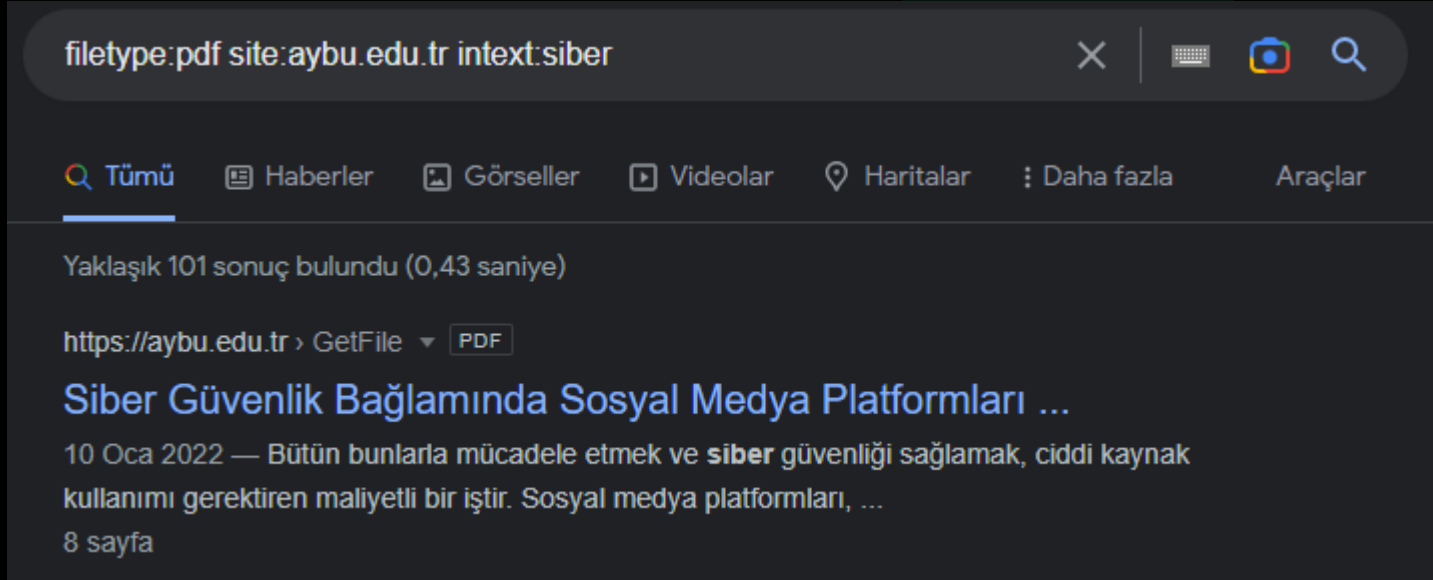
Intext dorku verdiğimiz parametreyi **sayfa içeriği** içerisinde arar.





## filetype

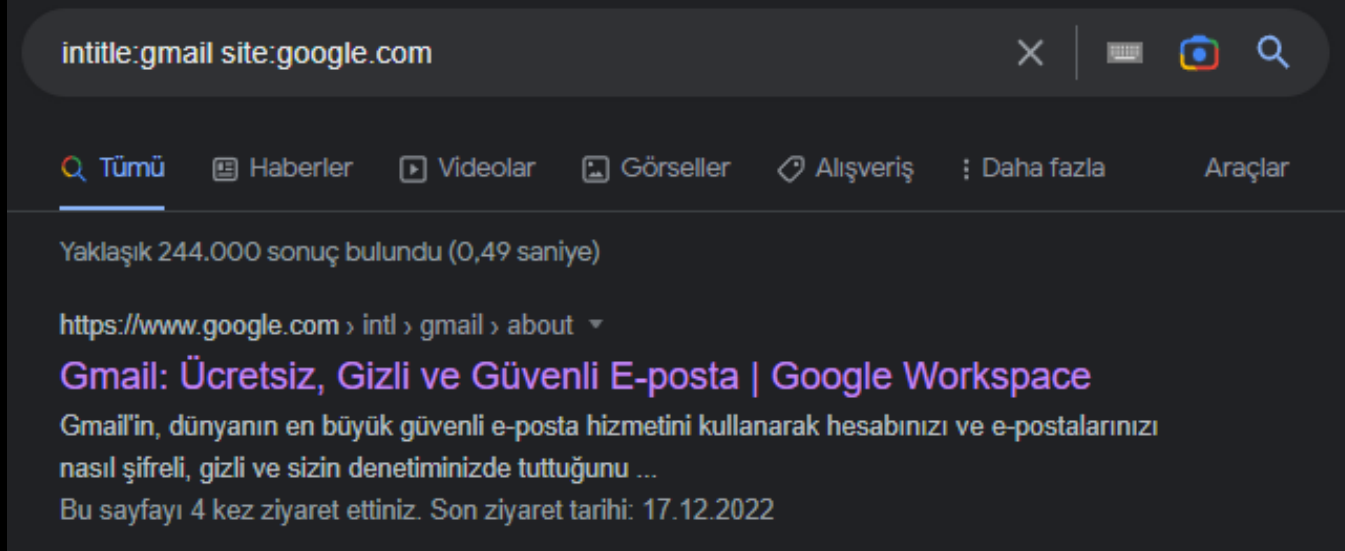
filetype dorku ile arama yaparak istediğiniz türde dökümana( (doc, docx, pdf, psd...) ulaşabilirsiniz.Bu örnekte içerisinde **siber** kelimesi bulunan **pdf dökümanlarını** listeledik.





