# Exploit-DB (SearchSploit) – Açıklama ve Kullanım Rehberi

## Exploit-DB Nedir?

Exploit-DB, güvenlik açıkları ve istismar kodlarını (exploit) içeren açık kaynaklı bir veritabanıdır. Offensive Security tarafından yönetilen bu platform, araştırmacıların ve güvenlik profesyonellerinin zafiyetleri keşfetmesine, test etmesine olanak sağlar. Web tabanlı erişiminin yanı sıra komut satırı aracı olan SearchSploit ile de kullanılabilir.

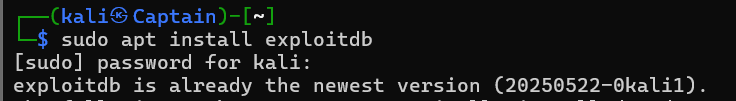
## SearchSploit Nedir?

SearchSploit, Exploit-DB arşivine komut satırından erişim sağlayan bir araçtır. İnternete ihtiyaç duymadan, yerel olarak exploit araması yapmanıza olanak tanır. Bu sayede pentest yapanlar veya offline çalışan araştırmacılar için idealdir.

## Kurulum

Aşağıdaki komutlar ile kurulum yapabilirsiniz:

sudo apt update  
sudo apt install exploitdb



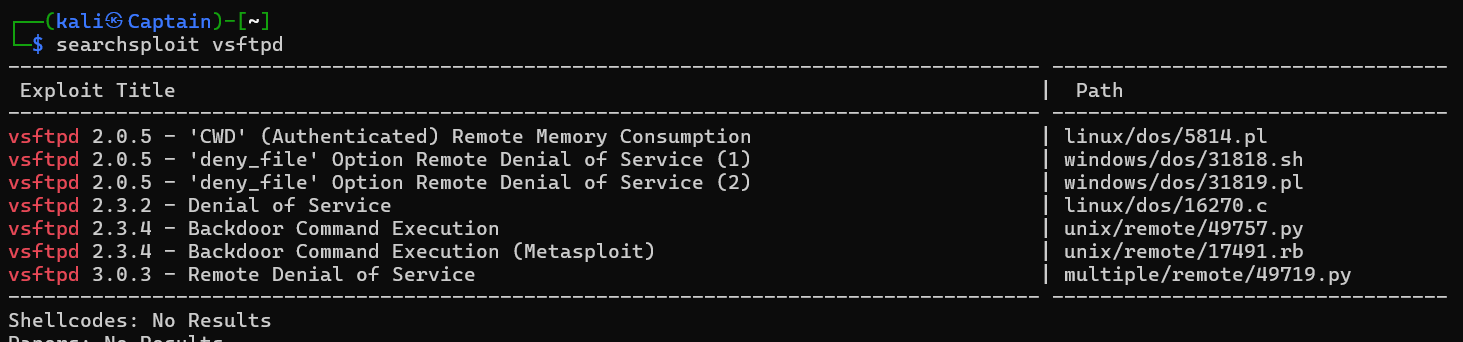
Ya da manuel kurulum:

git clone https://github.com/offensive-security/exploitdb.git /opt/exploitdb

## Temel Kullanım Örnekleri

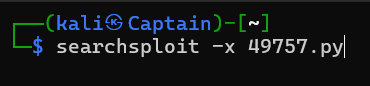
**1. Belirli bir yazılımda açık arama (örnek: vsftpd):**

