OSCRAT

Open-Source Cyber Resilience Act Tools

D3.3

OSCRAT -Testing Report M6

Submission date: 31/05/2025

Author: 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.

OSCRAT: Testing report M6

Project acronym	OSCRAT
Project title	Open-Source Cyber Resilience Act Tools
Number	101190180
Work package	WP3 – Software design and development
Due Date	31/05/2025
Submission Date	31/05/2025
Lead Partner	OVES Enterprise
Author name(s)	Liliana Hornea
Version	1.0
Language	EN
Format	Digital
Status	Final Version
Type:	☒ R – Document, Report ☐ DEC – Websites, patent filings, videos, etc. ☐ DEM – Demonstrator, pilot, prototype
Dissemination level:	☒ PU - Public ☐ SEN - Sensitive

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.

Abstract

This QA Test Report presents the verification and validation of two core functionalities within the OSCRAT system: the Eligibility form and the Product List Management interface. The Eligibility form is designed to assess whether a product falls under the Cyber Resilience Act by guiding the user through a series of mandatory single-answer questions, with immediate disqualification options and progress tracking. Upon eligibility confirmation, users can create or log into an account. The Product List Management interface enables users to view, add, and manage products via a data table, search and filter capabilities, and detailed product-specific actions including editing, incident and vulnerability tracking, SBOM file uploads, and product activity logs. The report notes that the data used in testing is mocked and not final.

Keywords

test scenario, functionality, methodologies

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

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. - Project: 101190180.

Table of contents

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

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

List of Figures

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

1. Introduction

Due to the extended timeframe required by our WP2 colleagues to complete the Research and Discovery phase & our decision to approach the project in an Agile fashion, we are currently experiencing a slight delay in the overall project timeline. This stage plays a pivotal role in laying a solid foundation for the next components of the project, and the additional time invested was essential to ensure both the quality and reliability of the deliverables.

Concurrently, we have encountered challenges in accessing the necessary information—particularly in relation to clear and detailed working specifications—which has impacted the momentum of our own activities.

As shared during the TPM in Berlin, the entire OSCRAT team is aligned on the nature of these delays. In response, OVES Enterprise is actively recalibrating the subsequent phases in order to mitigate the impact on the global schedule. We remain confident in our ability to maintain progress and deliver in line with the adjusted milestones.

This QA Test Report documents the verification and validation of two functionalities implemented in the OSCRAT platform:

1. **Product Eligibility Form** – This form is designed to determine whether a product falls under the scope of the **Cyber Resilience Act**.

2. **Product List Management Interface** – a table-based interface that allows users to manage, view, and interact with product records and associated metadata (e.g., incidents, files, SBOMs).

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. Objectives

- Validate that all functional and business requirements are implemented correctly
- Ensure form logic (conditional flow, eliminatory rules, and result screens) works as intended
- Confirm data integrity and interactivity across product-related views
- Verify that usability features such as progress indicators and tabbed navigation are intuitive and stable

---

3. Testing Methodologies Used

To ensure thorough and reliable coverage, the following **testing methodologies** were applied:

3.1 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)

3.2 Exploratory Testing

- Performed around areas involving conditional branching, dynamic screen changes, and tab-based product sections

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

- Allowed identification of unexpected behaviors and edge cases not explicitly documented

3.3 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

3.4 Regression Testing

- Ensured that enhancements or fixes did not break previously working functionality like Sign In and Create Account

4. Functionality Overviews

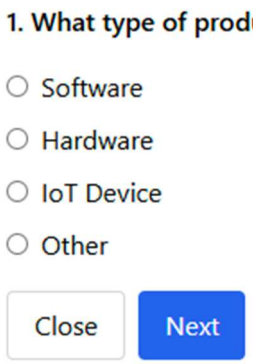
4.1 Product Eligibility Form

This form is used to determine whether a product falls under the scope of the Cyber Resilience Act based on the user's responses to a predefined set of mandatory questions.

Key behavior includes:

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

- Each question allows a single selection (radio button)



1.

Figure 1: Question selection

- Each answer is categorized as either:
    - eliminatoryTrue: instantly ends the form and marks the product **out of scope**.
    - eliminatoryFalse: allows the form to proceed.

- If **any** eliminatoryTrue answer is selected, the form stops and displays a **"No qualification needed"** message.

