DEMYSTIFYING BUG BOUNTY

: What I Learned from My Journey as an Independent Researcher

Tan See Jou - @pinkmeimei

INTRODUCTION

Tan See Jou - a.k.a pinkmeimei

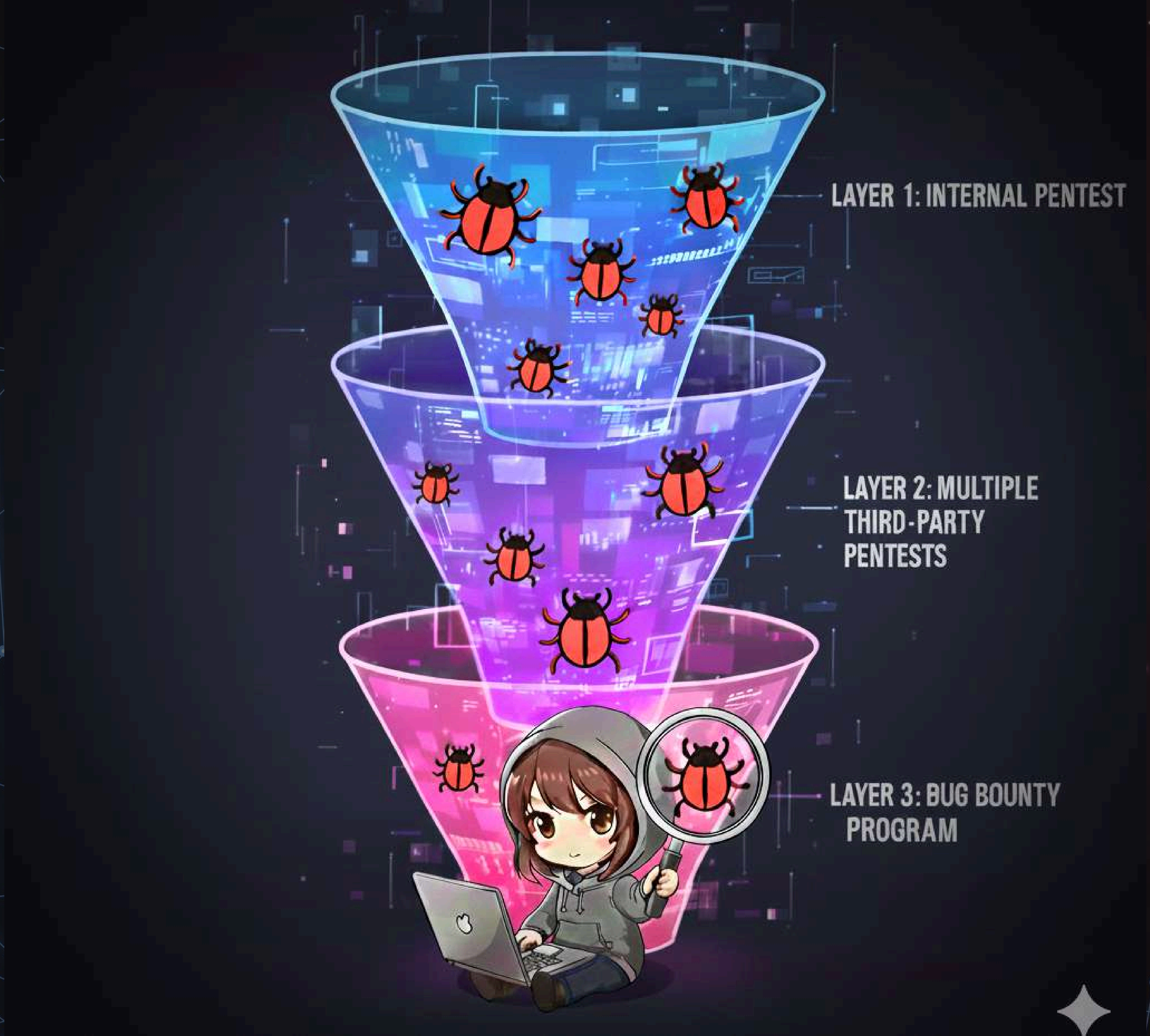
- Bachelor of Computer Science (Graphics & Multimedia Software) : University Technology Malaysia (UTM)
- Independent CyberSecurity Researcher, Ethical Hacker
- HackerOne's Hacker Advisory Board member 2025-2026
- 1st in HackerOne MY leaderboard 2023, 2024, 2025, so far :)

