Attack related:

1. Tool to exploit the buffer overflow:
    a. Increasing the chances by inputting the shell code in various location with nops filled in between them since we can't guess the exact memory address. We can adjust this window.
2. XSS attack and defense:
    a. Write a parser for PHP files which will scan for possible XSS vulnerabilities.
3. SQL injection attack and defense:
    a. Write a parser for PHP files which will scan for possible SQL injection vulnerabilities.
4. All types of path traversal attack tool.(dot-dot, sym links, environment variable, string substitution). Identify the type and use appropriate functions/methods to substitute our code in it.

Defense ideas:

1. Script to make sure environment variables are same as the initial set and/or check for shellcode and new environment variables.
2. Make a document of all common vulnerabilities (code patterns) and fixes against web and binaries. This will help us quickly refer the solution to patch our vulnerable services.

Housekeeping and additional tasks:

1. IRC for team for secure communication and file transfer if needed.
2. Ansible script to automate system setup for our use and to harden the system.
   Chroot to limit the scope for execution only to our services and other ways to limit the possibility vulnerabilities.
3. Scripts for automating login, extracting key information for available services, targets to save the valuable time.
4. Using pwntools library and scapy for any other scripts to automate tasks for network based attacks.

//Develop countermeasures for all attack and defense tools that we build.