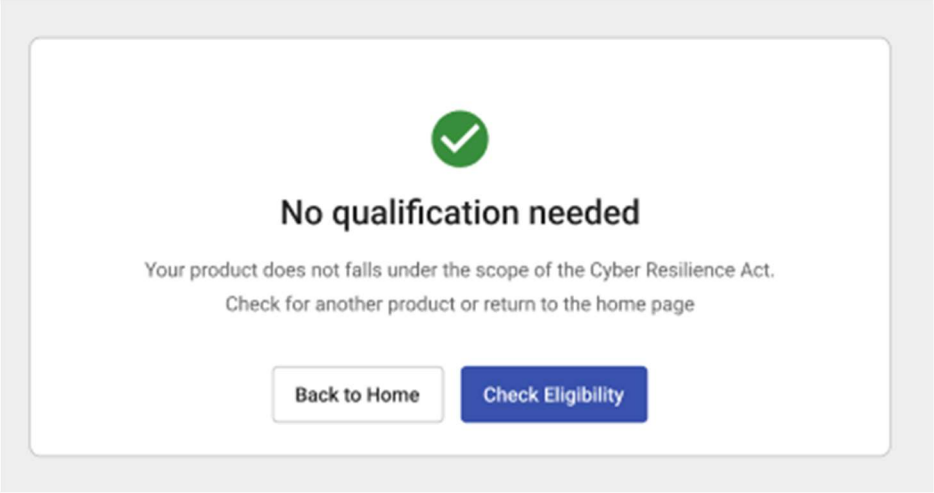


Figure 2: No qualification needed screen

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

- If **all** answers are eliminatoryFalse, the form confirms the product is **under scope** and shows a **"Continue eligibility check"** message.

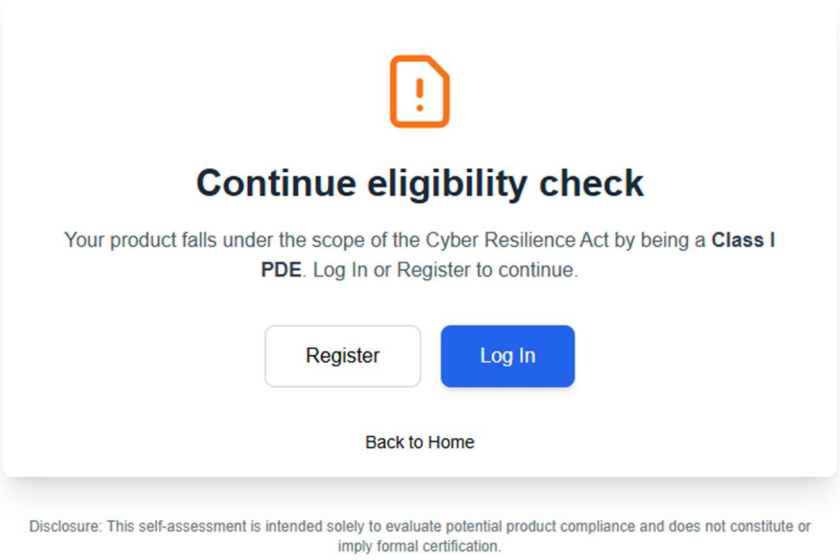


Figure 3: Continue eligibility check screen

- A **progress bar** updates dynamically to reflect the number of questions answered and remaining.

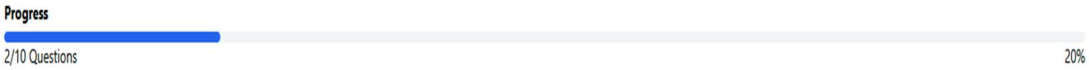


Figure 4: Progress bar screen

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

ii. 4.2 Product List Interface

The product list interface allows users to manage previously added products. Features include:

- A **data table** displaying each product's key details.

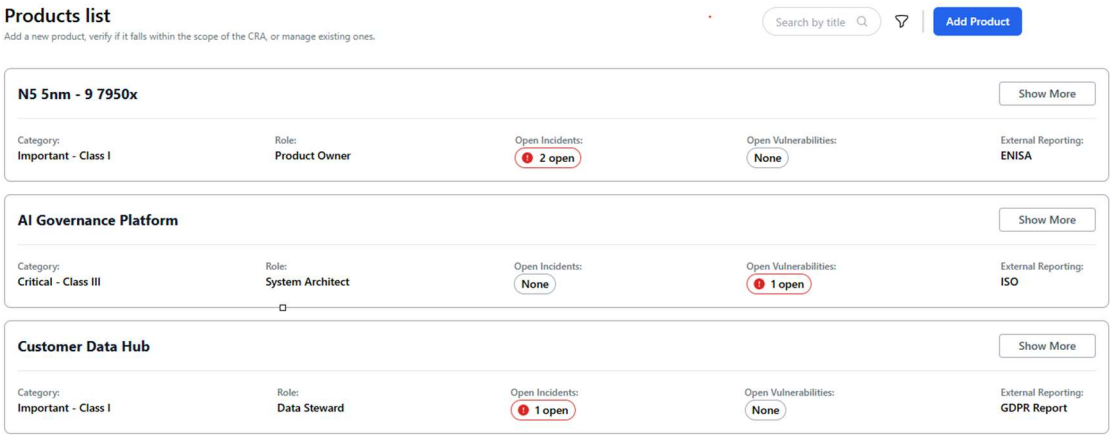


Figure 5: Data table display

- **Filtering** options based on main characteristics.