## intitle

intitle dorku, sayfanın başlığında arama yapmamıza yarıyor.  
intitle:"text" -> text bölümüne istediğiniz metni yazabilirsiniz.





BiltekCyber

## cache

Bu dork sayesinde aranan sitenin önbelleğe alınmış sürümü karşımıza gelecektir.






# book

Bu dork aradığımız sayfalara benzer sayfaları karşımıza getirir.

[Tümü](#) [Görseller](#) [Alışveriş](#) [Haberler](#) [Videolar](#) [Daha fazla](#) [Araçlar](#)

Yaklaşık 448.000 sonuç bulundu (0,61 saniye)



## Da Vinci Şifresi

Dan Brown tarafından yazılan roman

[Genel Bakış](#) [Yorumlar](#) [Karakterler](#) [Kitap alın](#) [Yazarın Diğer Kitapları](#)

<https://www.dr.com.tr> > ... > Edebiyat > Roman > Macera

### Da Vinci Şifresi (Dan Brown) - Fiyat & Satın Al - D&R

Langdon ve yetenekli Fransız kriptoloji uzmanı Sophie Neveu, cesedin etrafındaki izleri takip ederek bu garip esrar perdesini araladıkça, ipuçlarının onları Da ...

★★★★★ Kullanıcı oyu: 4,5 · 91 inceleme · ₺84,50 · Stokta var

<https://www.kitapyurdu.com> > kitap > da-vinci-sifresi

### Da Vinci Şifresi (Dan Brown) Fiyatı, Yorumları, Satın Al

Da Vinci Şifresi düşündürücü olduğu kadar aynı zamanda büyüleyici. Tarih meraklıları, komplo çılgınları, bulmaca meraklıları ve gerilim öyküsü severlerin ...

★★★★★ Kullanıcı oyu: 5 · 1.477 inceleme · ₺84,50 · Stokta Yok

#### Hakkında

%91 oranında kullanıcı bu kitabı beğendi

Google kullanıcıları

Da Vinci Şifresi ya da özgün adıyla The Da Vinci Code, Dan Brown'un kaleme aldığı bir romandır.

[Vikipedi](#)

**İlk Yayınlanma Tarihi:** 18 Mart 2003

**Yazar:** Dan Brown

**Karakterler:** Robert Langdon, Silas, Sir Leigh





### İki nokta(..)

Bu operatör kendisinden önceki ve sonraki değerlerin aralığında olan sonuçları listeler. Örneğin, fiyatı 5000TL ile 10000TL arasındaki bilgisayarları aramak için “**bilgisayar 5000TL..10000TL**” şeklinde yazmamız yeterli olacaktır.

### Artı(+)

Girdiğimiz kelime gruplarının arasında kullanılır ve kelimeleri birleştirmeyi sağlar. Birden fazla belirli anahtarın bulunduğu sayfaları filtreleyerek

### Eksi(-)

Bu operatör ise öncesine yerleştirdiğimiz kelimeyi arama filtremizin dışına çıkararak o kelimeyi içermeyen siteleri bize sunar. Örneğin network konusu dışındaki siber güvenlik bilgisi aratmak istiyorsak “siber güvenlik –network” yazmamız yeterli olacaktır.

### Yıldız(\*)

Sözcük öbeğinin arasında o öbeği mantıklı bir şekilde tamamlayan kelime gruplarını yerine yerleştirerek aratan komuttur. Örneğin “how to \* a game” şeklinde kullanacak olursak “how to...” develop/download/play, etc.. “a game” şeklindeki arama sonuçlarını gösterecektir.



# Advanced Google Dorking

Buraya kadar olan bölümde genel anlamda Google dorklarından bahsettik. Bu kullanımları genellikle siber güvenlik uzmanları, akademisyenler, araştırmacılar kullanmaktadır. Fakat sizde aramalarınızı daha rahat yapabilmek için bu dorkları kullanabilirsiniz. Şimdi “Hacking” konusu ile ilgili dorklara göz atalım. Burada dorklar sayesinde açıkları bulunan siteler bulunabilmektedir.





