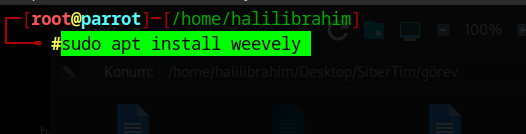
## Weevely Nedir, Neden Kullanılır?

Weevely, uzak bir sistemde PHP tabanlı gizli bir terminal (web shell) oluşturmak ve bu terminal üzerinden komut yürütmek için kullanılan açık kaynaklı bir araçtır. Özellikle sızma testleri sırasında, web sunucusunda komut çalıştırma (RCE) açığı tespit edildiğinde kullanılabilir. Hafif ve gizlenmesi kolay bir yapıya sahiptir.

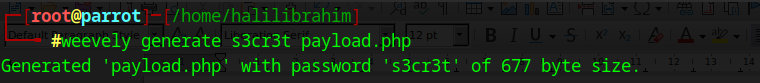
Weevely’nin en büyük avantajlarından biri, oluşturduğu PHP arka kapı dosyasının basit ve zararsız gibi görünmesidir. Böylece WAF (Web Application Firewall) gibi güvenlik önlemlerini aşmak için ideal bir çözümdür. Penetrasyon testlerinde, istismar sonrası aşamada hedef sistemle etkileşim kurmak için yaygın olarak tercih edilir.

Weevely genellikle Kali Linux gibi dağıtımlarla yüklü gelir. Ancak manuel olarak kurmak isterseniz aşağıdaki komutu terminale girmeniz yeterlidir:



**Kullanım Örneği**

İlk olarak, hedef sisteme yüklenmek üzere bir PHP arka kapı dosyası (agent) oluşturmamız gerekir:



Bu komutla s3cr3t parolası ile şifrelenmiş payload.php adlı bir dosya oluşturulur. Bu dosya hedef sunucunun herhangi bir yerine yüklendikten sonra, onun üzerinden komut çalıştırılabilir.

Bağlantı kurmak için:

weevely http://hedefsite.com/uploads/payload.php s3cr3t komutunu gireriz.

Bu komut çalıştırıldığında, terminal ekranı üzerinden uzak sunucuda komut çalıştırma kabiliyetine sahip bir kabuk (shell) elde edilir.

## Elde Edilebilecek Bilgilerden Örnekler

Bağlantı sağlandıktan sonra aşağıdaki işlemler yapılabilir:

* ls, cat, pwd gibi komutlarla dosya sistemi gezilebilir.
* ps, whoami, uname -a gibi sistem komutları çalıştırılabilir.
* MySQL bağlantıları denenebilir, config dosyaları okunabilir.
* Gerekirse başka zararlı yazılımlar yüklenerek privilege escalation (yetki yükseltme) denenebilir.

## Kullanılabilecek Bazı Komutlar ve Özellikler

Weevely, yalnızca kabuk erişimi sağlamaz. İçerisinde yerleşik olarak gelen modüller sayesinde çeşitli görevleri yerine getirebilir:

* system\_info: Hedef sistemin işletim sistemi, çekirdek ve kullanıcı bilgilerini listeler.
* file\_download ve file\_upload: Hedef sistemden dosya indirme veya yükleme yapılabilir.
* shell: Tam bir interaktif kabuk elde edilir.
* audit\_sql: SQL bağlantı bilgilerini keşfetmeye çalışır.
* backdoor: Yeni arka kapılar bırakmak için ek scriptler çalıştırabilir.

Bu komutlar ile sızma testi sırasında elde edilen erişim seviyesi daha etkili şekilde kullanılabilir.