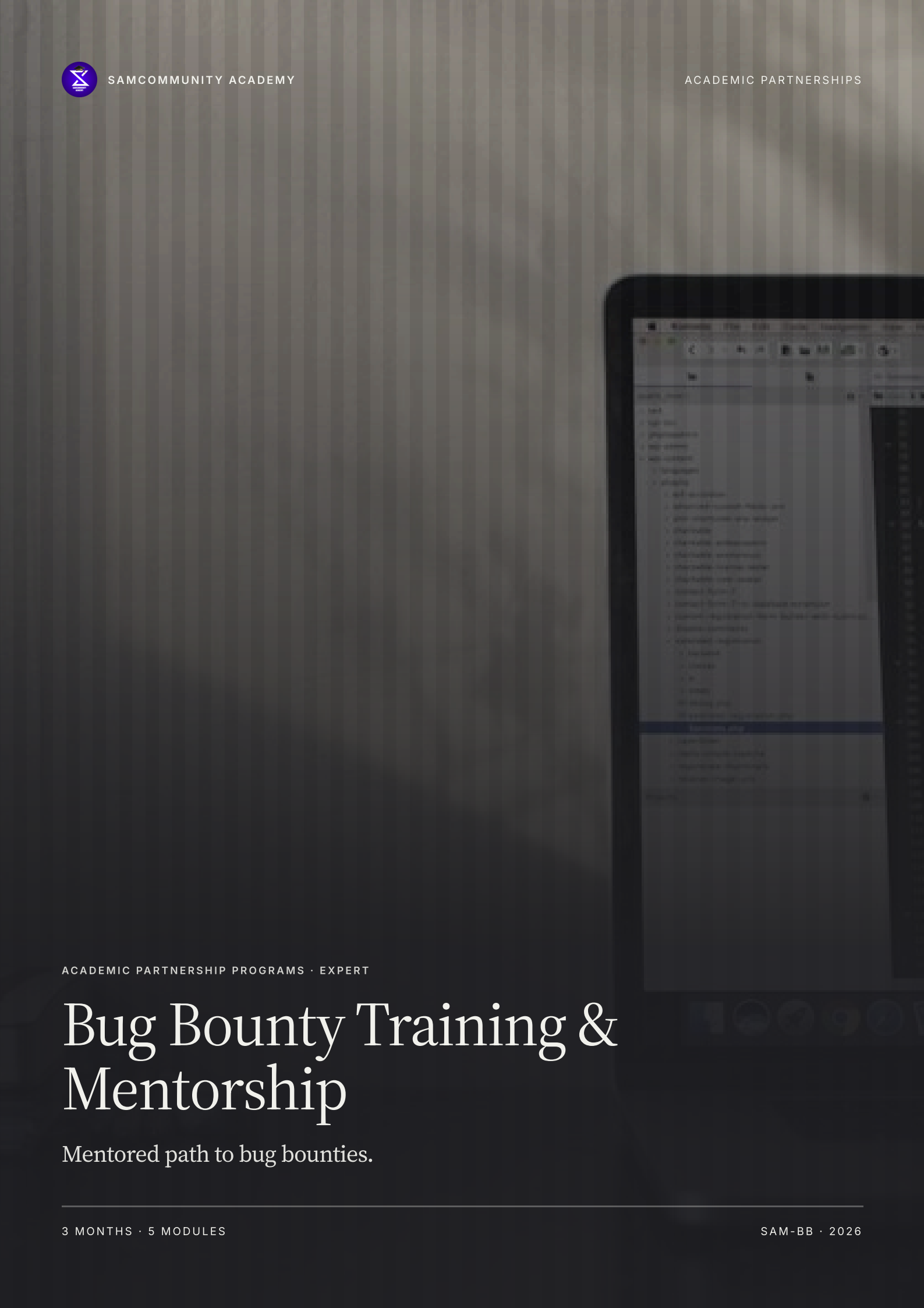


ACADEMIC PARTNERSHIP PROGRAMS · EXPERT

Bug Bounty Training & Mentorship

Mentored path to bug bounties.

