**Penetration Testing Report**

**Client:** Inlane Freight  
**Assessment Type:** WordPress Security Assessment  
**Date:** [Insert Date]  
**Prepared by:** [Your Name/Your Company]

**Executive Summary**

This report outlines the findings from the penetration test conducted on the WordPress site hosted at **http://blog.inlanefreight.local/**. The assessment aimed to identify vulnerabilities, exploit them, and provide recommendations for improving the security posture of the WordPress installation.

**Findings**

**1. Site Enumeration**

* **Accessed Site:** **http://blog.inlanefreight.local/**
* **WordPress Version:** 5.1.6
* **Active Theme:** Twenty Nineteen

**2. User Enumeration**

Identified users through various methods:

* **Users Found:**
  + **erika**
    - Confirmed by: Author Posts, RSS Generator, Author ID Brute Forcing, Login Error Messages
  + **admin**
    - Confirmed by: Author Posts, RSS Generator, Author ID Brute Forcing, Login Error Messages
  + **Charlie Wiggins**
    - Confirmed by: Author ID Brute Forcing

**3. Password Attacks**

* **Performed XML-RPC password attack:**
  + Users targeted: **admin**, **erika**
  + **Successful Login:** **erika** / **010203**

**4. Remote Code Execution (RCE)**

* **Exploited the Twenty Seventeen theme:**
  + Uploaded a web shell via **404.php**.
  + Validated RCE by executing commands:
    - **curl -X GET "http://blog.inlanefreight.local/wp-content/themes/twentyseventeen/404.php?cmd=id"**
    - Retrieved flag: **HTB{w0rdPr355\_4SS3ssm3n7}**

**5. Database Credentials Extraction**

* Retrieved database credentials from **wp-config.php**:
  + **DB User:** wp-admin
  + **DB Password:** WP\_wp\_skillz!

**6. File Disclosure Vulnerability**

* **Vulnerable Plugin:** Email Subscribers & Newsletters < 4.2.3
* **Exploited to retrieve user information:**
  + Retrieved flag: **HTB{unauTh\_d0wn10ad!}**

**7. Local File Inclusion (LFI)**

* **Vulnerable Plugin:** Site Editor <= 1.1.1
* **Exploited to read /etc/passwd:**
  + Identified user: **frank.mclane**

**8. Shell Access**

* **Gained shell access using Metasploit and manual methods.**
* **Commands executed:**
  + **whoami**
  + **cat wp-config.php**
  + **Retrieved DB credentials.**

**9. Privilege Escalation Attempts**

* **Identified SUID binaries and writable directories:**
  + **/usr/bin/sudo**, **/usr/bin/passwd**, **/bin/mount**, **/usr/bin/pkexec**
  + Writable directories: **/tmp**, **/run/lock**, **/var/tmp**, **/var/lib/php/sessions**
* **Attempts to escalate privileges were unsuccessful due to password protection on sudo.**

**Recommendations**

**WordPress Hardening Best Practices**

1. **Perform Regular Updates**
   * Keep WordPress core, plugins, and themes up-to-date to mitigate vulnerabilities.
2. **Plugin and Theme Management**
   * Only install trusted plugins and themes. Regularly audit and remove unused ones.
3. **Enhance WordPress Security**
   * Utilize security plugins such as Sucuri Security, iThemes Security, and Wordfence Security.
4. **User Management**
   * Disable the default admin user and enforce strong password policies.
   * Implement two-factor authentication (2FA) for all users.
5. **Configuration Management**
   * Limit login attempts and consider renaming the login page.
   * Install plugins to disallow user enumeration.
6. **Backup and Recovery**
   * Regularly back up the WordPress site and database to ensure recovery in case of an incident.

**Conclusion**

The penetration test revealed several vulnerabilities in the WordPress installation, including user enumeration, password weaknesses, and exploitable plugins. Immediate action is recommended to address these vulnerabilities and enhance the overall security posture of the site.

**Prepared by:**  
[Your Name]  
[Your Contact Information]  
[Your Company Name]

# WordPress Hardening

## Best Practices

Below are some best practices for preventing attacks against a WordPress site.

## Perform Regular Updates

This is a key principle for any application or system and can greatly reduce the risk of a successful attack. Make sure that WordPress core, as well as all installed plugins and themes, are kept up-to-date. Researchers continuously find flaws in third-party WordPress plugins. Some hosting providers will even perform continuous automatic updates of WordPress core. The WordPress admin console will usually prompt us when plugins or themes need to be updated or when WordPress itself requires an upgrade. We can even modify the wp-config.php file to enable automatic updates by inserting the following lines:

Code: php

define( 'WP\_AUTO\_UPDATE\_CORE', true );

Code: php

add\_filter( 'auto\_update\_plugin', '\_\_return\_true' );

Code: php

add\_filter( 'auto\_update\_theme', '\_\_return\_true' );

## Plugin and Theme Management

Only install trusted themes and plugins from the WordPress.org website. Before installing a plugin or theme, check its reviews, popularity, number of installs, and last update date. If either has not been updated in years, it could be a sign that it is no longer maintained and may suffer from unpatched vulnerabilities. Routinely audit your WordPress site and remove any unused themes and plugins. This will help to ensure that no outdated plugins are left forgotten and potentially vulnerable.

## Enhance WordPress Security

Several WordPress security plugins can be used to enhance the website's security. These plugins can be used as a Web Application Firewall (WAF), a malware scanner, monitoring, activity auditing, brute force attack prevention, and strong password enforcement for users. Here are a few examples of popular WordPress security plugins.

#### [Sucuri Security](https://wordpress.org/plugins/sucuri-scanner/)

* This plugin is a security suite consisting of the following features:
  + Security Activity Auditing
  + File Integrity Monitoring
  + Remote Malware Scanning
  + Blacklist Monitoring.

#### [iThemes Security](https://wordpress.org/plugins/better-wp-security/)

* iThemes Security provides 30+ ways to secure and protect a WordPress site such as:
  + Two-Factor Authentication (2FA)
  + WordPress Salts & Security Keys
  + Google reCAPTCHA
  + User Action Logging

#### [Wordfence Security](https://wordpress.org/plugins/wordfence/)

* Wordfence Security consists of an endpoint firewall and malware scanner.
  + The WAF identifies and blocks malicious traffic.
  + The premium version provides real-time firewall rule and malware signature updates
  + Premium also enables real-time IP blacklisting to block all requests from known most malicious IPs.

## User Management

Users are often targeted as they are generally seen as the weakest link in an organization. The following user-related best practices will help improve the overall security of a WordPress site.

* Disable the standard admin user and create accounts with difficult to guess usernames
* Enforce strong passwords
* Enable and enforce two-factor authentication (2FA) for all users
* Restrict users' access based on the concept of least privilege
* Periodically audit user rights and access. Remove any unused accounts or revoke access that is no longer needed

## Configuration Management

Certain configuration changes can increase the overall security posture of a WordPress installation.

* Install a plugin that disallows user enumeration so an attacker cannot gather valid usernames to be used in a password spraying attack
* Limit login attempts to prevent password brute-forcing attacks
* Rename the wp-admin.php login page or relocate it to make it either not accessible to the internet or only accessible by certain IP addresses