***SHODAN NEDIR? NE İŞE YARAR ?***

SHODAN (Sentient Hyper-Optimized Data Access Network), internet uzerinde herkese acik sekilde bagli olan cihazlari, sunuculari ve servisleri tarayip bu bilgileri arama motoru mantigi ile sunan bir siber guvenlik aracidir. Google gibi web sitelerini indekslemez; bunun yerine IP adreslerine bagli servisleri, sistemleri ve cihazlari listeler.

**SHODAN NASIL ÇALIŞIR**

**SHODAN NASIL CALISIR?**

Shodan, belirli portlari (80, 443, 21, 22 vb.) tarar ve bu portlardan gelen "banner" bilgilerini toplar. Bu banner'lar genellikle su bilgileri icerir:

* Sunucu turu (Apache, nginx, IIS vs.)
* Yazilim versiyonlari
* Isletim sistemi bilgileri
* IP ve lokasyon
* Hizmetin acik oldugu port bilgileri
* Potansiyel zafiyetler (CVE numaralariyla birlikte)

**SHODAN NE ICIN KULLANILIR?**

*Yasal Kullanimlar:*

* Sistem yoneticileri tarafindan kendi sistemlerini kontrol etmek
* Siber guvenlik uzmanlari tarafindan zafiyet analizi yapmak
* Arastirmacilarin internete bagli cihazlar uzerine istatistik toplamalari
* SCADA, IoT ve endustriyel sistemlerin guvenlik denetimleri

*Yasadisi Kullanimlar:*

* Parola korumasi olmayan IP kameralarini izlemek
* Zafiyet barindiran cihazlara izinsiz giris yapmak
* IoT cihazlarini botnet'e dahil etmek

*UYARI:* Shodan'in sunduğu veriler kamuya acık olsa da, bu verileri kullanarak herhangi bir sisteme izinsiz giriş yapmak hukuken SUCTUR (TCK 243).

**Shodan'ın Pentest Uzmanları İçin Önemi**

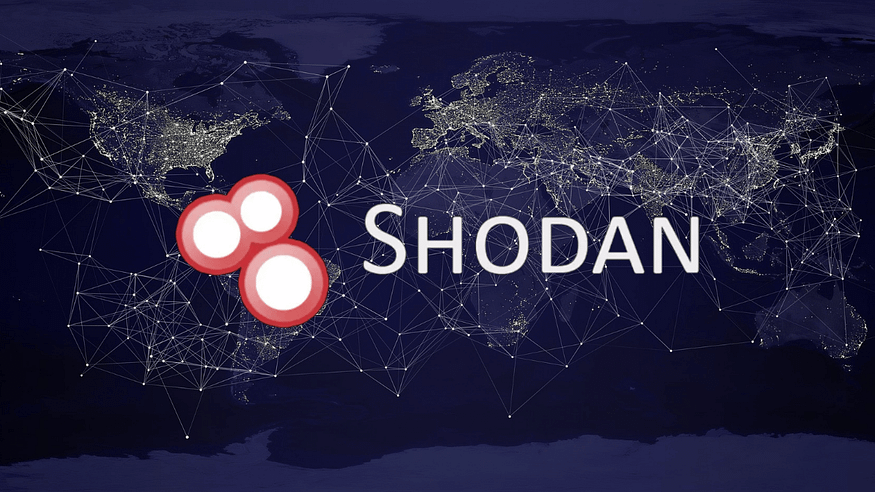
Penetrasyon testi, açıkta kalan hizmetler ve yanlış yapılandırılmış cihazlar hakkında bilgi toplamayı gerektirir. Shodan, herkese açık sistemleri, çalışan hizmetleri ve güvenlik açıklarını tespit etmeye yardımcı olarak önemli bir keşif aracıdır.

Nmap gibi geleneksel tarayıcıların aksine, Shodan interneti sürekli tarar ve açık servislerin aranabilir bir veritabanını tutar. Bu, zamandan tasarruf sağlar ve sızma test uzmanlarının bir hedefi aktif olarak araştırmadan önce potansiyel saldırı yüzeylerini belirlemelerine yardımcı olur.

