

# Implementing Robust Security Measures for WordPress Website

**Julian Song** \ [ulument.com](https://www.juliansong.com)

## Julian Song \ ulement.com

Years of experience with WordPress, jury for the Malaysia Website Awards. Recognizes me as a Performance Expert by Elementor — only a few worldwide and the only one in Malaysia. I also partners with several hosting providers to deliver WordPress solutions to their enterprise clients.

My clients from SMEs, GLCs, MNCs, universities, news portals, etc

Additionally, I also organiser WCKL 2019, WC Asia 23 & 24; lead organiser WCMY 23 and team lead WC Asia 25.



# WordPress Security

Here are some tips and tricks I've gathered from working with enterprise clients over the years. In this talk, I will cover five sections, with the final section being the most important according to my experience.

- 1 // Secure Hosting Environment**
- 2 // User Management**
- 3 // Plugin and Theme Management**
- 4 // Improve WordPress Security**
- 5 // Education**

# 1 // Secure Hosting Environment

## 1. **Web Penetration Testing**

Conduct web penetration testing before launch and annually thereafter. This proactive approach helps identify and address potential vulnerabilities.

## 2. **Secure Hosting Environment**

Opt for VPS / Dedicated or managed WordPress hosting offers better isolation and security features.

## 3. **SSL Certificate**

Implement SSL to encrypt data transmission. This protects sensitive information from interception.

# 1 // Secure Hosting Environment

## 4. **Firewall Implementation**

Deploy services like CloudFlare, Imunify360 or Bitninja. To add an extra layer of protection. These firewalls can block malicious traffic before it reaches your server, mitigating DDoS attacks and other cyber threats.

## 5. **Content Security Policy Header (CSP Header)**

Prevent cross-site scripting (XSS) attacks by defining the sources from where are allowed to load resources like scripts, images, and stylesheets.

# 1 // Secure Hosting Environment

## 6. **HTTP Strict Transport Security Header (HSTS)**

This prevents man-in-the-middle attacks and ensures secure connections for all users.

## 7. **Secure File Transfer**

Use SFTP (Secure File Transfer Protocol) or SSH (Secure Shell) for file transfers to ensure encrypted communication between your local machine and the server.

# 1 // Secure Hosting Environment

## 8. **Close Unused Ports**

Review and close unused ports on your server to minimize potential attack vectors.

## 9. **Server Logging**

Maintain detailed server logs. This aids in tracking and analysing suspicious activities.

## 10. **Backup Strategy**

Never rely solely on third-party. Store backups securely off-site for disaster recovery. Make sure able to restore.

## 2 // User Management

### 1. **Implement Strong Password Policies**

Enforce the use of complex passwords combining uppercase and lowercase letters, numbers, and special characters. Implement a password expiry policy, requiring users to update their passwords every 90 days. Disallow the reuse of old passwords to maintain security integrity.

### 2. **Two-Factor Authentication (2FA)**

Enable 2FA for all user accounts, especially administrative ones.



## 2 // User Management

### 3. **Login Whitelisting**

Restrict login attempts to specific IP addresses where possible. This significantly reduces the attack surface for brute force attempts.

### 4. **Account Management**

Limit the number of administrative accounts and regularly audit user roles to ensure appropriate access levels.

## 2 // User Management

### 5. **Implement Stronger Password Hashing**

Utilise bcrypt hashing for storing passwords. This method is more secure than current MD5 algorithms and provides better protection.

### 6. **User Activity Logging**

Maintain detailed logs of user activities. This helps in tracking and investigating suspicious actions.

# 3 // Plugin and Theme Management

## 1. **Official Sources Only**

Never use nulled themes or plugins, as well as those from Shopee. Always download themes and plugins from official WordPress repositories or the original developers.

## 2. **Regular Updates**

Keep all themes and plugins up-to-date. Developers regularly release patches for security vulnerabilities.

# 3 // Plugin and Theme Management

## 3. **Minimise Vulnerabilities**

Regular audit your site. Remove unused themes and plugins promptly. Each inactive theme or plugin is a potential entry point for attackers.

## 4. **Daily Vulnerability Scanning**

Detects threats early, ensures prompt updates.

# 4 // Improve WP Security

## 1. **Disable PHP Execution**

Prevent malicious scripts from running by disabling PHP execution in directories where it's not required.

## 2. **Disable File Editing**

Prevents potential attackers from injecting malicious code through the built-in editor.

