Forebrain — Ethical Hacking & Bug Bounty (3 Months / 12 Weeks)

Duration: 3 Months (12 Weeks / 60 instructional days)

Format: 1 hour class + 1 hour lab practice (Monday–Friday). Saturday = Activity Day (practical session based on weekly topics).

Focus: Practical bug-hunting skills, responsible disclosure, and building a sustainable bug bounty portfolio.

Outcome: A minimum of 3 documented vulnerability reports, platform-ready disclosures, and a capstone bug-hunting engagement.

Daily Routine (Standard)

- 1 hr: Concept lecture & demo

- 1 hr: Guided hands-on bug-hunting lab

- Saturday: Activity Day – live hunting sprints, write-ups, guest talks

- Learning Model: 90% practical, 10% theory — focus on reproducible reports and PoCs

Phase-wise Curriculum Overview

Phase 1 — Foundations & Recon for Bug Bounty (Weeks 1–3)

- Introduction to bug bounty platforms and disclosure policies (HackerOne, Bugcrowd, Open Bug Bounty)

- Rules of Engagement, scope definitions, C2 and legal boundaries for hunting

- OSINT & passive recon: Amass, Subfinder, crt.sh, wayback, GitHub token discovery

- Subdomain takeover checks, certificate transparency and asset inventory creation

- Web fingerprinting and tech stack identification (Wappalyzer, WhatWeb)

- Automation basics: using ffuf, aquatone, and masscan for asset discovery

Practical Assignment I: Recon Pack — scoped asset list, live subdomain findings, priority targets

Phase 2 — Web Vulnerabilities & Hunting Techniques (Weeks 4–6)

- Deep-dive into OWASP Top 10 from a bounty perspective

- Burp Suite mastery: proxy, repeater, intruder, extender & Collaborator usage

- Manual testing techniques: parameter tampering, logic flaws, IDOR, auth bypass

- Automated scanning & templating: Nuclei, Nikto, OWASP ZAP templates

- Exploit development for web: SQLi, XSS, SSRF, XXE and blind techniques

- API security testing: JWT, auth bypass, parameter pollution and fuzzing APIs

Practical Assignment II: Web Bounty Write-up — reproduce a vuln in lab, craft PoC, and remediation steps

Phase 3 — Advanced Targets & Specialized Hunting (Weeks 7–9)

- Advanced recon pipelines and cache/wayback analysis for hidden endpoints

- Subdomain takeover and cloud misconfiguration hunting (S3, Azure blobs)

- Mobile and API-focused testing: Android/iOS app reverse engineering basics and API fuzzing

- Bypass techniques: WAF evasion, input sanitization bypasses, logic bypass strategies

- Writing custom scanners and Burp extensions for targeted hunts

- Safe use of exploit frameworks and responsible proof-of-concept generation

Practical Assignment III: Advanced Hunt — cloud misconfig or subdomain takeover PoC (lab-safe)

Phase 4 — Reporting, Disclosure, & Capstone (Weeks 10–12)

- Writing high-quality vulnerability reports: executive summary, technical details, impact, and remediation

- Responsible disclosure workflows: timelines, vendor communication, and escalation

- Monetization strategies: bug bounty platforms, private programs, and responsible selling

- Building a public portfolio & safe disclosure ethics

- Capstone: live simulated bug-hunt on a seeded target with full report submission and remediation verification

- Career handoff: preparing bug bounty profiles, pitching to private programs, and interview demo prep

Capstone Deliverables: 3+ professional write-ups, PoC artifacts, final capstone report

Tools & Technologies Covered

Recon & Asset Discovery:

- Amass
- Subfinder
- crt.sh
- Wayback Machine
- Shodan
- masscan
- aquatone
- ffuf

Web Testing & Exploitation:

- Burp Suite (Community/Pro)
- Burp Collaborator
- OWASP ZAP
- sqlmap
- Nikto
- Nuclei
- ffuf
- dirsearch

API & Mobile:

- Postman
- jwt.io

- Burp Mobile Assistant
- Frida (conceptual)

Automation & Scripting:

- Python 3
- Bash
- Custom Burp extensions (basic)

Reporting & Platforms:

- HackerOne, Bugcrowd, GitHub Security Advisories, Markdown
- Proof-of-Concept tools (screenshots, curl commands)

Deliverables & Assessment

- Recon Pack with prioritized targets and evidence
- Three professional vulnerability write-ups (lab-seeded or responsible disclosure)
- Capstone live hunt report and PoC artifacts
- Weekly lab submissions and activity logs
- Guidance for real-world platform submissions and ethical practices