



QAOps-Based Quality Automation (Static analysis • Unit • API • Perf • Security)

QAOps Implementation & Results

VIRNECT QA Team

Sungtae Kim

I. Project Overview

Purpose

- Establish a test automation pipeline and standardize code quality measurement to systematically ensure overall project quality.
- Enhance collaboration efficiency between development and QA teams by integrating Agile and CI/CD processes.
- Centralize multi-stack environments (Frontend, Backend, Unity C#) into a single SonarQube dashboard for unified quality visualization.
- Strengthen release stability by implementing a continuous regression testing framework and fostering a team-wide quality culture.
- Conduct Postman-based API functional testing to validate backend API behavior and data integrity.
- Perform JMeter-based performance testing and OWASP ZAP-based security testing to proactively verify not only functional quality but also non-functional quality aspects such as performance and security.

Goals

1. Build a Static Analysis Environment for Automated Test Code
 - Integrate SonarQube into the Jenkins pipeline to identify code smells, bugs, and security vulnerabilities at an early stage.
2. Secure and Visualize Test Coverage
 - Use tools such as Jest, JaCoCo, and Istanbul to measure Statement, Branch, and Line coverage with automated reporting.
3. Enforce CI/CD Quality Gates
 - Apply merge-blocking policies on pull requests when quality gate conditions are not met to mitigate risks in advance.
4. Strengthen Development-QA Collaboration
 - Share test and quality reports in real time through Jenkins, Slack, and GitHub to facilitate Agile team collaboration.
5. Reduce Code Duplication and Promote Modular Refactoring
 - Lower duplication rates and introduce common modules to reduce maintenance costs and improve development productivity.
6. Implement Unified Quality Management Across Multi-Stack Projects
 - Standardize overall project quality metrics by managing Java, TypeScript, and C# codebases on a single platform.

I. Project Overview

Goals

7. Establish a Postman-Based API Testing Framework

- Validate request/response behavior, status codes, and data consistency through unit-level and scenario-based API tests.
- Improve regression stability by automating repeated test executions and maintaining structured test reports.

8. Establish a JMeter-Based Performance Testing Framework

- Execute load and concurrency tests on login flows, core APIs, and critical user scenarios to verify TPS, response time, and system stability.
- Manage performance test results as quantitative metrics to define clear release criteria.

9. Conduct OWASP ZAP-Based Security Testing

- Perform vulnerability scans on web and API endpoints to proactively identify security risks based on the OWASP Top 10.
- Document security test results to systematically track remediation actions and maintain security test history.

I. Project Overview

Schedule

No.	Schedule	Category	Key Tasks	Responsible Person		Remarks
1	Monday, April 14, 2025	Configuration & Integration	<ul style="list-style-type: none">Configure advanced quality gates and rules per tech stack (Java, TS, C#).Implement branch coverage thresholds in CI.Automate Slack and GitHub PR notifications for quality gate results.	VIRNECT Co., Ltd. QA Team	Kim Sung-tae, Senior Engineer	
2	Tuesday, May 13, 2025	Test Coverage Expansion	<ul style="list-style-type: none">Expand unit test coverage with Jest, JUnit, and Istanbul.Identify and address coverage blind spots.Create coverage heatmap dashboards in SonarQube.	VIRNECT Co., Ltd. QA Team	Kim Sung-tae, Senior Engineer	Target coverage ≥80% (backend)
3	Monday, June 16, 2025	Automation & Optimization	<ul style="list-style-type: none">Optimize Jenkins pipeline parallelization for faster builds.Integrate caching mechanisms for test runs.Refactor repetitive modules to reduce duplication.	VIRNECT Co., Ltd. QA Team	Kim Sung-tae, Senior Engineer	
4	Monday, July 14, 2025	Security & Vulnerability	<ul style="list-style-type: none">Enable SonarQube security hotspot analysis.Conduct vulnerability scanning and remediation.Establish monthly security quality gate reviews.	VIRNECT Co., Ltd. QA Team	Kim Sung-tae, Senior Engineer	
5	Monday, August 11, 2025	Stabilization & Reporting	<ul style="list-style-type: none">Finalize dashboards for CI/CD & QA metrics.Automate quarterly test coverage & quality trend reports.Conduct knowledge-sharing sessions across teams.	VIRNECT Co., Ltd. QA Team	Kim Sung-tae, Senior Engineer	Quarterly summary planned

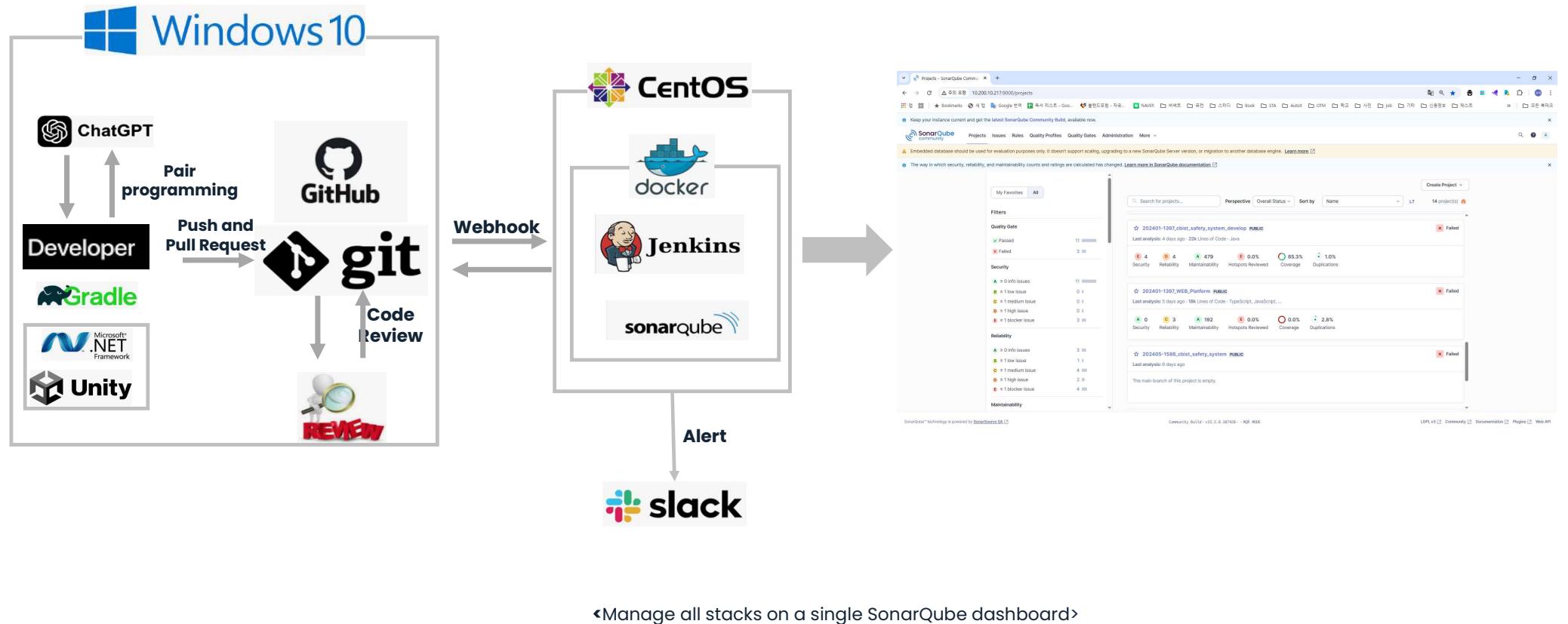
I. Project Overview

Schedule

No.	Schedule	Category	Key Tasks	Responsible Person	Remarks
6	August 26, 2025 (Tuesday)	Performance Test Planning	<ul style="list-style-type: none">Design JMeter-based performance test scenarios.Establish load and concurrency test plans for key APIs and critical user flows.Define performance metrics such as TPS, response time, and error rate.	VIRNECT Co., Ltd. QA Team	Kim Sung-tae, Senior Engineer
7	August 29, 2025 (Friday)	Performance Testing (Internal)	<ul style="list-style-type: none">Execute internal performance tests using JMeter.Analyze test results and identify system bottlenecks.Document performance test results and derive improvement actions.	VIRNECT Co., Ltd. QA Team	Kim Sung-tae, Senior Engineer
8	December 1, 2025 (Monday)	Final Performance Testing	<ul style="list-style-type: none">Execute final performance tests on the system with applied improvements.Verify whether target performance metrics (TPS, response time, stability) are satisfied.Prepare the final performance test report and assess release readiness.	VIRNECT Co., Ltd. QA Team	Kim Sung-tae, Senior Engineer
9	December 8, 2025 (Monday) - December 12, 2025 (Friday)	API Integration Testing	<ul style="list-style-type: none">Execute API integration tests for Platform and Admin APIs.Validate authentication, request/response, and integration flows.Identify defects and document test results for release readiness.	VIRNECT Co., Ltd. QA Team	Kim Sung-tae, Senior Engineer
10	December 12, 2025 (Friday) - December 19, 2025 (Tuesday)	ZAP Security Testing	<ul style="list-style-type: none">Define security test scope for Platform/Admin APIs & key web pages (target URLs, environments, exclusions, test accounts).Configure OWASP ZAP (Context/Authentication, session handling, headers/tokens) and run Spider/AJAX Spider to discover endpoints.Execute Automated Scan (Passive Scan + Active Scan) to detect common vulnerabilities (XSS, SQLi, auth/authorization issues, misconfigurations).Analyze and triage findings (severity/impact, false positives), document results, and re-test critical fixes before release readiness.	VIRNECT Co., Ltd. QA Team	Kim Sung-tae, Senior Engineer

I. Project Overview

Building an Integrated Quality Management Pipeline (Java + TS + C#)



I. Project Overview

1. SonarQube Static Analysis Status – Frontend (TypeScript)

- **Language / Environment**

- TypeScript (Web Frontend)