Contents

Why this program 03

Who it's for 04

Learning outcomes 05

Program runway 06

Detailed curriculum 07

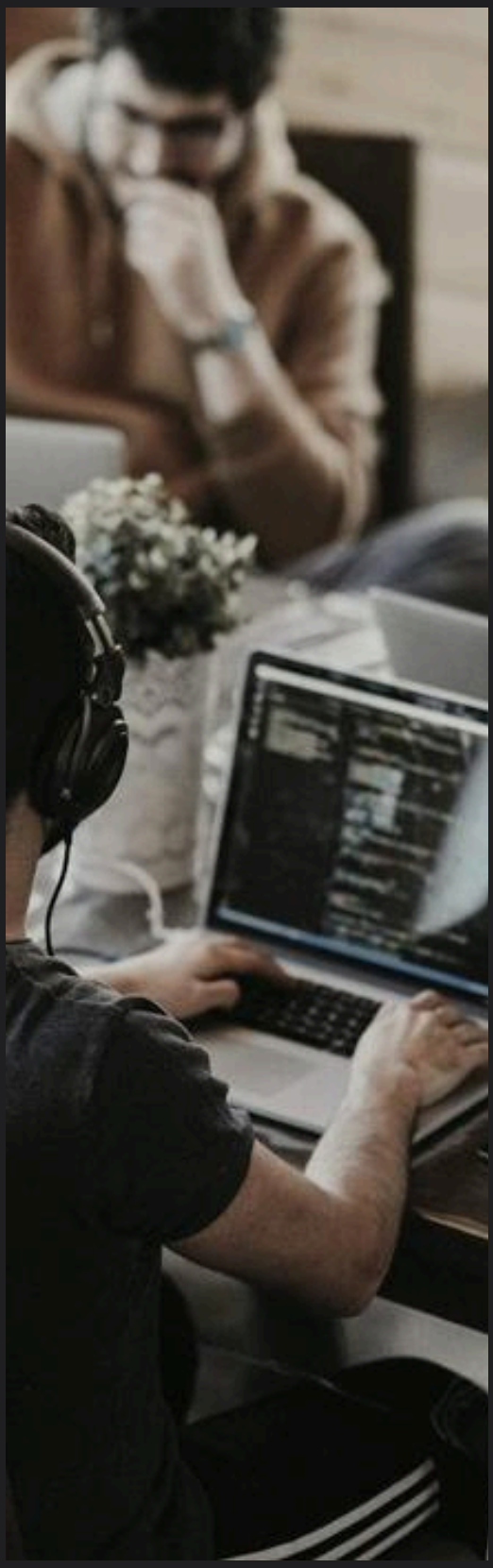
Frameworks & tools 09

Projects & capstone 10

Certification & method 11

Learning path 12

FAQs 13

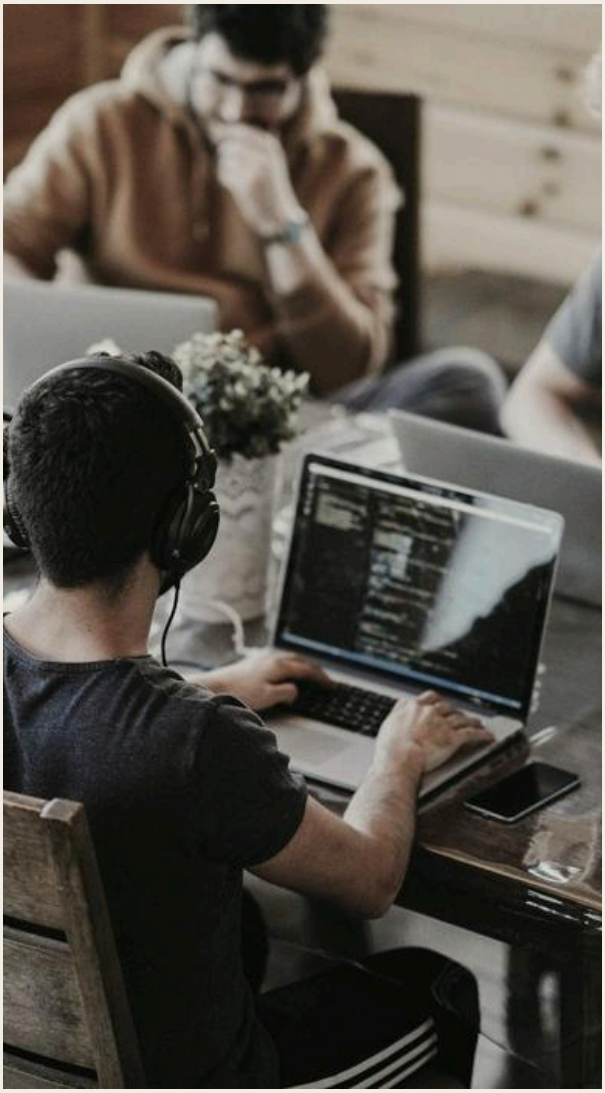


LEVEL	Expert
DURATION	3 Months
MODULES	5
CERTIFICATE	SAM-BB

Why this program

Guided bug bounty training and mentorship for students.

