target = 10.10.11.25

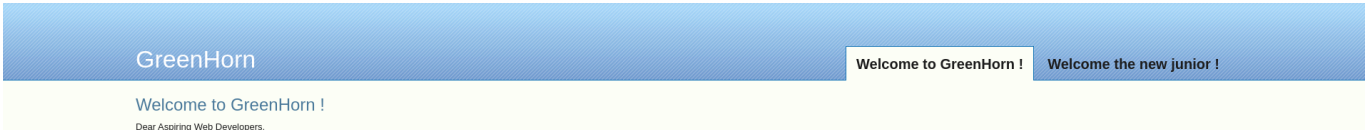
nmap scan

```
# Nmap 7.94SVN scan initiated Wed Sep 25 10:05:49 2024 as: nmap -sC -A -v -
oN scan.txt 10.10.11.25
Nmap scan report for 10.10.11.25
Host is up (0.15s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE    SERVICE        VERSION
22/tcp   open     ssh            OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu
Linux; protocol 2.0)
| ssh-hostkey:
|   256 57:d6:92:8a:72:44:84:17:29:eb:5c:c9:63:6a:fe:fd (ECDSA)
|_  256 40:ea:17:b1:b6:c5:3f:42:56:67:4a:3c:ee:75:23:2f (ED25519)
26/tcp   filtered rsftp
80/tcp   open     http           nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://greenhorn.htb/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.18.0 (Ubuntu)
1501/tcp filtered sas-3
1533/tcp filtered virtual-places
3000/tcp open     ppp?
| fingerprint-strings:
|   GenericLines, Help, RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Cache-Control: max-age=0, private, must-revalidate, no-transform
|     Content-Type: text/html; charset=utf-8
|     Set-Cookie: i_like_gitea=027886c560764173; Path=/; HttpOnly;
SameSite=Lax
|     Set-Cookie:
_csrf=Kl4aaR_QAQQeX9XPp5urHUXsHyk6MTcyNzI0Nzk2MjAyOTI3MzMyMg; Path=/; Max-
Age=86400; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
|     Date: Wed, 25 Sep 2024 07:06:02 GMT
|     <!DOCTYPE html>
|     <html lang="en-US" class="theme-auto">
|     <head>
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <title>GreenHorn</title>
|     <link rel="manifest"
href="data:application/json;base64,eyJuYW1lIjoiR3JlZW5Ib3JuIiwic2hvcnRfbmFt
ZSI6IkdyZWVuSG9ybiIsInN0YXJ0X3VybCI6Imh0dHA6Ly9ncmVlbmhvcm4uaHRiOjMwMDAvIiw
iaWNvbnMiOlt7InNyYyI6Imh0dHA6Ly9ncmVlbmhvcm4uaHRiOjMwMDAvYXNzZXRzL2ltZy9sb2
dvLnBuZyIsInR5cGUiOiJpbWFnZS9wbmciLCJzaXplcyI6IjUxMng1MTIifSx7InNyYyI6Imh0d
```

```
HA6Ly9ncmVlbmhvcm4uaHRiOjMwMDAvYX
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Allow: HEAD
|     Allow: HEAD
|     Allow: GET
|     Cache-Control: max-age=0, private, must-revalidate, no-transform
|     Set-Cookie: i_like_gitea=abe57f49dd804ec9; Path=/; HttpOnly;
SameSite=Lax
|     Set-Cookie:
_csrf=_14HcXHw5T8aesZ8vOG7ZWfFTLQ6MTcyNzI0Nzk2NzgyMTg2MTQ5MA; Path=/; Max-
Age=86400; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
|     Date: Wed, 25 Sep 2024 07:06:07 GMT
|_    Content-Length: 0
4443/tcp filtered pharos
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Wed Sep 25 10:07:46 2024 -- 1 IP address (1 host up) scanned
in 117.13 seconds
```