GOAL

demystify bug bounty, inspire, encourage

WHAT IS BUG BOUNTY?

- a program where companies reward security researchers for finding and reporting valid vulnerabilities
- purpose: discover bugs missed by internal teams and fix security bugs before attackers exploit them
- conducted under legal permission & defined scope provided by the company
- researcher follow responsible disclosure guidelines & program rules to report bugs ethically
- run internally by companies or managed on platforms like HackerOne, Bugcrowd, Intigriti and ...



LAYER 1: INTERNAL PENTEST

LAYER 2: MULTIPLE THIRD-PARTY PENTESTS

LAYER 3: ĐUG BOUNTY PROGRAM

BBP - VDP

BBP [Bug Bounty Program] - VDP [Vulnerability Disclosure Program]

- Both allow responsible & safe reporting
- VDP usually has no reward
- BBP rewards incentive - money, swags

THE FULL FLOW OF BUG BOUNTY

Not just finding bugs!

i. Find a vulnerability

ii. Writing a report

iii. Triage Team Review { managed program }

iv. Program Internal Team Review

v. Final Decision

THE FULL FLOW OF BUG BOUNTY

Not just finding bugs!

i. Find a vulnerability

ii. Writing a report

iii. Triage Team Review { managed program }

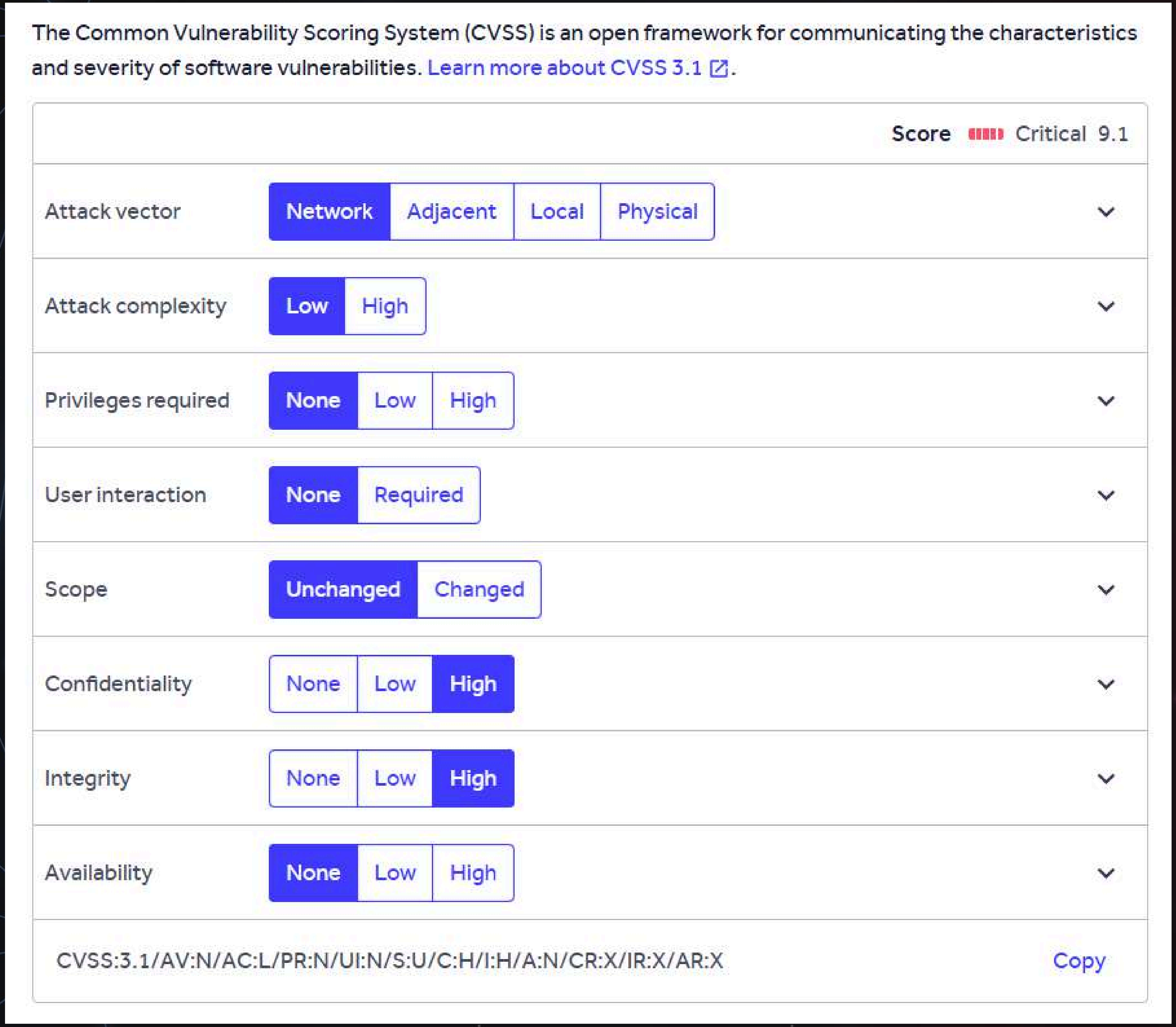
iv. Program Internal Team Review

v. Final Decision

WHAT IS CONSIDERED A VULNERABILITY?

- an issue that goes against the intended security design and business rule
- can be abused to break confidentiality, integrity, and availability
- Common Vulnerability Scoring System (CVSS) - a industry-standard calculator used to determine the severity of a vulnerability
- BBP is impact-based

https://www.first.org/cvss/v3-1/specification-document



The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. Learn more about CVSS 3.1.

Score Critical 9.1

Attack vector [✓ Network] Adjacent Local Physical

