INFORMATION SECURITY GUIDELINE

Securing WordPress

Introduction

1. WordPress is a popular content management system and is frequently targeted for attacks; this hardening guide is meant to further enhance the level of security for WordPress by reducing the exposed attack surface and by providing configuration guidance.
2. This guideline has been issued by the Chief Information Officer to supplement the Vulnerability Management standard. Compliance with this guideline is recommended, but not mandatory. Questions about this guideline may be referred to information.security@ubc.ca.

Best Practices for Protecting the Application Platform

3. Once installed, ensure that all patches and security fixes for plugins are applied and auto updates are enabled.
4. If using blogging on the site, consider enabling Akismet to aid in preventing comment SPAM.
5. Brute Force Login Attacks predominantly have three types of requests:
    - /wp-signup.php
    - /wp-login.php
    - /wp-login.php?action=register

    To block Brute Force Login and comment requests from a remote HTTP_REFERER, add the following .htaccess rule (replacing the HTTP_REFERER with your site domains), which performs a redirect to a nonexistent site.

    ```
    <IfModule mod_rewrite.c>
         RewriteEngine On
         RewriteCond %{REQUEST_METHOD} POST
         RewriteCond %{REQUEST_URI} .(wp-comments-post|wp-login)\.php*
         RewriteCond %{HTTP_REFERER} !.*(yourdomain.ubc.ca|yourdomain2.ubc.ca).* [OR]
         RewriteCond %{HTTP_USER_AGENT} ^$
         RewriteRule (.*) http://0.0.0.0/$ [R=301,L] </ifModule>
    ```

6. If you are not using WordPress XML-RPC features, which is highly likely, consider blocking it with the following .htaccess rule:

    ```
    # disbale access to xmlrpc
    <Files "xmlrpc.php">
    Order Allow,Deny
    deny from all
    </Files>
    ```

7. Resulting from a recent article on CryptoPHP, be mindful of utilizing free third party plugins.
8. To enhance the overall security it is also important to harden the operating system that will be hosting the WordPress installation.

Recommended Sites

9. The following sites provide additional information on securing WordPress

Topic Area	Site
Hardening WordPress	http://codex.wordpress.org/Hardening_WordPress
Combating Spam	http://codex.wordpress.org/Combating_Comment_Spam
Brute Force Attacks	http://codex.wordpress.org/Brute_Force_Attacks http://blog.sucuri.net/2014/07/new-brute-force-attacks-exploiting-xmlrpc-in-wordpress.html
Hardening the Operating System	https://benchmarks.cisecurity.org/downloads/multiform/index.cfm
Article on CryptoPHP	https://foxitsecurity.files.wordpress.com/2014/11/cryptophp-whitepaper-foxsrt-v4.pdf

Related Documents

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems
Vulnerability Management standard
UBC Systems and Application Hardening Guides guideline