Bug Bounty

Learn to find real web vulnerabilities, write clear reports, and hunt on live bug bounty programs.

Duration: 2 months | Certificate: NUEXUS Bug Bounty completion certificate | Format: Online or onsite, 1-on-1 or batch | NUEXUS certificate on completion

OVERVIEW

This is a hands-on, 2-month training that takes you from web application fundamentals to actively hunting for security vulnerabilities on real bug bounty platforms. You learn to find, exploit, and responsibly report flaws like XSS, IDOR, SSRF, authentication bypasses, and injection issues, using the same tools and methodology that professional hunters use. Every module is lab-based and mentor-led by certified trainers, and you finish with a portfolio of practical findings, well-written reports, and a repeatable hunting workflow. Delivered online from anywhere or onsite in Islamabad, in batches or 1-on-1, on weekends or weekday evenings.

SKILLS YOU WILL GAIN

Web Recon | Burp Suite | OWASP Top 10 | XSS | SQL Injection | IDOR & Access Control | SSRF | Authentication Flaws | API Testing | Report Writing

WHAT YOU WILL BE ABLE TO DO

- Set up a complete hunting environment with Burp Suite, a browser proxy, and a Kali Linux toolkit
- Perform reconnaissance on a target: subdomain enumeration, content discovery, and mapping the attack surface
- Find and exploit common web vulnerabilities including XSS, SQL injection, IDOR, SSRF, CSRF, and authentication flaws
- Understand and test against the OWASP Top 10 in realistic, deliberately vulnerable lab applications
- Write clear, reproducible vulnerability reports with impact, steps to reproduce, and remediation advice
- Read program scope and rules, hunt responsibly on live bug bounty platforms, and manage disclosure ethically

WHO IT IS FOR

- Aspiring bug bounty hunters and ethical hackers who want a structured, practical starting point
- Students and fresh graduates in IT, computer science, or cybersecurity looking to build hands-on offensive skills
- Web and software developers who want to understand how their applications get attacked and how to harden them
- IT and security professionals moving into penetration testing or application security roles
- Self-taught learners who have watched tutorials but want a guided, lab-based path with mentor feedback

PREREQUISITES

- Basic computer literacy and comfort browsing the web and installing software
- A laptop capable of running a virtual machine or Kali Linux (we help you set this up in the first module)
- Helpful but not required: basic HTML and how websites work, and a little familiarity with the command line
- No prior hacking or programming experience required, beginner friendly

WHAT'S INCLUDED

- Mentor-led live sessions, online or onsite, in batch or 1-on-1
- Hands-on labs and real-world projects, not slides alone
- Recordings of your own sessions to revisit anytime
- Exam-aligned study material and practice questions
- Doubt-clearing and revision support through the program
- A verifiable NUEXUS completion certificate
- Career and next-step guidance after you finish

COURSE CURRICULUM

1 Bug Bounty Foundations and Your Lab

- How bug bounty and vulnerability disclosure programs work (HackerOne, Bugcrowd, Intigriti, direct VDPs)
- Reading scope, rules of engagement, and staying legal and ethical
- Setting up your environment: Kali Linux, a virtual machine, and a browser proxy
- Responsible disclosure mindset and what makes a valid, in-scope finding

2 Web and HTTP Fundamentals for Hunters

- How the web works: HTTP requests and responses, methods, status codes, and headers
- Cookies, sessions, and how authentication state is maintained
- Client side vs server side, and where trust boundaries break
- Using browser developer tools to inspect and understand a web application

3 Recon and Attack Surface Mapping

- Subdomain enumeration and asset discovery
- Content and directory discovery with tools like ffuf and gobuster
- Fingerprinting technologies, frameworks, and versions
- Building a target map and prioritizing where to hunt

4 Mastering Burp Suite and the Proxy Workflow

- Intercepting, editing, and replaying requests with Burp Proxy and Repeater
- Automating request tampering with Intruder
- Using the target site map, scope, and match and replace rules
- A practical, repeatable manual testing workflow

5 OWASP Top 10 in Practice

- Walking the OWASP Top 10 categories with hands-on examples
- Broken access control, cryptographic and misconfiguration issues
- Practicing safely in deliberately vulnerable apps (Juice Shop, DVWA, PortSwigger labs)
- Recognizing patterns that repeat across real targets

6 Injection Attacks

- SQL injection: detection, exploitation, and data extraction with and without sqlmap
- Cross site scripting (XSS): reflected, stored, and DOM based
- Command injection and template injection basics
- Understanding impact and writing proof of concept payloads

7 Authentication, Authorization, and Business Logic

- Insecure Direct Object References (IDOR) and broken access control
- Authentication bypasses, weak password reset, and session flaws
- Cross Site Request Forgery (CSRF) and its impact
- Business logic flaws and abusing intended functionality

8 Server Side and Advanced Vulnerabilities

- Server Side Request Forgery (SSRF) and its escalation paths
- File upload vulnerabilities and path traversal
- Security misconfigurations, exposed secrets, and information disclosure
- Introduction to chaining bugs for higher impact

9 Report Writing and Impact Communication

- Structuring a report: title, summary, steps to reproduce, and impact
- Writing clear proof of concept steps a triager can follow
- Rating severity and explaining real world impact
- Suggesting remediation and handling duplicates and triage feedback

10 Live Hunting, Ethics, and Your Path Forward

- Choosing programs, selecting targets, and time boxing your hunts
- Guided practice hunting on live programs within scope
- Building a personal methodology, checklist, and note taking system
- Ethics, staying in scope, and continuing to grow as a hunter

CAREER OUTCOMES

- Bug Bounty Hunter
- Web Application Pentester
- Application Security Analyst
- Security Researcher

CERTIFICATION

On successfully completing the course and its practical assessment, you receive the NUEXUS Bug Bounty completion certificate, which recognizes that you have demonstrated hands-on web application testing and reporting skills. It is a NUEXUS credential rather than a third-party exam, and the course is job-focused and built to strengthen your readiness for real hunting and application security roles, though no certificate can guarantee a job, a bounty, or income.