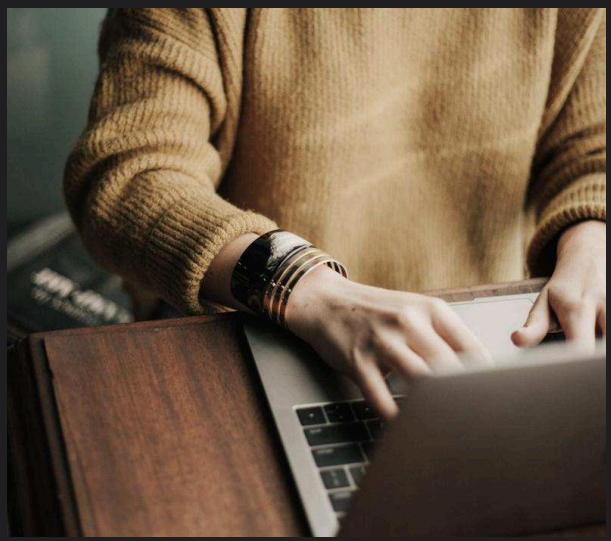
Bug bounty programs let organisations improve their security by inviting researchers to report vulnerabilities responsibly. This mentored program prepares students to take part ethically and effectively, covering web fundamentals, program rules and scope, testing methodology with Burp Suite, OWASP vulnerability classes practised in intentionally vulnerable labs, and clear reporting and responsible disclosure, before guided participation in suitable public programs.



3
months of compact, practical sessions

5
focused modules, built around real work

3
projects plus a capstone presentation



Who this program is for



01

Vice-chancellors & deans

CoE, curriculum and accreditation support

02

Training & placement cells

Certification and placement readiness

03

Faculty

Faculty development programs

04

Top-tier students

Research internships, CTF academy, incubation

PREREQUISITES

- Strong understanding of web technologies and HTTP
- Comfort with Linux and basic scripting
- Prior web security coursework or CTF experience

DESIGNED FOR

- Bug bounty researchers
- Application security analysts
- Web penetration testers in authorised engagements
- Vulnerability triage analysts
- Product security engineers

What you'll be able to do.

01 Interpret bug bounty program rules, scope and safe harbour terms

02 Apply a structured web testing methodology using Burp Suite

03 Identify OWASP vulnerability classes in intentionally vulnerable applications

04 Assess severity accurately using CVSS and demonstrated business impact

05 Write clear, reproducible vulnerability reports for triage teams

06 Follow responsible disclosure practices on legal, in-scope targets

How the program works

Weeks 1–2: Web Fundamentals and Ethics

HTTP, cookies and sessions, Web application architecture, Program rules and scope, Legal boundaries and safe harbour.

Weeks 3–4: Tooling and Methodology

Burp Suite fundamentals, Mapping application functionality, Testing methodology checklists, Note-taking and evidence capture.

Weeks 5–8: OWASP Vulnerability Classes

OWASP Top 10 overview, Access control weaknesses, Injection vulnerability concepts, Authentication and session issues.

Weeks 9–10: Reporting and Disclosure

Writing clear vulnerability reports, Severity rating with CVSS, Demonstrating impact responsibly, Responsible disclosure process.

