Web Application Hacking - Advance Level 2.0

Day One

Module 1: Bug hunters VPS & Training Lab access

- What is Bughunters VPS and a walk through of the VPS.
  - How to use the VPS?
  - Best tools (online and offline), guides, Hacker's Mind Map etc.
- What's new on the improved Bughunters VPS:
  - New tools
  - More security
  - More Power
- How to make best use of Bug Hunter's VPS.

Module 2: Basics of everything (in security) & Client side vulnerabilities

- Basics about Web application and Http Protocols
- Using Burp Suite - Basic to Advance
- Information gathering /Recon to increase the attack surface
    - Subdomain scanning + takeover
    - Using VPS to find vulnerabilities related to misconfigurations
- Client Side vulnerabilities
    - Cross site scripting
        - Stored XSS exploitation
        - Reflected XSS exploitation
        - How to exploit real world Self XSS (getting paid for self XSS)
        - Finding & Exploiting the XSS in a real world application
    - HTML Injection
    - SOP & CORS misconfigurations and exploiting the misconfiguration
    - Cross Site Request Forgery
        - Basics & approach for testing
        - Finding & Exploiting the CSRF in a real world application
    - Other client side vulnerabilities

Module 3: Authentication & Authorisation vulnerabilities

- Finding and Exploiting vulnerabilities in:
    - Oauth
    - JWT
    - SAML authentication
- Missing access control vulnerabilities
- Insecure direct object reference
- Finding & Exploiting the IDOR in real world application

Day Two

Module 4: Server Side vulnerabilities

- SQL injection
  - Basics and test cases
  - Finding & Exploiting the SQL in a real world application
- XML External Entity
  - XML injection in REST API?
  - Finding & Exploiting the XXE in a real world application
- Server Side Request Forgery
  - How to test for SSRF
  - SSRF exploitation in a real world application
- Server Side Template injection (SSTI)
  - Finding & Exploiting the XXE in a real world application

Module 5: Remote Code Execution

- What is RCE?
  - Ways to achieve a remote code execution on a web/app server
- Using Metasploit and public exploits for finding and exploiting RCE
- RFI to Remote shell (On a real world application)
- SSTI to Remote shell (On a real world application)
  - Exploiting server side template injection to achieve remote shell
- Deserialization to Remote code execution (On a real world application)
  - Exploiting a vulnerability in deserialisation in application
- Command injection to Remote shell (On a real world application)
  - Exploiting a vulnerability in an application source code
- Remote code execution (remote shell) due to misconfigurations

---