

★ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



# TryHackMe Content Discovery Walkthrough



Orhan Öztaş · [Follow](#)

3 min read · Apr 22, 2022



Listen



Share

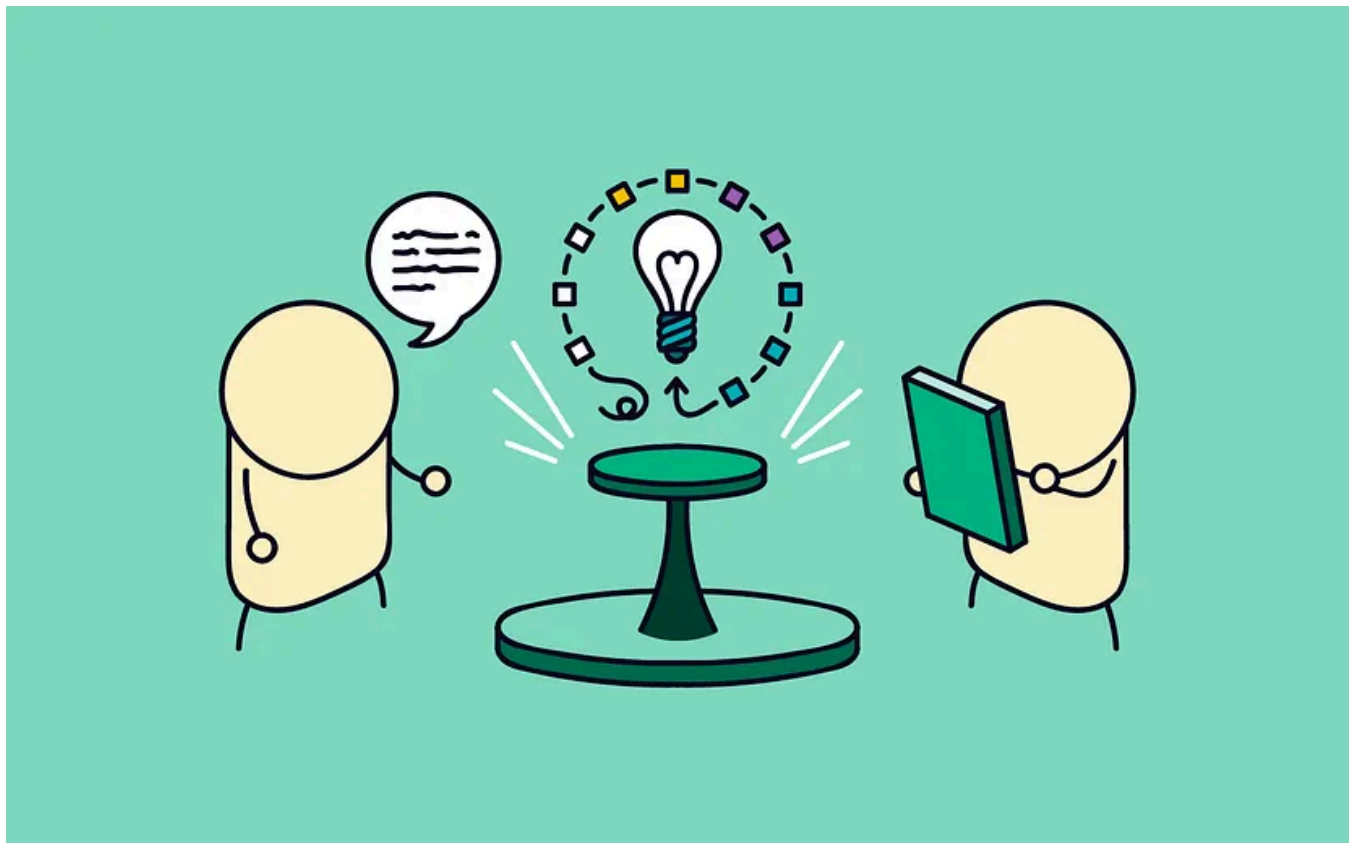


More

Today im gonna finish the Content Discovery room from the TryHackMe.

You can reach the room from here:

<https://tryhackme.com/room/contentdiscovery>



We will learn how can find a content directory in websites. Let's Go!

First 3 question coming from the above text. We can find answer in What Is Content Discovery text.

