WPSCAN PLUGIN SECURITY COMMANDMENTS

1. VALIDATE AND SANITIZE USER INPUT WITH SANITIZE_*() FUNCTIONS.
2. ESCAPE DATA BEFORE BEING OUTPUT WITH ESC_*() FUNCTIONS.
3. ALWAYS USE $WPDB->PREPARE() FOR SQL QUERIES.
4. VALIDATE DATA BEFORE UNSERIALIZING IT.
5. CHECK USER CAPABILITIES WITH CURRENT_USER_CAN().
6. ADD CSRF NONCES TO FORMS AND VALIDATE THEM SERVER-SIDE.
7. USE HTTPS LINKS WHEN HARD CODING URLS.
8. VALIDATE DATA BEFORE PASSING IT TO UPDATE_OPTION() OR DO_ACTION().
9. REGULARLY TEST YOUR PLUGIN FOR SECURITY ISSUES.
10. ENSURE THAT SECURITY RESEARCHERS ARE ABLE TO CONTACT YOU.

WPScan