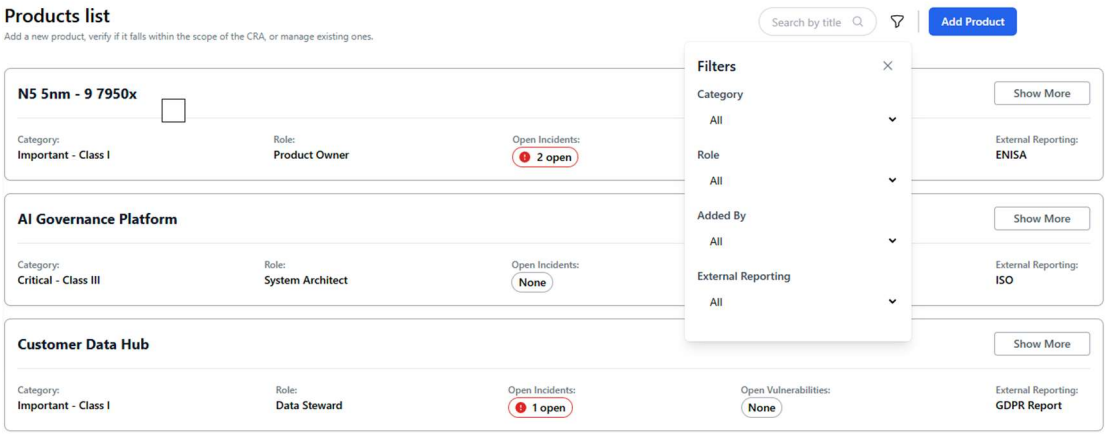
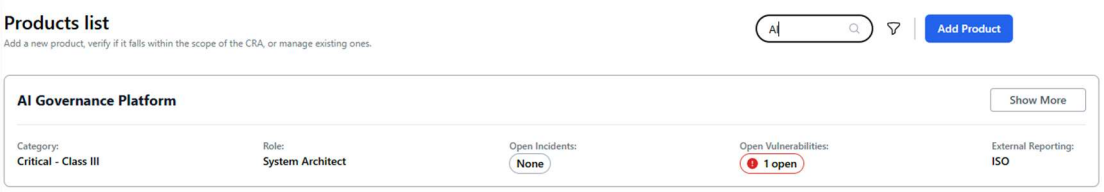


Figure 6: Filter options

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

- A **search bar** for quick product lookup by title.



1. *Figure 7: Search bar*

- A **"Show more"** button that reveals detailed product information and the following tabs:
  - **Edit / Delete / Withdraw actions**

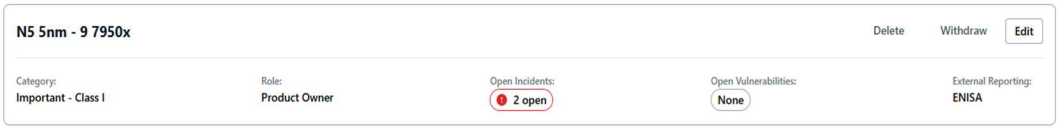
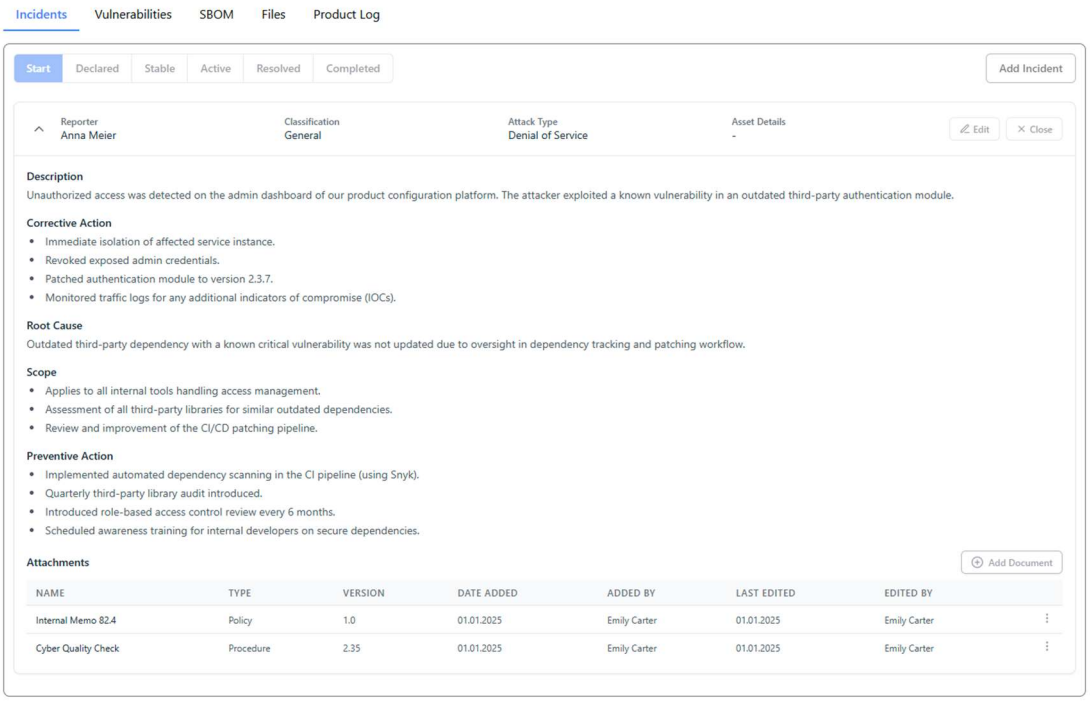


