OSCRAT

Open-Source Cyber Resilience Act Tools

D3.5.

OSCRAT – Testing Report M12

Submission date: 30/11/2025

Author: Liliana Hornea – Oves Enterprise

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.
The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Project acronym	OSCRAT
Project title	Open-Source Cyber Resilience Act Tools
Name	D3.5. – Testing Report M12
Number	101190180
Work package	Work Package 3 – Software design and development
Due Date	30/11/2025
Submission Date	12/11/2025
Lead Partner	OVES Enterprise
Author name(s)	Liliana Hornea
Version	1.0
Status	Draft
Type:	Document, report
Dissemination level:	Public

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Document History			
Version	**Date**	**Modified by**	**Comments**
0	14/11/2025	Liliana Hornea	First draft
1.0	18/11/2025	Francesco Antonio Alescio	Changes in layout to adapt the format + tables formatting

Abstract

This report summarizes end-to-end testing of the Product Management and Compliance Assessment Platform. The testing validated functional workflows, data consistency, UI behaviour, and file handling across modules including Product Management, Compliance Assessment, Dashboards, SBOM/Scan, Vulnerabilities, and Incidents. Manual, exploratory, black box, and regression testing confirmed correct system behaviour, business rule enforcement, and reliable report generation.

Keywords

Product Management, Compliance Assessment, Functional Testing, Vulnerability Management, Incident Tracking, Dashboard, SBOM, Data Integrity, Regression Testing

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

DISCLAIMER

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Table of contents

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Figures

List of Tables

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

1. Executive Summary

1.1 Summary

Between August and November 2025, the OSCRAT platform expanded from its product management foundation to include security compliance and risk management capabilities. Development efforts focused on four core areas: Security & Compliance Operations, Organizational Assessment Framework, Repository & SBOM Management, and Platform Experience & Reliability. These improvements prepare OSCRAT to support organizations working with regulatory requirements including the EU Cyber Resilience Act.

1.2. Security & Compliance Operations

The platform now includes security management capabilities that help organizations identify, track, and remediate vulnerabilities across their software portfolios. The vulnerability management system integrates the Grype scanner to provide automated vulnerability detection that connects with SBOM generation workflows. When organizations generate or import SBOMs, the system automatically initiates vulnerability scanning, creating detailed reports that classify threats by severity using CVSS scoring metrics. The system maintains complete linkage between discovered vulnerabilities and their source components, enabling precise impact analysis and targeted remediation efforts.

Beyond vulnerability detection, the platform introduced a complete incident management system that serves as a centralized repository for security incident documentation and response coordination. Teams can create incidents linked to specific product versions, documenting timelines, impacts, and remediation actions while attaching relevant forensic evidence and supporting documentation. This integration with the broader product management framework ensures that incident data remains contextual and actionable, appearing directly within product and version overview pages for immediate visibility.

Cyber Resilience Act (CRA) compliance assessment capabilities were implemented with purpose-built forms that capture all required compliance data points. These assessments integrate with the broader assessment framework to generate audit-ready documentation. The system maintains full assessment history with versioning for tracking changes over time.

1.3. Organizational Assessment Framework

The period saw the implementation of a multi-tiered assessment of architecture with three levels: organization-wide baselines, team-specific assessments, and version-level assessments. This system uses an inheritance model where

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

organizational requirements cascade down while allowing overrides for specific contexts. The platform now includes versioning and history tracking for all assessments, supporting audit requirements and regulatory compliance.

The organizational data model was enhanced to capture size classifications, product support dates, and acronyms for improved reporting. Organizations can establish reporting relationships between teams, supporting complex hierarchies. Assessment reset and update capabilities allow organizations to adapt to changing compliance requirements while maintaining historical records for audit purposes.

1.4. Repository & SBOM Management

SBOM generation and management capabilities now support both automated generation from repositories and manual file import. The system uses worker architecture for background processing of repository analysis and SBOM creation. Both private and public repositories are supported, with configuration options for specific branches, tags, or committees.
Lockfile generation captures exact dependency versions, enabling precise vulnerability impact assessment.
The file attachment system was redesigned to provide unified document management across all platform features. Teams can attach documentation to products, remediation plans to vulnerabilities, and evidence to incidents. The system includes validation for file types and sizes, with special handling for SBOM files to maintain scanning pipeline integrity.

1.5. Platform Experience & Reliability

User experience improvements include breadcrumb navigation for orientation, side panels for contextual information, and semantic status badges for visual state indication. Page layouts and tab navigation were harmonized across product and version views, with empty states now providing actionable guidance. From validation and error handling improvements span sign-up flows, repository configuration, and assessment forms, with real-time feedback and clear error messages.

Authentication and team management refinements streamline onboarding and collaboration. The sign-up process captures organizational details for compliance workflows, while email notifications support team invitations. Infrastructure improvements include deployment configuration with health monitoring, building pipeline optimizations, enhanced database migrations, and comprehensive error codes for debugging. Translation system enhancements enable internationalization support.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

1.6. Technical Approach

Development focused on architectural quality through conversion to a monorepo architecture with separate worker services, enabling clear separation of concerns and code reuse. Asynchronous job processing keeps the platform responsive under load, while error handling and retry mechanisms provide resilience. Database schema improvements enhanced data normalization and query performance with backward compatibility maintained through careful migration management. Type safety improvements and validation at system boundaries reduce runtime errors and prevent data corruption. The architecture supports horizontal scaling for enterprise deployments while remaining manageable for smaller organizations.

1.7. Conclusion

In summary, the last three months of development brought major advances to the OSCRAT platform, particularly in security, system architecture, and assessment scalability. The introduction of the Vulnerability Management System, the re-engineered Assessment Framework, and the CRA, Team, and Version assessment implementations represent significant milestones, laying a strong foundation for future growth.
Combined with improvements in file handling, job reliability, organizational data structure, and interface consistency, these contributions mark a period of meaningful and high-impact progress for OSCRAT.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

2. Introduction

This testing effort covers the complete end-to-end functionality of the **Product Management and Compliance Assessment Platform**, ensuring that all core modules operate as expected and that data consistency, integrity, and user actions perform correctly across the system.
The tests validate the functional flow from product creation and assessment setup through vulnerability and incident tracking, reporting dashboards, and scan integrations.
The objective of testing was to verify:

- Correct rendering of all UI components and navigation
- Validation and enforcement of required business rules
- Data consistency between lists, detail pages, and cross-linked entities
- Correct behavior of all user actions (create, edit, delete, close, download, upload)
- Status transitions and visual indicators (progress bars, charts, completeness metrics)
- File handling integrity across attachments and report exports.

3. Functional Areas Covered

3.1. Product Creation and Management

The platform allows users to create new products in three ways:

- Add Product from Scratch – user completes applicability check, fills product details, and saves.
- Add Product from Cache – uses previously stored applicability data for faster entry.
- Add Product by Loading Existing Product – prepopulates data from an existing record for reuse.

Testing validated mandatory field handling, form warnings based on organizational role, retake survey behavior, and button visibility after applicability checks.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

3.2. Team Compliance Assessment

Each area contains multiple requirements, each with mandatory questions (free text or Yes/No answers) and an evidence upload option.
The system provides Next and Back navigation, reset functionality to clear all answers, and a progress bar displaying completion percentage per requirement.

Tests verified:

- Navigation through questions
- Validation of mandatory answers
- Evidence uploads controls
- Status selection after completion
- Reset and progress bar accuracy

3.3. Dashboard

The Dashboard visually summarizes assessment progress:

- Progress Bar – overall percentage of completed requirements
- Pie chart Evaluation Status - evaluation status (finished vs. unfinished requirements)
- Pie Chart Conformity Status Breakdown – conformity status distribution by requirement status
- It also includes an Export to PDF function that generates a detailed report with progress, status summary, and requirement list.
- Testing validated correct data reflection, dynamic chart updates, and PDF export accuracy.

It also includes an Export to PDF function that generates a detailed report with progress, status summary, and requirement list.

Testing validated correct data reflection, dynamic chart updates, and PDF export accuracy.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

3.4. SBOM and Scan Management

The Scan tab (triggered from the SBOM tab) displays all performed scans with details:

Status, Source, Started, Triggered By, Duration, Total, Critical, High, Medium, Low, Actions (Download/Delete), and includes a Refresh button.

Testing confirmed:

- Accurate rendering of scan results and counts
- Correct operation of Download, Delete, and Refresh actions
- Proper error handling for missing or failed downloads

3.5. Vulnerability Report and Management

After selecting a scan, the Vulnerability Report lists all detected vulnerabilities with columns: CVE, Severity, Package, Version, Fixed In, Description, Actions (Create).

The Create button opens the Add Vulnerability form, where most fields are prefilled from scan data (Name, Status, Severity, Date of Discovery, Summary, CVE).

The form supports file attachments and has Cancel and Add buttons.

Tests covered:

- Correct prefilled data from scans
- Validation and field behavior
- Attachment upload/download/delete
- Record persistence and reflection in report view

3.6. Vulnerabilities Tab

The Vulnerabilities tab lists all added vulnerabilities in a table: Name, Status, Severity, Date of Discovery, Description.

Users can Add Vulnerability (same form as above but empty) or open existing ones for details.

The Vulnerability Details page includes:

- **Context Information** – main metadata and **Edit/Close** buttons
- **Extended Data** – system-generated fields (CVE, Created/Updated info)
- **Attachments** – file management (one per upload, with Download/Delete)

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

3.7. Incidents Tab

The Incidents module tracks security incidents with columns: Status, Classification, Attack Type, Severity, Date Detected, Reporter, Description, Actions (Delete).

The Add Incident form includes:

- **Mandatory fields**: Status, Classification, Attack Type, Reporter (prefilled), Date of Detection, Severity, Description, Scope
- **Optional fields**: Asset Details, Handling Date, Corrective Actions, Root Cause, Preventive Actions
- **Dynamic checkboxes**:
    - *Unlawful/Malicious* and *Cross-border impact*, each showing a required free-text field when checked
- **Attachments section** identical to other modules

Clicking a row opens **Incident Details** with an **Edit** button (to update info) and Close button (to mark as Complete).

