Race Conditions -Tryhackme Writeup

MAGESH · Following

3 min read · Jun 13, 2024

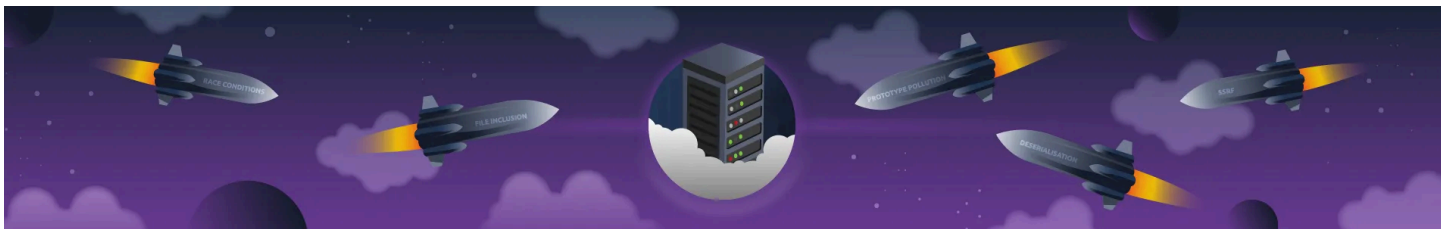(▶) Listen   (⬆) Share   (•••) More

Learn about race conditions and how they affect web application security

This is room is accessible only for subscribers, so if you wish to subscribe you can use this link and get $5 credits 💰 💵 *when you become a member.* https://tryhackme.com/signup?referrer=633819acb90069005f4fd623.

Link to the room https://tryhackme.com/r/room/raceconditionsattacks

Task 1:Introduction

Let's say we are tasked with testing the security of an online shopping web application. Many questions pop up. Can we reuse a single $10 gift card to pay for a $100 item? Can we apply the same discount to our shopping cart multiple times? The answer is *maybe*! If the system is susceptible to a race condition vulnerability, we can do all this and more.

This room introduces the race conditions vulnerability. A race condition is a situation in computer programs where the timing of events influences the behaviour and outcome of the program. It typically happens when a variable gets accessed and modified by multiple threads. Due to a lack of proper lock

mechanisms and synchronization between the different threads, an attacker might abuse the system and apply a discount multiple times or make money transactions beyond their balance.

Task 2:Multi-Threading

> *You downloaded an instruction booklet on how to make an origami crane. What would this instruction booklet resemble in computer terms?*

Ans: Program

> *What is the name of the state where a process is waiting for an I/O event?*

Ans: Waiting

Task 3:Race Conditions

> *Does the presented Python script guarantee which thread will reach 100% first? (Yea/Nay)*

Ans: nay

> *In the second execution of the Python script, what is the name of the thread that reached 100% first?*

Ans: Thread-1

Task 4:Web Application Architecture

> *How many states did the original state diagram of "validating and conducting money transfer" have?*

Ans: 2

> *How many states did the updated state diagram of "validating and conducting money transfer" have?*
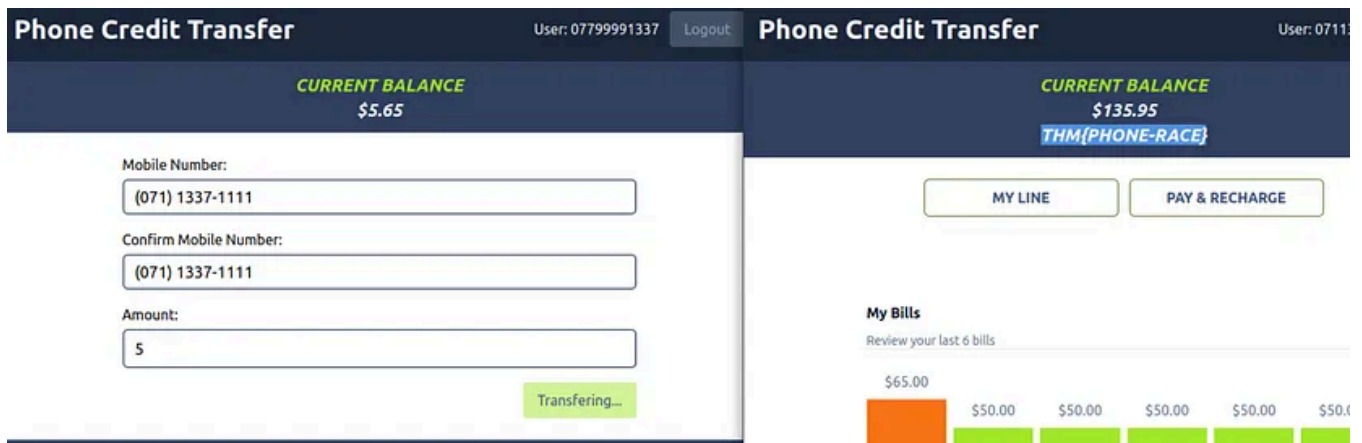
Ans: 3

