0	0	0	0	0	0	0
0	0	0	0	0	0	0
	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0

# Sparrow SAST/SAQT 사용 설명서

www.SparrowFasoo.com



Sparrow Enterprise는 (주)스패로우에서 개발한 다양한 제품을 사용할 수 있는 통합 플랫폼입니다. Sparrow Enterprise를 통해 소프트웨어 개발부터 운영에 이르는 전과정에 필요한 보안 솔루션, 테스트 케이스 최적화, 워크플로 관리를 하나의 플랫폼에서 사용하실 수 있습니다.

#### SDLC에서 발생하는 이슈 통합 관리

Sparrow Enterprise는 소프트웨어 개발과 운영 과정에서 발생하는 다양한 보안 취약점 및 품질 이슈를 검출 하고 확인함으로써 사용자가 소프트웨어 개발 수명 주기(SDLC)를 통합 관리할 수 있는 기반을 제공합니다.

#### 워크플로 실행

워크플로 기능을 통해 DevSecOps를 구현하기 위해 필요한 태스크를 설정함으로써 프로세스를 하나로 연결 할 수 있습니다. 동시에 현재 실행한 워크플로를 모니터링하고 장기적으로 워크플로의 히스토리 및 워크플 로에서 발생한 이슈를 확인하고 관리할 수 있습니다.

#### 검출 규칙 관리

Sparrow Enterprise에서는 분석에 사용할 검출 규칙을 활성화하거나 비활성화하여 규칙을 변경할 수 있습니 다. 작업 프로파일을 통해 프로젝트에 따라 필요한 레퍼런스나 검출 규칙으로 필요한 이슈만을 검사하도록 조정할 수 있습니다.

#### 웹 기반 사용자 인터페이스

Sparrow Enterprise는 웹 브라우저를 이용하여 손쉽게 분석을 수행하고 결과를 확인하도록 지원합니다. 프 로젝트라는 단위로 분석 작업을 구분하고 대시보드 및 프로젝트 요약 정보 페이지를 제공하여 작업 결과 검 출한 이슈를 한 눈에 확인하고 추이를 파악할 수 있습니다.

#### 다수 사용자에 최적화된 시스템

Sparrow Enterprise는 사용자의 권한 및 역할을 커스터마이징하여 개별 사용자에게 필요한 역할을 분배합니 다. 시스템뿐만 아니라 프로젝트에서도 세부적인 권한을 지정할 수 있습니다. 동시에 결재선을 통해 주요 동 작을 실행하기 전에 관리자의 승인을 거치도록 설계되었습니다.

이제 Sparrow Enterprise에서 사용하실 수 있는 제품을 소개하겠습니다. Sparrow Enterprise에서 제공하는 솔루션은 소스코드의 보안 취약점과 품질을 점검하는 Sparrow SAST/SAQT, 웹 애플리케이션의 취약점을 분석하는 Sparrow DAST, 오픈소스 라이선스와 컴포넌트를 관리하는 Sparrow SCA, 웹 애플리케이션을 모 니터링하며 방어하는 Sparrow RASP, 테스트 케이스를 관리하는 Sparrow TSO 등이며 개발 사이클 전반에 DevSecOps를 구현하는 관리 도구인 워크플로를 기본 기능으로 사용할 수 있습니다. 필요에 따라 원하는 제 품의 라이선스를 구입하시고 해당하는 솔루션의 기능을 단일 웹 페이지에서 자유롭게 사용해보세요.

### Sparrow SAST/SAQT 둘러보기

Sparrow SAST/SAQT는 정적분석을 통해 보안이나 품질과 관련하여 소스코드에 존재하는 취약점이나 잠재 적인 문제를 정확하고 빠르게 검출하는 소스코드 분석 도구입니다. 웹 기반의 인터페이스뿐만 아니라 클라 이언트를 통해 GUI 및 CLI 분석을 수행할 수 있으며 IDE 플러그인을 사용할 수도 있습니다. 이러한 높은 사용 성과 접근성으로 인해 다양한 개발 환경에서 활용할 수 있는 제품입니다.

#### Sparrow SAST/SAQT 주요 기능

Sparrow SAST/SAQT에서 제공하는 주요 기능은 소스코드 분석이며 다음과 같습니다.

#### 소스코드에 포함된 잠재적 취약점 검출

소스코드에 포함된 보안 문제는 소프트웨어의 취약점으로 이어질 수 있는 잠재적인 원인이 됩니다. Sparrow SAST/SAQT에서는 국내외 주요 레퍼런스를 기준으로 코드를 배포하기 전에 이러한 보안약점이 존재하는지 먼저 찾아냅니다.

#### 소스코드에 포함된 품질 이슈 검출

보안 문제와 함께 품질 결함도 애플리케이션 배포와 운영 과정에서 중요한 이슈입니다. Sparrow SAST/SAQT에서는 국내외 주요 코딩 스탠다드 혹은 컨벤션과 관련된 기준을 제공합니다.

#### 폭 넓은 지원 언어

Sparrow SAST/SAQT에서는 소프트웨어에 가장 널리 사용하는 언어에서부터 최신 언어까지 다양한 개발 언어를 분석합니다. 필요한 경우 개발 환경에 따라 분석 대상을 구분하여 보다 정확한 분석을 수행할 수도 있고 빌드 없이 대략적인 이슈를 확인하는 기능도 사용하실 수 있습니다.

## 제품 구성

Sparrow Enterprise는 분석 엔진과 DB를 포함하는 **서버**와 각 제품의 분석을 실행하는 **클라이언트** 및 분석 명령을 전달하는 **에이전트**로 구성됩니다.

### 제품 사양 및 지원 환경

#### Sparrow Enterprise 서버

**Sparrow Enterprise 서버**는 다음과 같은 하드웨어 및 지원 환경에서 설치하도록 권장합니다. 프로그램을 설치하시기 전에 확인해주세요.

CPU : Quad Core 2.50 GHz 이상

RAM : 16.0 GB 이상

HDD : 300 GB 이상

OS : Windows 10

Rocky 9.1

데이터베이스 : PostgreSQL (자체 내장)

브라우저 : Chrome 100.0.4896.88

Internet Explorer 11

Sparrow Enterprise 클라이언트

**Sparrow Enterprise 클라이언트**는 다음과 같은 하드웨어 및 지원 환경에서 설치하도록 권장합니다. 프로그 램을 설치하시기 전에 확인해주세요.

CPU : Quad Core 2.50 GHz 이상

RAM : 16.0 GB 이상

HDD : 130 GB 이상

OS : Windows 10

Rocky 9.1

데이터베이스 : PostgreSQL (자체 내장)

플러그인 : Eclipse 2018-09

IntelliJ 2023.1.6

Visual Studio Code 1.88.1

Sparrow 태스크 에이전트

**Sparrow 태스크 에이전트**는 다음과 같은 지원 환경에서 설치하도록 권장합니다. 프로그램을 설치하시기 전 에 확인해주세요.

Java 11

## 빠른 시작

## 사용 방법 가이드

✔ 실행하기

1. Sparrow Enterprise 서버를 시작하세요.

2. 웹 브라우저에서 Sparrow Enterprise 서버 URL(https://{Sparrow Enterprise 서버 IP 주소}:{포트 번 호})로 이동하세요.

3. 최고 관리자에게 받은 ID와 비밀번호를 입력한 후에 로그인 버튼을 클릭하세요.

자세한 내용은 서버 시작하기 혹은 로그인하기에서 확인하시기 바랍니다.

#### ✔ 프로젝트 만들기

1. 왼쪽 사이드 바에서 프로젝트 목록 아이콘을 클릭하세요.

2. **프로젝트 추가하기** 버튼을 클릭하세요.

3. 프로젝트 정보를 입력하세요.

4. 추가 버튼을 클릭하세요.

자세한 내용은 새 프로젝트 만들기에서 확인하시기 바랍니다.

✔ Sparrow SAST/SAQT 소스코드 분석 수행하기

웹 서버에서 직접 분석하는 방법은 다음과 같습니다.

1. 웹 브라우저에서 Sparrow Enterprise 서버 URL(**https://{Sparrow Enterprise 서버 IP 주소}:{포트 번** 호})로 이동하세요.

2. 프로젝트 상세 정보 페이지에서 새 작업 시작하기 버튼을 클릭하세요.

3. 전수 분석 혹은 수시 분석 카드를 클릭하고 작업 프로파일을 선택하세요.

4. 분석 대상 중에서 압축 파일을 선택하세요.

5. 압축된 소스코드 파일을 선택하고 **확장자**를 선택하세요.

6. 선택하기 버튼과 시작하기 버튼을 차례대로 클릭하세요.

자세한 내용은 웹 서버에서 소스코드 분석하기에서 확인하시기 바랍니다.

클라이언트를 통해 분석하는 방법은 다음과 같습니다.

1. Sparrow Enterprise 클라이언트 설치 디렉토리로 이동하세요.

2. Windows 환경에서는 **sparrow-client-manager.exe** 파일을 실행하고 작업을 수행할 프로젝트 및 작 업 프로파일을 선택하고 실행하세요.

자세한 내용은 클라이언트 GUI: 소스코드 분석하기에서 확인하시기 바랍니다.

3. 다른 환경인 경우 sparrow-cli 파일을 명령어 및 옵션과 함께 실행하세요.

자세한 내용은 클라이언트 CLI: 소스코드 분석하기에서 확인하시기 바랍니다.

✔ 분석 이슈 보기

1. 왼쪽 사이드 바에서 프로젝트 목록 아이콘을 클릭하세요.

2. 확인하려는 프로젝트를 클릭하세요.

- 3. 오른쪽 탭에서 **이슈**를 클릭하세요.
- 4. 해당 정보를 확인할 수 있습니다.

자세한 내용은 라이선스에 따라 **최근 이슈 확인하기**, 소스코드 이슈, 컴포넌트 이슈, 웹 취약점 이슈, 자가 방어 이슈에서 확인하시기 바랍니다.

✔ 워크플로 실행하기

이 작업은 워크플로 관리 권한을 가진 사용자만 사용할 수 있습니다.

- 1. 왼쪽 사이드 바에서 **워크플로** 아이콘을 클릭하세요.
- 2. 워크플로를 추가하세요.
- 3. 태스크와 액션을 추가하세요.
- 4. 워크플로 상세 정보 페이지에서 워크플로 실행하기 버튼을 클릭하세요.

자세한 내용은 워크플로에서 확인하시기 바랍니다.

### 사용자 혹은 관리자를 위한 가이드

본 가이드는 Sparrow Enterprise를 사용하는 기본적인 방법을 설명하고 있습니다. 사용자는 부여된 권한에 따라 필요한 내용을 참고하시기 바랍니다.

✔ 사용자용 매뉴얼

새 프로젝트 만들기

프로젝트 수정하기

분석하기

작업 예약하기

Eclipse 플러그인 사용하기

IntelliJ 플러그인 사용하기

Visual Studio Code 플러그인 사용하기

자산 확인하기

이슈 확인하기

이슈 제외하기

✔ 관리자용 매뉴얼

Sparrow Enterprise 서버 설치하기 Sparrow Enterprise 클라이언트 설치하기 Sparrow 태스크 에이전트 설치하기 제품 라이선스 적용하기

워크플로 만들기

시스템 역할 관리하기 및 프로젝트 역할 관리하기

결재선 관리하기

사용자 관리하기 및 사용자 그룹 관리하기

이슈 검출 규칙 관리하기 및 작업 프로파일 관리하기

태스크 에이전트 관리하기

보고서 템플릿 관리하기

시스템 정보 확인하기 및 제품 라이선스 정보 확인하기

이제 Sparrow Enterprise를 설치하는 과정부터 시작해서, 프로젝트를 생성하고, 각 제품에서 분석 및 방어, 최적화를 수행하며, 결과를 확인하는 등 Sparrow Enterprise를 사용하는 과정 및 계정 정보를 확인하고,

## 설치하기

## Sparrow Enterprise 서버 설치하기

Windows 환경에서 Sparrow Enterprise를 설치하는 경우 **서버 매니저**를 사용할 수 있습니다. Linux 환경에 서버를 설치해야 하거나 Windows에서 GUI를 사용하지 않고 설치하려면 **CMD**로 설치 명령어를 입력하세요.

Tip: 자가 방어를 수행하려면 Sparrow Enterprise를 Linux 환경에 설치하세요.

워크플로를 실행하려면 시스템 환경 변수에 JAVA\_HOME을 설정했는지 확인하세요.

Sparrow Enterprise 서버 매니저로 설치하기

Windows에서는 서버 매니저를 사용하여 Sparrow Enterprise를 설치하고 시작할 수 있습니다.

- 1. 패키지에 포함된 CD를 설치할 컴퓨터에 삽입하세요.
- 2. CD에 포함된 sparrow-enterprise-server-{OS+version}.zip 파일을 원하는 영문 디렉토리에 복사한 후 압축을 해제하세요.

📙 🛛 🔁 📒 🖛 🛛 sparrow-enterprise-server-wir	dows-r1545-20231211		- 0	×
파업 홈 공유 보기				~ 🔞
★ 대 이동 위기 물거찾기에 복사 불여보기 고정	지 - ★ 삭제 • 지 - 프 (이름 바꾸기		· 문 선택	
클립보드	구성 사	로 만들기   열기		
← → × ↑ 🧧 « ser > sparro	v ð ,≏ span	row-enterprise-server-w	indows-r1545-	202
이름 ^	수정한 날짜	유형	크기	
db	2023-12-12 오전 9:54	파일 풀더		
🔚 jre	2023-12-12 오전 9:54	파일 뿔더		
mq	2023-12-12 오전 9:54	파일 뿔더		
node	2023-12-12 오전 9:54	파일 물더		
ops	2023-12-12 오전 9:54	파일 뿔더		
service	2023-12-12 오전 9:54	파일 물더		
storage	2023-12-12 오전 9:54	파일 뿔더		
install.cmd	2023-12-11 오후 9:44	Windows 명령이	1KB	
😽 server-manager.exe	2023-12-11 오후 9:44	응용 프로그램	77,911KB	
sparrow.cmd	2023-12-11 오후 9:44	Windows 명령어	1KB	
sparrow.properties	2023-12-11 오후 9:44	Properties 원본 파	2KB	
start.cmd	2023-12-11 오후 9:44	Windows 명령어	1KB	
istatus.cmd	2023-12-11 오후 9:44	Windows 명령어	1KB	
stop.cmd	2023-12-11 오후 9:44	Windows 명령어	1KB	
uninstall.cmd	2023-12-11 오후 9:44	Windows 명령이	1KB	
15개 항목				

Warning: Sparrow Enterprise의 설치 경로에 한글 또는 공백이 포함되어 있으면 정상적으로 설치되 지 않습니다.

3. **{Sparrow Enterprise 서버 설치 디렉토리}** 폴더에 있는 server-manager.exe 파일을 실행하세요.



4. Sparrow Enterprise가 설치됩니다.

서버 매니저를 사용해서 Sparrow Enterprise 서버를 시작하는 방법은 다음과 같습니다.

5. 서버 매니저를 실행하세요.

Sparrow				-		$\times$			
Sparrow E	Sparrow Enterprise								
	사	버가 중지도	있습니	다.					
데이터베이스		ActiveMO		게이트웨이	_				
efotetetetet=	=	Activenta		. Internet		1			
객체 저장소	_	백엔드		브로커	_	J			
SAST	-	DAST	-	SCA	-	J			
TSO	-	워크플로	-	프론트엔드	-	J			
				삭제하기	실행하기				
						-			

6. 모두 실행하기 버튼을 클릭하세요.