- **Analysis Metrics**

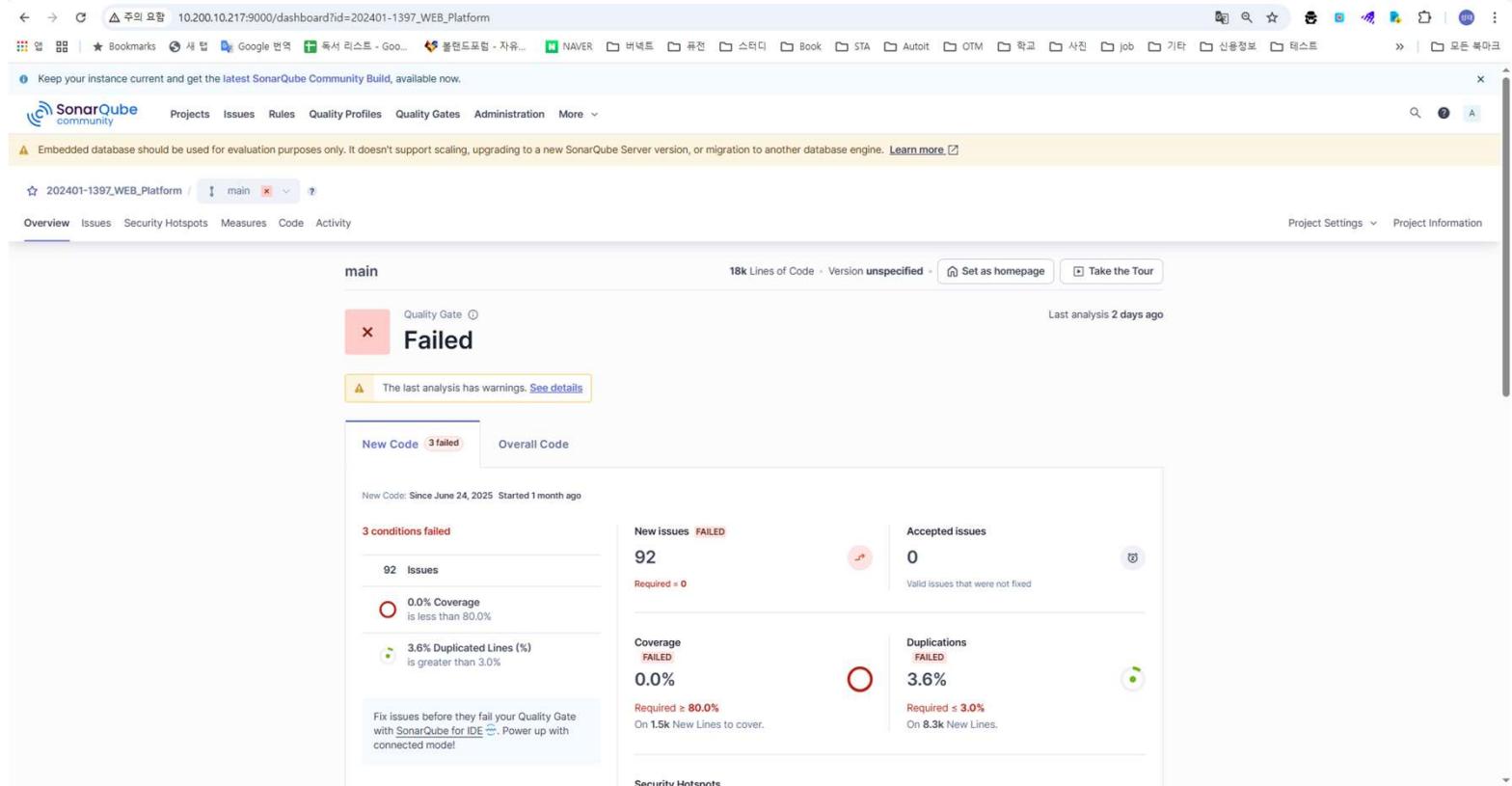
- Coverage: 0.0% (Needs collection/integration)
- New issues: 92
- Duplication: 3.6% (Exceeds threshold of $\leq 3.0\%$)
- Quality Gate: X Failed (3 conditions failed)
- Last analysis: 2 days ago

- **Key Points**

- Current coverage not collected
→ Plan to integrate with Jest lcov.
- Code duplication and new issues are the main reasons for Quality Gate failure.

- **Role**

- Build SonarQube environment & integrate with CI pipeline.
- Configure language-specific rules and Quality Gate settings.
- Visualize and manage coverage, issues, and code duplication.



I. Project Overview

2. SonarQube Static Analysis Status – Backend (Java)

• Language / Environment

- Java (Spring Boot)
- Gradle + JUnit + JaCoCo

• Analysis Metrics

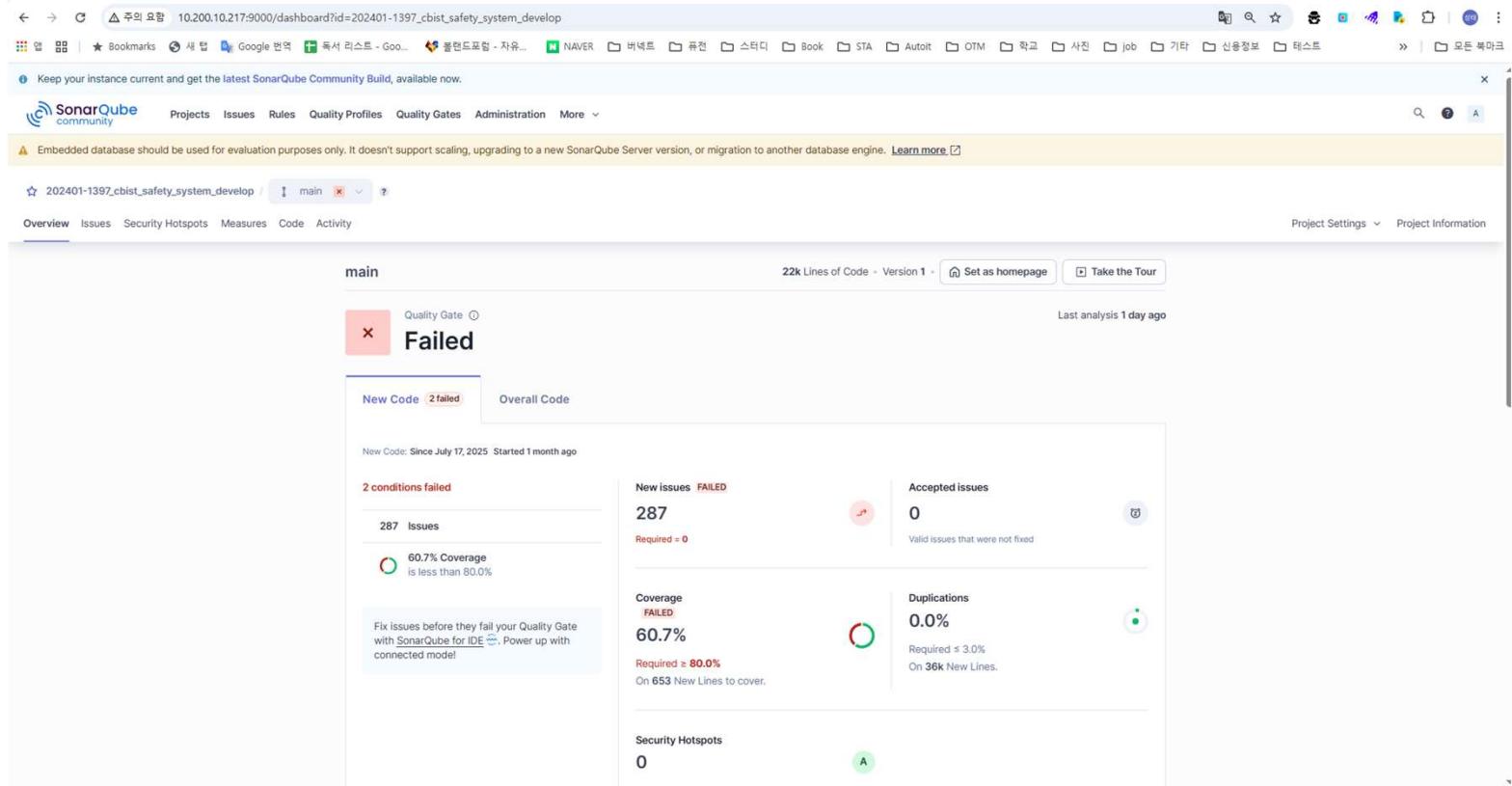
- Coverage: 60.7% (Target ≥ 80%)
- New issues: 287
- Duplication: 0.0%
- Quality Gate: X Failed (2 conditions failed)
- Last analysis: 1 day ago

• Key Points

- Coverage collection enabled through JaCoCo integration.
- Coverage has been collected but does not meet the target.
- A large number of new issues are the main reason for Quality Gate failure.

• Role

- Build SonarQube environment & integrate with CI pipeline.
- Configure quality rules and Quality Gate settings per language.
- Visualize and manage coverage, issues, and code duplication.