Testing verified:

- Form validations and checkbox behavior
- Data persistence and edit correctness
- Status transition (Complete) handling
- Attachment upload/download/delete validation

Consistence between table and detail view.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

4. Testing Methodologies Used

4.1. Manual Functional Testing

- Step-by-step validation of UI workflows, logic conditions, and form behavior
- Performed in modern desktop browsers to simulate end-user interaction
- Focused on validating business rules (e.g., eliminatory answers stop the form)

4.2. Exploratory Testing

- Performed around areas involving conditional branching, dynamic screen changes, and tab-based product sections
- Allowed identification of unexpected behaviors and edge cases not explicitly documented

4.3. Black Box Testing

- Tests were written from the perspective of an end user, without knowledge of the internal code.

Inputs and outputs were validated against expected behavior, especially in areas like form validation, progress tracking, and data filtering

4.4. Regression Testing

- Ensured that enhancements or fixes did not break previously working functionalities like Search and Filter options

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

5. Testing Methodologies Uses

5.1. Add a New Product from Scratch

Description:

When a user selects “*Add a new product from scratch*”, the system first displays an applicability check form, which the user must complete before continuing.

After completing the form:

Product falls within the scope	System response
Yes	The system displays “Add product” and “Try again” buttons
No	The system displays “Go home” and “Try again” buttons.

Table 1: Add New Product

Choosing Add Product opens an empty product creation form where the user must fill in the following fields:

- Product Acronym / Short Name (required)
- Product Full Name (required)
- Product Version (required)
- Product Short Description (optional)

On this form:

- Two read-only fields display results from the first survey.
- A **“Retake Survey”** button allows users to redo the applicability check.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

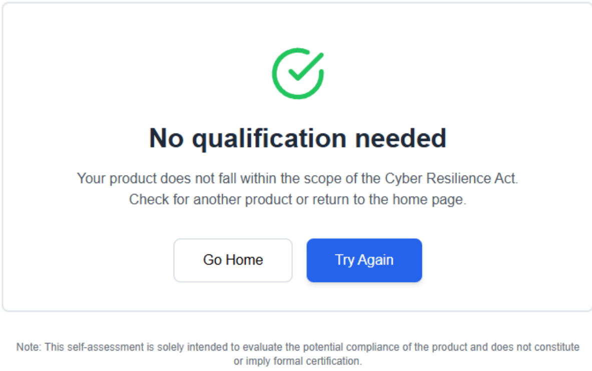


Figure 1: No qualification needed

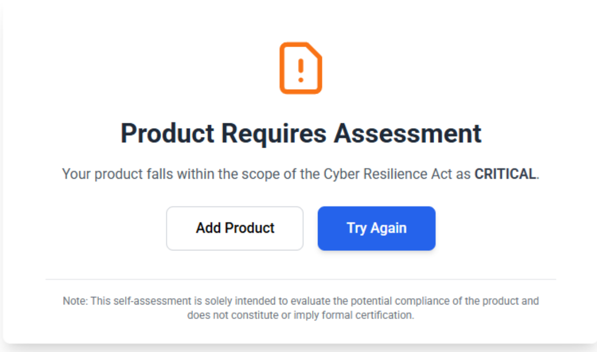


Figure 2: Product Requires Assessment

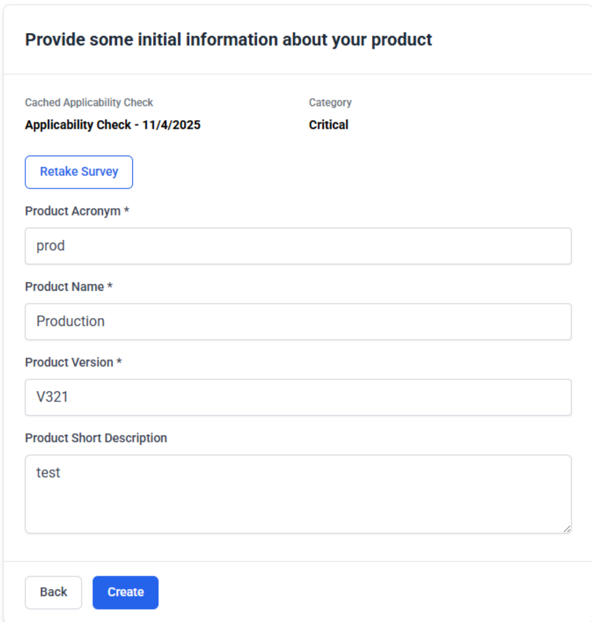


Figure 3: Add Product Menu

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Test cases executed and passed

Test ID	Description	Precondition	Steps	Expected Results
TC-PRD-ADD-01	"Add a new product from scratch" displays applicability check form	User logged in	Click **Add a new product from scratch**	Applicability check form appears as the first step
TC-PRD-ADD-02	Users can proceed only after completing applicability form	Applicability form displayed	Fill required fields → **Continue**	Applicability result screen is displayed
TC-PRD-ADD-03	In-scope result shows correct buttons	Applicability result = in scope	Complete applicability form so it falls within scope	Buttons displayed: **Add Product** and **Try again**
TC-PRD-ADD-04	Out-of-scope result shows correct buttons	Applicability result = out of scope	Complete applicability form so it's outside scope	Buttons displayed: **Go home** and **try again**
TC-PRD-ADD-05	"Add Product" opens the product creation form	Applicability result = in scope	Click **Add Product**	Product form opens with empty fields; required fields marked
TC-PRD-ADD-06	Survey result summary fields are displayed above the product form	Product form opens	—	Two read-only survey result fields visible above form
TC-PRD-ADD-07	Survey result fields show correct values from the first survey	Product form opens	Compare displayed values with first survey answers	Both fields correctly reflect the original survey results
TC-PRD-ADD-08	Survey result fields are read-only	Product form opens	Attempt to edit or focus survey result fields	Fields are non-editable (read-only or disabled)
TC-PRD-ADD-09	"Retake Survey" button is visible and enabled on product form	Product form opens	—	**Retake Survey** button visible and active
TC-PRD-ADD-10	Retake Survey (with unsaved changes) prompts for confirmation	Product form has unsaved data	Modify any field → Click **Retake Survey**	Confirmation dialog warns about unsaved changes (Yes/No)
TC-PRD-ADD-11	Retake Survey (confirm) returns to applicability form	Confirmation shown	Click **Yes/Continue**	Navigated back to applicability form; product form closed
TC-PRD-ADD-12	"Try again" (in-scope path) returns to applicability form	Applicability result = in scope	Click **Try again**	Applicability form reloads for a new input
TC-PRD-ADD-13	"Try again" (out-of-scope path) returns to applicability form	Applicability result = out of scope	Click **Try again**	Applicability form reloads for a new input

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

TC-PRD-ADD-14	"Go home" (out-of-scope path) navigates to home screen	Applicability result = out of scope	Click **Go home**	User navigated to home/main dashboard; flow ends
TC-PRD-ADD-15	Applicability form validation blocks incomplete submission	Applicability form opens	Leave mandatory fields empty → Click **Continue**	Inline validation messages shown; cannot proceed
TC-PRD-ADD-16	Required product fields are clearly marked	Product form opens	—	Acronym, Full Name, Version marked required; Short Description optional
TC-PRD-ADD-17	Save succeeds with only required fields filled	Product form opens	Fill required fields → Click **Save**	Product successfully created and visible in list/details
TC-PRD-ADD-18	Save blocked when required fields missing/whitespace only	Product form opens	Leave a required field blank or whitespace → Click **Save**	Save blocked; inline validation errors shown
TC-PRD-ADD-19	Optional Short Description field behaves as optional	Product form opens	Leave Short Description empty → Click **Save**	Product saved successfully; description stored as empty
TC-PRD-ADD-20	Back does not create product	Product form open with unsaved data	Click **Back**	No product created; no data saved
TC-PRD-ADD-21	Data integrity verified after save	Product saved	Open product details page	All fields display correctly; optional description appears only if provided

Table 2: Add New Product from Scratch – Executed and Passed Test

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

5.2. Add a New Product from Cache

Description:

When a user selects **“Add a new product from cache”**, the system loads data retained from a previously completed **applicability check (cached)** and displays the **product creation form** directly.

All fields are pre-populated using cached values from the last applicability survey, and the user can review or modify them before saving. After reviewing, the user clicks **Save** to finalize the new product creation.

Test cases executed and passed

Test ID	Description	Precondition	Steps	Expected Results
TC-PRD-CACHE-01	“Add a new product from cache” opens pre-populated product form	Cached applicability data exists	Click **Add a new product from cache**	Product creation form opens directly with fields pre-filled
TC-PRD-CACHE-02	Cached data correctly populates product fields	Cached applicability data exists	Open product form	Acronym, Full Name, Version fields show data from previous applicability check
TC-PRD-CACHE-03	Survey result summary fields display cached values above the form	Cached applicability data exists	Open product form	Two read-only survey result fields are visible and correctly reflect cached results
TC-PRD-CACHE-04	Survey result fields are read-only	Product form opens	Try editing or focusing on survey result fields	Fields remain non-editable (read-only/disabled)
TC-PRD-CACHE-05	“Retake Survey” button is visible and enabled	Product form opens	—	“Retake Survey” button visible and active
TC-PRD-CACHE-06	Retake Survey clears cached data and returns to applicability form	Product form opens	Click **Retake Survey**	User navigated to applicability form; cached data cleared or refreshed
TC-PRD-CACHE-07	Users can edit pre-filled product fields before saving	Product form opens	Modify any of the pre-filled fields → Click **Save**	Product saved successfully with updated field values
TC-PRD-CACHE-08	Users can save products without changing cached values	Product form opens	Click **Save** without editing fields	Products created successfully using cached data
TC-PRD-CACHE-09	Required field validation still applies	Product form opens	Clear a required field → Click **Save**	Save blocked; inline validation errors shown

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

TC-PRD-CACHE-10	Optional Short Description field behaves as optional	Product form opens	Leave Short Description empty → Click **Save**	Product saved successfully; description stored as empty
TC-PRD-CACHE-11	Back does not create product	Product form opens	Click **Back**	No product created; no data saved
TC-PRD-CACHE-12	Data integrity verified after save	Product saved	Open product details page	All saved fields match displayed values; optional fields stored correctly

Table 3: Add New Product from Cache – Executed and Passed Test

5.3. Add a New Product by Loading an Existing Product

Description:

When the user selects **“Add a new product by loading an existing product”**, the system prompts them to choose an existing product. After selection, the **product creation form** opens **pre-populated** only with the **applicability check data** from the selected product.

