DerScanner 11

Release Notes

New capabilities

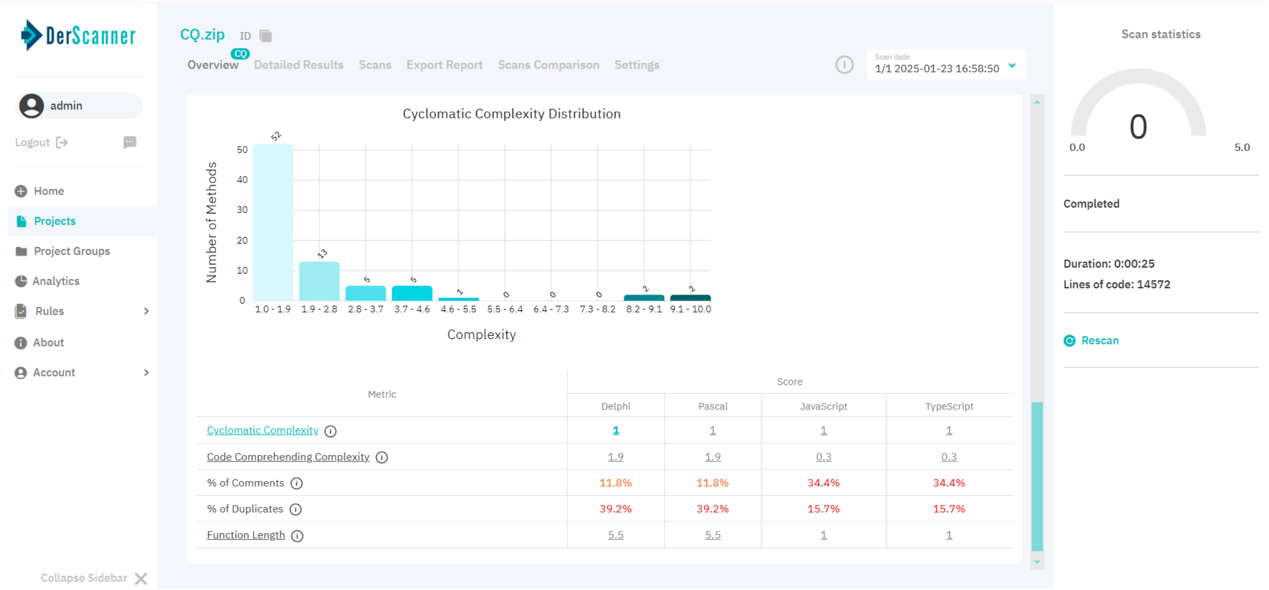
Static Code Quality Analysis

Why it's important

Writing clean, maintainable code is essential for creating secure, reliable, and long-lasting applications. Yet, legacy code, poor practices, and overly complex structures can add unnecessary confusion, increase technical debt, and slow down development. The new Code Quality Analysis in DerScanner addresses these challenges head-on. With nearly **100 new rules,** this feature helps developers spot and fix issues early, improving readability, reducing future maintenance costs, and minimizing errors. By building on industry best practices, Code Quality Analysis ensures your projects are not just functional but also future-proof and easier to manage.