> *How many states did the final state diagram of "validating coupon codes and applying discounts" have?*

Ans: 5

Task 5:Exploiting Race Conditions

> *You need to get either of the accounts to get more than $100 of credit to get the flag.*
> *What is the flag that you obtained?*

Ans: THM{PHONE-RACE}

Task 7:Challenge Web App

Challenge

Following what you have learned, it is time to attempt discovering and exploiting a race condition without guidance.

These are the credentials for the three users:

Name: Rasser Cond

- Username: `4621`

- Password: `blueApple`

Name: Zavodni Stav

- Username: `6282`

- Password: `whiteHorse`

Name: Warunki Wyscigu

- Username: `9317`

- **Password:** `green0range`

This web application belongs to a bank and allows clients to transfer online money. You need to get one of the accounts to amass more than **$1000**.

> *What flag did you obtain after getting an account's balance above $1000?*

Ans: THM{BANK-RED-FLAG}

I used two accounts to transfer amount to a single account, some request were successful and some failed.

THANK YOU FOR READING!!! ❤️ 💫

Following

Written by MAGESH

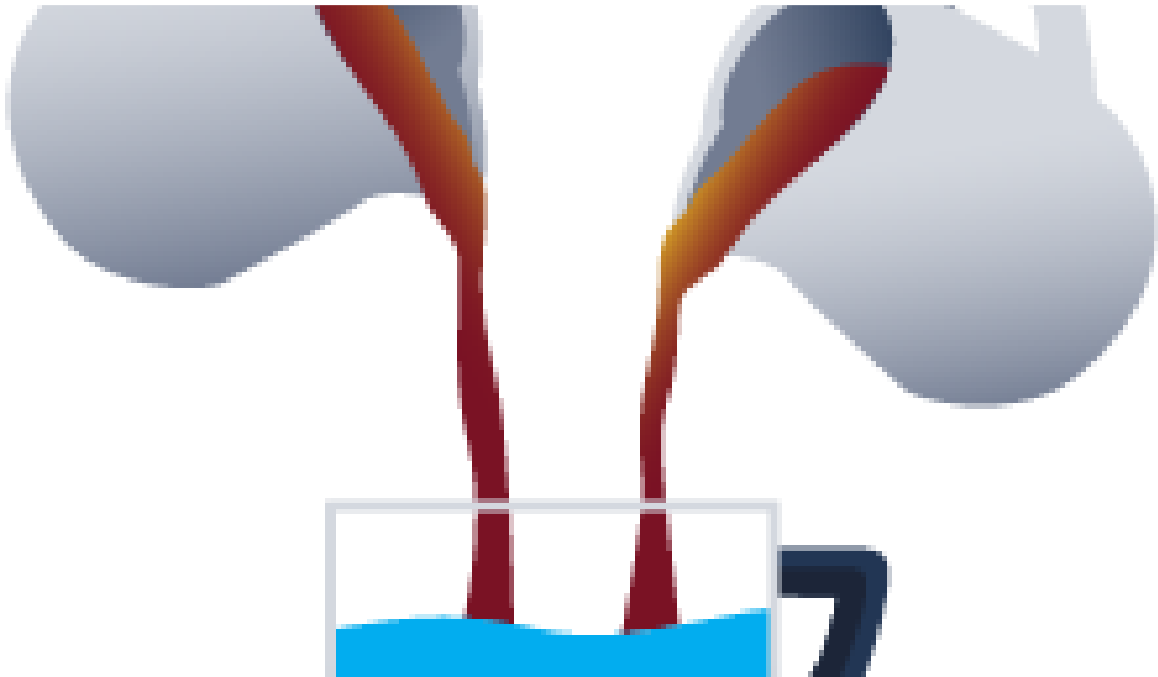40 Followers · 11 Following

Cybersecurity | Tryhackme

No responses yet

What are your thoughts?