The user reviews the pre-filled applicability information displayed above the form and can then fill in new product details manually before clicking **Save** to create the product.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Test cases executed and passed

Test ID	Description	Precondition	Steps	Expected Results
TC-PRD-LOAD-01	Entry point opens product selector	User logged in; at “Add product” area	Click **from existing product**	A selector dialog appears to choose an existing product
TC-PRD-LOAD-02	Product list loads existing products	Existing products available	Observe selector	List displays existing products with identifiers (name)
TC-PRD-LOAD-03	Handle empty state when no existing products	No products available	Open selector	Empty state message appears with guidance; no selection possible
TC-PRD-LOAD-04	Selecting a product opens pre-populated form	Selector open; products available	Select a product	Product creation form opens with survey result fields populated from the selected product’s applicability check
TC-PRD-LOAD-05	Survey summary fields show correct applicability data	Product form opens	Compare displayed survey values with source product’s applicability check	Category field correctly matches the selected product’s applicability data
TC-PRD-LOAD-06	Survey summary fields are read-only	Product form opens	Attempt to edit survey fields	Fields are non-editable (read-only or disabled)
TC-PRD-LOAD-07	Users can enter new product details	Product form opens	Fill Acronym, Full Name, Version; optionally fill Short Description	All fields accept input as expected
TC-PRD-LOAD-08	Required product fields are enforced	Product form opens	Leave any required field empty → **Save**	Save blocked; inline validation displayed for missing fields
TC-PRD-LOAD-09	Save succeeds when required fields are filled	Product form opens	Fill required fields → **Save**	Product created successfully and appears in product list/details
TC-PRD-LOAD-10	Optional Short Description field behaves as optional	Product form opens	Leave Short Description empty → **Save**	Product saved successfully with empty description
TC-PRD-LOAD-11	Cancel or back does not create product	Product form opens	Click **Back**	No product created; user navigates away safely
TC-PRD-LOAD-12	Data integrity verified after save	Product saved	Open product details page	Saved data matches user input; optional description appears only if provided

Table 4: Add New Product by loading an Existing Product – Executed and Passed Test

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

5.4. Team Compliance Assessment

Description:

Each Area contains one or more Requirements; each Requirement contains one or more mandatory Questions (Free-Text or Yes/No), each with evidence upload. Users navigate with Next/Back. A Requirement can have exactly one Status (chosen only after *all* its questions are answered).

New: The Requirement screen has a Reset button that clears all question answers and evidence for the current Requirement and returns it to an unanswered state. Also, each Requirement header shows an area progress bar: % = (Completed Requirements in Area / Total Requirements in Area) × 100. A Requirement counts as completed when all its questions are answered and a Status is set.

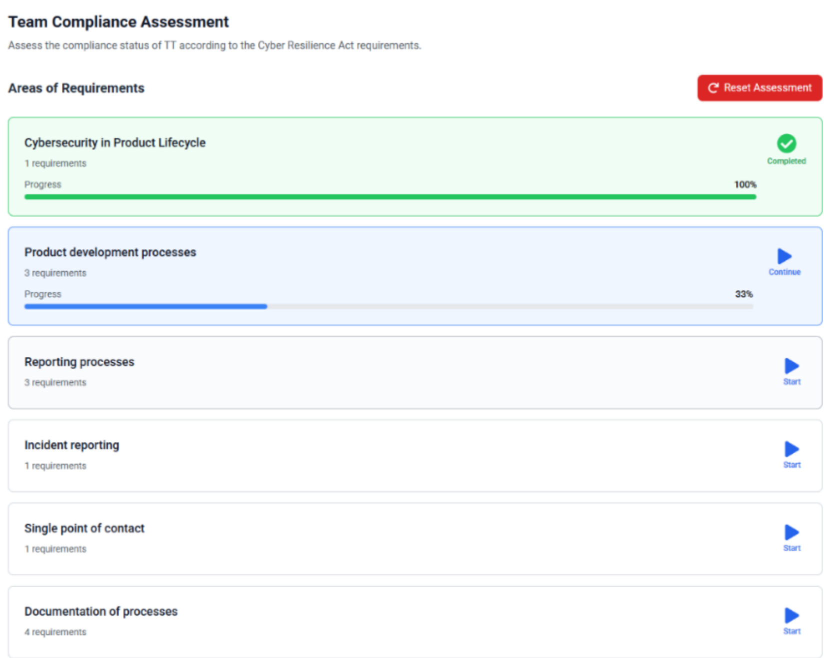


Figure 4: Team Compliance Assessment Page

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Key Features:

- Question types: Free Text (single text area) and Yes/No (radio buttons).
- Evidence: accepts multiple files per question
- Requiredness: every question is mandatory
- Status set is enumerated (e.g., Compliant / Partially Compliant / Not Compliant / Not Applicable).
- Navigation: Next moves to next question; Back moves to previous; prevents leaving unanswered mandatory questions.
- Reset Assessment feature (reset button)
- Progress bar indicating % of finished requirements in an area

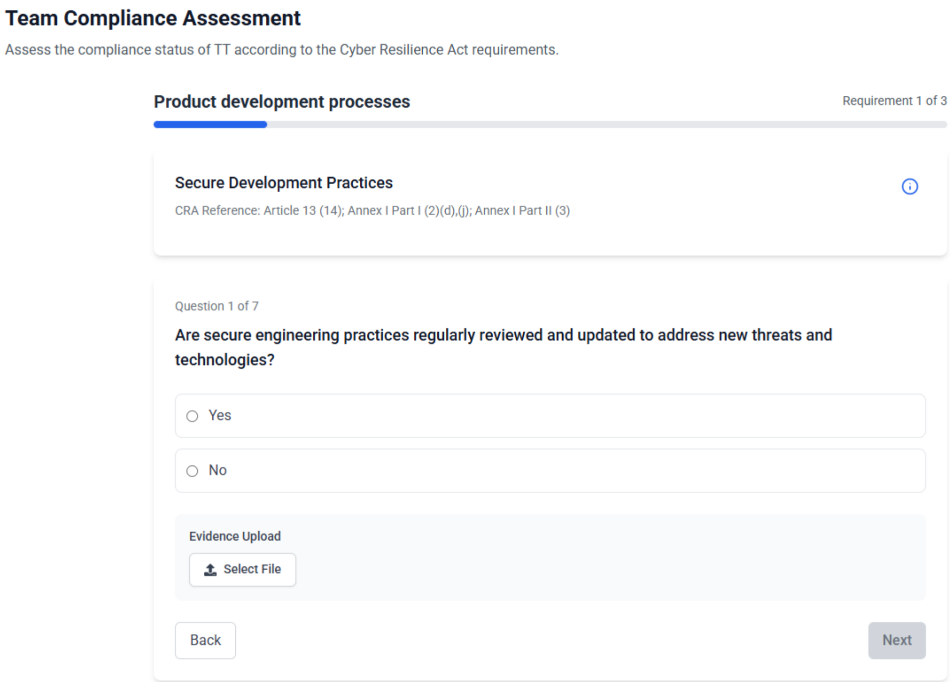


Figure 5: Example of Yes/No question

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Test cases executed and passed

Test ID	Description	Precondition	Steps	Expected Results
TC-REQ-01	Requirement displays its list of questions	Requirement with N questions	Open Requirement	Displays Q1 of N, showing question type and required markers
TC-REQ-03	Question types render correctly	Requirement with both types	View Free-Text and Yes/No questions	Free-Text shows input; Yes/No shows radio group
TC-REQ-04	Initial state has no answers/evidence	New Requirement	Open it	Inputs empty, radios unselected, no evidence
TC-REQ-05	Area progress bar is visible on header	Area with ≥1 Requirement	Open Requirement	Progress bar visible with percentage label
TC-REQ-06	Area progress % calculated and labelled correctly	Area has 4 Requirements, 1 completed	Open any Requirement	Progress shows 25% (1/4); label matches value
TC-REQ-10	“Next” blocked if Free-Text unanswered	On Free-Text question	Leave empty → click **Next**	Inline error shown; cannot advance
TC-REQ-11	“Next” blocked if Yes/No unanswered	On Yes/No question	Leave unselected → click **Next**	Inline error; cannot advance
TC-REQ-12	“Next” allowed when question answered	On any question	Provide valid answer → **Next**	Advances to next question
TC-REQ-13	“Back” retains previous answer	On Q2 with answer	Click **Back**	Q1 still shows previous answer
TC-REQ-15	Cannot bypass unanswered question via direct navigation	TOC present	Click later question while current unanswered	Navigation blocked or prompted
TC-REQ-30	Only one Yes/No option selectable	Yes/No visible	Select Yes, then No	Only latest selection remains
TC-REQ-32	Selection persists across navigation	Question answered	**Next** → **Back**	Same option remains selected
TC-REQ-40	Upload accepts allowed types	Evidence control visible	Upload PDF/JPG/DOCX	Files listed with name/size
TC-REQ-41	Rejects disallowed file types	Evidence control visible	Upload EXE	Error displayed; not listed