Attack complexity [✓ Low] High

Privileges required [✓ None] Low High

User interaction [✓ None] Required

Scope [✓ Unchanged] Changed

Confidentiality None Low [✓ High]

Integrity None Low [✓ High]

Availability [✓ None] Low High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/CR:X/IR:X/AR:X

I. FIND A VULNERABILITY

- understand the business model of the target, what is important to them
- research, explore the application
- identify a security-impacting issue

THE FULL FLOW OF BUG BOUNTY

Not just finding bugs!

i. Find a vulnerability

ii. Writing a report

iii. Triage Team Review { managed program }

iv. Program Internal Team Review

v. Final Decision

II. WRITING A REPORT

- detail step-by-step reproduction steps
- include impact

THE FULL FLOW OF BUG BOUNTY

Not just finding bugs!

i. Find a vulnerability

ii. Writing a report

iii. Triage Team Review { managed program }

iv. Program Internal Team Review

v. Final Decision

III. TRIAGE TEAM REVIEW

- triage team will check if
  - is the vulnerability is in scope ?
  - is the vulnerability valid ?
  - is it reproducible ?
  - is it not a duplicate of earlier reports by other researchers (including if the vulnerability originates from the same root cause) ?
- set the severity for the vulnerability

THE FULL FLOW OF BUG BOUNTY

Not just finding bugs!

i. Find a vulnerability

ii. Writing a report

iii. Triage Team Review { managed program }

iv. Program Internal Team Review

v. Final Decision

III. PROGRAM INTERNAL TEAM REVIEW

- program team will verify on their side
  - if it is a valid vulnerability or is intended behaviour ?
  - if it is a duplicate with internal testing ?
  - if this vulnerability shared the same root cause as other earlier submitted reports
  - whether the impact is as stated (severity status may be changed)

