CMS - Bug #18636

Security audit - reported issues

2026-09-03 12:19 PM - Ancy A

Status:	New	**Start date:**	2026-09-03
Priority:	Normal	**Due date:**	2026-09-04
Assignee:	Divya S	**Estimated time:**	0.00 hour
Category:		**Spent time:**	0.00 hour
Target version:			
Affected Version:	1.0	**Reproducible:**	

Description

Security audit issues:

1)No Rate Limiting on Login Attempt
We have noted that IP-based rate limiting will be implemented for the Administrator login interface in the production environment. Kindly confirm the planned timeline/date for implementing the rate-limiting and temporary blocking mechanism. Once implemented, we will retest the Administrator login interface to verify the effectiveness of the control.

2)Use of Vulnerable and Unsupported Web Server Version
We have noted that nginx 1.30.4 (Stable) will be used in the production environment. Kindly provide a relevant screenshot or supporting evidence confirming that the production environment is utilizing the stated nginx version.

3)Dependency on Vulnerable and Unsupported Third-Party Components
We have noted your clarification that the reported vulnerabilities are associated with other applications hosted on the same server. We will consider this clarification during the assessment.

4)Improper Input Validation
Restricting access to the Administrator login interface through the internal network/VPN reduces external exposure but does not address the underlying input validation issue. We recommend implementing proper server-side input validation and sanitization for all user-supplied input. An allowlist-based approach should be implemented to permit only the required characters and input formats, while unwanted or unnecessary special characters should be blocked. Appropriate context-aware output encoding should also be implemented before rendering user-supplied data.