How it works

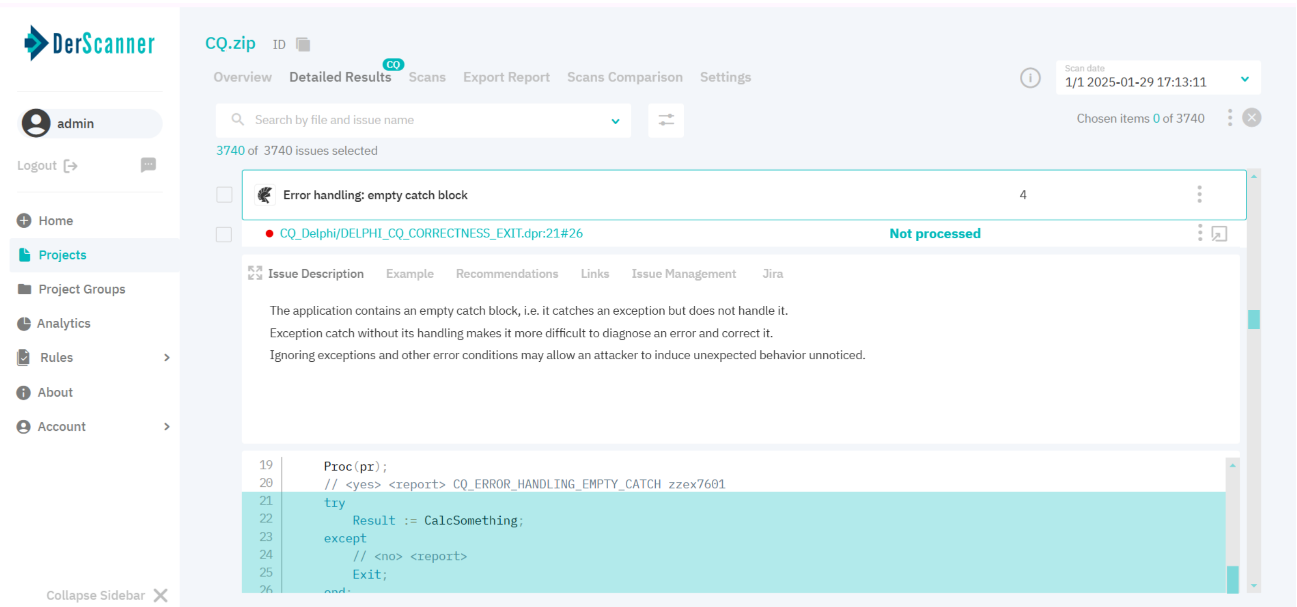
Code Quality Analysis is integrated directly into DerScanner and supports applications written in **JavaScript/TypeScript/TSX**, as well as **Delphi/Pascal**. It highlights legacy code, poor practices, duplicate sections, and overly complex functions or methods. The feature works by applying advanced static rules to detect structural and conceptual inconsistencies in your code. It can be launched alongside standard static analysis for seamless integration or used independently for targeted quality checks.



Metric	Score			
	Delphi	Pascal	JavaScript	TypeScript
Cyclomatic Complexity ⓘ	1	1	1	1
Code Comprehending Complexity ⓘ	1.9	1.9	0.3	0.3
% of Comments ⓘ	11.8%	11.8%	34.4%	34.4%
% of Duplicates ⓘ	39.2%	39.2%	15.7%	15.7%
Function Length ⓘ	5.5	5.5	1	1

Completed

Duration: 0:00:25
Lines of code: 14572



Scan date: 1/1 2025-01-29 17:13:11

Chosen items 0 of 3740

3740 of 3740 issues selected

Error handling: empty catch block 4

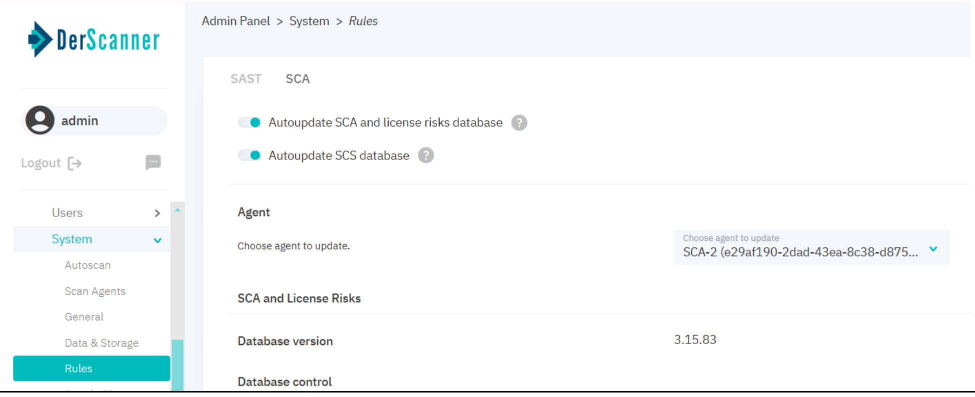
CQ_Delphi/DELPHI_CQ_CORRECTNESS_EXIT.dpr:21#26 Not processed