THE FULL FLOW OF BUG BOUNTY

Not just finding bugs!

i. Find a vulnerability

ii. Writing a report

iii. Triage Team Review { managed program }

iv. Program Internal Team Review

v. Final Decision

V. FINAL DECISION

- program team will make the decision
  - if valid → rewards
  - if severity is debated → more communication, show impact is needed
  - If is invalid/duplicate/informative/out of scope → report closed, no reward

MY JOURNEY

Phase 1 :
Learning the Fundamentals

Phase 2 :
First Hands-On
&
First Paid Bug

Phase 3 :
Improve Skills & Growing Confidence

Phase 4 :
Developed Methodology & Hunting Style

MY JOURNEY

Phase 1 : Learning the Fundamentals

Phase 2 : First Hands-On & First Paid Bug

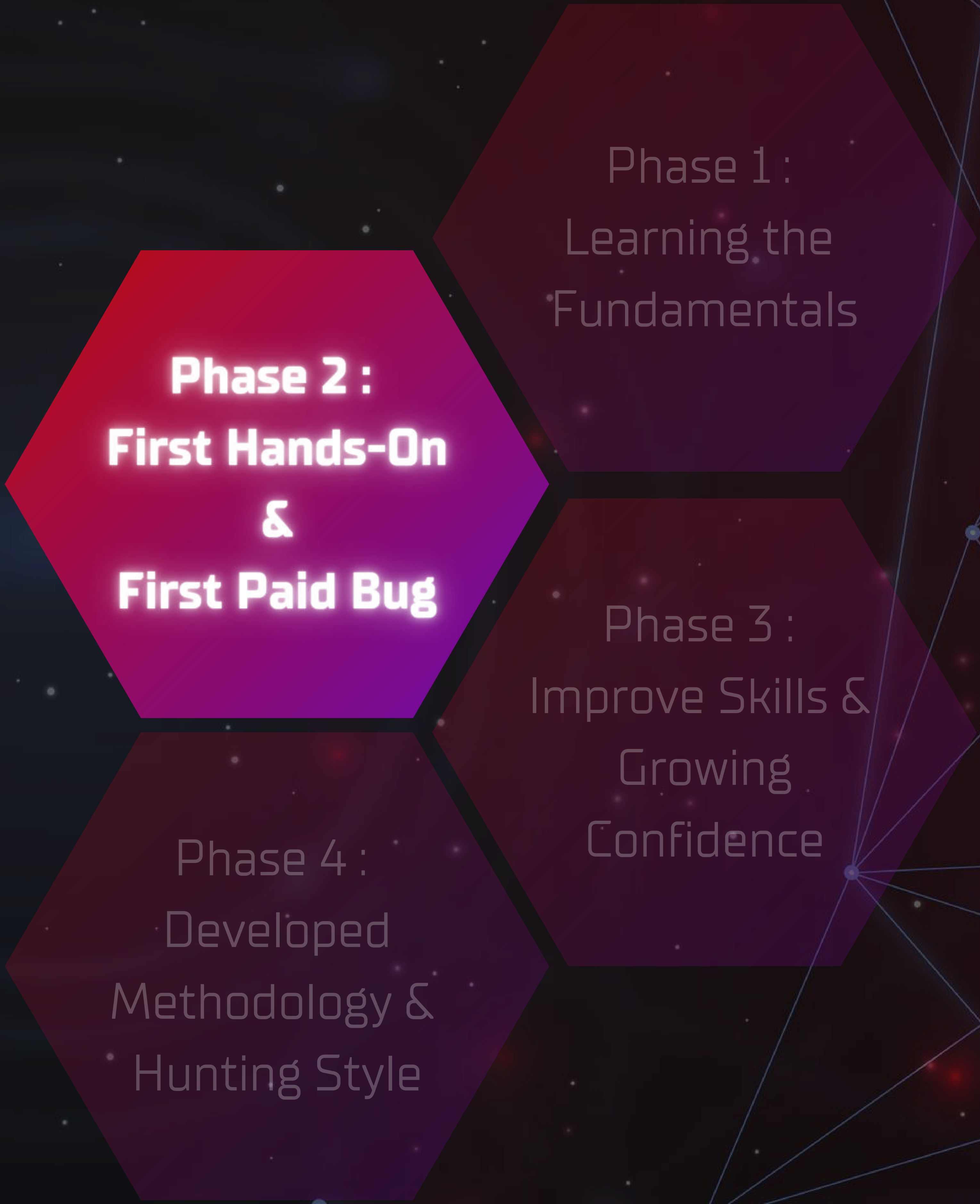
Phase 3 : Improve Skills & Growing Confidence

