# Google Dork Nedir?

Oluşturulma tarihi: 25 September 2025 08:06

## Kısa cevap

Google dork (veya Google dorking / Google hacking), Google gibi arama motorlarının gelişmiş arama operatörlerini kullanıp otomatikleştirerek internette yanlışlıkla herkese açılmış — çoğu kez hassas — bilgileri bulma tekniğidir. Örneğin geliştiricilerin, yöneticilerin veya kullanıcıların istemeden açık bıraktığı dosyalar, yapılandırma dosyaları, zafiyetli uygulama sayfaları vb. bu yöntemle keşfedilebilir.

## Nasıl çalışır (kısaca, teknik ama zararsız şekilde)

Google’ın sunduğu site:, filetype:, inurl:, intitle: gibi operatörler bir araya getirilerek arama çok daraltılır. Bu operatörler ile arama motorunun indekslediği içerikler içinden belirli dosya tipleri veya URL yolları hedeflenir; ortaya çıkan sonuçlar bazen asla kamuya açılmaması gereken verileri gösterebilir.

## Tarih / Kaynak

Bu yaklaşımın bilinen bir arşivi Google Hacking Database (GHDB)'dir — pentester’lar ve araştırmacılar için sınıflandırılmış dork sorgularının toplandığı bir listedir. GHDB genellikle Exploit-DB gibi platformlarda barındırılır.

## Riskler ve yasal durum

Google dorking, bilgi toplama (reconnaissance) aşamasında kullanılır; kötü niyetli kişiler bunu kullanarak zayıf nokta arayabilir. Ancak yalnızca arama yapmak her zaman doğrudan suça girmez — elde edilen bilgiyi yetkisiz erişim için kullanmak çoğu ülkede suçtur. Etik ve yasal değerlendirme önemlidir.

## Site sahibine / geliştiriciye öneriler (savunma/önleme)

1. Hassas dosyaları sunucuda halka açık klasörlere koyma (kimlik bilgileri, yapılandırma dosyaları vb.).  
2. Erişim kontrolü / kimlik doğrulama uygulayın — kritik sayfalar sadece oturum açmış kullanıcıya açık olmalı.  
3. robots.txt ve noindex meta etiketleri yalnızca arama motorlarına “indexleme yapma” demek içindir; gizli olması gereken şeyleri sadece buna güvenerek bırakma.  
4. Sunucu yapılandırmasını düzelt: dizin listelemeyi kapat, hata sayfalarında detaylı yığın izi/konfigürasyon gösterme.  
5. Düzenli tarama ve test: OWASP rehberleri, sızma testi araçları ve GHDB kontrolü ile sitenin istemeden neleri ifşa ettiğini düzenli kontrol et.

## Etik / güvenlik notu

Google dorking’in kendisi bir “araştırma” tekniğidir; fakat bu teknik kötü amaçlı kullanım için de sıkça tercih edilir. Eğer güvenlik araştırması yapıyorsan izin al (pentest izni), yoksa yalnızca kendi altyapını test et veya durumu site sahibine sorumlulukla bildir (responsible disclosure).

## İstersen

Bu konuyu örneklerle (sadece savunma amaçlı, zararlı örnekler içermeyecek şekilde) daha detaylı anlatabilirim; veya kendi siteni hızlıca kontrol etmek istiyorsan hangi adımları (log kontrolü, robot taramaları, yanlış açıklar) uygulayabileceğini adım adım yazarım.