**Shodan'a Başlarken**

Shodan'ı etkili bir şekilde kullanmak için bir hesaba ihtiyacınız var. Ücretsiz hesabın işlevselliği sınırlıdır, ancak **Shodan Academic Plus'a** yükseltmek ek özelliklerin kilidini açar; ben de bu hesap seviyesindeki bazı özellikleri kullanıyorum. Ayrıca, ihtiyaçlarınıza göre daha yüksek seviyeli bir hesap da seçebilirsiniz.

**Eğer bir üniversite e-posta kimliğiniz** varsa , bunu kullanarak kaydolabilir, giriş yapabilir ve ek özelliklere erişebilirsiniz.



**Shodan'ın Bazı Temel Özellikleri**

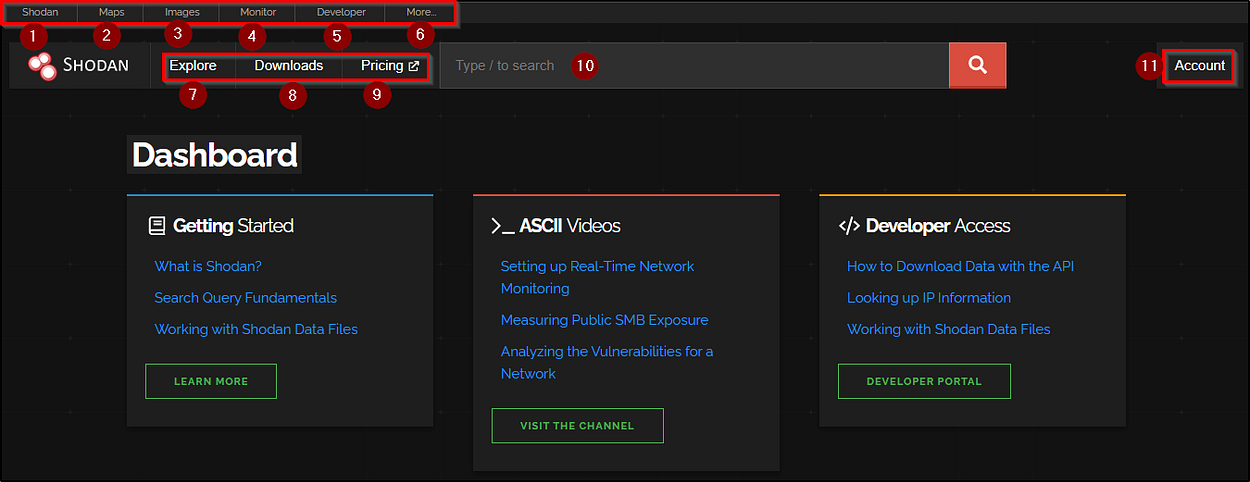
* **Arama Filtreleri** — Çeşitli filtreler kullanarak belirli cihazları, hizmetleri veya güvenlik açıklarını tespit edin.
* **Banner Bilgileri** — Yazılım sürümü, işletim sistemi, açık portlar ve meta veriler gibi ayrıntıları toplar.
* **Exploit Finder** — Güvenlik açığı olan yazılım sürümlerini çalıştıran sistemleri belirler.
* **Ağ Haritalama** — Kuruluşlar için internete bakan varlıkları haritalar.
* **IoT Cihaz Keşfi** — Açığa çıkmış ve yanlış yapılandırılmış IoT cihazlarını tespit eder

**Shodan.io'ya Başlarken**

Shodan.io'yu kullanmaya başlamak için bir hesap oluşturun ve bağlı cihazlar için güçlü arama motorunu keşfedin. Kontrol paneli, belirli filtreleri kullanarak dünya çapında cihazları, hizmetleri ve güvenlik açıklarını kolayca aramanıza olanak tanır.

**Cihaz konumlarını Haritalar'da** görselleştirebilir , cihaz görüntülerini görüntüleyebilir ve devam eden uyarılar için **İzleme** özelliğini ayarlayabilirsiniz . Geliştiriciler, Shodan'ın işlevselliğini **API** aracılığıyla özel uygulamalara entegre edebilir .

