Google Dork (veya Google dorking, Google hacking), Google ve benzeri arama motorlarının gelişmiş arama operatörlerini kullanarak belirli türde içerikleri bulma tekniğidir. Amaç genelde hedefe özel ve hassas bilgileri daha hızlı filtrelemek: örneğin belirli bir sitedeki PDF’ler, belirli başlığı içeren sayfalar, belirli dosya türleri vb.

Bu tekniği araştırma, akademik çalışma, bilgi bulma veya sitenizde yanlışlıkla yayılan içerikleri tespit etmek için kullanabilirsiniz. Aynı yöntem kötü niyetli kişiler tarafından yanlış yapılandırılmış sunucuları, gizli dosyaları veya hassas bilgileri aramak için de kullanılabildiğinden etik ve yasal sınırlar çok önemli.

Temel arama operatörleri (güvenli, meşru kullanım örnekleriyle)

Aşağıdakiler genel arama operatörleridir; zarar verici veya istismar edici arama dizileri paylaşmayacağım. Bu operatörleri meşru amaçlarla kullanarak hızlıca bilgi bulabilirsin.

site:example.com

Belirli bir alan içinde arama yapar.

Örnek: site:university.edu syllabus filetype:pdf — üniversitenin sitesindeki PDF ders programlarını aramak için.

filetype:pdf (veya doc, xls vs.)

Belirli dosya türlerini arar.

Örnek: filetype:ppt "machine learning" site:edu.tr — Türkiye üniversitelerindeki ML sunumlarını aramak.

intitle:"kelime"

Sayfa başlığında (title) arama yapar.

Örnek: intitle:"kurumsal rapor" site:company.com

inurl:kelime

URL’de belirli kelimenin geçtiği sayfaları bulur.

Örnek: inurl:blog site:example.com

cache:URL

Google’ın önbelleğindeki halini gösterir (bazen silinmiş sayfaları görmek için).

"-kelime"

Aramadan bir kelimeyi hariç tutar.

Örnek: python tutorial -django

Kombinasyonlar:

Operatörleri birleştirerek hedefe daha hızlı ulaşabilirsin: site:gov.tr filetype:pdf intitle:"bütçe"

Not: Bu operatörlerin kendileri zararlı değil; asıl mesele ne aradığın ve ne amaçla kullandığın.

Google Dork neden tehlikeli olabilir?

Yanlış yapılandırılmış sunucular veya erişime açık dosyalar, Google tarafından dizine eklenmiş olabilir. Kötü niyetli kişiler bu dizinlenmiş bilgileri suistimal edebilir.

Otomatik araçlarla birleştiğinde büyük ölçekli tarama (reconnaissance) ve başarılı saldırılar için başlangıç noktası olabilir.

Bu yüzden güvenlik araştırmacıları etik kurallar çerçevesinde (sorumlu açıklama / responsible disclosure) hareket eder.

Güvenli / etik kullanım örnekleri

Kendi siteni tarayıp yanlışlıkla herkese açık hale gelmiş gizli dosyaları bulmak.

Akademik araştırma için belirli türde dosyaları (tezler, raporlar) bulmak.

Rakip analizinde (kamu bilgisiyle) kamuya açık dokümanları taramak.

İçerik yöneticilerine kullanıcının yanlışlıkla paylaşmış olduğu verileri bildirmek.

Her zaman hedefin sahibiyle iletişime geç: eğer hassas bir şey bulursan, kötü niyetli olarak kullanma; sorumlu şekilde bildir.

Nasıl korunulur? (web yöneticileri / geliştiriciler için)

Eğer sen bir site yöneticisiysen veya bir projeyi koruman gerekiyorsa, işte uygulanacak pratikler:

Gizli dosyaları halka açık sunucularda saklama. Hassas konfigürasyon veya yedek dosyalarını (backup, .env, vb.) sunucuda herkese açık dizinlere koyma.

Robots.txt güvenlik aracı değildir. Sadece arama motorlarına yol gösterir; hassas dosyaları oraya koyma (çünkü bu dosya etik olarak “ne gizli” olduğunu ilan eder).

Erişim kontrolü: Önemli sayfalarda kimlik doğrulaması (authentication) ve yetkilendirme (authorization) kullan.

Dizin listelemeyi kapat: Eğer bir dizinde index yoksa server otomatik liste göstermesin.

Arama motoru dizinlemesini sınırlandır: noindex meta etiketi veya uygun header’larla gizli sayfaların dizine eklenmesini engelle. (Ancak bu mutlak güvenlik sağlamaz.)

Günlükleri ve uyarıları takip et: Olağandışı tarama aktivitelerini tespit etmek için log ve WAF (Web Application Firewall) kurallarını izle.

Sorumlu açıklama politikası oluştur: Eğer bir güvenlik araştırmacısı hassas bir şey bulursa nasıl iletişime geçeceğini açıkça belirt.

Hukuk ve etik

Başkasının sistemine izinsiz erişim, veri toplama veya veri ihlali yasal sorumluluk doğurabilir.

Google Dork ile hassas bilgi bulduğunda en doğru adım: kötüye kullanmamak, site sahibiyle temasa geçmek ve gerekiyorsa yetkili mercilere/iyileştirme adımlarına yönlendirmek.