Vulnerability Analysis

a. Perform vulnerability research with vulnerability scoring systems and databases

i. **Perform vulnerability research in Common Weakness Enumeration (CWE)**

- https://cwe.mitre.org/

ii. **Perform vulnerability research in Common Vulnerabilities and Exposures (CVE)**

- https://cve.mitre.org/

iii. **Perform vulnerability research in National Vulnerability Database (NVD)**

- https://nvd.nist.gov/

b. Perform vulnerability assessment using various vulnerability assessment tools

i. **Perform vulnerability analysis using OpenVAS**

ii. **Perform vulnerability scanning using Nessus**

iii. **Perform web servers and applications vulnerability scanning using CGI Scanner Nikto**

- nikto -h [Target website] -Tuning x
  (The -Tuning option in Nikto allows you to fine-tune which types of tests are run. The letter x in this case means that all types of checks will be performed (i.e., no filtering, so Nikto will run all its tests).)

- nikto -h [Target website] -Cgidirs all
  (-Cgidirs all: This option tells Nikto to check for CGI directories. CGI (Common Gateway Interface) is a standard for running external programs (usually scripts) via web servers. Using all will have Nikto scan all potential CGI directories it knows about, instead of just the default ones.)
- nikto -h [Target website] -o result.txt -F txt