- What is the Content Discovery method that begins with M?

*manually*

- What is the Content Discovery method that begins with A?

*automated*

- What is the Content Discovery method that begins with O?

*osint*

When we go to <http://10.10.249.237/robots.txt> see the directory in pages content and we will go the /staff-portal directory. We can see the “You found the robots.txt endpoint” comment.

- What is the directory in the robots.txt that isn’t allowed to be viewed by web crawlers?

*/staff-portal*

At favicon section firstly we will go to <https://static-labs.tryhackme.cloud/sites/favicon/> website. Then we will run command

`curl https://static-labs.tryhackme.cloud/sites/favicon/images/favicon.ico | md5sum`

And this command give us a md5 hash. When we check to [https://wiki.owasp.org/index.php/OWASP favicon database](https://wiki.owasp.org/index.php/OWASP_favicon_database)

this website find the answer.

- What framework did the favicon belong to?

*cgiirc*

At Acme IT support’s website we going to **Sitemap.xml** directory and a xml file return. This page has 5 directory. When we check the all directory find the “You found the sitemap endpoint” text.

- What is the path of the secret area that can be found in the sitemap.xml file?

At the HTTP Header section we will request a <http://10.10.249.237> with verbose. Verbose give us a x-flag at their response header.

- What is the flag value from the X-FLAG header?

---

*thm{header\_flag}*

---

At the **Framework Stack** section we will go <https://static-labs.tryhackme.cloud/sites/thm-web-framework/documentation.html>

firstly. Then we can see Admin credential and Acme IT website directory ( /thm-framework-login) at there. When we add the directory back to ip address can see the login page for admins.

Username: admin

Password: admin

- What is the flag from the framework's administration portal?

---

*THM{CHANGE\_DEFAULT\_CREDENTIALS}*

---

At the Google Hacking/Dorking section we will read the all text and answer the question.

- What Google dork operator can be used to only show results from a particular site?

---

*site:*

---

At the Wappalyzer section we will read the all text and answer the question.

- What online tool can be used to identify what technologies a website is running?

---

*Wappalyzer*

---

- What is the website address for the Wayback Machine?

---

<https://archive.org/web>

---

At the Git section we will read the all text and answer the question.

- What is Git?

*version control system*

- What URL format do Amazon S3 buckets end in?

*s3.amazonaws.com*

At the last question we will discovering automatically.

```
=====
[+] Url:          http://10.10.10.180/
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/SecLists/Discovery/Web-Content/common.t
xt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
=====
2021/10/04 20:19:51 Starting gobuster
=====
/assets (Status: 301)
/contact (Status: 200)
/customers (Status: 302)
/development.log (Status: 200)
/monthly (Status: 200)
/news (Status: 200)
/private (Status: 301)
/robots.txt (Status: 200)
/sitemap.xml (Status: 200)
=====
2021/10/04 20:19:53 Finished
```

After execute the commands we will see information above.

- What is the name of the directory beginning “/mo...” that was discovered?

*/monthly*

- What is the name of the log file that was discovered?

*/development.log*

Thanks for reading.

\

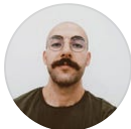
Cybersecurity

Tryhackme Walkthrough

Tryhackme

Recon

Technology



Follow

## Written by Orhan Öztaş

440 Followers · 141 Following

Cyber Security Consultant. Writing articles for helping you about cyber security.

### Responses (1)



What are your thoughts?

Respond



Samar

2 months ago




thanks



Reply

### More from Orhan Öztaş



 Orhan Öztaş

## Cyberdefenders ELASTIC CASE write up

Cyberdefenders is a big opportunity for cyber security analysts. Platform has a very different rooms for investigate for cyber crimes. One...