**Tip**: **설치되지 않은 모듈**이 있는 경우 **실행하기** 버튼을 클릭할 수 없습니다. 모든 모듈이 설치되었는 지 확인하세요.

7. 서버가 시작됩니다.



서버 매니저를 사용해서 Sparrow Enterprise 서버를 중지하는 방법은 다음과 같습니다.

- 8. 서버 매니저를 실행하세요.
- 9. 모두 중지하기 버튼을 클릭하세요.
- 10. 서버가 중지됩니다.

CMD 명령어로 Sparrow Enterprise 설치하기

<Windows 환경>

서버 매니저 대신 CMD 명령어로 Sparrow Enterprise 서버를 설치할 수 있습니다.

- 1. 패키지에 포함된 CD를 설치할 컴퓨터에 삽입하세요.
- 2. CD에 포함된 **sparrow-enterprise-server-{OS+version}.zip** 파일을 원하는 영문 디렉토리에 복사한 후 압축을 해제하세요.



Warning: Sparrow Enterprise의 설치 경로에 한글 또는 공백이 포함되어 있으면 정상적으로 설치되지 않습니다.

3. **{Sparrow Enterprise 서버 설치 디렉토리}** 폴더에 있는 **install.cmd** 파일을 실행하세요.





#### 4. Sparrow Enterprise가 설치됩니다.

설치된 Sparrow Enterprise 서버를 시작하는 방법은 다음과 같습니다.

5. {Sparrow Enterprise 서버 설치 디렉토리} 경로로 이동하세요.

C:#Windows#System32#cmd.exe	_	×
C:#Sparrow#ENTERPRISE#server>cd sparrow-enterprise-server-windows-r1594-20231222		^
C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-windows-r1594-20231222>		
		$\sim$

6. **start.cmd** 파일을 실행하세요.

7. 다음과 같은 메시지가 표시되면서 서버가 시작됩니다.

C:#Windows#System32#cmd.exe -		×
C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-windows-r1594-20231222>start.cmd [INFO ] Task [start] started [INFO ] Modules: all modules INFO ]		/
[INFO ] start db : [INFO ] Template updated to C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-windows-r1594-2023 nfig#application.yml	1222₩db†	₩со
[INFO ] Asynchronous script executed at C:\Sparrow\ENTERPRISE\server\sparrow-enterprise-server-window 231222\db [INFO ]	s-r1594	-20
[INFO ] start activemq : [INFO ] Asynchronous script executed at C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-window 231222#mq [INFO ]	s-r1594	-20
[INFO] start gateway: [INFO] Template updated to C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-windows-r1594-2023 ce#gateway#config#application.yml [INFO] Asynchronous script executed at C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-window 231222#service#gateway [INFO]	1222₩sei s-r1594	rvi -20
[INFO ] start storage : [INFO ] Asynchronous script executed at C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-window 231222#storage [INFO ]	s-r1594	-20
[INFO] start backend : [INFO] Template updated to C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-windows-r1594-2023 ce#backend#config#application.yml	1222₩se	rvi -20
231222#service#backend [INFO] [INFO]] start broker :	5 1 1 3 3 4	20
[INFO] Template updated to C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-windows-r1594-2023 ce#broker#config#config.json [INFO] Asynchronous script executed at C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-window 231222#service#broker [INFO]	1222₩sei s-r1594	rvi -20
[INFO] start sast : [INFO] Template updated to C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-windows-r1594-2023 ce#sast#config#application.yml [INFO] Asynchronous script executed at C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-window 231222#service#sast	1222₩sei s-r1594	rvi 20
[INFO] start dast : [INFO] Template updated to C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-windows-r1594-2023 ce#dast#config#application.yml [INFO] Asynchronous script executed at C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-window 231222#service#dast [INFO]	1222₩se s-r1594	rvi -20
[INFO ] start sca : [INFO ] Template updated to C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-windows-r1594-2023 ce#sca#config#application.yml [INFO ] Asynchronous script executed at C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-window 231222#service#sca	1222₩sei s-r1594	rvi 20
[INFO ] start tso : [INFO ] Template updated to C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-windows-r1594-2023 ce#tso#config#application.yml [INFO ] Asynchronous script executed at C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-window 231222#service#tso [INFO ]	1222₩sei s-r1594	rvi 20
[INFO] start workflow : [INFO] Template updated to C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-windows-r1594-2023 ce#workflow#config#application.properties [INFO] Asynchronous script executed at C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-window 231222#service#workflow	1222₩sei s-r1594	rvi -20
[INFO] start frontend : [INFO] Template updated to C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-windows-r1594-2023 ce#frontend#.env [INFO] Asynchronous script executed at C:#Sparrow#ENTERPRISE#server#sparrow-enterprise-server-window 231222#service#frontend [INFO]	1222₩sei s-r1594	rvi 20
[INF0 ] [INF0 ] Entry point: https://localhost:10880 [INF0 ]		
[INFO] TASK FINISHED [INFO]		
[INFO ] Total time: 67.326s [INFO ] Task ended: 2023-12-22T17:07:25.788		

시작된 Sparrow Enterprise 서버를 중지하는 방법은 다음과 같습니다.

8. **{Sparrow Enterprise 서버 설치 디렉토리}** 경로로 이동하세요.



#### 9. stop.cmd 파일을 실행하세요.

10. 다음과 같은 메시지가 표시되면서 서버가 중지됩니다.

<b>⊡••</b> C:₩W	Vindows#System32#cmd.exe	_	×
C:#Spar [INF0] [INF0]	row#ENTERPRISE#server#sparrow-enterprise-server-windows-r1594-20231222>stop.cmd Task [ <mark>stop</mark> ] started Modules: all modules		^
[INFO] [INFO]	stop frontend : Process (pid 42396) destroyed		
[INFO] [INFO]	stop workflow : Process (pid 42868) destroyed		
[INFO] [INFO] [INFO]	<mark>stop</mark> tso : Process (pid 34548) destroyed		
[INFO] [INFO] [INFO]	stop sca : Process (pid 27708) destroyed		
[INFO] [INFO] [INFO]	stop dast : Process (pid 24408) destroyed		
[INFO] [INFO] [INFO]	stop sast : Process (pid 39472) destroyed		
[INFO] [INFO] [INFO]	stop broker : Process (pid 38360) destroyed		
[INFO] [INFO] [INFO]	stop backend : Process (pid 7440) destroyed		
LINFO ] [INFO ] [INFO ]	stop storage : Process (pid 29156) destroyed		
[INFO] [INFO]	stop activenq : Process (pid 36292) destroyed		
[INFO] [INFO] [INFO]	stop gateway : Process (pid 47360) destroyed		
[INFO] [INFO]	stop db : Process (pid 45516) destroyed		
[INFO] [INFO]	TASK FINISHED		
[INFO]	Task ended: 2023-12-22T17:08:08.302		Ų

<Linux 환경>

Sparrow Enterprise 서버는 Rocky 9.1 환경에서 CMD 명령어로 설치할 수 있습니다.

- 1. 패키지에 포함된 CD를 설치할 컴퓨터에 삽입하세요.
- 2. CD에 포함된 sparrow-server-{OS+version}-{YYYYMMDD}.tar.gz 파일을 원하는 영문 디렉토리에 복사한 후 압축을 해제하세요.

Warning: Sparrow Enterprise의 설치 경로에 한글 또는 공백이 포함되어 있으면 정상적으로 설치되지 않습니다.

3. **{Sparrow Enterprise 서버 설치 디렉토리}** 폴더에 있는 **install** 파일을 실행하세요.

4. Sparrow Enterprise가 설치됩니다.

설치된 Sparrow Enterprise 서버를 시작하는 방법은 다음과 같습니다.

#### 5. {Sparrow Enterprise 서버 설치 디렉토리} 경로로 이동하세요.

- 6. ./start 명령어를 실행하세요.
- 7. 서버가 시작됩니다.

시작된 Sparrow Enterprise 서버를 중지하는 방법은 다음과 같습니다.

- 8. {Sparrow Enterprise 서버 설치 디렉토리} 경로로 이동하세요.
- 9. ./stop 명령어를 실행하세요.
- 10. 서버가 중지됩니다.

#### Sparrow Enterprise 프로퍼티 설정하기

Sparrow Enterprise 서버를 설치할 때 필요한 설정 정보는 \*\*{Sparrow Enterprise 서버 설치 디렉토리}\*\*에 있 는 **sparrow.properties** 파일에 기록됩니다. 다음을 참고하여 해당 파일에 저장된 내용을 수정하고 저장함으 로써 프로그램 설정을 변경할 수 있습니다.

#### √ 서비스 설정

#### service.host

Sparrow Enterprise 서버의 호스트 주소입니다.(기본값: localhost)

#### service.public.host

Sparrow Enterprise 서버를 외부에 공개할 목적으로 사용하는 호스트 주소입니다. 예를 들어, 이 호스트 주 소를 사용하여 분석이 완료되고 해당 결과에 접근하는 주소를 안내할 수 있습니다.(기본값: localhost)

#### service.frontend.port

Sparrow Enterprise 서버의 프론트엔드 포트 번호입니다.(기본값: 10880)

#### service.gateway.port

Sparrow Enterprise 서버의 게이트웨이 포트 번호입니다.(기본값: 10500)

#### service.backend.port

Sparrow Enterprise 서버의 백엔드 포트 번호입니다.(기본값: 10610)

#### service.brocker.port

Sparrow Enterprise 서버의 브로커 포트 번호입니다.(기본값: 10700)

#### service.brocker.grpc.port

Sparrow Enterprise 서버의 브로커에서 사용하는 gRPC(google Remote Procedure Call) 포트 번호입니다. (기본값: 10800)

#### service.sast.port

Sparrow SAST 서버의 포트 번호입니다.(기본값: 10900)

#### service.dast.port

Sparrow DAST 서버의 포트 번호입니다.(기본값: 10910)

#### service.rasp.port

Sparrow RASP 서버의 포트 번호입니다.(기본값: 10920)

#### service.sca.port

Sparrow SCA 서버의 포트 번호입니다.(기본값: 10930)

#### service.tso.port

Sparrow TSO 서버의 포트 번호입니다.(기본값: 10950)

#### service.workflow.port

워크플로 서버의 포트 번호입니다.(기본값: 10960)

#### service.entrypoint

Sparrow Enterprise 서버에 접속하기 위해 사용하는 포트를 지정합니다.(기본값: frontend)

#### √ 솔루션 구동 설정

#### service.db.enabled

Sparrow Enterprise 데이터베이스를 구동하는 옵션이며 true, false로 구분합니다.(기본값: true)

#### service.storage.enabled

Sparrow Enterprise에서 사용하는 객체 저장소를 구동하는 옵션이며 true, false로 구분합니다.(기본값: true)

#### service.activemq.enabled

워크플로의 미들웨어로 사용되는 ActiveMQ 서버를 구동하는 옵션이며 true, false로 구분합니다.(기본 값: true)

#### service.frontend.enabled

Sparrow Enterprise 서버의 프론트엔드를 구동하는 옵션이며 true, false로 구분합니다.(기본값: true)

#### service.gateway.enabled

Sparrow Enterprise 서버의 게이트웨이를 구동하는 옵션이며 true, false로 구분합니다.(기본값: true)

#### service.backend.enabled

Sparrow Enterprise 서버의 백엔드를 구동하는 옵션이며 true, false로 구분합니다.(기본값: true)

#### service.broker.enabled

Sparrow Enterprise 서버의 브로커를 구동하는 옵션이며 true, false로 구분합니다.(기본값: true)

#### service.sast.enabled

Sparrow SAST 서버를 구동하는 옵션이며 true, false로 구분합니다.(기본값: true)

#### service.dast.enabled

Sparrow DAST 서버를 구동하는 옵션이며 true, false로 구분합니다.(기본값: true)

#### service.rasp.enabled

Sparrow RASP 서버를 구동하는 옵션이며 true, false로 구분합니다.(기본값: true)

#### service.sca.enabled

Sparrow SCA 서버를 구동하는 옵션이며 true, false로 구분합니다.(기본값: true)

#### service.tso.enabled

Sparrow TSO 서버를 구동하는 옵션이며 true, false로 구분합니다.(기본값: true)

#### service.workflow.enabled

워크플로 서버를 구동하는 옵션이며 true, false로 구분합니다.(기본값: true)

#### service.frontend.https

Sparrow Enterprise 서버의 프론트엔드 프로토콜을 HTTPS로 설정하는 옵션이며 true, false로 구분합니 다.(기본값: true)

#### ✓ 데이터베이스 설정

#### db.home

Sparrow Enterprise 데이터베이스의 홈 디렉토리 경로입니다.(기본값: ./db)

#### db.host

Sparrow Enterprise 데이터베이스의 호스트입니다.(기본값: localhost)

#### db.port

Sparrow Enterprise 데이터베이스의 포트 번호입니다.(기본값: 10620)

#### db.name

Sparrow Enterprise 데이터베이스의 이름입니다.(기본값: sparrow)

#### db.username

Sparrow Enterprise 데이터베이스의 사용자 이름입니다.(기본값: postgres)

#### db.password

Sparrow Enterprise 데이터베이스의 사용자 비밀번호입니다. 설치 후 기본 비밀번호를 변경하는 것을 권 장합니다.(기본값: iXzVzYiX12U3W9X82wbA4w==)

**Tip**: AES-256 알고리즘으로 암호화된 경우 비밀번호가 다르게 표시됩니다. Sparrow Enterprise에서 는 AES-256을 사용하여 프로퍼티 파일의 비밀번호를 암호화합니다.

#### √ 스토리지 설정

#### storage.home

Sparrow Enterprise에서 사용하는 객체 저장소의 홈 디렉토리 경로입니다.(기본값: ./storage)

#### storage.port

Sparrow Enterprise에서 사용하는 객체 저장소의 포트 번호입니다.(기본값: 10621)

#### storage.console.port

Sparrow Enterprise에서 사용하는 객체 저장소의 콘솔 포트 번호입니다.(기본값: 8888)

#### storage.username

Sparrow Enterprise에서 사용하는 객체 저장소의 사용자 이름입니다.(기본값: sparrow)

#### storage.password

Sparrow Enterprise에서 사용하는 객체 저장소의 사용자 비밀번호입니다.(기본값: gLUZGcZAoyhjXtvwBFEd9g==)

#### ✓ ActiveMQ 설정

#### activemq.port

워크플로의 미들웨어로 사용되는 ActiveMQ 서버의 포트 번호입니다.(기본값: 61616)

#### activemq.console.port

워크플로의 미들웨어로 사용되는 ActiveMQ 서버의 콘솔 포트 번호입니다.(기본값: 8161)

#### activemq.username

워크플로의 미들웨어로 사용되는 ActiveMQ 서버의 사용자 이름입니다.(기본값: sparrow)

#### activemq.password

워크플로의 미들웨어로 사용되는 ActiveMQ 서버의 사용자 비밀번호입니다.(기본값:

qRqXD92vMcDFs5BuroCvZtXwKFqCuFF8)

#### √ 기타 설정

#### jre.home

Java 런타임 환경의 홈 디렉토리 경로입니다.(기본값: ./jre)

#### node.home

Node.js 런타임 환경의 홈 디렉토리 경로입니다.(기본값: ./node)

#### √ 보안 설정

#### security.auth.trials.max

사용자 계정에서 비밀번호를 잘못 입력하여 실패한 로그인 시도를 허용하는 횟수입니다. 한 번 로그인하 면 해당 로그인 이전에 시도한 잘못된 로그인 기록은 삭제됩니다.(기본값: 5)

#### security.auth.password.pattern

사용자 계정에서 비밀번호가 만족해야 할 조건입니다. 기본적으로 **영문자, 숫자, 특수문자의 조합으로 이 루어진 최소 9자에서 최대 16자까지의 문자열**로 설정되어 있습니다.(기본값: ^(?\=.\*\\d)(?\=.\*[a-zA-Z])(?\=.\*[^\\da-zA-Z]).{9,16}\$)

#### security.session.age

사용자 세션이 만료되는 시간이며 사용자가 Sparrow Enterprise 서버에 로그인한 시점부터 측정합니다. (단위: ms, 기본값: 86,400,000)

#### security.ip.allowed

Sparrow Enterprise에 접속 가능한 사용자의 IP를 가리키며 하나 이상의 IP를 입력하고 띄어쓰기 없이 쉼 표(,)로 구분할 수 있습니다.

