**W3af Nedir?**

Siber güvenlik alanında sıkça kullanılan araçlardan biri olan **W3af**, “Web Application Attack and Audit Framework” (Web Uygulama Saldırı ve Denetim Çatısı) ifadesinin kısaltmasıdır.

Basitçe anlatmak gerekirse, W3af bir web sitesini test ederek orada bulunabilecek zafiyetleri (güvenlik açıklarını) tespit etmeye yarayan bir yazılımdır. Özellikle web uygulamalarında görülen zafiyet türlerine odaklanır. Bu sayede siber güvenlik uzmanları, bir siteyi saldırganlardan önce tarayıp zayıf noktaları belirleyebilir.

**Unutma:** W3af bir “etik hacker” aracıdır. Yani kötü amaçla değil, sistemleri daha güvenli hale getirmek için kullanılır.

**W3af Nasıl İndirilir/Yüklenir?**

W3af hem **grafiksel arayüz (GUI)** hem de **komut satırı (CLI)** üzerinden çalışabilir. Genellikle Linux sistemlerde kullanılır ve Kali Linux gibi siber güvenlik dağıtımlarında ön yüklü gelir.

W3af’ı Yüklemek için komut;

***sudo apt update***

***sudo apt install w3af***

**W3af ile Neler Yapılabilir?**

W3af, bir web sitesine saldırmak yerine onu analiz ederek güvenlik açıklarını raporlayan bir araçtır. İşte W3af ile yapabileceklerin:

* SQL Injection, XSS gibi yaygın web zafiyetlerini tespit edebilirsin.
* Otomatik olarak hedef siteyi tarayıp zayıflıkları bulabilir.
* Raporlama özelliğiyle zafiyetleri düzenli şekilde çıktı olarak sunabilir.
* Kendi modüllerini seçip özel taramalar yapabilirsin.

W3af, içinde yüzlerce “plugin” barındırır. Bu plugin’ler farklı test türlerini gerçekleştirir. Örneğin auth plugin’i kimlik doğrulama açıklarını tarar.

**W3af Kullanımı (Temel Adımlar)**

İster grafik arayüzü ister terminali kullanın; ikisinde de temel adımlar şunlardır:

1. **Hedef Siteyi Belirle:**

***target set target*** [***http://hedefsite.com***](http://hedefsite.com)

1. **Kullanılacak Modülleri Ayarla:**

***plugins***

***output console,text\_file***

***audit xss,sqli***

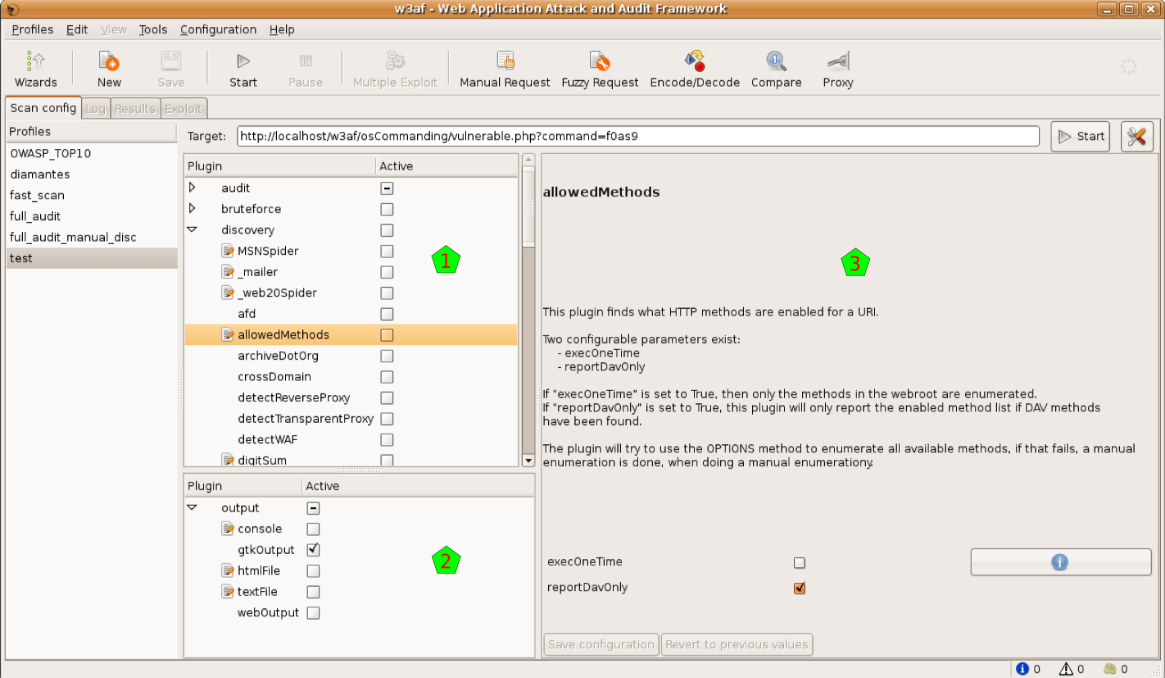
***crawl web\_spider***

***back***

1. **Taramayı Başlat:**

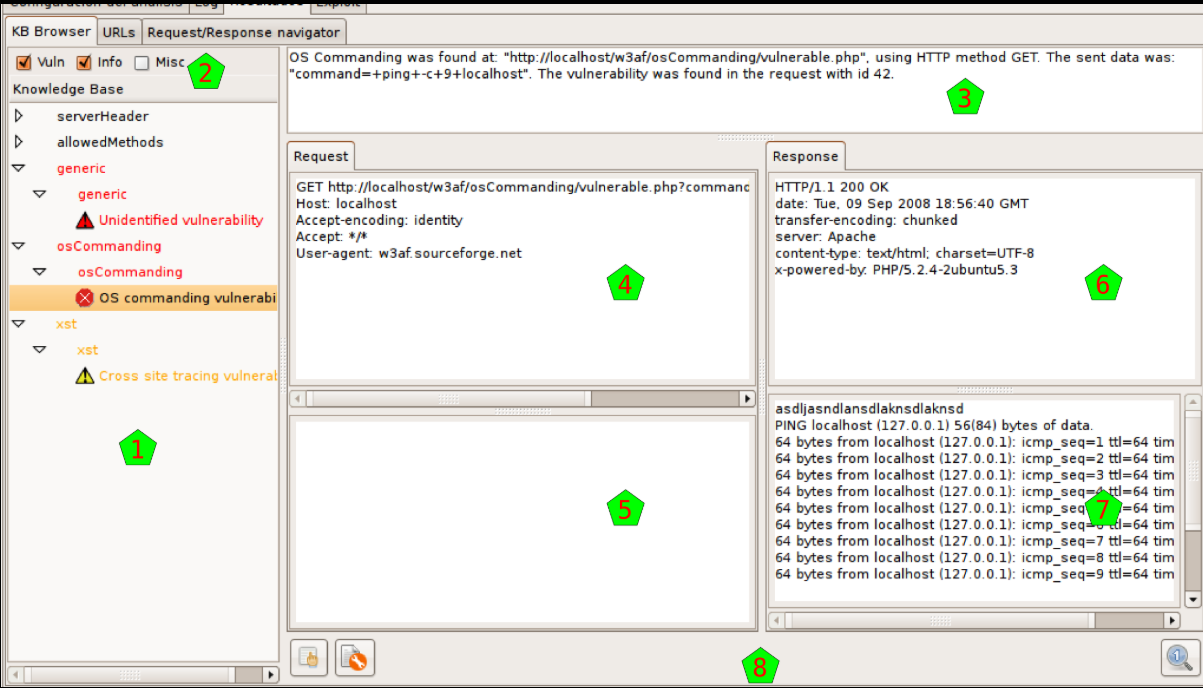
Start

Tarama Başladıktan Sonra Ekran Görünümü:



**4. Raporları Görüntüle:**

Tarama tamamlandıktan sonra bulunan zafiyetler rapor olarak gösterilir.



**W3af Tarayıcı Modülleri**

W3af içinde 3 ana modül bulunur:

* **Discovery (Keşif):** Web sitesindeki sayfaları ve parametreleri bulur.
* **Audit (Denetim):** Zafiyet testleri yapılır. Örn: SQLi, XSS.
* **Attack (Saldırı):** Denetimde bulunan açıklar sömürülür (genelde test amaçlı).

Her adımın kendine özel alt plugin’leri vardır. Örneğin:

* **crawl web\_spider → Sayfaları otomatik gezer**
* **audit sqli → SQL injection açıklarını tarar**

Öğrenciler İçin Tavsiyeler

* **Pratik yap:** W3af’ı kurduktan sonra sanal bir hedef sistem (örneğin: DVWA, Juice Shop) üzerinde deneme yap.
* **Zararsız testler yap:** Gerçek siteleri taramak yerine test amaçlı ortamlar kur (etik kurallara uy!).
* **Plugin listesini keşfet:** plugins yazarak aktif modülleri gör ve hangi testlerin yapılabileceğini öğren.
* **Sadece öğrenme amaçlı kullan:** W3af gibi araçları yalnızca iznin olan sistemlerde kullan. Aksi durumda hukuki sorunlar doğabilir.
* W3af, web uygulamalarını test etmek için kullanılan açık kaynak kodlu güçlü bir araçtır. Özellikle etik hacker’ların eğitim sürecinde sıkça kullandığı bu yazılım, bir siteyi derinlemesine analiz etme imkânı sunar. Diğer güvenlik araçlarıyla (Burp Suite, Nikto, ZAP) birlikte kullanıldığında oldukça etkili sonuçlar elde edebilirsin.