**WordPress Güvenliğinin Gözcüsü: WPScan Nedir ve Sitenizi Nasıl Korur?**

İnternetteki tüm web sitelerinin %40'ından fazlasına güç veren WordPress, şüphesiz dünyanın en popüler içerik yönetim sistemidir (CMS). Ancak bu popülerlik, onu aynı zamanda siber saldırganların da bir numaralı hedefi haline getiriyor. Eski bir eklenti, zayıf bir şifre veya yanlış bir yapılandırma, sitenizin kapılarını davetsiz misafirlere sonuna kadar açabilir. Peki, sitenizin güvenlik duvarındaki çatlakları bir saldırgan fark etmeden önce siz nasıl bulabilirsiniz? İşte bu sorunun cevabı, WordPress'e özel olarak geliştirilmiş en güçlü güvenlik tarayıcısı olan **WPScan**'de gizli.

Bu yazıda, WPScan'in ne olduğunu, neden her WordPress site sahibi veya güvenlik uzmanı tarafından kullanılması gerektiğini, nasıl kurulduğunu ve bu güçlü aracı kullanarak sitenizin güvenlik duruşunu nasıl analiz edebileceğinizi etkili örneklerle anlatacağız.

**1. WPScan Aracı Nedir?**

**WPScan**, yalnızca WordPress tabanlı web sitelerinin güvenliğini denetlemek için tasarlanmış, Ruby ile yazılmış, açık kaynaklı bir "kara kutu" zafiyet tarayıcısıdır. "Kara kutu" olması, sitenin kaynak koduna veya sunucuya erişimi olmadan, dışarıdan bir ziyaretçi gibi davranarak testleri gerçekleştirdiği anlamına gelir.

WPScan, hedef bir WordPress sitesini analiz ederek aşağıdaki gibi kritik bilgileri ve potansiyel zafiyetleri ortaya çıkarır:

* **WordPress Sürümü:** Sitenin hangi WordPress sürümünü kullandığını tespit eder ve bu sürümle ilişkili bilinen güvenlik açıklarını listeler.
* **Eklentiler (Plugins):** Sitede yüklü olan eklentileri ve sürümlerini bulmaya çalışır. Bilinen zafiyetlere sahip eklentiler en yaygın saldırı vektörlerinden biridir.
* **Temalar (Themes):** Aktif olan temayı ve sürümünü tespit ederek bu temayla ilgili güvenlik açıklarını kontrol eder.
* **Kullanıcı Listeleme (User Enumeration):** Sitedeki kayıtlı kullanıcı adlarını (admin, editor vb.) ortaya çıkarmaya çalışır. Bu, kaba kuvvet (brute-force) saldırıları için ilk adımdır.
* **Yapılandırma Hataları:** wp-config.php yedek dosyası gibi hassas dosyaların erişilebilir olup olmadığını veya dizin listelemenin açık olup olmadığını kontrol eder.
* **Zayıf Şifre Kontrolü:** Belirtilen kullanıcı adlarına karşı bir kelime listesi (wordlist) kullanarak kaba kuvvet saldırısı gerçekleştirebilir.

**2. Neden Kullanılır?**

WPScan, hem site sahipleri (defansif) hem de etik hacker'lar (ofansif) için vazgeçilmez bir araçtır:

* **Proaktif Güvenlik Denetimi:** Site sahipleri, kendi sitelerini düzenli olarak tarayarak bir saldırganın kullanabileceği zafiyetleri önceden tespit edip düzeltebilirler.
* **Saldırı Yüzeyini Anlama:** Sızma testi uzmanları, bir WordPress sitesine yönelik testlere başlamadan önce WPScan ile sitenin genel yapısını, kullanılan bileşenleri ve bariz zafiyetleri hızlıca anlarlar.
* **Bileşen Güvenliği:** Sitenizin kullandığı bir eklenti veya temada yeni bir zafiyet çıktığında anında haberdar olmanızı sağlar.
* **Kullanıcı Güvenliği:** Zayıf şifreye sahip kullanıcı hesaplarını tespit ederek olası bir hesap ele geçirme senaryosunun önüne geçmenize yardımcı olur.
* **Otomasyon:** Sürekli ve düzenli güvenlik taramalarını otomatikleştirmek için kullanılabilir.