# Advanced Google Dorking Komutları

## WordPress Config

index of" "wp-config.php.bak " dorku ile **wordpress config** dosyasının içeriğine ulaşabilirsiniz. **WordPress** sitenize ait bazı önemli verileri içerisinde barındıran bir dosyadır. Bu dosya içerisinde **veritabanınıza ait, veritabanı adı, veritabanı kullanıcı adı, veri tabanı şifresi ve veritabanınıza ait sunucu bilgisi** barındırılmaktadır.





# WordPress Config

index of "wp-config.php.bak"

×

🖨

🗣

🔍

🔍 Tümü

📺 Videolar

🖼 Görseller

📰 Haberler

🛒 Alışveriş

⋮ Daha fazla

Araçlar

Yaklaşık 14.100.000 sonuç bulundu (0,78 saniye)

Index of /b2b-store

Name	Last modified	Size
Parent Directory		-
info.php	2018-11-02 17:03	19
wp-config.php.bak	2018-11-02 17:03	3.1K
wp-config.php.old.bak	2018-11-02 17:03	3.0K

2 satır daha

<https://greenlighting.co.uk> > ...

Index of /b2b-store - Green Lighting

?

Öne çıkan snippet'ler hakkında • 

🗨

Geri bildirim





## Log Dosyaları

Websiteler içerisinde hassas bilgilerin çoğu log(günlük) dosyalarında depolanır. Hata erişim ve diğer uygulama günlükleri genellikle web sitelerinin genel HTTP alanında bulunur. Bu zafiyet hackerların sizin kullandığınız PHP versiyonunuzu öğrenmesine, büyük önem arz eden CMS(Content management system) veya yapı sistem yollarını bulmasını sağlar. Bu tür saldırılar, eğer önceden önlem alınmazsa, site sahibinin mevcut veritabanı adını, kullanıcı girişlerini, şifrelerini ve e-posta değerlerini ele geçirilmesine olanak sağlar.



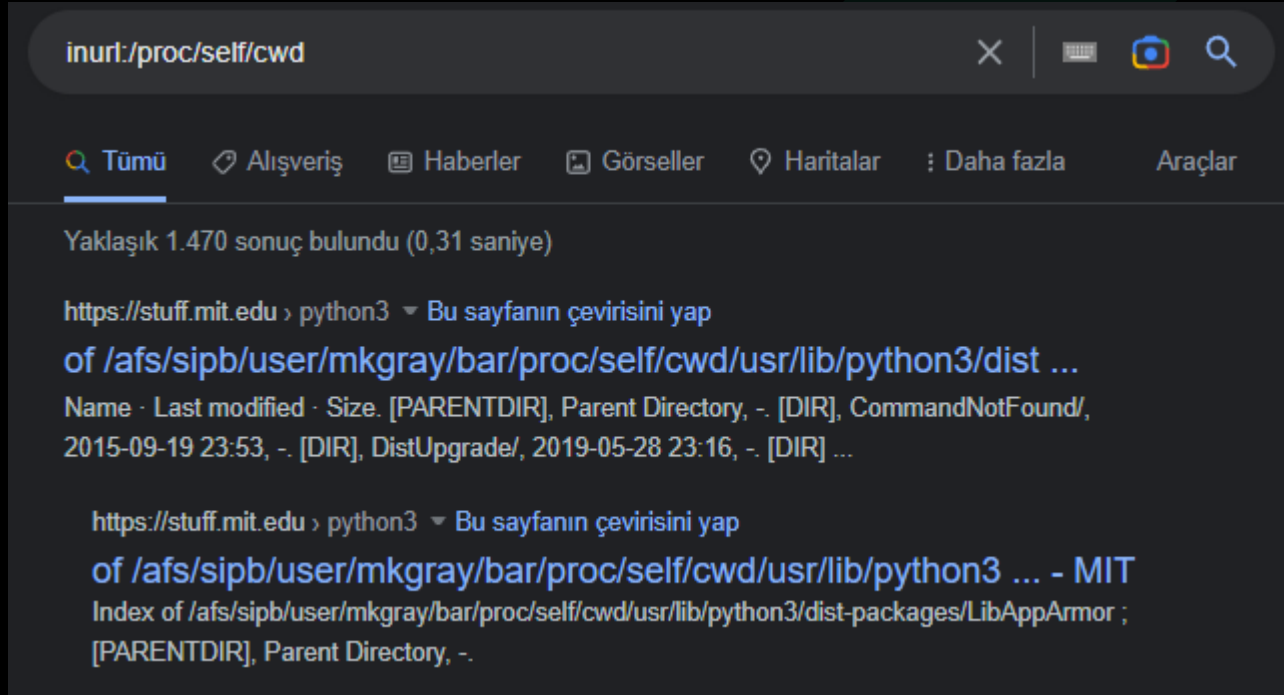




## Güvenlik Açığı Bulunan Web Sunucuları

"/proc/self/cwd/" komutunu url içerisinde aratarak güvenlik zafiyeti bulunan veya hacklenmiş web sunucularını görmenizi sağlar.