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

TC-REQ-42	Enforces file size limit	Limit configured	Upload file > limit	Error shown; file not attached
TC-REQ-43	Allows single file uploads	Control visible	Upload 2–3 files	Only 1 file can be selected for upload
TC-REQ-44	Remove uploaded file	Evidence attached	Click **Remove**	File removed successfully
TC-REQ-45	Evidence persists across navigation	Evidence added	**Next** → **Back**	Evidence remains attached
TC-REQ-46	Evidence is not mandatory	Evidence not required	Attempt to continue without evidence	Next question is displayed
TC-REQ-53	Reset confirmation dialog appears	Answers/evidence/status exist	Click **Reset**	Confirmation dialog warns that all data will be cleared
TC-REQ-54	Cancel Reset keeps data intact	Confirmation shown	Click **Cancel**	Nothing changes
TC-REQ-55	Confirm Reset clears all answers and evidence	Requirement contains data	Confirm **Reset Assessment**	All inputs and evidence cleared
TC-REQ-56	Reset clears Status and disables Status controls	Requirement has Status	Confirm **Reset Assessment**	Status removed; selector disabled
TC-REQ-57	Reset decreases Area progress accordingly	Requirement contributed to progress	Confirm **Reset Assessment**	Progress decreases to reflect change
TC-REQ-61	Status selection enabled after all questions answered	All questions answered	Open Status section	Four options visible and enabled
TC-REQ-62	Only one Status selectable	Status visible	Select one, then another	Only last one remains active
TC-REQ-63	Save stores selected Status	Status chosen	Click **Save**	Requirement saved with chosen Status
TC-REQ-66	Area progress increases when Requirement completed	Area=4, completed=1	Complete and set Status	Progress updates correctly (e.g., 50%)
TC-REQ-67	Progress does not increase until Status set	All Qs answered, no Status	Observe progress	Progress remains unchanged until Status selected

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

TC-REQ-70	Multiple Requirements listed for Area	Area has ≥2 Requirements	Open Area	All Requirements shown with progress indicators
TC-REQ-71	Each Requirement enforces its own Status	Area open	Complete Req A, leave Req B partial	Req A complete; Req B incomplete
TC-REQ-72	Area supports multiple Requirement statuses	Two Requirements complete	Set different statuses	Area summary shows both
TC-REQ-73	Switching between Requirements retains data	Working in Req A	Switch to Req B → return to Req A	Answers/evidence remain saved
TC-REQ-74	Area progress reflects Requirement completion	Area view	Complete Requirements	Progress % updates correctly
TC-REQ-75	Progress updates dynamically when another Requirement completes	Current Requirement open	Complete a different Requirement	Progress bar updates automatically
TC-REQ-76	Progress remains accurate after Reset	Two Requirements complete	Reset one	Progress recalculates correctly
TC-REQ-77	Single Requirement Area displays 0% or 100%	Area has 1 Requirement	Toggle Status	Progress updates from 0% to 100%
TC-REQ-78	Progress rounding and format consistent	Area with 3 Requirements	Complete 1 Requirement	Progress shows 33% (rounded per rule)

Table 5: Team Compliance Assessment – Executed and Passed Test

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

5.5. Team Compliance Assessment Dashboard

Description:

The Dashboard summarizes Requirement completion across a team. It shows:

- ***Progress Bar*** = % of Requirements finished,
- ***Pie Chart Evaluation Status*** = split of Evaluated vs Not Evaluated Requirements
- ***Pie Chart Conformity Status Breakdown*** = count distribution of Requirements by Status (the four statuses).
- ***Export to PDF*** button generates a PDF containing Overall Progress, a Status Summary, and a Requirements list with Name, Evaluation state (Evaluated/Not), and Conformity (the chosen status for finished items).

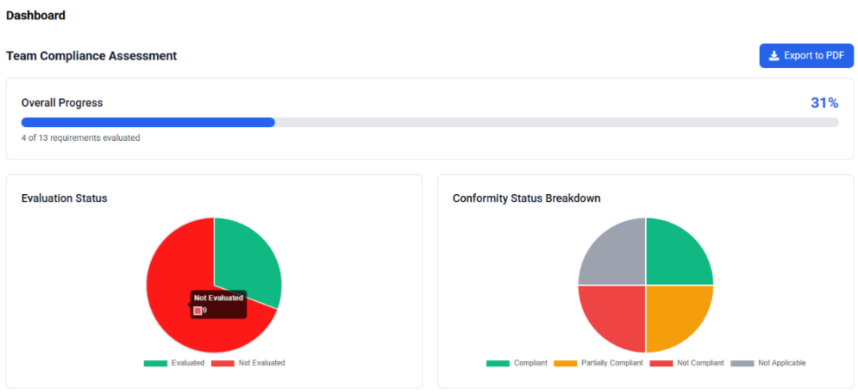


Figure 6: Team Compliance Assessment Dashboard

Test cases executed and passed

Test ID	Description	Precondition	Steps	Expected Results
TC-DASH-01	Dashboard loads with progress bar and both pie charts	Area exists	Open Dashboard	Progress bar, Evaluations Status pie, and Conformity Status pie are visible; no errors
TC-DASH-10	Progress formula correctness	Area with 8 Requirements (3 finished)	Open Dashboard	Progress shows 37–38%; label shows 3/8
TC-DASH-11	0% and 100% edge cases	Areas with all or none finished	Open Dashboard	Displays correct 0% or 100%
TC-DASH-12	Live update of progress	Another tab completes a Requirement	Keep Dashboard open	Progress bar updates automatically or after refresh
TC-DASH-13	Progress rounding consistency	1/3 finished	Open Dashboard	Displays 33% (or 33.3%) consistently

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

TC-DASH-20	**Evaluations Status Pie (A)** – slice counts correct	10 Requirements, 4 evaluated	Open Dashboard	Pie shows **Evaluated=4**, **Not Evaluated=6**
TC-DASH-21	**Evaluations Status Pie (A)** – percentage accuracy	Same as above	Hover or view legend	Displays 40% Evaluated, 60% Not Evaluated; sums ≈100%
TC-DASH-22	**Evaluations Status Pie (A)** – zero state	No evaluated Requirements	Open Dashboard	Evaluated = 0, Not Evaluated = Total; chart renders properly
TC-DASH-23	**Evaluations Status Pie (A)** – full completion	All evaluated	Open Dashboard	Evaluated=Total, Not Evaluated=0
TC-DASH-24	**Evaluations Status Pie (A)** – color/legend stability	Any dataset	Reload page	Colors and labels consistent on reload
TC-DASH-30	**Conformity Status Pie (B)** – slice counts correct	Area with mixed statuses	Open Dashboard	Each slice count matches number of Requirements with that conformity status
TC-DASH-31	**Conformity Status Pie (B)** – percentage accuracy	Same dataset	Hover or view legend	Percentages sum ≈100%; consistent rounding
TC-DASH-32	**Conformity Status Pie (B)** – zero-count status handling	One status unused	Open Dashboard	Status with 0 count hidden or shown as 0 (per design)
TC-DASH-33	**Conformity Status Pie (B)** – color stability per status	Multiple reloads	Reload Dashboard	Each status keeps its assigned color consistently
TC-DASH-40	Cross-check: Progress vs Evaluations Pie	Any data	Compare progress and Evaluations Pie (A)	Progress % = Evaluated / Total; Pie A counts match
TC-DASH-41	Cross-check: Conformity Pie totals vs Evaluations Pie	Any data	Compare Pie B with Pie A	Sum of Pie B slices = Evaluated count in Pie A
TC-DASH-42	Updates after Requirement Reset	A completed Requirement reset	Refresh Dashboard	Evaluated count decreases; both pies and progress update correctly
TC-DASH-43	Updates after status change	Change conformity status of Requirement	Refresh Dashboard	Pie B updates: Evaluations Pie A and Progress unchanged (still evaluated)
TC-DASH-50	Export button visible and enabled	Dashboard open	Observe	**Export to PDF** button visible and enabled

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

TC-DASH-51	PDF generates successfully	Any dataset	Click **Export to PDF**	PDF downloaded; logical filename (compliance-assessment-teamName-date.pdf)
TC-DASH-52	PDF includes Overall Progress	PDF generated	Open PDF	Section includes progress % and counts (e.g., “3 of 8 completed – 37%”)
TC-DASH-53	PDF includes Status Summary	PDF generated	Open PDF	Section lists all conformity statuses with counts and optionally percentages
TC-DASH-54	PDF includes Requirements list	PDF generated	Open PDF	Table columns: **Requirement Name**, **Evaluated/Not**, **Conformity**
TC-DASH-55	PDF “Evaluated/Not” logic correct	Mixed finished/unfinished Requirements	Export PDF	Evaluated = finished; Not Evaluated = unfinished
TC-DASH-56	PDF “Conformity” logic corrects	Mixed data	Export PDF	Finished show conformity status; unfinished show “—” or “N/A”
TC-DASH-57	PDF matches on-screen data	Dashboard values noted	Export → Open PDF	Counts & percentages match on-screen charts at export time
TC-DASH-58	PDF handles many Requirements (pagination)	200+ Requirements	Export → Open PDF	Multi-page PDF rendered; no layout clipping
TC-DASH-71	Handles no-data / empty Area	Area with 0 Requirements	Open Dashboard	Progress = 0%; Evaluations Pie = all Not Evaluated; Conformity Pie empty; friendly message
TC-DASH-73	Data changes mid-export	Update data during export	Export PDF → Open PDF	PDF snapshot reflects state at export moment
TC-DASH-80	Percent rounding sums ≈100%	Uneven dataset	Open Dashboard	Pie values round correctly; total ~100%
TC-DASH-81	Data consistency with Requirements views	Same Area viewed in Requirements	Compare both screens	Numbers match between Requirements and Dashboard

Table 6: Team Compliance Assessment Dashboard – Executed and Passed Test

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

5.6. Scan Tabs

Description:

The Scans tab (distinct from the SBOM tab) lists previously triggered scans in a table. Scans are initiated via the Scan button located on the SBOM tab; this tab is read/act focused.