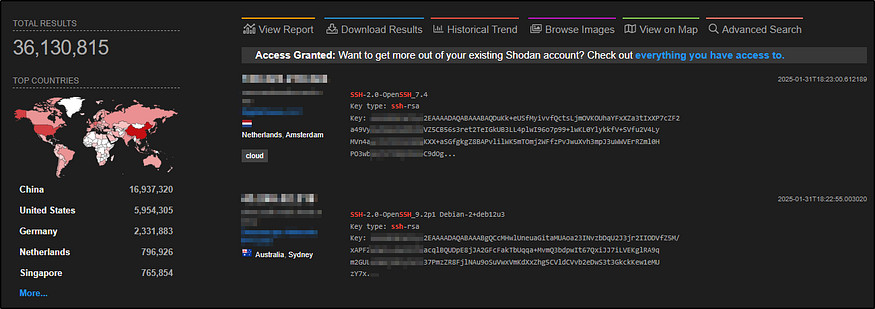
Burada her sekmeyi açıklayan panoda gezineceğiz.



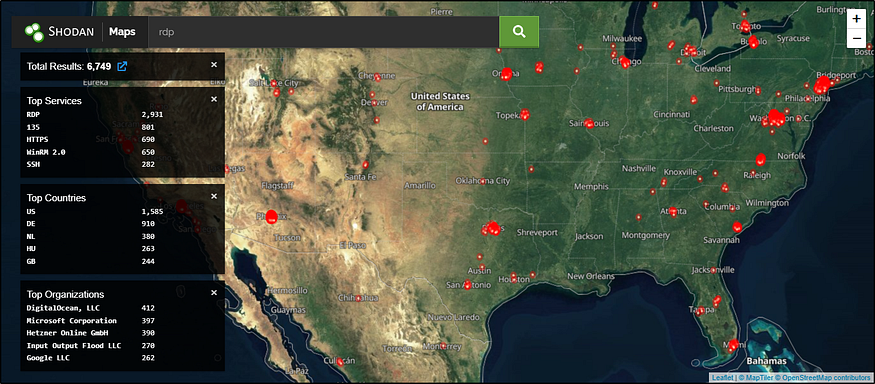
- Shodan Kontrol Paneli -

**1. Shodan:**  
Ana sekme, aramalarınızı başlatabileceğiniz, hesabınıza erişebileceğiniz ve Shodan hakkında genel bilgileri görüntüleyebileceğiniz yerdir. Platformun ana sayfasıdır.

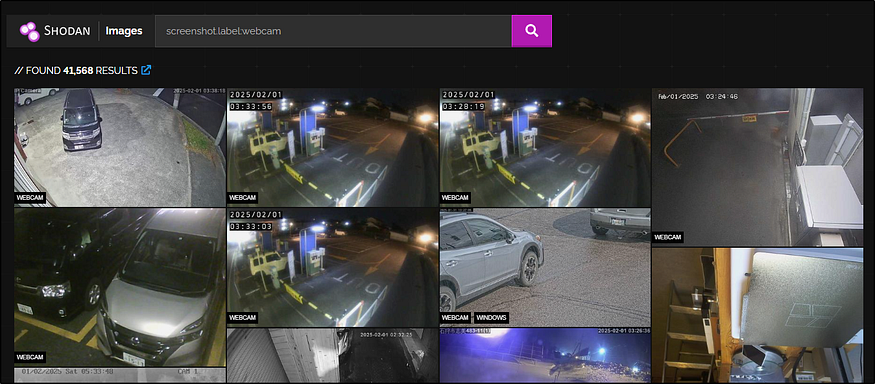
İşte Shodan'ın nasıl çalıştığına dair bir görüntü.



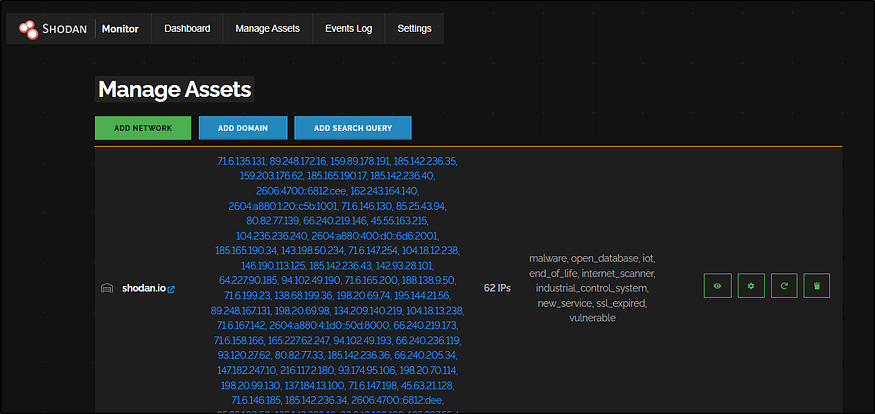
**2. Haritalar:**  
Dünya genelinde internete bağlı cihazların görsel bir temsilini sunar. Shodan'ın endekslediği cihazların coğrafi dağılımına ilişkin gerçek zamanlı verileri görebilirsiniz.



