

[Open in app](#)

Medium

 Search

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



Obfuscation Principles : Tryhackme Walkthrough

0xUN7H1NK4BLE · [Follow](#)

Dec 14, 2022



Listen



Share



More

How many core layers make up the Layered Obfuscation Taxonomy?

4

What sub-layer of the Layered Obfuscation Taxonomy encompasses meaningless identifiers?

Obfuscating layout

What obfuscation method will break or split an object?

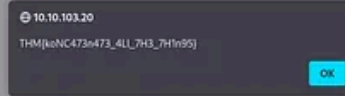
data splitting

What obfuscation method is used to rewrite static data with a procedure call?

data procedurization

What flag is found after uploading a properly obfuscated snippet?

The file script.ps1 has been uploaded.fail!
Warning: unlink(C:\Users\Administrator\Desktop\pass-1.txt): No such file or directory in C:\xampp\htdocs\upload-1.php on line 42



THM{koNC473n473_4Ll_7H3_7H1n95}

What are junk instructions referred to as in junk code?

Code Stubs

What obfuscation layer aims to confuse an analyst by manipulating the code flow and abstract syntax trees?

Obfuscating controls

Can logic change and impact the control flow of a program? (T/F)

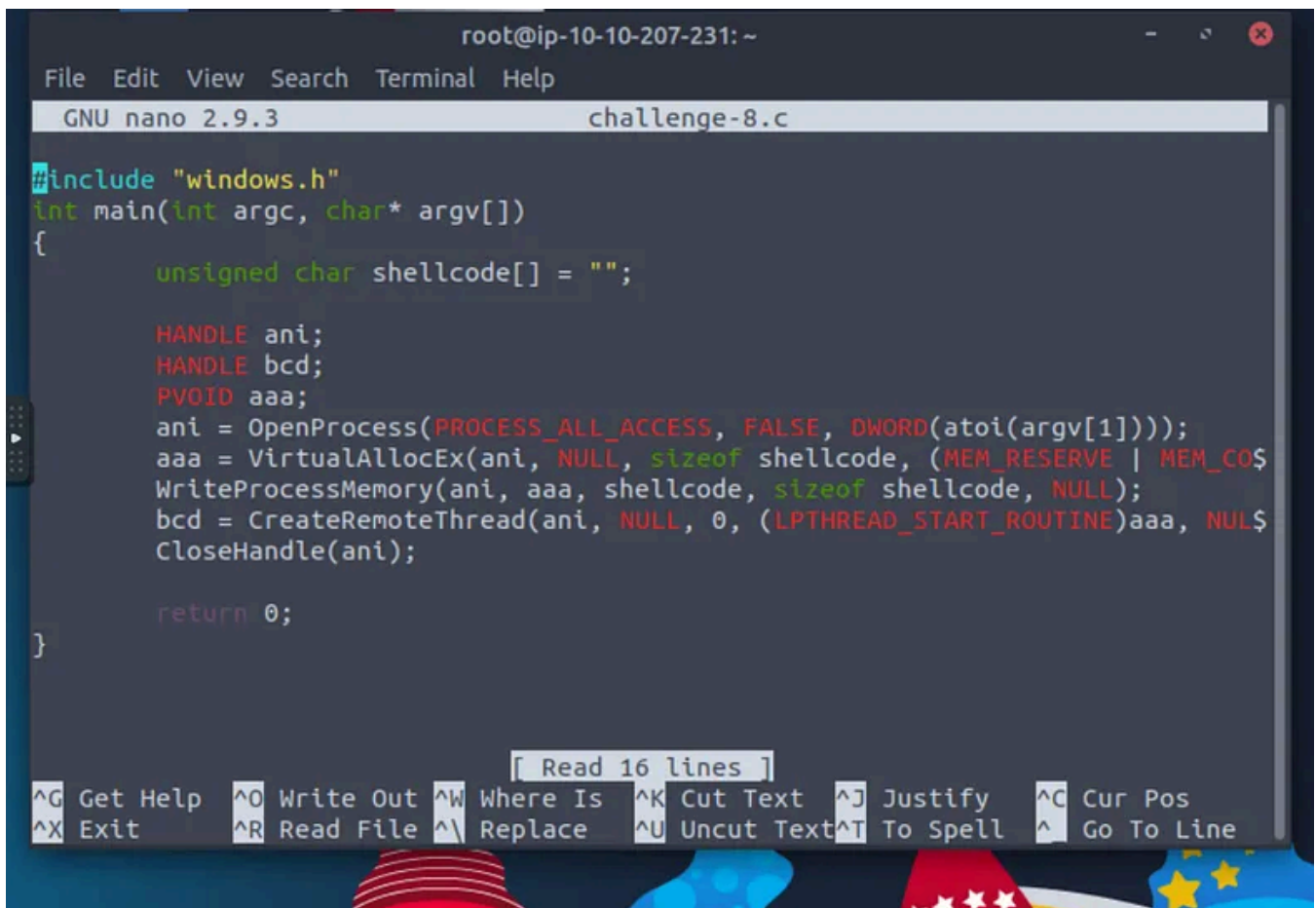
T

What flag is found after properly reversing the provided snippet?

THM{D3cod3d!!!}

What flag is found after uploading a properly obfuscated snippet?

THM{Y0Ur_1NF0_15_M1N3}



```
root@ip-10-10-207-231: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 challenge-8.c

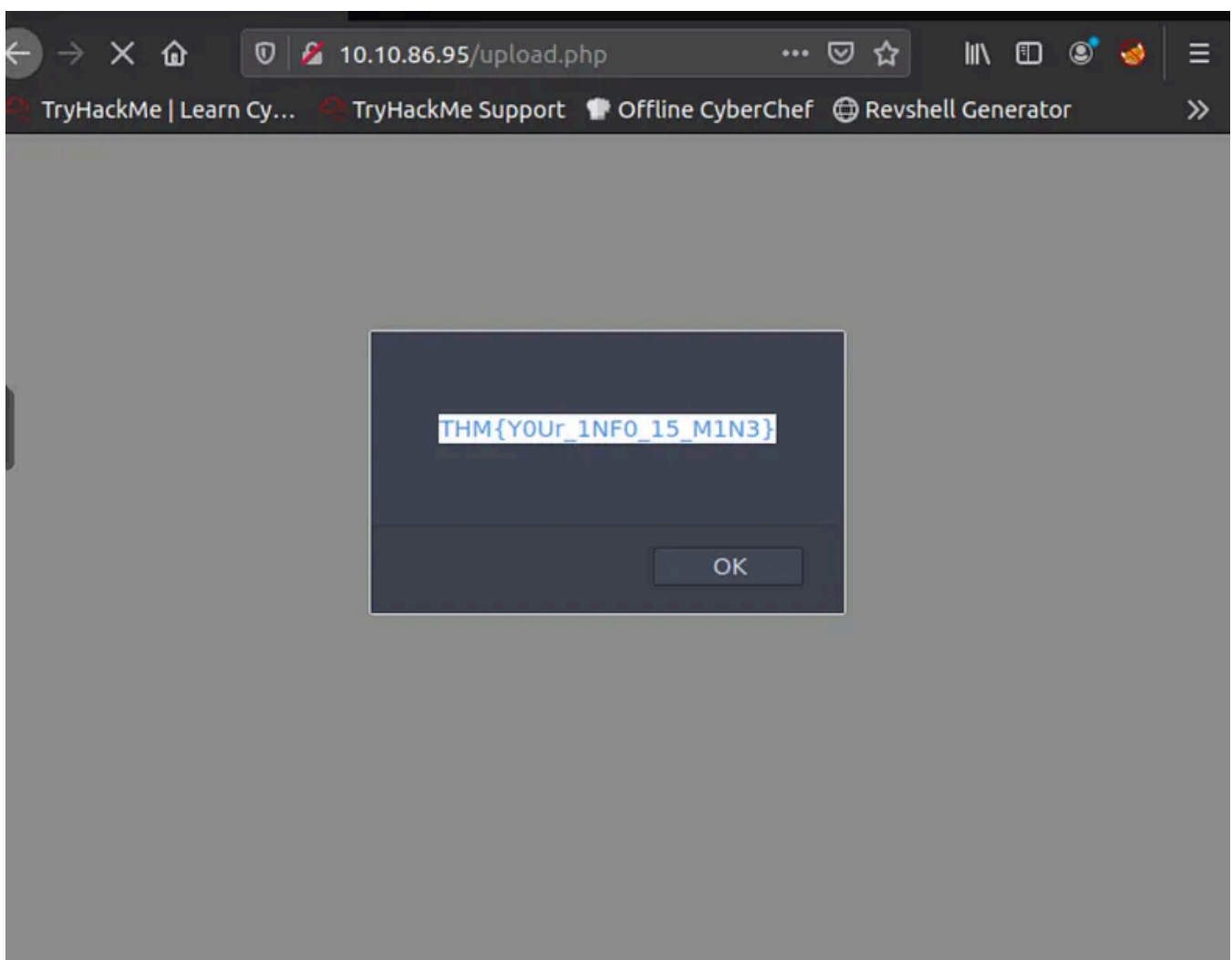
#include "windows.h"
int main(int argc, char* argv[])
{
    unsigned char shellcode[] = "";

    HANDLE ani;
    HANDLE bcd;
    PVOID aaa;
    ani = OpenProcess(PROCESS_ALL_ACCESS, FALSE, DWORD(atoi(argv[1])));
    aaa = VirtualAllocEx(ani, NULL, sizeof shellcode, (MEM_RESERVE | MEM_COMMIT));
    WriteProcessMemory(ani, aaa, shellcode, sizeof shellcode, NULL);
    bcd = CreateRemoteThread(ani, NULL, 0, (LPTHREAD_START_ROUTINE)aaa, NULL, 0, 0);
    CloseHandle(ani);

    return 0;
}
```