Scans can be triggered using the Scan button from the SBOM tab. The scans are listed in a table containing the following:

- **Status** (e.g., Pending, Running, Completed, Failed)
- **Source** (what triggered it: SBOM/Repo/Artifact/etc.)
- **Started** (timestamp)
- **Triggered By** (user/service)
- **Duration** (elapsed for completed/failed; live for running)
- **Total / Critical / High / Medium / Low** (finding counts)
- **Actions** (buttons: **Download**, **Delete**)

Top-right (or header) has a Refresh button that reloads the list and summary counts.

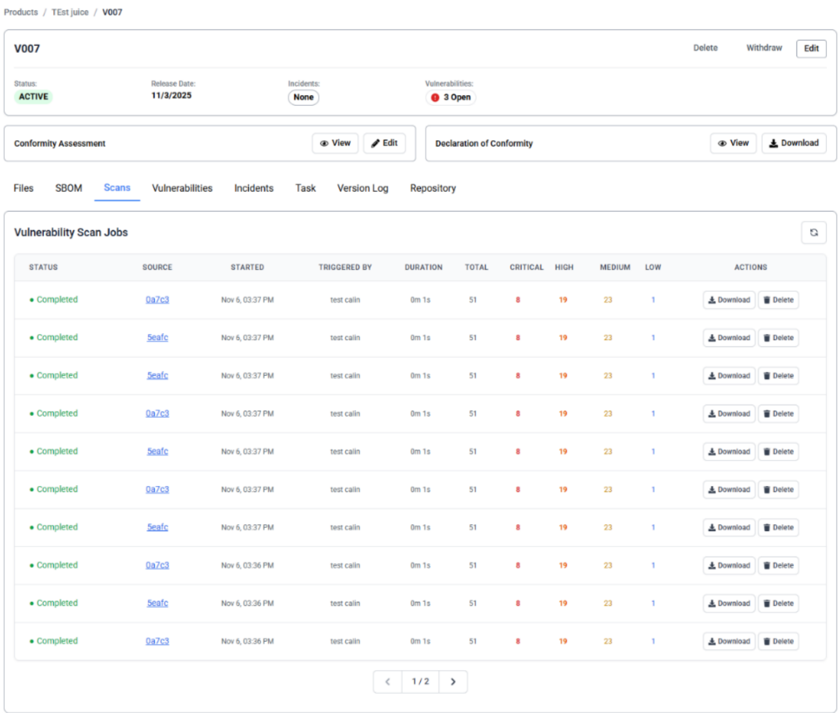


Figure 7: Scans tab

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Test cases executed and passed

Test ID	Description	Precondition	Steps	Expected Results
TC-SCAN-01	Scan tab loads with table and Refresh button	Project/Area exists	Open **Scan** tab	Table renders with headers in correct order; **Refresh** button visible
TC-SCAN-02	Empty state (no scans yet)	No scans exist	Open **Scan** tab	Empty-state message shown; no rows displayed
TC-SCAN-03	Scan triggered from SBOM appears in list	SBOM tab accessible	Trigger a scan from **SBOM** → Open **Scan** tab	New scan row appears with **Status=Pending/Queued**
TC-SCAN-04	Column presence and order	—	Inspect header row	Headers exactly: **Status, Source, Started, Triggered By, Duration, Total, Critical, High, Medium, Low, Actions**
TC-SCAN-06	Started timestamp formatting/time zone	Rows exist	Inspect **Started** column	Correct timestamp format and time zone; consistent with system settings
TC-SCAN-07	Duration updates while running	A scan is Running	Observe **Duration**	Duration dynamically increments until scan completes
TC-SCAN-08	Duration fixed after completion	A scan Completed/Failed	Observe **Duration**	Duration stops updating once scan finishes
TC-SCAN-09	Severity totals integrity	Row with counts	Compare **Total** to sum	**Total = Critical + High + Medium + Low**
TC-SCAN-10	Large count formatting	Row with big counts	Inspect counts	Large numbers formatted with thousand separators: zero values shown as "0"
TC-SCAN-15	Pagination functionality	> page size scans exist	Navigate pages	Page changes update correctly; data accurate for each page
TC-SCAN-16	Manual **Refresh** Reloads data	Rows exist	Click **Refresh**	Data reloads successfully; table preserves sort/filter state
TC-SCAN-17	Refresh updates running scan to completed	A scan finishes during test	Click **Refresh**	Status updates to **Completed** with final Duration and counts
TC-SCAN-20	Download file properties	Completed scan available	Click **Download**	File downloads successfully with correct filename, extension, and type
TC-SCAN-25	Delete requires confirmation dialog	Deletable row exists	Click **Delete**	Confirmation dialog appears warning about irreversible action

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

TC-SCAN-26	Cancel delete keeps row intact	Confirmation dialog open	Click **Cancel**	Row remains in table; no deletion occurs
TC-SCAN-27	Confirm delete removes row	Deletable scan available	Click **Delete → Confirm**	Row removed from table; pagination adjusts automatically
TC-SCAN-31	Multiple concurrent scans handled correctly	Trigger 2+ scans	Refresh periodically	Each scan row updates independently; no data crossover
TC-SCAN-32	Failed scan display behavior	A scan fails	Observe row	**Status=Failed**; Duration fixed; counts set to 0 or "N/A"; Download disabled per spec
TC-SCAN-36	Performance with large dataset	1000+ scans	Open tab and scroll/page	UI remains responsive; actions functional
TC-SCAN-71	Empty or no-data area handling	Area has 0 scans	Open **Scan** tab	Progress/scan list empty; friendly message shown ("No scans available")
TC-SCAN-73	Data changes mid-download/export	Scan data updates during download	Download scan report	Report reflects consistent data snapshot at download time

Table 7: Team Compliance Assessment Dashboard – Executed and Passed Test

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

5.7. Vulnerability Report & Add Vulnerability

Description:

From the ***Scan tab***, selecting a scan opens the **Vulnerability Report**: a table listing vulnerabilities with columns CVE, Severity, Package, Version, Fixed In, Description, Actions.

In **Actions**, **Create** opens the **Add Vulnerability page**. The Add Vulnerability form is shown with inputs (some prefilled):

- Name (prefilled)
- Status (prefilled),
- Severity (prefilled),
- Date of Discovery (prefilled),
- Summary (prefilled),
- Advisory IDs (empty),
- Assigner (current user preselected),
- checkbox “Has the product been made available on the territory of other Member States?” (unchecked by default)
- CVE (prefilled)
- Attachment section,
- Cancel / Add buttons.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

