NAME: TERRENCE MACHOGU KEGENGO

EMAIL: [terrence.tech@proton.me](mailto:terrence.tech@proton.me)

WEDNESDAY 23RD JULY 2025

|  |
| --- |
| **H4K-IT CYBERSECURITY BOOTCAMP 2025 – CTF CHALLENGE REPORT** |

# Introduction

The H4K-IT Bootcamp Capture the Flag (CTF) Challenge, held from **July 17 to July 19, 2025**, was a practical, hands-on cybersecurity competition tailored for participants of **Cohort 3** of the H4K-IT Cybersecurity Bootcamp. The event simulated real-world cyber threats, requiring players to apply offensive and defensive skills to solve a series of security-related challenges across various domains such as Web Exploitation, Pentesting, Code Review (PPC), OSINT and Forensics.

This report documents my approach, methodologies, tools used, and key takeaways from the CTF. It aims to provide both a reflection of my problem-solving techniques and a technical breakdown of the challenges I tackled. Additionally, the report highlights how this CTF contributed to my growth as a cybersecurity practitioner, aligning with the bootcamp’s objective to produce industry-ready talent through immersive learning.

Table of Contents

[Introduction 2](#_Toc204146624)

[Detailed Walkthrough 4](#_Toc204146625)

[Challenge Summary 5](#_Toc204146626)

[Conclusion 6](#_Toc204146627)

# Detailed Walkthrough

# Challenge Summary

Over the course of the H4K-IT 2025 Cybersecurity Bootcamp CTF, I successfully tackled a wide array of challenges spanning across Web Exploitation, Pentesting, Code Review (PPC), OSINT, and Forensics. The instance tasks simulated realistic vulnerabilities drawn from SaaS platforms, banking systems, e-commerce logic, file upload pipelines, password recovery systems, and more.

I solved 51 questions, totaling 7475 points, through diverse attack vectors such as:

* IDOR and Broken Access Control (e.g., AI Solutions Portal, DevPortal, CorpDocs)
* Business Logic Flaws and Race Conditions (e.g., Pennies, The Royalties, Transfer Us)
* Code Injection and Upload Vulnerabilities (ScriptServe)
* Predictable Token Generation and Insecure Authentication (ResetRealm, Misunderstood)
* Server-Side Request Forgery (SSRF) (PDFVault)
* Weak Client-side Validation (Greek Gods)
* Log Analysis and Email Forensics (Memory Leak, PhishCheck, SSH Breach, Browser Trail)

Tools used included Gobuster, FFUF, curl, Nmap, browser DevTools, Python, and manual log/file inspection over SSH. I also simulated exploits using multithreading and local testing environments to recreate logic bugs.

This CTF tested not only my technical skills but also sharpened my methodical thinking, persistence, and real-world attack simulation mindset.

# Conclusion