



# Mojaloop Platform Quality & Security

PI-23 Mid-PI review



# Workstream Update



Workstream Name:	Mojaloop Platform quality and security
Roadmap Pillar:	Quality Product (Foundation)
Lead:	Sam Kummary
Workstream Objectives:	<ol style="list-style-type: none"><li>1. Hardening of Mojaloop releases</li><li>2. Security testing of Mojaloop</li><li>3. Documenting Mojaloop standards</li><li>4. Identify maintenance tasks and issues to be addressed to harden current Mojaloop releases</li></ol>
Progress Against Objectives:	<ol style="list-style-type: none"><li>1. Security testing of Mojaloop's finance portal completed</li><li>2. Documentation of standards<ul style="list-style-type: none"><li>○ CQS guidance on release quality</li><li>○ Mojaloop CVD standards - <a href="#">PR</a></li></ul></li><li>3. GitHub maintenance related tasks in progress</li></ol>
Anticipated Progress by PI End:	
Roadblocks:	
Support Needed:	<ol style="list-style-type: none"><li>1. Help with execution of adopted standards</li></ol>



# Observations on Finance Portal security



Best practices being followed on:

1. AuthN and AuthZ
2. Input validation/sanitization testing
3. Security Headers & Best practices assessment.
4. Session management

Recommendations to:

1. Keep services up-to-date in relation to underlying dependencies
2. Ensure proper configuration of features for production (for example disable features for testing, exploration, in Production)

Thanks to Upanzi Network / Cylab-Africa team for performing the security assessment on a Mojaloop sandbox (v15.1.0)



# Mojaloop PQS: PI-23 updates



1. Guidance around moving from alpha / beta to release quality:  
[https://community.mojaloop.io/mojaloop\\_foundation/pi-22-core-releases-work-stream-reviews-4ami](https://community.mojaloop.io/mojaloop_foundation/pi-22-core-releases-work-stream-reviews-4ami)
2. Mojaloop's coordinated vulnerability disclosure policy in-progress. PR:  
<https://github.com/mojaloop/documentation/pull/431/files>
3. Mojaloop cyber-security architecture PR out for review:  
<https://github.com/mojaloop/documentation/pull/430>



# Mojaloop PQS: Objectives



1. Hardening of Mojaloop releases
2. Security testing of Mojaloop
  - Assess feedback from the testing internally
  - Prioritize issues based on criticality and severity
  - Update backlog with stories to address issues
3. Review core and related repositories released with Mojaloop for
  - Ensure dependabot alerts are addressed
  - Ensure Snyk issues are addressed
4. Review any tasks “to-do” in the codebase and related quality issues
5. Review PRs in critical repositories and address (close, approve / reject)
6. Update nodejs version for any services not yet upgraded
7. Update maintenance tooling (license-scanner and such)