I. Project Overview

3. SonarQube Static Analysis Status – Unity (C#)

- **Language / Environment**

- C# (Unity WebGL)

- **Analysis Metrics**

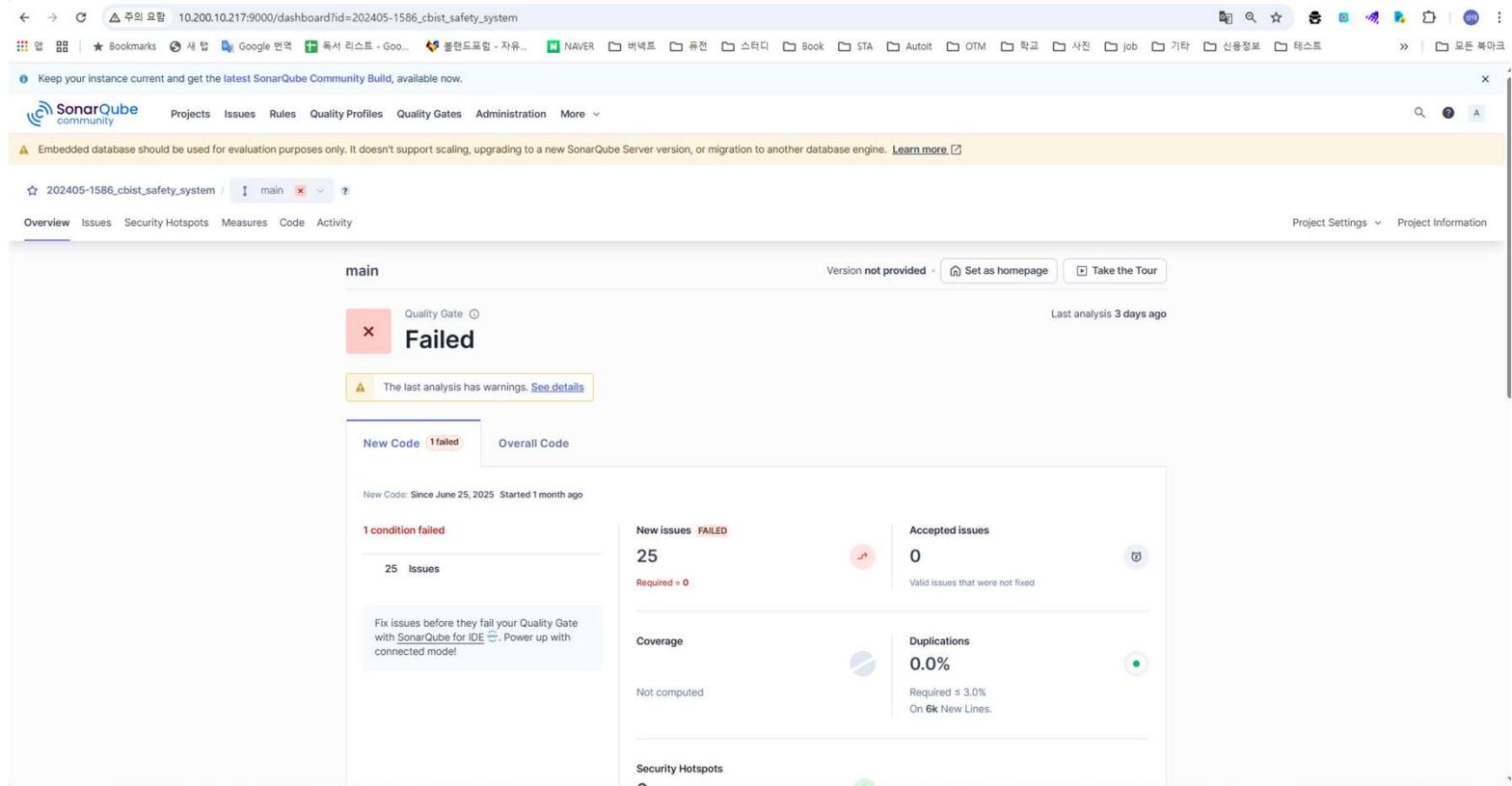
- Coverage: Not computed (Unable to collect)
- New issues: 25
- Duplication: 0.0%
- Quality Gate: X Failed (1 condition failed)
- Last analysis: 3 days ago

- **Key Points**

- Unity project also managed under SonarQube.
- Environment makes coverage collection difficult (Test framework not integrated).
- 25 new issues caused Quality Gate failure.

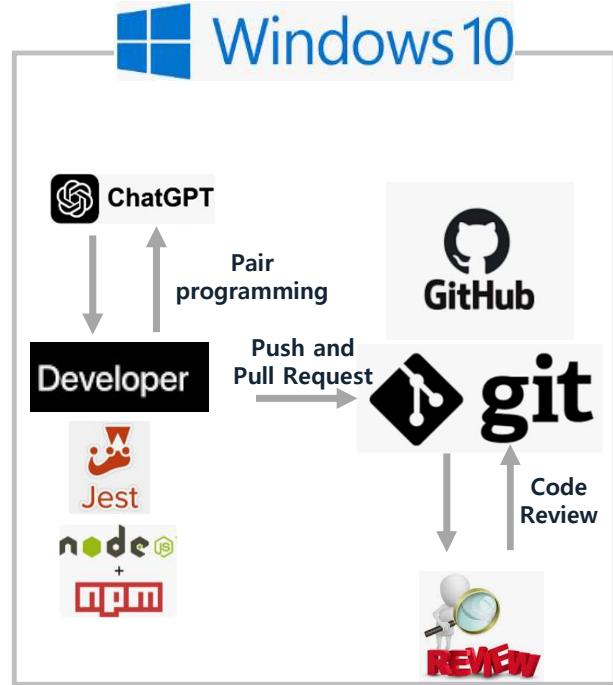
- **Role**

- Build SonarQube environment & integrate with CI pipeline.
- Configure quality rules and Quality Gate settings per language.
- Visualize and manage coverage, issues, and code duplication.



I. Project Overview

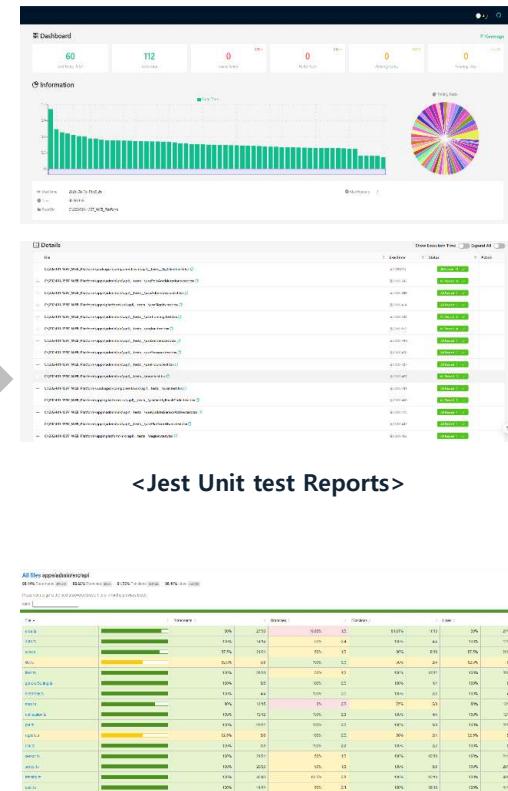
4. Unit Test Automation Pipeline – Frontend (TypeScript)



Webhook

Alert

<GitHub → Jenkins → Jest → Slack>



<Jest Unit test Coverage>

I. Project Overview

5. Frontend (TypeScript) – Test Execution Results & Coverage

• QA Environment

- Node.js / pnpm-based Frontend Monorepo environment
- CI Environment: Automated tests executed via Jenkins

• Technologies Used

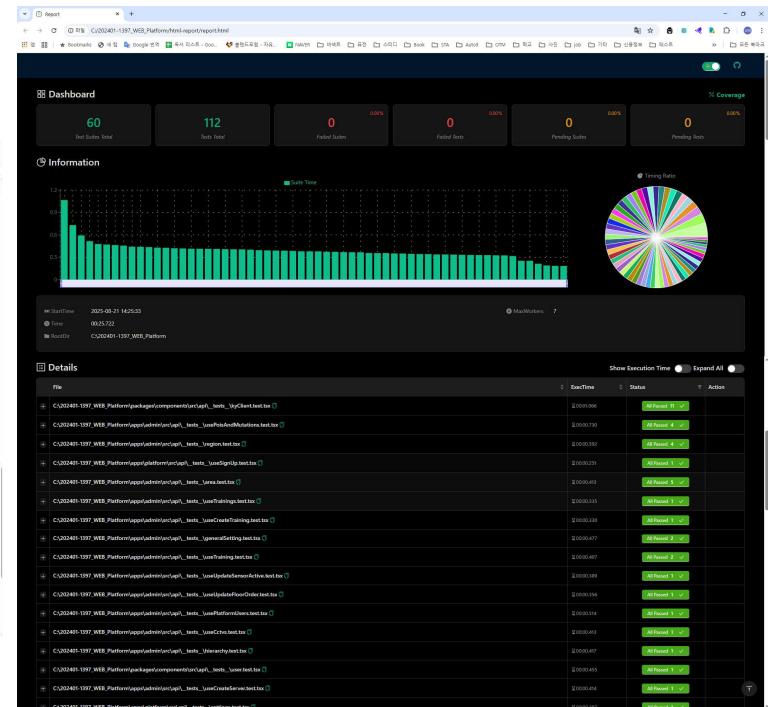
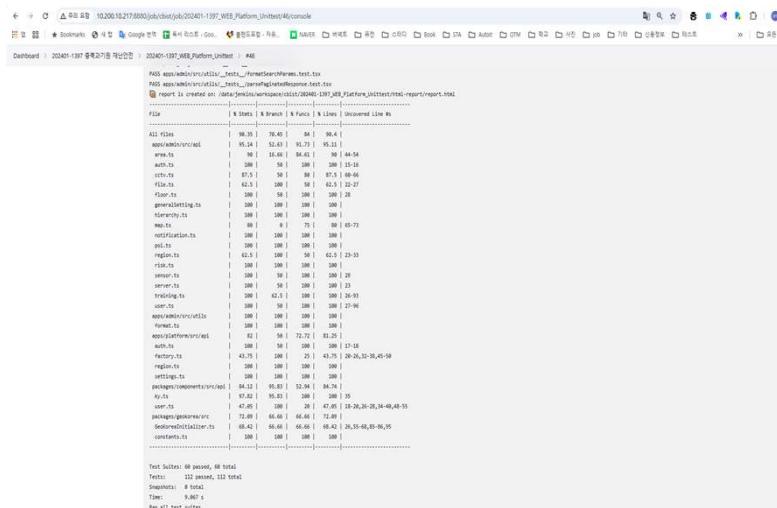
- TypeScript-based module-level unit testing
- React Query / Hooks / API unit-level validation

• Tools Used

- Jest (Test framework)
- Jenkins (Test automation and execution history management)
- HTML Report (Visualization of execution time and duration by module)

• Achievements

- Test Suites: 60 / Tests: 112 → 100% passed (All tests passed)
- Visualized execution time and per-module duration of tests
- Automatically reflected results in Jenkins pipeline → Strengthened regression test reliability



<Jenkins Log · Jest HTML Report · Coverage>

I. Project Overview

6. Run the Docker Compose file

- **QA Environment**

- Unit tests applied per business domain based on TypeScript/React.