이 옵션에 접속을 허용할 사용자의 IP를 입력하는 경우 해당 IP에서 접속을 요청하지 않는 사용자는 시스 템에 연결할 수 없습니다. 이 옵션에 값을 입력하지 않으면 사용자의 접속을 제한하지 않습니다.

## Sparrow Enterprise 클라이언트 설치하기

Sparrow Enterprise 클라이언트에서는 소스코드 분석과 컴포넌트 분석을 수행할 수 있습니다. 특히 컴포넌 트 분석은 Sparrow Enterprise 서버로 연결된 웹 브라우저에서 직접 명령할 수 없습니다. 따라서 서버를 설 치한 후 Sparrow Enterprise 클라이언트도 설치해야 합니다. 아래를 참고하여 Sparrow Enterprise 클라이언 트를 설치하세요.

**Tip**: **Sparrow Enterprise 클라이언트**는 Windows 환경의 경우 **GUI**와 **CLI**, Linux 계열의 경우 **CLI**를 사용하는 분석을 지원합니다.

<Windows 환경>

- 1. 패키지에 포함된 Sparrow Enterprise CD를 설치할 컴퓨터에 삽입하세요.
- 2. Sparrow Enterprise 클라이언트 경로로 이동하여, sparrow-client-{OS+version}-{YYYYMMDD}.zip 파일을 원하는 영문 디렉토리 경로에 복사한 뒤 압축을 해제하세요.



3. 이제 클라이언트 설치가 완료되었습니다.

<Linux 환경>

- 1. 패키지에 포함된 Sparrow Enterprise CD를 설치할 컴퓨터에 삽입하세요.
- Sparrow Enterprise 클라이언트 경로로 이동하여, sparrow-client-{OS+version}-{YYYYMMDD}.tar.gz 파일을 원하는 영문 디렉토리 경로에 복사한 뒤 압축을 해제하세요.

Warning: root 계정이 아닌 일반 계정으로 Sparrow Enterprise 클라이언트를 설치해야 합니다. 또한, Sparrow Enterprise 클라이언트의 설치 경로에 한글 또는 공백이 포함되어 있으면 정상적으로 설치되 지 않습니다.

3. 이제 클라이언트 설치가 완료되었습니다.

**Sparrow Enterprise 클라이언트**를 사용해서 분석을 시작하려면 소스코드 분석 및 컴포넌트 분석을 참고하 세요.

Sparrow Enterprise 클라이언트 환경 설정하기

클라이언트 GUI의 오른쪽 위에 있는 설정 아이콘을 클릭하면 클라이언트에서 분석에 사용되는 설정을 저장 할 수 있습니다. 여기에서 저장한 내용은 클라이언트 GUI를 사용하여 수행하는 모든 분석에 적용됩니다.

#### ✓ 데이터 관리

#### 분석 임시 파일 경로

분석을 수행할 때 전처리 파일과 같은 임시 파일을 저장하는 위치입니다. **찾아보기** 버튼을 클릭하여 경로 를 선택할 수 있습니다.

#### 분석 후 임시 파일 삭제

분석 임시 파일 경로에 저장된 임시 파일을 분석이 완료된 후 제거하도록 설정하는 옵션이며 예, 아니요 로 구분합니다.

이 옵션을 예로 설정하면 분석이 완료된 후 분석의 임시 파일을 자동으로 삭제합니다. 이 옵션을 아니요 로 설정하면 분석이 완료된 후에도 임시 파일을 삭제하지 않고 그대로 둡니다.(기본값: 아니요)

#### √ IDE 설정

소스코드 분석을 수행할 때 C/C++ 관련 IDE와 연동한 경우 **찾아보기** 버튼을 클릭하여 Visual Studio, Code Warrior, Code Composer Studio, Wind River와 같은 개발 도구의 경로를 설정합니다.

이 옵션에 입력한 값은 소스코드 분석을 수행하기 위해 입력하는 옵션 중 하나인 **IDE 경로**의 기본값으로 입력됩니다. 자세한 내용은 클라이언트 GUI: 소스코드 분석하기를 참고하세요.

## Sparrow 태스크 에이전트 설치하기

태스크 에이전트는 워크플로에서 태스크에 명령을 전달하는 모듈을 가리킵니다.

1. task-agent.jar 파일을 태스크를 실행할 머신의 로컬에 배치하세요.

2. 아래 내용을 참고하여 실행하세요.

```
java -Dsparrow.agent={AGENT_NAME} -Dsparrow.url={GATEWAY_HOST}:{GATEWAY_PORT} -
Dsparrow.username={USER_NAME} -Dsparrow.password={USER_PASSWORD} -
Dsparrow.opt.server.port={AGENT_PORT} -jar task-agent.jar
```

Tip: Java 명령어에서 입력할 때는 옵션 앞에 -D를 붙여야 합니다.

#### sparrow.agent

{AGENT\_NAME}은 태스크 에이전트의 이름이며 64자까지 표시됩니다. 워크플로에서 태스크에 지정 태스 크 에이전트를 선택하거나 워크플로 실행에서 태스크 목록을 표시하는 경우 해당 태스크가 사용한 태스크 에이전트의 이름이 표시됩니다. 자세한 내용은 태스크 추가하기 혹은 워크플로 실행 확인하기를 참고하세 요.(예시: local agent)

#### sparrow.url

{GATEWAY\_HOST}는 HTTP 프로토콜을 포함한 게이트웨이의 호스트 주소이고 {GATEWAY\_PORT}는 게이트웨이의 포트 번호입니다. 게이트웨이는 Sparrow Enterprise 서버를 설치할 때 함께 설치됩니다. SparrowEnterprise 서버의 설정 파일인 sparrow.properties에서 정보를 확인하세요. 자세한 내용은 SparrowEnterprise 프로퍼티 설정하기를 참고하세요.(예시: https://192.168.100.98:10500)

#### sparrow.username

{USER\_NAME}은 태스크 에이전트를 사용하는 사용자의 이름입니다. 이 옵션을 올바르게 입력하지 않은 경우 구동할 수 없습니다.

#### sparrow.password

{USER\_PASSWORD}는 태스크 에이전트를 사용하는 사용자의 비밀번호입니다. 올바르게 입력하지 않은 경 우 구동에 실패합니다.

#### sparrow.opt.server.port

{AGENT\_PORT}는 태스크 에이전트의 포트 번호입니다. 태스크 에이전트에서 사용할 포트를 지정하세요. (예시: 10110)

## 시작하기

## 제품 라이선스 적용하기

Sparrow Enterprise를 사용하기 위해서는 Sparrow Enterprise **제품 라이선스**가 필요합니다. Sparrow Enterprise 제품 라이선스를 적용하는 방법은 다음과 같습니다.

- 1. 웹 브라우저를 여세요.
- 2. \*\*Sparrow Enterprise 서버 URL(https://{Sparrow Enterprise 서버 IP 주소}:{포트 번호})\*\*를 입력하세 요.
- 3. 최고 관리자로 로그인하세요.

Tip: 기본 설정된 최고 관리자 계정의 ID는 admin이며, 비밀번호는 a1234567! 입니다.

4. 최초로 로그인하면 비밀번호를 새로 설정한 후 제품 라이선스를 입력하는 화면이 표시됩니다. 제품 라이선스를 만들기 위해 시스템 ID를 복사하여 스패로우 엔지니어에게 전달하세요.

Sparrow Enterprise
반갑습니다! Spannw를 제집 사용하시 157 제품을 사용하기 위해서는 먼저 제품 라이선스를 제용해야 합니다. 말급받은 제품 라이선스를 입려하세요.
Аста D 2057/50 D
제품 적이선스 * 제품 리아선스를 압력하세요.
세종 타이언스 영업위가

5. 담당자에게서 발급 받은 제품 라이선스 키를 **제품 라이선스**에 입력하고 **제품 라이선스 갱신하기** 버 튼을 클릭하세요.

이미 적용된 제품 라이선스가 무엇인지 확인하려면 제품 라이선스 정보 확인을 참고하세요.

## 로그인하기

Sparrow Enterprise를 사용하기 위해서는 다른 클라이언트보다 먼저 Sparrow Enterprise 서버에 로그인해 야 합니다. 시스템의 인증 및 사용자 관리 권한을 가진 관리자가 설정한 ID와 비밀번호를 입력하여 로그인합 니다. ID와 비밀번호를 알 수 없는 경우 관리자에게 문의하시기 바랍니다.

1. 웹 브라우저를 여세요.

Tip: Sparrow Enterprise는 Google Chrome 웹 브라우저에 최적화되어 있습니다.

2. Sparrow Enterprise 서버 URL(https://{Sparrow Enterprise 서버 IP 주소}:{포트 번호})을 입력하세요.

3. 관리자에게서 전달 받은 사용자 계정 ID와 비밀번호를 입력하고 로그인 버튼을 클릭하세요.

ি Carcon Enterprise
<b>로그인</b> 제3 Stear & Stear DevideoCparts 사위해요 서와 자 * 서와 자 5 전역 전역 생4도. - - - - - - - - - - - - - - - - - - -
사용자 D * 
비밀번호율 강역하세요. 요그것 Copyright (C) 2023 Epuryow Ca., Ma Hights Reserved.

4. 처음 사용자 비밀번호 변경 슬라이드에서 비밀번호를 변경하고 확인 버튼을 클릭하세요.

	처음 사용자 비밀번호 변경 ×
	처음 로그인을 하는 사용자는 비밀번호를 새롭게 변경해야 합니 다.
Sparrow Enterprise	배발전 • 비입번호를 입력하세요. 배달전 유런 • 비입번호를 다시 한 번 입력하세요.
로그인 제3 Smart & Secan DevSecOpeE 41981402	취소하기 <mark>변경적기</mark>
AlBA to * SuperAdmin	
238 	

Tip: 모든 사용자는 최초로 로그인할 때 비밀번호를 새로 설정해야 합니다.

6. 이제 Sparrow Enterprise에 로그인됩니다.

## 새 프로젝트 만들기

Sparrow Enterprise에서는 분석을 묶어서 프로젝트 단위로 저장합니다. 다수의 분석을 수행하는 경우 사용 자가 분석을 프로젝트 단위로 쉽게 구분할 수 있습니다. 프로젝트에는 분석할 소스코드를 비롯하여 분석과 관련된 정보를 모아두었습니다. 따라서 분석을 수행하기 위해서는 이미 생성된 프로젝트를 활용하거나 먼 저 프로젝트를 만들어야 합니다. 시스템의 **프로젝트 관리** 권한이 있는 관리자만 프로젝트를 새로 생성할 수 있습니다. 또한 생성된 프로젝트 의 설정은 나중에 프로젝트 설정에서 다시 수정할 수 있습니다.

1. **마이페이지** 혹은 전체 프로젝트 목록의 오른쪽에 있는 프로젝트 추가하기 버튼을 클릭하세요.



 프로젝트 추가 슬라이드에서 아래를 참고하여 프로젝트 키, 프로젝트 이름을 입력하세요.(\*는 필수 입 력 항목)



3. 추가하기 버튼을 클릭하면 추가한 프로젝트로 이동합니다.

Tip: 이제 필요한 작업에 맞춰 소스코드 분석, 웹 취약점 분석, 컴포넌트 분석, 자가 방어, 테스트 케이 스, 워크플로를 실행하세요.

#### 프로젝트 키\*

프로젝트를 구분하는 키이며 영문, 숫자, 하이픈(-), 밑줄(\_), 마침표(.)로 최대 50자까지 입력할 수 있습니 다. Tip: 프로젝트 이름을 입력하지 않으면 프로젝트 키가 자동으로 프로젝트 이름으로 사용됩니다.

#### 프로젝트 이름

프로젝트의 이름이며 한글, 영문, 숫자, 하이픈(-), 밑줄(\_), 마침표(.), 공백으로 최대 50자까지 입력할 수 있 습니다. 프로젝트 키에 문자를 입력하면 동일한 문자가 자동으로 프로젝트 이름에도 입력됩니다. 다른 프로 젝트 이름을 사용하려면 원하는 이름을 입력하세요.

## 새 작업 시작하기

이제 본격적으로 작업을 시작해봅시다. 먼저, 프로젝트에서 작업을 수행하려면 1) 프로젝트의 **프로젝트 구** 성원으로써 프로젝트 권한 중 2) 작업 수행 권한을 포함한 프로젝트 역할을 가져야 합니다.

#### 작업 프로파일

작업에서 대상을 분석하고, 앱을 보호하고, 테스크 케이스를 확인하는 기준을 **작업 프로파일**이라는 정보에 모아두었습니다. **작업 프로파일**은 시스템의 **작업 및 규칙 관리** 권한을 가진 관리자가 특정 작업에 사용하도 록 미리 설정해둡니다. 사용자는 이렇게 미리 설정한 작업 프로파일을 가져와서 그대로 작업에 적용하기만 하면 됩니다. 프로젝트 구성원으로써 주어진 역할에 따라 작업 프로파일을 사용하세요.

**Tip**: 작업 프로파일을 설정하는 방법은 작업 프로파일 관리하기를 참고하세요.

### 분석

분석은 **전수 분석**과 **수시 분석**으로 구분합니다. 두 분석은 분석 결과를 업데이트하는 방식이 다릅니다. **전수 분석**은 프로젝트에서 이전에 수행한 분석의 결과를 고려하지 않고 해당 분석의 결과만 표시합니다. 따라서 프로젝트를 처음 시작할 때나 최종적으로 마무리할 때 사용하는 것이 좋습니다. 반면, **수시 분석**은 프로젝트 에서 이미 수행한 전수 분석의 결과를 그대로 두고 변경된 결과만 업데이트합니다. 따라서 프로젝트를 진행 하는 도중 변경되거나 추가된 내용을 재확인할 때 사용하는 것이 좋습니다.

Tip: 프로젝트에서 전수 분석을 먼저 수행해야 수시 분석을 수행할 수 있습니다.

