ENCIPHERS

NOTE: All the practicals to be done on the Bug Hunter’s VPS only. You can connect to your dedicated VPS via SSH or remote desktop credentials.

Web Hacking - Advanced Level

Module 1 - Bug Hunter's VPS :

A. What is unique about the VPS?
B. Walkthrough of the VPS:
    a. ENCIPHER pentest/bug bounty guides & tutorials
    b. VPS tools and how to use them
    c. Other resources available on VPS: payloads, onlines tools, etc
C. Accessing your personal VPS via SSH/Remote desktop
D. How to make best use of Bug Hunter’s VPS.

Recap of XSS, CSRF, IDOR low severity issues, burp suite etc.

Module 2 - Input Validation Issues:

A. REST API with JSON & XML inputs
    1. XML injection
    2. XXE
    3. Other API related vulnerabilities
    4. SQL injection in API

B. Server Side Request Forgery
    1. How to test for SSRF
    2. SSRF exploitation scenarios
    3. Using tools and guide on VPS to find SSRF

C. Pentesting and finding bugs in GraphQL

D. Finding and exploiting SQL injections

Module 3 - Remote Code Execution:

A. What is RCE? How to find it? Approach to find RCE in bug bounty or pentests.

B. Some easy to find RCE, earning huge bounty for you.

C. Using Metasploit and public exploits for finding RCE

D. How to report RCE in the best way?

Module 4 - Authentication Vulnerabilities:

A. How does authentication work? What all types of authentication are generally used these days?

B. Finding vulnerabilities in each of those authentication flow.

Module 5 - Let’s build some approach: **(Choose your target)**

A. Attacking authentication flow of the app
    a. Login page testing
    b. API based authentication and possible security issues
    c. Testing Password reset function

B. Testing the app for Access control:
    a. Where to look for those issues?
    b. What are the possible vulnerabilities? IDOR, Access control missing etc.

C. Testing each feature/functionality:
    a. Input validation issues
        i. XSS/XXE/SSRF/SQLi etc
        ii. RCE via known vulnerable software version
        iii. RCE via misconfigurations
        iv. Privilege escalations