Security Assessment and Recommendations for Pandora Company Limited

Prepared by: Muaadh MNM

200401J

Date: Sep 2023

Contents

Introduction

This report outlines the security assessment conducted for the corporate website of Pandora Company Limited. The assessment identifies potential risks, vulnerabilities, and proposes security interventions and best practices for future maintenance.

1 Assessment of Current State

1.1 Potential Risks

1. **Unencrypted Data Transmission:** Serving the website over HTTP instead of HTTPS can expose the data transmitted between the server and the clients to eavesdropping and man-in-the-middle attacks.

2. **Unopened Admin Credentials:**

   - **Unauthorized Access:** Risk of unauthorized access and control over the website if the envelope containing the credentials falls into the wrong hands.
   - **Loss of Credentials:** Since the envelope has not been opened for a long time, there is a risk of misplacing or losing it, which could lead to serious issues in managing the website in the future .

3. **Outdated Website:**

   - **Security Vulnerabilities:** Older versions of WordPress often have known vulnerabilities that can be exploited by attackers.
   - **Compatibility Issues:** There might be compatibility issues with newer browsers or plugins, leading to poor user experience.

4. **Data Collection through "Sales Inquiries" Form:**

   - **Data Leakage**: The collection of sensitive personal information could potentially be misused or leaked, violating user privacy.
   - **Non-Compliance with GDPR**: The website might not be compliant with GDPR or other privacy regulations, posing legal risks.

5. **Database Interaction using MySQL/MariaDB Root User:**

   - **Security Risks:** Using the root user for database interactions is a significant security risk as it grants full permissions, making it a lucrative target for attackers [**?**].
   - **Data Corruption:** In case of a system failure or cyber attack, there is a high risk of data corruption or loss .

2 Identification of Potential Vulnerabilities

1. **SQL Injection:** Given that the website uses the root user for database interactions, it might be vulnerable to SQL injection attacks, where attackers can manipulate SQL queries to extract, modify, or delete data from the database.

   Granting root user access for database interactions comes with a host of potential pitfalls that significantly elevate the risk profile of a system. Primarily, it opens up the avenues for severe security breaches, including unauthorized data access, alteration, and deletion due to the unfettered permissions associated with a root account. This omnipotent access can turn minor vulnerabilities into catastrophic ones, as an attacker gaining root privileges would have the ability to execute far-reaching commands, potentially manipulating or erasing entire databases.

2. **Insecure Data Transfer:** The website is served over HTTP, not HTTPS, meaning the data transmitted is unencrypted and can be intercepted by attackers.

   Utilizing HTTP (HyperText Transfer Protocol) for data transmission in the modern web ecosystem harbors several pronounced drawbacks, primarily revolving around security and data integrity. First and foremost, HTTP operates in plaintext, meaning that data transmitted over HTTP can be intercepted and read easily by third parties, paving the way for eavesdropping and man-in-the-middle (MitM) attacks where confidential information such as usernames, passwords, and financial details can be stolen. This plaintext transmission also implies a vulnerability to data manipulation; malicious actors can alter data during transmission, affecting the integrity of the information exchanged. Besides security concerns, using HTTP can result in diminished trust from users and lower SEO rankings, as search engines prioritize secure HTTPs sites. Modern browsers flag HTTP sites as "Not Secure," dissuading users from interacting with such websites, thereby potentially reducing traffic and user engagement.

3. **Cross-Site Scripting (XSS):** The WordPress platform might be susceptible to XSS attacks, where attackers can inject malicious scripts into the website, affecting the users who visit the site.

   Cross-Site Scripting (XSS) is a prevalent vulnerability in WordPress websites, stemming primarily from poorly coded themes and plugins. In an XSS attack, malicious scripts are injected into websites and executed in the browsers of unsuspecting users who visit the compromised site. These scripts can then steal information such as cookies, session tokens, or other sensitive information from the user's browser.

   WordPress sites can be particularly susceptible to XSS attacks due to the vast array of plugins and themes available, many of which are developed without stringent security practices. Moreover, outdated WordPress core files can contain known vulnerabilities that might be exploited via XSS attacks.

4. **Outdated Software:** Since the website was launched two years ago and hasn't been maintained actively, there might be outdated plugins or WordPress versions running, which could have known vulnerabilities.

   Using outdated software is a prominent security risk, particularly in platforms as extensively used as WordPress. Outdated software often contains well-known vulnerabilities that have been addressed in newer versions. These vulnerabilities can potentially be exploited by cybercriminals to initiate a range of attacks, including SQL injection, cross-site scripting (XSS), and more, leveraging the uncovered weaknesses to infiltrate websites, steal sensitive data, or even take control of the site's operations.