#### 소스코드 분석

Sparrow SAST/SAQT에서는 다양한 방법의 소스코드 분석을 지원하고 있습니다. 먼저, 브라우저에서 웹 서 버로 이동하여 간단히 분석을 수행할 수 있습니다. 하지만, 업로드할 수 있는 파일의 형식과 크기에 제한이 있고 개발 환경을 고려하여 분석할 수 없다는 단점이 있습니다. 클라이언트 GUI나 CLI 명령어를 사용하면 개 발 환경에 따른 정확한 결과를 확인하실 수 있습니다. 클라이언트를 사용하려면 Sparrow Enterprise 클라이 언트를 설치하세요. 플러그인을 설치하면 IDE에서 직접 분석을 수행할 수 있습니다. Sparrow Enterprise는 현재 Eclipse, IntelliJ 및 Visual Studio Code 플러그인을 지원합니다. **Tip**: 형상 관리 시스템에 Sparrow Enterprise 연동을 설정하면 파일을 푸시할 때 해당 파일의 해시값 을 확인하여 커밋을 거절하거나 혹은 승인하도록 제어할 수 있습니다. 자세한 내용은 스패로우 엔지 니어에게 문의하세요.

웹 서버에서 소스코드 분석

웹 서버에서 소스코드를 분석하는 방법은 다음과 같습니다.

1. 웹 서버에 로그인하고 분석하려는 프로젝트를 클릭하세요.

🧐 s	99 TestProject TW	лили 🔿 Ф				내무대기 🗸	분성 결과 비고하	다. 지 전역 이런 보기	admin ∨
88	프로젝트키 <u>TestProject_TW</u> 이 · 현태	일 에이컨트 업용 · 마지막 분석 업용 · 방어 미진행				httph/	E d Bri ofredy		
<b>.</b>	Q, 검색어를 입력하세요	♡ 프로제티호					0.09	이스 자사	원포너트
<u></u>	는 파일								840-
Ð	URL	위험도별 이슈 수			상태별 이슈 수				
٢	(E) 4(A.S. NOLA)	© se O			≗ ∞₀ 0	ा ए । २ व्य			
		유형별 이슈 수			기간별 이슈 추이	5 05-19	05-23	<b>양병</b> 05-28	말법 연범 06-04

2. 새 작업 시작하기 버튼을 클릭하세요.

Sparrow Enterprise			새 작업 시작
응용 TestProject () 프로젝트 키 TestProject () · 컨타임	상세 정보 💽 😨	내보네기	프로웨트 * TestProject ·
Q. 검색이를 입력하세요	응 프로젝트 홈		시작할 작업 유형을 선택하세요.
URL	위험도별 이슈 수	상태별 이슈 수	분석을 수행하고 잠재된 보안 취약점 및 품질 문제를 찾 아냅니다. 기존 분석 결과가 새롭게 대체됩니다.
를 테스트케이스	te ore O	© ∞⇔ 0	수시분석           분석율 수행하고 정책된 보안 취약형 및 품질 문제를 찾 아쉽니다. 기존 분석 물과력 추가입니다.           한 전수 문제표 전 수행하요.
	유형별 이슈 수	<b>기간별 이슈 추이</b>	자가 방어           실행 시간 동안 소프트웨어에서 발생하는 보안 취약용을 고니티성됩니다.
		80 60 40 20 0 05-00 05-11 05-15 05-11	대스트 개이스 최적화           변경된 소 2010 양동을 받는 최적의 대스트 개이스 분 찾아냅니다.           ·           ··           ··           ··           ··

3. 전수 분석 또는 수시 분석 카드를 클릭하세요.

Tip: 전수 분석과 수시 분석에 대한 설명은 분석을 참고하세요.

<b>(</b>	parrow Enterprise			작업 프로파일 선택
2 88 89	응응         TestProject         ·            <	) 상세 정보 <b>●                                  </b>	যয়ন্য) ∨	요구해트 TestProject 지갑 유용 진수 분석
8 8 9	ট শথ ⊕ URL	위험도별 이슈 수	상태별 이슈 수	적용할 작업 프로피일을 선택하세요. 작업 프로피일을 선택하면 사전에 설정된 검출 규칙과 작업 옵션이 자동으로 적용됩니다.
۲	臣 4668 1406	8 %⊕ 0	8 110 O	모든 작업과 신승 규식
		유형별 이슈 수	<b>기간별 이슈 추이</b> 100 80 90 40	Rust ANSSI guide v1.0 (97)대적 소프트웨어 전반영왕 담당 목록 (명위·사업철 포당라직) 소프트웨어 방안영왕 전단가이드 2021 (우규영보통산기전·사실 위약형 문석·환기 기존
			0 20 0 05-06 05-11 05-15 05-19	소프트웨어 보안약점 전단가이드 검출 규직 》 © 552 전출 규직

#### 4. **작업 프로파일**을 선택하세요.

**Tip**: **작업 프로파일**은 이슈 검출 규칙과 작업 옵션 등 작업에 필요한 정보를 모아둔 데이터입니다. 자 세한 내용은 <mark>작업 프로파일을</mark> 참고하세요.

S 😵	oarrow Enterprise				◎ 새 전수 분석	역 시작			◎ 새분	년석 <b>분석 대상 선택</b>	×
æ 88	문문제트키 TestProject_TW 이 · 한타양	실세 정보  ② 실세 정보  ③ 에이전트 javaAgent · 마지막분석 업용			프로젝트 TestProject_TW				분석하고지 을 시작하; 할 수도 있	ት 하는 대상의 유행을 선택 기 전에는 자유롭게 변경힐 습니다.	하세요. 선택한 유형은 분석 1 수 있으며 다른 대상을 추가
- <u>-01</u>	Q. 검색어를 입력하세요	88 <u>프로젝트 홈</u>			🗅 분석 대상				<b>E1</b>	압축 파일	*
8	URL	위험도별 이슈 수						분석 대상이 존지	٠	웹 사이트 URL	>>
8	Η 4ΔΕ 494Δ	유형별 이슈 수	8 0(0 0		<ul> <li>・ 休元名名①</li> <li>・ 秋元名名②</li> <li>・ 秋日名○</li> <li>・ 秋日名○</li> <li>・ 秋日名○</li> <li>・ 和日名○</li> <li>・ 和日名○&lt;</li></ul>	· · · · · · · · · · · · · · · · · · ·	사진오. 위원호 2 이미미 - 이미미 - 이미미 - 이미미 - 이미미 - 이미미 - 이미미 - 이미미 -	규칙 이용 ↑ # 쪽은 ## 연년 ## 지시자 사용 #pragma 지시 #undef 지시자 * 및 & 도큰 규 + 및 += 연신 위 + 연신에 사용 += 연신자로 □			

5. 분석 대상 중에서 압축 파일을 선택하세요.

😵 si	oarrow Enterprise					③ 새 전수 분석	1시작		Ø 새분석 분석 대상·	선택	×
*	문제도키 TestProject_TW D · 한다	<ul> <li>상세 정보</li> <li>용세 정보</li> <li>용 (이)전드 javaAgent · 미지막 분석 요)</li> </ul>				프로젝트 TestProject_TW			유형 <b>압축 파일</b> 문석 대상 압축 파일 •		
		8 프로젝트 홈				🗅 분석 대상			i #9	일 여기로 끌어오기 또는 <mark>일 찾아보기</mark>	
e: Q	URL URL	위험도별 이슈 수						분석 대상이 존재			
8		유형별 이슈 수	ê tirê O			① 君舎 규칙 (           Q 검색이들 두           ※ 검색이를 두           ※ 검색지를           ※ 검색지를	· · · · · · · · · · · · · · · · · · ·	규칙 여름 ↑ # 속은 ## 연순 ## 지시자 사용 #pragma 지시 #undef 지시자 * 및 & 도큰 규 + 및 += 연산 + 연산이 사용! += 연산지로 드			
									취소하기	다른 유형 선택하기	선택하기

6. 분석 대상 압축 파일에서 분석할 파일을 끌어오거나 파일 찾아보기를 클릭하여 파일을 선택하세요.

S S	parrow Enterprise					④ 새 전수 분석	시작			에 새 분석 분석 대상 선	택 ×
*	स्टलह ग TestProject         •           महलह ग TestProject         •         स्पन्न ग	상세 정보 <b>() 응</b> 이이전트 일용 · 마지막 분석 일용 · 쌍이				프로젝트 TestProject			I	유형 압축 파일 분석 대상 압추 파일 *	
*		※ 프로젝트 홈				🕒 분석 대상				Enterprise.zip	11 MB ×
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	ि मध • URL	위험도별 이슈 수							분석 대상이 존지	분석 대상 학장자 •	<ul> <li>✓ .aspx (12개 파일)</li> <li>✓ .c (1개 파일)</li> <li>✓ cc (21개 파일)</li> </ul>
۲										<ul> <li>.jsp (3개 파일)</li> </ul>	.m (1개 파일)
			총 이슈 0			① 검출 규칙 @	•			✔ .xml (2개 파일)	✔ .zip (2개 파일)
						Q, 검색어를 두	글자 이상 입력하	세요.			
						유형 ③	언어 💲	위험도 💲	규칙 이름		
						S 소스코드	C++	○ 매우 낮음	# 혹은 ##		
		유영멸 이슈 수				S 소스코드	C++	◎ 낮음	#if 지시지		
						8 소스코드	C++	◎ 낮음	#pragma		
						8 소스코드	C++	◎ 낮음	#undef		
						8 소스코드	C++	○ 매우 낮음	* 및 & 토		
						8 소스코드	Java	이 매우 낮음	+ 및 += 9		
						8 소스코드	C#	<ul> <li>보통</li> </ul>	+ 연산에		
						8 소스코드	C#	<ul> <li>보통</li> </ul>	+= 연산지		
										취소하기	다른 유형 선택하기 <b>선택하기</b>

7. 분석할 언어의 파일 확장자를 선택하세요.

8. **선택하기** 버튼을 클릭하세요.

S 🕲	parrow Enterprise					@ 새전수 분석	시작					×
*	<b>응용 TestProject (</b> 프로젝트키 <u>TestProject</u> <b>()</b> · 관태원	) 상세 정보 <b>() (</b> ) 에이핀드 영웅 · 미지막 분석 영웅 · 방어				프로젝트 TestProject			작업 프로파일 * 모든 작업과 검출 규칙			~
99 	Q. 검색어를 입력하세요	88 프로젝트 홈				🗅 분석 대상						
1 1 1	ig myg ⊕ URL	위험도별 이슈 수				🔐 압축 파일 Enterprise.zip						수정 삭제
۲	語 테스트 케이스		충이슈			① 검출 규칙 @	•				분석 (	대상 추가하기
			U			Q, 검색어를 두	글자 이상 입력하	세요.	필터 🗸	10개씩 보기	1 🗸	열편집 🗸
						유형 () () () () () () () () () () () () ()	언어 () C++	위험도 ()	규칙 이름 ↑ # 혹은 ## 연산자 사용			
		유형별 이슈 수				8 소스코드	C++	◎ 낮음	#if 지시자 사용			
						8 소스코드	C++	∘ ¥8	#pragma 지시자 사용			
						8 소스코드	C++	• 낮음	#undef 지시자 사용			
						8 소스코드	C++	○ 매우 낮음	* 및 & 토큰 규칙 위반			
						8 소스코드	Java	○ 매우 낮음	+ 및 += 연산자로 더해진 문자열			
						8 소스코드	C#	<ul> <li>보통</li> </ul>	+ 연산에 사용된 빈 문자열			
						S 소스코드	C#	● 보통	+= 연산자로 더해진 문자열	취소하기	예약하기	시작하기

9. 시작하기 버튼을 클릭하세요.

**Tip**: 웹 서버에서는 zip 형식의 파일만 분석할 수 있습니다. 나머지 형식의 파일을 분석하려면 클라이 언트 GUI: 소스코드 분석하기 혹은 클라이언트 CLI: 소스코드 분석하기를 참고하세요.

#### 클라이언트 GUI로 소스코드 분석

클라이언트 GUI: 로그인하기

클라이언트 GUI를 실행하기 위해서는 Sparrow Enterprise 클라이언트를 설치해야 합니다. 또한 사용자가 Sparrow Enterprise 서버에 먼저 로그인하지 않았다면 클라이언트에서도 로그인할 수 없습니다.

Warning: Sparrow Enterprise를 처음 사용하는 사용자는 Sparrow Enterprise 서버에 먼저 로그인하 여 비밀번호를 변경한 후, 변경한 비밀번호로 클라이언트에 로그인하세요.

Sparrow Enterprise 클라이언트 GUI에 로그인하는 방법은 다음과 같습니다.

1. \*\*{Sparrow Enterprise 클라이언트 설치 디렉토리}\*\*로 이동하세요.

다. I I I I I I I I I I I I I I I I I I I	rise-client-windov	ws-r157-20	231211			-		× ^ 8
★ 마이 바이	🔜 이동 위지 - 🔝 복사 위지 -	★ 삭제 ■ 이름 구성	바꾸기	세종 만들기	호성 역기	-	문 선택	
← → * ↑	sparro	v 0	,P st	parrow-enterpri	ise-client-w	indows	s-r157-2	20231
OI ∰ ^	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	수정한 날짜 1023-12-12 1023-12-12 1023-12-12 1023-12-12 1023-12-11 1023-12-11	오전 10: 오전 10: 오전 10: 오전 10: 오후 5:3 오후 5:3 오후 5:4	유형 23 파일 볼디 23 파일 볼디 23 파일 볼디 23 파일 볼디 4 Properties 4 Windows 1 응용 프로	원본 파 명령어 그림	르기 56	1KB 1KB ,182KB	
7개 항육								111 K

2. **sparrow-gui.exe** 파일을 실행하세요.

Sparrow Enterprise Client -	×
Sparrow Enterprise	
<b>로그인</b> 지금 Smart & Secure DevSecOps를 시작하세요.	
서버 주소 * 서버 주소를 입력하세요.	
사용자 ID * 사용자 ID를 입력하세요.	
비밀번호 * 비밀번호를 입력하세요.	
Copyright (C) 2023 Sparrow Co., Ltd. All Rights Reserved.	

3. Sparrow Enterprise의 서버 주소, 사용자 ID, 비밀번호를 입력하세요.

 Tip: 서버 주소에는 \*\*https://{Sparrow Enterprise 서버 IP 주소}:{포트 번호}\*\*를 입력해야 합니다.

 Sparrow Enterprise 서버를 기본값으로 설치하신 경우 포트 번호는 10880입니다.

3. **로그인** 버튼을 클릭하세요.

그러면 Sparrow Enterprise 클라이언트 GUI에 로그인하게 됩니다.

클라이언트 GUI: 소스코드 분석하기

클라이언트 GUI를 통해 소스코드를 분석하는 방법은 다음과 같습니다.

1. 클라이언트 GUI의 프로젝트 목록에서 분석할 프로젝트를 선택하거나 새로운 프로젝트를 추가하세 요.

Sparrow Enterprise Client	- 🗆 X
Sparrow Enterprise	⊗ admin ∨
Q, 검색어를 입력하세요	⑦ 프로젝트추가하기 최근 분석순 ✓
88 TestProject	2023-07-31 15:12:49에 생성됨
분석이 없습니다.	+ 새 분석 시작



2. 프로젝트로 이동하세요.