**3. Görüntüler:**  
Shodan'ın taramaları sırasında bulduğu cihazların (web kameraları, yönlendiriciler vb.) görüntülerini gösterir. Bunlar genellikle internete bağlı cihazlardan alınan ve herkesin erişimine açık görüntülerdir.

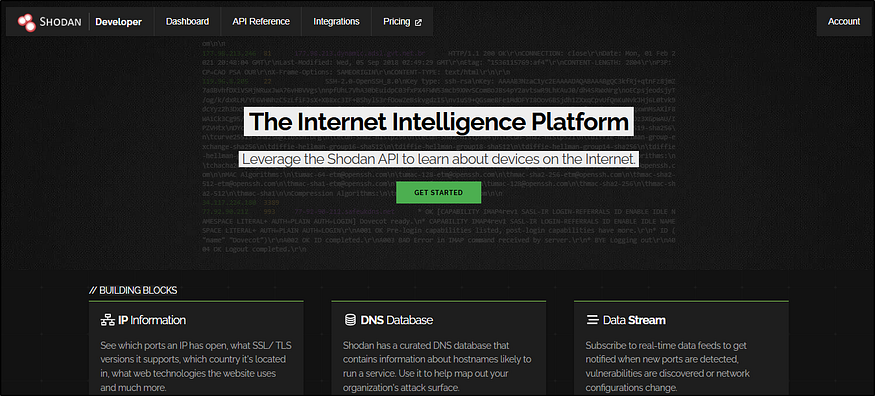


**4. İzleme:**  
Belirli etki alanları veya IP aralıkları için uyarılar veya sürekli izleme ayarlayabilirsiniz. Zaman içindeki değişiklikleri takip edebilir ve belirli olaylar meydana geldiğinde bildirim alabilirsiniz.

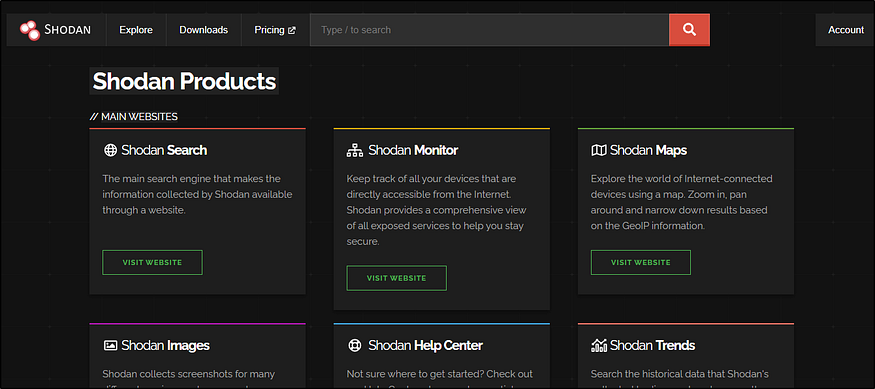


Örnek: shodan.io alan adı

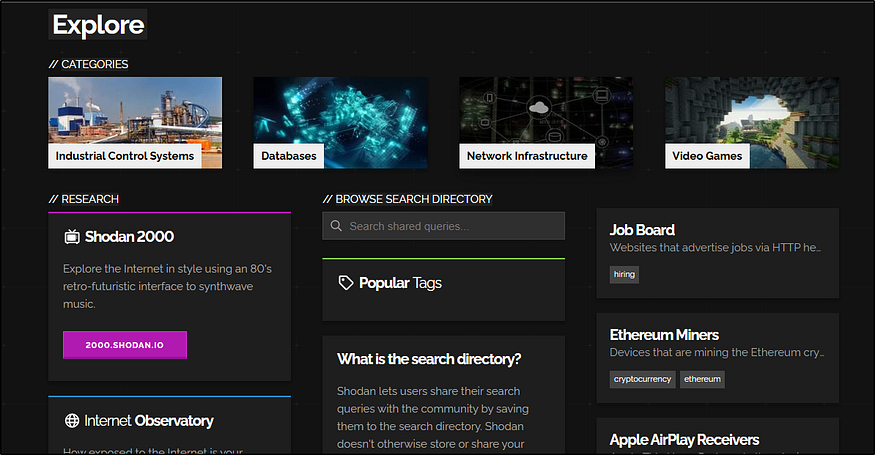
**5.Geliştirici:**  
Shodan'ın API belgelerine erişim sağlayarak, geliştiricilerin Shodan'ın işlevlerini kendi uygulamalarına entegre etmelerine olanak tanır. API anahtarlarını buradan alabilir ve nasıl kullanılacağını öğrenebilirsiniz.



