Question Number 9

- Visit https://maliciousssha1.github.io/
- Find out what is the vulnerability.

Solution. The vulnerability lies in the modification of SHA-1's predefined constants K_1, K_2, K_3, K_4, which are used in different 20-step rounds of the algorithm. By carefully tweaking these constants, attackers can introduce undetectable backdoors in the cryptographic function. This does not weaken the original SHA-1 but affects custom implementations where these constants are altered.

Below were few Exploitation Process that attacker can use:
Differential Characteristics: Attackers use state-of-the-art differential cryptanalysis to find high-probability patterns of differences in message blocks, which propagate through the SHA-1 algorithm.
Message Construction: Colliding messages are created by modifying input blocks and the constants to align with the chosen differential characteristic.
Collision Generation: Maliciously modified SHA-1 allows the designer to generate files that hash to the same value while containing completely different content.

Key Implications:
Backdoors: Custom SHA-1 versions can act as cryptographic backdoors, exploitable only by the designer.
Undetectable: These modifications remain as strong as the original SHA-1, making the backdoor invisible to external analysis.
Polyglot Collisions: Attackers can create colliding files across multiple formats, such as archives and executables, with controlled payloads.