Jun 5, 2022



54



2



Open in app ↗

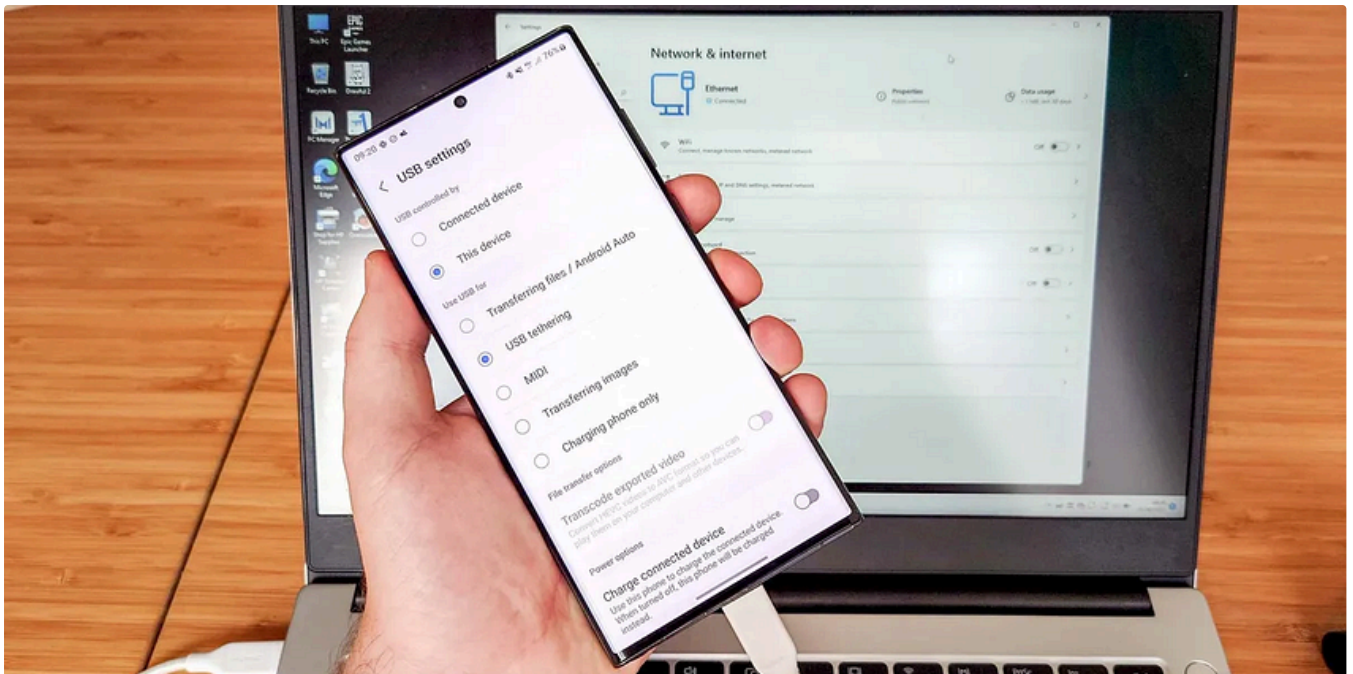
Medium




Search



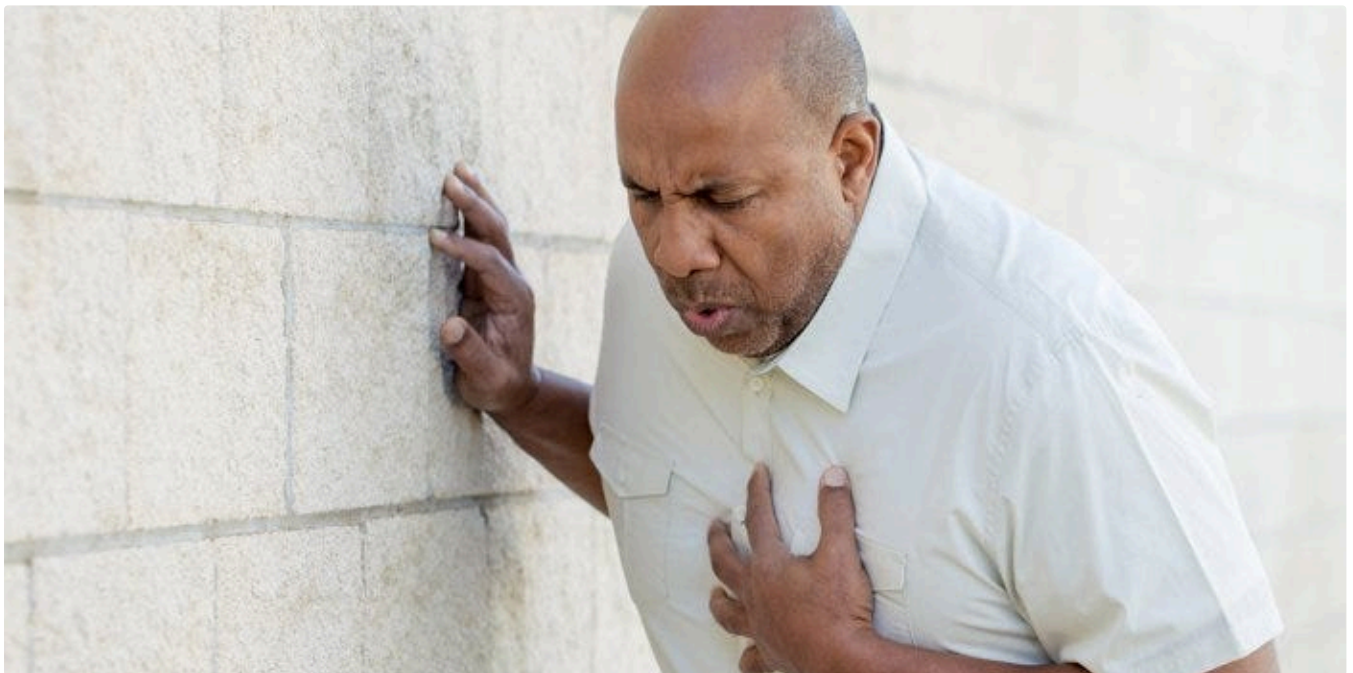




 Orhan Öztaş

## Prevent Hotspot and USB Tethering with SEP Location Awareness

Feb 9, 2024  88



 Orhan Öztaş

## If you see this PowerShell Commands on your pc, sorry you probably got hacked

If you suspicious to hacked your