Documentation Submission for Network Vulnerability Assessment

1. Introduction

- **Project Overview:**
  - The purpose of this assessment was to identify and mitigate critical vulnerabilities in an imaginary website to enhance its security posture. The assessment was conducted using tools like Nessus/OpenVAS, and the findings were used to develop a comprehensive mitigation plan.
- **Scope:**
  - The assessment covered all aspects of the website's network infrastructure, including web applications, database connections, and user authentication mechanisms.
- **Objective:**
  - The primary objective was to evaluate the website's security, identify at least five critical vulnerabilities, and propose actionable remediation strategies to mitigate these risks.

2. Vulnerabilities Identified

1. **Outdated CMS Version:**
   - **Description:** The website was running an outdated version of its Content Management System (CMS), making it vulnerable to known exploits.
   - **Severity:** High
   - **Potential Impact:** An attacker could exploit known vulnerabilities to gain unauthorized access or execute arbitrary code on the server.
   - **Evidence:** [Include a screenshot or report snippet from Nessus/OpenVAS highlighting the outdated CMS version.]
2. **SQL Injection Vulnerability:**
   - **Description:** The search functionality was susceptible to SQL injection, allowing attackers to manipulate database queries.
   - **Severity:** Critical
   - **Potential Impact:** An attacker could gain unauthorized access to sensitive data or manipulate the database.
   - **Evidence:** [Include a screenshot or code snippet demonstrating the SQL injection vulnerability.]
3. **Cross-Site Scripting (XSS):**
   - **Description:** The website allowed the input of malicious scripts that could execute in users' browsers, leading to potential data theft or session hijacking.
   - **Severity:** High
   - **Potential Impact:** An attacker could execute arbitrary scripts in the context of a user's session, potentially leading to data breaches.
   - **Evidence:** [Include a screenshot or report snippet showing the XSS vulnerability.]
4. **Weak Password Policy:**
   - **Description:** The administrative accounts were using weak passwords that could be easily guessed or cracked using brute-force attacks.
   - **Severity:** Medium
   - **Potential Impact:** An attacker could gain unauthorized access to administrative accounts, compromising the entire website.

    - **Evidence:** [Include details or a screenshot showing the weak password policy.]
5. **Unencrypted Data Transmission:**
    - **Description:** Sensitive data was being transmitted over HTTP instead of HTTPS, making it susceptible to interception by attackers.
    - **Severity:** High
    - **Potential Impact:** An attacker could intercept and manipulate data transmitted between the client and server.
    - **Evidence:** [Include a screenshot or report snippet indicating the lack of HTTPS.]

3. Mitigation Plan

- **Outdated CMS Version:**
    - **Remediation Steps:**
        - Backup the website.
        - Update to the latest CMS version.
        - Test for functionality post-update.
    - **Timeline:** 1-2 days
    - **Resources:** Backup tools, developer expertise.
- **SQL Injection Vulnerability:**
    - **Remediation Steps:**
        - Sanitize inputs using parameterized queries.
        - Test to ensure vulnerability is mitigated.
    - **Timeline:** 2-3 days
    - **Resources:** Developer expertise, code access.
- **Cross-Site Scripting (XSS):**
    - **Remediation Steps:**
        - Implement input validation and output encoding.
        - Test for XSS vulnerabilities.
    - **Timeline:** 2-3 days
    - **Resources:** Developer expertise, code access.
- **Weak Password Policy:**
    - **Remediation Steps:**
        - Implement a strong password policy.
        - Enforce a password reset.
        - Implement multi-factor authentication.
    - **Timeline:** 1 day
    - **Resources:** Admin access, MFA tools.
- **Unencrypted Data Transmission:**
    - **Remediation Steps:**
        - Obtain and install an SSL/TLS certificate.
        - Configure HTTPS and redirect HTTP traffic.
        - Test for secure transmission.
    - **Timeline:** 1-2 days
    - **Resources:** SSL/TLS certificate, web server configuration access.

4. Additional Recommendations

- **Regular Vulnerability Scans:**
  - Schedule regular vulnerability scans using Nessus/OpenVAS to identify new vulnerabilities.
- **User Training:**
  - Conduct regular security training for users to prevent human error-related vulnerabilities.
- **Security Incident Response Plan:**
  - Develop and implement a security incident response plan to quickly address any potential breaches.

5. Conclusion

- The network vulnerability assessment identified five critical vulnerabilities in the website. A comprehensive mitigation plan was developed and implemented to address these issues, significantly improving the security of the website. Ongoing monitoring and regular updates are recommended to maintain a robust security posture.

6. Appendices

- **Appendix A:** Full Vulnerability Scan Report
- **Appendix B:** Code Snippets/Configuration Files
- **Appendix C:** Presentation Slides

7. Submission Details

- **Report Submission Date:** 12.08.2024
- **Prepared By:** Swarnadyuti Sarkar