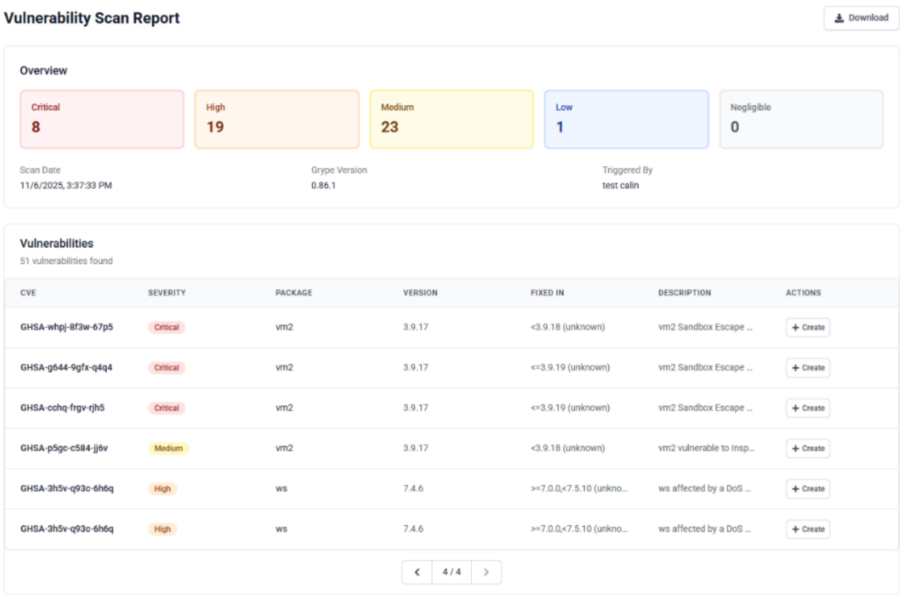


Figure 8: Vulnerability Scan Report page

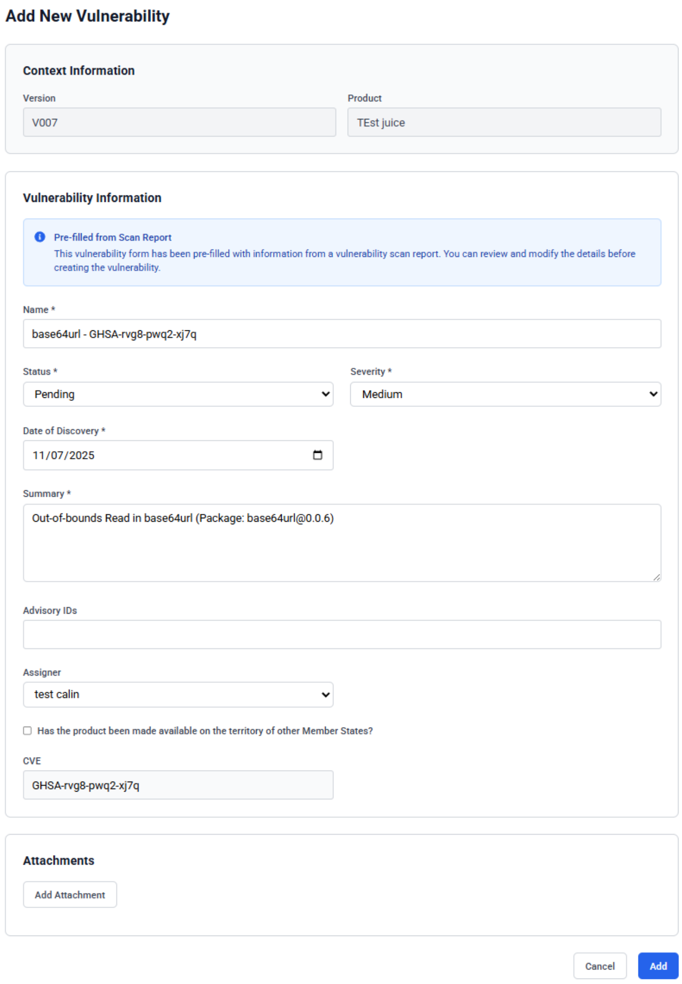


Figure 9: Add New Vulnerability from the Scan report

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

Test cases executed and passed

Test ID	Description	Precondition	Steps	Expected Results
TC-VULN-01	Open Vulnerability Report from a scan	A completed scan with vulnerabilities exists	From **Scan** tab, click a scan row	**Vulnerability Report** opens
TC-VULN-02	Report columns and order	Report is open	Inspect header row	Columns exactly: **CVE, Severity, Package, Version, Fixed In, Description, Actions**
TC-VULN-03	Row data renders correctly	Report has vulnerabilities	Inspect rows	Each row displays valid data in all columns
TC-VULN-04	Actions column shows **Create** button	Report opens	Inspect **Actions** column	Each row has a visible **Create** button
TC-VULN-05	**Download** button visible on top of report	Report opens	Observe top-right header area	**Download** button displayed on Vulnerability Report
TC-VULN-06	Download file properties	Report open with vulnerabilities	Click **Download**	File download starts with correct filename and type Json
TC-VULN-07	**Create** opens Add Vulnerability form	Report opens	Click **Create** on a row	**Add Vulnerability** form opens
TC-VULN-08	Prefilled fields visible	Form opened via **Create**	Observe inputs	**Name, Status, Severity, Date of Discovery, Summary, CVE** prefilled with data from selected row
TC-VULN-09	Assigner defaults to current user	Form open	Observe **Assigner** field	Current logged-in user preselected
TC-VULN-10	Advisory IDs field empty	Form open	Observe **Advisory IDs** input	Field empty and ready for entry
TC-VULN-11	Member States checkbox default	Form open	Observe checkbox “Has the product been made available on the territory of other Member States?”	Checkbox unchecked by default
TC-VULN-12	Attachment section visible	Form open	Scroll to **Attachments**	Upload component visible and active
TC-VULN-13	Editable fields	Form open	Edit **Name**, **Summary**, change **Status/Severity**	Edits accepted; dropdowns show valid options

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

TC-VULN-14	Required-field validation	Form open	Clear a required field (e.g., **Name**) → click **Add**	Inline validation appears; cannot save until corrected
TC-VULN-15	CVE field edit rule	Form open	Try editing **CVE**	Behaves per design (read-only or validated if editable)
TC-VULN-16	Advisory IDs format validation	Form open	Enter invalid Advisory ID → click **Add**	Validation error displayed; cannot save
TC-VULN-17	Checkbox value saved correctly	Form open	Toggle checkbox → click **Add**	Saved record reflects correct checkbox state
TC-VULN-18	Successful Add	All required fields valid	Click **Add**	Success message; new vulnerability created and linked
TC-VULN-19	Cancel discards changes	Form edited	Click **Cancel**	Returns to report; no new record created
TC-VULN-20	Attachments: allowed file types	Form open	Upload PDF/PNG/DOCX	Files appear in list with name and size
TC-VULN-21	Attachments: reject disallowed files	Form open	Upload EXE	Error shown; file not attached
TC-VULN-22	Attachments: enforce file size limit	Limit configured	Upload file exceeding limit	Error displayed; file rejected
TC-VULN-23	Multiple attachments and removal	Form open	Upload several files, remove one	All valid files shown; removed file disappears
TC-VULN-24	Attachments persist after save	Files attached	Click **Add** → open created record	Attached files visible in saved record
TC-VULN-25	New vulnerability visible in report	Creation succeeded	Return to **Vulnerability Report**	New vulnerability entry displayed in table
TC-VULN-26	Data integrity after creation	Record created	Open created record/details	All saved fields (Assigner, Dates, Status, Severity, Checkbox, Attachments) match user input

Table 8: Vulnerability Report & Add Vulnerability – Executed and Passed Test

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

5.8. Vulnerabilities Tab

Description:

The Vulnerabilities tab displays all vulnerabilities that have been added in the system.

It contains a table with the following columns:

- Name
- Status
- Severity
- Date of Discovery
- Description
- Actions

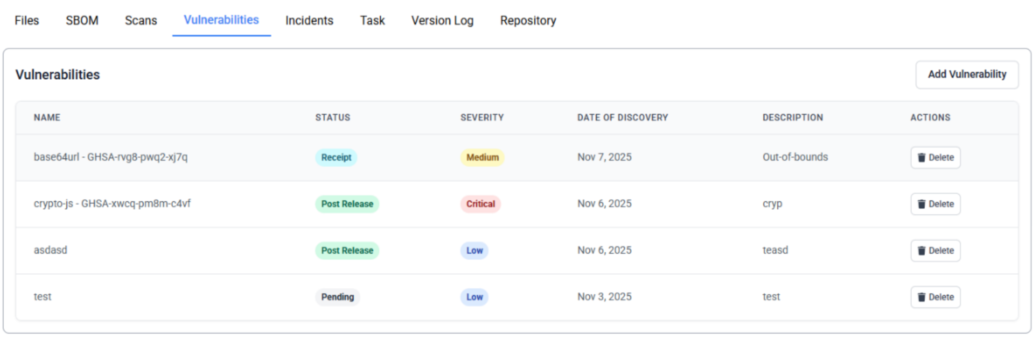


Figure 10: Vulnerabilities tab

Above the table, there is an "**Add Vulnerability**" button.

When clicked, it opens the ***Add Vulnerability form*** (same layout as the previous one from the Vulnerability Report), but none of the fields are prefilled. Also, for each vulnerability row there is a **Delete button**, which removes that vulnerability.

Clicking on any row in the table opens the **Vulnerability Details page**, which is divided into three sections:

1. **Context Information**:
    - Vulnerability Name
    - Status
    - Severity

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

- Affected Version
- Affected Product
- Affected Vendor
  Contains two buttons:
- **Edit** – opens an edit pop-up allowing the user to modify the vulnerability information
- **Close** – sets the vulnerability's **Status** to *Post release*

2. **Extended Data**:
   - CVE
   - Description
   - Created By
   - Updated By
   - Created At
   - Updated At

3. **Attachments**: contains an "***Add Attachment***" button that allows the user to upload one file at a time. The files are then displayed in the table with the previously mentioned columns.

Test cases executed and passed

Test ID	Description	Precondition	Steps	Expected Results
TC-VULNS-01	Verify that the Vulnerabilities tab loads with table and Add button	Project/Area exists	Open the **Vulnerabilities** tab	Table is displayed; **Add Vulnerability** button visible above it
TC-VULNS-02	Verify table column headers and order	Vulnerabilities tab open	Inspect table header row	Headers appear exactly as: **Name, Status, Severity, Date of Discovery, Description**
TC-VULNS-03	Verify row data is correctly displayed	Existing vulnerabilities present	Inspect table rows	Each row shows valid data for Name, Status, Severity, Date, and Description
TC-VULNS-04	Verify empty state when there are no vulnerabilities	No vulnerabilities exist	Open the **Vulnerabilities** tab	Empty state message shown; no rows visible
TC-VULNS-05	Verify Add Vulnerability button	Vulnerabilities tab open	Click **Add Vulnerability**	Add Vulnerability form opens; all fields are

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

	opens an empty Add form			empty (no prefilled data)
TC-VULNS-06	Verify all fields and default states on Add Vulnerability form	Add Vulnerability form opens	Observe all fields	All fields are empty; dropdowns unselected; checkbox unchecked by default
TC-VULNS-07	Verify required field validation	Add form open	Leave required fields empty → click **Add**	Inline validation appears; saving blocked until required fields are completed
TC-VULNS-08	Verify successful vulnerability creation	All required fields filled	Click **Add**	Success notification displayed; vulnerability added to the list
TC-VULNS-09	Verify cancel button discards changes	Form filled	Click **Cancel**	Navigates back to list; no data saved
TC-VULNS-10	Verify new vulnerability appears in the list after creation	Vulnerability created	Return to **Vulnerabilities** tab	Newly added vulnerability appears in table with correct data
TC-VULNS-11	Verify clicking a vulnerability opens the details page	Vulnerability exists	Click on a row	**Vulnerability Details** page opens
TC-VULNS-12	Verify fields in Context Information section	Details page open	Observe Context Information section	Displays: Name, Status, Severity, Affected Version, Affected Product, Affected Vendor
TC-VULNS-13	Verify Edit button opens edit pop-up	Details page open	Click **Edit**	Edit pop-up opens with current vulnerability information
TC-VULNS-14	Verify required field validation in edit pop-up	Edit pop-up open	Clear required field → click **Save**	Inline validation displayed; save blocked
TC-VULNS-15	Verify successful update of vulnerability	Edit pop-up open	Modify fields → click **Save**	Pop-up closes: updated information displayed in Context Information section
TC-VULNS-16	Verify Close button changes status to Post release	Details page open	Click **Close**; confirm action if prompted	Status field changes to **Post release**
TC-VULNS-17	Verify updated status appears in vulnerabilities list	Vulnerability closed	Return to **Vulnerabilities** tab	Status in list updated to **Post release**
TC-VULNS-18	Verify Extended Data fields are displayed correctly	Details page open	Observe Extended Data section	Displays: CVE, Description, Created By, Updated By, Created At, Updated At
TC-VULNS-19	Verify Updated by and Updated At fields refresh on edit	Vulnerability edited	Observe Extended Data section	Updated By and Updated At fields reflect last modification