computer and you do not have any experience about cybersecurity field, you are correct place. But since...

May 16, 2022 🖱 281 💬 4



# Malware



Orhan Öztaş

## Cyberdefenders EMOTET malware write up

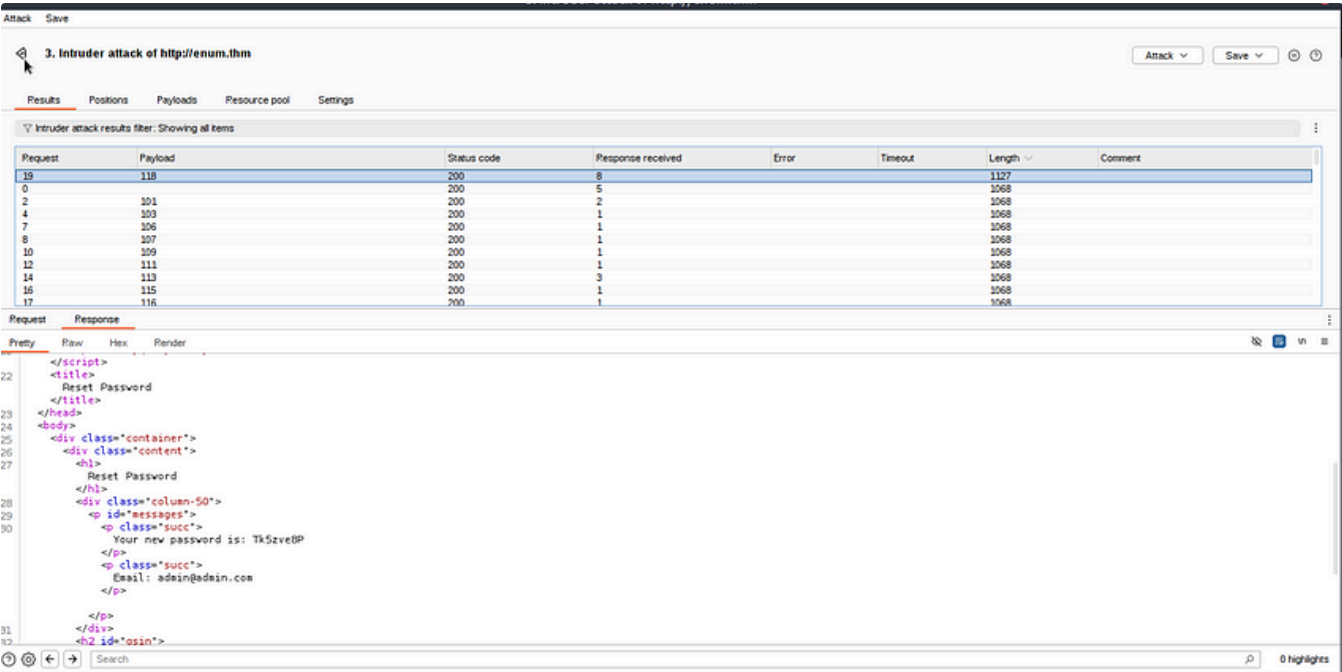
In this write up we will solve EMOTET room for malware practice. We need Volatility tool and memory dump. For install the Volatillity...


