LexiConn Knowledgebase

WordPress Plugin - How To Configure Limit Login Attempts

Limit Login Attempts
By default WordPress allows unlimited login attempts either through the login page or by sending special cookies. This allows passwords (or hashes) to be brute-force cracked with relative ease.
Limit Login Attempts blocks an Internet address from making further attempts after a specified limit on retries is reached, making a brute-force attack difficult or impossible.
Plugin homepage: https://wordpress.org/plugins/limit-login-attempts/

1. From the WordPress dashboard, navigate to Plugins > Installed Plugins.
2. Find Limit Login Attempts and click Activate.
3. By default, the following standard settings apply:

    a. Number of retries prior to short-duration lockout: 4
    b. Short-duration lockout: 20 minutes
    c. Number of lockouts prior to long duration lockout: 4
    d. Long-duration lockout: 1 day
4. These default options can be modified from Settings > Limit Login Attempts

https://support.lexiconn.com/kb/questions/395/