   Apart from security risks, outdated software can lead to compatibility issues. New plugins, themes, or other software updates might not function correctly with older versions, leading to broken functionalities and a deteriorated user experience. Moreover, older versions might not be optimized for performance, leading to slower load times and inefficiencies, which can negatively impact the user experience and SEO rankings.

5. **Brute Force Attacks:** The WordPress admin panel might be vulnerable to brute force attacks, where attackers try numerous combinations of usernames and passwords to gain access.

   For WordPress websites, brute force attacks typically manifest in repeated login attempts to the admin panel, leveraging automated scripts to guess the username and password. This not only poses a severe risk of unauthorized access but can also strain the server resources, leading to a slower website performance and, in severe cases, a denial of service.

The ramifications of a successful brute force attack are serious; unauthorized users can gain complete control over the WordPress site, potentially altering content, stealing sensitive data, or injecting malicious content aimed at site visitors.

3 Proposed Security Interventions

1. **Change Credentials:** Immediately change the admin credentials and store them securely using a password management solution.
   (a) **Importance**
      i. **Preventing Unauthorized Access:** Admin accounts hold the keys to your website's kingdom; they have the highest level of access and control. Thus, ensuring that only authorized individuals have the admin credentials is paramount to prevent unauthorized access and potential misuse.
      ii. **Mitigating Insider Threats:** Changing credentials periodically can mitigate risks associated with insider threats, which involves individuals within the organization misusing their access rights.
      iii. **Compliance:** Many industry standards and regulations mandate periodic changes to admin credentials to ensure a high level of security.
2. **Implement HTTPS:** Transition the website to HTTPS to encrypt data in transit, protecting it from eavesdroppers and man-in-the-middle attacks.
   (a) **Importance**
      i. Data Encryption
         A. **Confidentiality**: HTTPS encrypts the data transmitted between the user's browser and the website, protecting sensitive information from eavesdroppers.
         B. **Integrity:** It ensures that the data cannot be modified during transmission without detection.
      ii. Authentication and Trust
         A. **Authenticity:** HTTPS verifies the identity of the website, reassuring users that they are communicating with the genuine site and not a fraudulent one.
         B. **Trust**: Websites with HTTPS are often highlighted with a padlock symbol or a green address bar in browsers, signaling a secure connection and building user trust.
      iii. SEO Ranking
         A. **SEO Boost:** Search engines favor HTTPS websites, potentially enhancing the site's SEO rankings.
      iv. Compliance
         A. **Legal Compliance:** Various regulations and standards require websites to secure data transmission, fulfilling legal and compliance requirements.
         B. **Payment Card Industry (PCI) Compliance**: If the site handles transactions, implementing HTTPS is a requirement to comply with PCI standards.
      v. **Protection from Man-in-the-Middle (MitM) Attacks**
         A. Security: HTTPS helps in protecting the website from MitM attacks where attackers can intercept and alter communications between the website and the user.
      vi. **Secure Online Transactions**
         A. Safety: For e-commerce websites, HTTPS is essential in securing online transactions and protecting customer data.

3. **Restrict Database Privileges:** Change the database user to one with limited privileges to reduce the potential damage in case of SQL injection attacks.

   (a) **Importance**

      i. **Preventing Unauthorized Access:** Helps to avert potential unauthorized access to various database segments.
      ii. **Mitigating SQL Injections:** Limits the damage potential of SQL injection attacks by restricting the areas an injected SQL query can access.
      iii. **Ensuring Data Integrity:** Maintains the consistency and accuracy of data over its entire lifecycle by preventing unauthorized alterations.
      iv. **Maintaining Data Confidentiality:** Facilitates the protection of sensitive data by limiting the number of users who can access it.
      v. **Abiding by the Principle of Least Privilege:** Adheres to security best practices by only granting necessary access rights to users, thus minimizing potential damage from security breaches.
      vi. **Facilitating Regulatory Compliance:** Helps in complying with various legal and industry standards that mandate restricted access to sensitive data.
      vii. **Simplified Troubleshooting:** Makes it easier to identify issues and fix them due to the clear delineation of access levels.
      viii. **Protecting Business Reputation:** Helps in safeguarding the organization's reputation by minimizing the potential damage from data breaches.
      ix. **Enhancing Efficiency in Management:** Allows for a smoother management process by clearly defining user roles and access levels.

4. **Principle of Least Privilege (PoLP):** Configure the database to follow the PoLP, ensuring services and users have the minimum access — and permissions — necessary to accomplish their tasks.

   (a) **Importance**

      i. **Security Enhancement:** Reducing the access level of various users minimizes the risk of a potential security breach.
      ii. **Mitigating Insider Threats:** Restricts the potential for misuse from inside the organization.
      iii. **Simplified Troubleshooting:** Makes it easier to pinpoint issues since users have limited and defined roles and permissions.

