DSpace 7 Security Analysis

Overview

This page details security-related checks/analysis which is planned to be performed on DSpace 7 prior to the 7.0 final release.

Automated Security Checks

DSpace 7 enables the following types of automated security checks for both the REST API and Angular UI:

- GitHub's Dependabot Alerts: Automatically analyzes all third-party libraries/dependencies & notifies us of any known vulnerabilities
- LGTM.com's automatic security & code analysis: Continuously scans all DSpace code to identify likely vulnerabilities or bugs. Also provides automatic code reviews on new Pull Requests to identify any likely bugs or vulnerabilities that might be introduced by the PR.
- Integration & Unit Testing: We require all new code to come with valid Unit and/or Integration Tests, including tests to prove expected access permissions (in REST API or UI). New Pull Requests must increase code coverage (automatically analyzed via Codecov.io), and code reviewers check (manually) that tests prove expected access permissions. See also Code Testing Guide.

Manual Security Checks

Prior to DSpace 7.0, the following security checks should be performed on DSpace 7:

- **Run a security scan/analysis of the REST API** (e.g. see OWASP list of vulnerability scanning tools or list of free security tools) and report back any discovered potential security issues. *(Required expertise: developer / sysadmin / security expert, ideally one who is not yet a DSpace 7 expert)*
- **Run a security scan/analysis of the Angular UI** (e.g. see OWASP list of vulnerability scanning tools or list of free security tools) and report back any discovered potential security issues. *(Required expertise: developer / sysadmin / security expert, ideally one who is not yet a DSpace 7 expert)*
    - *ZAP Analysis of Angular UI run by DSquare Technologies on May 15, 2021 Summary:*
        - High Risk Alerts: 0
        - Medium Risk Alerts: 4 (Tim reviewed and these were all false positives & do not have to do with our codebase itself)
        - Low Risk Alerts: 7 (A few minor suggestions here, but 4 other false positives)
- **Re-analyze all existing Integration Tests** to ensure all restricted REST API endpoints include tests which check/verify access permissions on the endpoint. This analysis may concentrate on endpoints added since March 2020 (see note below). *(Required expertise: DSpace 7 core developer)*
    - An initial analysis of REST API endpoints was completed by Andrea Bollini (4Science) , Mykhaylo Boychuk in March 2020 as part of 7.0 Beta 2. See DS-4411 and the accompanying detailed analysis document.
- **Analyze/update REST Contract documentation** to ensure all endpoints document expected permissions to access that endpoint. This will simply help ensure our documentation is accurately describing our security checks. *(Require expertise: DSpace 7 core developer)*