Week Four at Pandora Company Limited: Web Woes Uncovered

Project Part 3

Name : Lahiru Randika **Index :** 210527J

Introduction

The corporate website of Pandora Company Limited, accessible at http://www.pandora.lk, was developed using WordPress and has been operational for two years. It includes a "Sales Inquiries" form that collects sensitive client information, such as names, mobile numbers, and addresses. Since its launch, the admin credentials have remained sealed and unused, raising security concerns. Furthermore, the site relies on the MySQL/MariaDB root user for database access, which poses significant risks. This report evaluates these vulnerabilities and provides recommendations for improving the website's security

Risk Assessment

Risk assessment is the process of identifying, analyzing, and evaluating potential threats to an organization's systems or data to mitigate vulnerabilities. After reviewing the provided details of the Pandora company, several critical security risks were identified:

1. **Lack of HTTPS**: The website is served over HTTP instead of HTTPS. This means all data transmitted through the website, including sensitive personal information submitted via forms, is vulnerable to interception by malicious actors. Attackers could use techniques like Man-in-the-Middle (MITM) attacks to steal or tamper with this data.
2. **Unaccessed Admin Credentials**: The admin credentials, sealed and untouched since launch, pose a risk of outdated or weak passwords. This increases the likelihood of brute-force attacks or unauthorized access.
3. **Use of Root Database User**: The WordPress installation interacts with the database using the root MySQL/MariaDB account, which has unrestricted access to all database functions. This could lead to severe consequences if the website is compromised, allowing attackers full control over the database.
4. **Outdated WordPress Version**: If the WordPress installation has not been updated since its launch (assumption), it may be running an outdated version that contains known vulnerabilities. This can make the website an easy target for attackers.

Identified Vulnerabilities

Considering Pandora Company Limited's current website configuration and its handling of sensitive client data, the following vulnerabilities were identified:

1. **Lack of Encryption (No SSL/TLS)**: The website is served over HTTP, which means that all data transmitted between users and the server is not encrypted. This poses a critical risk, especially for sensitive information collected through the "Sales Inquiries" form. Attackers can easily intercept this data using techniques like packet sniffing or Man-in-the-Middle (MITM) attacks, leading to potential data breaches and identity theft. Implementing SSL/TLS would ensure that data is encrypted during transmission, significantly reducing this risk.
2. **Weak Admin Credentials**: The admin credentials have remained unchanged since the website's launch, which raises concerns about their strength. If the credentials are weak (e.g., simple passwords or common passwords), they are vulnerable to brute-force attacks, where attackers use automated tools to guess

passwords. Additionally, if no multi-factor authentication (MFA) is in place, the risk of unauthorized access increases significantly. A strong password policy and regular updates to credentials are essential to mitigate this vulnerability.

3. **Database Root Access**: Utilizing the MySQL/MariaDB root user for database interactions is a serious misconfiguration. The root user has unrestricted access to all database functions, which is unnecessary and poses a significant security risk. If an attacker gains access to the WordPress installation (e.g., through a plugin vulnerability or compromised admin account), they could exploit this to execute arbitrary SQL commands, leading to data manipulation, deletion, or even full database compromise. Creating a dedicated database user with limited privileges tailored to the WordPress application's needs is crucial for minimizing this risk.

4. **Potential Outdated Software**: Given that the website has been operational for two years without updates, both the WordPress core and its plugins are likely outdated. Outdated software can contain known vulnerabilities that attackers can exploit. Many security vulnerabilities are regularly patched by developers, and failing to update the software leaves the site exposed to these risks. Regular maintenance and timely updates are vital to protect against exploits that target outdated code.

5. **Insufficient Input Validation (Assumption):** The "Sales Inquiries" form may lack proper input validation and sanitization measures. This could make it susceptible to attacks such as SQL injection, where an attacker injects malicious SQL code through user input to manipulate the database. Ensuring that all user inputs are validated and sanitized can prevent such vulnerabilities.

Security Interventions

To address and mitigate the identified risks associated with Pandora Company Limited's website and its management of sensitive client information, the following security measures are strongly recommended:

1. **Implement SSL/TLS Encryption**: It is crucial for Pandora company to immediately obtain and install an SSL/TLS certificate to enable HTTPS on the website. This encryption ensures that all data transmitted between the client and server is secure, protecting sensitive information from interception by malicious actors. In addition to securing data in transit, HTTPS also boosts user trust and may improve search engine rankings. A well-configured SSL certificate can also prevent certain types of attacks, such as eavesdropping and session hijacking.

2. **Update Admin Credentials**: The admin credentials should be changed immediately to a strong and unique password. Implementing a lengthy, strong password policy that requires a mix of upper and lower-case letters, numbers, and special characters will enhance security. Additionally, enabling multi-factor authentication (MFA) is critical. MFA adds an extra layer of protection by requiring users to provide two or more verification factors to access their accounts, significantly reducing the risk of unauthorized access even if passwords are compromised.

3. **Use a Dedicated Database User**: To enhance database security, Pandora company should create a dedicated database user specifically for the WordPress installation. This user should have the minimum necessary privileges required for the application to function, following the principle of least privilege. This approach minimizes the potential damage if the website is compromised, as attackers would have restricted access to the database. Regularly reviewing and adjusting user permissions can further improve security.