# 4 // Improve WP Security

## 3. **Disable Directory Browsing**

Enhances security by preventing unauthorized users from viewing file structures and accessing sensitive information on the server.

## 4. **XML-RPC**

Disable if not needed. Mitigates brute force attacks via xmlrpc.php.

## 5. **REST API**

Restrict for non-admins, to limits potential information exposure.

# 4 // Improve WP Security

## 6. **Noindex Search Results**

Prevent SEO Spam

Portal Rasmi Kementerian Kewangan

dominos kelana jaya 🍀 [【2yuo.com】](#) 🍀 Menang lebih banyak dengan setiap taruhan di platform kami!

dominos kelana jaya [【2yuo.com】](#) Menang lebih banyak dengan setiap taruhan di platform kami!

2 weeks ago



belanjawan.mof.gov.my

kamboja result 🍀 [【2yuo.com】](#) 🍀 Bertaruh pada 9 lotto dan dapatkan bonus eksklusif untuk pelanggan setia!

kamboja result [【2yuo.com】](#) Bertaruh pada 9 lotto dan dapatkan bonus eksklusif untuk pelanggan setia!

2 weeks ago



Portal Rasmi Kementerian Kewangan

unreal

unreal 2yuo.com Bertaruhlah untuk kemenangan, hiduplah untuk keseronokan!

2 weeks ago



belanjawan.mof.gov.my

lotto 4.4.2020

lotto 4.4.2020 [【2yuo.com】](#) Bertaruh untuk keseronokan, menang untuk kepuasan yang tiada tara!

2 weeks ago



belanjawan.mof.gov.my

super lotto lucky numbers

super lotto lucky numbers [【2yuo.com】](#) Bertaruhlah dengan kami dan manfaatkan promosi eksklusif serta bonus yang besar dalam lingkungan...

2 weeks ago



**Blackhat SEO. Can be easily solved by noindex search results, add Content Security Policy header, disable PHP Execution.**



# 5 // Education

## 1. **Security Training Sessions**

Conduct security awareness training. This helps client stay updated on best practices.

## 2. **Incident Response Planning**

Develop and regularly update incident response plans. This ensures quick and effective action during breaches.

# Note

Based on years of experience, the security problems is mostly caused by human error.


- Expect hosting providers to handle all aspects of website management.
- Client's in-house / agency use easy password.
- Client's in-house / agency use nulled plugins/theme.
- Client's in-house / agency use unlicensed plugins/theme.
- Client didn't know they are using WordPress.
- Multiple websites inside a single account.
- Poorly managed Web Server.

# Slider Revolution










Deactivate | [Go Premium](#)

Slider Revolution - More than just a WordPress Slider

Version 6.6.13 | By [ThemePunch](#) | [Visit plugin site](#)

 There is a new version ([6.7.20](#)) of Slider Revolution available. To update directly [register your license key now](#) or [purchase a new license key](#) to access [all premium features](#).

Irresponsible agency  
use unlicensed plugin  
for client's website.

Plugin	Slider Revolution	<= 6.718	Authenticated (Author+) Stored Cross-Site Scripting via SVG File Upload vulnerability		5.9	1 October, 2024
Plugin	Slider Revolution	<= 6.713	Cross Site Scripting (XSS) vulnerability		5.9	28 June, 2024
Plugin	Slider Revolution	< 6.711	Cross Site Scripting (XSS) vulnerability		5.9	28 May, 2024
Plugin	Slider Revolution	< 6.70	Unauthenticated Broken Access Control vulnerability		7.1	28 May, 2024
Plugin	Slider Revolution	<= 6.77	Authenticated (Author+) Stored Cross-Site Scripting via Htmntag Parameter vulnerability		6.5	1 May, 2024
Plugin	Slider Revolution	<= 6.6.20	Authenticated (Author+) Stored Cross-Site Scripting vulnerability		5.9	9 April, 2024
Plugin	Slider Revolution	<= 6.6.15	Author+ Arbitrary File Upload vulnerability		8.4	14 November, 2023
Plugin	Slider Revolution	<= 6.6.14	Cross Site Scripting (XSS) vulnerability		6.5	14 November, 2023
Plugin	Slider Revolution	<= 6.6.12	Author+ Remote Code Execution Vulnerability		9.1	30 May, 2023

# Thank you.

Page to Download PDF



**Julian Song** \\ [ulement.com](http://ulement.com)