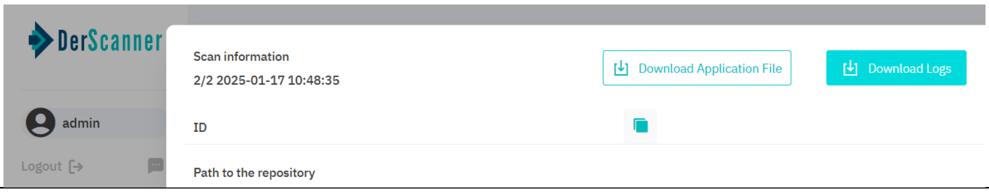
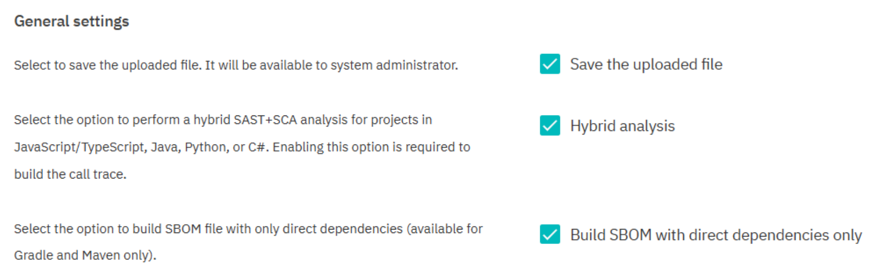
The application contains an empty catch block, i.e. it catches an exception but does not handle it.
Exception catch without its handling makes it more difficult to diagnose an error and correct it.
Ignoring exceptions and other error conditions may allow an attacker to induce unexpected behavior unnoticed.

```
    Proc(pr);
    // <yes> <report> CQ_ERROR_HANDLING_EMPTY_CATCH zzex7601
    try
        Result := CalcSomething;
    except
        // <no> <report>
        Exit;
    end;
```

Significant Update to Software Composition Analysis

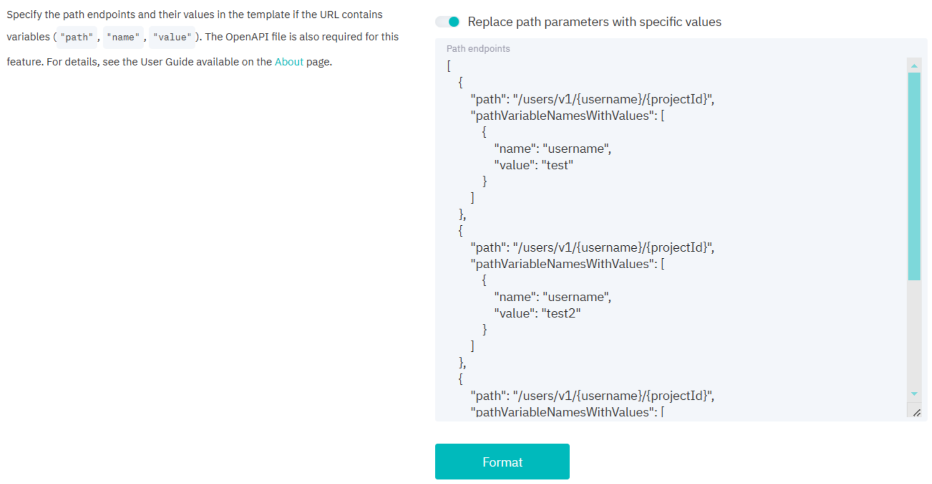
We've made major enhancements to our Software Composition Analysis (SCA) to deliver a faster, more accurate, and user-friendly experience.