Sparrow Enterprise				8	admin	
Q, 김색어를 입력하세요	5 T	estProject	ß	G 📲	막업 시작하	21
최근 분석순 🔹	·	2141				
88 TestProject	2023	8-12-12 10:38:20				
분석이 없습니다. 🕂 새 분석 시작						
		분석이 존지	위하지 않순	합니다.		
	새작	<b>분석이 존지</b> 업 시작하기 버튼을 클	<b>해하지 않</b> 습 리하여 새로	<b>}니다.</b> 운 분석을 수	행하세요.	
	새 작(	<b>분석이 존지</b> 업 시작하기 버튼을 클	<b>해하지 않</b> 습 리하여 새로	<b>}니다.</b> 운 분석을 수	행하세요.	
	새작	분석이 존재 업 시작하기 버튼을 클	<b>레하지 않</b> ( 리하여 새로	<b>}니다.</b> 운 분석을 수	행하세요.	
	세작	분석이 존지 업 시작하기 버튼을 클	해 <b>하지 않</b> 습	<b>)니다.</b> 운 분석을 수	행하세요.	

3. 새 작업 시작하기 버튼을 클릭하세요.



4. 전수 분석 또는 수시 분석 카드를 클릭하세요.

Tip: 전수 분석과 수시 분석에 대한 설명은 분석을 참고하세요.

		-	
Sparrow Enterprise		작업 프로파일 선택	×
Q, 검색어를 입력하세요	6	프로젝트 TestProject	
비근 분석순 🗸		작업 유형 제소 부서	
82 log_level	-	27 24	
최근 분석 10.47 • @ 원로		적용할 작업 프로파일을 선택하세요. 작업 프로파일	길을 선택하면
# stopped		사전에 설정된 검출 규칙과 작업 옵션이 자동으로 7	적용됩니다.
최근 분석 10.46 • @ 중지			
81 gui		모든 작업과 경출 규칙	>>
최근 분석 10.41 • @ 원로		1111 2,711 검출 규칙 🤫	
# webserver		.NET framework design guideline CWE 65	8.4.7
최근분석 D 8 • 🛞 완료		CWE 659 4.7 CWE 660 4.7	
11 TestProject		JavaScript 시큐어코딩 카이트 2022 MISRA-C	2004
분석이 없습니다. + 세 작업 사작		MISRA-C 2012 MISRA-C++ 2008 OWA	SP 2017
		OWASP 2021 Python 시큐어코딩 가이드 202	2
		Rust ANSSI guide v1.0	
		CONTRACT OF CONTRACT.	

5. 작업 프로파일을 선택하세요.

**Tip**: **작업 프로파일**은 이슈 검출 규칙과 작업 옵션 등 작업에 필요한 정보를 모아둔 데이터입니다. 자 세한 내용은 작업 프로파일을 참고하세요.

Sparrow Enterprise Client		-	• ×
Sparrow Enter @ भा र	연수 분석 시작	분석 대상 선택	×
Q 검색어를 입력하시 프로젝트 지금 분석순	ject	분석하고자 하는 대상의 유형을 선택하세요. 선택한 위 을 시작하기 전에는 자유롭게 변경할 수 있습니다.	<i>루형은 분석</i>
13 TestProject ED 분 의근 분석 ID1 ●	석대상	타일 및 디해토리	*
		🔀 빌드 환경	>>
		Eclipse 프로젝트	>>
		Visual Studio 프로젝트	>>
			취소하기

- 6. 분석하려는 대상에 따라 **파일 및 디렉토리**, **빌드 환경**, **Eclipse 프로젝트**, **Visual Studio 프로젝트** 중 하나를 클릭하세요.
- 7. 파일 및 디렉토리를 선택한 경우 분석 대상에 분석할 파일의 경로를 직접 입력하거나 경로 추가하기 버튼을 클릭하여 폴더를 선택하세요.

Sparrow Enterprise Client		- 0 X
Sparrow Enterp	◎ 새 전수 분석 시작	ଔ 새 분석 분석 대상 선택 ★
Q, 검색어를 입력하지 최근 분석순	프로젝트 TestProject	유형 파일 및 디렉토리 분석 대상 •
St TestProject	🗈 분석 대상	분석 대상 경로를 입력하세요. 여러 개의 경로를 입력할 수 있으며 엔터 혹은 세미콜론(;)으로 구분합니다.
		관로 추가하기         포함된 확장자 확인하기           분석 대상 확장자를         *           한 분석 대상 확장자를 신액하려면 먼저 분석 대상 경로를 입력한 뒤 경로에 보항된 확장지를 확인하세요.
		취소하기 다른 유형 선택하기 <mark>성택하기</mark>

8. 포함된 확장자 확인하기 버튼을 클릭하면 위에서 선택한 파일에 포함된 파일 형식이 분석 대상 확장
 자에 표시됩니다. 그 중에 분석할 파일의 확장자를 선택하고 선택하기 버튼을 클릭하세요.

Sparrow Enterprise Client		- 0 ×
Sparrow Entern	③ 새 전수 분석 시작	@ 새 분석 분석 대상 선택 X
Q 검색어를 입력하지	≝⊋≋s TestProject	유형 파일 및 디렉토리
최근 문역문		C:(Testcode)Enterprise
# TestProject	🗅 분석 대상	
최근 문서 101 •	_	경로 추가하기 도함된 학장자 확인하기
		분석 대상 확장자 *
		✓ .aspx (12개 파일)
		✓ .bat (1개 파일)
		<ul> <li>(1개 파일)</li> </ul>
		✓ .cpp (2개 파일)
		✓ .cs (21개 파일)
		✓ .jsp (3개 파일)
		🔽 .m (1개 파일)
		🗹 .xmi (2개 파일)
		✓ .zip (2개 파일)
		🔽 활장자 업용 (1개 파일)
		취소하기 다른 유형 선택하기 선택하기

 9. 분석하려는 대상이 빌드 환경인 경우 빌드 경로, C/C++ 프리셋, 빌드 명령어, 컴파일러 이름, 컴파일 러 버전, 빌드 실패 무시 등 추가적으로 입력해야 하는 옵션이 표시됩니다. 이 옵션은 컴파일러 혹은 IDE 도구를 미리 설치한 경우에 정상적으로 분석에 사용할 수 있습니다. 자세한 내용은 아래 내용을 참고하세요. 옵션을 입력하고 선택하기 버튼을 클릭하세요. (\*는 필수 입력 항목)

Sparrow Enterprise Client		-	
Sparrow Entern	🝘 새 전수 분석 시작	④ 새 분석 분석 대상 선택	×
Q, 검색어를 입력하시 최근 분석순	프로젝트 TestProject	유형 별드 환경 필드 경로 •	
		빌드 경로를 입력하세요.	찾아보기
18 TestProject 申己 世代 (D.1) ●	🗈 분석 대상	C/C++ 프리넷 •	
		GNU C/C++ 컴파일러	~
		받드 명령어 *	
		빌드 명령어를 입력하세요.	찾아보기
		김짜일러 이름	
		컴파일러 이름을 입력하세요.	
		함파 있어 버전	
		컴파일러 버전을 입력하세요.	
		빌드실패 무시 〇 예 💿 아니오	
		취소하기 다른 유형 선택하기	선택하기

10. 분석 대상으로 Eclipse 프로젝트를 선택한 경우 프로젝트 파일을 선택하고 선택하기 버튼을 클릭하세요.
| Sparrow Enterprise Client      |                     | -                               | o x  |
|--------------------------------|---------------------|---------------------------------|------|
| Sparrow Entern                 | @ 새 전수 분석 시작        | ④ 새 분석 분석 대상 선택                 | ×    |
| Q. 검색어를 입력하세<br>최근 분석순         | 프로젝트<br>TestProject | 유형<br>Eclipse 프로젝트<br>프로젝트 파일 • |      |
| 81 TestProject<br>최근 분석 ID.1 ● | 🗈 분석대상              | 경로를 입착하세요.                      | 찾아보기 |
|                                |                     |                                 |      |
|                                |                     |                                 |      |
|                                |                     |                                 |      |
|                                |                     |                                 |      |
|                                |                     | 취소하기 다른 유형 선택하기                 | 선택하기 |

11. **Visual Studio 프로젝트**를 분석하려는 경우 **프로젝트 파일**, **IDE 경로**, **빌드 구성**을 선택하세요. 이 옵 션은 Visual Studio를 미리 설치한 경우에 정상적으로 분석에 사용할 수 있습니다. 자세한 내용은 아래 내용을 참고하세요. 옵션을 입력하고 **선택하기** 버튼을 클릭하세요. (\*는 필수 입력 항목)

Sparrow Enterprise Client		-	• ×	
Sparrow Entern	🐵 새 전수 분석 시작	④ 새 분석 분석 대상 선택	×	
Q, 검색어를 입력하지 최근 분석순	프로젝트 TestProject	유형 Visual Studio 프로팩트 프로팩트 파일 •		
		경로를 입력하세요.	찾아보기	
31 TestProject	🕒 분석 대상	IDE 경로 •		
NC 24 101		경로를 입력하세요.	찾아보기	
		빌드 구성 •		
		빌드 구성을 입력하세요.	~	
		취소하기 다른 유형 선택하기	선택하기	

- 12. **시작하기** 버튼을 클릭하세요.
- 13. \*\*프로젝트에 대해 분석을 시작하시겠습니까?\*\*라는 메시지에 **시작하기** 버튼을 클릭하면 작업이 시 작됩니다.



#### √ 파일 및 디렉토리

#### 분석 대상\*

취약점 및 품질 문제를 포함하는 이슈를 분석할 대상인 소스코드의 파일 혹은 디렉토리 경로입니다. 분석 을 시작하기 전에 하나 이상의 경로를 입력하고 엔터로 구분할 수 있습니다.

### 분석 대상 확장자\*

분석 대상에 포함된 분석 대상 파일의 확장자이며 하나 이상의 확장자를 선택할 수 있습니다. 이렇게 확 장자를 선택함으로써 분석 대상에 존재하는 파일의 소스코드에서 해당하는 언어만 분석하도록 지정하게 됩 니다.

#### √ 빌드 환경

#### 빌드 경로

C/C++ 언어를 분석하는 경우 사용할 빌드를 수행할 경로입니다. 빌드 경로를 직접 입력하거나, **찾아보기** 버튼을 클릭하여 폴더를 선택할 수 있습니다.

#### C/C++ 프리셋

C/C++ 언어를 분석하는 경우 사용할 프리셋입니다. C/C++ 언어의 컴파일러 혹은 IDE 도구가 프리셋으로 지정되어 있습니다.

현재 버전에서는 GNU C/C++ 컴파일러만 선택할 수 있습니다.

### 빌드 명령어

C/C++ 언어를 분석하는 경우 사용할 빌드 명령어입니다. 빌드 명령어를 직접 입력하거나 **찾아보기** 버튼 을 클릭하여 파일을 선택할 수 있습니다. 선택한 파일은 기본적으로 **exe, bat, com, cmd**와 같은 실행 파일 로 지정됩니다.

#### 컴파일러 이름

빌드 환경에서 사용한 컴파일러의 이름입니다. 특정한 컴파일러를 사용해서 C/C++ 언어의 소스코드를 빌드한 경우 입력하면 됩니다. 이 옵션에 값을 입력하지 않으면 사용자가 입력한 C/C++ 프리셋 옵션에 해당 하는 컴파일러 이름을 사용하게 됩니다.

#### 컴파일러 버전

빌드 환경에서 사용한 컴파일러의 버전입니다. 특정한 컴파일러를 사용해서 C/C++ 언어의 소스코드를 빌드한 경우 입력하면 됩니다. 이 옵션에 값을 입력하지 않으면 사용자가 입력한 C/C++ 프리셋 옵션에 해당 하는 컴파일러 버전을 사용하게 됩니다

#### 빌드 실패 무시

C/C++ 언어를 분석하는 경우 빌드 단계에서 실패가 발생하더라도 분석을 계속 진행하도록 강제하는 분 석 방법을 의미하며 예, 아니요로 구분합니다.

이 옵션을 예로 설정하면 **빌드가 실패하더라도 무시하고 분석을 계속 진행**합니다. 따라서 빌드 실패로 인 해 분석이 실패하지 않게 됩니다. 이 옵션을 아니요로 설정하면 **빌드가 실패하는 경우 자동으로 분석도 실패** 하게 됩니다. 따라서 분석을 수행하지 못할 가능성이 있지만 빌드가 정상적으로 이루어졌는지를 확인할 수 있습니다.(기본값: 아니요)

#### √ Eclipse 프로젝트

#### 프로젝트 파일\*

소스코드를 분석할 Eclipse 프로젝트 파일인 **.project** 파일의 디렉토리 경로입니다. 하나의 경로만 입력할 수 있습니다.

#### ✓ Visual Studio 프로젝트

#### 프로젝트 파일\*

소스코드를 분석할 Visual Studio 프로젝트 파일인 **.project** 파일의 디렉토리 경로입니다. 하나의 경로만 입력할 수 있습니다.

#### IDE 경로\*

**프로젝트 파일** 옵션에 입력한 Visual Studio 프로젝트 파일을 작성한 Visual Studio의 설치 경로입니다. Visual Studio 버전을 다수 설치하고 사용하는 경우 정확한 버전의 Visual Studio를 선택하도록 주의하세요.

이 옵션은 클라이언트 GUI 설정의 **IDE 경로**에서 저장한 값을 자동으로 가져옵니다. 자세한 내용은 Sparrow Enterprise 클라이언트 환경 설정하기를 참고하세요.

#### 빌드 구성\*

Visual Studio 프로젝트 파일을 빌드할 때 구성을 의미합니다. **프로젝트 파일** 혹은 **IDE 경로**를 선택하는 경우 자동으로 입력됩니다.

## 클라이언트 CLI로 소스코드 분석

클라이언트 CLI로 분석을 수행하는 경우 웹 서버를 사용하는 것보다 제한 없이 분석을 수행할 수 있습니다. 또한 클라이언트 GUI와 달리 GUI 기반이 아닌 OS를 사용하는 장치에서 사용하기에 적합합니다. CLI는 클라 이언트 분석 방법 중에 하나이며 Sparrow Enterprise 클라이언트를 설치할 때 함께 설치됩니다. 클라이언트 를 설치하는 방법은 Sparrow Enterprise 클라이언트 설치하기를 참고하세요.

**Tip**: **-h 또는 --help** 옵션과 함께 Sparrow Enterprise 클라이언트 CLI 파일을 실행하면 명령어에 대한 도움말을 확인할 수 있습니다.

#### 클라이언트 CLI: 새 프로젝트 추가하기

Sparrow Enterprise 클라이언트 CLI에서 새로운 프로젝트를 추가하려면 다음을 수행하세요.

- 1. 명령 프롬프트를 실행하세요.
- 2. {Sparrow Enterprise 클라이언트 설치 디렉토리}로 이동하세요.

3. Linux 환경에서는 sparrow-cli 파일과 create project 명령어 및 옵션을 입력하세요.

./sparrow-cli create project -f /home/user/workspace/project.json -s
https://localhost:10880 -u admin -p /home/user/workspace/password.txt

4. Windows 환경에서는 sparrow-cli.cmd 파일과 create project 명령어 및 옵션을 입력하세요.

sparrow-cli.cmd create project -f C:\workspace\project.json -s
https://localhost:10880 -u admin -p C:\workspace\password.txt

5. 아래 내용을 참고하여 옵션을 입력하고 실행하세요.(\*는 필수 입력 항목)

## -f 또는 --file\*

추가할 프로젝트의 설정을 입력한 JSON 파일의 경로입니다. 해당 파일에는 **프로젝트 키(key)**, \*\*프로젝 트 이름(name)\*\*을 다음과 같은 형식으로 입력해야 합니다.(예시: -f {JSON 파일 경로}.json)

```
{
    "key": "myapp",
    "name": "my-application"
}
```

JSON 파일에서 \*\*프로젝트 키(key)\*\*는 필수 입력 항목입니다. \*\*프로젝트 이름(name)\*\*을 입력하지 않으 면 프로젝트 키가 자동으로 프로젝트 이름으로 사용됩니다.

