Risk ID	Technical Risk	Technical Risk Indicators	Related CVE, CWE, or OSVDB IDs	Impact Rating	Impact	Mitigation	Validation Steps
Sequential identifier for risk	*Brief Description*	*Evidence of the risk occuring*	*Use comma to separate multiple IDs*	*Use NIST Standard: (H)igh, (M)edium, (L)ow*	*Possible results of the risk, impacting the goals of the product.*	*Action taken to reduce the probability of the risk actually occurring (or how to actually fix the bug). There may be more than one way to mitigate a risk.*	*How do you ensure that risk was mitigated?*
1	User authentication to system can be brute-forced	Number of incorrect logins for accounts seen in logs; performance of login server has been degrading	OSVDB-902, CVE-1999-1074	H	Increased load on login server; slower performance; possible denial of service	Lock out user account on 5 incorrect password tries by setting aaccount lockout flag to true	Account flag set for user account on 5 incorrect password tries.
1	Browser side script can be executed	Untrusted form input is used in output without validation or encoding.	CWE 80	M	DOM can be maliciously manipulated; bad script can be executed to perform unwanted actions	Sanitize all output from user-supplied input; Validate input via white lists	Output not generated if data contains HTML tags or doesn't fit required format
2	Unwanted SQL query can be made	Data input is used to dynamically construct a SQL query	CWE 89	H	Data can be accessed, modified, or deleted; Attackers can gain administrative privilege	Validate input via white lists; Normalize user-supplied data	Query invalid if input doesn't fit requirement or reduce encoding schemes to their interal character representation
3	Authentication system can be bypassed every time	Authentication form can be bypassed by always returning true (e.g., appending 'and 1=1' to password field)	CWE 89	H	Authentication system can be breached	Validate input via password formatting (typically doesn't contain spaces as SQL queries do)	Authentication not given with ill formatted password
4	Exposing credentials creates broad vulnerabilities	Hardcoded usernames, passwords, and other sensitive data	CWE 259	M	Credentials are easily discoverable and can be compromised	Encrypt passwords and store in locations that are not easily accessible	Password is not discoverable and decrypting is near impossible
5	Transfered files viewable and vulnerable to exposure	Unencrypted protocols viewable via network protocol analyzer (e.g., Wireshark)	CWE 319	H	Files are exposed to attacker and available for dowload	Encrypt protocols so files and sensitive information is not viewable on the server	Attempt to view FTP traffic on the network
6	Inherent vulnerabilities in platform	Various vulnerabilities (xss, sql injection, code injection, credential management) found in old version of WordPress		M	Web application can be more vulnerable because of existing security flaws	Ensure platforms used have high security standards; Use trusted platforms	Run static scan on app created
7	Cookies can be changed to manipulate web app	Sensitive data is stored in cookies which are mutable	CWE 565		Data stored in cookies can be changed to manipulate results and actions of a web application	Store sensitive data in app rather than in cookies to protect it and prevent tampering	Keep sensitive data out of cookies
8	Unwarranted directory traversal can be accessed	Client side action can access restricted directory levels	CWE 73	M	Files and higher profile information can be exploited and compromised	Validate user input via white lists and required formatting; Use sanitizing routine (black lists) for input	Rule input invalid if it doesn't follow requirements or meet white list