4. **Update WordPress and Plugins**: It is essential to regularly update the WordPress core, themes, and all plugins to ensure that any known vulnerabilities are patched. Setting up automatic updates (under controlled conditions) where possible can help keep the site secure with minimal manual intervention. Additionally, conducting routine maintenance checks to evaluate the necessity and security of installed plugins can help to eliminate any that are outdated or no longer needed, reducing the attack surface.

5. **Conduct Regular Security Audits**: Implement a routine schedule for comprehensive security audits and vulnerability assessments of the website. This process should include penetration testing, code reviews, and

assessments of third-party plugins and themes to identify and address potential weaknesses before they can be exploited.

6. **Establish a Backup and Recovery Plan**: Implement a robust backup strategy that includes regular backups of the website files and database. These backups should be stored securely and tested periodically to ensure they can be restored successfully. A well-defined recovery plan will help minimize downtime and data loss in the event of a cyber incident or other failures.

7. **Enhance Input Validation and Sanitization**: It is vital to implement strict input validation and sanitization measures for all user input fields, particularly for the "Sales Inquiries" form. This will help prevent common vulnerabilities such as SQL injection and cross-site scripting (XSS). Utilizing security libraries and frameworks that provide built-in protections against these attacks can further enhance the site's security posture.

8. **Implement Web Application Firewalls (WAF)**: Consider deploying a Web Application Firewall to monitor and filter incoming traffic to the website. A WAF can help detect and block malicious traffic, protect against common web attacks, and provide an additional layer of security by analyzing incoming requests and filtering out harmful content.

Best Practices for Future Security

Best practices are standardized, effective methods or techniques that have been proven to achieve optimal results in a particular field or process. To maintain the long-term security of the website, Pandora Company Limited should adopt the following practices:

1. **Regular Security Audits**: Conduct periodic security assessments to proactively identify vulnerabilities and potential threats. These audits should include vulnerability scans, penetration tests, and code reviews. Engaging with third-party security experts for independent assessments can provide an objective view of the site's security posture. Regular audits help ensure that new vulnerabilities are addressed swiftly and that security measures are effective.

2. **Patch Management**: Establish a structured patch management process that includes regular updates for WordPress, all installed plugins, and server software. Automated notifications for updates should be enabled to keep the site secure against newly discovered vulnerabilities. A patch management policy should also outline the testing of updates in a staging environment before deployment to ensure that updates do not disrupt the website's functionality.

3. **Backup and Recovery Plan**: Implement a comprehensive backup strategy that includes automated, regular backups of both the website files and the database. Backups should be stored securely in multiple locations, including offsite or cloud-based storage solutions. Regularly testing the restoration process is crucial to ensure that backups can be successfully recovered in the event of data loss due to an attack or system failure, minimizing downtime and loss of critical data.

4. **Monitoring and Logging**: Set up real-time monitoring and logging of all website activities to detect suspicious behavior and potential security incidents. Implementing tools like intrusion detection systems (IDS) can alert the technical team to any abnormal activities. Additionally, maintaining detailed logs of user activity can provide insights into potential security breaches and help in forensic investigations if an incident occurs.

5. **Least Privilege Principle**: Apply the principle of least privilege when assigning access rights to users, ensuring that they only have the necessary permissions to perform their tasks. Regularly reviewing and updating user roles and permissions can help prevent unauthorized access and limit the potential damage from compromised accounts. Training employees on security best practices and the importance of access controls further enhances the effectiveness of this principle.

6. **User Education and Awareness**: Conduct regular training sessions for all employees to raise awareness of cybersecurity threats, including phishing attacks and social engineering. Educating staff on how to recognize

suspicious activities and follow security protocols will strengthen the overall security culture within the organization.

7. **Incident Response Plan**: Develop and maintain a comprehensive incident response plan that outlines the steps to take in the event of a security breach. This plan should include roles and responsibilities, communication protocols, and procedures for containment, eradication, and recovery. Regular drills and reviews of the plan can help ensure that all team members are prepared to respond effectively to incidents.

References

- National Institute of Standards and Technology (NIST) Cybersecurity Framework < https://www.nist.gov/quick-start-guides/ >
- OWASP Top 10 Security Risks for Web Applications < https://owasp.org/www-project-top-ten/ >
- Acunetix < https://www.acunetix.com/blog/wordpress-security/risks-in-using-the-root-account/ >
- WordPress.org. < https://developer.wordpress.org/advanced-administration/security/hardening/ >

  < https://wordpress.org/documentation/article/updating-wordpress/ >
- Kaspersky articles < https://www.kaspersky.com/resource-center/preemptive-safety/are-online-survey-sites-safe/ > < https://www.kaspersky.com/resource-center/preemptive-safety/how-often-password-change >
- Web.dev < https://web.dev/articles/why-https-matters/ >
- Calpoly < https://security.calpoly.edu/content/practices/good_practices/ >
- Netwrix < https://blog.netwrix.com/2014/06/17/why-you-need-to-ensure-administrators-change-passwords-regularly/ >
- Coursera < https://www.coursera.org/articles/cybersecurity-best-practices/ >
- PhoenixNap < https://phoenixnap.com/blog/cybersecurity-best-practices/ >