01 · Weeks 1–2: Web Fundamentals and Ethics

02 · Weeks 3–4: Tooling and Methodology

03 · Weeks 5–8: OWASP Vulnerability Classes

04 · Weeks 9–10: Reporting and Disclosure

05 · Weeks 11–12: Mentored Program Participation

★ Capstone · Mentored Bug Bounty Engagement



The curriculum

MODULES 01–03

01 Weeks 1–2: Web Fundamentals and Ethics

Practical: Set up a personal lab and review scope rules of three public programs

Kali Linux Linux

- HTTP, cookies and sessions
- Web application architecture
- Program rules and scope
- Legal boundaries and safe harbour
- Lab setup with Kali Linux

02 Weeks 3–4: Tooling and Methodology

Practical: Map an intentionally vulnerable application's features and attack surface using Burp Suite

Burp Suite

- Burp Suite fundamentals
- Mapping application functionality
- Testing methodology checklists
- Note-taking and evidence capture
- Scope discipline

03 Weeks 5–8: OWASP Vulnerability Classes

Practical: Practise identifying access control flaws in an intentionally vulnerable training application

OWASP

- OWASP Top 10 overview
- Access control weaknesses
- Injection vulnerability concepts
- Authentication and session issues
- Business logic flaws



Curriculum, continued

MODULES 04–05

04 Weeks 9–10: Reporting and Disclosure

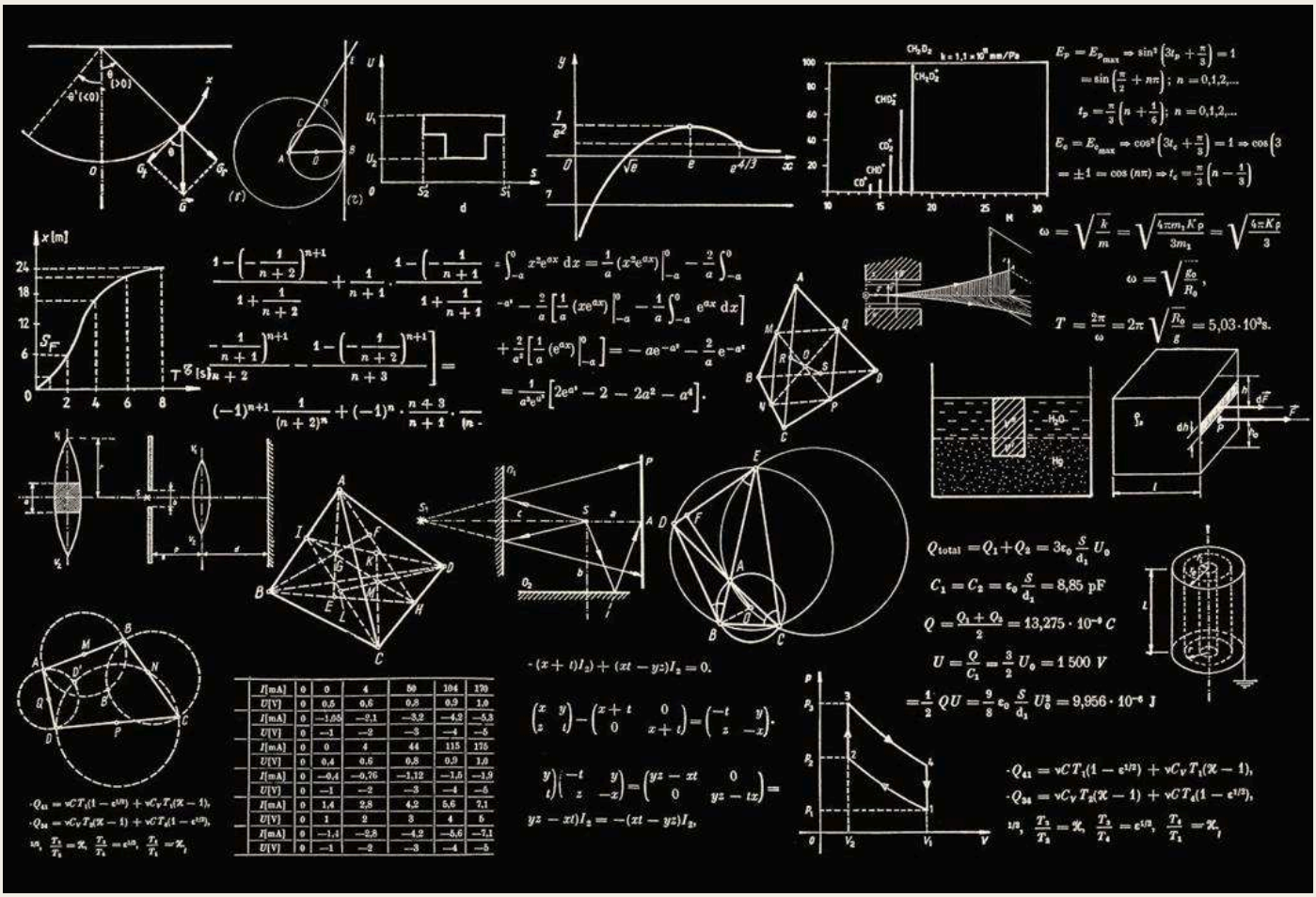
Practical: Write a complete vulnerability report for a lab finding and peer review it

