HOSTINGER

Three. Two. Online

WordPress Security Checklist

WordPress Security Checklist

Implementing the right security measures is essential to protect your website from cyberattacks. While these practices don't require extensive technical knowledge, they can significantly improve WordPress security. To help improve your site security, we prepared a checklist with the best WordPress security practices and tips.

Update WordPress Core Software

Every WordPress update brings security improvements such as bug fixes and new features. Running the newest software version reduces the risk of security breaches on your site.

Update Themes and Plugins

Similar to the core software, WordPress themes and plugins also receive updates to patch any vulnerabilities. Update them as soon as a new version is available.

Use Trusted WordPress Themes

Choose themes from the official WordPress repository or reputable developers. Never use a nulled theme as it may have security flaws.

Use Secure WP-admin Login Credentials

A strong password and unique username make it harder to guess your login details and protect you from brute force attacks.

Enable Two-Factor Authentication

Add an extra security layer to the login process. Users will have to input a unique code provided via text message or an authentication app to complete their login.

Back Up WordPress Regularly

A mitigation step that will help recover the website data if any incident, cyber-attack, or data center disruption occurs.

Check for Malware

Schedule regular scans to prevent any damage due to malware and, if detected, remove it as soon as possible.

Remove Unused Plugins and Themes

Prevent backdoor attacks caused by outdated and unused plugins and themes.

Install an SSL Certificate

Establish a secure data transfer protocol to protect information exchanged between your website and its users.

Set Up a Whitelist and Blacklist for The Admin Page

Prevent your login and admin page from being accessed by unauthorized IP addresses.

Limit Login Attempts

Use a security plugin to block logins from an IP address after a specified number of failed attempts.

Change The URL of The WordPress Login Page

A unique URL makes it harder for attackers to get into the page.

Log Idle Users Out Automatically

Often, users forget to log out of their websites, leaving their sessions running. Use a security plugin to prevent an unauthorized person from accessing the admin page when using the same device.

Hide The WordPress Version

Giving away information about your WordPress version helps attackers exploit vulnerabilities, especially if you run an older version.

Monitor User Activity

Detect any unusual activity and changes that may compromise the website. This step is crucial if you have multiple users accessing the WordPress admin.

Disable Error Reporting

The PHP error report displays vulnerabilities and other information about your website's back-end that unauthorized users can exploit.

Migrate to a Secure Web Host

The hosting provider should ensure all website data and files on their server are safe. Pick one with excellent security features such as updates and monitors.

Turn Off File Editing

Unauthorized parties can exploit the built-in file editor in WordPress to access your site. Adding a simple line of code in the **wp-config.php** file will disable the feature:

```
define( 'DISALLOW_FILE_EDIT', true );
```

Restrict Access Using .htaccess

Use the .htaccess file to configure permissions to execute PHP in specific folders and protect the wp-config.php file.

Change The Default WordPress Database Prefix

Prevent SQL injection attacks by replacing the default wp_ database prefix.

Disable XML-RPC

This feature has weaknesses that attackers can exploit in brute force and DDoS attacks.

Block Hotlinking

Other websites that hotlink to your content may take up your server resources and slow down your website.

Manage File Permissions

Use an FTP client or the web hosting file manager to determine which users can read, write, and execute permissions on your core WordPress files and folder.

Bonus Tips

- Create a strong password for WordPress login by using more than 12 characters or generating it using a password generator.
- Avoid generic usernames like **admin** or **administrator**.
- Install a comprehensive security plugin such as Wordfence. It should offer features like two-factor authentication, login attempts limit, and malware scan.
- Use Patchstack to detect vulnerabilities in your themes and plugins.
- Store your website backup data in multiple locations, such as a local computer, USB flash drive, and cloud storage.