Hack The Box Certified Bug Bounty Hunter (HTB CBBH)

Course Overview

HTB Certified Bug Bounty Hunter (HTB CBBH) is a highly hands-on certification that assesses the candidates' bug bounty hunting and web application pentesting skills. HTB Certified Bug Bounty Hunter certification holders will possess technical competency in the bug bounty hunting and web application penetration testing domains at an intermediate level. They will be able to spot security issues and identify avenues of exploitation that may not be immediately apparent from searching for CVEs or known exploit PoCs. They can also think outside the box, chain multiple vulnerabilities to showcase maximum impact, and actionably help developers remediate vulnerabilities through commercial-grade bug reports.

Knowledge Domains

- Bug Bounty Hunting processes and methodologies
- Web application/web service static and dynamic analysis
- Information gathering techniques
- Web application, web service and API vulnerability identification and analysis
- Manual and automated exploitation of various vulnerability classes
- Vulnerability communication and reporting

Target Audience

- Entry level Bug Bounty Hunters
- Junior Web Application
- Penetration Testers
- Web Developers
- Offensive Security Engineer

Course Objectives

- Bug Bounty Hunting processes and methodologies
- Web application/web service static and dynamic analysis
- Information gathering techniques
- Web application, web service and API vulnerability identification and analysis
- Manual and automated exploitation of various vulnerability classes
- Vulnerability communication and reporting

Duration

eLearning

Certifications

CBBH

Contact Us

(800) 674-3550

2151 W. Hillsboro Blvd.,
Suite 210
Deerfield Beach, FL 33442

Connect with us

APPLIED TECHNOLOGY ACADEMY

Sign Up Today!

AppliedTechnologyAcademy.com

Hack The Box Certified Bug Bounty Hunter (HTB CBBH)

APPLIED TECHNOLOGY ACADEMY

Course Outline

- Web Requests
- Introduction to Web Applications
- Using Web Proxies
- Information Gathering – Web Edition
- Attacking Web Applications with Ffuf
- JavaScript Deobfuscation
- Cross-Site Scripting (XSS)
- SQL Injection Fundamentals
- Command Injections
- File Upload Attacks
- Login Brute Forcing
- Broken Authentication
- Web Attacks
- File Inclusion
- Session Security
- Web Service & API Attacks
- Hacking WordPress
- Bug Bounty Hunting Process

Key Differentiators

- **Continuous Evaluation** - To be eligible to start the examination process, one must have completed all modules of the "Bug Bounty Hunter" job-role path 100% first. Each module in the path comes with its own hands-on skills assessment at the end that students must complete to prove their understanding of the presented topics. The answers to the skills assessment exercises are not provided. Evaluation takes place throughout the journey, not only during the examination!
- **Hands-on & Real-world Exam Environment** - HTB Certified Bug Bounty Hunter (HTB CBBH) candidates will be required to perform actual bug hunting activities against multiple real-world applications. HTB certifications are not based on and do not include multiple-choice questions!
- **Outside-the-box Thinking & Vulnerability Chaining** - HTB Certified Bug Bounty Hunter (HTB CBBH) candidates will be required to think outside the box and chain multiple vulnerabilities to achieve the exam's objectives. Like in real-world engagements, creativity, and in-depth knowledge will be necessary for a successful outcome.
- **Commercial-grade Report Requirement -** Successfully completing all bug bounty hunting activities is not enough to obtain the HTB Certified Bug Bounty Hunter (HTB CBBH) certification. Candidates will also be required to compose a commercial-grade report as part of their evaluation. HTB Certified Bug Bounty Hunter candidates will have to prove they are market-ready and client-centric professionals.
- **Seamless Experience Powered By Pwnbox** - The entire exam and certification process can be conducted through the candidates' browser, from start to finish. All bug bounty hunting activities can be performed via the provided and in-browser Pwnbox. There are no infrastructural or tool requirements.

The Exam

The candidate will have to perform bug bounty hunting activities against multiple real-world applications hosted in HTB's infrastructure and accessible via VPN (using Pwnbox or their own local VM). Upon starting the examination process, a letter of engagement will be provided that will clearly state all engagement details, requirements, objectives, and scope. All a candidate needs to perform the required bug bounty hunting activities is a stable internet connection and VPN software. HTB Certified Bug Bounty Hunter certification is the most practical certification for Bug Bounty Hunters that focuses on both bug hunting and professionally communicating findings.