- **Technologies Used**

- Measure Statement, Branch, Function, and Line Coverage per feature.

- **Tools Used**

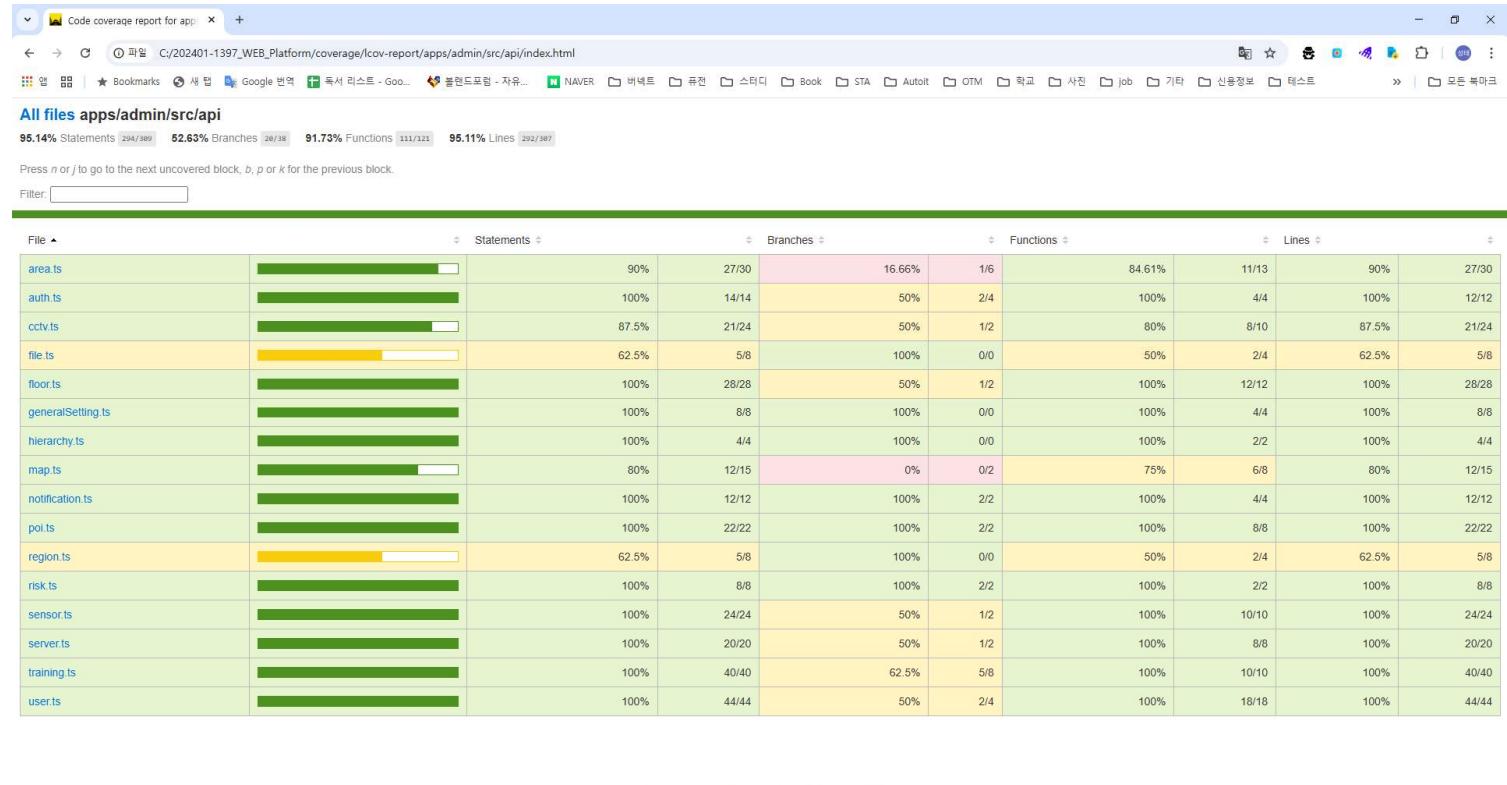
- Jest + Istanbul (Coverage collection)
- HTML Coverage Report (Visualize coverage by file)

- **Achievements**

- Achieved 96%+ average Statement coverage overall.
- Achieved 100% Line coverage for most critical business files.
- Identified low Branch coverage (conditional logic) areas.
- Able to visually track per-feature coverage differences for risk management.

- **Role**

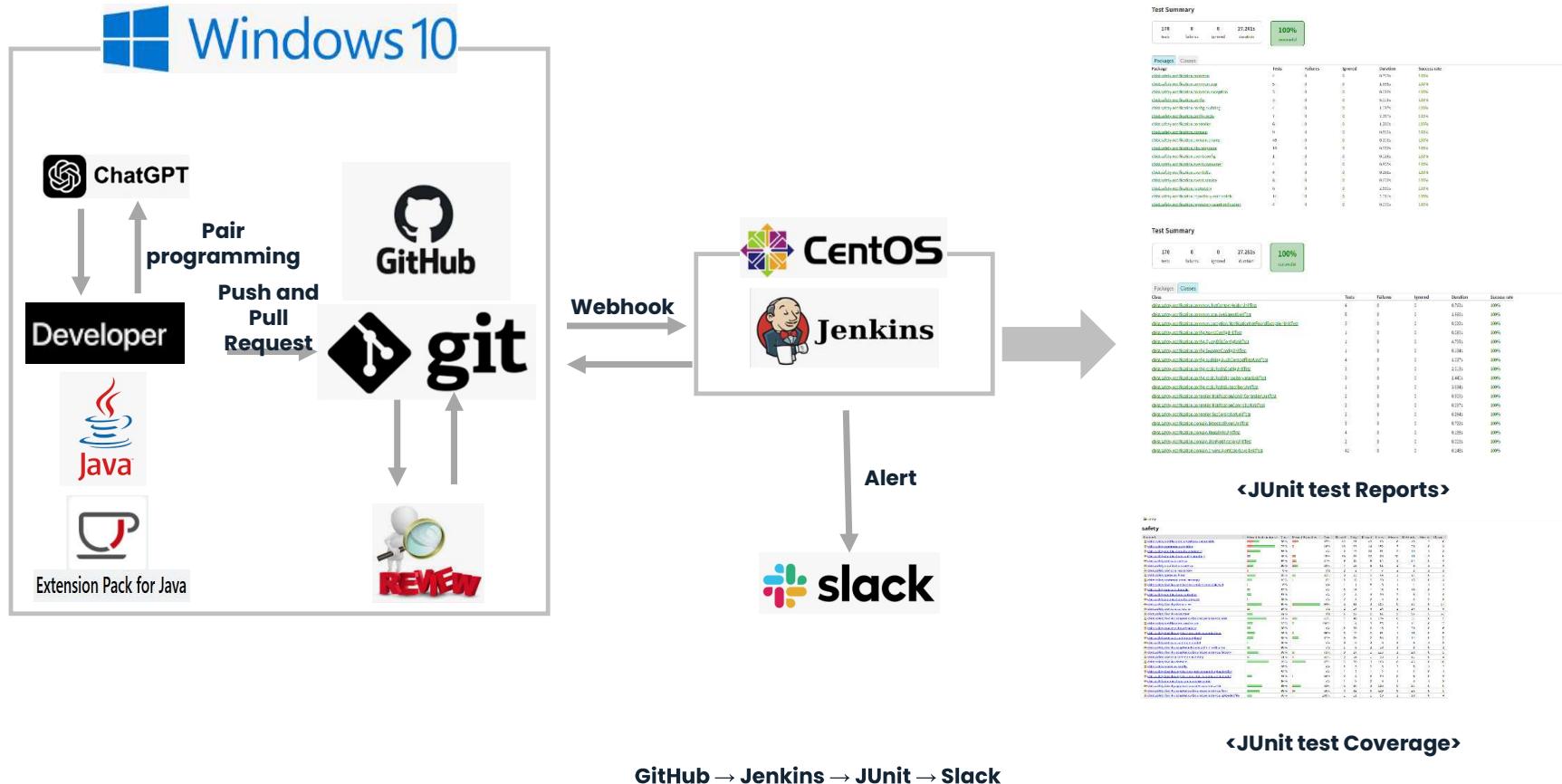
- Standardized frontend test code writing practices.
- Built Jenkins Job & Slack notification automation pipeline.



