## Webponized Nedir, Neden Kullanılır?

Webponized, PHP diliyle yazılmış, kullanımı oldukça kolay ve etkili bir **web shell** aracıdır. Sızma testleri veya CTF (Capture The Flag) senaryolarında, hedef sistem üzerinde uzaktan komut çalıştırma ihtiyacı doğduğunda devreye girer. Özellikle dosya yükleme zafiyeti olan sistemlerde, saldırganın hedef sunucuda kalıcı veya geçici bir terminal elde etmesini sağlar.

Webponized’in temel amacı, web tabanlı bir terminal ortamı sunmaktır. Grafiksel arayüzü sayesinde, yalnızca terminal komutu değil; dosya yönetimi, sistem bilgisi görüntüleme, dosya yükleme ve indirme gibi birçok işlemi tek ekrandan yapmanıza olanak tanır.

Bir sızma testi uzmanı için Webponized, istismar (exploit) sonrası aşamada hedef sistemle etkileşimi sürdürebilmek ve sistem kaynaklarını keşfedebilmek adına oldukça pratik bir çözümdür. Aynı zamanda shell üzerinden özel betikler çalıştırılabilir, geri bağlantı (reverse shell) veya daha gelişmiş sızma yolları da planlanabilir.

## Kurulum

Webponized’in en büyük avantajı, klasik anlamda bir kurulum gerektirmemesidir. Sadece bir .php dosyası olarak çalışır. Bu dosyayı edinip hedef web sunucusuna yüklemeniz yeterlidir. Yükleme yöntemleri şunlar olabilir:

* Dosya yükleme (file upload) zafiyetinden yararlanmak
* Komut enjeksiyonu ile wget, curl veya echo komutları kullanarak dosyayı yazdırmak
* LFI (Local File Inclusion) zafiyeti üzerinden betiği tetiklemek
* Daha önce ele geçirilmiş başka bir shell veya yönetici paneli üzerinden yerleştirmek

PHP dosyası sunucuda uygun bir dizine yüklendikten sonra, tarayıcı üzerinden http://hedefsite.com/uploads/webponized.php gibi bir bağlantı ile erişim sağlanabilir.

**Kullanım Örneği**

Webponized’e erişim sağladığınızda, sizi sade ama işlevsel bir arayüz karşılar. Bu arayüzde birkaç ana bileşen bulunur:

* Komut satırı (command interface)
* Dosya yöneticisi (file browser)
* Sistem bilgisi (system info)
* Dosya yükleme alanı (file upload)

Örneğin, “uname -a” komutunu girerek hedef sistemin çekirdek sürümünü öğrenebilir, “ls -la” komutuyla dizin içeriğini görebilir veya “cat /etc/passwd” gibi işlemlerle hassas bilgileri analiz edebilirsiniz. Arayüzdeki form alanına girilen komutlar, arka planda PHP’nin shell\_exec() veya system() fonksiyonları ile yürütülür ve çıktı aynı sayfa üzerinde görüntülenir.

Ayrıca dosya yöneticisi sayesinde, sunucu üzerinde klasörler arasında gezebilir, dosya silebilir, yeniden adlandırabilir ve kendi makinenizden dosya yükleyebilirsiniz.

## Elde Edilebilecek Bilgilerden ve Yetkilerden Örnekler

Webponized üzerinden alınan shell ile aşağıdaki bilgilere erişilebilir:

* whoami komutu ile mevcut kullanıcı öğrenilebilir.
* hostname, uname -a gibi komutlarla sistemin işletim sistemi ve çekirdek bilgileri alınabilir.
* ps aux, netstat -tulpn gibi komutlarla çalışan servisler, açık portlar ve bağlantılar listelenebilir.
* cat /var/www/html/config.php gibi komutlarla web uygulamalarının yapılandırma dosyaları incelenebilir.
* mysql -u root -p gibi veritabanı bağlantıları test edilebilir.
* wget, curl, nc gibi araçlar varsa reverse shell başlatılabilir veya ek payloadlar indirilebilir.

Bu bilgiler ve kontroller, saldırganın sistemde kalıcılık elde etmesine ya da privilege escalation gibi daha derinlemesine adımlar atmasına olanak tanır.

## Kullanılabilecek Özellikler ve Güçlü Yanları

Webponized sadece bir komut çalıştırma paneli değildir. Aşağıda sunduğu başlıca yetenekler sıralanmıştır:

* **Komut yürütme**: Tüm temel Unix/Linux komutları desteklenir. PHP’nin komut çalıştırma fonksiyonları üzerinden işlem yapılır.
* **Dosya yönetimi**: Dosya listeleme, silme, taşıma, yükleme ve indirme işlemleri arayüz üzerinden yapılabilir.
* **Sistem keşfi**: Kullanıcı, hostname, PHP sürümü, çalışma dizini gibi bilgiler sayfa üzerinde anlık görüntülenir.
* **Upload özelliği**: Yeni shell'ler, reverse shell betikleri veya keylogger gibi ekstra bileşenler kolayca yüklenebilir.
* **Kolay gizlenebilirlik**: Kod yapısı sade olduğundan, antivirüs ve WAF sistemleri tarafından algılanması daha zordur.
* **Taşınabilirlik**: Tek bir PHP dosyasıyla çalıştığı için, her sunucuya uyumlu ve kurulumu hızlıdır.

Webponized, sade yapısı ama geniş etkisiyle, sızma testlerinde hedef sistem üzerinde kalıcı kontrol sağlamak için oldukça etkili bir araçtır.