- Writing clear vulnerability reports
- Severity rating with CVSS
- Demonstrating impact responsibly
- Responsible disclosure process
- Communicating with triage teams

05 Weeks 11–12: Mentored Program Participation

Practical: Test an in-scope public program under mentor review and document findings

- Choosing suitable public programs
- Mentor-reviewed testing plans
- Avoiding duplicates and noise
- Building researcher reputation
- Continuous learning plan



What you'll focus on.

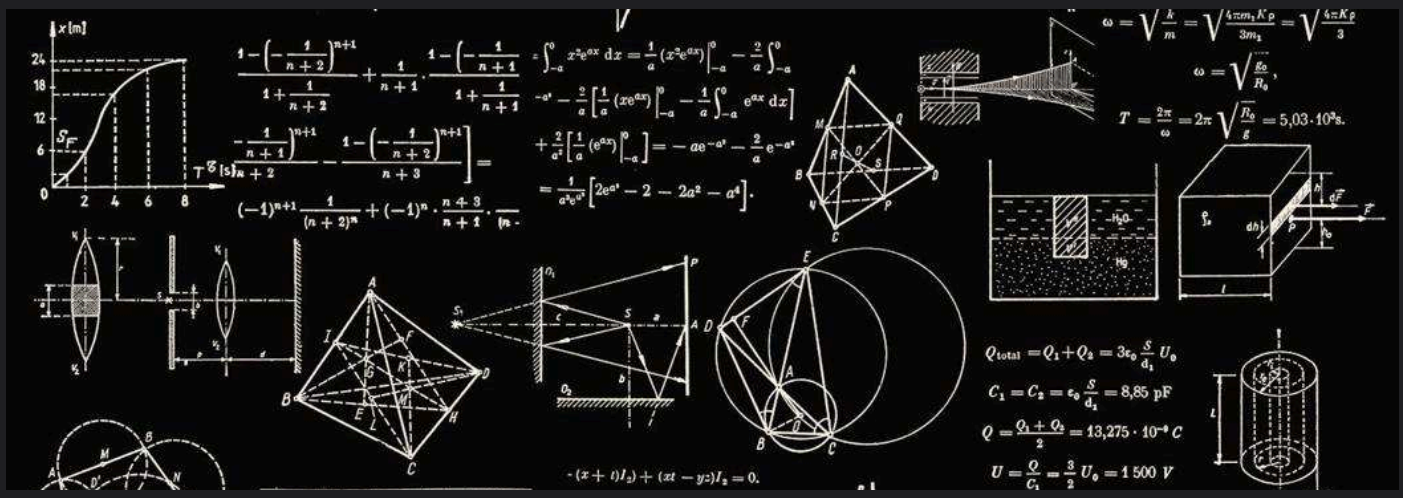
OWASP 01

Weeks 1–2: Web Fundamentals and Ethics 02

Weeks 3–4: Tooling and Methodology 03

Weeks 5–8: OWASP Vulnerability Classes 04

Weeks 9–10: Reporting and Disclosure 05



Burp Suite
Web app security testing

OWASP
Top 10 & testing standards

Kali Linux
Security testing distribution

Linux
Server & CLI fundamentals

Projects & capstone

01

Lab Vulnerability Portfolio

Identify and document vulnerabilities across OWASP categories in intentionally vulnerable labs, with reproduction steps, impact and remediation advice.