Read 16 lines

Get Help Write Out Where Is Cut Text Justify Cur Pos
Exit Read File Replace Uncut Text To Spell Go To Line



Obfuscation

Principles

Tryhackme

Thm

Writeup



Follow

Written by 0xUN7H1NK4BLE

48 Followers · 13 Following

Cyber Security Enthusiast | A learner

No responses yet




What are your thoughts?

Respond

More from 0xUN7H1NK4BLE

<code>appendnullbyte.py</code>	Appends the encoded NULL byte character at the end of the payload.
<code>base64encode.py</code>	Base64 all characters in a given payload.
<code>between.py</code>	Replaces greater than operator (>) with NOT BETWEEN 0 AND #.
<code>bluecoat.py</code>	Replaces the space character after an SQL statement with a valid random blank character. Afterward, it replaces the character = with a LIKE operator.
<code>chardoubleencode.py</code>	Double URL—encodes all characters in a given payload (not processing those that are already encoded).
<code>commalesslimit.py</code>	Replaces instances like LIMIT M, N with LIMIT N OFFSET M.
<code>commalessmid.py</code>	Replaces instances like MID(A, B, C) with MID(A FROM B FOR C).
<code>concat2concatws.py</code>	Replaces instances like CONCAT(A, B) with CONCAT_WS(MID(CHAR(0), 0, 0), A, B).
<code>charencode.py</code>	URL—encodes all characters in a given payload (not processing those already


 0xUN7H1NK4BLE

SQLmap like a pro...

sqlmap—automatic SQL injection tool

Jan 30, 2023  414  2



 0xUN7H1NK4BLE


Data Exfiltration Tips/Tricks

As a security researcher, you have been hired to test the security of a company's network. During your analysis, you discover a...