**3. Nasıl Kurulum Yapılır?**

WPScan'i kurmanın birkaç yolu vardır. Ruby tabanlı olduğu için sisteminizde Ruby'nin kurulu olması gerekir.

**Yöntem 1: Gem ile Kurulum (Ruby'nin Paket Yöneticisi)**

Bu en yaygın ve önerilen yöntemdir.

# Gerekli bağımlılıkları kurun (Debian/Ubuntu için)

sudo apt-get install build-essential libcurl4-openssl-dev libxml2 libxml2-dev libxslt1-dev ruby-dev

# WPScan gem'ini kurun

sudo gem install wpscan

**Yöntem 2: Kali Linux (Zaten Kurulu Gelir)**

Eğer Kali Linux kullanıyorsanız, şanslısınız! WPScan genellikle sisteme önceden yüklenmiş olarak gelir. Sadece wpscan komutunu çalıştırmanız yeterlidir.

**Yöntem 3: Docker ile Kurulum**

Sisteminize Ruby ve bağımlılıklarını kurmak istemiyorsanız, Docker en temiz çözümdür.

docker pull wpscanteam/wpscan

# Kullanım: docker run -it --rm wpscanteam/wpscan --url https://hedefsite.com

**API Anahtarı:** WPScan'in zafiyet veritabanını tam olarak kullanabilmesi için [WPScan.com](https://www.google.com/url?sa=E&q=https%3A%2F%2Fwpscan.com%2F) adresinden ücretsiz bir API anahtarı almanız ve wpscan --update komutuyla veya tarama komutuna --api-token parametresi ekleyerek kullanmanız şiddetle tavsiye edilir.

**4. Kullanım Parametreleri Nedir?**

WPScan'in gücü, taramalarınızı detaylandırmanızı sağlayan parametrelerinde yatar.

* --url: Taranacak WordPress sitesinin URL'si. Bu temel parametredir.
* --enumerate: Nelerin listeleneceğini belirtir. Seçenekler:
  + u: Kullanıcı adlarını listeler.
  + p: Popüler eklentileri listeler.
  + vp: Sadece zafiyetli eklentileri listeler (API anahtarı gerektirir).
  + t: Popüler temaları listeler.
  + vt: Sadece zafiyetli temaları listeler (API anahtarı gerektirir).
* --passwords veya -P: Belirtilen kelime listesi dosyası ile kaba kuvvet (brute-force) saldırısı yapar.
* --usernames veya -U: Kaba kuvvet saldırısı için hedef kullanıcı ad(lar)ını belirtir.
* --api-token: WPScan.com'dan aldığınız API anahtarını belirtir.
* --random-user-agent veya -r: Her istekte farklı bir User-Agent kullanarak basit WAF'ları atlatmaya çalışır.
* --detection-mode: Taramanın ne kadar "agresif" olacağını belirler (passive, mixed, aggressive).
* -o veya --output: Tarama sonuçlarını belirtilen dosyaya kaydeder.
* -f veya --format: Çıktı formatını belirtir (cli, json, html vb.).

**5. Etkili Kullanım İçin 5 Örnek ve Açıklamaları**

Şimdi WPScan'i pratik senaryolarla nasıl kullanacağımıza bakalım.

**Örnek 1: Temel ve Kapsamlı Zafiyet Taraması (API ile)**

Bu, bir site hakkında genel bir güvenlik değerlendirmesi yapmak için en iyi başlangıç noktasıdır.

wpscan --url https://hedefsite.com --api-token YOUR\_API\_TOKEN --enumerate vp,vt

* **Açıklama:** Bu komut, hedefsite.com adresini tarar. --api-token sayesinde en güncel zafiyet veritabanını kullanır. --enumerate vp,vt parametreleri ile sadece **bilinen bir zafiyeti olan** eklentileri ve temaları bulmaya odaklanır. Bu, çıktıyı temiz tutar ve doğrudan aksiyon alınması gereken noktalara işaret eder.

