

[Open in app](#)

Medium

 Search

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



Vulnerabilities 101 | TryHackMe | Solutions

Neharidha Murali · [Follow](#)

3 min read · Apr 9, 2024

Listen

Share

More

Vulnerabilities 101

Understand the flaws of an application and apply your researching skills on some vulnerability databases.

Task1

1) Read this task!

Correct Answer : No answer needed.

Task2

2.1) An attacker has been able to upgrade the permissions of their system account from “user” to “administrator”. What type of vulnerability is this?

Correct Answer:Operating System

2.2) You manage to bypass a login panel using cookies to authenticate. What type of vulnerability is this?

Correct Answer : Application Logic

Task3

3.1) What year was the first iteration of CVSS published?

Correct Answer : 2005

3.2) If you wanted to assess vulnerability based on the risk it poses to an organisation, what framework would you use?

Note: We are looking for the acronym here.

Correct Answer : vpr

3.3) If you wanted to use a framework that was free and open-source, what framework would that be?

Note: We are looking for the acronym here.

Correct Answer : cvss

Task4

4.1) Using NVD, how many CVEs were published in July 2021?

Correct Answer : 1554

4.2) Who is the author of Exploit-DB?

Correct Answer : OffSec

Task5

5.1) What type of vulnerability did we use to find the name and version of the application in this example?

Correct Answer : Version Disclosure

Task6

6.1) Follow along with the showcase of exploiting ACKme's application to the end to retrieve a flag. What is this flag?

Correct Answer : THM{ACKME_ENGAGEMENT}

Task7

7.1) Continue on your learning with the additional rooms in this [module](#).

Correct Answer : No answer needed.

Happy Learning — Hope this helps you out :)

For in-depth solutions, check this out — <https://github.com/neharidha?tab=repositories>

-Neharidha Murali

Vulnerabilities 101

Tryhackme

Neharidhamurali



Follow

Written by Neharidha Murali

37 Followers · 3 Following

Neharidha Murali - Security Engineer | : <https://github.com/neharidha>: Interested in Development & Hacking, University of Maryland US



Responses (1)

What are your thoughts?

Respond



Prakash Tiwari

Jan 16



Hey it's have been month's you didn't post anything



Reply

More from Neharidha Murali



Neharidha Murali

Linux Fundamentals Part 3 | TryHackMe | Solution

Module - Linux Fundamentals

Nov 26, 2023



Neharidha Murali

How websites work | TryHackMe | Solution

How websites work

Nov 4, 2023

👏 2



Neharidha Murali

Core Windows Processes | TryHackMe | Solution

Task1:

Jul 31, 2023 🖱 10



Neharidha Murali

Autopsy | TryHackMe | Solutions

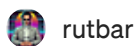
Task1:

Jun 11, 2023



See all from Neharidha Murali

Recommended from Medium

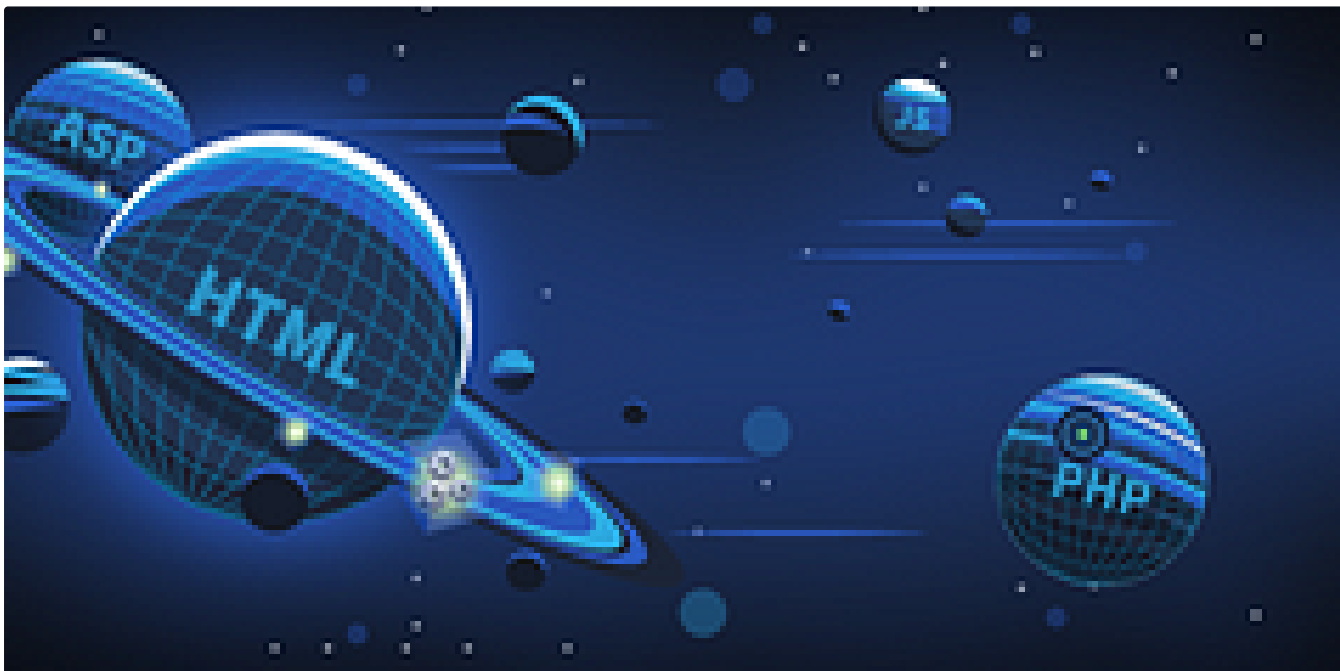


rutbar

TryHackMe—Web Application Basics | Cyber Security 101 (THM)

Web Application Overview

★ Oct 26, 2024



In T3CH by Axoloth

TryHackMe | Web Application Basics | WriteUp

Learn the basics of web applications: HTTP, URLs, request methods, response codes, and headers

★ Oct 26, 2024 🖱 56



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



In T3CH by Axoloth

TryHackMe | Vulnerability Scanner Overview | WriteUp

Learn about vulnerability scanners and how they work in a practical scenario

★ Nov 23, 2024 🖱 50



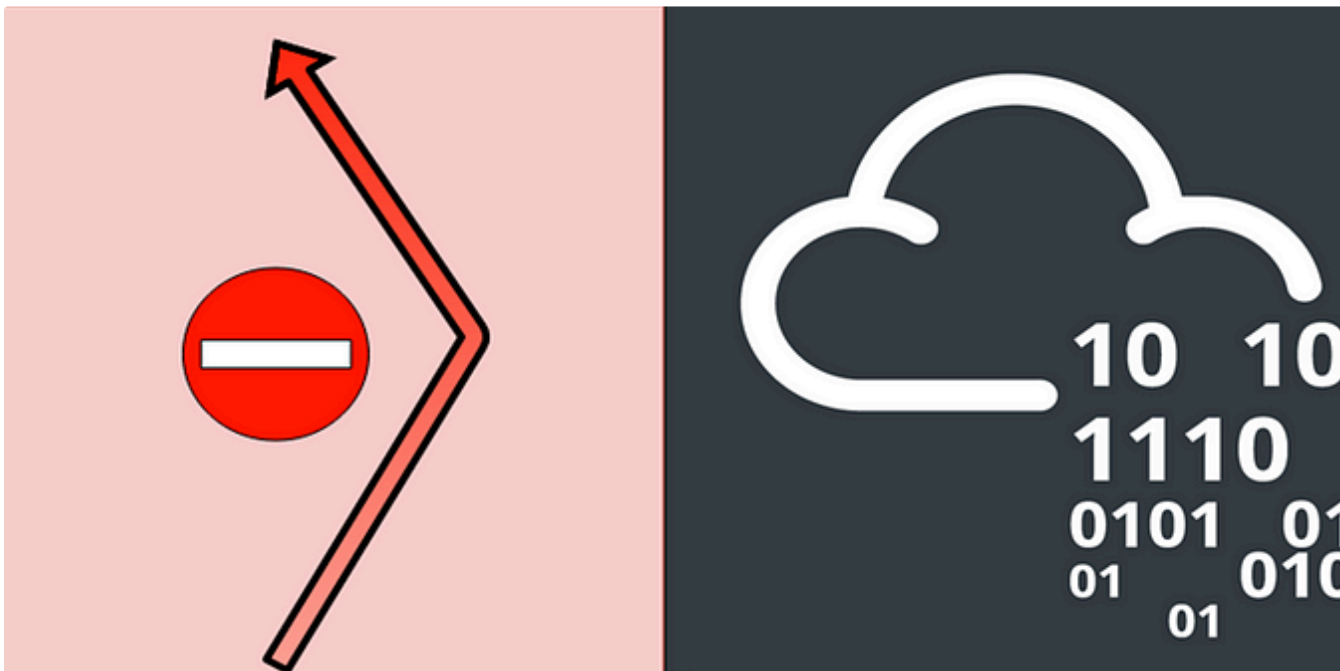



 In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

★ Nov 5, 2024 🖱 60



 IritT

TryHackMe Authentication Bypass—walkthrough

Learn how to defeat logins and other authentication mechanisms to allow you access to unpermitted areas.

Sep 2, 2024

 MAGESH

John the Ripper: The Basics-Tryhackme Writeup

Learn how to use John the Ripper, a powerful and adaptable hash-cracking tool

Oct 25, 2024

[See more recommendations](#)