Security

Plugins

- To check the security of installed plugins WPVulnDB is useful. You can search the name of the plugin and it will show you any vulnerabilities that have been reported and which version numbers are affected e.g. <=2.0.0 indicates version 2.0.0 and before are affected.
- Wordfence has a scan feature that you can run either spontaneously or on a schedule which will tell you any vulnerabilities in your site.
    - Also make sure to configure Wordfence with brute force protection so it can mitigate attacks on your site.

WPScan

- WPScan is another popular option which is installed on your server rather than through a plugin. The installation instructions are on the GitHub page found through the link.

Passwords

- Always make sure that your passwords are long and secure; tools like LastPass can generate and store secure passwords.
- Additionally it is better to use different passwords for all the things relating to your WordPress installation e.g. server SSH and MySQL.
- Two Factor Authentication can be enabled for your site which greatly increases its security.

General WordPress security

- WordPress has a page of advice on "hardening" your site: Hardening WordPress