Figure 8: Edit / Delete / Withdraw actions

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

- **Incidents** tab (user-submitted issues)



2. *Figure 9: Incidents tab*

- **Vulnerabilities** tab

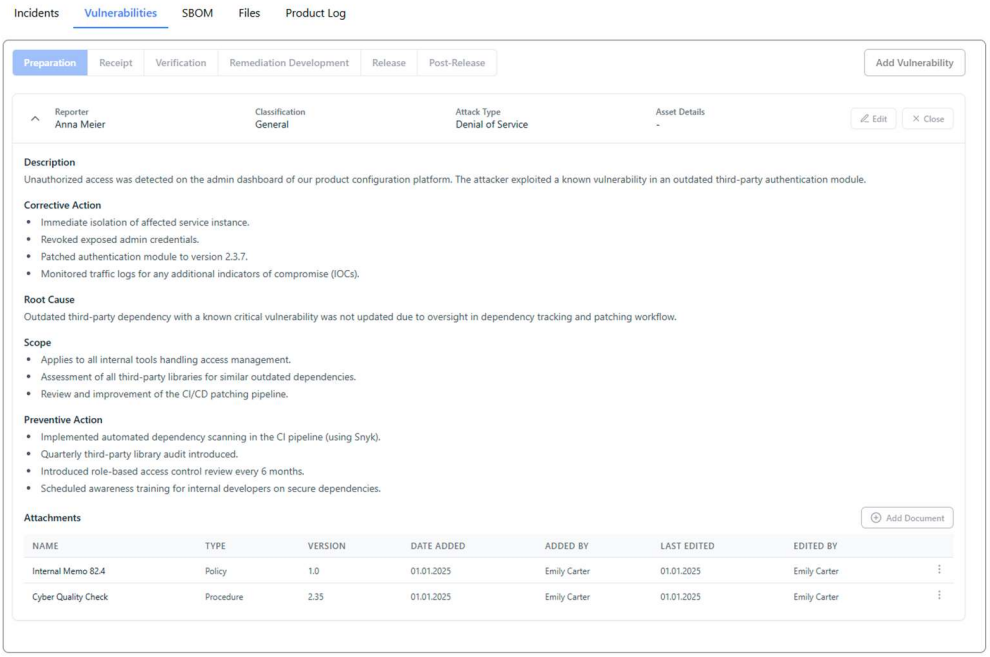


Figure 10: Vulnerabilities tab

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

- **SBOM** (Software Bill of Materials) upload area

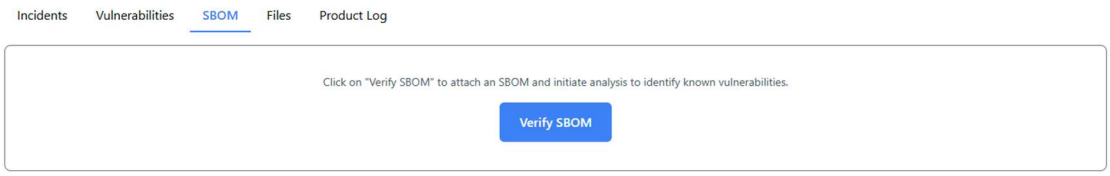


Figure 11: SBOM

- **Files** tab for related documentation

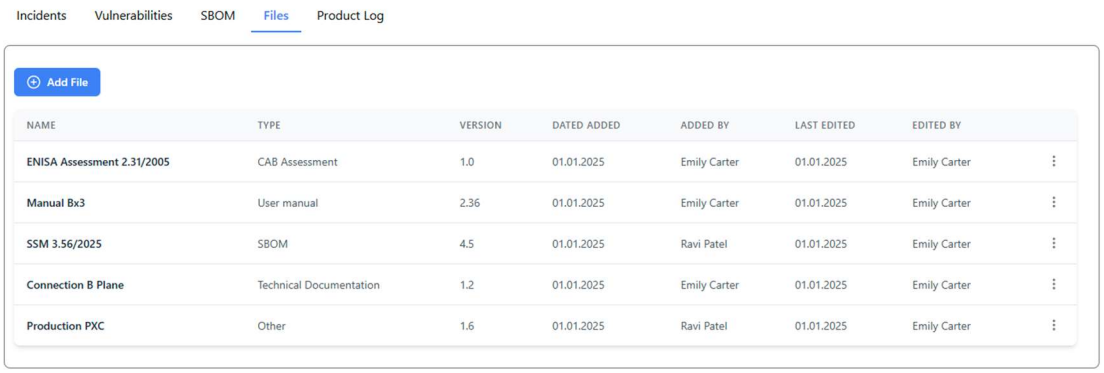


Figure 12: Files tab for related documentation

- **Product Log** tracking all changes made

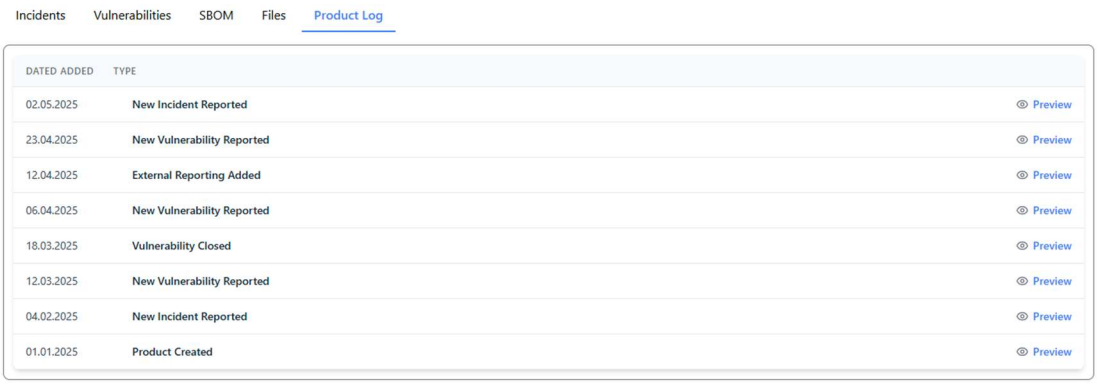


Figure 13: Product Log tracking

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

5. Test Scenarios

5.1 Eligibility Form

TC ID	Scenario	Steps	Expected Result	Status
TC-FORM-01	Load form correctly	Navigate to the form page	The form loads with the first question visible and the progress bar at 0%	☑ Pass
TC-FORM-02	Single answer per question (radio button)	Attempt to select multiple answers for a question	Only one answer is selectable per question (radio behavior enforced)	☑ Pass
TC-FORM-03	Question left unanswered	Try to submit the form with an unanswered question	A validation error is shown: “This field is required”	☑ Pass
TC-FORM-04	Stop form on first eliminatoryTrue answer	Select an eliminatoryTrue answer for Q1	The form stops immediately and shows “No qualification needed”; progress halts	☑ Pass
