Insecure Randomness | TryHackMe

Overview: Insecure randomness occurs when web applications use predictable or poorly generated random values, making them vulnerable to attacks. While randomness is essential for securing tokens, session IDs, and cryptographic keys, insecure implementation can allow attackers to exploit these predictable values to bypass authentication, hijack sessions, or even decrypt sensitive data.

0xDK · Follow
2 min read · Jan 15, 2025

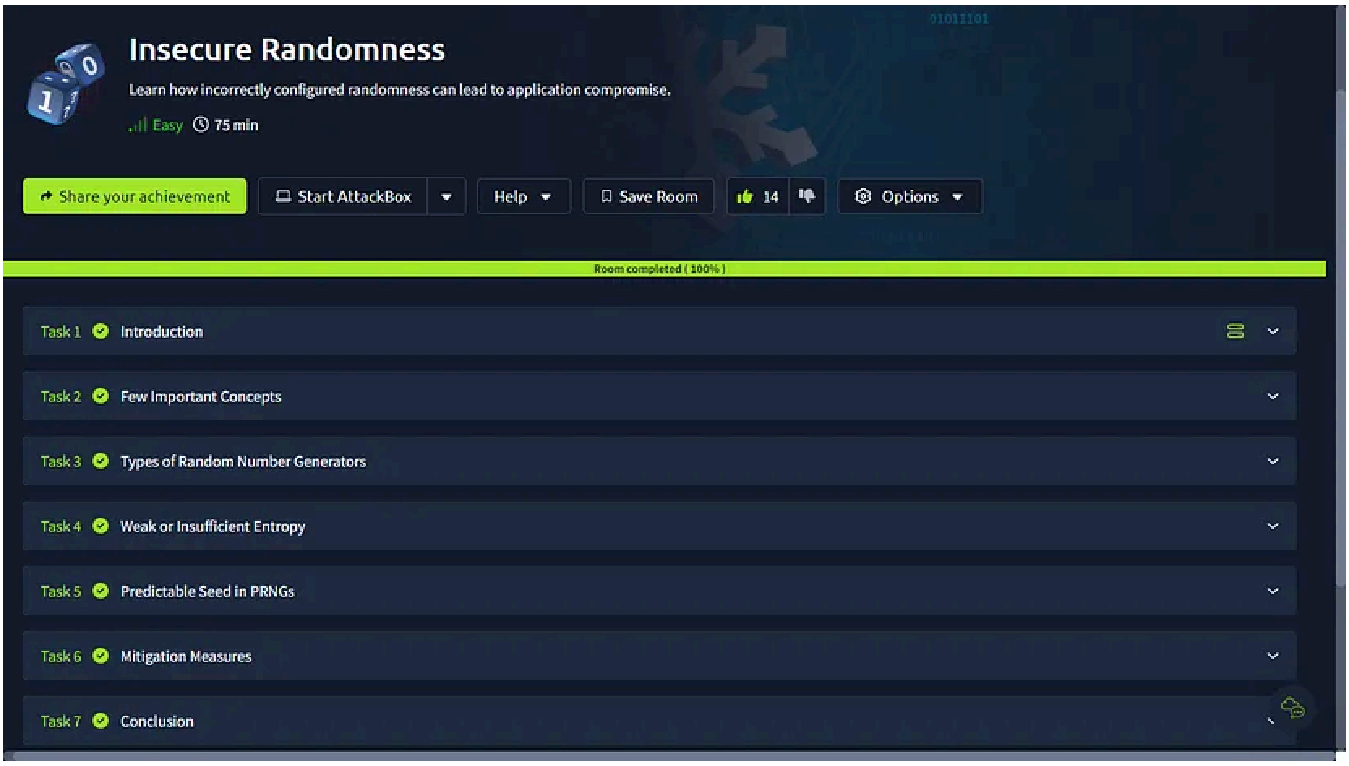
Listen Share More

In this room, we will explore techniques to identify and exploit vulnerabilities caused by insecure randomness. This will provide you with the knowledge to assess and enhance the security of web applications by ensuring proper random number generation practices.

Learning Objectives

Throughout this room, you will gain a comprehensive understanding of the following key concepts:

- Understanding insecure randomness
- Type of random number generators
- Weak or Insufficient Entropy
- Predictable seeds during token generation



Insecure Randomness

Learn how incorrectly configured randomness can lead to application compromise.