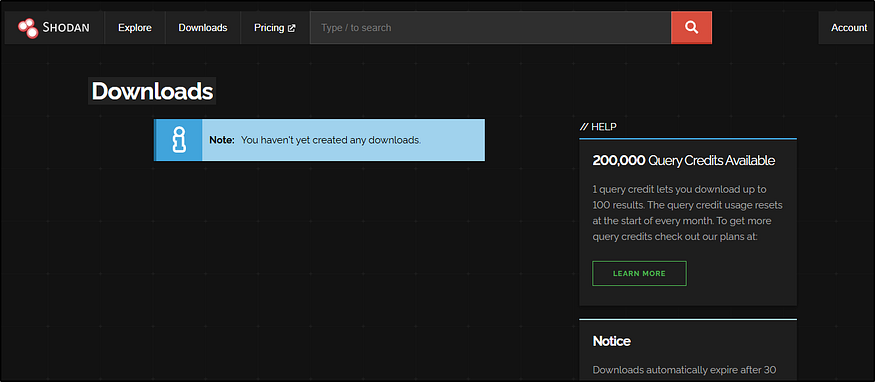
**6.Daha Fazla:**  
Bu bölüm, birincil menüde bulunmayan ek özellikler veya ayarlar, ürünler, hizmetler ve daha fazlasını (araçlar, belgeler ve gelişmiş arama filtreleri gibi) içerebilir.



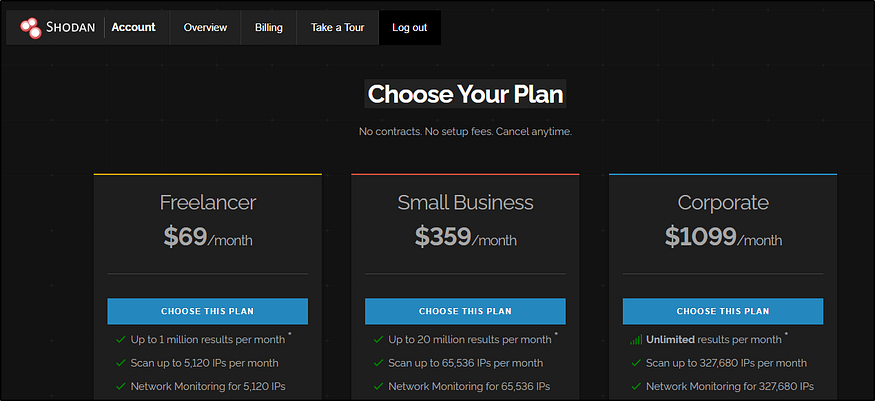
**7. Keşfet:**  
Shodan'da ilgi çekici ve popüler aramaları keşfetmenin bir yolu. Bu, trend olan cihazları, güvenlik açıklarını veya ilginç ağ modellerini içerebilir.



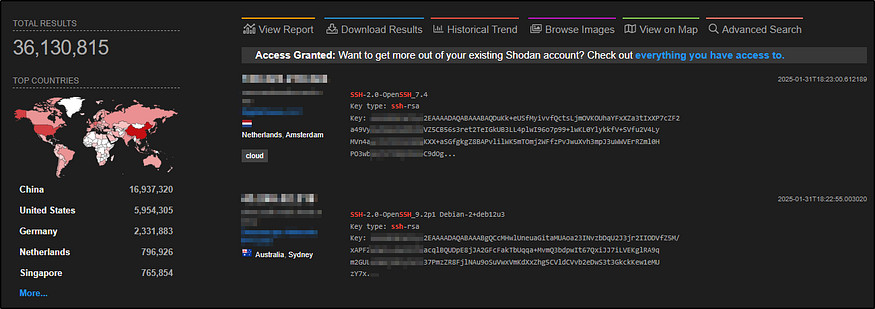
**8.İndirmeler:**  
İndirebileceğiniz tüm kaynaklarınız ve raporlarınız burada yer alacaktır.