5. **Regular Updates:** Ensure that the WordPress installation, along with all plugins and themes, are regularly updated to patch known vulnerabilities.

   (a) **Importance**

      i. **Security:** Patching known vulnerabilities helps in protecting the site from known threats.
      ii. **Performance:** Updates often come with improvements in performance, offering a better user experience.
      iii. **New Features:** Regular updates often bring new features, enhancing the functionality of the website.

6. **Multi-Factor Authentication (MFA):** Implement MFA for the admin panel to add an extra layer of security against brute force and other unauthorized access attempts.

   (a) **Importance**

      i. **Improved Security:** Adds an additional layer of security, making it harder for unauthorized users to gain access.
      ii. **Protection Against Phishing:** MFA can provide protection even if login credentials are compromised.
      iii. **Compliance:** Meets regulatory requirements that mandate stronger authentication processes.

7. **Data Encryption:** Encrypt sensitive data both at rest and in transit to protect it from unauthorized access.

   (a) **Importance**

      i. **Data Security:** Protects sensitive data from unauthorized access.

      ii. **Compliance:** Helps in fulfilling various legal and compliance requirements related to data protection.

      iii. **Trust:** Builds user trust by showcasing a commitment to protecting their data.

4 Recommended Best Practices for the Future

(a) **Regular Security Audits and Penetration Testing:** Regularly conduct security audits and penetration tests to identify and fix vulnerabilities.

   i. **Importance**

      A. **Proactive Security:** Identifies vulnerabilities before they can be exploited, enhancing security posture.

      B. **Regulatory Compliance:** Helps in meeting regulatory requirements, avoiding penalties and preserving reputation.

      C. **Improving User Trust:** Demonstrates a commitment to security, fostering trust with users and clients.

(b) **Data Minimization:** Collect only the necessary data from clients to reduce the risk associated with data handling.

   i. **Importance**

      A. **Reduced Risk Exposure:** Minimizes the risk of data breaches by limiting the amount of data stored.

      B. **Legal Compliance:** Aids in adhering to regulations that emphasize data minimization, mitigating legal risks.

      C. **Improved User Experience:** Can lead to a streamlined user experience by requesting less information from users.

(c) **Data Privacy Compliance:** Ensure the website complies with data protection regulations such as GDPR to mitigate legal risks.

   i. **Importance**

      A. **Legal Safety:** Ensures adherence to prevailing laws, reducing legal risks and potential fines.

      B. **Reputation Management:** Upholding data privacy principles can foster a good reputation and client trust.

      C. **User Trust:** Being compliant with regulations demonstrates a commitment to user privacy, building trust.

(d) **Incident Response Plan:** Develop an incident response plan to handle potential security incidents efficiently and minimize damage.

   i. **Importance**

      A. **Damage Mitigation:** Enables a swift response to security incidents, potentially reducing the damage incurred.

      B. **Operational Continuity:** Ensures that the business can continue operating smoothly even in the event of an incident.

      C. **Legal Preparedness:** Helps in meeting legal and regulatory obligations in case of data breaches or other incidents.

(e) **Employee Training:** Train employees on cybersecurity best practices to foster a security-conscious work environment.

   i. **Importance**

      A. **Threat Reduction:** Educated employees can identify and avoid potential security threats, reducing the risk of breaches.

B. **Best Practices:** Ensures that employees follow best practices, enhancing overall security posture.

C. **Culture of Security:** Cultivates a culture where security is everyone's responsibility, promoting proactive security measures.

(f) **Backup and Recovery:** Establish a robust backup and recovery strategy to ensure data integrity and availability in case of incidents like data corruption or hardware failure.

i. **Importance**

A. **Data Integrity:** Ensures data is recoverable, maintaining data integrity in various failure scenarios.

B. **Business Continuity:** Facilitates business continuity by allowing quick recovery from incidents.

C. **Avoiding Data Loss:** Regular backups prevent total data loss, safeguarding critical business and customer data.

Conclusion

By addressing these vulnerabilities and implementing the recommended security interventions, Pandora Company Limited can significantly enhance the security posture of its corporate website. It is essential to adopt a proactive approach to cybersecurity, focusing on regular updates, monitoring, and employee training to ensure the website's ongoing security and resilience to cyber threats.

References

(a) Security in Computing , Fifth Edition by Charles P. Fleeger

i. Chapter 2 - Toolbox

ii. Chapter 4 - Database Security

iii. Chapter 6 - Web Security

iv. Chapter 4 - The Web User Side

v. Chapter 11 - Legal Issues and Ethics