Google Dork (Google Dorking) Hakkında Bilgi

*Kısa Bilgi Notu • Hazırlayan: ChatGPT — Tarih: 03 Ekim 2025*

**Özet:** Google Dork (veya Google Dorking), arama motoru operatörlerini kullanarak daha hedefli ve gelişmiş aramalar yapma tekniğidir. Bu teknik hem bilgi keşfi (reconnaissance) hem de yanlış yapılandırılmış veya kazara ifşa olmuş bilgileri tespit etmek için kullanılabilir.

# 1. Google Dork Nedir?

Google Dork, arama motorunun desteklediği özel operatörleri (ör. site:, filetype:, inurl:, intitle: vb.) kullanarak belirli içerikleri, dosya türlerini veya sayfa özelliklerini hedeflemeye yarayan aramalardır. Siber güvenlik topluluklarında bazen 'dork' olarak anılır ve hem güvenlik testi hem de kötü amaçlı keşif için kullanılabilir.

# 2. Yaygın Operatörler (Genel Tanım)

* Aşağıdaki operatörler arama davranışını daraltmak için kullanılır. Bu kısım operatörlerin işlevlerini açıklar; zararlı kullanım için örnek kombinasyonlar verilmez.
* site: — Belirli bir alan içinde arama yapar.
* filetype: veya ext: — Belirli bir dosya türünü arar (ör. PDF, DOCX).
* inurl: — URL içinde belirli bir kelime arar.
* intitle: — Sayfa başlığında belirli bir kelime arar.
* cache: — Arama motorunun önbelleğindeki sürümü gösterir.
* related: — Benzer siteleri bulmaya yardımcı olur.

# 3. Kullanım Alanları (Etik ve Savunma Odaklı)

* • Güvenlik testleri: Bir kuruluşun açıkça izin verdiği durumlarda, yanlış yapılandırılmış sunucuları, herkese açık belgeleri veya test ortamlarını bulmak için kullanılabilir.
* • Bilgi keşfi (recon): IT ekipleri, istemeden indekslenmiş hassas bilgileri tespit edip temizlemek için aramalar yapabilir.
* • İçerik yönetimi: Arama sonuçlarında görünmesi istenmeyen eski belgeleri veya dökümanları bulup güncellemek için kullanılabilir.

# 4. Yasal ve Etik Hususlar

Google Dorking, kendiliğinden yasa dışı değildir; fakat elde edilen bilgilerin kötüye kullanılması (ör. yetkisiz erişim, veri hırsızlığı) suç teşkil eder. Güvenlik taramaları yapmadan veya bir kuruluşun verilerini aramadan önce mutlaka yazılı izin alınmalıdır.

# 5. Savunma İçin Pratik Öneriler (Önleyici Adımlar)

* Aşağıdaki adımlar kurumların istemeden indekslenen hassas içerikleri azaltmasına ve arama motorları üzerinden bilgi sızıntısını önlemesine yardımcı olur:
* • Hassas veriyi herkese açık sunucularda tutmayın; kimlik doğrulama gerektiren alanlar için uygun erişim kontrolü uygulayın.
* • Robots.txt ve meta noindex etiketleri kullanarak arama motoru indekslemesini kontrol edin (robots.txt tek başına güvenlik sağlamaz, ancak indekslenmeyi azaltır).
* • Sızan belgeleri ve eski yedekleri düzenli olarak temizleyin ve şifrelenmiş depolama kullanın.
* • Web uygulamalarında gizlilik/konfigürasyon kontrolleri uygulayın; erişim kontrollerini test edin.
* • WAF, güvenlik izleme (SIEM) ve düzenli taramalar ile şüpheli tarama aktivitelerini ve otomatik dorking girişimlerini tespit edin.
* • Hassas bilgilerin yanlışlıkla dosya adlarına veya URL parametrelerine konulmadığından emin olun (örn. parola veya gizli anahtar içermesin).
* • Çalışanlara veri güvenliği ve ‘what not to publish’ eğitimi verin.

# 6. Tespit ve İzleme (Defansif Yaklaşım)

* • Sunucu ve erişim loglarını analiz ederek anormal arama taramaları veya tek IP’den gelen yüksek hacimli sorguları tespit edin.
* • Honeypot/tuvalet sayfalar (guardian pages) kullanarak otomatik keşif araçlarını saptayabilirsiniz (etik kullanıma dikkat).
* • Düzenli içerik denetimleri (pentest, red-team) ile istem dışı veri sızıntılarını ortaya çıkarın.

# 7. Güvenli Eğitim ve Test Ortamı Önerisi

Google Dorking öğreniliyorsa, bunu yalnızca izole edilmiş test ortamlarında veya yasal izin alınmış hedeflerde uygulayın. Açık kaynaklı eğitim platformları ve CTF'ler güvenli pratik yapmak için uygundur.

# 8. Örnekler (Güvenli ve Zararsız Tutumlu Açıklamalar)

* Aşağıda operatörlerin kullanımına dair örnek gösterimler vardır. Bu örnekler bilgi amaçlıdır ve hiçbir hassas bilgi aramayı teşvik etmez:
* • site:example.com — Sadece example.com alanı içinde arama yapar.
* • filetype:pdf — PDF dosya türlerini aramaya yardımcı olur (genel döküman aramaları için).
* Bu örnekler, operatörlerin ne işe yaradığını anlamanız için verilmiştir; lütfen bunları kötü amaçlı keşif için kullanmayın.

# 9. Kaynakça ve İleri Okuma

• Google arama operatörleri resmi dökümantasyonu ve yardım sayfaları.

• OWASP — Bilgi toplama ve keşif (reconnaissance) kılavuzları (savunma odaklı).

• Siber güvenlik etik kuralları ve yerel yasalar (Türkiye için KVKK, ilgili bilişim suçları mevzuatı).

Not: Bu belge eğitim ve savunma amaçlı hazırlanmıştır. Google Dorking ile elde edilen bilgilerin yetkisiz veya zararlı kullanımı yasal sorumluluk doğurur.