#### -s 또는 --server\*

연결하려는 Sparrow Enterprise 서버의 IP 주소 및 포트 번호입니다.(예시: -s {Sparrow Enterprise 서 버 IP 주소}:{포트 번호})

#### -u 또는 -–user\*

프로젝트를 추가하려는 사용자 계정의 ID입니다.(예시: -u {사용자 ID})

### -p 또는 --password

분석을 수행하려는 사용자 계정의 비밀번호를 저장한 txt 파일의 위치입니다. 이 옵션에 값을 입력하지 않은 경우 사용자 계정의 비밀번호를 입력하라는 메시지가 추가로 표시되며 해당 메시지에 비밀번호를 입력하면 됩니다.(예시: -p {txt 파일 경로})

## 클라이언트 CLI: 소스코드 분석하기

Sparrow Enterprise 클라이언트 CLI에서 분석 작업을 수행하는 방법은 다음과 같습니다.

1. 명령 프롬프트를 실행하세요.

2. {Sparrow Enterprise 클라이언트 설치 디렉토리}로 이동하세요.

3. Linux 환경에서는 sparrow-cli 파일과 create analysis 명령어 및 옵션을 입력하세요.

./sparrow-cli create analysis -k myapp -f /home/user/workspace/sast.json -s
https://localhost:10880 -u admin -p /home/user/workspace/password.txt

4. Windows 환경에서는 sparrow-cli.cmd 파일과 create analysis 명령어 및 옵션을 입력하세요.

sparrow-cli.cmd create analysis -k myapp -f C:\workspace\sast.json -s
https://localhost:10880 -u admin -p C:\workspace\password.txt

5. 아래 내용을 참고하여 옵션을 입력하고 실행하세요.(\*는 필수 입력 항목)

#### -k 또는 --key\*

분석 작업을 수행할 프로젝트의 프로젝트 키입니다.(예시: -k {프로젝트 키})

### -f 또는 --file\*

수행할 분석의 설정을 입력한 JSON 파일의 경로입니다. 해당 파일에는 다음과 같은 정보가 포함되어야 합니다.(예시: -f {JSON 파일 경로})

아래의 형식에서 \*\*작업 유형(type)\*\*은 작업의 유형을 **전수 분석(full)**, **수시 분석(adhoc)** 중 하나로 입 력할 수 있습니다. \*\*작업 프로파일(profile)\*\*은 설정한 작업 프로파일 중 하나를 입력할 수 있습니다. \*\*분 석 대상(targets)\*\*의 \*\*유형(type)\*\*은 파일 및 디렉토리(file), 빌드 환경(build), Eclipse 프로젝트 (eclipse), Visual Studio 프로젝트(vs) 중 하나를 입력할 수 있습니다. 또한, \*\*분석 대상 경로(path)\*\*는 분 석 대상의 절대 경로입니다.

```
{
    "type": "full",
    "profile": "내 작업 프로파일",
    "targets": [{
        "type": "file",
        "path": [
            "C:\\workspace\\src\\all"
        ],
        "extensions": [
            "java", "jsp", "cpp"
        ]
    }]
}
```

분석 대상의 \*\*유형(type)\*\*이 파일 및 디렉토리(file)인 경우 \*\*분석 대상 경로(path)\*\*에 해당하는 파일 이나 폴더를 입력하면 됩니다. \*\*분석 대상 파일 확장자 목록(extentions)\*\*은 분석 대상에 포함된 파일의 확장자를 입력하면 됩니다. \*을 입력하는 경우 모든 확장자에 대해서 분석을 수행합니다.

```
{
    "type": "full",
    "profile": "내 작업 프로파일",
    "targets": [{
        "type": "build"
        "preset": "gnu",
        "buildCommand": "D:\\testcode\\c\\simple\\make.bat",
        "buildPath": "D:\\testcode\\git_testcode\\util\\testcode\\c\\simple",
        "ignoreBuildError": false
    }]
}
```

\*\*유형(type)\*\*이 빌드 환경(build)인 경우 C/C++ 프리셋(preset), 빌드 명령어(buildCommand), 빌드 경로(buildPath), \*\*빌드 실패 무시(ignorebuildError)\*\*를 입력해야 합니다.

```
{

"type": "full",

"profile": "내 작업 프로파일",

"targets" : [{

"type" : "vs",

"path": [

"C:\\testcode\\c\\simple\\build\\simple.vcxproj"

],
```

```
"buildConfiguration" : "Debug|x64",
    "idePath" : "C:\\Program Files (x86)\\Microsoft Visual
Studio\\2022\\Community\\Common7\\IDE\\devenv.com"
    }]
}
```

\*\*유형(type)\*\*이 Visual Studio 프로젝트(vs)인 경우 **분석 대상 경로(path)**, **빌드 구성** (buildConfiguration) 및 \*\*IDE 경로(idePath)\*\*를 입력해야 합니다. 단, \*\*IDE 경로(idePath)\*\*는 devenv.com 파일의 경로를 의미합니다.

```
{
    "type": "full",
    "profile": "내 작업 프로파일",
    "targets": [{
        "type": "eclipse",
        "path": [
            "C:\\workspace\\src\\all\\testProject.project"
        ]
    }]
}
```

\*\*유형(type)\*\*이 Eclipse 프로젝트(eclipse)인 경우 \*\*분석 대상 경로(path)\*\*를 입력해야 합니다.

#### -s 또는 --server\*

연결하려는 Sparrow Enterprise 서버의 IP 주소 및 포트 번호입니다.(예시: -s {Sparrow Enterprise 서 버 IP 주소}:{포트 번호})

## -u 또는 -–user\*

분석을 수행하려는 사용자 계정의 ID입니다.(예시: -u {사용자 ID})

### -p 또는 --password

분석을 수행하려는 사용자 계정의 비밀번호를 저장한 txt 파일의 위치입니다. 이 옵션에 값을 입력하지 않은 경우 사용자 계정의 비밀번호를 입력하라는 메시지가 추가로 표시되며 해당 메시지에 비밀번호를 입력하면 됩니다.(예시: -p {txt 파일 경로})

소스코드 분석에서 검출한 이슈를 확인하려면 소스코드 이슈를 참고하세요.

## 작업 예약

특정 대상을 일정한 시간마다 분석하거나 서버의 부하가 높은 시간을 피해서 분석을 수행하려는 경우 **작업** 예약 기능을 사용할 수 있습니다. Tip: 현재 웹 서버에서만 소스코드 분석과 웹 취약점 분석을 대상으로 작업 예약을 사용할 수 있습니 다.

1. 웹 브라우저에서 분석하려는 프로젝트로 이동하세요.

Testroject_1		테모네가 🗸 분석 물과 비교야.	시 작업 아직 모기 세 작
Q. 검색어를 입력하세요	에 위에이크 프랑 · 에서의 문의 동방 · 영어 이근정	29t	이슈 자산 컴퓨
파일			
URL	위험도별 이슈 수	상태별 이슈 수	
동 데스트 케이스	8 40 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	출 연수 이 전 전 (1995년 1997년 이 전 제공 0.07	
	유형별 이슈 수	기간별 이슈 추이	<mark>일별</mark> 월별 연
		100 80 40 20	
		00 80 40	

2. 새 작업 시작하기 버튼을 클릭하세요.

Sparrow Enterprise			새 작업 시작
응용         TestProject         ●           프로젝트 키         TestProject         ●         현태용	3 상세 정보 <b>()</b> (3) 9 에이전트 일을 · 미지막 분석 일을 · 방어 미진행	હાલનાવગ	Y TestProject >
Q, 검색어를 입력하세요 문 파일	88 프로젝트 홈		시작할 작업 유형을 선택하세요. ③ 전수 분석 》
URL	위험도별 이슈 수	상태별 이슈 수	분석율 수명하고 장재된 보안 취약점 및 품질 문제를 찾 아냅니다. 기존 분석 결과가 새롭게 대체됩니다.
晉 네스트 케이스	**** 0	© % 0	수시분석           분석을 수행되고 휴객은 보인 취약점 및 폭월 단체를 찾 아냅니다. 기존 분석 결과적 추가입니다.           한 운부를 단지 수행해요.
	유형별 이슈 수	<b>기간별 이슈 추이</b>	자가 받어           실행 시간 동안 소프트웨어에서 발생하는 보안 취약됨을 모니타링합니다.
		80 60 40 20 05-08 05-11 05-15 05-15	응         태스트 카이스 직적자           반경된 소스 프트이 영향을 받는 취직의 테스트 케이스 로 찾아냅니다.         유통력 태스트 케이스 문 같아냅니다.

3. 전수 분석 또는 수시 분석 카드를 클릭하세요.

응용         TestProject           프로젝트키         TestProject         ····· 현태	💿 상세 정보 💽 😳	내보내기 🗸	프로젝트 TestProject 자연 유형
Q, 검색어를 입력하세요	88 프로젝트 홈		전수 분석
मध			적용할 작업 프로파일을 선택하세요. 작업 프로파일을 사전에 설정된 검출 규칙과 작업 옵션이 자동으로 적용
	위험도별 이슈 수 8 아아 0	상태별 이슈 수 0	모든 학업과 감율 규칙           © 2,711 강율 규식           MET formework design guideline           CWE 659 47           Coxe 6594 77           Code conventions for the Java Programming La           JanaScript Alexity Mission - 2022           Mission - 2022           Mission - 2023           OWASP 2021           Python Alexity Professor
	유형별 이슈 수	<b>フI간増 이슈 추이</b> 100 40 40	Batt AMSS gude v 10           Ø704# △ ±Ende VE1085 80 4#           월81458 월624           월81459           ▲프트웨어 보면1051 5.001           ◆프트웨어 보면1051 5.001           ▲프트웨어 보면1051 5.001

Tip: 전수 분석과 수시 분석에 대한 설명은 분석을 참고하세요.

4. 작업 프로파일을 선택하세요.

**Tip**: **작업 프로파일**은 이슈 검출 규칙과 작업 옵션 등 작업에 필요한 정보를 모아둔 데이터입니다. 자 세한 내용은 작업 프로파일을 참고하세요.

<b>S</b> •	parrow Enterprise				③ 새 전수 분석	시작		◎ 새분	석 분석 대상 선택	×
~	<b>양 TestProject_TW</b> 표도해도 키 <u>TestProject_TW</u> 이 · 현대임이	<ul> <li>상세 정보</li> <li>양</li> <li>여전드 javaAgent · 마지막 문석 일을</li> </ul>			프로젝트 TestProject_TW			분석하고자 을 시작하기 할 수도 있(	하는 대상의 유행을 선택히   전에는 자유롭게 변경할 = 습니다.	카세요. 선택한 유형은 분석 수 있으며 다른 대상을 추가
<u></u>	<ul> <li>김색어를 입력하세요</li> <li>확일</li> </ul>	88 <u>프로젝트 홈</u>			🗅 분석 대상			<b>i</b>	압축 파일	*
ili Ø	URL	위험도별 이슈 수					분석 대상이 존지	٠	웹 사이트 URL	»
8	₩ 4625 ¥962	유형별 이슈 수	6 016 O		<ul> <li>건설 규칙 《</li> <li>건생이들 두</li> <li>위험 :</li> <li>소스코드</li> </ul>	문자 이상 입력하기 언어 C++ C++ C++ C++ C++ C++ C# C#	국칙 이름 ↑ # 특은 ## 연소 #If 지시자 사원 #pragma 지시 #undef 지시자 * 및 & 도근 규 + 및 += 연산자 + 연산이 사용 += 연산자료 C			

5. **압축 파일** 또는 웹 사이트 URL을 선택하세요.

6. 분석하려는 분석 대상을 선택하거나 입력하고 선택하기 버튼을 클릭하세요.

Tip: 분석 대상에 대한 자세한 내용은 앞에서 설명한 분석을 참고하세요.

row Enterprise					◎ 새 전수 분석	시작				
<b>양 TestProject</b> 프로젝트키 <u>TestProject</u> () · 현태	상세 정보 ● ②           양세 정보         ● ○           1일 에이전트         값을 · · · · · · · · · · · · · · · · · · ·				프로젝트 TestProject			작업 프로피일 • 모든 작업과 검출 규칙	4	
Q 검색어를 입력하세요	88 프로젝트 홈				🕒 분석대상					
ि मध URL	위험도별 이슈 수				🔐 গ্রন্থ মথ Enterprise.zip					수정
응드 테스트 케이스					● 웹사이트 U http://211.39.1	RL 41.177:8080/b	enchmark/Bench	markTest01660.html		수정
		종 이슈 <b>O</b>								분석 대상 추
					① 검출 규칙 🛙	•				
					Q, 검색어를 두	글자 이상 입력히	세요.	필터 🗸	10개씩 보기	~ 열편집
	유형별 이슈 수				유형 💲	언어 💲	위험도 💲	규칙 이름 🔨		
					S 소스코드	C++	○ 매우 낮음	# 혹은 ## 연산자 사용		
				0	S 소스코드	C++	⊙ 낮음	#if 지시자 사용		
				0	S 소스코드	C++	⊙ 낮음	#pragma 지시자 사용		
				0	8 소스코드	C++	◎ 낮음	#undef 지시자 사용		
					8 소스코드	C++	○ 매우 낮음	* 및 & 토큰 규칙 위반		
					S 소스코드	Java	이 매우 낮음	+ 및 += 연산자로 더해진 문자열		

- 7. 예약하기 버튼을 클릭하세요.
- 8. 아래를 참고하여 예약 일시와 반복 주기를 선택하세요.

Sparrow Enterprise					@ 새 전수 분석	시작			작업 예약	
응용 TestProject ( 프로젝트 키 <u>TestProject</u> () · 현태	) 상세 정보 <b>() 양</b> 3 여이전트 일종 - 마지막 문석 일종 - 방어				프로젝트 TestProject				프로젝트 TestProject 예약 일시 *	
Q. 검색여를 입력하세요 문 파일	※ 프로젝트 홈				🗈 분석 대상				예약 일시를 입력하세요. 반복 주기 * 반복 안함	
URL	위험도별 이슈 수				대한 암축 파일 Enterprise.zip					취소하기
行 제소도 케이스					● 웹사이트 UI http://211.39.1	41.177:8080/bi	enchmark/Bench	markTest016		
		<u>ତ</u> ମନ 0								
					<ul> <li>(1) 검출 규칙 @</li> <li>Q. 검색어를 두</li> </ul>	글자 이상 입력히	세요.			
	유형별 이슈 수				유형 ()	언어 🔅	위험도 💲	규칙 이름		
					8 소스코드	C++	이 매우 낮음	# 혹은 ##		
				0	S 4495	C++	○ 낮음	#if 지시지		
				0	S 소스코드	C++	◎ 낮음	#pragma		
				0	8 소스코드	C++	⊙ 낮음	#undef 3		
					8 소스코드	C++	○ 매우 낮음	* 및 & 도		
					-					

9. 예약하기 버튼을 클릭하세요.