Aşağıdaki ekran görüntüsünde görebileceğiniz gibi, savunmasız sunucu sonuçları dizinleriyle birlikte gözükecektir.





## FTP Sunucuları Bulma

Google yalnızca HTTP tabanlı sunucuları değil, açık FTP sunucularını da dizine ekler. “intitle:"index of" inurl:ftp” komutunu kullanarak bu tür sunucuları aratabilirsiniz.

intitle:"index of" inurl:ftp

Tümü Görseller Haberler Videolar Alışveriş Daha fazla Araçlar

Yaklaşık 535.000 sonuç bulundu (0,34 saniye)

<https://surfer.nmr.mgh.harvard.edu> > ... Bu sayfanın çevirisini yap

**Index of /ftp**

Name	Last modified	Size
Parent Directory		-
ID-pubftp	2022-12-10 01:08	0
articles/	2021-10-15 11:13	-

Diğer 7 satırı daha göster

<https://mirbase.org> > ftp Bu sayfanın çevirisini yap

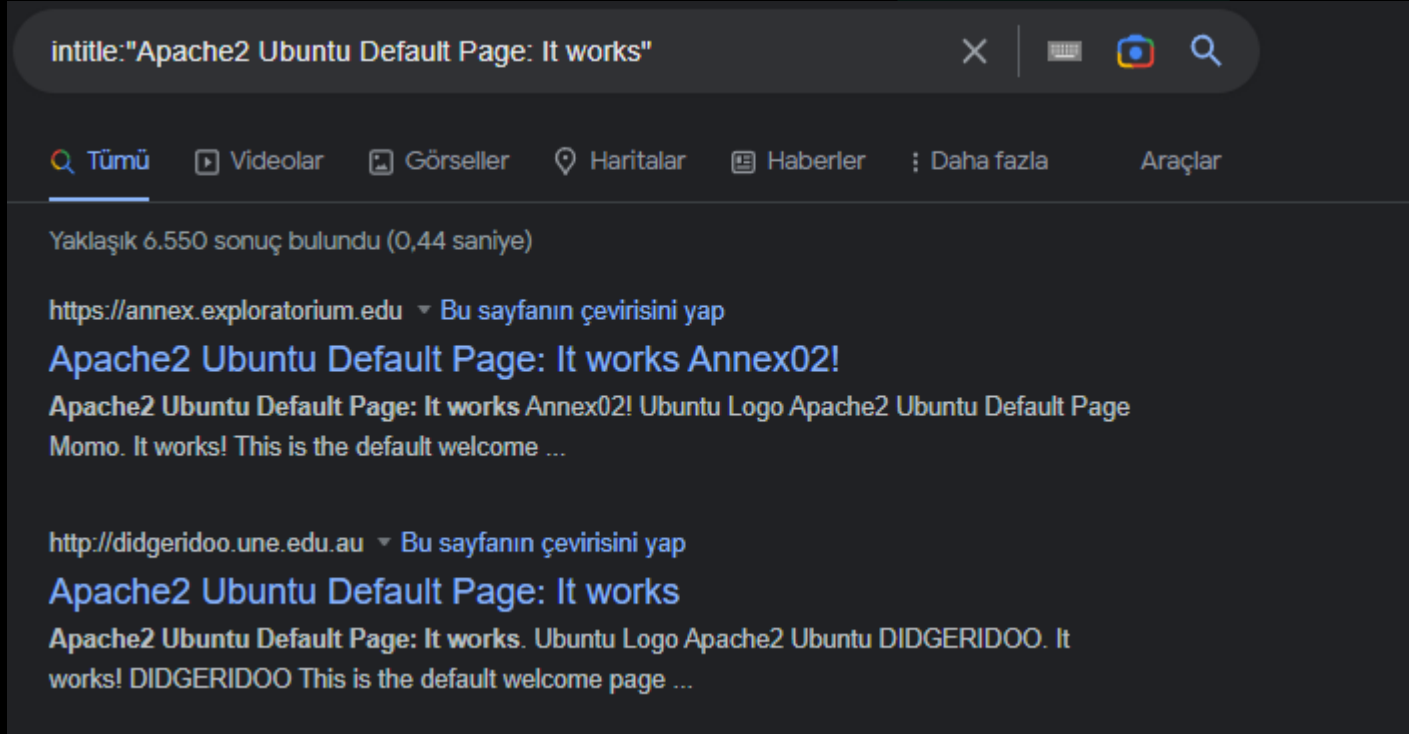
**Index of /ftp - miRBase**

Index of /ftp. Index of /ftp. [ICO], Name · Last modified · Size · Description ...



