Week Four at Pandora Company Limited

Web Woes Uncovered

Name – Nonis S.S.L Index No – 210439P

Introduction

Pandora Company Limited's corporate website, hosted at http://www.pandora.lk, was developed on the WordPress platform and has been running for two years. The website features a "Sales Inquiries" form, which collects sensitive personal information from clients, including names, mobile numbers, and home addresses. Since its launch, the admin credentials have remained sealed and unused, raising concerns about potential security lapses. Moreover, the website relies on the MySQL/MariaDB root account for database access, posing significant risks. This report will analyze these vulnerabilities and offer recommendations to enhance the security of the website.

Assessing the Current State

1. **Absence of HTTPS**
   The website is served over http://www.pandora.lk, which indicates that it is not utilizing HTTPS for encrypted communication. This poses a significant risk, as sensitive data submitted via forms (like the "Sales Inquiries" form) could be intercepted in transit, exposing clients' personal information (Name, Mobile Number, Date of Birth, NIC, and Home Address).

2. **Use of MySQL/MariaDB Root User**
   The WordPress installation uses the database root user for all interactions. This practice violates the principle of least privilege. Any vulnerability within the website could lead to complete database compromise, given the extensive permissions of the root user.

3. **Admin Credentials in a Sealed Envelope**
   It is concerning that the admin credentials have not been updated or verified since the website's launch two years ago. The default credentials may still be in place, which is a potential vector for brute-force or credential-stuffing attacks.

4. **Outdated WordPress Version**
   If the WordPress installation has not been updated since its initial launch two years ago (as assumed), it is likely running an outdated version that may contain known vulnerabilities. WordPress regularly releases updates to address security flaws, performance issues, and compatibility problems.

Potential Vulnerabilities

1. **Lack of HTTPS**
   Without HTTPS, there is a potential vulnerability to **Man-in-the-Middle (MITM) attacks**, where attackers can intercept and manipulate communication between clients and the server.

2. **Exposed Sensitive Data**
   Sensitive personal information is being collected through the "Sales Inquiries" form, which, if improperly secured, could be leaked. Since the form submits data over HTTP, an attacker could capture this data with ease.

3. **Database Access with Root Privileges**
   Using the root database account for daily interactions increases the risk of privilege escalation. A compromised WordPress plugin, theme, or weak point in the code could allow an attacker to execute malicious queries with full control over the database.

4. **Outdated Admin Credentials**
   The fact that admin credentials have remained unused since the launch of the website may mean they were never updated from their default settings, leaving the website vulnerable to common credential-based attacks.

Security Intervention Proposals

1. **Implement HTTPS**
   Pandora Company Limited must secure the website by enforcing HTTPS. This can be achieved by obtaining an SSL/TLS certificate and configuring the webserver to redirect all HTTP requests to HTTPS.

2. **Database Access Best Practices**
   The website should be configured to use a specific database user with limited privileges. Without the DROP or ALTER privileges, this user should have only the necessary permissions for WordPress to function, such as SELECT, INSERT, UPDATE, and DELETE for relevant tables.

3. **Update Admin Credentials**
   The sealed envelope containing admin credentials should be discarded, and the WordPress admin credentials should be updated immediately. Passwords should be strong, random, and stored securely. Additionally, two-factor authentication (2FA) should be implemented for admin accounts.

4. **Form Data Protection**
   To protect form submissions, the site should be configured to use HTTPS as mentioned. Additionally, consider using data encryption for storing sensitive information like NICs and home addresses in the database. WordPress plugins that handle personal data should be reviewed to ensure they are safe and up to date.

Recommending Best Practices for Future Security

1. **Regular Security Audits**
   Pandora Company Limited should conduct regular security audits, including vulnerability scanning and penetration testing, to identify and address potential issues before they are exploited.

2. **Keeping Software Up to Date**
   WordPress and all installed plugins and themes should be regularly updated to patch known vulnerabilities. This can be managed via automatic updates or a dedicated technical team to ensure timely updates.

3. **Backup and Disaster Recovery Plan**
   Regular backups of the website and its database should be maintained to ensure data can be restored in case of a breach. These backups should be stored securely and verified periodically.

4. **Implement Web Application Firewall (WAF)**
   Deploying a WAF can help prevent common web-based attacks like SQL injection, cross-site scripting (XSS), and brute-force attacks. A WAF can inspect and filter incoming traffic to ensure malicious activity is blocked.

5. **User Role Management**
   Ensure that all WordPress users have appropriate roles and permissions. Admin-level access should be restricted to essential personnel, and any inactive or unnecessary accounts should be removed.

Reference

- WordPress. (n.d.). Hardening WordPress. Retrieved from https://wordpress.org/support/article/hardening-wordpress/
- OWASP Top Ten Web Application Security Risks. Retrieved from https://owasp.org/www-project-top-ten/
- National Institute of Standards and Technology (NIST) Cybersecurity Framework https://www.nist.gov/quickstart-guides/
- Kaspersky articles
  https://www.kaspersky.com/resource-center/preemptive-safety/are-online-survey-sitessafe/
  https://www.kaspersky.com/resource-center/preemptive-safety/how-often-password-change
- Coursera
  https://www.coursera.org/articles/cybersecurity-best-practices/