Sources utilized to conduct static and dynamic analysis of Wi-Fi router firmware.

1. Learning's
    a. https://www.pentestpartners.com/security-blog/how-to-do-firmware-analysis-tools-tips-and-tricks/
    b. https://prabhankar.medium.com/firmware-analysis-part-1-cd43a1ad3f38
    c. https://www.youtube.com/watch?v=hevWfbWOIew
    d. https://medium.com/@attify/firmware-analysis-for-iot-devices-fb8df961c19d

2. D-link dir 823g
    a. https://www.bleepingcomputer.com/news/security/5-severe-d-link-router-vulnerabilities-disclosed-patchnow/ /
    b. https://www.dlink.com/uk/en/support/security
    c. https://cve.ics-csirt.io/cve?vendor=dlink&product=dir-823g
    d. https://nvd.nist.gov/vuln/detail/CVE-2023-33735
    e. https://medium.com/codex/eda-stackoverflow-2020-70f22bea8f1c

3. D-link dir 846
    a. https://www.opencve.io/cve?vendor=dlink&product=dir-846
    b. https://www.cloudflare.com/learning/security/what-is-remote-code-execution/
    c. https://forum.openwrt.org/t/d-link-dir-846/60198
    d. https://nvd.nist.gov/vuln/detail/CVE-2022-46552
    e. https://cwe.mitre.org/data/definitions/78.html
    f. https://github.com/c2dc/cve-reported/blob/main/CVE-2022-46552/CVE-2022-46552.md
    g. https://www.dlink.com/en/security-bulletin/
    h. https://www.php.net/manual/en/ref.exec.php