Capability	Why it's important and how it works
Real-Time Vulnerability Updates	Our vulnerability databases for SCA and SCS now update every 1-2 hours, ensuring you never miss dangerous new threats. This consistent update cycle keeps your projects protected against emerging vulnerabilities. *For air-gapped installations, manual updates are possible.*  Admin Panel > System > Rules SAST SCA ● Autoupdate SCA and license risks database ● Autoupdate SCS database Agent Choose agent to update. Choose agent to update: SCA-2 (e29af190-2dad-43ea-8c38-d875... SCA and License Risks Database version 3.15.83 Database control
Improved Hybrid Analysis	Enhancements provide more accurate detection of vulnerable functions or imports, reducing the chance of missed issues in hybrid analysis.
Faster & Efficient Dependency Mapping	With improved graph construction algorithms, drawing dependency graphs is now significantly faster and places minimal load on your device, enhancing the interface's responsiveness. Optimized algorithms for library import tracing have reduced overall scan times, enabling quicker results.

Enhanced Logging and Diagnostics	Detailed scan logs can now be stored and uploaded separately, offering a clear view of any issues. This feature simplifies troubleshooting and improves overall reliability.  DerScanner admin Logout Download Application File Download Logs Scan information 2/2 2025-01-17 10:48:35 ID Path to the repository
Speed Optimization	The ability to disable hybrid SCA+SAST analysis provides an enormous boost to scanning speed, especially for projects with extensive dependencies. This option can cut scan times for large projects by hours.  General settings Select to save the uploaded file. It will be available to system administrator. ☑ Save the uploaded file Select the option to perform a hybrid SAST+SCA analysis for projects in JavaScript/TypeScript, Java, Python, or C#. Enabling this option is required to build the call trace. ☑ Hybrid analysis Select the option to build SBOM file with only direct dependencies (available for Gradle and Maven only). ☑ Build SBOM with direct dependencies only
Bug Fixes and Accuracy Improvements	We've resolved issues like duplicate library imports, incorrect vulnerability triggers, and errors in library version comparisons to ensure more precise results. Addressed bugs in graph construction across multiple languages, reducing errors when working on multilingual projects.
Direct Dependency Collection for JAVA Projects	This new feature addresses challenges faced during the analysis of Java projects with dependencies from private repositories or when access to public repositories is restricted. By enabling the collection of direct dependencies directly from project files, it ensures that even in environments with limited repository access, thorough and accurate analysis can still be performed.

Dynamic Application Security Testing

Capability	Why it's important and how it works
URL Variable Scanning	The new URL Variable Scanning functionality significantly enhances test coverage. By allowing multiple URL combinations to be analyzed in a single run, it ensures a thorough and comprehensive evaluation of various endpoint scenarios, uncovering potential issues that might have been previously overlooked. With this feature, users can specify endpoints and their variable values directly in the analysis settings. By providing an OpenAPI file, the system can accurately map and test the specified combinations, delivering detailed results and boosting overall testing efficiency.

	 Specify the path endpoints and their values in the template if the URL contains variables ("path" , "name" , "value"). The OpenAPI file is also required for this feature. For details, see the User Guide available on the About page. ● Replace path parameters with specific values Path endpoints Format
NTLM Authorization Support	The addition of NTLM Authorization Support enhances security and compatibility for environments that rely on NTLM authentication. This ensures seamless interaction with systems and resources protected by NTLM, providing users with a more reliable and secure experience.

