Bug Bounty Hunting

TBUG
Bug Bounty Hunting

3 Month Program	36 CPEs	Laptop Required

You Will Learn

- Get ready to don your detective hat, because we're diving into the world of bug hunting! We'll be learning how to track down sneaky bugs lurking in websites and web applications, plus the latest techniques to outsmart them. We'll also put our skills to the test with hands-on attacks, so we're fully equipped to handle any cyber villains out there. And the cherry on top? You'll get to show off your skills by submitting a bug report on top platforms like Bugcrowd or Hackerone. Let's get to work!

TBUG
Bug Hunter

TIAC BUG BOUNTY Certification

Our comprehensive guide, "Unleashing Your Inner Detective: A Guide to Bug Hunting," provides an in-depth look into the world of bug hunting. By following our expert guidance, you'll learn how to identify elusive bugs hidden within websites and web applications. Our guide also includes hands-on exercises, allowing you to put your newly acquired skills to use and enhance your ability to thwart cyber threats. Additionally, you'll have the opportunity to showcase your expertise by submitting bug reports on premier platforms such as Bugcrowd and Hackerone. Put on your detective hat and let's embark on this thrilling journey!

Bug Bounty programs are for researchers and cybersecurity professionals to test their skills on a variety of targets online and get paid if they find any vulnerabilities in the application. It is a penetration testing program that rewards for finding bugs and ways to exploit. Cyber Security is next Big thing. There are many people who are learning how to develop web application and yet only a few are learning to secure those applications. This course is designed so that you can learn to secure web applications even if you don't know how to design or develop a web app.

- **Introduction**
  - Basic Network Terminologies
  - Virtualisation & OS Setup
  - Server & Linux Basics
  - Introduction to HTML, Python & Webhosting
  - Information Gathering & Social Reconnaissance
  - Introduction to Bug Crowd & Hackerone
  - Vulnerability Analysis
  - Penetration testing Vs Bug Bounty
  - OWASP Test Cases Check List
  - Vulnerability Rating Taxonomy (VRT)
  - SANS Top25 Applications Errors
  - OWASP CWE Vulnerabilities
  - Common Attack Pattern Enumeration and Classification(CAPEC)
  - Common Vulnerabilities & Exposures (CVE) rating
- **Burpsuit**
  - Spidering - Scanning websites and web applications
  - Investigating web security
  - Advanced manual tools
  - Module - Repeater | Intruder | Decoder | Comparer
  - Burpsuite Collaborator Client
  - Burpsuite Clickbandi

"This course taught me to truly focus on the methodology while performing a pen test. During the Capture-the-Flag event, I realized how much time can be wasted if you fail to respect your methodology."

-Sandya Jalesh - Security Engineer, **Shell Corp.**

Module Descriptions

- **TEST CASE - Common Low Priority Bugs**
  - Clickjacking
  - Missing SPF/DMARC Record
  - Open Redirection
  - Lack of Email Notification & Verification
  - Mail Server Misconfiguration
  - Missing HTTP Only Cookie Flag
  - No Rate Limiting
  - Captcha Bypass
  - Missing Authentication
  - Parameter Pollution

- **TEST CASE - Sensitive Data Exposure**
  - Internal IP Disclosure
  - Path Disclosure
  - Token Disclosure in URL
  - EXIF Geolocation Data
  - User Enumeration
  - Server Configuration
  - Private API key Disclosure
  - Sensitive Configuration Files

- **TEST CASE - Encryption Flaws**
  - Improper Certificate Validation
  - Cleartext Transmission of Session Token
  - Encrypted Cookies
  - Cleartext Storage of Sensitive Information
  - Missing Encryption of Sensitive Data
  - Cryptographic Issue (Generic)

- **TEST CASE - Injection**
  - Client-Side Template Injection
  - Server-Side Template Injection
  - SQL Injection
  - OS Command Injection
  - XML Injection
  - XML RPC
  - PHP Code Injection
  - HTML Injection

- **TEST CASE - Access Control Issues**
  - Path traversal
  - Information Disclosure
  - Information Exposure Through an Error Message
  - Information Exposure Through Debug Information
  - Privilege Escalation
  - Improper Access Control
  - Improper Authentication
  - Disallowed Robots file Access

- **TEST CASE - Authorization & Authentication**
  - Improper Authorization & Authentication
  - Insufficient Session Expiration & Session Fixation
  - Issues with OAuth Redirection & Permissions
  - Insecure Direct Object Reference (IDOR)
  - Misconfigured Login pages
  - Bypass Single factor & Two factor Authentication
  - Account Take Over
  - Account Lockout
  - Cross Site Request Forgery (CSRF)
  - Server Side Request Forgery (SSRF)
  - DNS Zone Transfer

- **TEST CASE - High Risk Bugs**
  - Cross site scripting
  - JSONHijacking
  - Wordpress | Joomla | Drupal Bugs
  - CMS Vulnerability Analysis
  - Remote Code Execution
  - Critical File Found
  - File Inclusion (LFI /RFI)
  - File Upload Vulnerabilities
  - Directory Traversal
  - CORS
  - Script Source Code Disclosure
  - HTTP Parameter Pollution Attack
  - Subdomain Takeover
  - Documenting & Reporting Vulnerability

Who Should Attend

- IT Professionals: Individuals working in IT roles who seek to specialize in cyber security and enhance their skills to effectively protect digital assets and networks.
- Security Analysts: Those currently in security roles looking to advance their knowledge in specific areas such as penetration testing, incident response, or digital forensics.
- Network Administrators: Professionals responsible for managing and securing networks who want to broaden their understanding of cyber threats and mitigation techniques.
- System Administrators: Individuals handling system configuration and management, interested in securing systems against potential cyber attacks.
- Software Developers: Developers aiming to create secure applications by understanding vulnerabilities and incorporating robust security measures into their coding practices.
- Risk Managers: Those tasked with assessing and mitigating risks, including cyber risks, who wish to incorporate advanced cyber security strategies into their risk management approach.
- Cybersecurity Enthusiasts: Individuals passionate about cyber security, even without prior experience, looking to kickstart their career in the field and develop practical skills.
- Recent Graduates and Students: Graduates and students studying computer science, IT, or related fields who want to specialize in cyber security to meet the growing industry demand.
- Security Consultants: Those consulting organizations on security matters, aiming to expand their expertise and provide more comprehensive solutions.
- Professionals Switching Careers: Individuals transitioning from other fields into cyber security, attracted by its dynamism and the increasing need for skilled professionals.

NICE Framework Work Roles

1. **Ethical Hacker/Penetration Tester**
2. **Security Analyst**
3. **Security Consultant**
4. **Incident Responder**
5. **Cybersecurity Researcher**
6. **Security Engineer**
7. **Bug Hunter**
8. **Red Teamer**
9. **Threat Hunter**
10. **Security Auditor**
11. **Security Trainer/Educator**
12. **Malware Analyst**
13. **IoT Security Specialist**
14. **Cloud Security Engineer**
15. **Application Security Specialist**