02

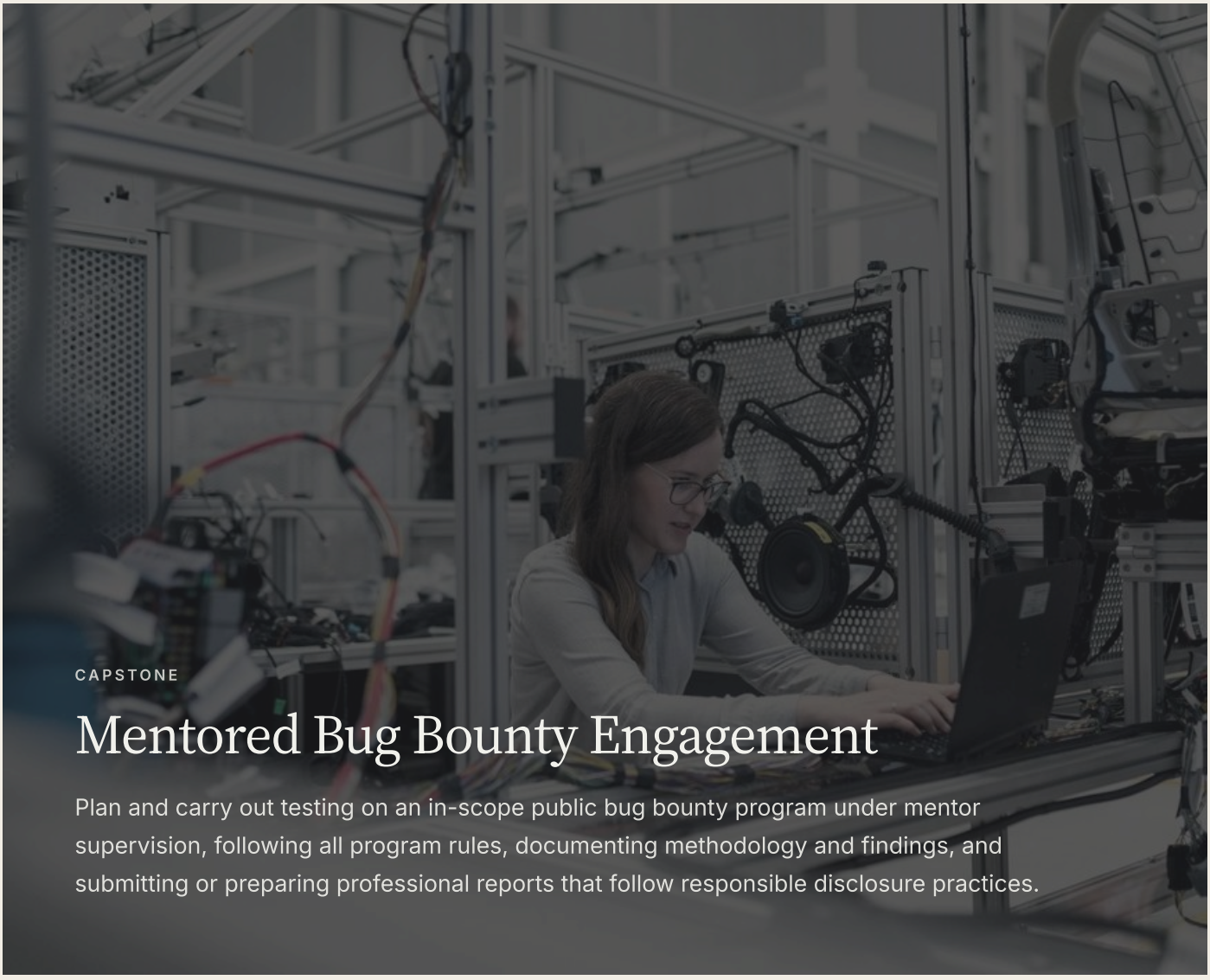
Program Scope Analysis

Analyse several public bug bounty programs, comparing scope, rules, exclusions and safe harbour terms to choose suitable targets.

03

Professional Report Set

Write a set of polished vulnerability reports with CVSS ratings, clear evidence and remediation guidance, reviewed by mentors.



CAPSTONE

Mentored Bug Bounty Engagement

Plan and carry out testing on an in-scope public bug bounty program under mentor supervision, following all program rules, documenting methodology and findings, and submitting or preparing professional reports that follow responsible disclosure practices.

CERTIFICATION

SAM-BB

Awarded on successful completion of the program assessments.

- MCQ assessments
- Practical lab evaluation
- Project & capstone review
- Final presentation

HOW YOU LEARN · THE SAM LEARNING FRAMEWORK™

01 Scenario

Real-world attack and use-case scenarios open every module.

