

# CERTIFICATION JOURNEY

## TryHackMe AI Security (AI1)

What I expected • what I faced • what I would do differently

### FIELD NOTES

An honest review with public context



# A practical exam with a practical amount of friction

My experience in one sentence: the learning is valuable, but the delivery layer can become part of the challenge.

## VALUE

**Hands-on and  
scenario-based**

## TENSION

**Knowledge +  
navigation + stamina**

## TAKEAWAY

**Prepare for the  
platform, not just the  
topic**



EXPECTATIONS



REALITY



VERDICT

# What AI1 is designed to validate

The certification is positioned around attacking and defending real AI systems, not only recalling terminology.

## THE OFFICIAL PROMISE

**Prove you can  
attack and defend  
real AI systems.**

That framing matters: it makes the exam feel closer to an assessment workflow than a quiz.



# The shape of the challenge

Four numbers explain why this is different from a conventional multiple-choice certification.

**48**

hours

**4**

sections

**13**

hands-on scenarios

**6–8**

hours expected

01

Static sites

02

Live chatbots

03

Attack + defend

04

Submit under time

Browser-based • non-proctored • no local installation required

# What I expected to encounter

My mental model was narrower than the actual experience.

## I EXPECTED

- Pentesting AI systems
- Prompt injection and related attacks
- Some practical remediation
- A mostly technical challenge

## I DID NOT FULLY ANTICIPATE

- Scenario switching
- Platform/UI variation
- Submission details
- Time lost to friction

# Where the experience delivered

The strongest part was the conversion of theory into a repeatable assessment mindset.

1

## Hands-on

Theoretical concepts are attached to practical scenarios.

2

## Assessment mindset

You leave with a clearer way to interrogate an AI system.

3

## Learning loop

The exam forces you to show that the lessons stuck.

4

## Feedback culture

TryHackMe appears willing to listen and iterate.

# When the platform becomes part of the exam

A time-boxed practical exam amplifies small usability issues.

## THE BAD

- 48 hours sounds generous until you realizing you have a lot less
- Boxes can break or behave inconsistently
- You can arrive technically capable but operationally underprepared

## THE UGLY

- Room interfaces are not always consistent
- Small controls can be easy to miss
- A retake may mean restarting a long, timed experience

# Beginner-friendly content? Not sure about that

The training may welcome newcomers, but the exam rewards security maturity and calm execution.



**Best fit: someone ready to combine AI security fundamentals with hands-on testing habits.**

# Prepare for the exam you will actually sit

My practical recommendations, based on the gap between expectation and reality.

01

**Learn the concepts**

Do not memorise payloads without understanding the failure mode.

---

02

**Practise the workflow**

For every scenario: observe, test, capture evidence, explain impact.

---

03

**Rehearse the platform**

Get comfortable with browser labs, room navigation, and note-taking.

---

04

**Protect your mood**

Do not let one broken path consume the attempt.

---

05

**Plan your restart**

Keep structured notes so a retake is not a total reset.

# Would I recommend it?

Maybe with the right expectations.

## MY VERDICT

**Worth doing if you want practical AI security exposure.**

Go in expecting a blended assessment: threat modeling, security knowledge, hands-on testing.

Learning value



Practicality



Operational friction



What materials prepare you for



# Public context used in this deck

01

## TryHackMe — AI Security (AI1) Certification

<https://tryhackme.com/certification/ai-security/>

02

## TryHackMe Customer Hub — AI1 Exam Guide

<https://help.tryhackme.com/en/articles/15301082-ai1-exam-guide>

03

## TryHackMe Customer Hub — AI1 Training Content

<https://help.tryhackme.com/en/articles/15300494-ai1-training-content>