# Apache2

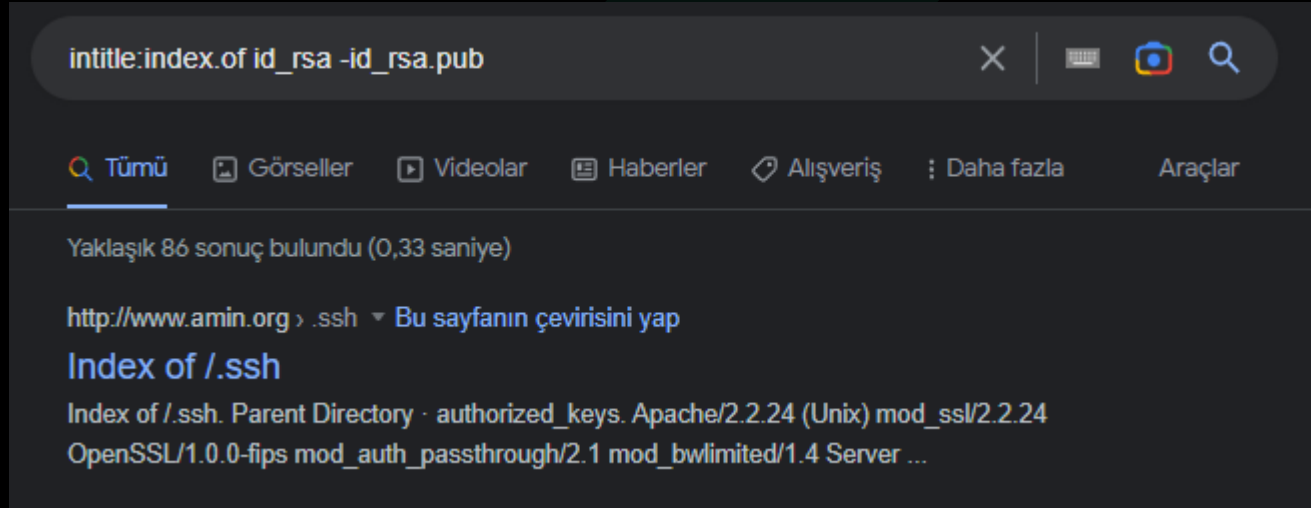
Apache2 güvenlik açığı bulunan web sunucularının alt başlığı olarak da düşünülebilir. Bu Apache sunucuları yanlış yapılandırılmış/unutulmuş olabilir veya kurulumun bir aşamasında olabilir, bu da onları botnet'ler için harika hedefler haline getirir.





## SSH Özel Anahtarları

SSH özel anahtarları SSH protokolü tarafından şifrelenen bilgileri deşifre etmek için kullanılır. Genel bir güvenlik kuralı olarak, bu anahtarlar SSH sunucularına uzaktan erişim sağlayan sistemlerde saklanmalı ve başkalarıyla paylaşılmamalıdır.”intitle:index.of id\_rsa - id\_rsa.pub” komutu ile SSH özel anahtarlarına erişim sağlayabilirsiniz. PUTTY SSH istemcili bir Windows işletim sistemi kullanıyorsanız, bu program her zaman SSH bağlantılarınızın kullanıcı adlarını günlüğe kaydeder. Bu istemciyi kullanan kişilerin kayıtlarına”filetype:log username putty” komutu ile ulaşabilirsiniz.





## Canlı Kamera Yayınları

Google hacking tekniklerinden biri de IP tarafından kısıtlanmamış canlı kamera yayını web sitelerine erişebilirsiniz.