02 Apply

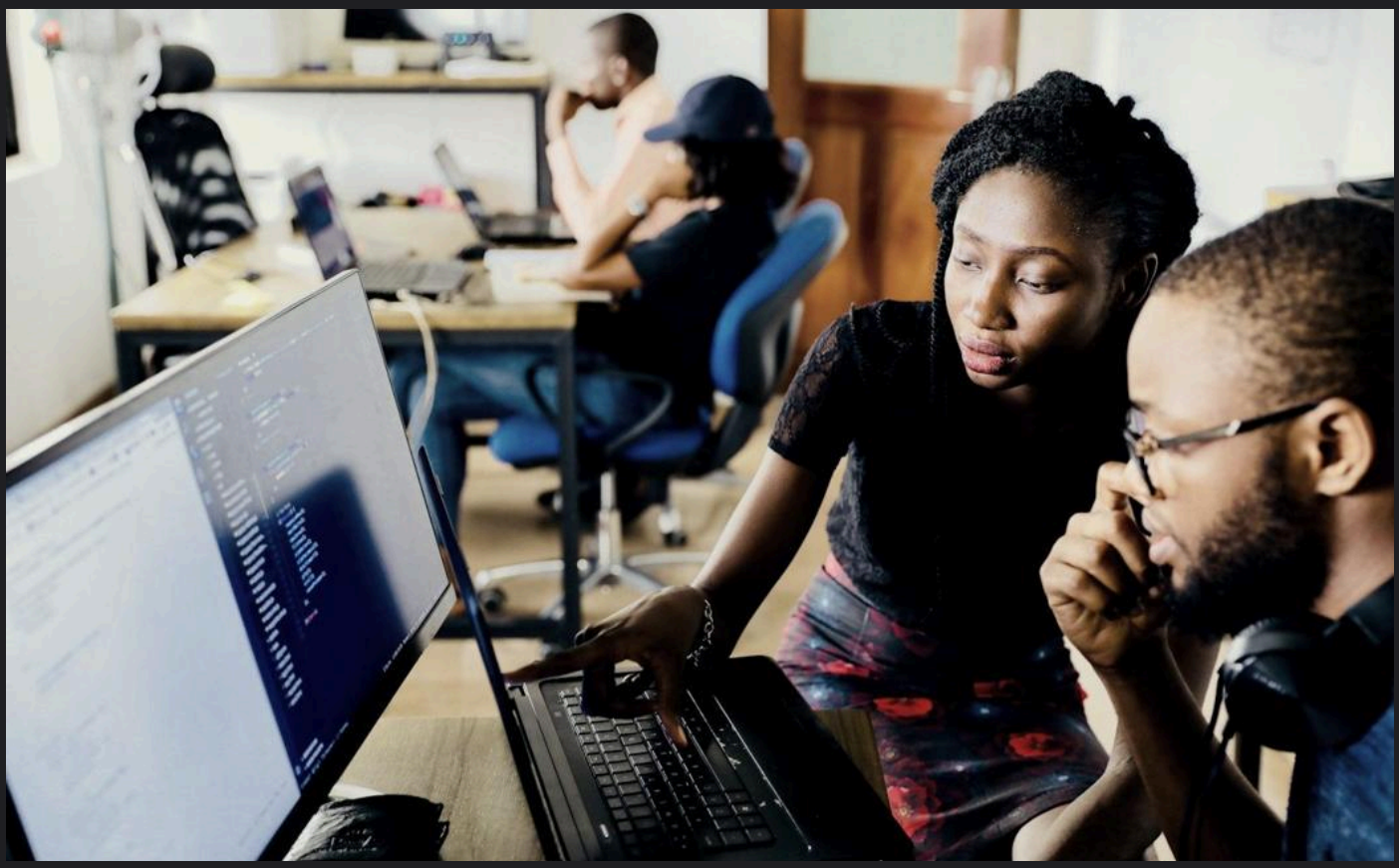
Hands-on lab work, CTF challenges and live projects.

03 Master

Assessment, peer review and certification prep.

04 Mentor

Post-program career guidance and support.