Easy 75 min

Room completed (100%)

Task 1 Introduction

Task 2 Few Important Concepts

Task 3 Types of Random Number Generators

Task 4 Weak or Insufficient Entropy

Task 5 Predictable Seed in PRNGs

Task 6 Mitigation Measures

Task 7 Conclusion

Answers:

Task 1

1)I am ready to start the room.

> *Ans: No answer needed*

Task 2

2)What measures the amount of randomness or unpredictability in a system?

> *Ans: entropy*

3)Is it a good practice to keep the same seed value for all cryptographic functions? (yea/nay)

> *Ans: nay*

Task 3

4)You prepare a game involving immediate interaction and random event simulation but with no critical security requirements. Which type of RNG would be most appropriate for this purpose? Write the correct option only.
a) TRNG
b) Statistical PRNG
c) We should not use randomness in games
d) None of the above

> *Ans: b*

Task 4

5)What is the flag value after logging in as the victim user?

> *Ans: THM{VICTIM_SIGNED_IN}*

6)What is the flag value after logging in as the master user?

> *Ans: THM{ADMIN_SIGNED_IN007}*

7)What is the PHP function used to create the token variable in the code above?

> *Ans: time()*

Task 5

8)What is the flag value after logging in as magic@mail.random.thm?

> *Ans: THM{MAGIC_SIGNED_IN11010}*

9)What is the flag value after logging in as hr@mail.random.thm?

> *Ans: THM{HR_SIGNED_IN1337}*

10)What is the PHP function used to seed the RNG in the code above?

> *Ans: mt_srand*

Task 6

11)Which of the following can be considered as a weak seed value? Write the correct letter only.
a) Timestamp
b) IP Address
c) 6-digit constant value
d) All of the above

> *Ans: d*

Task 7:

12)I have completed the room.

> *Ans: No answer needed*

Thank YOu :)

Randomness Tryhackme Walkthrough Entropy Cryptographic Key Seeding

Follow

Written by 0xDK

48 Followers · 133 Following

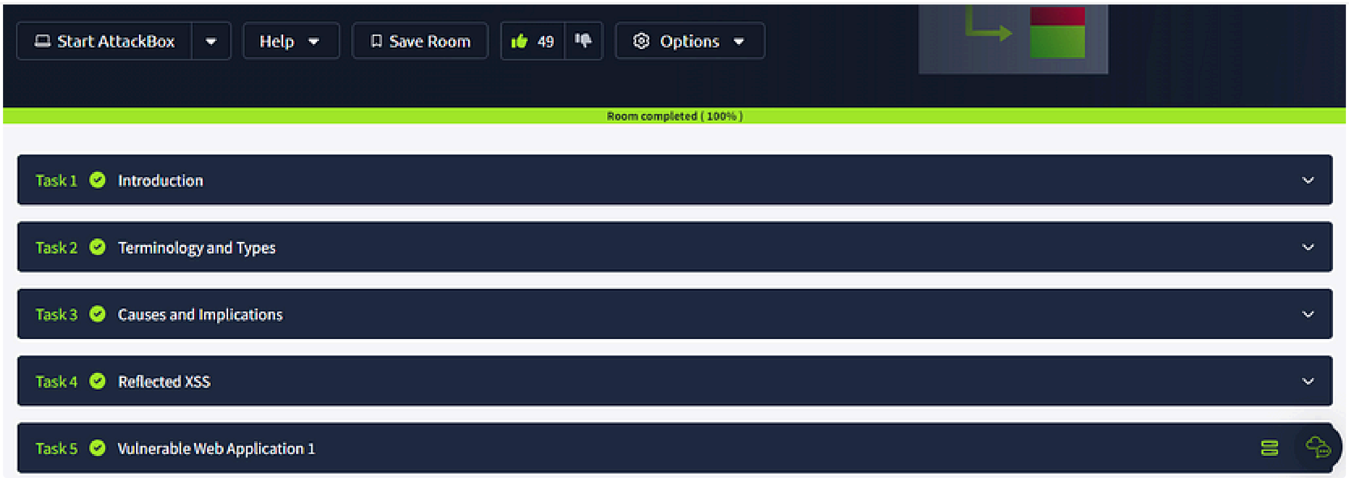
Cyb3r 3nthu5ia5t

No responses yet

What are your thoughts?