port 80

http://greenhorn.htb

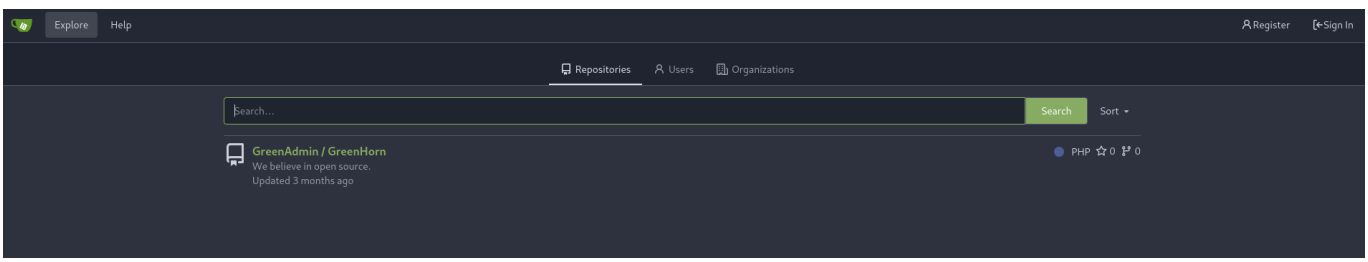


Here I found a login page at /login.php but I had no password.

pluck4.7.18 is vulnerable to authenticated remote code execution(RCE) but no password yet. link

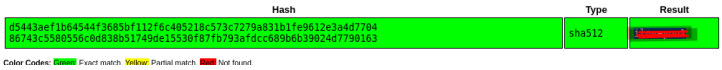
port 3000

http://greenhorn.htb:3000



The source code to the whole web app is here and all is left is to find the config file to gain the password.

I used crackstation.net to crack it



Back the rce I had found earlier and now with the password and having set up a listener once the exploit is uploaded.

After scanning the system I found a few users

```
git:x:114:120:Git Version Control,,,:/home/git:/bin/bash
junior:x:1000:1000::/home/junior:/bin/bash
root:x:0:0:root:/root:/bin/bash
```

The same password seems to work for user junior

Privilege Escalation

> Hello junior,
>
> We have recently installed OpenVAS on our server to actively monitor and identify potential security vulnerabilities. Currently, only the root user, represented by myself, has the authorization to execute OpenVAS using the following command:
>
> `sudo /usr/sbin/openvas`
>
> Enter password: [redacted]
>
> As part of your familiarization with this tool, we encourage you to learn how to use OpenVAS effectively. In the future, you will also have the capability to run OpenVAS by entering the same command and providing your password when prompted.
>
> Feel free to reach out if you have any questions or need further assistance.
>
> Have a great week,
>
> Mr. Green

Reversing pixelation

This was a new one.

Lets start with the pdf in the home dir
Pixelation is a process where an image is divided into blocks, and each block is averaged into a single color. This makes the details within the block indistinguishable. So it is deterministic and can be reversed if the original image's characteristics and the pixelation process are known.

- Tools
  - pdfimages - To generate an image containing pixeled data
  - Depix link - reversing

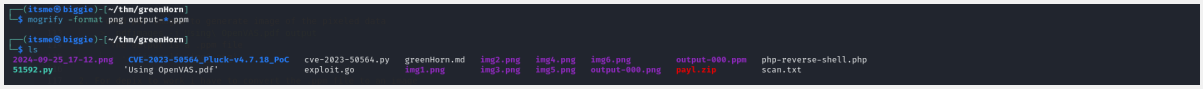
1. I used pdf images to generate image of the pixeled data

   > pdfimages -j Using\ OpenVAS.pdf output

   - The output is a .ppm file

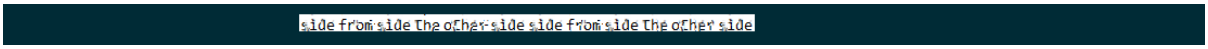
2. For depix to work i have to convert the .ppm file to an image

> mogrify -format png output-*.ppm -



3. I run depix against the image output generated.

> python3 /home/itsme/thm/t00ls/Depix/depix.py -p /home/itsme/thm/greenHorn/output-000.png -s /home/itsme/thm/t00ls/Depix/images/searchimages/debruinseq_notepad_Windows10_closeAndSpaced.png -o output.png

- 

With the password, Lets try su root.