TC-FORM-05	Stop form on third eliminatoryTrue answer	Answer Q1 and Q2 with eliminatoryFalse; Q3 with eliminatoryTrue	The form stops at Q3 with a "No qualification needed" message; progress halts	☑ Pass

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

TC-FORM-06	All answers are eliminatoryFalse	Complete all questions with eliminatoryFalse answers	Form completes and shows “Continue eligibility check”; progress bar at 100%	☑ Pass
TC-FORM-07	Mixed eliminatoryTrue and False answers	Select eliminatoryTrue on any question in the flow	The form stops immediately and marks the product as "No qualification needed"	☑ Pass
TC-FORM-08	eliminatoryTrue answer on last question	Answer all prior questions with eliminatoryFalse, last with True	The form stops at the last question and shows “No qualification needed”	☑ Pass
TC-FORM-09	Progress bar updates with each answer	Answer questions sequentially	The progress bar increments dynamically after each question is answered	☑ Pass
TC-FORM-10	Progress bar caps at final question	Answer all questions in the form	The progress bar reaches and stops at 100% completion	☑ Pass
TC-FORM-11	Navigate back to previous question	Click “Back” on Q3	Q2 is displayed again; previously selected answer in Q2 is still selected	☑ Pass
TC-FORM-12	Navigate forward after going back	Click “Back” to Q2, then “Next”	Q3 is displayed again; answer in Q3 remains selected	☑ Pass