**Örnek 2: Kullanıcıları Keşfetme**

Bir saldırganın ilk adımı, geçerli kullanıcı adlarını bulmaktır.

wpscan --url https://hedefsite.com --enumerate u

* **Açıklama:** --enumerate u parametresi, WPScan'e 1'den 10'a kadar olan yazar ID'lerini (/?author=1, /?author=2 vb.) deneyerek kullanıcı adlarını ortaya çıkarmasını söyler. Eğer başarılı olursa, admin, editor gibi kullanıcı adlarını listeleyecektir. Bu, sitenizde kullanıcı adı sızdırma zafiyeti olup olmadığını gösterir.

**Örnek 3: Zayıf Şifreleri Test Etme (Brute-Force Saldırısı)**

Kullanıcı adlarını bulduktan sonraki adım, şifreleri tahmin etmektir.

wpscan --url https://hedefsite.com -U admin,editor -P /usr/share/wordlists/rockyou.txt

* **Açıklama:**
  + -U admin,editor: Saldırının sadece admin ve editor kullanıcılarına yönelik olacağını belirtir.
  + -P /usr/share/wordlists/rockyou.txt: Şifre denemeleri için rockyou.txt gibi yaygın bir kelime listesini kullanır. Eğer bu kullanıcılardan birinin şifresi bu listede yer alıyorsa, WPScan şifreyi bulacak ve raporlayacaktır. **Bu testi sadece izinli sistemlerde yapın!**

**Örnek 4: Agresif Eklenti Tespiti ve Raporlama**

Bazen eklentiler gizlenir. Agresif mod, daha fazla eklenti bulmaya çalışır.

wpscan --url https://hedefsite.com --plugins-detection aggressive --enumerate p -f json -o wpscan\_report.json

* **Açıklama:**
  + --plugins-detection aggressive: WPScan'in eklentileri bulmak için daha fazla yöntem (pasif taramanın yanı sıra sitenin HTML'ini analiz etme gibi) kullanmasını sağlar.
  + --enumerate p: Tüm popüler eklentileri tarar.
  + -f json -o wpscan\_report.json: Sonuçları, başka araçlarla işlenmesi veya raporlama sistemlerine entegre edilmesi kolay olan JSON formatında bir dosyaya kaydeder.

**Örnek 5: Tespit Edilmekten Kaçınmaya Çalışarak Tarama**

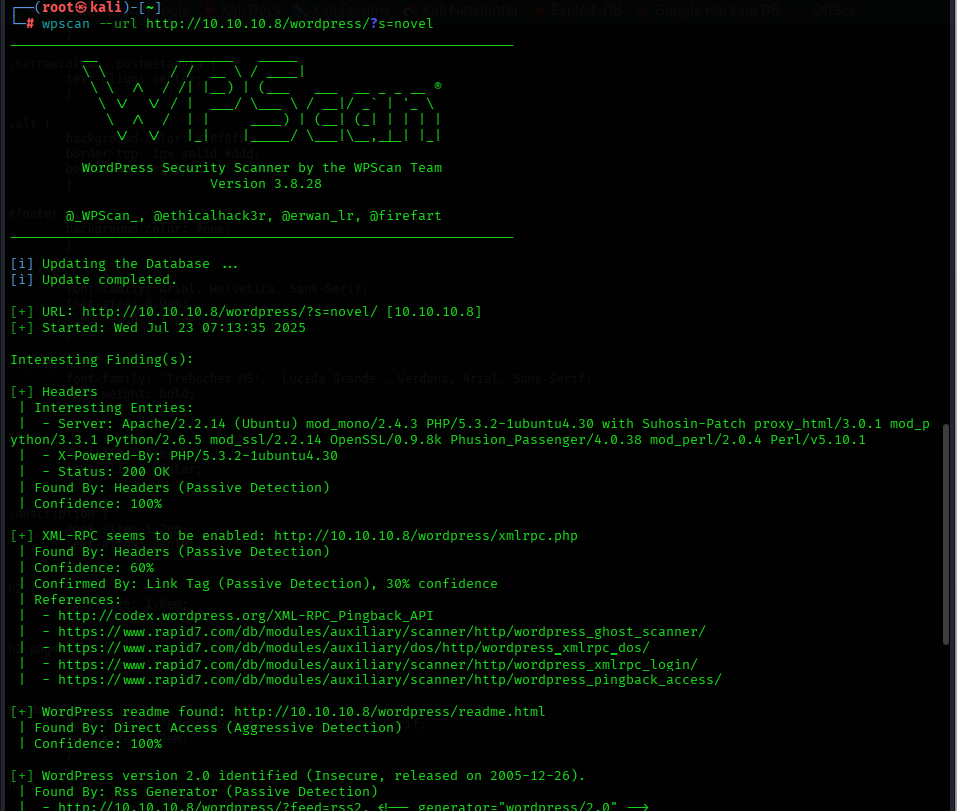
Bazı güvenlik duvarları (WAF), WPScan'in standart taramalarını engelleyebilir.

