

# CTF Preparation

1. Prepare your own hot-spot or VPN: local Wi-Fi may interfere or block manipulated requests.
  2. Set up a public web server with valid TLS for use in CTF challenges like XSS or data exfiltration; ideally with access to request log.
  3. Prepare PWN scripts that can use `netcat` or run local processes and debuggers and send payloads in response to input data.
  4. Prepare tools for:
    - Image forensics
    - Data conversion like Base64, HEX etc; e.g. CyberChef.
    - Extracting data from files; like cutting or replacing headers etc.
    - cURL script for sending encoded query strings or posting forms
  5. Check latest exploitation methods blogs and collect tools from them.
  6. Water bottle with electrolytes, coffee, sugar bars.
- 

Revision #4

Created 2026-03-22 13:51:54 GMT by hxd

Updated 2026-03-22 14:01:07 GMT by hxd