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.

			unless changed manually	
TC-FORM-13	Navigate back from first question	Try clicking “Back” on Q1	Button is disabled or form remains on Q1 (no crash or error)	☑ Pass
TC-FORM-14	Answer updated after going back	Click “Back” to Q2, change the answer, then proceed	New answer is saved; logic adjusts accordingly (e.g., form continues or ends)	☑ Pass

5.2 Product List Management Interface

TC ID	Scenario	Steps	Expected Result	Status
TC-LIST-01	Load product list	Navigate to the product list view	Table of user-added products is displayed	☑ Pass
TC-LIST-02	Search by product title	Type a full or partial product title in the search bar	Product list filters and displays only matching results	☑ Pass
TC-LIST-03	Filter by characteristic	Apply a filter based on product attribute (e.g., category, role)	Table updates to show only products matching selected filter(s)	☑ Pass

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-LIST-04	Expand product details with “Show more”	Click “Show more” on a product row	Additional product details and tabs become visible	☑ Pass
TC-LIST-05	View Incidents tab	Expand a product and click “Incidents” tab	Tab opens and displays incident list (or message if no incidents)	☑ Pass
TC-LIST-06	View Vulnerabilities tab	Click the “Vulnerabilities” tab	List of known vulnerabilities is shown or empty state message is displayed	☑ Pass
TC-LIST-07	Upload SBOM file	Go to “SBOM” tab, upload a valid SBOM file	File is accepted, and vulnerabilities (if detected) are shown	☑ Pass
TC-LIST-08	Upload supporting files	Go to “Files” tab, upload a document (PDF, image, etc.)	File appears in the uploaded files list	☑ Pass
TC-LIST-09	View product log	Open the “Product Log” tab	Table of timestamped product actions is displayed	☑ Pass

5.3. User Login - regression

TC ID	Scenario	Steps	Expected Result	Status

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

TC-LOGIN-01	Login with valid credentials	Enter registered email and correct password, click “Sign In”	User is successfully logged in and redirected to the dashboard	☑ Pass
TC-LOGIN-02	Invalid password	Enter correct email but wrong password, click “Sign In”	Error message displayed: “Invalid credentials”	☑ Pass
TC-LOGIN-03	Unregistered email	Enter an email that is not in the system	Error message displayed: “Invalid credentials”	☑ Pass
TC-LOGIN-04	Empty email and password fields	Leave fields empty and attempt to log in	Validation errors shown: “Email is required field”, “Password is required field”	☑ Pass
TC-LOGIN-05	Email format validation	Enter an invalid email format (e.g., user@)	Validation error displayed: “Email must be a valid email”	☑ Pass
TC-LOGIN-06	Password field is masked	Type into the password field	Characters are hidden (e.g., replaced by •••••)	☑ Pass

5.4 Create account - regression

TC ID	Scenario	Steps	Expected Result	Status

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

TC-SIGNUP-01	Create account with valid data	Enter valid values in all fields including a strong password (8+ chars); click “Register”	Account is created successfully; user is logged in or redirected	☑ Pass
TC-SIGNUP-02	All fields required	Leave one or more fields (e.g., First Name or Team) empty; attempt to submit	Validation errors shown for each missing field	☑ Pass
TC-SIGNUP-03	Duplicate email	Enter an email already registered; fill in other valid fields	Error message shown: “Email already in use”	☑ Pass
TC-SIGNUP-04	Invalid email format	Enter an incorrectly formatted email (e.g., john.doe@)	Error message displayed: “Enter a valid email address”	☑ Pass
TC-SIGNUP-05	Password under 8 characters	Enter a password with fewer than 8 characters (e.g., test123)	Error message displayed: “Password must be at least 8 characters”	☑ Pass
TC-SIGNUP-07	Password exactly 8 characters	Enter a password with exactly 8 characters (e.g., Test1234)	Password accepted; form submits if all other data is valid	☑ Pass

6. Conclusion

The QA validation process for the latest release of the OSCART Platform confirms that the new and existing functionalities are **functionally stable**, **logically consistent**, and meet the **defined business requirements**.