Delivery: Instructor-Led (ILT) · Virtual Instructor-Led · Self-Paced Online · E-Learning Licensing · Blended Learning · Corporate Onsite

Where this program fits

Advanced
3 programs

Expert
You are here

BEFORE THIS

Advanced Cybersecurity Research Internship	3 Months
AI Research & Innovation Program	3 Months
Cloud Architecture Challenge Program	6 Weeks

UP NEXT

The top of this pathway — explore related programs.



Questions, answered

Do I need prior experience to join?

Yes. This is an expert-level program that assumes prior experience in web technologies, HTTP and basic web security testing. It moves quickly into frameworks, case studies and hands-on work, so participants should meet the listed prerequisites before enrolling.

How is the program delivered and scheduled?

The 3 months program is instructor-led and mentor-guided, delivered live virtual or in a blended format with partner institutions. It combines scheduled sessions, mentor check-ins and independent project work planned around the academic calendar.

Will I receive a certificate?

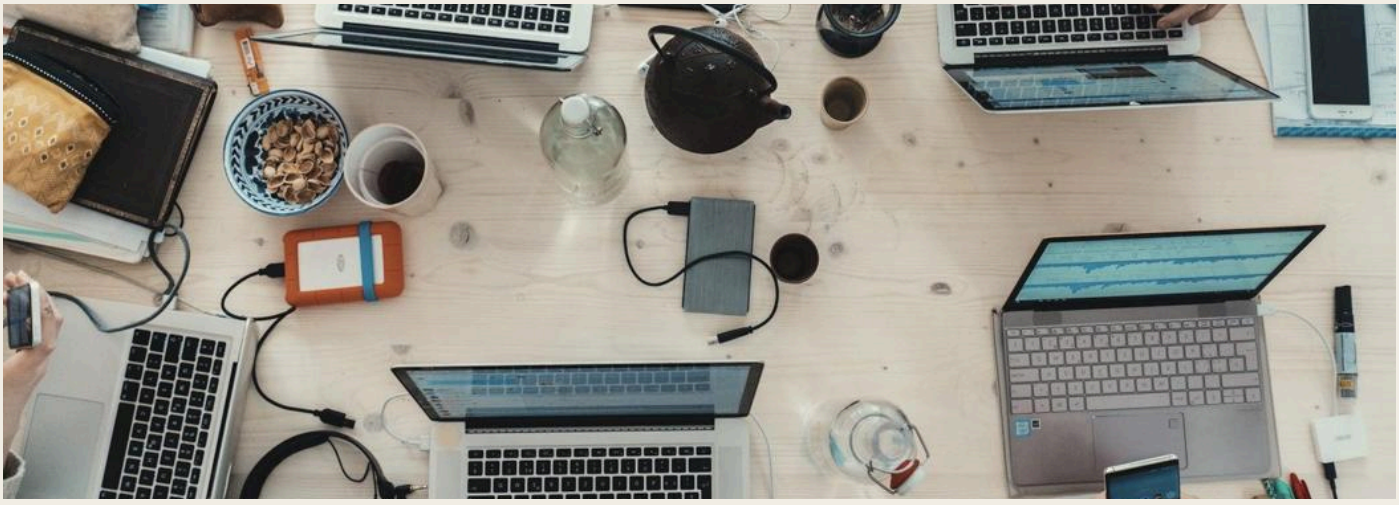
Yes. Participants who meet attendance requirements and successfully complete the assessments receive the Samcommunity Academy SAM-BB certificate. Assessments may include quizzes, practical exercises and a final capstone review, depending on the program format.

Will I get access to labs and tools?

Yes. Hands-on work uses a prepared lab environment with tools such as Burp Suite, OWASP resources, Kali Linux. Access details are shared before the program starts, and all exercises run in isolated, authorised environments rather than live production systems.

Is career support included?

Participants receive mentor feedback, portfolio guidance and help presenting their work professionally. Samcommunity Academy may share relevant opportunities where available, but does not guarantee internships, jobs, rewards, bounty earnings or salary outcomes.





SAMCOMMUNITY ACADEMY

CONTACT

Begin with Bug Bounty Training & Mentorship.

INDIVIDUALS

academy@samcommunity.in

CORPORATE & INSTITUTIONS

corporate@samcommunity.in

samcommunity.in · @samcommunity_ · Xylyn Samcommunity Private Limited · DPIIT-recognized startup · Surat, Gujarat, India