1. OS command injection, simple case:
   * In the given case the vulnerability was in the product stock check option and we exploited it using BurpSuite’s Repeater by appending the OS Command with the parameter.
2. Blind OS command injection with time delays:
   * Exploited the vulnerability present in the feedback input field to inject an OS command to the backend and triggered a delay by pinging the localhost by appending the command to the email input field.
3. Blind OS command injection with output redirection:
   * Exploited the vulnerability present in the email input field of the feedback form by first forcing the OS to execute the given command and then the output of that command is stored in a file and at the end retrieved that file from the backend database.
4. Blind OS command injection with out-of-band interaction:
   * Exploited the vulnerability present in the email input field of the feedback form by forcing the OS to execute the supplied command to interact with the external BurpSuite’s Collaborator Client.
5. Blind OS command injection with out-of-band data exfiltration:
   * Exploited the vulnerability present in the email input field of the feedback form by forcing the OS to execute the supplied command to interact with the external BurpSuite’s Collaborator Client and send data with the request.