Respond

More from MAGESH

MAGESH

Secret Recipe-Tryhackme Writeup

Perform Registry Forensics to Investigate a case.

Aug 21, 2024   👏 2

Medium

🔍 Search

Sep 5, 2024   👋 1

👤 MAGESH

Windows PowerShell-Tryhackme Writeup

Discover the "Power" in PowerShell and learn the basics.

Oct 23, 2024   👋 8

In System Weakness by MAGESH

Boogeyman 3-Tryhackme Writeup

The Boogeyman emerges from the darkness again.

Sep 2, 2024

See all from MAGESH

Recommended from Medium

In System Weakness by MAGESH

Boogeyman 3-Tryhackme Writeup

The Boogeyman emerges from the darkness again.

ents

	User Name	Name	Surname	Email
3	student1	Student1		stud
4	student2	Student2		stud
5	student3	Student3		stud
9	anatacker	Ana Tacker		
10	THM{Got.the.User}	X		
11	qweqwe	qweqwe		

‹‹   ‹   **1**   ›   ››

✅ embossdotar

TryHackMe — Session Management — Writeup

Key points: Session Management | Authentication | Authorisation | Session Management Lifecycle | Exploit of vulnerable session management...

✦   Aug 7, 2024   👋 27

🦅 CyferNest Sec

CSRF | TryHackMe Walkthrough

CSRF: The Art of Sneaky Online Mischief

Jan 3   👋 1   🔖⁺   •••

Lists

Staff picks

798 stories · 1566 saves

Stories to Help You Level-Up at Work
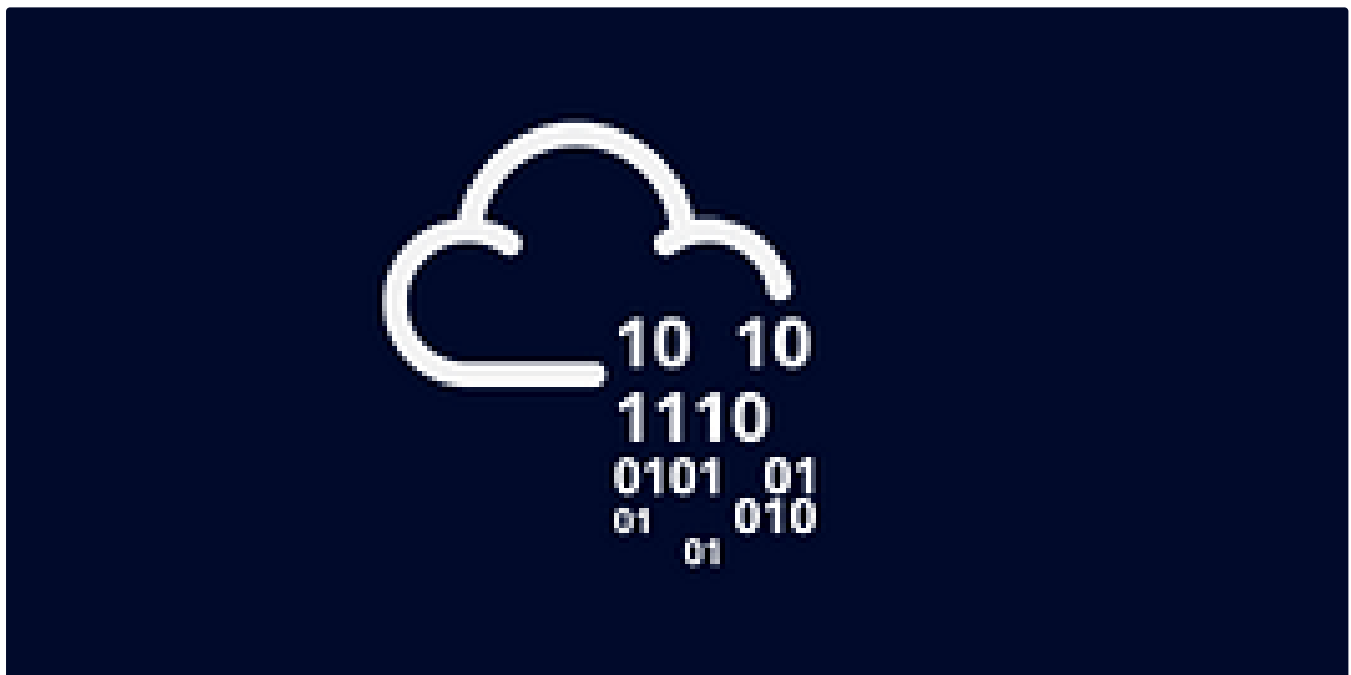
19 stories · 915 saves

Self-Improvement 101

20 stories · 3212 saves

Productivity 101

20 stories · 2714 saves

 In T3CH by Axoloth

TryHackMe | Deja Vu | WriteUp

Exploit a recent code injection vulnerability to take over a website full of cute dog pictures!

