Beginner Bug Bounty Training

Detailed curriculum | From web fundamentals to practical vulnerability research

NEW BATCH · 5 DECEMBER 2026

01 Bug Bounty Foundations & Research Setup

01.1 Bug bounty and ethical hacking

Understand vulnerability disclosure programs, bounty platforms, researcher responsibilities and how a finding becomes a defensible security report.

01.2 Getting started with a repeatable workflow

Learn to read program rules, form test hypotheses, collect evidence, validate results and avoid duplicate or out-of-scope submissions.

01.3 Responsible disclosure models

Compare coordinated, private and public disclosure; understand safe testing limits, severity communication and professional conduct.

01.4 Burp Suite fundamentals

Configure the browser proxy and certificates; inspect HTTP traffic, use Repeater, and understand methods, headers, cookies and sessions.

01.5 Linux workstation and practice labs

Set up a research environment with browser profiles, essential tools, notes, wordlists and safe, authorized practice targets.

02 Target Selection & Reconnaissance

02.1 Active and passive reconnaissance

Discover domains, subdomains, web technologies, endpoints and public records while distinguishing passive research from active probing.

02.2 Choosing targets and reading scope

Interpret program exclusions, wildcard rules, rate limits and asset ownership; prioritize realistic attack surfaces.

02.3 Search, archives and asset discovery

Use search operators, archived URLs and JavaScript references to map forgotten routes and publicly exposed functionality.

02.4 Sensitive data gathering and EXIF metadata

Identify accidental exposure of configuration details, metadata, personal information and document location data; assess real impact.

03 Client-Side & Session Vulnerabilities

03.1 Reflected and stored XSS

Trace input into browser execution contexts, understand encoding and persistence, and validate security impact safely.

03.2 Cross-site request forgery (CSRF)

Examine state-changing requests, anti-CSRF tokens, SameSite cookies and account-action protections.

03.3 Session management: five patterns

Study session fixation, missing invalidation, weak rotation, insecure cookie attributes and session reuse after logout.

03.4 Open redirects and broken link hijacking

Identify unsafe redirect parameters, abandoned external destinations and realistic phishing or trust-boundary impact.

04 Authentication, Access & Abuse Controls

04.1 Unauthorized access: three patterns

Test horizontal access, vertical privilege escalation and missing authorization on sensitive functions.

04.2 Weak or missing authentication

Analyze unprotected endpoints, default credentials, inconsistent login enforcement and exposed administrative functions.

04.3 Password reset and account takeover

Review reset token lifecycle, identity verification, recovery logic, session handling and account recovery abuse.

04.4 Rate limits: five bypass patterns

Understand per-account, per-IP, endpoint, identifier and workflow limits; document abuse without disrupting services.

Practical Security & Reporting

Continued syllabus | Controlled testing, evidence and professional disclosure

05 Injection & Server-Side Security

05.1 SQL injection in GET and POST

Understand query construction, input handling, error-based clues and safe validation in parameterized requests.

05.2 Server-side request forgery (SSRF)

Identify server-side URL fetch features, trust boundaries, redirect behavior and controlled internal reachability tests.

05.3 Insecure protocol handling

Recognize insecure transport, mixed content, weak redirects and sensitive data transmitted without appropriate protection.

05.4 Denial-of-service and resource exhaustion

Learn how expensive operations and missing safeguards create availability risks; use non-disruptive evidence and program-approved tests.

06 Information Disclosure & Misconfiguration

06.1 Information disclosure vulnerabilities

Assess leaked stack traces, internal paths, configuration, tokens and PII; separate meaningful exposure from benign metadata.

06.2 Directory listing and exposed files

Inspect accidental directory indexes, backup artifacts, public storage and source maps; verify sensitivity and accessibility.

06.3 Weak password policies

Evaluate password creation, reuse, lockout and recovery controls against realistic account compromise scenarios.

06.4 Sensitive files and configuration discovery

Review publicly reachable files, JavaScript bundles and repositories for secrets or internal endpoints, with safe validation.

07 API Security & Business Logic

07.1 API vulnerability fundamentals

Map REST endpoints, JSON parameters, tokens and authorization; test object and function-level access controls.

07.2 Payment and checkout logic flaws

Analyze amount, currency, order-state and discount assumptions in sandbox or explicitly authorized payment workflows.

07.3 Application workflow abuse

Identify missing step validation, inconsistent server-side checks and state transitions that allow unintended actions.

07.4 Evidence-driven impact assessment

Demonstrate the affected role, object, workflow and business consequence while minimizing data access.

08 Practical Hunting & Reporting

08.1 Five surprise real-world bug patterns

Walk through five instructor-selected vulnerability classes, emphasizing discovery signals, reproducibility and common false positives.

08.2 Professional vulnerability reporting

Write concise titles, reproduction steps, proof-of-concept evidence, severity rationale and remediation guidance.

08.3 End-to-end beginner hunting workflow

Combine recon, Burp testing, validation, notes and disclosure into a repeatable approach for authorized programs.

READY TO START BUG BOUNTY HUNTING?

Beginner batch starts 5 December 2026 · Live weekend training

Register: https://walink.me/wm5ndl