«Jenkins 로그 · Jest HTML Report · Coverage»

I. Project Overview

7. Unit Test Automation Pipeline – Backend (Java)



GitHub → Jenkins → JUnit → Slack

I. Project Overview

8. Backend (Java) – Test Execution Results & Coverage

• QA Environment

- Spring Boot-based modular architecture
- Automated test execution in a Jenkins-based CI environment

• Technologies Used

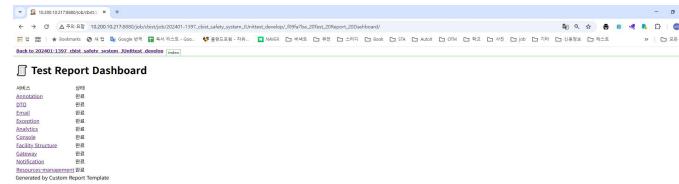
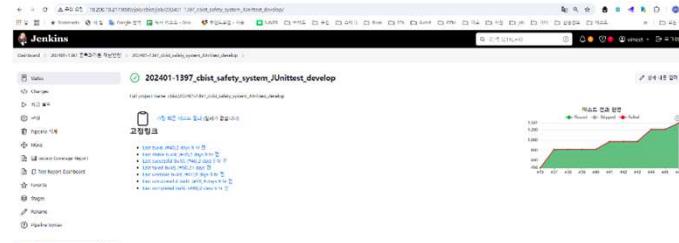
- Java + JUnit-based unit testing
- Verification at Domain / Application / Adapter layer levels

• Tools Used

- JUnit Report Dashboard
- Jenkins Test Trend (Graph & History)
- Gradle-based automated report generation

• Achievements

- Recent builds: 1,341 tests executed, 100% success rate
- Established a module-level test execution status dashboard
- Built a foundation for regression test automation and continuous expansion



◀ Jenkins Trend · JUnit Report · JaCoCo Coverage ▶

I. Project Overview

9. Verify that SonarQube is installed in Docker

• QA Environment

- Spring Boot-based modular architecture
- Automated test execution in a Jenkins-based CI environment

• Technologies Used

- Measure Statement, Branch, Line Coverage using JaCoCo
- Detailed coverage tracking per module and detection of uncovered lines

• Tools Used

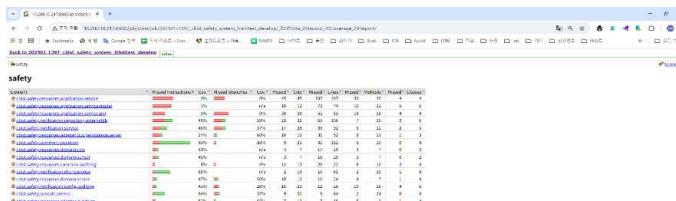
- JaCoCo Coverage Report
- Jenkins Coverage Integrated View
- Gradle automated report generation scripts

• Achievements

- Achieved 60%+ average Statement coverage overall
- Achieved 90%+ coverage for core business modules
- Identified coverage blind spots for future improvement

• Role

- Designed and implemented backend service unit test cases
- Configured JaCoCo-based coverage collection and automated reports



<Jenkins Trend · JUnit Report · JaCoCo Coverage>

I. Project Overview

10. API(Application Programming Interface) Testing

- RESTful API integration testing

Swagger UI

Select a definition console-service

Console Swagger 1.0.0 OAS 3.1

/docs/console/api/v2/api-docs

Console 관련 API Documentation

Servers / Authorize

Platform-settings API Platform-settings

GET /platform-settings Platform setting 관리

Schemas

ConfigKeyValue > Expand all object

DataResponsePlatformSettingsResponse > Expand all object

PlatformSettingsResponse > Expand all object

Authorize

- RESTful API integration testing

Swagger UI

Select a definition console-service-admin

Console Swagger 1.0.0 OAS 3.1

/docs/console/admin-api/v2/api-docs

Console 관련 API Documentation

Servers / Authorize

Design API 플랫폼 디자인을 관리하는 API입니다.

PATCH /admin/design/platform-name Design platform name 수정

PATCH /admin/design/logo Design logo 수정

PATCH /admin/design/favicon Design favicon 수정

GET /admin/design Design 정보 조회

DELETE /admin/design/design Design favicon, logoUrl 삭제합니다.

Menu API Menu를 관리하는 API입니다.

GET /admin/menu Menu 조회

Authorize

I. Project Overview

10. API(Application Programming Interface) Testing

- RESTful API integration testing

Facility Structure API v1 OAS 3.1

Region, Factory, Area 관리 API 문서

Servers: / Authorize

Factory 사용자 플랫폼 공정 조회 API

- GET /regions/{regionId}/factories 지역별 Factory 목록 조회
- GET /factories 전체 활성화 공장 목록 조회
- GET /factories/map 공장 위치 정보 목록 조회

Region 사용자 플랫폼 지역 조회 API

- GET /regions 지역 목록 조회

File 파일 다운로드 API

- GET /facilities/files/{contentFileId}/download-url Presigned URL 발급

- RESTful API integration testing

User Swagger 1.0.0 OAS 3.1

User 관련 API Documentation

Servers: / Authorize

Platform User API 플랫폼 메뉴에 사용되는 API입니다.

- PATCH /platform/users/{userId}/password 다른 플랫폼 유저 비밀번호 변경
- GET /platform/users 플랫폼 유저 목록 조회
- GET /platform/users/{userId} 플랫폼 유저 상세 조회
- DELETE /platform/users/{userId} 다른 플랫폼 유저 비활성화로 변경
- GET /platform/users/status 플랫폼 유저 상태값 조회

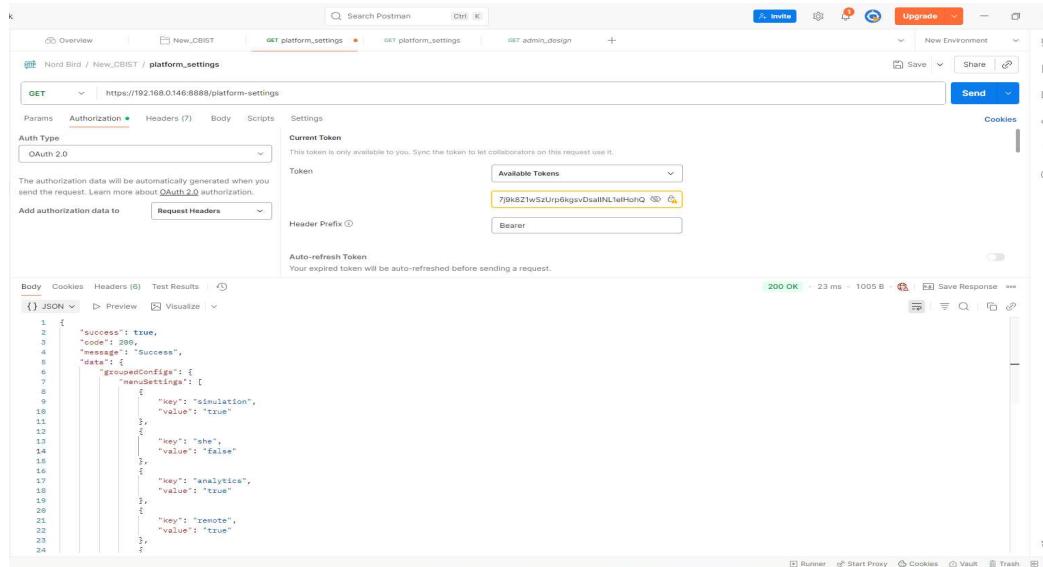
Admin User API 관리자 메뉴에 사용되는 API입니다.

- GET /admin/users 관리자 유저 List

I. Project Overview

10. API(Application Programming Interface) Testing

- RESTful API integration testing

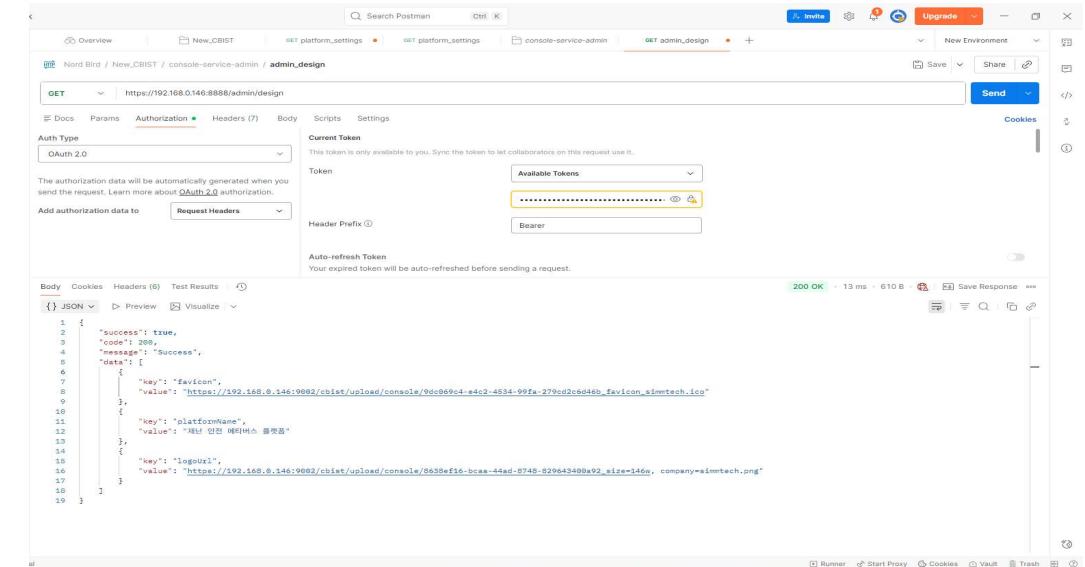


Postman screenshot showing a successful GET request to `/platform_settings` with OAuth 2.0 authentication. The response body is:

```

1   "success": true,
2   "code": 200,
3   "message": "Success",
4   "data": [
5     {
6       "groupConfig": [
7         {
8           "menuSettings": [
9             {
10               "key": "simulation",
11               "value": "true"
12             },
13             {
14               "key": "she",
15               "value": "false"
16             },
17             {
18               "key": "analytics",
19               "value": "true"
20             },
21             {
22               "key": "remote",
23               "value": "true"
24             }
25           ]
26         }
27       ]
28     }
29   ]
30 }
```

- RESTful API integration testing



Postman screenshot showing a successful GET request to `/admin_design` with OAuth 2.0 authentication. The response body is:

