# WSO (Web Shell by Orb)

WSO Shell (Web Shell by Orb), PHP tabanlı gelişmiş bir web shell aracıdır. Saldırganlar tarafından genellikle arka kapı (backdoor) olarak web sunucularına yerleştirilir. Gelişmiş dosya yöneticisi, komut yürütme, bağlantı tünelleme ve veritabanı yönetimi gibi işlevlere sahiptir. WSO Shell, şifre korumalı arayüzü sayesinde gizli çalışabilir ve kullanıcı dostu bir panel sunar.

# Bu aracın özellikleri nelerdir?

- PHP tabanlı ve tek dosyalık yapıya sahiptir.

- Gelişmiş dosya yöneticisi (yükleme, silme, CHMOD ayarı).

- Terminal benzeri komut yürütme paneli (RCE).

- MySQL veritabanı yönetimi.

- PHP kod yürütme paneli.

- Arayüz şifre koruması (şifreli oturum).

- Back-connect (ters bağlantı) desteği.

- Shell renklendirme ve gizleme seçenekleri.

# WSO Shell Nasıl Oluşturulur ve Kullanılır?

**Adım 1:** WSO Shell açık kaynaklıdır ve genellikle GitHub gibi platformlarda bulunur. Örnek bir WSO Shell içeriği aşağıdaki gibi olabilir:  
  
<?php /\* WSO Shell Başlangıcı \*/ eval(base64\_decode('...')); ?>  
  
**Adım 2:** Bu kodu shell.php gibi bir dosyaya kaydedin.

**Adım 3:** shell.php dosyasını hedef web sunucusuna yükleyin. Yükleme için:  
- Zafiyetli dosya yükleme formu  
- FTP erişimi  
- RFI veya LFI istismarları kullanılabilir.

# WSO Shell Kullanımı (Tarayıcı Üzerinden)

**Adım 1:** Tarayıcıdan shell adresine gidin:  
  
http://hedef.com/shell.php

**Adım 2:** Şifre korumalı giriş ekranı açılır. (Varsayılan şifre yoktur, shell'e gömülüdür.)

**Adım 3:** Giriş yaptıktan sonra aşağıdaki işlemler yapılabilir:  
- Komut yürütme (id, whoami, uname -a)  
- Dosya yönetimi (yeni dosya, silme, chmod)  
- Reverse shell başlatma  
- MySQL bağlantısı üzerinden veri çekme

# Shelli Komut Satırı (CLI) ile Test Etme

WSO Shell'e komut göndermek yerine yüklemenin başarılı olup olmadığını kontrol etmek için şunu kullanabilirsiniz:  
  
curl http://hedef.com/shell.php

# Önlem Yöntemleri

- Sunucuya yüklenen PHP dosyalarını düzenli tarayın.

- Dosya yükleme işlemlerinde MIME türü ve uzantı kontrollerini sıkılaştırın.

- WAF (Web Application Firewall) kullanarak shell imzalarını engelleyin.

- Sunucu dosya sistemine yazma izinlerini sınırlandırın.

- Sunucu loglarını düzenli olarak inceleyin.

- Şüpheli dosyaları tespit eden antivirüs yazılımları kullanın.