Phase 4 : Developed Methodology & Hunting Style

LEARNING THE FUNDAMENTALS

- Focus fully on learning web security concepts & vulnerability types
- Resources:
    - Web application Hacker's Handbook (WAHH)
    - Portswigger Web Academy Labs - *https://portswigger.net/web-security*
    - reading write-ups, research blogs
    - watching YouTube: @InsiderPhD , @RanaKhalil101 , @NahamSec , @BugBountyReportsExplained
- get familiar with Burp Proxy
- Involve my everyday life with cybersecurity

MY JOURNEY



Phase 1 : Learning the Fundamentals

Phase 2 : First Hands-On & First Paid Bug

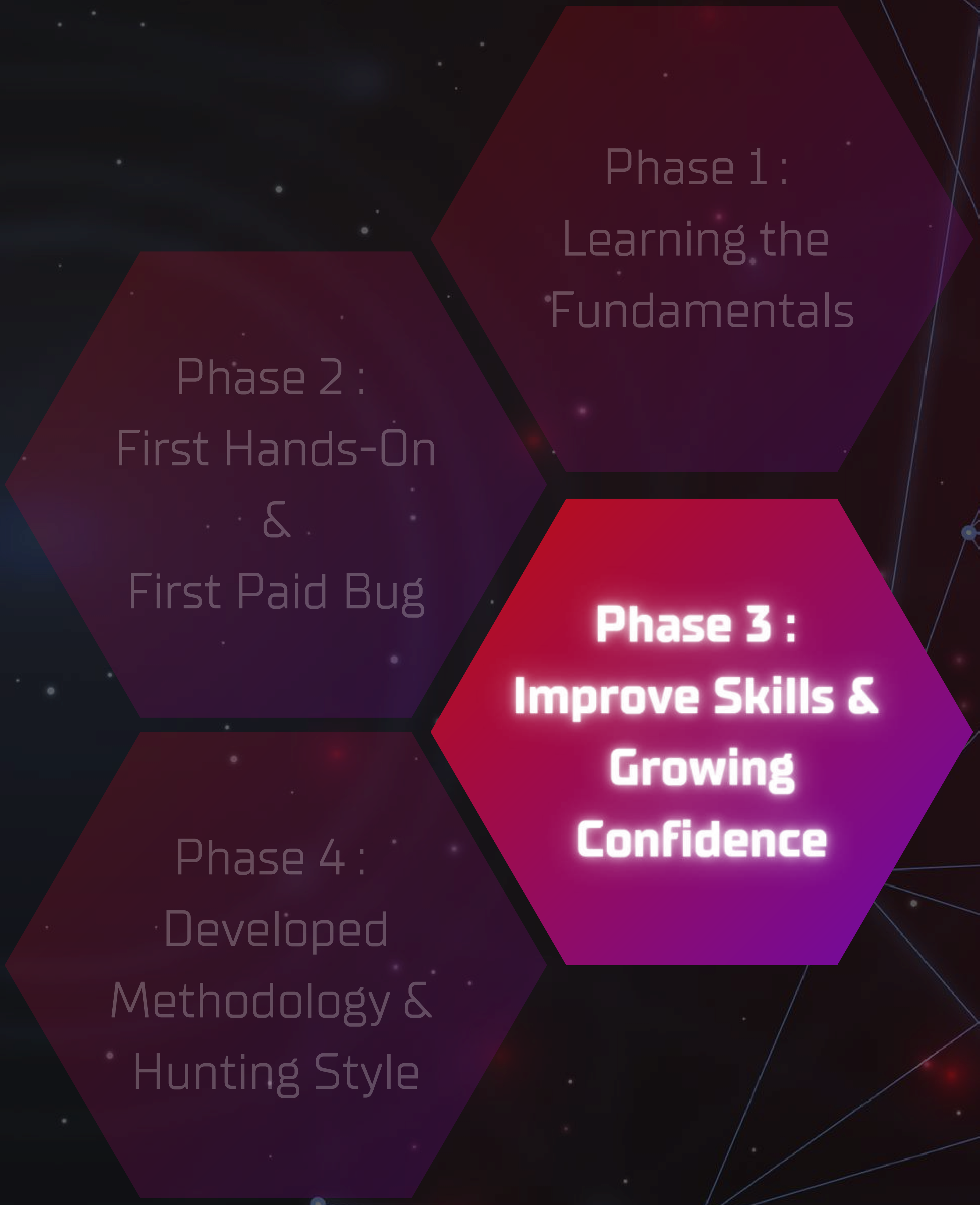
Phase 3 : Improve Skills & Growing Confidence