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

TC-VULNS-20	Verify Created by and Created remain unchanged	Vulnerability edited	Observe Extended Data section	Created By and Created At remain consistent with original record
TC-VULNS-18	Verify Extended Data fields are displayed correctly	Details page open	Observe Extended Data section	Displays: CVE, Description, Created By, Updated By, Created At, Updated At
TC-VULNS-19	Verify Updated by and Updated At fields refresh on edit	Vulnerability edited	Observe Extended Data section	Updated By and Updated At fields reflect last modification
TC-VULNS-20	Verify Created by and Created remain unchanged	Vulnerability edited	Observe Extended Data section	Created By and Created At remain consistent with original record
TC-VULNS-21	Verify Add Attachment button is displayed	Details page open	Scroll to Attachments section	**Add Attachment** button visible
TC-VULNS-22	Verify uploading one file per action	Details page open	Click **Add Attachment** → select one file	One file uploaded successfully; appears in attachments table
TC-VULNS-23	Verify file type validation	Details page open	Upload unsupported file (e.g., .exe)	Error displayed; file rejected
TC-VULNS-24	Verify file size validation	File size limit defined	Upload file exceeding size limit	Error displayed; file not uploaded
TC-VULNS-25	Verify attachments table headers and order	Attachment uploaded	Inspect table headers	Headers: **Name, Type, Date Added, Added By, Actions**
TC-VULNS-26	Verify attachment data displayed correctly	Attachment uploaded	Inspect row in table	Displays correct file name, type, date, and added by user
TC-VULNS-27	Verify Download button downloads file	Attachment uploaded	Click **Download** in Actions	File downloads successfully; correct content and filename
TC-VULNS-28	Verify Delete button removes file	Attachment uploaded	Click **Delete** → confirm	File removed from table and storage
TC-VULNS-29	Verify multiple uploads over time	Details page open	Upload file A → upload file B	Both files listed in table with correct order
TC-VULNS-30	Verify attachment persistence	Attachment uploaded	Leave details page → return	File remains listed in Attachments table

Table 9: Vulnerability Tabs – Executed and Passed Test

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

5.9. Incidents

Description:

The **Incidents** tab displays all created incidents in a table with the following columns:

- Status
- Classifications
- Attack Type
- Severity
- Date Detected
- Reporter
- Description
- Actions:
  - View Button
  - Delete button
- Add Incident

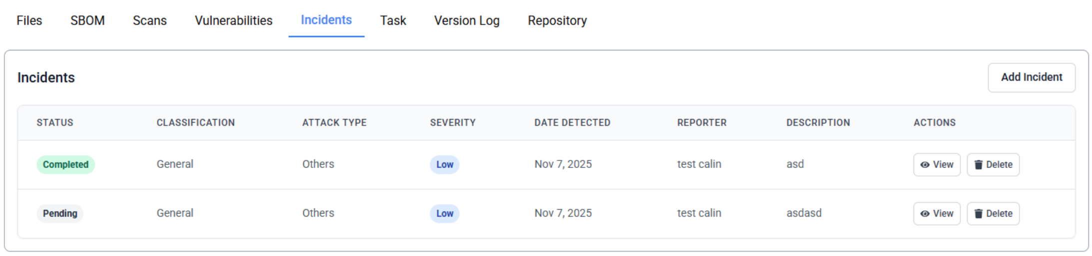
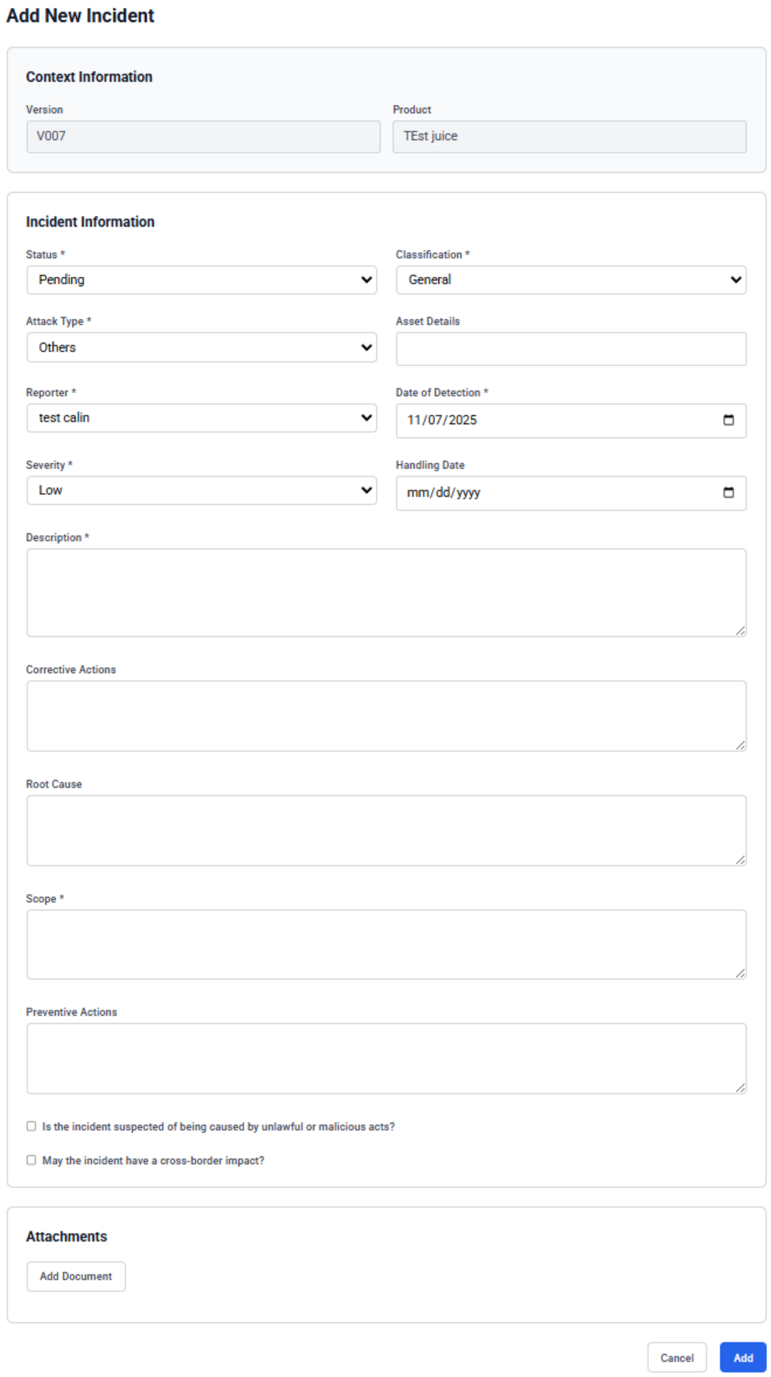


Figure 11: Incidents tab

The Add Incident buttons open another page:

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.



Mandatory Fields:

- Status
- Classification
- Attack Type
- Reporter (prefilled with current user)
- Date of Detection
- Severity
- Description
- Scope

Optional Fields:

- Asset Details
- Handling Date
- Corrective Actions
- Root Cause
- Preventing Actions

Figure 12: Add New Incident tab

Checkboxes are unchecked by default:

- *Is the incident suspected of being caused by unlawful or malicious acts?* → reveals a mandatory free-text input when checked
- *May the incident have a cross-border impact?* → reveals a mandatory free-text input when checked

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

At the bottom of the page, there's an **Attachment section** (same as in Vulnerabilities Section) allowing one file upload per action, displayed in a table with the same column options.

Clicking a row opens the "**Incident Details**" page, showing all fields from creation and two top buttons:

- **Edit**: opens edit page with editable fields.
- **Close**: sets Status to "Complete"

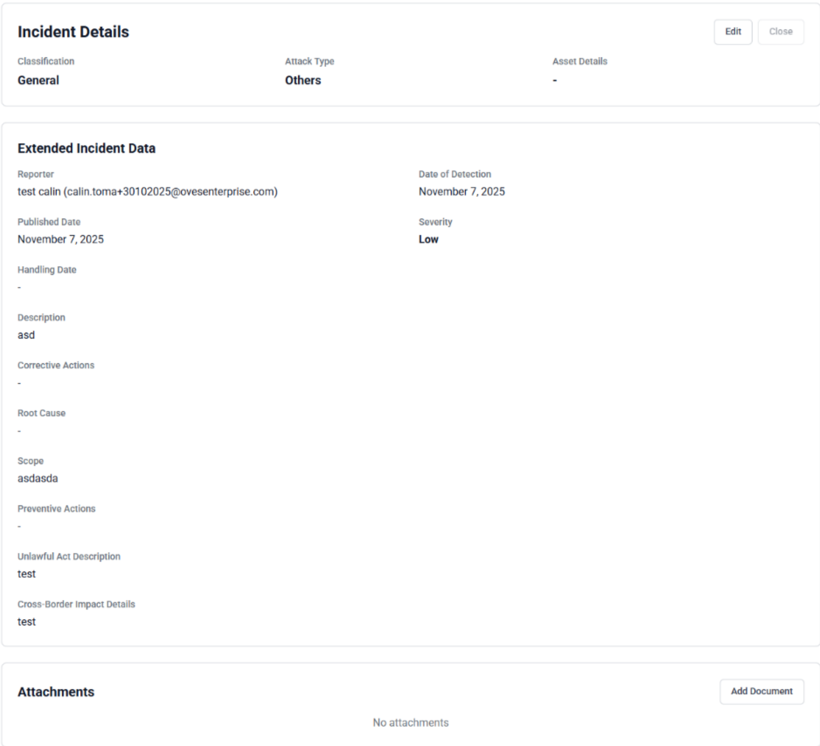


Figure 13: Incident Details page

Test cases executed and passed

Test ID	Description	Precondition	Steps	Expected Results
TC-INC-01	Verify that the Incidents tab loads correctly	Project/Area exists	Open **Incidents** tab	Table displays with all incidents; **Add Incident** button visible
TC-INC-02	Verify the table column headers and order	Incidents tab open	Inspect table header row	Headers appear in this order: **Status, Classification, Attack Type, Severity, Date Detected, Reporter, Description, Actions**