6.1 Summary of Tested Functionalities:

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

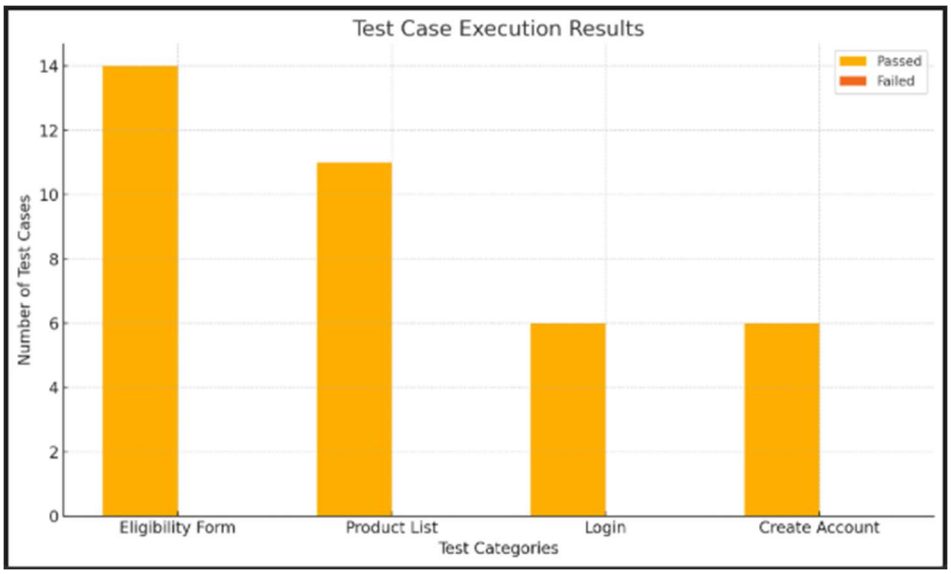
- **Product Eligibility Form**
  Thoroughly validated for eliminatory logic, progress tracking, back-and-forth navigation, and input validation. The form behaves as expected and dynamically adapts based on user answers.

- **Product List Management Interface**
  Core operations such as displaying products, filtering, searching, and accessing detailed tabs (Incidents, Vulnerabilities, SBOM, Files, Product Logs) function smoothly. Actions such as edit/delete/withdraw were excluded from this cycle by request.

- **Authentication Flows (Login & Create Account)**
  All critical scenarios — including valid/invalid credentials, email validation, password constraints, and required field checks — were covered and passed. The account creation flow correctly enforces password length and required inputs.

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

6.2 Test Case Execution Summary:



3. *Figure 14: Test Case Execution Results*

Category	Executed	Passed	Failed	Notes
Eligibility Form	14	14	0	All scenarios passed
Product List Interface	11	11	0	Contains mocked data
Login	6	6	0	Fully covered
Create Account	6	6	0	Validations enforced correctly
Total	**37**	**37**	**0**	✔ No blocking defects detected

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

6.3 Overall Assessment:

The system is **ready for release** from a QA standpoint. All verified features are working as expected. Please keep in mind that most of the data is mocked and does not represent the final version.

7. Dev Summary

7.1 Project Setup & Early Foundations

From the very beginning, we made it a point to approach the project with a strong emphasis on scalability, exceptional user experience, robust security, and a seamless onboarding process for future developers. We knew that getting the foundation right would save time and effort down the road, so we focused early efforts on cloning the repository, configuring the environment, reviewing dependencies, and diving into the document allowed us to ramp up quickly, contribute meaningfully, and build with clarity and confidence right from the start.

7.2 Front-End Optimization and Design Consistency

We placed particular importance on improving the front-end, not just from a visual perspective but also in terms of responsiveness, accessibility, and maintainability. Beyoation to understand both the architecture and workflows. This initial groundwork and just making things look nice, we restructured the UI to be more user-friendly and easier to work with. This included enforcing consistent design patterns, improving component reuse, and aligning with modern development standards. These efforts paid off by reducing friction during development and making it easier for designers and developers to stay aligned as the project evolved.

7.3 Improving Developer Experience and Onboarding

At the same time, we worked to improve the internal developer experience by enhancing documentation across the board. We added detailed inline

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

comments, wrote comprehensive setup guides, and collected useful learning resources to make onboarding smoother for future contributors. These efforts aimed to minimize context switching and confusion for new team members, helping them understand the system faster and start delivering value sooner.

7.4 Theming System Overhaul

Another major improvement was the overhaul of the theming system. We reworked it to support clean, efficient light and dark mode toggling, while also eliminating layout inconsistencies and visual bugs that had accumulated over time. Fixing things like button padding, text alignment, and color usage across the app may seem minor individually, but collectively, they created a noticeably more polished and cohesive interface.

7.5 Infrastructure Enhancements and Security

On the infrastructure side, we established a streamlined deployment pipeline using Vercel, and integrated Supabase as our backend platform. While setting this up, we resolved a few early connectivity and configuration issues that were slowing development, ensuring a smoother experience for the whole team. We also introduced password protection on the staging environment to prevent scraping or unwanted access, which provided an immediate security boost with minimal overhead.

