References

- **MS17-010 (EternalBlue)**
  Microsoft Security Bulletin: `https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0144`
  Description: A critical vulnerability in Microsoft's SMBv1 protocol that allows remote code execution.

- **Weak Credential Authentication (Brute-force)**
  OWASP Authentication Cheat Sheet: `https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html`
  Description: Weak or default passwords can be brute-forced to gain unauthorized access.

- **Local File Inclusion (LFI)**
  OWASP LFI Guide: `https://owasp.org/www-community/attacks/Local_File_Inclusion`
  Description: LFI allows attackers to read files on the server via vulnerable input parameters.

- **Log Poisoning (Attempted)**
  CWE-117: Improper Output Neutralization for Logs: `https://cwe.mitre.org/data/definitions/117.html`
  Description: An attacker injects PHP code or commands into logs and uses LFI to execute them.