Advanced Bug Bounty Training

Integrated curriculum | Offensive research + AI-assisted hunting

Weekend batch · Starts 5 December 2026 · Beginner prerequisites recommended

01 Research Environment & AI Inventory

01.1 Ubuntu research workstation
Configure Ubuntu, browser profiles, Burp Suite, Python tooling, recon utilities, wordlists and reproducible project directories.

01.2 Claude, Codex & AI inventory
Set up Claude and Codex-assisted workflows; catalog available models, tool permissions, context sources, API usage and operational limits.

01.3 Target selection & scope intelligence
Prioritize authorized programs using asset exposure, technology, business workflows, attack surface and duplicate-risk signals.

01.4 AI-assisted reconnaissance
Correlate subdomains, DNS, HTTP fingerprints, endpoints and JavaScript assets; validate model-generated leads against real evidence.

02 Prompt Intelligence, Files & Archives

02.1 Requirements-driven prompt generation
Design task-specific prompts for recon, code review and hypothesis testing; use structured outputs, constraints and evidence checks.

02.2 AI-powered sensitive-file discovery
Review JavaScript bundles, configuration files, source maps, backups and public repositories for exposed tokens, credentials and internal paths.

02.3 Archive and historical intelligence
Mine Wayback snapshots, archived endpoints, old API versions and retired assets to identify changed controls and forgotten attack surface.

02.4 Dorking and PII exposure
Build targeted search queries; distinguish reportable information disclosure from harmless public metadata and false positives.

03 Custom AI Tooling & Agentic Workflows

03.1 Build your own hunting utilities
Create focused Python-based recon helpers, parsers and enrichment tools; define input, output, logging and test cases.

03.2 MVP framework development
Prototype modular AI-assisted research pipelines with retrieval, tools, retries, guardrails and analyst approval checkpoints.

03.3 Agentic analysis flows
Chain discovery, classification, triage and verification steps without blindly trusting agent decisions or generated findings.

03.4 Anti-AI-slop validation
Reject hallucinated endpoints, fabricated exploit claims and weak reports through reproducibility, response comparison and manual review.

04 Code, API & Burp Suite Exploitation

04.1 Advanced code intelligence
Trace frontend-to-backend data flows, exposed secrets, authorization assumptions and insecure application logic.

04.2 Burp Suite with Codex / Astra
Analyze captured HTTP requests and responses, generate test hypotheses and controlled payload variants, then verify results in Burp.

04.3 API key and token exploitation
Assess key scope, privileges, token validation, expiry and authorization boundaries; demonstrate impact safely.

04.4 Request/response differential testing
Compare user roles, objects, parameters and error behavior to uncover access-control gaps and hidden functionality.

05 Authentication & Authorization Attacks

05.1 Broken access control / IDOR
Investigate object-level and function-level authorization across tenants, accounts and administrative workflows.

05.2 MFA and session bypass
Study enrollment, recovery, step-up authentication, session fixation and inconsistent MFA enforcement.

05.3 Token and identity validation
Review JWT claims, audience and issuer handling, refresh flows, privilege changes and session invalidation.

05.4 Desktop and session manipulation
Explore client-state assumptions and server-side trust failures; distinguish UI bypasses from exploitable authorization flaws.

06 SSRF, Internal Services & Misconfiguration

06.1 SSRF from fundamentals to advanced
Map URL-fetching features, redirect handling, parser behavior and allowlist/denylist weaknesses.

06.2 Internal network exposure
Assess localhost, internal services and metadata endpoints within authorized scope; document reachability and concrete impact.

06.3 Platform misconfigurations
Review debug endpoints, insecure defaults, exposed admin interfaces, deployment artifacts and environment leaks.

06.4 Blind and indirect verification
Use controlled callbacks, timing and response differentials to validate server-side behavior without destructive testing.

Curriculum / Advanced Exploitation & Applied Research

Continued from page 1 · Practical, evidence-led methodology

07 High-Impact Exploitation & Data Exposure

07.1 Unauthenticated RCE paths
Study upload handlers, command injection, unsafe interpreters and exposed management functions; prove execution with non-destructive checks.

07.2 Database and credential weaknesses
Identify injection opportunities, hardcoded credentials, overly broad permissions and sensitive-data enumeration.

07.3 Information disclosure to impact
Turn exposed keys, PII and internal configuration into defensible risk narratives using authorized validation.

07.4 Chained vulnerability analysis
Combine low-severity weaknesses into realistic attack paths and assess preconditions, exploitability and blast radius.

08 Business Logic & Organization Impact

08.1 Business logic abuse
Test pricing, payments, approvals, quotas, state transitions and workflow assumptions beyond scanner-based findings.

08.2 Cross-tenant and organization impact
Investigate organization-level privilege boundaries, role inheritance and multi-account access patterns.

08.3 Functional and blind attacks
Build hypotheses around hidden operations, asynchronous workflows and limited-feedback endpoints.

08.4 Mitigation-oriented reasoning
Explain root cause, affected trust boundary, exploit sequence and practical remediation options.

09 AI Models for Hunting-Surface Analysis

09.1 Model-assisted vulnerability classification
Prepare labeled examples and evaluation sets to prioritize suspicious endpoints, code patterns and response anomalies.

09.2 Training and evaluation fundamentals
Understand dataset quality, feature leakage, precision/recall and human review; compare lightweight models with prompt-based approaches.

09.3 Hacking the bots / AI attack surface
Assess authorized LLM integrations for prompt injection, tool misuse, data leakage and unsafe agent permissions.

09.4 Human-in-the-loop research
Use AI to accelerate candidate discovery while requiring independent proof before severity claims or disclosure.

10 Recon Automation & Research Operations

10.1 Google recon and subdomain discovery
Combine advanced search, enumeration, fingerprinting and asset relationship mapping for scoped programs.

10.2 Automation frameworks and tool setup
Configure repeatable command-line workflows, key bindings, environment management and rate-aware scanning.

10.3 Monitoring and change detection
Track JavaScript deployments, new endpoints, infrastructure changes and newly exposed resources.

10.4 Research evidence management
Preserve minimal reproducible requests, timestamps, screenshots and structured notes for accurate triage.

11 P1 Hunting & Professional Reporting

11.1 High-severity hypothesis development
Study realistic P1-class impact patterns such as account compromise, privilege escalation, data exposure and exploit chains.

11.2 Proof of concept and severity
Document prerequisites, affected assets, reproduction steps, impact and limitations; avoid unsupported severity inflation.

11.3 Professional report writing
Produce concise titles, clear steps, redacted evidence, expected versus actual behavior and remediation guidance.

11.4 Triage, duplicates and disclosure
Navigate scope, safe-harbor rules, validation requests, retesting and responsible disclosure etiquette.

12 Applied Labs & Capstone Workflow

12.1 End-to-end authorized hunt
Select a target, map attack surface, generate hypotheses, test manually and use AI for bounded assistance.

12.2 Tool-building mini-project
Deliver a small functional AI-assisted recon or analysis utility with documentation and verification checks.

12.3 Case-study review
Analyze representative high-impact bug patterns, including failed leads and why they did not meet reporting thresholds.

12.4 Final research deliverable
Submit a structured finding or a documented negative result, with evidence, methodology and next-step recommendations.