Phase 4 : Developed Methodology & Hunting Style

FIRST HANDS-ON & FIRST PAID BUGS

- After ~4 months of learning, I started hunting in a small-scoped e-commerce program
- First paid bug: payment bypass (checkout any item for $ 0.10)~ rated Critical
- Learn the importance of
  - Don't assume, validate it! (real system still have "old classic" bugs)
  - Try simple things, even if they feel "too obvious"

MY JOURNEY



Phase 1 : Learning the Fundamentals

Phase 2 : First Hands-On & First Paid Bug

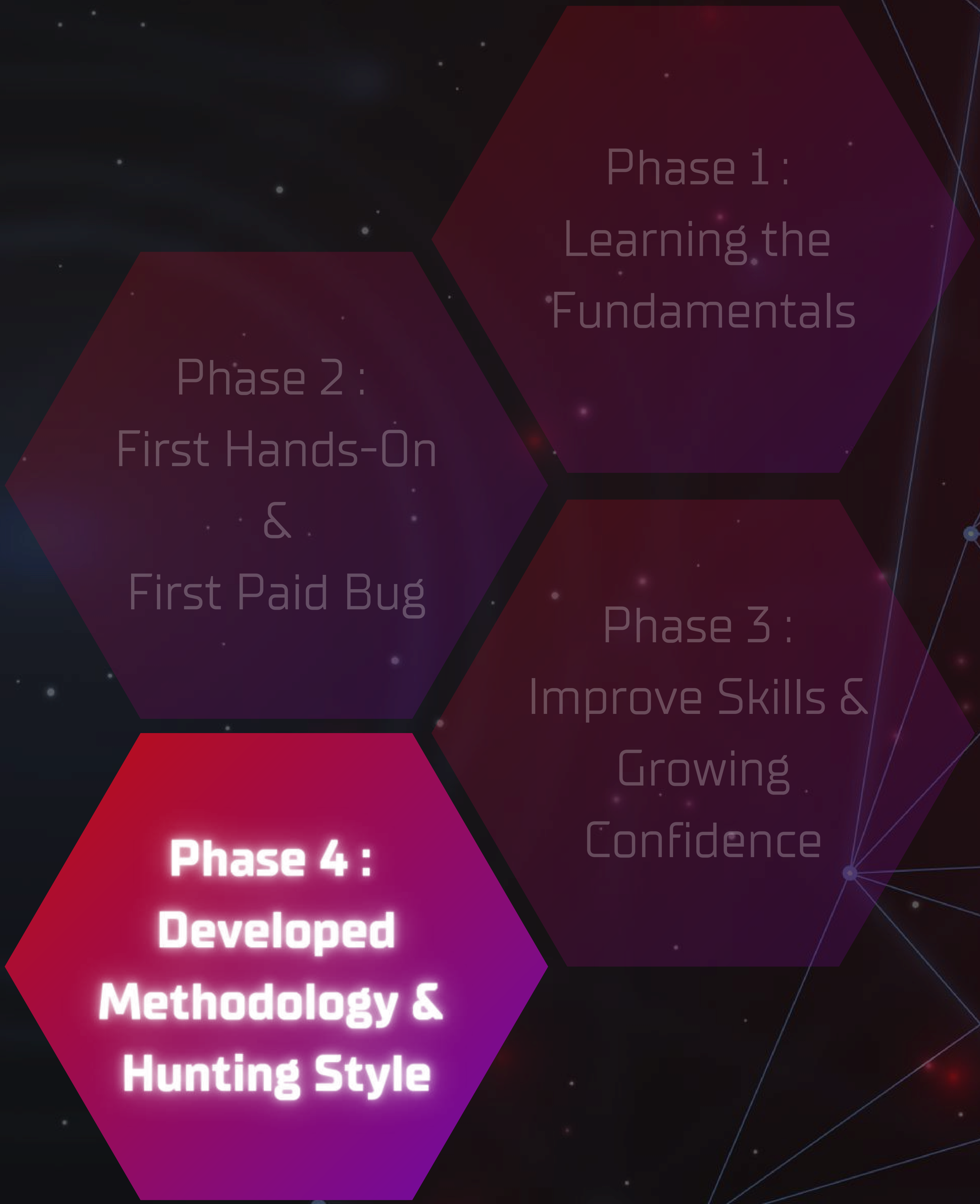
Phase 3 : Improve Skills & Growing Confidence

Phase 4 : Developed Methodology & Hunting Style

IMPROVE SKILLS & GROWING CONFIDENCE

- still lacked confidence - only targeted medium-sized programs
- still believing “smaller program = less competitive = high chance to find bug” (not always true)
- When stuck → go back to the learning cycle
    - study new vuln types
    - completing more labs (PortSwigger, TryHackMe)
    - writing write-ups to reinforce understanding
- Focus on understanding why a payload works

MY JOURNEY



Phase 1 : Learning the Fundamentals

Phase 2 : First Hands-On & First Paid Bug

Phase 3 : Improve Skills & Growing Confidence

Phase 4 : Developed Methodology & Hunting Style

DEVELOPED METHODOLOGY & HUNTING STYLE

- realised it's impossible to master every technology → learn along the way
- developed own hunting style and methodology: hacking in depth
- understand features & endpoint thoroughly
- write detailed notes about the target
  - interesting endpoints
  - useful responses
  - potential chains
- chain small findings into a bigger impact; focus on high-impact vulnerability
- dive deeper than others hunter → find what they missed, or have not reached
- I started to hunt in big programs despite heavy competition

LAST WORDS

- Focus on learning, not just bounty. With enough time and experience, valuable vulns and bounties will come.
- Always respect the program scope and rules
- Always write detailed reports, communicate patiently, politely, and professionally.
- You don't need to be an expert to start, you just need to start. Keep learning and sharpening your skills along the way.
- Everyone can start from zero and grow with persistence and dedication
- Bug bounty can be stressful and sometimes overwhelming. Don't focus on others, cherish your every win and enjoy the journey.

RESOURCES

https://portswigger.net/web-security

https://tryhackme.com/

Youtube:

@InsiderPhD

@RanaKhalil101

@NahamSec

@BugBountyReportsExplained

https://www.criticalthinkingpodcast.io/

THANK YOU