wpscan --url https://hedefsite.com --random-user-agent --detection-mode passive

* **Açıklama:**
  + --random-user-agent: Her istekte farklı bir tarayıcı kimliği göndererek "WPScan tarayıcısı" olarak etiketlenmeyi zorlaştırır.
  + --detection-mode passive: Sadece sitenin ana sayfasını ve robots.txt gibi dosyaları analiz ederek, aktif olarak siteye istek göndermeden bilgi toplamaya çalışır. Bu, daha "sessiz" bir tarama yöntemidir ancak daha az bilgi sağlar.

**🔐 Örnek: WPScan ile WordPress Güvenlik Analizi**

**WPScan**, WordPress tabanlı web sitelerinde güvenlik zafiyetlerini taramak ve yapılandırma açıklarını tespit etmek için kullanılan güçlü bir açık kaynak araçtır. Aşağıdaki örnekte, http://10.10.10.8/wordpress/ adresine karşı gerçekleştirilen bir WPScan taraması yer almaktadır.

  
wpscan --url http://10.10.10.8/wordpress/?s=novel komutu ile hedef URL'e yönelik bir tarama başlatılmıştır. Tarama sonucu şu önemli bulguları içermektedir:

* **Sunucu Bilgileri:** Apache/2.2.14, PHP 5.3.2 gibi bileşenler kullanıldığı tespit edilmiştir. Bu sürümler eski ve güvenlik zafiyetlerine açık olabilir.
* **XML-RPC Açıklığı:** xmlrpc.php dosyasının erişilebilir olduğu belirlenmiştir. Bu dosya brute force, pingback DDoS gibi saldırılar için kötüye kullanılabilir.
* **readme.html Dosyası:** WordPress’in varsayılan readme.html dosyasına erişim mümkündür. Bu dosya, versiyon bilgisi sızdırabilir ve saldırganların zafiyet hedeflemesine yardımcı olur.
* **WordPress Versiyonu:** 2.0 sürümünün yüklü olduğu tespit edilmiştir. Bu sürüm oldukça eski olup birçok bilinen güvenlik açığı içermektedir.

Tespit edilen veriler WPScan’in **pasif** (header analizi) ve **aktif** (doğrudan erişim) modülleriyle elde edilmiştir. Her bulguya ilişkin referans bağlantıları da WPScan tarafından otomatik olarak sağlanmıştır. Bu tür analizler, hedef sistemin savunmasız noktalarını tespit etmede kritik rol oynar.

**Sonuç**

WPScan, WordPress ekosisteminin vazgeçilmez bir güvenlik aracıdır. İster kendi sitenizi korumaya çalışan bir site sahibi, ister müşterilerinin sitelerini denetleyen bir ajans, isterse etik sınırlar içinde zafiyet arayan bir güvenlik araştırmacısı olun, WPScan size paha biçilmez bilgiler sunar. Popülerliğin getirdiği riskleri yönetmenin en iyi yolu, proaktif olmaktır. WPScan'i düzenli olarak kullanarak, sitenizin güvenlik duruşunu bir adım önde tutabilir ve potansiyel tehditlere karşı dijital kalenizi sağlamlaştırabilirsiniz.

Unutmayın, bu araç güçlü olduğu kadar sorumluluk da gerektirir. WPScan'i **sadece kendi sitenizde veya test etme izniniz olan sistemlerde** kullanarak, interneti herkes için daha güvenli bir yer haline getirmeye yardımcı olabilirsiniz.