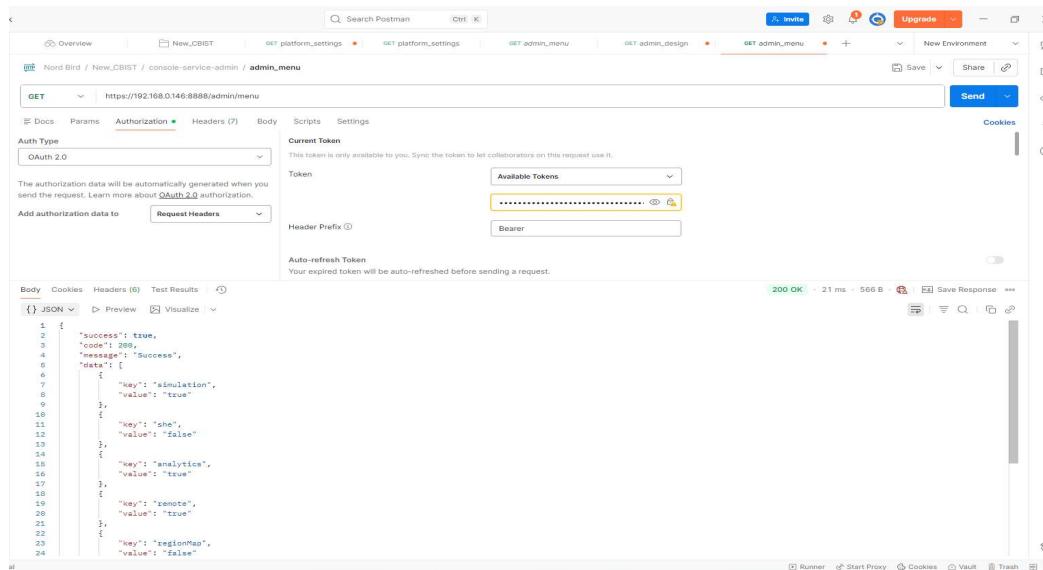
```

1   "success": true,
2   "code": 200,
3   "message": "Success",
4   "data": [
5     {
6       "key": "favicon",
7       "value": "https://192.168.0.146:9082/cbist/upload/console/9dc869c4-e4c2-4534-99fa-279cd2c6d460_favicon_simmttech.ico"
8     },
9     {
10       "key": "listfilename",
11       "value": "제작 업무 대시보드_설정.png"
12     },
13     {
14       "key": "logourl",
15       "value": "https://192.168.0.146:9082/cbist/upload/console/8638ef16-bc8a-44ad-8748-829643400a92_size=146m_company=simmttech.png"
16     }
17   ]
18 }
```

I. Project Overview

10. API(Application Programming Interface) Testing

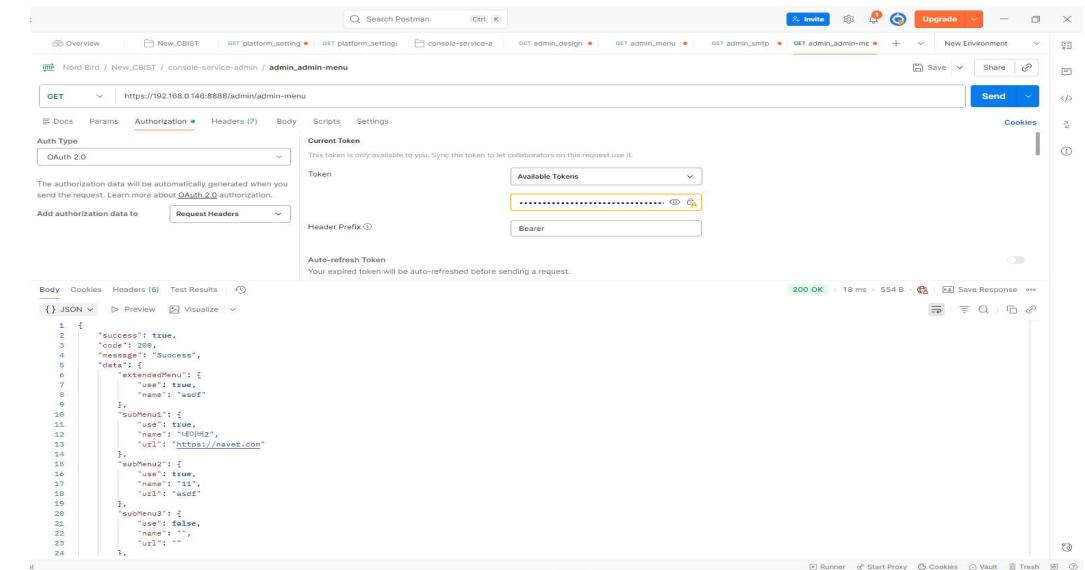
- RESTful API integration testing



```

1  {
2     "success": true,
3     "code": 200,
4     "message": "Success",
5     "data": [
6         {
7             "key": "simulation",
8             "value": "true"
9         },
10        {
11            "key": "she",
12            "value": "false"
13        },
14        {
15            "key": "analytics",
16            "value": "true"
17        },
18        {
19            "key": "remote",
20            "value": "true"
21        },
22        {
23            "key": "regionMap",
24            "value": "false"
25        }
26    ]
27 }
  
```

- RESTful API integration testing



```

1  {
2     "success": true,
3     "code": 200,
4     "message": "Success",
5     "data": [
6         {
7             "extendedMenu": [
8                 {
9                     "use": true,
10                    "name": "asdf"
11                },
12                {
13                    "subMenu1": [
14                        {
15                            "use": true,
16                            "name": "1100HD",
17                            "url": "https://naver.com"
18                        },
19                        {
20                            "subMenu2": [
21                                {
22                                    "use": true,
23                                    "name": "11",
24                                    "url": "asdf"
25                                }
26                            ]
27                        }
28                    ]
29                }
30            ]
31        }
32    ]
33 }
  
```

I. Project Overview

11. Performance Testing (JMeter)

- **Test Environment**

- RESTful API integration testing
- Platform & Admin APIs

- **Test Scenarios**

Platform APIs

- Platform settings, Region, Factory, Facility hierarchy
- Notification, Analytics, Resource (POI, Event) APIs

Admin APIs

- Factory / Floor / Area CRUD
- Facility hierarchy & evacuation routes
- File upload/download (Presigned URL)
- IoT & POI management APIs

- **Key Results**

API Coverage

- Total APIs tested: 50+
- Platform & Admin roles verified

Validation Results

- HTTP Status: 100% expected responses
- Authentication & authorization: No issues
- CRUD & hierarchy flow: All verified

- **Role**

- Designed and executed API integration tests
- Verified request/response and data consistency
- Supported release readiness decision

API Integration Test Summary Table

API Test Metrics

Metric	Platform APIs	Admin APIs	Analysis
API Coverage	Core user-facing APIs	Management & configuration APIs	Full functional coverage
Authentication	OAuth 2.0 (Bearer)	OAuth 2.0 (Bearer)	Stable authentication handling
HTTP Status Accuracy	100% expected	100% expected	No unexpected responses
Error Rate	0%	0%	Highly stable
CRUD Validation	Partial (read 중심)	Full CRUD verified	Data integrity confirmed
Integration Flow	Region → Factory → Floor → Area	Same hierarchy verified	Consistent hierarchy

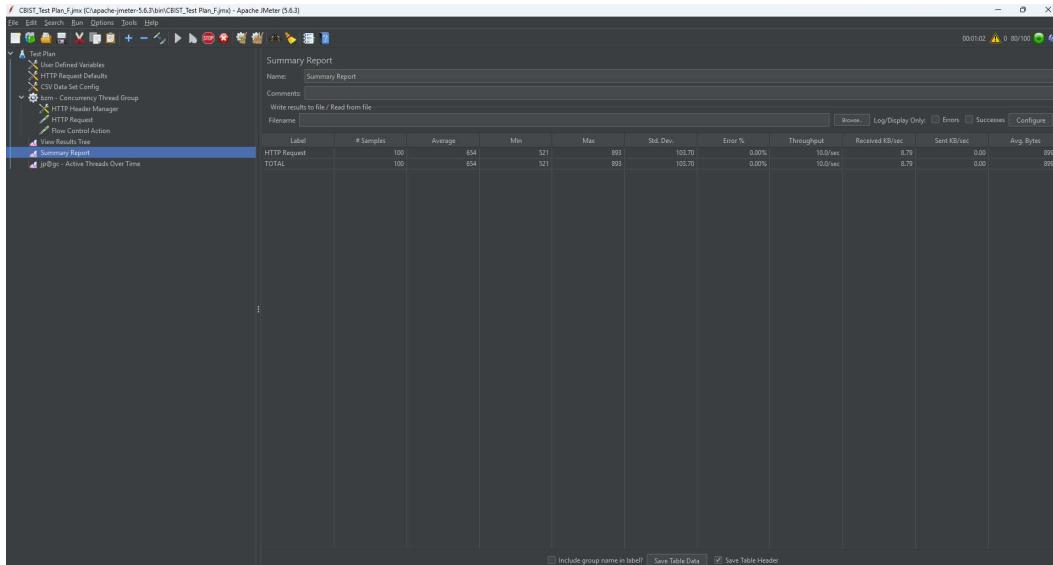
Summary Statement

- ✓ All platform and admin APIs operate stably and consistently
- ✓ API integration requirements are fully satisfied