7.6 CSC Module and Security Improvements

We gave special attention to the CSC module, which required addressing both technical and business needs. We tested multiple authentication flows, including GitHub OAuth, and added vulnerability scanning via Grype to catch security issues early. This helped us ensure a solid baseline of protection while keeping the user experience frictionless.

7.7 UI Consistency and New Feature Development

As we reviewed the broader application, we noticed visual and behavioral inconsistencies across components—such as spacing irregularities, hover

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

states that didn't match expectations, and inconsistent font scaling. We resolved these through multiple iterative passes, gradually establishing a uniform design language throughout the app. In parallel, we began building out new pages for the upcoming release cycle, translating mockups into production-ready, responsive components that seamlessly fit into the design system and tech stack.

7.8 Compliance Features for Security Standards

To strengthen the app's security posture, we added the OSCRAT module and rolled out the CRA Eligibility Form, both of which help users assess their own compliance with current EU cybersecurity requirements. These additions were not only valuable for end users, but also aligned the app with broader legal and regulatory frameworks, reducing future risk.

7.9 Product Pages and Information Architecture

On the product side, we developed the Product Listing and Product Details pages, giving users a clean, intuitive, and filterable way to explore offerings. All the relevant product details were centralized in one place, improving both usability and information architecture.

7.10 Technical Debt and Design Alignment

We also carved out time to address technical debt. This included updating outdated dependencies, applying critical security patches, and ensuring compatibility with the latest tools, frameworks, and build systems. Mockups played a crucial role here, serving as a visual source of truth that helped keep development and design in lockstep even as we moved quickly.

7.11 Re-Architecting Client-Side Logic

As we planned for future scalability, we took a step back and decided to re-architect the way the client-side logic interacted with the backend. We audited the existing implementation and identified areas where improper backend calls and inconsistent state management were leading to brittle, error-prone code. In some cases, temporary workarounds had been added

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

that tried to resolve issues caused by poor state flow, but these only added complexity and made the system harder to reason about.

7.12 Standardizing API Interaction with React Query

To address this, we standardized around a proven, scalable approach using React Query for both data fetching and state management. This gave us a consistent way to handle caching, background refetching, invalidation, and mutation logic across the entire app, significantly reducing code duplication and bugs.

We followed up by defining standardized API endpoints and creating a set of reusable hooks that introduced strong separation between the transport layer, business logic, and UI components. This not only improved testability, but also made the codebase far more modular and predictable.

To support this new architecture, we created a shared library for handling API interactions and error handling. This ensured that both server-side and client-side errors were caught and managed in a uniform way, and that serialization and deserialization of payloads were handled correctly every time.

7.13 Migration and Codebase Cleanup

Once we had confidence in the new structure, we migrated existing API calls to align with it, refactored components accordingly, and cleaned up obsolete logic and temporary workarounds. The result was a far cleaner, more maintainable codebase that's easier to work with and significantly more robust.

7.14 . Positioning for Future Growth

With all these improvements in place, the platform is now in an excellent position for future growth. We've laid a solid technical foundation, reduced complexity, eliminated redundancies, and improved the architecture in a way that will make it easier to extend with new features, pages, and APIs. We expect to see performance improvements, such as faster load times and

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

reduced re-renders, along with improved stability and a better overall developer experience.

8. Figma links

iii. 8.1 CRA Form:

https://www.figma.com/design/wHd4c4kYUYk6MCwL3OMHr8/OSCRAT?node-id=105-1811&t=UNhFzGQ1y40nyPjv-1

iv. 8.2 Dashboard:

https://www.figma.com/design/wHd4c4kYUYk6MCwL3OMHr8/OSCRAT?node-id=260-4857&t=UNhFzGQ1y40nyPjv-1

v. 8.3 User Tasks:

https://www.figma.com/design/wHd4c4kYUYk6MCwL3OMHr8/OSCRAT?node-id=395-29152&t=UNhFzGQ1y40nyPjv-1

vi. 8.4 Organisation Management:

https://www.figma.com/design/wHd4c4kYUYk6MCwL3OMHr8/OSCRAT?node-id=393-25111&t=UNhFzGQ1y40nyPjv-1

vii. 8.5 Prototype presented at TPM Berlin

https://www.figma.com/proto/wHd4c4kYUYk6MCwL3OMHr8/OSCRAT?page-id=117%3A11386&node-id=469-34886&p=f&viewport=208%2C601%2C0.09&t=svXW8Bi5kbuLSLVk-1&scaling=min-zoom&content-scaling=fixed&starting-point-node-id=469%3A34886

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 – Testing Report M6

OSCRAT

Open-Source Cyber Resilience Act Tools