

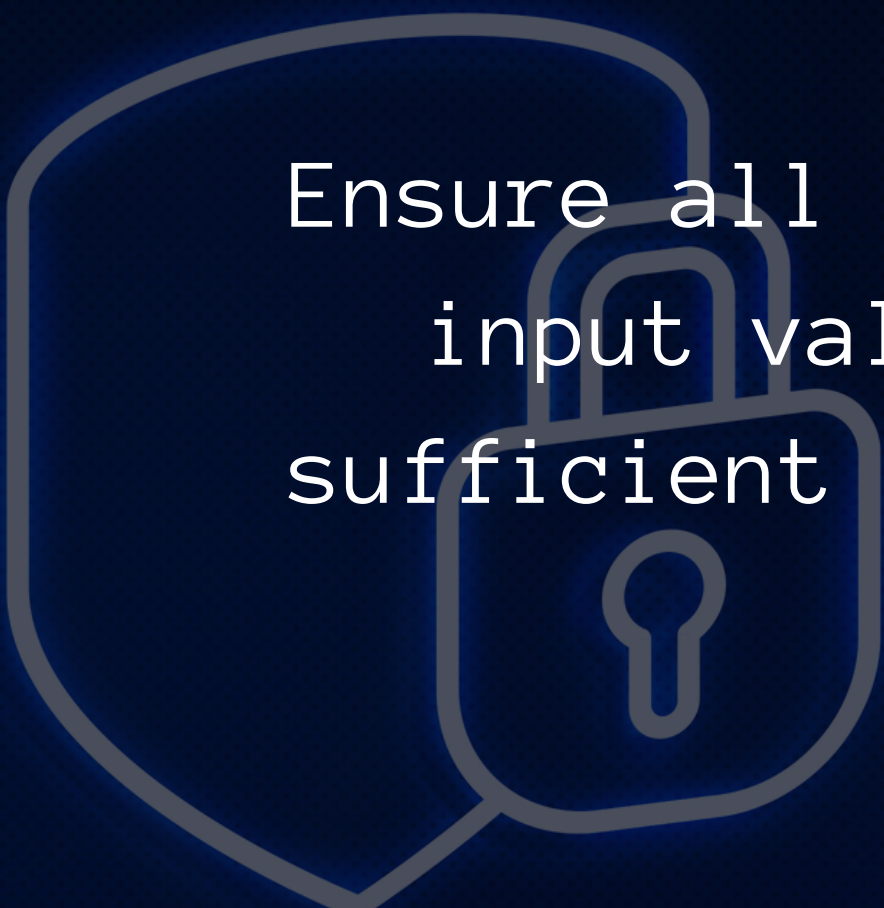
A 09:2021 - Security Logging & Monitoring Failures



Prevention



SLMF Prevention



Ensure all login, access control, and server-side input validation failures can be logged with sufficient user context to identify suspicious or malicious accounts



SLMF Prevention

All old logs should be kept for an extended period
for delayed forensic analysis and investigations



SLMF Prevention

All high-value transactions must have an audit trail with integrity controls to prevent tampering or deletion



SLMF Prevention

Effective incident response, response escalation and recovery plans must be established