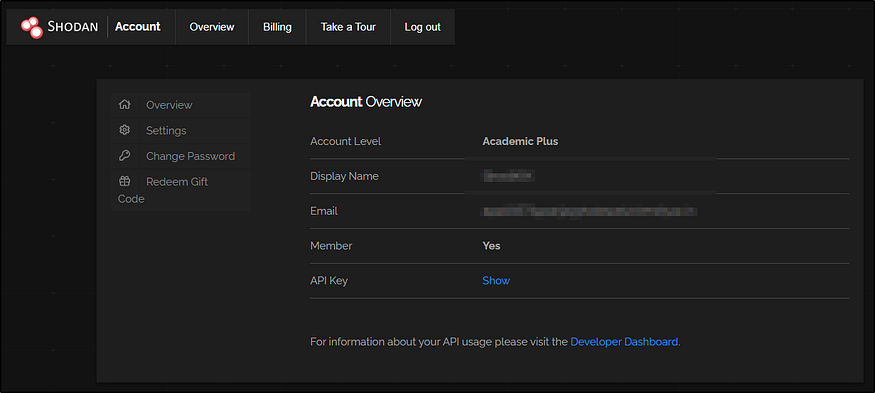
**9. Fiyatlandırma:**Shodan'ın farklı erişim seviyeleri için fiyatlandırma planlarını görüntüleyebileceğiniz bir bölüm. Bu bölüm, temel ücretsiz hesabın yanı sıra ek özellikler ve veri erişimi sunan çeşitli ücretli seçenekleri içerir.



**10.Arama Çubuğu:**Kontrol panelinin en üstünde yer alır ve Shodan'ın indekslenmiş verilerinde cihazlar, hizmetler, güvenlik açıkları veya belirli anahtar kelimeler için arama yapmanızı sağlar.

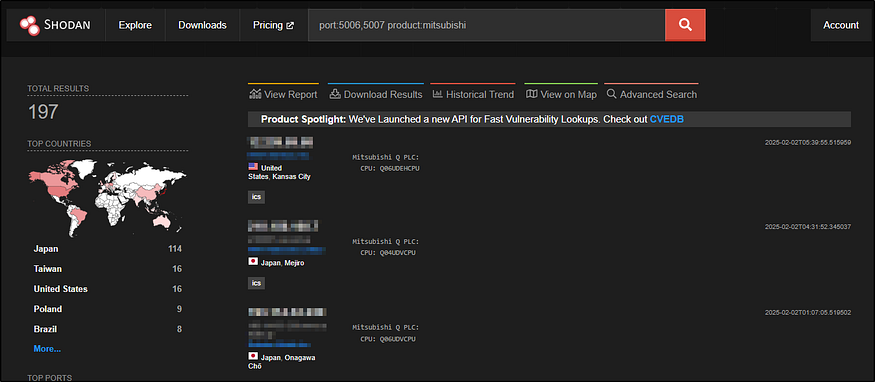
  
ara: ssh

**11. Hesap:**  
Shodan **Hesap Genel Bakışı** , Hesap Seviyeniz (Akademik Plus), Görünen Adınız (Hesap Adınız) ve E-postanız dahil olmak üzere hesap bilgilerinizi görüntüler. Ayrıca **API Anahtarınızı** yönetebilir ve API kullanım ayrıntıları için Geliştirici Kontrol Paneline erişebilirsiniz. Parolayı Değiştir ve Hediye Kodunu Kullan gibi seçenekler Ayarlar altında mevcuttur.

