# Google Dorks — Genel Bilgi ve Rehber

## 1. Google Dorks nedir?

Google Dorks (veya "Google dorking"), arama motoru operatörleri ve gelişmiş sorgular kullanarak Google'da hedefli bilgi arama yöntemine verilen addır. Bu teknik, arama operatörlerini birleştirerek belirli dosya türleri, URL parçaları, başlıklar veya belirli web sitelerinde yer alan içerikler gibi özelleşmiş sonuçlara ulaşmayı sağlar.

## 2. Temel amaçları ve kullanım alanları

Google Dorks çeşitli amaçlarla kullanılır:  
  
• Güvenlik değerlendirmesi: Penetrasyon testlerinde (izinli olarak) açık kaynak istihbaratı (OSINT) toplamak için.  
• Bilgi keşfi: Kamuya açık belgeler, raporlar veya belirli dosya türleri bulunurken.  
• Araştırma ve analiz: Akademik çalışmalar, sektör raporları veya teknik döküman ararken.  
  
Not: Google Dorks hem etik hem de kötü amaçlı kullanımlara açık bir tekniktir. Yasal izin olmadan başkalarına ait sistemleri araştırmak veya hassas bilgilere erişmeye çalışmak yasa dışıdır ve etik değildir.

## 3. Yaygın arama operatörleri (örnekler)

Aşağıdaki operatörler Google ve benzeri arama motorlarında sık kullanılır:  
  
• site: — Belirli bir alan içinde arama yapar. Örnek: site:example.com  
• filetype: — Belirli dosya türlerini arar. Örnek: filetype:pdf  
• inurl: / allinurl: — URL içinde belirli kelimeleri arar. Örnek: inurl:admin  
• intitle: / allintitle: — Sayfa başlığında arama yapar. Örnek: intitle:"index of"  
• intext: — Sayfa metninde geçen ifadeyi arar. Örnek: intext:"gizli"  
• cache: — Google'ın önbelleğinde saklanan sayfayı getirir. Örnek: cache:example.com  
• related: — Belirli bir siteyle ilişkili siteleri bulur. Örnek: related:example.com  
  
Bu operatörler tek başına veya kombinasyon halinde kullanılabilir.

## 4. Güvenli ve etik kullanım önerileri

• İzin alın: Bir kuruluşun güvenlik incelemesini yapıyorsanız önceden yazılı izin (scope belirlenmiş) alın.  
• Hassas bilgileri ifşa etmeyin: Yasal olmayan erişim veya açıklama yapmayın. Bulduğunuz hassas bilgi varsa uygun kanallarla (ör. sorumlu açıklama) yetkili kişilere bildirin.  
• Kayıt tutun: Yaptığınız aramalar, hangi veriler bulunduğu ve hangi izinlere dayanılarak yapıldığını belgeleyin.  
• Eğitim amaçlı kullanın: Google Dorks'u savunma ve farkındalık çalışmalarında kullanarak kurumların sızan bilgileri kapatmasına yardım edin.

## 5. Riskler ve yasal uyarı

Google Dorking yanlış ellere geçtiğinde kişisel verilerin, kimlik bilgileri veya hassas yapılandırma dosyalarının keşfine yol açabilir. Bu tür verilerin izinsiz toplanması ve kullanılması çoğu ülkede suçtur. Her zaman yerel yasa ve kurum politikalarına uyun.

## 6. Savunma: Kurumlar bu riski nasıl azaltır?

• Hassas verileri internette yayınlamayın; gerekiyorsa erişimi kimlik doğrulama ile sınırlandırın.  
• robots.txt'i hassas bilgileri gizlemek için birincil yöntem gibi kullanmayın (robots.txt yalnızca iyi niyetli botları yönlendirir).  
• Dosya izinlerini ve sunucu yapılandırmasını düzenli olarak kontrol edin.  
• Veri sızıntılarını ve yanlış yapılandırmaları tarayan otomatik araçlar kullanın.  
• Güvenlik farkındalığı eğitimi verin; çalışanların yanlışlıkla hassas dosyaları internete koymasını engelleyin.

## 7. Örnek (güvenli/zararsız kullanım)

Aşağıdaki örnekler eğitim ve halka açık içeriği bulma amaçlıdır:  
  
• site:university.edu filetype:pdf "ders notları" — Bir üniversitenin halka açık PDF ders notlarını bulmak.  
• site:gov.tr filetype:xls "istatistik" — Kamuya açık istatistik tablolarını aramak.  
  
Bu örnekler bilgiye erişim amaçlıdır; hassas sistemleri veya kişisel verileri aramaya yönelik değildir.

## 8. Kısa terminoloji sözlüğü

• OSINT: Open-Source Intelligence — Açık kaynaklardan toplanan istihbarat.  
• Dork: Gelişmiş arama sorgusu (genellikle operatörlerle birlikte kullanılır).  
• Scope: Bir test veya araştırma sırasında izin verilen hedeflerin sınırları.

## 9. Kaynakça ve ileri okuma önerileri

İleri okumalar ve araçlar için resmi güvenlik kaynakları, OWASP materyalleri ve siber güvenlik topluluğu dokümanları takip edilebilir.  
  
— OWASP (Open Web Application Security Project)  
— Sorumlu açıklama (responsible disclosure) rehberleri