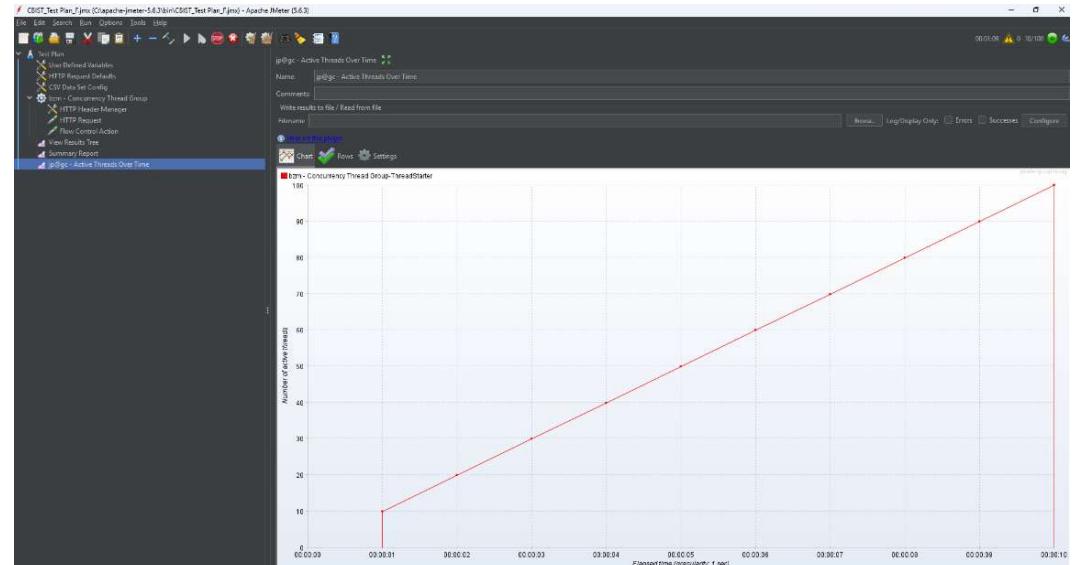
I. Project Overview

12. Performance Testing

- Summary Report of 100 concurrent users



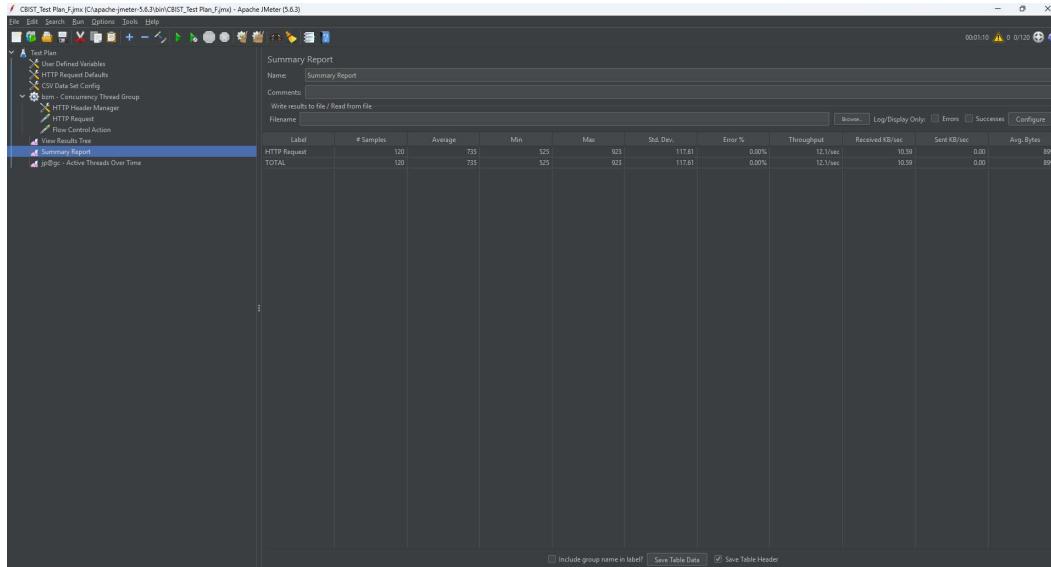
- Graph of 100 concurrent users



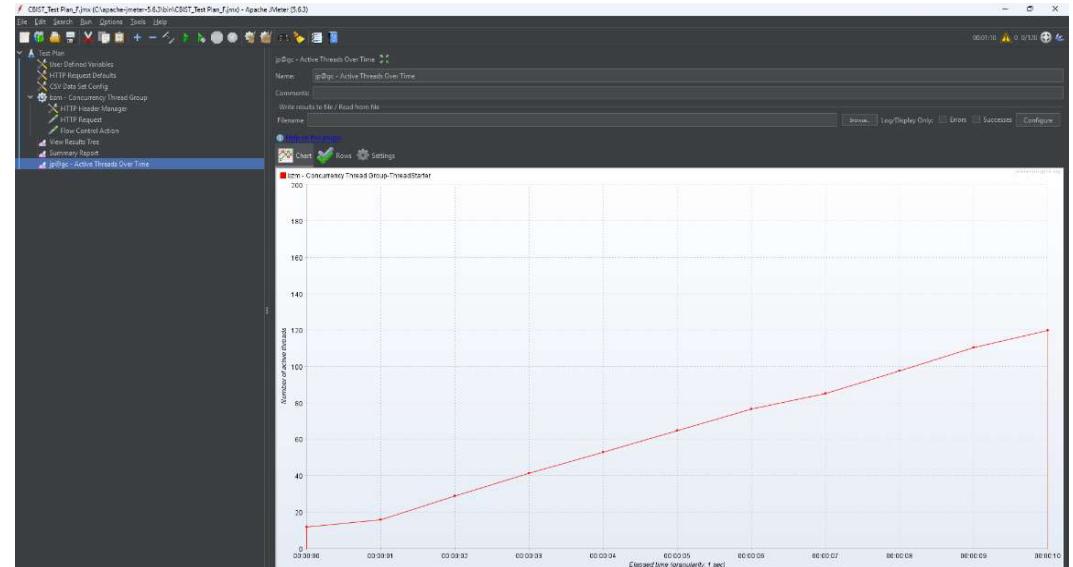
I. Project Overview

12. Performance Testing

- Summary Report of 120 concurrent users



- Graph of 120 concurrent users



I. Project Overview

13. Performance Testing (JMeter)

• Test Environment

- JMeter-based performance testing environment
- Backend API load and concurrency testing
- Step load pattern with gradual user increase

• Test Scenarios

100 Virtual Users

- Increased by 10 users step-by-step and sustained

120 Virtual Users

- Increased by 12 users step-by-step and sustained

• Key Results

100 Users

- Avg Response Time: 654 ms
- Error Rate: 0%, Success Rate: 100%

120 Users

- Avg Response Time: 735 ms
- Error Rate: 0%, Success Rate: 100%

• Role

- Designed and executed JMeter performance tests
- Analyzed results and supported release readiness assessment

Metric	100 Users	120 Users	Analysis
Average Response Time	654 ms	735 ms	Approx. +12% increase, acceptable
Maximum Response Time	893 ms	923 ms	No significant difference
Error Rate	0%	0%	Highly stable
Success Rate	100%	100%	Successful
Throughput	10.0 / sec	12.1 / sec	Linear increase

Key Strengths

Excellent response time (under 1 second)

Zero errors → high service reliability

Linear scaling with increased load → good scalability

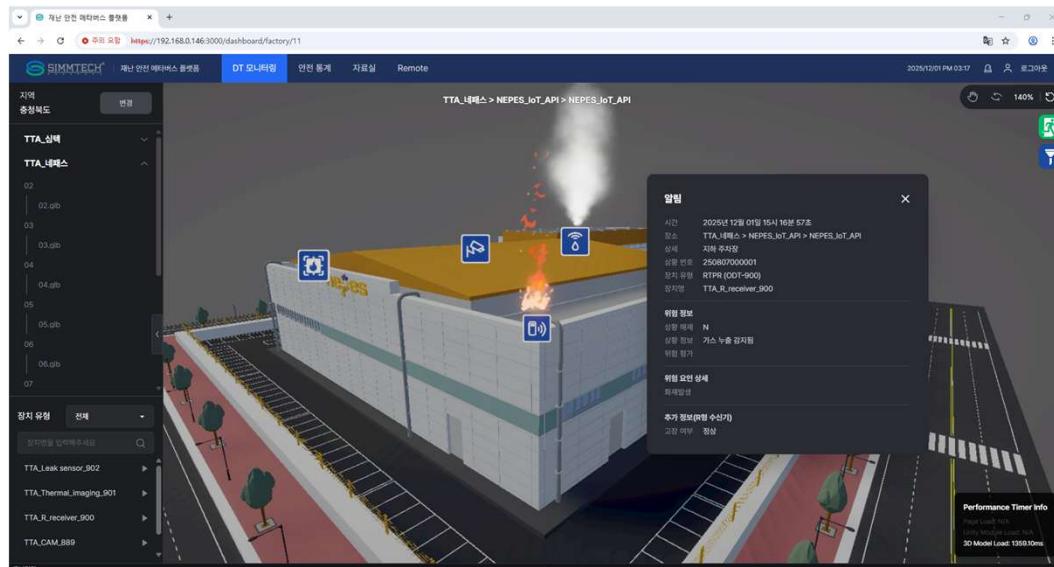
Summary Statement

✓ The login API remains stable and operates reliably **up to 120 concurrent users without performance degradation.**

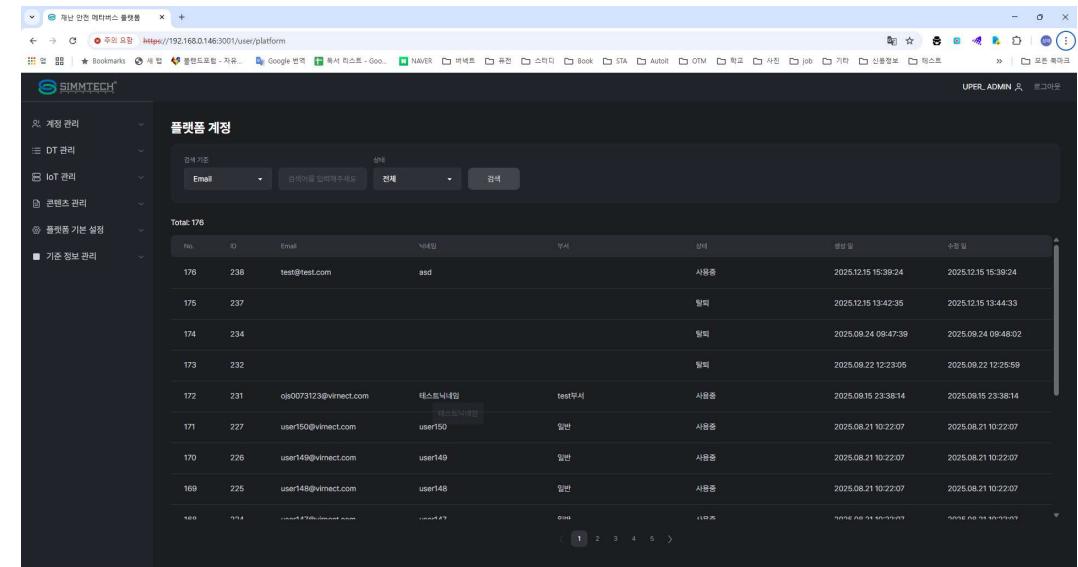
I. Project Overview

14. Security Testing

- User web age



- Admin web page



The screenshot shows an admin dashboard with a user list titled '풀랫폼 계정'. The table lists users with their ID, Email, Name, Status, Creation Date, and Last Activity. The last activity column shows dates ranging from 2025/12/15 to 2025/08/21.