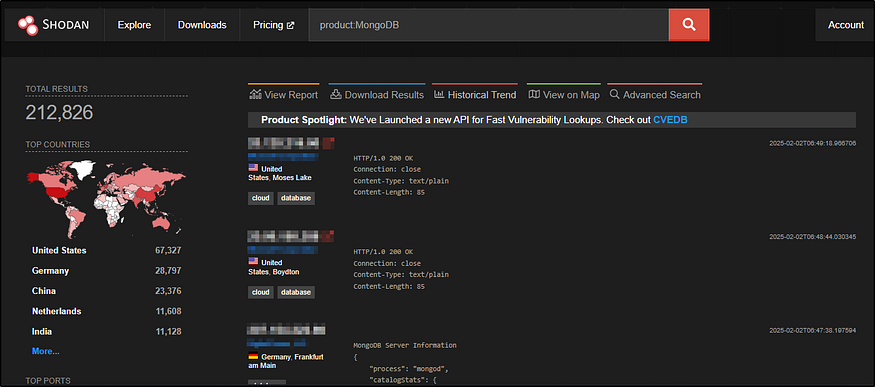


**Kategorilere Göre Bazı Aramalar**

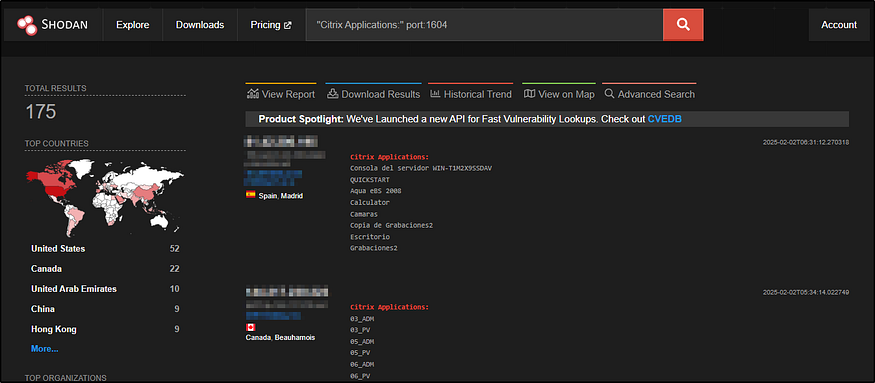
**1. port:5006,5007 ürün:mitsubishi [Endüstriyel Kontrol Sistemleri]**



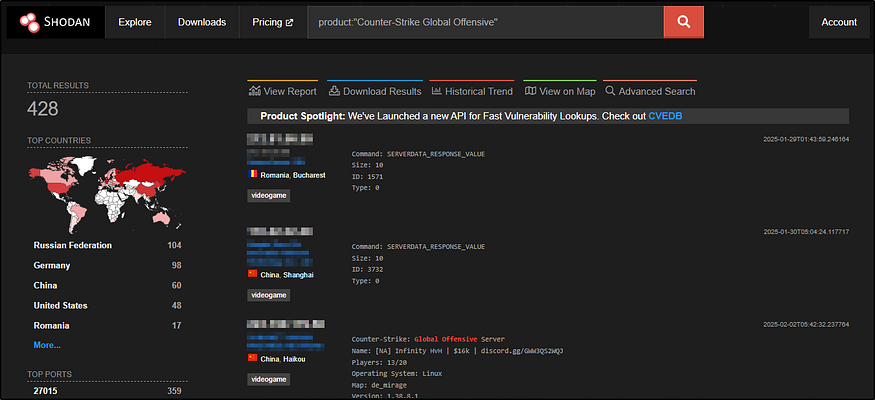
**2. ürün:MongoDB [Veritabanları]**



**3. "Citrix Uygulamaları:" port:1604 [Ağ Altyapısı]**



**4. ürün: “Counter-Strike Global Offensive” [Video Oyunları]**



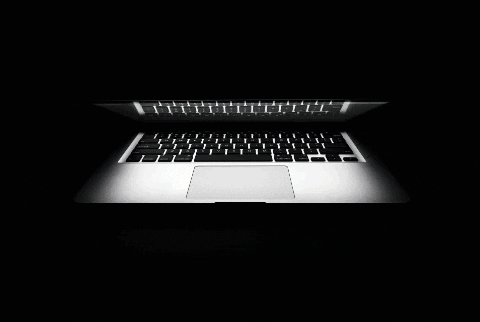
**Shodan kullanılarak bulunabilen cihazlar ve hizmetler**

Shodan, internete bağlı varlıklar hakkında derinlemesine bilgi toplama olanağı sunan, penetrasyon test uzmanları için vazgeçilmez bir araçtır. Bağlı cihazlardaki açık portları, işletim sistemlerini ve hizmetleri ortaya çıkararak olası güvenlik açıklarının ortaya çıkarılmasına yardımcı olabilir.