Respond

More from 0xDK



Task 1 ✓ Introduction

Task 2 ✓ Terminology and Types

Task 3 ✓ Causes and Implications

Task 4 ✓ Reflected XSS

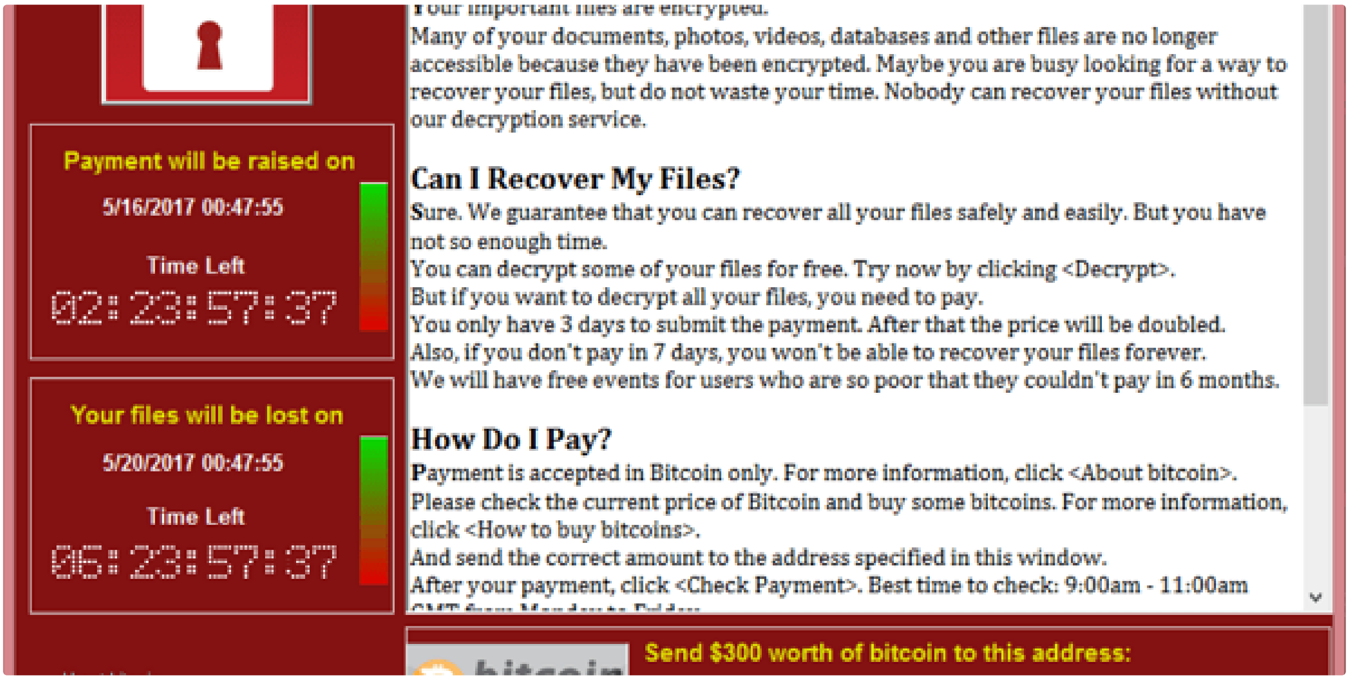
Task 5 ✓ Vulnerable Web Application 1

0xDK

XSS Room Walkthrough| TryHackMe

Overview: Real-world examples of XSS attacks (without confidential details) to illustrate the impact.