*inurl:top.htm inurl:currenttime*

Komutu ile çeşitli IP tabanlı kameralara ulaşmanızı,

*intitle:"webcamXP 5«*

Komutu WebcamXP tabanlı iletimleri bulmanızı,

*inurl:"lvappl.htm«*

Genel canlı kamera yayınlarını izlemenizi sağlar

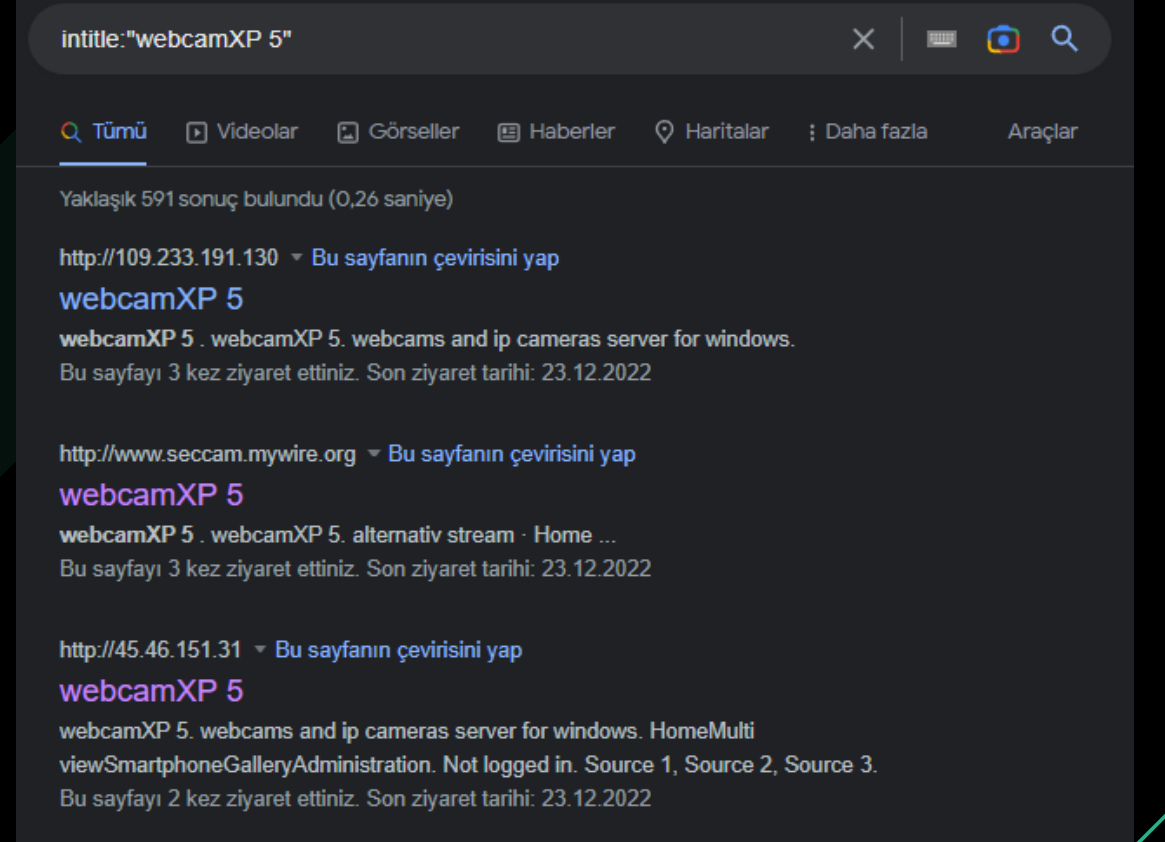
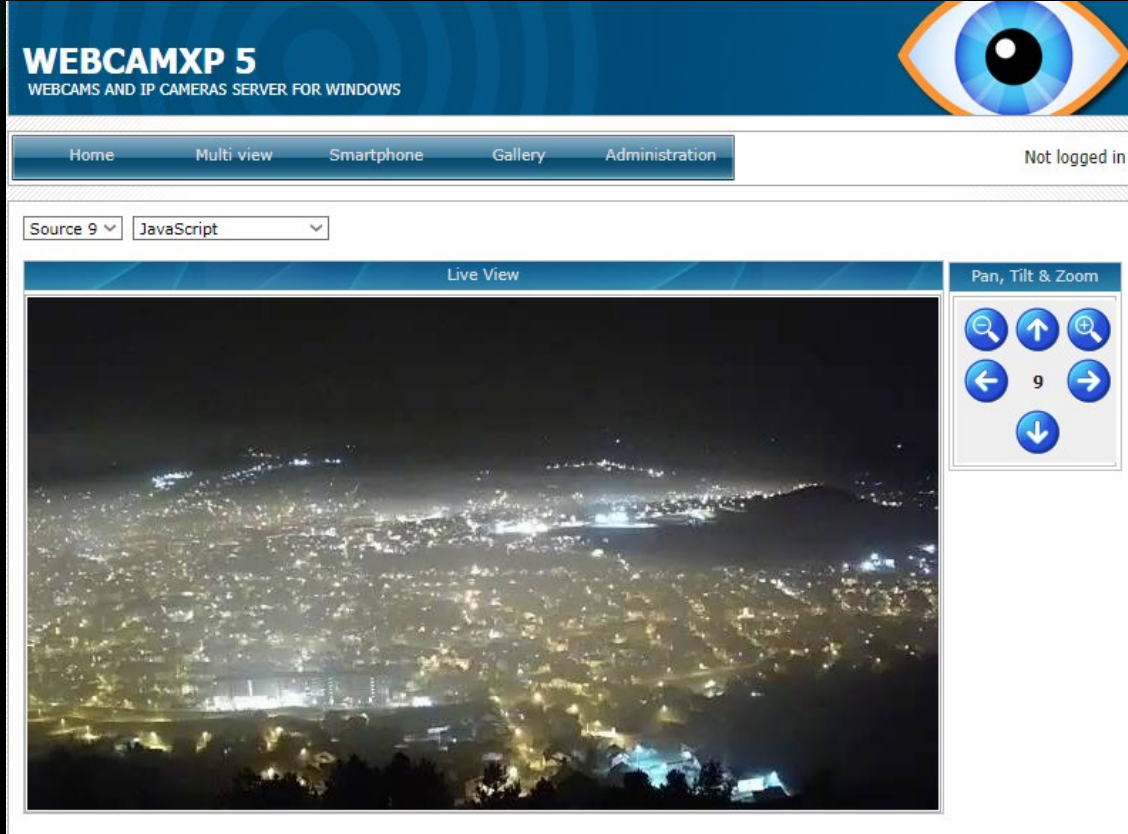