Shodan'ı kullanarak bulunabilecek bazı yaygın cihazlar ve hizmetler şunlardır:

1. **VoIP Telefonlar:** Bu cihazlar, yeterli güvenlik önlemleri alınmadığında saldırganların iletişimleri dinlemesine veya hatta yetkisiz ağ erişimi elde etmesine olanak tanıyabilir.
2. **RDP Hizmetleri:** Shodan, yanlış yapılandırılmış ve güvenlik riski oluşturabilecek açık Uzak Masaüstü Protokolü (RDP) hizmetlerini tespit edebilir.
3. **Endüstriyel Kontrol Sistemleri (ICS):** Üretim veya kamu hizmetleri gibi sektörlerde çalışan penetrasyon test uzmanları için PLC'ler (Programlanabilir Mantık Denetleyicileri) gibi ICS cihazlarındaki güvenlik açıklarını belirlemek hayati önem taşır.
4. **Yazıcılar:** Ağ yazıcıları bazen gözden kaçabilir, ancak önemli güvenlik riskleri oluşturabilirler. Ayrıca ağ içinde pivot noktaları olarak da kullanılabilirler.
5. **Açığa Çıkarılmış Veritabanları:** Shodan, MongoDB veya Elasticsearch gibi çevrimiçi olarak doğrudan erişilebilen ve düzgün bir şekilde güvence altına alınmadığı takdirde hassas verilerin sızdırılmasına neden olabilecek veritabanlarını tespit edebilir.
6. **Kameralar ve Web Kameraları:** Bu cihazlar uygun şekilde yapılandırılmazsa ciddi gizlilik riskleri oluşturabilirler. Bir sızma testinde bunların keşfedilmesi ve güvenliğinin sağlanması önemlidir.
7. **Akıllı Cihazlar:** Evlerde ve ofislerde giderek yaygınlaşan akıllı termostatlar, ışıklar ve buzdolapları gibi IoT cihazları genellikle güçlü bir güvenlikten yoksundur ve bu da onları penetrasyon test uzmanları için önemli bir hedef haline getirir.
8. **Sunucular:** Shodan kullanılarak web, e-posta, veritabanı, FTP, DNS ve diğer sunucu türleri bulunabilir ve bu sayede dikkat edilmesi gereken potansiyel güvenlik açıklarına daha derinlemesine bir bakış sağlanabilir.
9. **Yönlendiriciler ve Anahtarlar:** Bu kritik ağ cihazları Shodan tarafından tespit edilebilir ve açık portlar ve ilgili güvenlik açıkları hakkında bilgi ortaya çıkarılabilir.
10. **SMB Hizmetleri:** Shodan, uygun güvenlik yapılandırmaları veya kimlik doğrulama önlemlerinden yoksun olabilecek Sunucu İleti Bloğu (SMB) protokolünü kullanan cihazları tanımlamaya yardımcı olur.
11. **Güvenlik Duvarları ve IDS/IPS Cihazları:** Bir ağın savunma mekanizmalarını anlamak için güvenlik duvarlarını ve saldırı tespit/önleme sistemlerini analiz etmek önemlidir.
12. **Varsayılan Kimlik Bilgilerine Sahip Cihazlar:** Shodan, birçok internet bağlantılı cihazda görülen yaygın bir güvenlik açığı olan varsayılan kullanıcı adları ve parolaları kullanan cihazları vurgulayabilir.



**Özet**

**Penetrasyon Testi için Shodan: Kapsamlı ve Ayrıntılı** internete bağlı cihazları keşfetmek için güçlü bir arama motoru olan Shodan'ı tanıtıyor ve penetrasyon testlerinde keşif için olmazsa olmaz bir araç haline getiriyor. Shodan'ın çeşitli cihazlardan nasıl veri toplayıp indekslediğini açıklıyor. Kılavuz, temel arama sorgularını ve savunmasız sistemleri belirlemek için gelişmiş filtreleme tekniklerini kapsıyor. Etik kullanım ve pratik penetrasyon testi senaryoları da sonraki bölümlerde daha derinlemesine bir inceleme için temel olarak vurgulanıyor.