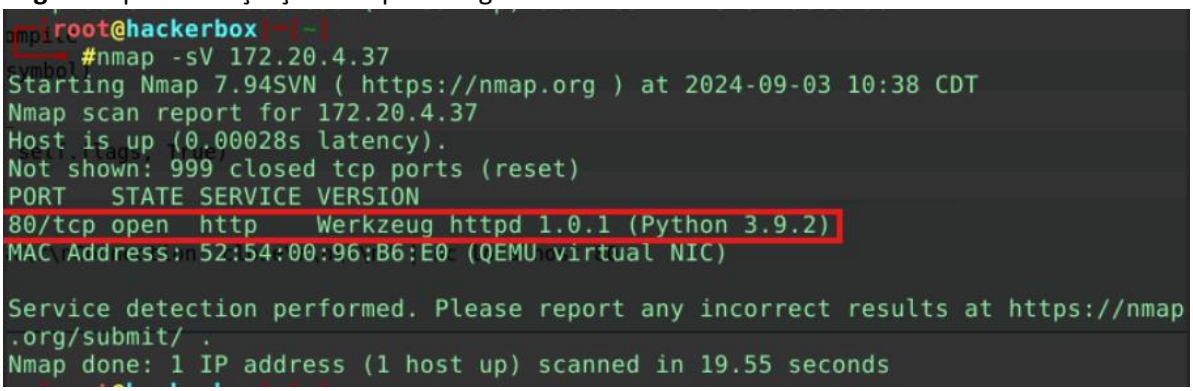
WORK STUFF ISINMASI

INFO: Werkzeug, Python tabanlı bir web uygulama araç setidir ve popüler web frameworkleri tarafından kullanılır. Esneklik ve modülerlik sağlayarak HTTP protokolüyle ilgili birçok karmaşık işlevi kolaylaştırır. Werkzeug kullanılarak oluşturulan web uygulamalarının güvenlik zafiyetlerini anlama ve bu zafiyetleri Metasploit Framework aracılığıyla istismar etme ile ilgili alıştırmalar yapmak için önerilir.

1. *80 portunda çalışan WSGI web uygulama kütüphanesi nedir?*
   Bilgi: nmap atılır ve çalışan kütüphane öğrenilir.

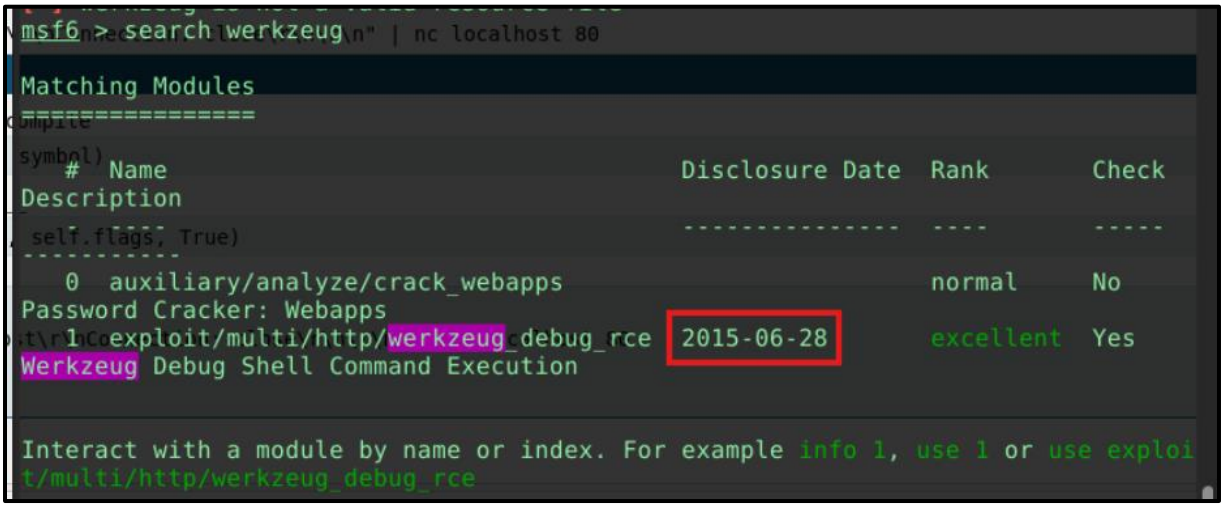


2. *Hata ayıklama modu etkinse hangi dizine erişilebilir?*
   Bilgi: Werkzeug'un eğer debug (hata ayıklama) modu etkinse /console yoluna erişilebilir.