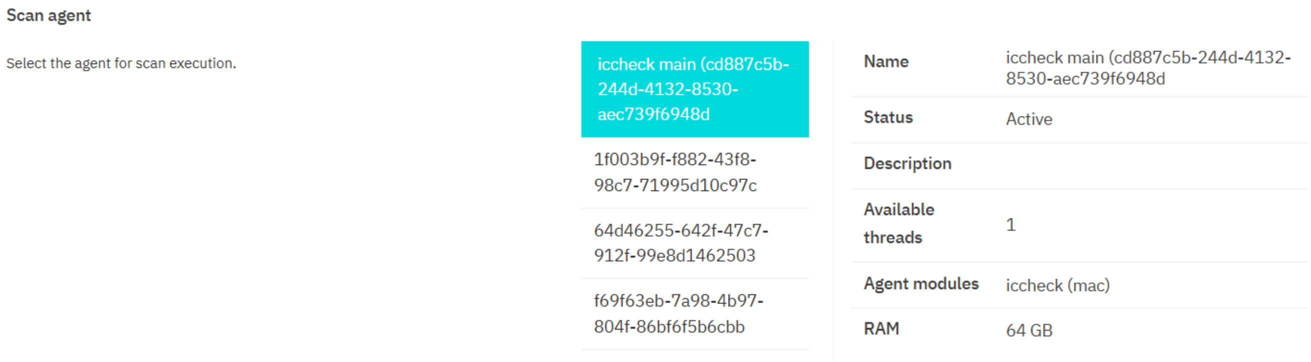
```
[
  {
    "path": "/users/v1/{username}/{projectId}",
    "pathVariableNamesWithValues": [
      {
        "name": "username",
        "value": "test"
      }
    ]
  },
  {
    "path": "/users/v1/{username}/{projectId}",
    "pathVariableNamesWithValues": [
      {
        "name": "username",
        "value": "test2"
      }
    ]
  },
  {
    "path": "/users/v1/{username}/{projectId}",
    "pathVariableNamesWithValues": [
```

Enhancements

- ## Vulnerability detection rules:
  - Significant improve taint analysis for **Delphi**.
  - Enhanced coverage of the **FireMonkey** framework for Delphi.
  - Improved data flow analysis for **Go**.
  - Updated helpful links for 500+ rules.
  - Added over **300** new vulnerability and code quality patterns for **C#, Delphi/Pascal, JavaScript, TypeScript, Perl, PHP and Python**.

- ## Analysis Modules:
  - Enhanced analysis speed, and optimized memory consumption, particularly noticeable on large projects.
  - Significantly sped up the preprocessing of JavaScript files.
  - Improved the logic for taint analysis patterns, specifically flag management when multiple patterns trigger at the same location in the code.
  - Improved handling of **.asp** files for VBScript.

- ## User Interface:
  - Introducing **scan agent** management. This feature enhances transparency and flexibility in resource management, for instance, for heavyweight Java projects.
    The list of agents resides in the analysis settings. Click on an agent to get detailed information about its status, workload, and supported technologies. Your choice can be saved for consecutive scans to make sure that your projects always get matched with the right resources.



Scan agent

Select the agent for scan execution.