May 13, 2022 🖱 209

[See all from Orhan Öztaş](#)

## Recommended from Medium





 embosssdotar

## TryHackMe—Enumeration & Brute Force—Writeup

Key points: Enumeration | Brute Force | Exploring Authentication Mechanisms | Common Places to Enumerate | Verbose Errors | Password Reset...

★ Jul 31, 2024 🖱 26

🔖 + ...



 In T3CH by Axoloth

## TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

★ Nov 5, 2024 🖱 60



## Lists



### AI Regulation

6 stories · 666 saves



### ChatGPT prompts

51 stories · 2424 saves



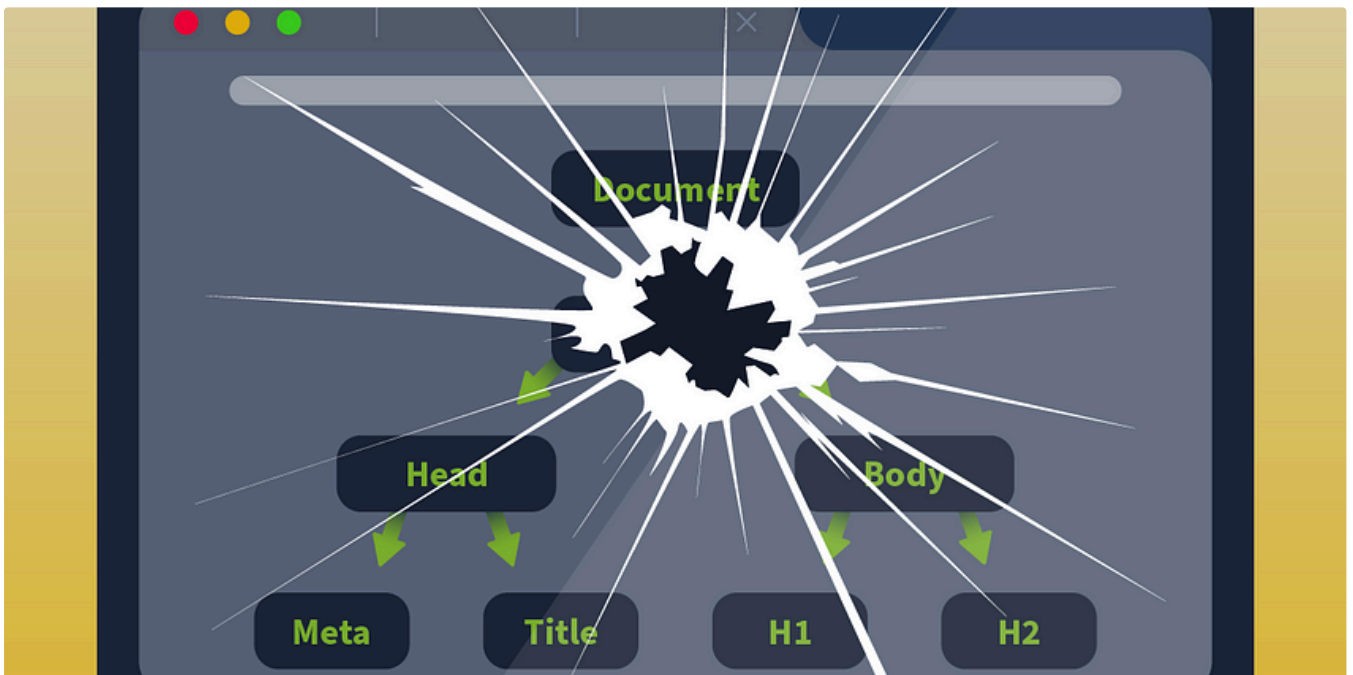
### Tech & Tools

22 stories · 377 saves



### Generative AI Recommended Reading

52 stories · 1582 saves



Jawstar

## DOM-Based Attacks Tryhackme Write-up

### Task 1 : Introduction

★ Nov 20, 2024





In System Weakness by Sunny Singh Verma [ SuNnY ]