## 예약 일시\*

예약한 작업을 처음으로 시작할 일시입니다. 달력에서 예약할 날짜를 선택하면 자동으로 현재 시간이 입 력됩니다. 필요한 경우 시간을 수정한 후에 **확인** 버튼을 클릭하세요.

#### 반복 주기\*

예약한 작업을 반복하는 기간입니다. 반복 안함, 매일, 매주, 매월, 매년 중 하나를 선택하세요.(기본값: 반 복 안함) 분석 예약이 성공하면 프로젝트 상세 정보 페이지에 '**예약된 작업이 있습니다.**'라는 알림 메시지가 표시됩니 다. 해당 알림의 오른쪽에 있는 **예약 모두 보기**를 클릭하여 예약된 작업이 무엇인지 확인할 수 있습니다.





# Eclipse 플러그인

개발 환경에서 Eclipse를 활용하고 있는 경우 웹 서버나 클라이언트 GUI, 클라이언트 CLI를 사용하지 않고 Sparrow Enterprise Eclipse 플러그인을 통해 직접 분석을 수행할 수 있습니다. Eclipse 플러그인은 Sparrow Enterprise 클라이언트를 설치할 때 함께 설치되지 않고 별도로 설치해야 합니다. 다음을 참고하여 Eclipse 플러그인을 설치하세요.

Eclipse 플러그인: 설치하기

Sparrow Enterprise Eclipse 플러그인을 실행하기 위해서는 Sparrow Enterprise 클라이언트와 Sparrow Enterprise 플러그인을 설치해야 합니다. 먼저 Sparrow Enterprise 클라이언트 설치하기를 참고하여 Sparrow Enterprise 클라이언트를 설치한 뒤 다음을 단계를 수행하세요.

1. Eclipse를 실행하세요.

eclipse-workspace - Eclipse IDE		– 🗆 X
File Edit Source Refactor Navigate Search Project Run Window Help		
Image: A state of the state	⇔ → ⇒ →	Quick Access
🛱 Package Explorer 🕱 🖳 🗖	- 8	🗐 Task List 🔀 🗖 🖥
E S Project		
		Find A + All + Activate (?)
		E Outline ⊠ 😜 ⊽ 🗖 🗖
		An outline is not available.
lest Project		🖓 🗢 🎢 🔞 🔝

2. Eclipse에 있는 Help 메뉴에서 \*\*Install New Software...\*\*를 클릭하세요.



3. Install 창이 표시되면 오른쪽 위에 있는 Add... 버튼을 클릭하세요.

<ul> <li>Install</li> </ul>		-	o x
Available Software Select a site or enter the location of a site.			
Work with: <sup>B</sup> type or select a site	~	Add	Manage
type filter text			Select All
Name	Version		Deselect All
			â
Show only the latest versions of available software Group items by category Show only software applicable to target environment Contact all update sites during install to find required software	Hide items that are already installed What is <u>already installed</u> ?		
0	< Back Next >	Finish	Cancel

4. Add Repository 창이 표시되면 Name에 Sparrow Enterprise를 입력하고 Archive... 버튼을 클릭하 세요.

🖨 Add R	epository	×
Name:		Local
Location:	http://	Archive
?	Add	Cancel

5. 다운로드한 Eclipse 플러그인 설치 파일을 선택하고 **열기** 버튼을 클릭하세요.

Repository archive						×
← → • ↑ <mark> </mark> «	Sp	arrow > ENTERPRISE > eclipse	ڻ ~	eclipse 검색		م
구성 ▼ 새 폴더				•	== -	•
💻 LII PC	^	이름	수정형	한 날짜	유형	
🧊 3D 개체		SPARROW_ENTERPRISE_PLUGIN_6.2.0.2	2024	-02-26 오전 9:08	압축(Z	[IP) 파일
🕹 Downloads						
🐺 동영상						
🔮 문서						
🔜 바탕 화면						
📰 사진						
🎝 음악						
🔜 로컬 디스크 (C:)						
🕳 로컬 디스크 (D:)	~	<				>
п	일	이름(N):	~	*.jar;*.zip 열기(O)		~ 취소

6. Add Repository 창에서 Add 버튼을 클릭하세요.

🖨 Add R	epository	×
Name:	Sparrow Enterprise	Local
Location:	[jar:file:/C:/sparrow/ENTERPRISE/plug-in/SPARROW_ENTE]	Archive
?	Add	Cancel

7. SPARROW\_ENTERPRISE\_PLUGIN 체크 박스를 선택하고 Contact all update sites during install to find required software 체크 박스의 선택을 해제한 다음 Next > 버튼을 클릭하세요.

Install			
Available Software Check the items that you wish to install.			
Work with: Sparrow Enterprise - jar.file:/C:/sparrow/ENTERPRISE/plug-in/SP	ARROW_ENTERPRISE_PLUGIN_0.8.1.zipl/	Add	Manage
type filter text			Select All
Name > 🖸 IIII SPARROW_ENTERPRISE_PLUGIN  1 Item selected  Details	Version		Deselect All
Show only the latest versions of available software	Hide items that are already installed		
Group items by category Show only software applicable to target environment Contact all update sites during install to find required software	What is <u>already installed</u> ?		
0	< Back Next >	Finish	Cancel

## 8. Next > 버튼을 클릭하세요.

<ul> <li>Install</li> </ul>		-	• ×
Install Details Review the items to be installed.			
Name	Version 6.2.0.202307041523	ld Sparrow Enterprise.feature.group	
Size: Unknown - Details			~ ~
0	< Back	Next > Finish	Cancel

9. Review Licenses 창에서 I accept the terms of the license agreement를 선택하고 Finish 버튼을 클 릭하세요.

Install			$\times$
Review Licenses		Γ	
Licenses must be reviewed and accepted before the software can be installed.		ø	-
License text (for SPARROW Enterprise Eclipse Plugin 6.2.0.202307041523):			
본 소프트웨어 사용 계약은 귀하에게 제공되는 ㈜스패로우 소프트웨어 제품에 대하여 귀하(개인 혹은 단일 업체)와 ㈜스패로우 간에 체결 소프트웨어 제품에는 컴퓨터 소프트웨어가 포함되며 관련 매제 및 인쇄물 등이 포함될 수 있습니다. 본 소프트웨어 제품에는 ㈜스패로우? 원래의 소프트웨어 제품에 대한 업데이트와 보증물도 포함됩니다. 귀하는 소프트웨어 제품을 설치, 복사 또는 사용함으로써 본 사용 계약 니다. 귀하가 본 사용 계약 조건에 동의하지 않을 경우에는 소프트웨어 제품을 설치하거나 사용할 수 없습니다.	되는 계의 1 귀하에 조건에 8	*입니다. 게 제공한 등의하게 -	× *
* 소프트웨어 제품 사용권 * 본 소프트웨어 제품은 국내 저작권법, 국제 저작권 협약 및 기타 지적 재산권 법률 및 협정에 의해 보호됩니다. 소프트웨어 제품은 판매되 사용이 허가되는 것입니다.	는 것이	아니고 그	L
1. 영토 공지 귀하는 본 소프트웨어 제품을 귀하가 필요로 하는 용도로만 사용할 수 있으며 제 3자에게 양도 또는 전매할 수 없습니다.			
<ol> <li>수정, 리버스 엔지니어링, 디컴파일, 디스어섬블리에 대한 제한 귀하는 소프트웨어 제품을 수정, 리버스 엔지니어링, 디컴파일 또는 디스어섬블 할 수 없습니다.</li> </ol>			
<ol> <li>상표 본 사용 계약서는 귀하에게 뛰스패로우의 상표나 서비스 표시와 관련된 어떤 권리도 부여하지 않습니다.</li> </ol>			
4. 임대 금지 귀하는 본 소프트웨어 제품을 임대, 대부 또는 대여할 수 없습니다.			
5. 해지 귀하가 본 사용 계약을 준수하지 않는 경우, ㈜스패로우는 여타 권리를 침해하지 않고 동 계약을 해지할 수 있습니다. 그러한 경우 귀하는 을 빈납하고 목사본물을 파기하여야 합니다.	본 소프!	트웨어 제	8
6. 저작권 소프트웨어 재풍(소프트웨어 제품에 포함된 모든 화상, 사진, 애니메이션, 비디오, 오디오, 음악, 텍스트 및 "보조 프로그램"을 포함), 부속 어 제품이 봉사보에 대하 소요권 및 저장권으 쓰스클루오 또는 그 공급자가 보요하니다.	인쇄물 9	및 소프트	្
I accept the terms of the license agreement			
O I do not accept the terms of the license agreement			
A Back Next > Finish		Cancel	I

10. Security Warning 창이 표시되면 Install anyway 버튼을 클릭하세요.



11. Software Updates 창이 표시되면 Restart Now 버튼을 클릭하여 Eclipse를 다시 시작하세요.



Tip: 다음과 같이 Trust Artifacts 창이 표시되면 Select All 버튼과 Trust Selected 버튼을 차례로 클 릭하세요.

	Trust Artifacts – 🗆 🗙							
	▲ Do you trust unsigned content of unknown origin?							
	Туре	Id/Fing	erprint	Name		Validity Dates		
	Unsigned	n/a		Unknown		n/a		
I	Always trust all content Deselect All Deselect All							All
	Classifier		Id		Version			
	osgi.bundle		com.sparrow.plugin		6.2.0.2024072223	02		
	org.eclipse.upda	te.fea	Sparrow Enterprise		6.2.0.2024072223	02		
	?					Trust Selected	Cancel	

12. Eclipse 플러그인 설치가 완료되었습니다.

Eclipse 플러그인: 로그인하기

Sparrow Enterprise 웹에 한 번도 로그인하지 않은 사용자 계정은 올바른 사용자 ID와 비밀번호를 입력하더 라도 Eclipse 플러그인과 같은 클라이언트에 로그인할 수 없습니다. 따라서 Sparrow Enterprise 웹에 먼저 로 그인하여 비밀번호를 변경한 후, 변경한 비밀번호로 플러그인에 로그인해야 합니다.

- 1. **Eclipse**를 실행하세요.
- 2. Window 메뉴에서 Preferences를 클릭하세요.

eclipse-workspace - Eclipse IDE					-		$\times$
File Edit Source Refactor Navigate Search Project Run Wi	ndow Help						
📑 • 🖩 💼   🗟 •   🔌 🕸 • 🔿 • 💁 • 🕼	New Window	╸╗╺╬╺┍╸┙╸		[	Quick Access	s]   🖻	<u>ال</u>
😫 Package Explorer 😢 🖳 🗖	Editor Appearance	>	- 8	🗐 Task List 🔀		- 0	
E 😌 🐨 🗸	Show View	>		1 🕈 🛨 🔁	× 👫 🖻	- 15	
Testcode	Perspective	>					@
	Navigation	>		Find 🔍 🖡 All	Activate	) (1	り 🛸
	Preferences						
				E Outline ⊠	<u>6</u> 9 ⊽	- 0	
				An outline is not available	э.		
Test Project					1 🗇 🖉	= 🎢	6

## 3. Preferences 창이 표시되면 Sparrow Enterprise를 선택하세요.

Preferences			— 🗆 X
type filter text	Sparrow Enterprise		← ▼ □ ▼ ▼
<ul> <li>&gt; General</li> <li>&gt; Ant</li> <li>&gt; Code Recommenders Gradle</li> <li>&gt; Help</li> <li>&gt; Install/Update</li> <li>&gt; Java</li> <li>&gt; JSON</li> <li>&gt; Maven Model Editor</li> <li>&gt; Mylyn</li> <li>&gt; Oomph</li> <li>&gt; Plug-in Development</li> <li>&gt; Run/Debug</li> <li>Sparrow Enterprise</li> <li>&gt; Team Validation</li> <li>&gt; XML</li> </ul>	인증 서버 주소 사용자 ID 비밀번호 설정 □ 재시작 시 자동 로그인	서버 주소를 입력하세요. 사용자 ID를 입력하세요. 비밀번호를 입력하세요.	
? 占 🖌 🖲			Apply and Close Cancel

**Tip**: Sparrow Enterprise 클라이언트를 설치하지 않은 경우 다음 메시지에서 **Yes**를 클릭하여 클라이 언트를 설치하세요.



● SPARROW 클라이언트 설치	×
설치가 완료되었습니다.	
	OK

## 4. 서버 주소, 사용자 ID, 비밀번호를 입력하고 로그인 버튼을 클릭하세요.

5. 로그인에 성공하면 Apply and Close 버튼을 클릭하세요.

Preferences			— 🗆 X
type filter text	Sparrow Enterprise		← ▼ □ → ▼
<ul> <li>&gt; General</li> <li>&gt; Ant</li> <li>&gt; Code Recommenders Gradle</li> <li>&gt; Help</li> <li>&gt; Install/Update</li> <li>&gt; Java</li> <li>&gt; JSON</li> <li>&gt; Maven Model Editor</li> <li>&gt; Mylyn</li> <li>&gt; Oomph</li> <li>&gt; Plug-in Development</li> <li>&gt; Run/Debug</li> <li>Sparrow Enterprise</li> <li>&gt; Team Validation</li> <li>&gt; XML</li> </ul>	인증         서버 주소         사용자	https://192.168.10.43:10880 admin (admin) 로그인	로그아웃
? 눱 🖆 🔘			Apply and Close Cancel

Tip: 재시작 시 자동 로그인 체크 박스를 선택하면 Eclipse를 실행할 때 자동으로 로그인하게 됩니다.

7. 이제 Eclipse 플러그인에서 Sparrow Enterprise에 로그인되었습니다.

📬 🕶 🔛 🐚 🛷 🐃 🖬 🌮 🍠 😜	। 🗏 👖 🛊 र 🚺 र 💁 🕬 😥		ə 👻 📑 👘						Q 🗄 😰 👷 😵
Package Explorer ×	E 😫 🕯 🗖 🗖	UntrustedDataInPrivilegedBloc	0 S_4.rs	ND_018.cpp	OrderExceptionsFromDerived	DO_NOT_RELY_ON_THE_DEFAU ×	- 0	Sparrow-Plugin-View ×	
⊨ 😸 External Files a 💕 MyJavaProject		<pre>1 package com.fasoo.sem.TJ 2 3@ import java.io.File;[]</pre>					^	ଓ + ଦ • ₹ • છ	
		14 15 public class DO_NOT_RELY	ON_THE_DEFA	ULT_AUTOMATIC_SI	GNATURE_VERIFICATION_TestCase e	xtends URLClassLoader {		프로젝트 목록	전체 3 프로젝트 〈 1 〉
		16         private URL url;           170         public DO_NOT_RELY_C           18         super(new URL[])           19         this.url = url;	<pre>\_THE_DEFAUL ( url });</pre>	T_AUTOMATIC_SIGN	ATURE_VERIFICATION_TestCase(URL	url) {		Q, 검색어를 입력하세요.	
		20 } 210 @SuppressWarnings("u	checked")					240724testProject	전체 3,134 이슈 🔸 1분 전 🗸 🚿
		22 public void invokeCl 23 throws Class 24 InvocationTa 25 Class c plandel	ass(String r NotFoundExce rgetExceptic	name, String[] ar option, NoSuchMet on {	gs) hodException,			eclipseTest	전제 0 이슈 • 업음 🏈
		25 Class C = load 26 Method m = c.get 27 m.setAccessible(	ass(name); Method("mair true);	", new Class[] {	args.getClass() });			TestProject	전체 348,017 이슈 • 5일 전 🗸 义
		29 if (m.getReturn 30 !!Modifie 31 throw new No	/pe() != voi .isPublic(m SuchMethodE>	d.class    !Modi mods)) { cception("main");	fier.isStatic(mods)				
		32 } 33 try {					- 11		
		34 m.invoke(nul 35 } catch (Illegal	L, new Object AccessExcept	t[] { args }); / tion e) {	* BUG */				
		36 System.out.p	rintln("Acce	ess denied");					
		38 } 390 #SuppressWarnings("u	checked")						
		40 public void invokeCl 41 throws Class	assSafe(Stri	ing name, String[ ntion, NoSuchMet	] args) hodException.				
		42 InvocationTa	getExceptio	n, GeneralSecuri	tyException,				
		44 Class c = loadCl	ass(name);		N CTD (				
		45 Certificate[] ce 46 c.getPro	<pre>ts = /* BUG tectionDomai</pre>	in().getCodeSourc	<pre>RN_SID (null from getCodeSource e().getCertificates();</pre>	)			
		47 if (certs == nul 48 // return, d	<pre>L) { p not execut</pre>	e if unsigned			~		
							>		
		SUT Color							
		border					^		
		sparrow.properties path : C:\	Jsers\ILLURI	~1\AppData\Local	\Temp\sparrow976891451887941713	0.properties			
		BGB {255, 255, 255}							
		RGB {0, 0, 0} SWT Color							
		border							
		browser unsafe							
		RGB {0, 0, 0}							
		SWT Color border							
		browser unsafe							
							~		

Eclipse 플러그인: 프로젝트 추가하기

먼저 분석을 수행할 프로젝트를 추가하겠습니다.

