Risk ID	Technical Risk	Technical Risk Indicators	Related CWE or CVE IDs	Impact Rating	Impact	Mitigation	Validation Steps
1	User authentication to the WordPress blog can be brute-forced.	Number of incorrect logins for accounts seen in logs; performance of login server has been degrading.	CWE-521: https://cwe.mitre.org/data/definitions/521.html	H	Increased load on login server; slower performance; possible denial of service	Lock out user account on 5 incorrect password tries by setting account lockout flag to true.	Account lockout flag set for user account on 5 incorrect password tries.
2	Credentials of database are hardcoded in code	Predefined “username” and “password” variables are used to connect to database File: board.php Lines: 14-15	CWE-798: https://cwe.mitre.org/data/definitions/798.html	H	No matter the user (authorized or not), a connection will be established with the database	Only establish a connection to the database if the user provides authorized credentials	Ask for user credentials and use provided username and password to (try to) connect to the database
3	Query is injectable (SQL Injection)	User input is directly put into query without being sanitized File: board.php Lines: 22 & 56	CWE-89: https://cwe.mitre.org/data/definitions/89.html	H	User can perform SQL injection attack	Sanitize and validate user input before inserting it into query	If input is validated good input, then it is used, otherwise it is not used and input is asked for again
4	Security by obscurity	Sensitive information (a flag) was hidden in an image File: logo.jpg	CWE-656: https://cwe.mitre.org/data/definitions/656.html	H	An attack just has to download the image file and decode it to get the sensitive information hidden in it	Put encrypted information, instead of open information, in an image	Download image, extract encrypted information, and checking it is in fact encrypted