## The Sticker Shop Motion Graphics TryHackMe Writeup | Beginner Friendly | Detailed Walkthrough |...

Motions graphics writeup for TryHackme Room → [ The Sticker Shop ]

Dec 22, 2024 🖱 55

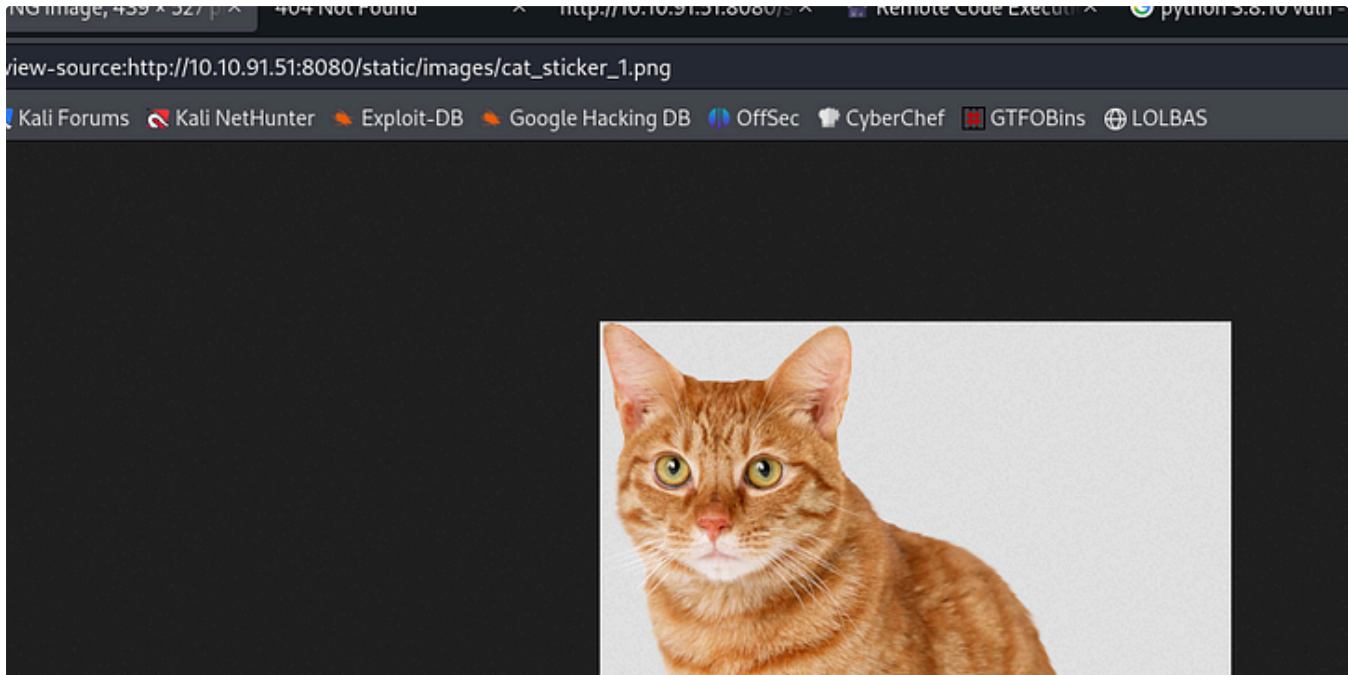


IritT

## Intro to Cross-site Scripting — TryHackMe Walkthrough

Learn how to detect and exploit XSS vulnerabilities, giving you control of other visitor's browsers.

Sep 10, 2024



James Jarvis

## The Sticker Shop | TryHackMe CTF Write-up + Summary

Greetings—another write-up awaits.

Dec 19, 2024



1

[See more recommendations](#)