3. *Hangi CLI aracı Exploit DB'de exploitleri arayabilir?*
   Bilgi: searchsploit aracı arar.

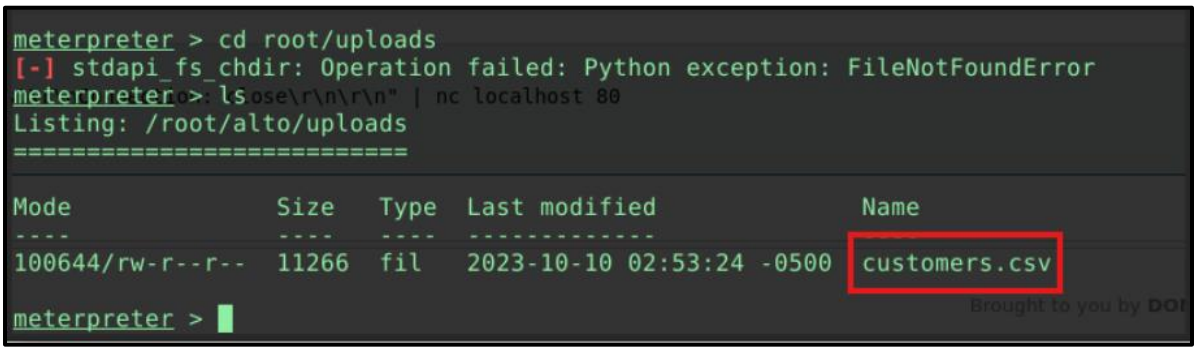
4. Exploitler, payloadlar ve çeşitli tarama komut dosyaları ile zengin bir içerik sunan CLI aracının adı nedir?
   Bilgi: metasploit framework – msfconsole aracı

5. Werkzeug ile ilgili bulunan exploitin açıklanma tarihi nedir?
   Bilgi: Önce msfconsole'a bağlanılır(msfconsole –q {bash}) ardından "werkzeug" ile yayınlanmış exploit var mı kontrol edilir ve ulaşılır.

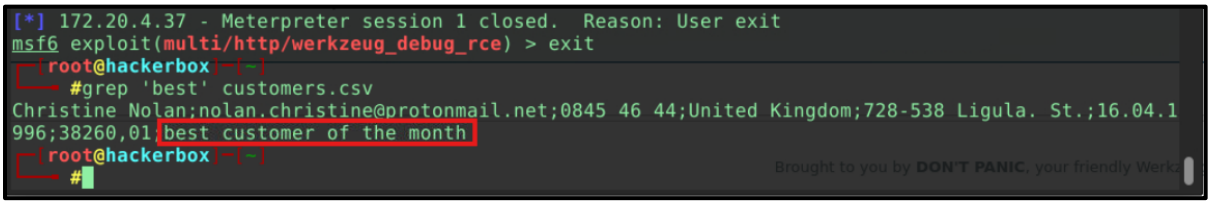


6. *Bir exploitin gerçekten çalışmadan önce çalışıp çalışmayacağını kontrol etmek için msfconsole komutu nedir?*
   Bilgi: check komutudur.

7. *Hangi dosyada müşteriler ile ilgili bilgiler vardır?*
   Bilgi: exploite bağlanılır ardından dosyaya erişilmeye çalışılır.
   - Use komutu ile kullanılmak istenen exploit seçilir.
   - Show options komutu ile gerkeli konfigürasyon ayarları yapılır.
   - Check komutu ile çalışıp çalışılmayacağı kontrol edilir.
   - Exploit komutu exploit çalıştırılır.
   - Exploit çalışır, root/uploads dizininde müşteriler ile ilgili bilgiler barındıran dosya bulunur.



8. *Ayın en iyi müşterisinin e-posta adresi nedir?*
   Bilgi: customers.csv indirilerek okunur.



-ISINMA TAMAMLANDI-