Limitations:

- False Positives: Automated scans and tools can generate false positive results, indicating a vulnerability that does not actually exist.
- False Negatives: Automated scans and tools can also miss real vulnerabilities, resulting in false negatives.
- Resource Constraints: The time and resources available for the assessment may impact the scope and depth of the assessment.
- Changes in the Environment: The website and its infrastructure can change during the course of the assessment, affecting the results.
- Limited Testing Scope: The assessment may only cover a portion of the website, leaving other areas untested.
- Technical Limitations: The assessment may be limited by the skills and expertise of the tester, as well as the tools and techniques available.

Assumptions:

- Active Threats: The assessment assumes that the website is currently under attack or at risk of attack.
- No Internal Access: The assessment assumes that the tester does not have access to internal systems or data.
- No Interference with Production: The assessment assumes that the testing will not interfere with the normal functioning of the website.
- No Prior Knowledge: The assessment assumes that the tester has no prior knowledge of the website or its infrastructure.
- No Tampering: The assessment assumes that the tester will not intentionally harm the website or its data.

These limitations and assumptions should be considered when conducting a vulnerability audit and assessment of a website. It is important to ensure that the results are interpreted correctly and that appropriate measures are taken to address any identified vulnerabilities.