No.	ID	Email	Name	Status	생성 일	수정 일
176	238	test@test.com	asd	사용중	2025.12.15 15:39:24	2025.12.15 15:39:24
175	237			탈퇴	2025.12.15 13:42:35	2025.12.15 13:44:33
174	234			탈퇴	2025.08.24 09:47:39	2025.08.24 09:48:02
173	232			탈퇴	2025.08.22 12:23:05	2025.08.22 12:25:59
172	231	obj0073123@vimect.com	테스트비내임	test부서	사용중	2025.09.15 23:38:14
171	227	user150@vimect.com	user150	일반	사용중	2025.08.21 10:22:07
170	226	user149@vimect.com	user149	일반	사용중	2025.08.21 10:22:07
169	225	user148@vimect.com	user148	일반	사용중	2025.08.21 10:22:07
460	774	user147@vimect.com	user147	일반	사용중	2025.08.21 10:22:07

I. Project Overview

15. Security Testing (ZAP)

- **Test Environment**

- OWASP ZAP (Checkmarx Scanning Report)
automated security scanning
- Target: Platform (User) web pages + related API endpoints
- Authenticated context applied for major user flows (login/session)

- **Test Scenarios**

- Spider / AJAX Spider for endpoint discovery
- Passive Scan + Active Scan on discovered URLs
- Validation on common web vulnerabilities and security headers

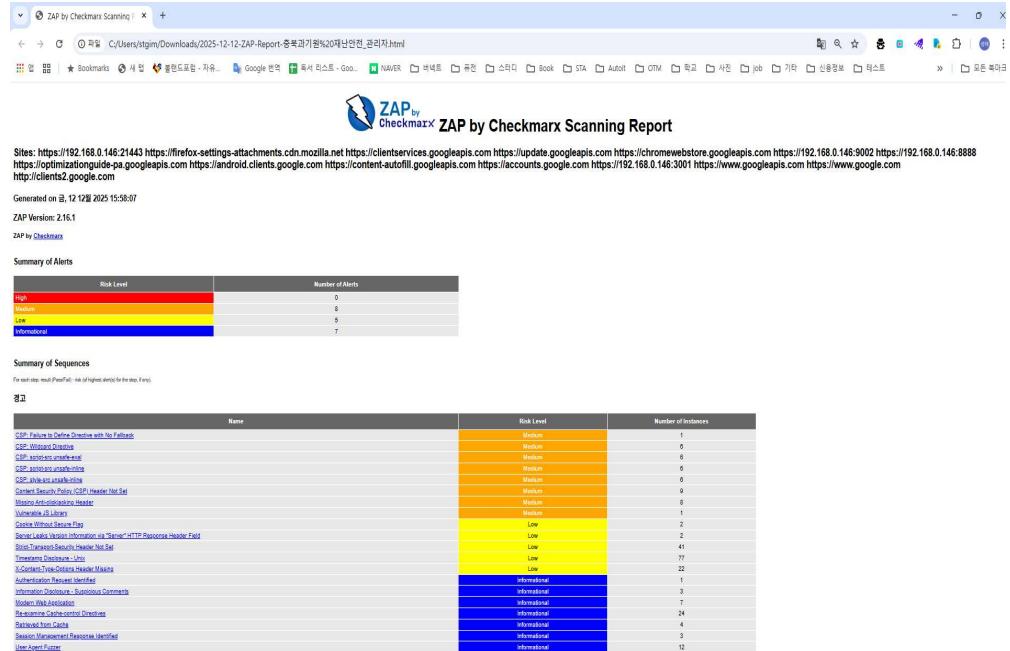
- **Key Results**

Key Medium findings:

- Content Security Policy (CSP) header not set / CSP misconfigurations (unsafe-inline, unsafe-eval, wildcard)
- Missing anti-clickjacking header
- Vulnerable JS library (identified)

Key Low findings:

HSTS header not set, X-Content-Type-Options missing
Timestamp disclosure / minor information exposure items



Summary Statement

✓ No High risk vulnerabilities were detected. Platform security is generally acceptable, and header hardening (CSP/HSTS/XCTO) and library patching are recommended before production release.

I. Project Overview

16. Security Testing (ZAP)

- **Test Environment**

- OWASP ZAP (Checkmarx Scanning Report) automated security scanning
- Target: Platform (User) web pages + related API endpoints
- Authenticated context applied for major user flows (login/session)

- **Test Scenarios**

- Spider / AJAX Spider for endpoint discovery
- Passive Scan + Active Scan on discovered URLs
- Validation on common web vulnerabilities and security headers

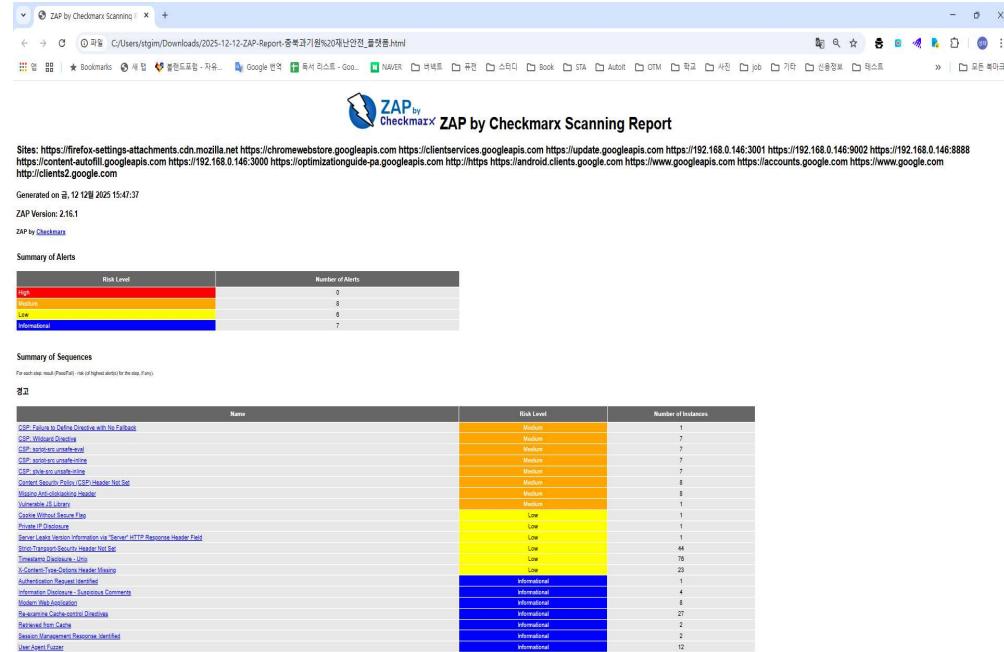
- **Key Results**

Key Medium findings:

- Content Security Policy (CSP) header not set / CSP misconfigurations (unsafe-inline, unsafe-eval, wildcard)
- Missing anti-clickjacking header
- Vulnerable JS library (identified)

Key Low findings:

HSTS header not set, X-Content-Type-Options missing
Timestamp disclosure / minor information exposure items



Summary Statement

✓ No High risk vulnerabilities were detected. Admin security readiness is acceptable, but CSP & security header reinforcement, cookie/security configuration, and JS library updates should be applied and re-validated.

2. Project Results

- Successfully deployed and configured SonarQube using Docker and Docker Compose on Linux, establishing a stable environment for continuous code quality analysis.
- Integrated SonarQube with Jenkins CI/CD pipelines, enabling automated static analysis and quality gate enforcement for frontend and backend services.
- Performed static analysis of automated test code using SonarScanner CLI, identifying code smells, bugs, and security vulnerabilities early in the development cycle.
- Built centralized SonarQube dashboards to visualize key quality metrics such as code duplication, coverage trends, and security hotspots, with real-time notifications via Slack.
- Designed and executed JMeter-based performance tests to validate backend API stability under concurrent user load.
- Conducted step-load performance scenarios with 100 and 120 virtual users, confirming that average response times remained under 1 second with 0% error rate and 100% success rate.
- Observed linear throughput growth as concurrency increased, demonstrating stable scalability and supporting release readiness.
- Achieved measurable improvements in test maintainability, system stability, and regression reliability, significantly reducing technical and performance-related risks.
- Conducted OWASP ZAP security scans for Platform and Admin, confirming no high-risk vulnerabilities and recommending security header hardening (CSP/HSTS) and library patching for release readiness.

Future Directions

- **Building an AI-Enhanced CI Pipeline for Quality Automation**

- AI-Assisted Test Recommendation & Generation
- Suggest Unit/API test cases based on code changes (diff-based coverage)

- **AI-Driven Quality Gates**

- Strengthen release criteria using risk-based analysis (beyond coverage only)

- **Flaky Test Detection & Stabilization with AI**

- Identify unstable tests from failure patterns and optimize retry strategies

- **Automated Security Validation with ZAP + AI Insights**

- Summarize vulnerabilities, prioritize risks, and generate remediation guidance

- **AI-Powered CI Reporting & Smart Notifications**

- Auto-summarize Jenkins/Sonar/ZAP results and share actionable insights via Slack

Goal: Faster feedback loops, safer releases, and scalable QA automation.