Apr 18, 2024 44



Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

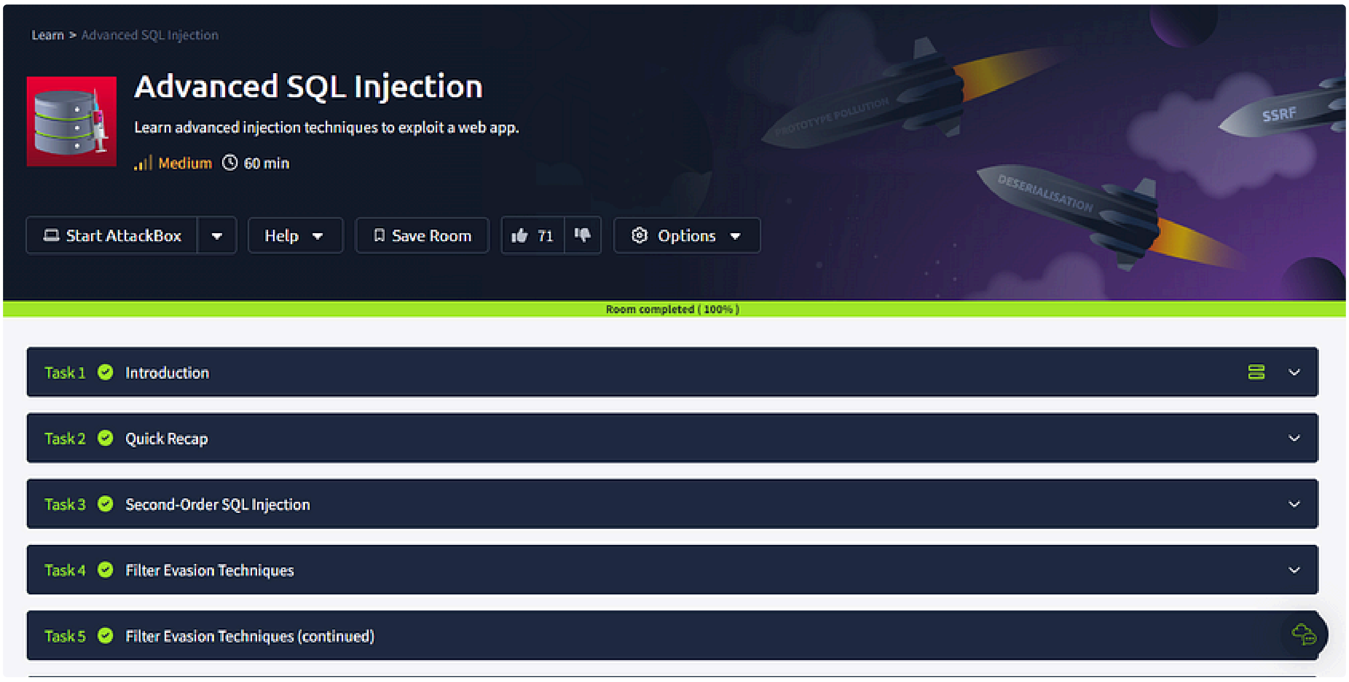
Send $300 worth of bitcoin to this address:

0xDK

Day 21: HELP ME...I'm REVERSE ENGINEERING! | Advent of Cyber 2024 | TryHackMe

Overview: Introduction to Reverse Engineering

Dec 21, 2024 1



Advanced SQL Injection

Learn advanced injection techniques to exploit a web app.

Task 1 Introduction

Task 2 Quick Recap

Task 3 Second-Order SQL Injection

Task 4 Filter Evasion Techniques

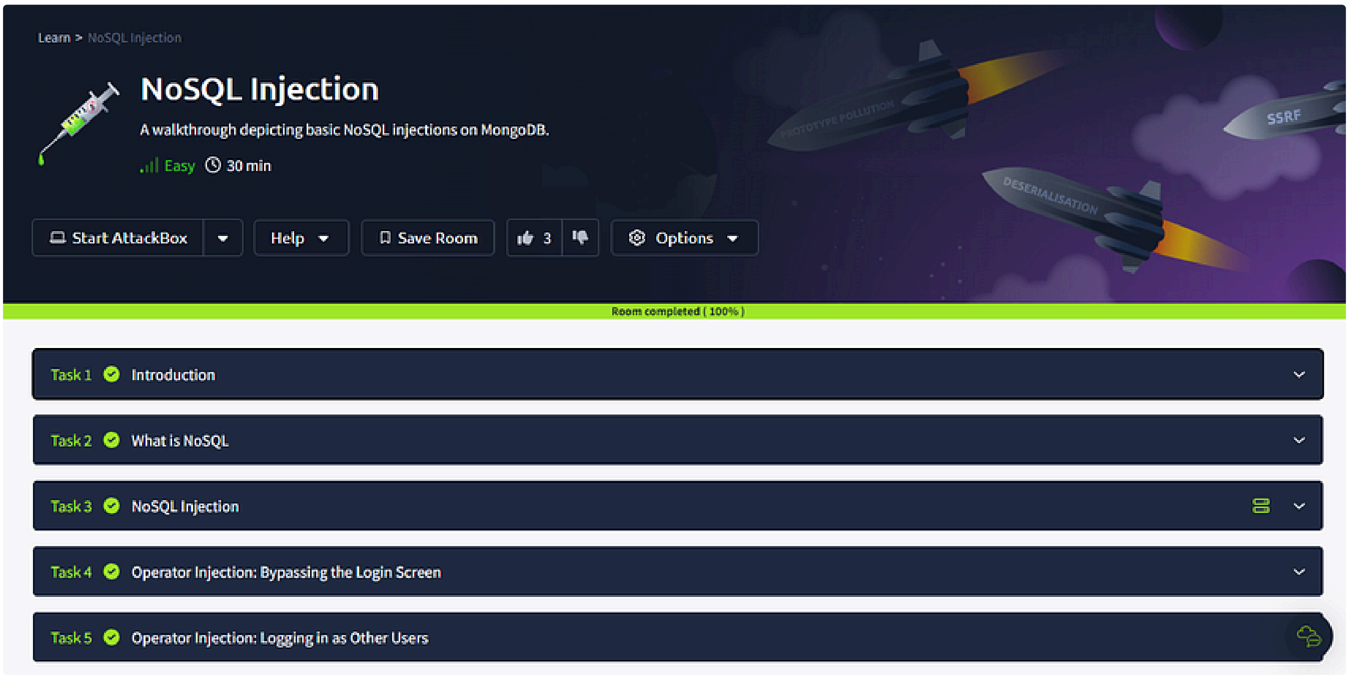
Task 5 Filter Evasion Techniques (continued)