BiltekCyber

# Canlı Kamera Yayınları





## .env dosyaları

.env dosyaları, popüler web geliştirme sistemleri tarafından yerel ve çevrimiçi geliştirme ortamları için genel değişkenleri ve yapılandırmaları bildirmek için kullanılan dosyalardır. Bu tür dosyalara herkesin erişim sağlaması büyük bir zafiyet göstergesidir.

## E-mail listeleri

Google Dorking ile e-mail listelerini kolaylıkla bulabilirsiniz.”filetype:xls inurl:"email.xls” ” komutu ile excel dosyası içinde bulunan e-mail bilgilerini bulabilirsiniz.





Daha fazla Google Dorks komutu öğrenmek için  
“<https://www.exploit-db.com/google-hacking-database>”  
sitesinden yararlanabilirsiniz.

**EXPLOIT DATABASE**

Google Hacking Database

Filters Reset All

Quick Search

Date Added	Dork	Category	Author
2022-09-19	intext:"index of" ".sql"	Files Containing Juicy Info	Gopalsamy Rajendran
2022-09-19	intitle:"index of" inurl:superadmin	Files Containing Juicy Info	Mahedi Hassan
2022-09-19	intitle:"WAMPSEVER Homepage"	Files Containing Juicy Info	HackerFrenzy
2022-09-19	inurl:json beautifier online	Files Containing Juicy Info	Nyein Chan Aung
2022-09-19	intitle:"IIS Windows Server"	Files Containing Juicy Info	HackerFrenzy
2022-09-19	intitle:"index of" inurl:SUID	Files Containing Juicy Info	Mahedi Hassan
2022-09-19	intitle:"index of" intext:"Apache/2.2.3"	Files Containing Juicy Info	Wagner Farias
2022-08-18	inurl:"index.php?page=news.php"	Advisories and Vulnerabilities	Omar Shash
2022-08-18	inurl:/sym404/root	Files Containing Juicy Info	Numen Blog
2022-08-17	inurl:viewer/live/index.html	Various Online Devices	Palvinder Singh Secuneus
2022-08-17	intitle:index of "/venv"	Sensitive Directories	Abhishek Singh
2022-08-17	intitle:"WEB SERVICE" "wan" "lan" "alarm"	Pages Containing Login Portals	Heverin Hacker
2022-08-17	allintitle:"Log on to MACH-ProWeb"	Pages Containing Login Portals	Under The Sea hacker
2022-08-17	intitle:"index of" "access_token.json"	Files Containing Juicy Info	Leonardo Venegas
2022-08-17	inurl:"admin/default.aspx"	Pages Containing Login Portals	Payal Yedhu

Showing 1 to 15 of 7,536 entries

FIRST PREVIOUS 1 2 3 4 5 ... 503 NEXT LAST

**Downloads** **Certifications** **Training** **Professional Services**

Kali Linux OSCP Penetration Testing with Kali Linux (PWK) (PEN-200) All new for 2020 Penetration Testing



# Google Dorking'i Önleme

Google Dorking'i sizin başka kişilerin sitesinde kullanabileceğiniz gibi başkaları da sizin sitenizden bilgilerinize erişmek isteyebilir. Bunun önüne geçebilmek için alınabilecek bazı önlemler şu şekildedir:

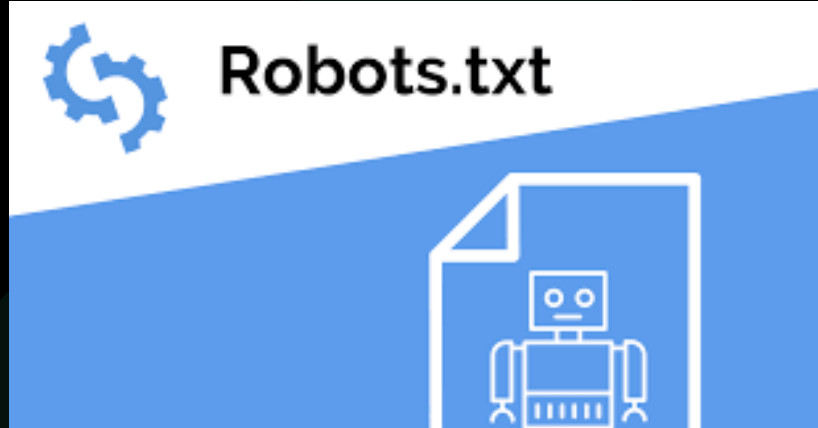
- Kullanıcı ve parola kimlik doğrulaması ile ve ayrıca IP tabanlı kısıtlamalar kullanarak özel alanları koruyun.
- Hassas bilgilerinizi (kullanıcı, şifreler, kredi kartları, e-postalar, adresler, IP adresleri, telefon numaraları vb.) şifreleyin.
- Sitenize karşı düzenli güvenlik açığı taramaları yapın; bunlar genellikle popüler Google Dorks sorgularını kullanır ve en yaygın olanları tespit etmede oldukça etkili olabilir.
- Kötü adamlar yapmadan önce önemli bilgileri bulabileceğinizi görmek için kendi web sitenize düzenli olarak dork sorguları çalıştırın. Hassas içeriğin açık olduğunu tespit ederseniz Google Search Console'u kullanarak kaldırılmasını isteyin.
- Kök düzeyindeki web sitesi dizininizde bulunan bir robots.txt dosyası kullanarak hassas içeriği engelleyin.





# Robot.txt Nedir ?

**Robot engelleme standardı**, (aynı zamanda Robot engelleme protokolü veya **robots.txt** olarak da bilinir) web spider gibi yazılımların web sunucularının kamuya açık bölümlerinin tamamına veya bir kısmına erişimini engellemeye yarayan bir standarttır. Genelde web sitelerini sınıflandırmak ve arşivlemek amacı ile arama motorları ya da düzeltilmiş kaynak kodları için site yöneticileri robotları kullanırlar. Robotlar bu işlem sonucunda web siteleri için site haritaları oluştururlar.







# Google Dorking'i Önlemek için robots.txt

## Yapılandırmalarını Kullanma

Aşağıdaki yapılandırma, web sitenizdeki herhangi bir dizinden yapılan tüm taramayı reddedecektir; bu, genel olarak dizine eklenebilir İnternet içeriğine güvenmeyen özel erişim web siteleri için oldukça yararlıdır.

```
User-agent: * Disallow: /
```

Ayrıca web taramasından hariç tutulacak belirli dizinleri de engelleyebilirsiniz. Bir / admin alanınız varsa ve ayrıca tüm alt dizinleri korumak istiyorsanız, bu kodu içine yerleştirin:

```
User-agent: * Disallow: /admin/
```





**Belirli dosyalara** erişimi kısıtlamak için

```
User-agent: * Disallow: /privatearea/file.htm
```

**'?'** İçeren **dinamik URL'lere** erişimi kısıtlayın sembol

```
User-agent: * Disallow: /*?
```





Belirli **dosya uzantılarına** erişimi kısıtlamak için

```
User-agent: * Disallow: /*.php$/
```

Bu komut sayesinde **“.php” dosyalarına** tüm erişim reddedilir.





Yahya akıcı

Hazırlanılan ierik, 2022-2023 Yılı BiltekCyber Takım Eđitimi iin hazırlanmıř olup  
izinsiz ođaltılamaz

### **Kaynaka:**

<https://mustafairan.wordpress.com/2014/09/29/google-hacking-nedir-ne-ise-yarar-nasil-yapilir/>

[https://tr.wikipedia.org/wiki/Robot\\_engelleme\\_standardı](https://tr.wikipedia.org/wiki/Robot_engelleme_standardı)

<https://www.turkhackteam.org/konular/google-dork-ile-pasif-kesif-admin-paneli-db-bilgilerine-erisim.2006699/>

[https://en.wikipedia.org/wiki/Google\\_hacking](https://en.wikipedia.org/wiki/Google_hacking)

<https://bbsteknoloji.com/google-dorks-nedir/>





Yahya akıcı

Hazırlanılan ierik, 2022-2023 Yılı BiltekCyber Takım Eđitimi iin hazırlanmıř olup

izinsiz ođaltılamaz

## Kaynaka

<https://www.siberguvenlik.web.tr/index.php/2021/01/16/google-dorks-nedir/>

<https://www.cybrary.it/blog/0p3n/advanced-google-dorking-commands/>

<https://www.exploit-db.com/google-hacking-database>

<https://securitytrails.com/blog/google-hacking-techniques>