✦   Oct 13, 2024   👋 50   🔖⁺   •••

👤 MAGESH

TryHack3M: Subscribe-Tryhackme Writeup

This is room is accessible only for subscribers, so if you wish to subscribe you can use this link and get $5 credits 💰 💵 when you become...
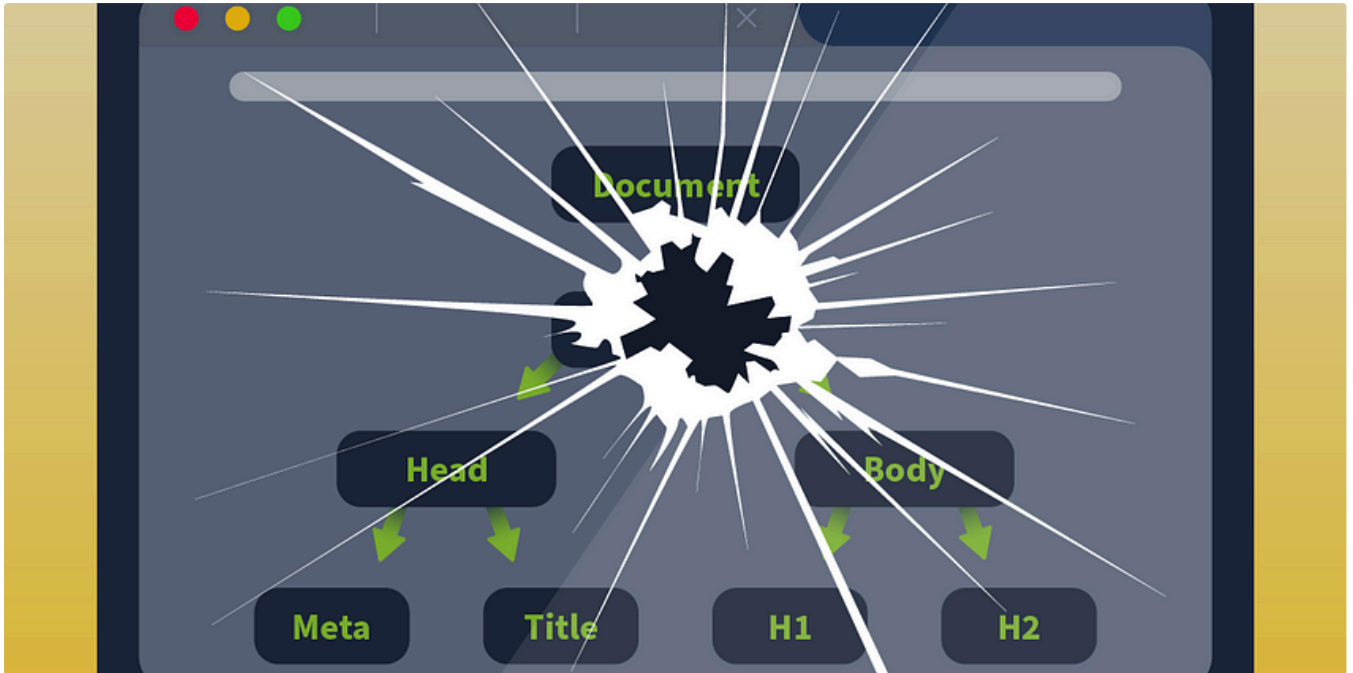
Sep 25, 2024 👏 1

👤 Abhijeet kumawat

Day 26 of 30 Day — 30 Vulnerabilities | Race Conditions

Day 26: Mastering Race Conditions — Essential Tricks & Techniques Based on Personal Experience and Valuable POCs

Jawstar

DOM-Based Attacks Tryhackme Write-up

Task 1 : Introduction

✦ Nov 20, 2024

See more recommendations