0xDK

Advanced SQL Injection | TryHackMe

overview: TryHackMe's Advanced SQL Injection lab expands your SQL injection skillset by delving into advanced techniques that bypass common…

Jun 14, 2024 4



NoSQL Injection

A walkthrough depicting basic NoSQL injections on MongoDB.

Task 1 Introduction

Task 2 What is NoSQL

Task 3 NoSQL Injection

Task 4 Operator Injection: Bypassing the Login Screen

Task 5 Operator Injection: Logging in as Other Users

0xDK

NoSQL Injection | TryHackMe

overview: In this room, you will learn about NoSQL Injection. While SQL-based databases are a popular choice for data storage of web...

Jul 9, 2024 107

See all from 0xDK

Recommended from Medium

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60

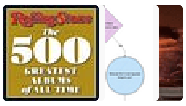
In InfoSec Write-ups by 0verlo0ked

THM Lo-Fi walkthrough

MODE : Easy

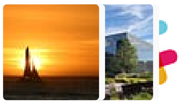
Jan 18 54 2

Lists



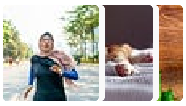
Staff picks

804 stories · 1587 saves



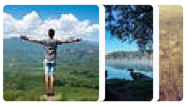
Stories to Help You Level-Up at Work

19 stories · 924 saves



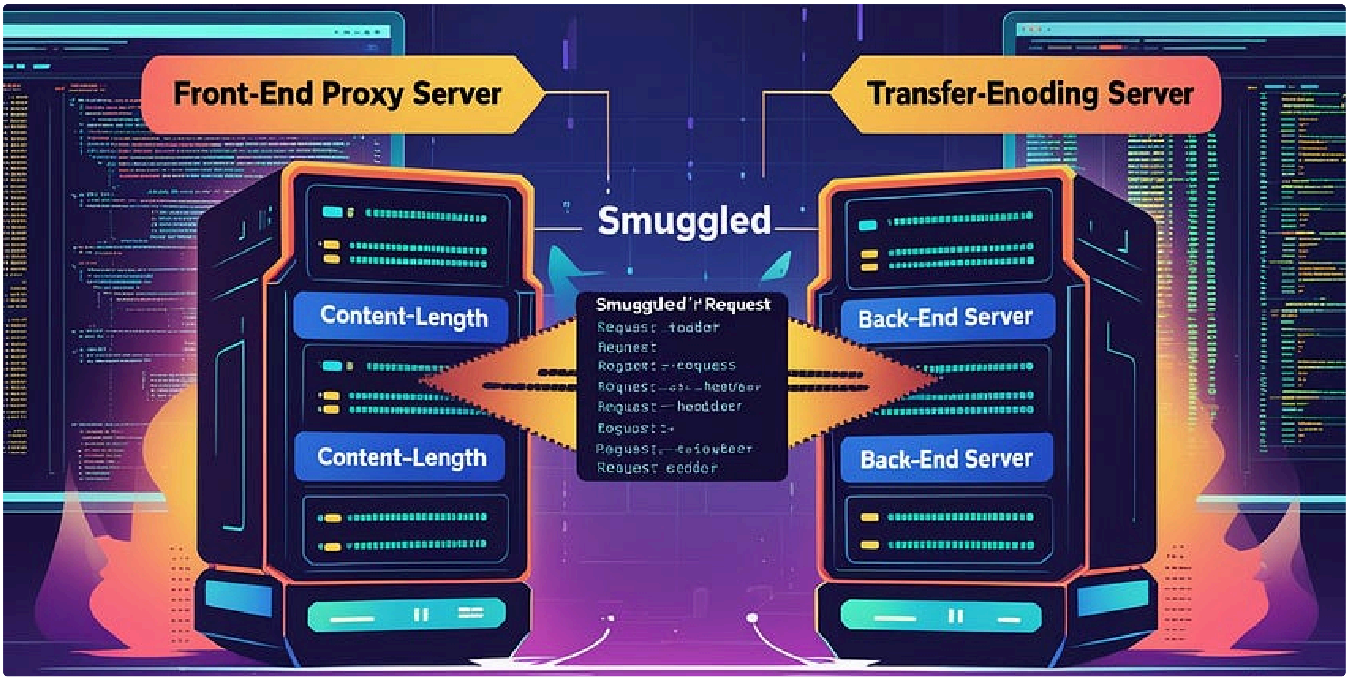
Self-Improvement 101

20 stories · 3240 saves



Productivity 101

20 stories · 2739 saves



CyferNest Sec

HTTP Request Smuggling | TryHackMe Walkthrough

TASK 2: Modern Infrastructure

Jan 5 1 1

Ansul Kotadia

Lo-Fi: TryHackMe Writeup.

Tackling the Lo-Fi TryHackMe room turned out to be a fascinating adventure! With a mix of curiosity and determination, I jumped right into…

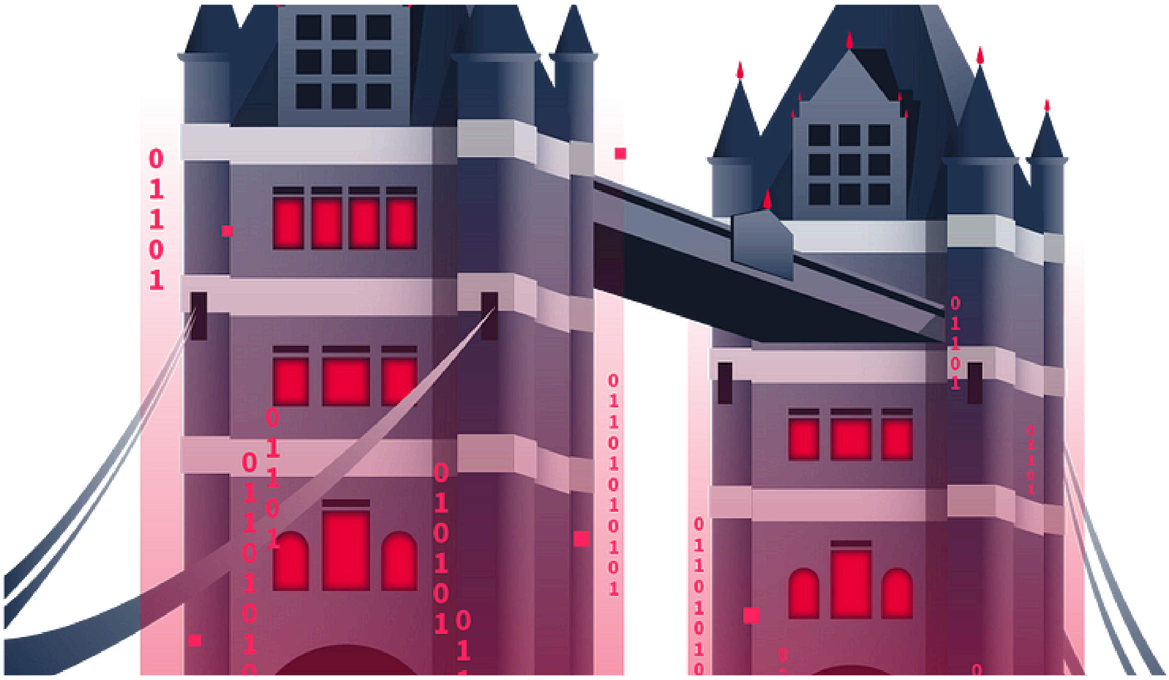
Jan 18 9 1

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



NTHSec

The London Bridge—TryHackMe CTF Walkthrough

Welcome to a medium-difficulty CTF challenge on TryHackMe! In this writeup, we'll walk through the steps taken to root this box, starting...

Oct 13, 2024 👏 3

See more recommendations