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

TC-INC-03	Verify that existing incidents are displayed correctly	One or more incidents exist	Inspect table rows	Each row shows valid data for all columns
TC-INC-04	Verify empty state when no incidents exist	No incidents exist	Open **Incidents** tab	Empty-state message displayed; no rows visible
TC-INC-05	Verify Delete button is displayed for each row	Incidents exist	Observe **Actions** column	Each row contains a **Delete** button
TC-INC-06	Verify Delete button removes the incident	Deletable incident exists	Click **Delete** → confirm	Incident removed from table; no longer visible
TC-INC-07	Verify clicking a row opens the Incident Details page	Incident exists	Click a row	**Incident Details** page opens showing all incident data
TC-INC-08	Verify Add Incident button opens empty form	Incidents tab open	Click **Add Incident**	Add Incident page opens; all fields empty except **Reporter**
TC-INC-09	Verify Reporter is prefilled with current user	Add page open	Inspect **Reporter** field	**Reporter** field automatically populated with current logged-in user
TC-INC-10	Verify all other fields are initially empty/unselected	Add page open	Inspect all fields	Text inputs empty, dropdowns unselected, checkboxes unchecked
TC-INC-11	Verify required field validation	Add page open	Leave required fields empty → click **Add**	Inline validation messages appear; form not submitted
TC-INC-12	Verify valid date entry for Date of Detection	Add page open	Enter valid date	Accepted without error
TC-INC-13	Verify “Unlawful/Malicious” checkbox behavior	Add page open	Check the box	A free-text input appears and becomes mandatory
TC-INC-14	Verify validation for “Unlawful/Malicious” free-text	Add page open	Check the box, leave text empty → click **Add**	Validation error shown; cannot save
TC-INC-15	Verify “Cross-border impact” checkbox behavior	Add page open	Check the box	A free-text input appears and becomes mandatory
TC-INC-16	Verify validation for “Cross-border impact” free-text	Add page open	Check the box, leave text empty → click **Add**	Validation error shown; cannot save
TC-INC-17	Verify both checkboxes and text fields work together	Add page open	Check both boxes, complete both text fields, fill required data → click **Add**	No validation errors; record created successfully
TC-INC-18	Verify optional fields can be filled	Add page open	Fill optional fields (**Asset Details**,	Values accepted; no validation triggered

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

			Handling Date, etc.)	
TC-INC-19	Verify successful creation of incident	All mandatory fields completed	Click **Add**	Success message displayed; incident created
TC-INC-20	Verify Cancel discards data	Form has inputs	Click **Cancel**	Return to Incidents tab; no data saved
TC-INC-21	Verify new incident appears in table	Incident created	Return to **Incidents** tab	New incident row appears with correct data
TC-INC-22	Verify details page shows all fields correctly	Incident exists	Open incident details	All fields (mandatory + optional) displayed with correct values
TC-INC-23	Verify Edit button opens edit page	Details open	Click **Edit**	Edit page opens with prefilled data
TC-INC-24	Verify required validation on edit	Edit page open	Clear required field → click **Save**	Inline validation message; save blocked
TC-INC-25	Verify dynamic checkbox validation on edit	Edit page open	Check one or both checkboxes without text → click **Save**	Validation errors shown for missing text fields
TC-INC-26	Verify successfully edit updates data	Edit page open	Modify field(s) → click **Save**	Updated values appear in details view
TC-INC-27	Verify Close button sets status to Complete	Details open	Click **Close**; confirm action	Status changes to **Complete** and persists
TC-INC-28	Verify list reflects closed status	Incident closed	Return to **Incidents** tab	Status column shows **Complete** for that incident
TC-INC-29	Verify Add Attachment button is visible	Details open	Scroll to **Attachments** section	**Add Attachment** button visible
TC-INC-30	Verify single file upload per action	Details open	Click **Add Attachment** → select one file	File uploaded and displayed in table
TC-INC-31	Verify file type validation	Details open	Upload unsupported file type (.exe)	Error message displayed; file not added
TC-INC-32	Verify file size validation	Limit configured	Upload file exceeding limit	Error displayed; upload blocked
TC-INC-33	Verify attachments table headers and data	Attachment exists	Inspect headers and row	Headers: **Name, Type, Date Added, Added**

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

				By, Actions; values displayed correctly
TC-INC-34	Verify Download button functionality	Attachment exists	Click **Download**	File downloads successfully with correct name/type
TC-INC-35	Verify Delete button removes attachment	Attachment exists	Click **Delete** → confirm	Attachment removed from list
TC-INC-36	Verify multiple uploads over time	Details open	Upload file A → upload file B	Both files listed in order added
TC-INC-37	Verify attachments persist after navigation	Attachment exists	Leave details → return	File remains visible in attachments table
TC-INC-38	Verify data consistency between list and details	Incident exists	Compare data from list vs details	**Status**, **Classification**, **Attack Type**, **Severity**, **Date**, **Reporter**, **Description** match
TC-INC-39	Verify edited data reflected in list	Edit completed	Return to **Incidents** tab	Updated data visible in table
TC-INC-40	Verify deleted incidents are no longer displayed	Incident deleted	Observe **Incidents** tab	Deleted incident removed from table

Table 10: Incidents Tabs – Executed and Passed Test

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

6. Testing Objectives and Results Summary

6.1. Objective

The primary objective of this testing effort was to validate the overall reliability, accuracy, and functional integrity of the Product Management and Compliance Assessment Platform. The focus was on ensuring that all workflows operate as intended across the platform's key modules, including product compliance management, vulnerability tracking, and incident monitoring. The tests aimed to verify proper enforcement of business rules, correct handling of mandatory fields, accurate status transitions, and consistent persistence of data across all user interactions and navigation paths.

6.2. Results

Testing covered approximately 180 test cases spanning all functional modules of the platform. Functional test cases confirmed that:

- User interface components were rendered correctly and consistently across workflows,
- Mandatory validations operated as expected, preventing incomplete or invalid data entry,
- Attachments could be uploaded, downloaded, and managed without errors,
- Status changes for products, vulnerabilities, and incidents persisted correctly across navigation and updates,
- Reports and dashboards accurately reflected the underlying data, including progress, conformity, and evaluation metrics.

6.3. Key Outcomes

The testing effort demonstrates that the platform meets expected behavior and functional requirements for the management of products, vulnerabilities, and incidents. All critical workflows were validated successfully, ensuring that data entry, visibility, and lifecycle management processes are reliable and consistent. The system provides a robust foundation for operational use, with confirmed compliance with business rules, accurate reporting, and dependable workflow enforcement.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

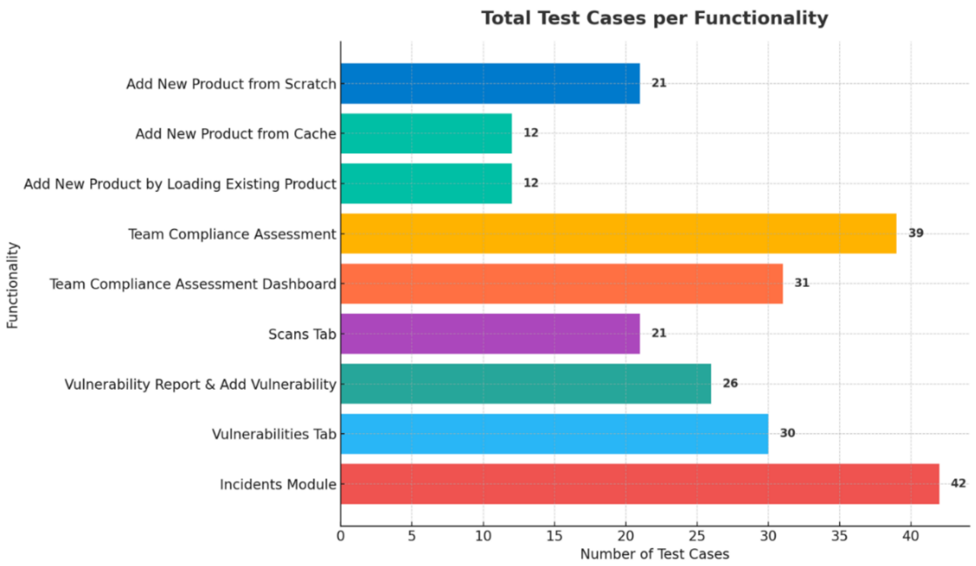


Figure 14: Total Test Cases per Functionality

7. Conclusion

The testing campaign comprehensively verified the Product Management and Compliance Assessment Platform's readiness for deployment.

All modules—from product setup through assessment tracking and reporting—were tested end-to-end to confirm that data integrity, business logic, and user interface behaviors align with requirements. The testing team executed manual, exploration, black box, and regression tests, ensuring full coverage of workflows and integrations.

Results demonstrated:

- Stable and consistent system behavior across all tested areas
- Correct enforcement of business rules and mandatory validations
- Reliable file management, including uploads and export reports
- Accurate and responsive dashboards and progress indicators
- Proper functionality of vulnerability and incident tracking features

No major blocking issues were observed. The platform is functionally sound, with validated workflows and robust handling of user operations, supporting its transition toward production or client acceptance phases.

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.

OSCRAT

Open-Source Cyber Resilience Act Tools

OSCRAT – Testing Report M12

www.oscrat.eu

https://www.linkedin.com/

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. The project funded under Grant Agreement No. 101190180 is supported by the European Cybersecurity Competence Centre.