iccheck main (cd887c5b-244d-4132-8530-aec739f6948d

1f003b9f-f882-43f8-98c7-71995d10c97c

64d46255-642f-47c7-912f-99e8d1462503

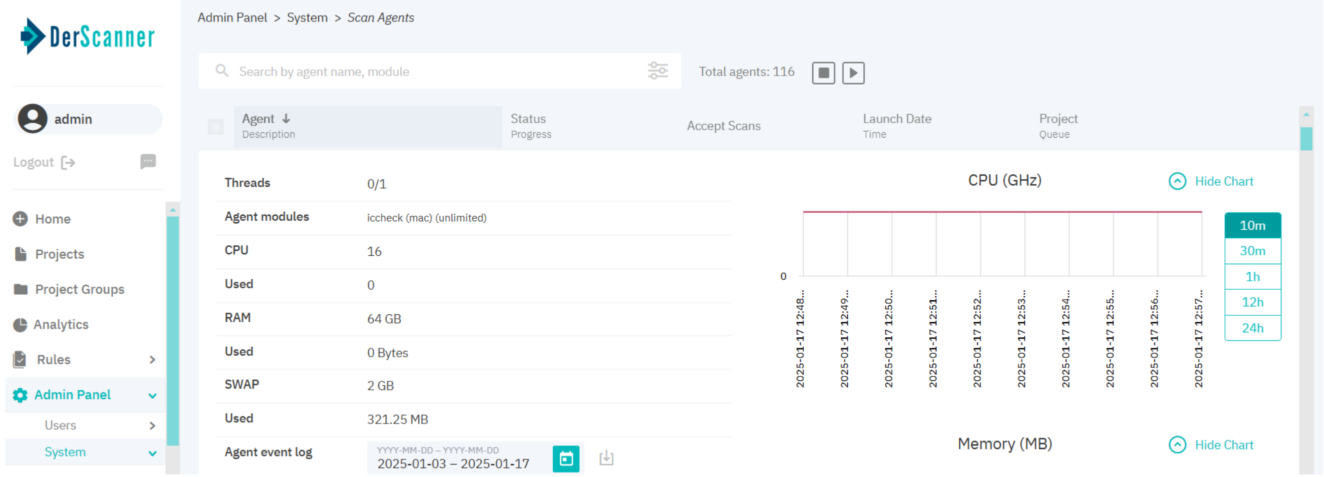
f69f63eb-7a98-4b97-804f-86bf6f5b6cbb

Name	iccheck main (cd887c5b-244d-4132-8530-aec739f6948d
Status	Active
Description	
Available threads	1
Agent modules	iccheck (mac)
RAM	64 GB

- A quality of life update for **expired licenses**. The results of your completed scans will now remain available for view permanently.

Administration:

- A new **Scan Agents** tab has been added to the Admin Panel. It's home to all agents as well as management tools. Each agent includes info about its technical specifications, workload data, and historical usage data: with graphs and logs.
  Manage analysis threads and memory allocation to facilitate scanning of chunky projects. If needed, agents can also de disabled from here.



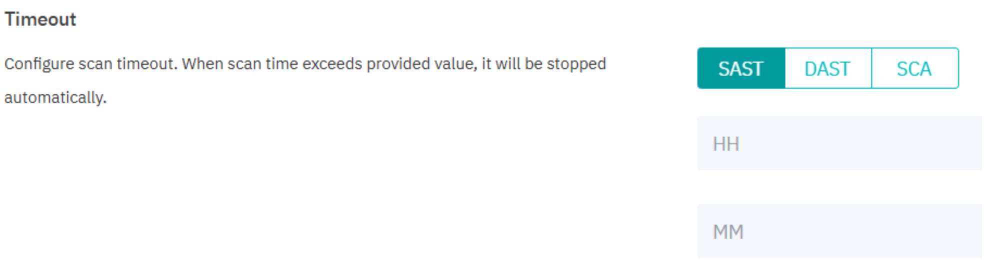
Admin Panel > System > *Scan Agents*

Total agents: 116

Agent / Description	Status / Progress	Accept Scans	Launch Date / Time	Project / Queue

Threads	0/1
Agent modules	iccheck (mac) (unlimited)
CPU	16
Used	0
RAM	64 GB
Used	0 Bytes
SWAP	2 GB
Used	321.25 MB
Agent event log	YYYY-MM-DD – YYYY-MM-DD 2025-01-03 – 2025-01-17

- Added **scan timeout** configuration for every analysis type. This, too, will be helpful in scan queue management.



Timeout

Configure scan timeout. When scan time exceeds provided value, it will be stopped automatically.

SAST | DAST | SCA

HH

MM

Deployment:

- Time to say bye! to the **ENV** module. This change enables support for more Linux distributions, and simplifies the system installation and update process.

- ## User Interface:
  - **Report**:
    - Made adjustments to our **SARIF** report format for compatibility with earlier versions of Defect Dojo.