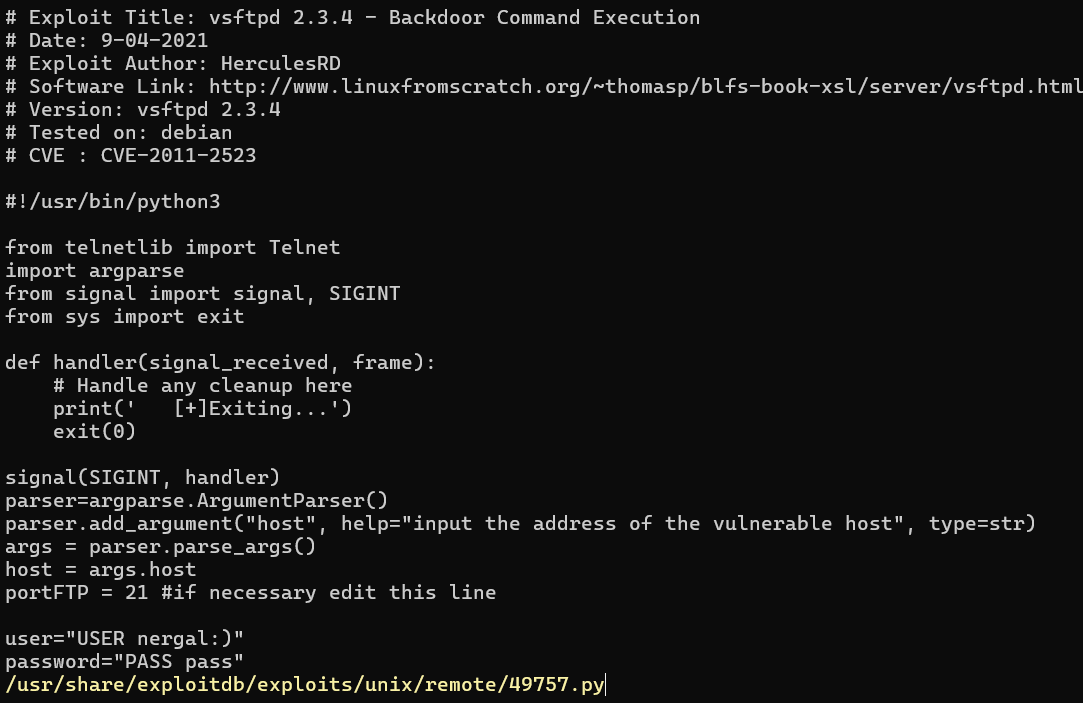
searchsploit vsftpd



**2. Exploit hakkında detayları görüntüleme:**

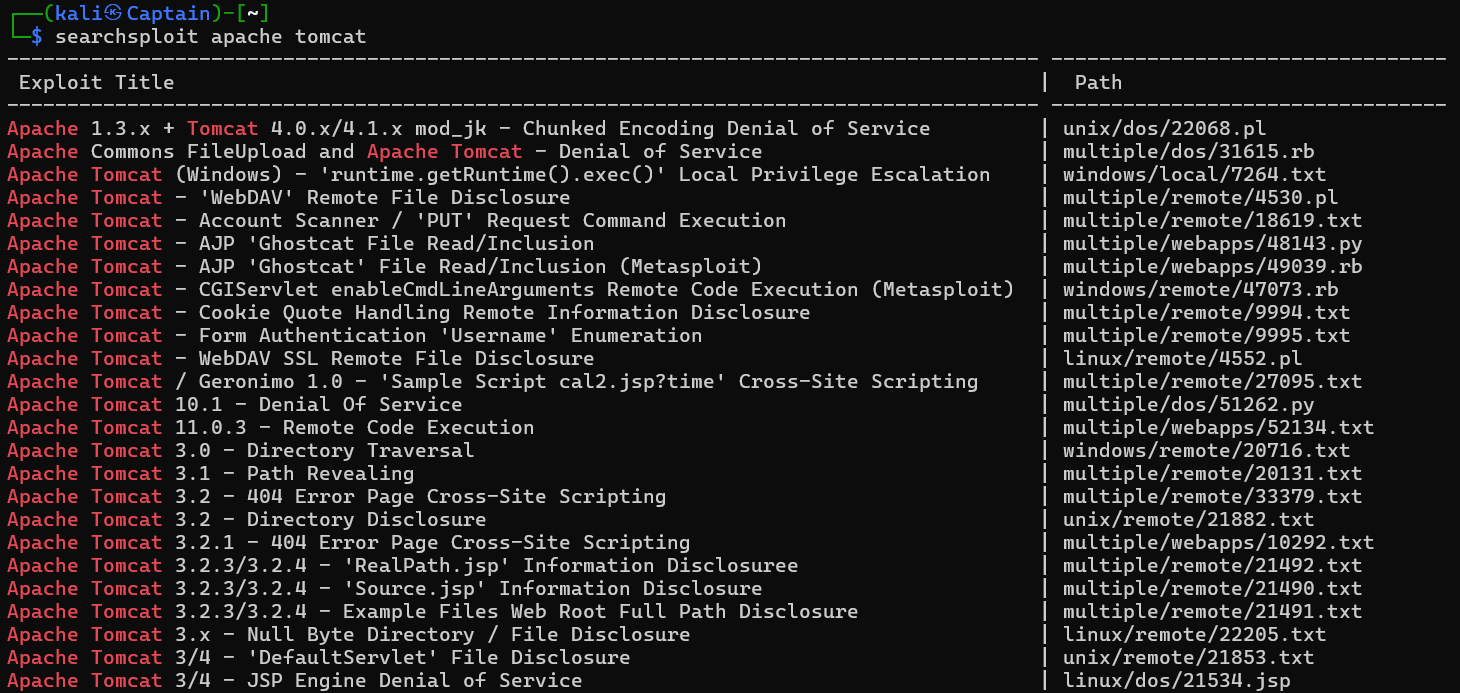
searchsploit -x 49757.py





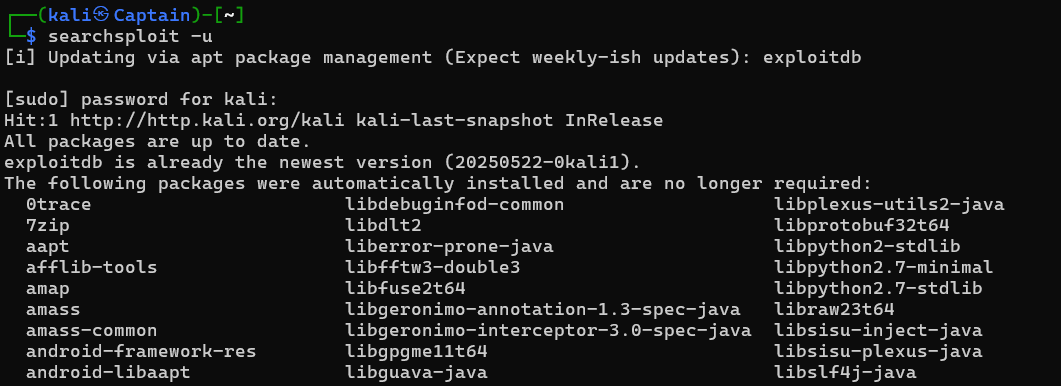
**3. Anahtar kelimelerle arama yapma:**

searchsploit apache tomcat



4. Güncellemeleri alma:

searchsploit –u



Bu komut ile Exploit-DB veritabanınızı güncel tutabilirsiniz.

## Exploit Dosyaları Nerede?

Exploit dosyaları genellikle şu dizinde yer alır:  
/usr/share/exploitdb/exploits/

Alternatif olarak, **~/.searchsploit\_rc** dosyasından yol yapılandırmasını kontrol edebilirsiniz.

## Kullanım Alanları

- Pentest / Red Team testlerinde hedef sistemdeki zafiyetleri kontrol etmek.

- Eğitim veya laboratuvar ortamlarında zafiyet sömürme senaryoları oluşturmak.

- CVE numaralarına karşılık gelen exploitleri hızlıca bulmak.