Mar 24, 2023 55



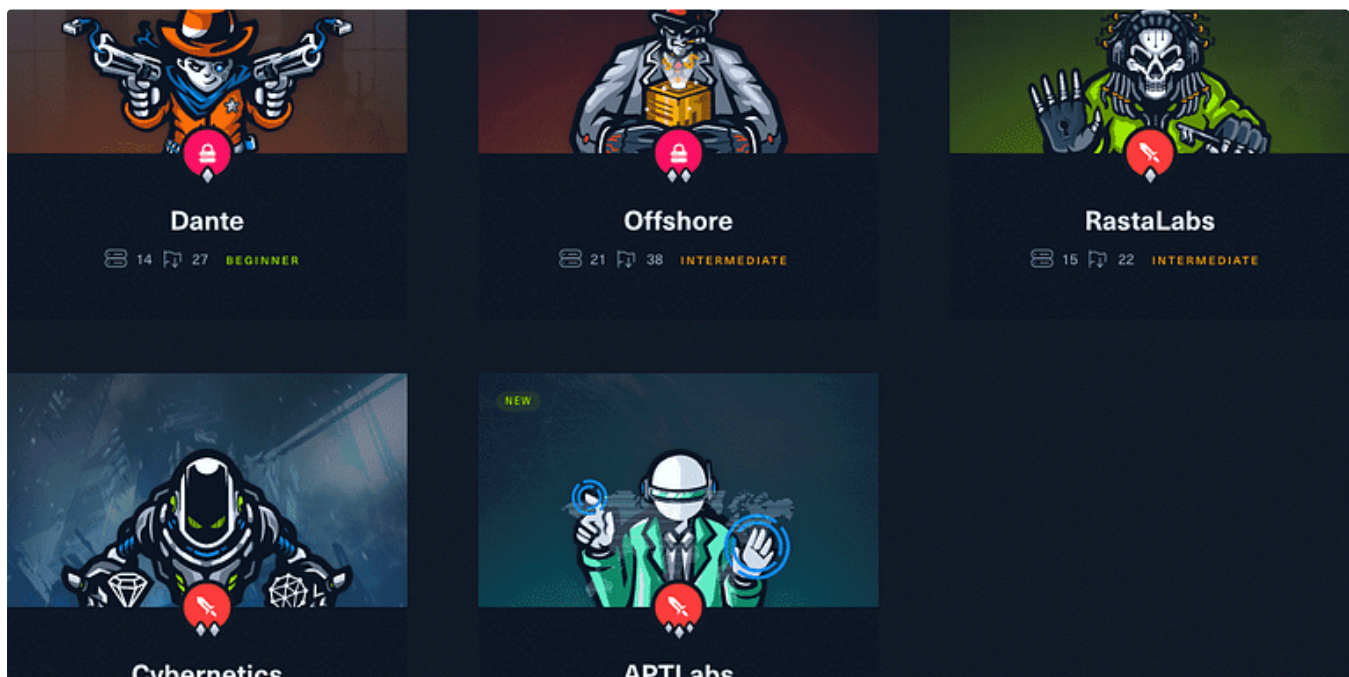
Are you Confident?

 0xUN7H1NK4BLE

All you want to know about ffuf

The term fuzzing refers to a testing technique that sends various types of user input to a certain interface to study how it would react...

Mar 13, 2023 52

 0xUN7H1NK4BLE

CPTS- Everything You Need to Know

I recently achieved a significant milestone in my cybersecurity career: I passed the HTB Certified Penetration Testing Specialist (HTB...

May 27, 2024 🖱️ 259 💬 2



See all from 0xUN7H1NK4BLE

Recommended from Medium



Day 11
Answers

cyberw1ng.medium.com

 In System Weakness by Karthikeyan Nagaraj


Advent of Cyber 2024 [Day 11] Writeup with Answers | TryHackMe Walkthrough

If you'd like to WPA, press the star key!

★ Dec 11, 2024 🖱️ 855 💬 1





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

Silver Platter TryHackMe Motion Graphics Writeup | Beginner Friendly | Detailed Walkthrough |...

A Detailed motion Graphics writeup for TryHackMe room Silver Platter

★ Jan 13 🖱 1

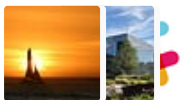


Lists



Staff picks

804 stories · 1587 saves



Stories to Help You Level-Up at Work

19 stories · 925 saves



Self-Improvement 101

20 stories · 3244 saves



Productivity 101

20 stories · 2740 saves



IritT

CyberChef: The Basics—Crypto 101—Defensive Security Tooling-Cryptography-TryHackMe Walkthrough

This room is an introduction to CyberChef, the Swiss Army knife for cyber security professionals.

Nov 2, 2024



Atharva

TryHackMe—Whiterose Writeup

Complete step-by-step writeup for TryHackMe challenge room Whiterose!

Nov 12, 2024 16

 TheHiker

Silver-Platter , TryHackMe Walkthrough | TheHiker

Hello everyone, today I'll be covering the "Silver-Platter" room on TryHackMe. I think that this room is great for intermediate students...

Jan 12 27



Cat Sticker 1

Price: \$2.99



Cat Sticker 2

Price: \$3.99

 Jiemook

The Sticker Shop—TryHackMe Walkthrough (DETAILED)

We don't need for some intro, let's get started!

Dec 1, 2024



See more recommendations