1. **프로젝트 목록** 창에서 **더하기** 아이콘을 클릭하세요.

Sparrow-Plugin-View 🗙	- 8
৫ + დ - ₣ - ֎	
프로젝트 목록	전체 4 프로젝트 < 1 >
Q 검색어를 입력하세요.	
240724_TW	전체 0 이슈 • 없음 ≫
240724testProject	전체 3,134 이슈 🔸 1시간 전 🗸 🏼 🎽
eclipseTest	전체 0 이슈 • 없음 🏼 🚿
TestProject	전체 3,352 이슈 🔸 44분 전 🗸 🚿

2. **프로젝트 키**, **프로젝트 이름**을 입력하세요.

● 새 프로젝트	L _		×
프로젝트 키 *	프로젝트 키를 입	력하세요.	
프로젝트 이름	프로젝트 이름을	입력하세요	
	취소하기	추가하	7

- 3. 추가하기 버튼을 클릭하세요.
- 4. '프로젝트를 생성했습니다.'라는 메시지가 표시되면 OK 버튼을 클릭하세요.

● 새 프로젝트	×
프로젝트를 생성했습니다.	
	ОК

Eclipse 플러그인: 분석하기

이제 Sparrow Enterprise 클라이언트에 연결된 Eclipse 플러그인을 사용하여 소스코드 이슈 및 컴포넌트 이 슈를 분석할 수 있습니다. 분석할 때 프로젝트, 패키지, 파일 등 사용자가 원하는 분석 대상을 선택하여 분석 할 수 있습니다.

1. sparrow-plugin 창의 프로젝트 목록에서 앞서 추가한 프로젝트를 선택하세요.

2. Project 창에서 분석할 대상을 선택하세요.

3. 마우스 오른쪽 버튼을 클릭하세요.

4. SPARROW 분석 시작을 클릭하세요.



5. 작업 유형에서 전수 분석 또는 수시 분석을 선택하세요.



Tip: 전수 분석과 수시 분석에 대한 설명은 분석을 참고하세요.

6. 작업 프로파일을 선택하세요.

**Tip**: **작업 프로파일**은 이슈 검출 규칙과 작업 옵션 등 작업에 필요한 정보를 모아둔 데이터입니다. 자 세한 내용은 작업 프로파일을 참고하세요.

7. 시작하기 버튼을 클릭하세요.

8. 이제 분석이 시작됩니다.

Tip: 분석이 수행되면 로그 창에 분석 로그가 표시됩니다.

Eclipse 플러그인: 결과 확인

분석이 끝나고 결과를 확인하려면 Sparrow-Plugin-View 창의 프로젝트 목록에서 분석을 수행한 프로젝트 를 클릭하세요. 해당 분석의 **이슈 목록**이 표시됩니다. 여기서 이슈에 대한 다양한 정보를 확인할 수 있습니 다.

## ✔ 이슈 목록

😵 Sparrow-Plugin-View 🗙	- 8
ઉ+ ૦- ા - છે	
TestProject	전체 348,017 이슈 🔸 5일 전 🗸
이슈 목록	전체 347,990 이슈 < 24 >
Q 검색어를 입력하세요.	
# <b>1111</b> # 71822 <b>할당 대신 비교 수행</b>	C:\testcode\sast\c\all_case\AllCheck @
#### # 61364 비교 대신 할당 수행	C:\testcode\sast\c\all_case\T.P.Case: @
┃ # 61271 비교 대신 할당 수행	C:\testcode\sast\c\all_case\T.P.Case: @
# <b>####</b> #55361 비교 대신 할당 수행	C:\testcode\sast\c\all_case\AllCheck
#### # 34299 부적절한 cargo 설	정 C:\testcode\sast\configchk\rule\sec @
##### # 34298 부적절한 cargo 설	정 C:\testcode\sast\configchk\rule\sec @
# <b>34297 부적절한 cargo 설</b>	정 C:\testcode\sast\configchk\rule\sec @
# 34296 부적절한 cargo 설	정 C:\testcode\sast\configchk\rule\sec @
■ 6458 취약한 컴포넌트 사용	C:\testcode\sca\cocoapods_src_vuln 🦁 🗌
#6457 <b>취약한 컴포넌트 사용</b>	C:\testcode\sca\cocoapods_src_vuln 🦁 🗌
₩₩₩ #6456 취약한 컴포넌트 사용	C:\testcode\sca\cocoapods_src_vuln 🦁 🗌
┃┃┃┃ # 6455 취약한 컴포넌트 사용	C:\testcode\sca\cocoapods_src_vuln 🦁 🗌
┃ # 6454 취약한 컴포넌트 사용	C:\testcode\sca\cocoapods_src_vuln  😨
┃┃┃┃ = 6453 취약한 컴포넌트 사용	C:\testcode\sca\cocoapods_src_vuln 🦁 🗌
┃┃┃┃ ≡ 6452 취약한 컴포넌트 사용	C:\testcode\sca\cocoapods_src_vuln 🦁 🗌
┃┃┃┃ = 6451 취약한 컴포넌트 사용	C:\testcode\sca\cocoapods_src_vuln 🦁 🗌
#### # 6450 취약한 컴포넌트 사용	C:\testcode\sca\cocoapods_src_vuln 🦁 🗌
┃┃┃┃ ≡ 6449 취약한 컴포넌트 사용	C:\testcode\sca\cocoapods_src_vuln 🦁 🗌
■■■■ # 6448 취약한 컴포넌트 사용	C:\testcode\sca\cocoapods_src_vuln 🦁 🗌

이슈 목록에서는 프로젝트의 최근 이슈 목록을 확인할 수 있습니다. 여기에는 이슈의 **ID**, 유형, 이슈 이름, 이슈가 검출된 **자산**, 위험도, 이슈 상태가 표시됩니다.

## ✔ 소스코드 이슈 상세 정보

검출한 이슈에 대한 정보를 표시합니다.

Sparrow-Plugin-View X			-	
ଓ + ଦ• ୍ ୮ •	0			
TestProject		전체 348,017 이슈	• 5일전 ✓	
🧑 # 347988 XQu	ery 삽입		×	
기본 정보 내비게이티	위험한 예시	안전한 예시		
■■■■ 매우 높음 〈/〉 VB.1	Net 📋 2024-07-18 19	:19:54		
XQuery 삽입 체커는 검증 다. XQuery를 사용하여 XML 값에 대해 적절한 검증 절가 경할 수 있게 됩니다. 이로 할 수 있습니다. 예를 들어 옴표를 사용하여 usemar 위해 삽입된 문자열에 작은 있습니다. " admin' or "= username = 'admin' or 회할 수 있습니다. XQuery에 사용되는 외부 야 합니다.	되지 않은 외부 입력값이 아가 존재하지 않으면 공 인해 허가되지 않은 데이 XQuery 문은 usernan ne과 비교할 문자열을 구 따옴표가 허용되는 경옥 '" 위 문자열을 사용한 쿠 "=" "="은 언제나 true 입력데이터에 대하여 특	포함된 XQuery 구문 리를 생성할 때 사용되 격자가 쿼리문의 구조를  터를 조회하거나 인증 ne='local_user1'과 급 '분합니다. 만약 외부어 2 다음과 같은 문자열을 니리의 조건문은 다음과 이므로 username 비 수문자 및 쿼리 예약어	응 검출합니 등 외부 입력 등 임의로 변 전차를 우회 같이 작은 따 네서 비교를 을 입력할 수 같습니다. 교 자체를 우 를 필터링해	I
이슈 의견을 입력하세요.				
사용자 선택	이전	<b> 확인</b> 확인 해결	다음 이슈	]

소스코드 이슈 상세 정보에는 이슈 검출 규칙에 대한 기본 정보, 검출된 이슈의 소스코드 라인에 대한 설 명인 내비게이터, 해당 이슈에 대한 위험한 예시 및 안전한 예시가 탭으로 표시됩니다.

😵 Sparrow-Plugin-View 🗙	-	
(7 + 40 • ↓≣ • 8	3	
« TestProject	전체 348,017 이슈 🔹 5일 전 🗸	
# 347988 XQue	ry 삽입 X	
기본 정보 내비게이터	위험한 예시 안전한 예시	
분기 표시		
C:\testcode\sast\vb n.vb:7)	된 <b>값이 입력되었습니다.</b> onet\rule\security\XQueryInjection\XQueryInjectio	
C:\testcode\sast\vb n.vb:7)	onet\rule\security\XQueryInjection\XQueryInjectio	
<ul> <li>XQueryExpression (C:\testcode\sast\vb n.vb:10)</li> </ul>	<b>I서 신뢰할 수 없는 값이 사용되었습니다.</b> onet\rule\security\XQueryInjection\XQueryInjectio	
이슈 의견을 입력하세요.		
사용자 선택	이전 미활인 확인 해결 다음이슈	]

## √ 이슈 상태

이슈 상세 정보의 맨 아래에 있는 이슈 톡에서 이슈 담당자를 지정하거나 이슈 상태를 변경할 수 있습니다. 이슈 담당자를 지정하거나 이슈 상태를 변경하려면 1) 프로젝트의 프로젝트 구성원으로써 프로젝트 권한 중 2) 이슈 참여 권한을 포함한 프로젝트 역할을 가져야 합니다.

## 이슈 담당자

해당 이슈를 검토할 담당자를 표시합니다. 권한 있는 사용자 혹은 사용자 그룹 중에서 선택할 수 있으며 담당자를 지정하기 전에는 아무 것도 표시되지 않습니다.

### 이슈 상태

이슈가 검출되면 해당 이슈를 확인하고 해결하거나, 오탐 또는 다른 원인으로 인해 이슈에서 제외하도록 처리해야 합니다. 이슈를 어떻게 처리했는지 표시하기 위해서 이슈마다 **이슈 상태**를 다음과 같이 표시합니 다.

- 미확인 : 담당자가 검출된 이슈를 아직 검토하지 않음
- 확인 : 담당자가 해당 이슈를 확인함
- 해결 : 담당자가 해당 이슈에서 발견된 문제를 해결함

Eclipse 플러그인: 삭제하기

1. Eclipse의 Help 메뉴에서 About Eclipse IDE를 클릭하세요.

2. About Eclipse 창이 표시되면 Installation Details 버튼을 클릭하세요.

3. Sparrow Eclipse Plugin을 선택한 후 Uninstall 버튼을 클릭하세요.

4. Uninstall Details 창에서 Finish 버튼을 클릭하세요.

5. Restart Now 버튼을 클릭하여 Eclipse 플러그인이 삭제되었는지 확인하세요.

6. 로컬에서 Eclipse의 워크스페이스가 있는 경로로 이동하세요.

7. 다음 폴더를 삭제하세요.

{Eclipse 워크스페이스 디렉토리}\.metadata\.plugins\com.sparrow.plugin\sparrow\_client

8. 이제 삭제가 완료되었습니다.

Eclipse 플러그인에서 분석한 소스코드 및 컴포넌트 결과는 웹에서도 확인할 수 있습니다. 자세한 내용은 소 스코드 이슈, 컴포넌트 이슈 및 최근 컴포넌트 확인하기를 참고하세요.

## IntelliJ 플러그인

IntelliJ를 활용하고 있는 사용자라면 **Sparrow Enterprise IntelliJ 플러그인**을 설치해서 웹 서버나 GUI, CLI 클라이언트를 사용하는 것보다 편리하게 분석을 수행할 수 있습니다. IntelliJ 플러그인은 클라이언트를 사용 하는 분석 방법이기 때문에 먼저 클라이언트를 설치해야 합니다. 클라이언트를 설치하는 방법은 <mark>클라이언</mark> 트 설치하기를 참고하세요.

IntelliJ 플러그인: 설치하기

1. IntelliJ를 실행하세요.

2. File 메뉴에서 Settings를 클릭하세요.



3. Settings 창의 Plugin 메뉴를 클릭하고 오른쪽 위에 있는 설정 아이콘을 클릭하세요.

Settings				×
Q.	Plugins	Marketplace	ce installed 🕕 🌣	$\leftarrow \   \rightarrow$
> Appearance & Behavior Keymap	Qr Type / to see options		Manage Plugin Repositories Program: HTTP Proxy Settings	
Editor     Hogins     Version Control	Featured Scala ± 20.1M ♀4.40 JetBrains s.r.o.	Show all	Scala Manage Plugin Certificates     JetBrains s C install Plugin from Disk      Instal     Disable All Downloaded Plugins	
Build, Execution, Deployment     Languages & Frameworks     Tools	AWS Toolkit - Amazon Q, Code ± 6.2M ± 2.42 Amazon Web Service	Install	Cvervlew Wfar s new neveews wadrucitar into	
Settings Sync Advanced Settings	Grazie Pro ≜ 479.8K № 4.79 JetBrains s.r.o.	Install		
	IdeaWim     土 14.6M	install		-
	Solarized Theme ≜ 339.7K ☆ 4.42 Tyler Thrailkill	Install		
	JetBrains Academy ±3.1M ±4.13 JetBrains s.r.o.	Install	Adds support for the Scala language. The following features a	ire
	Key Promoter X ±5.6M ☆4.95 Hal's Corner	Install	Avauable for free with intella IDEA Community Edition:     Coding assistance (highlighting, completion, formatting     refactorings, etc.)	L
	Nord	Install	Navigation, search, information about types and implicit	ts
?			OK Cancel	Apply

4. Install Plugin from Disk..를 클릭하세요.

Choose Plugin File	$\times$
JAR and ZIP archives are accepted	
n ⊟ ⊕ n, n, n, x S G	Hide path
C:\Sparrow\ENTERPRISE\intellij\enterprise_ij_plugin-0.1.20240305000	1.zip 💌
<ul> <li>&gt; PerfLogs</li> <li>&gt; Program Files</li> <li>&gt; Program Files (x86)</li> <li>&gt; Sparrow</li> <li>&gt; DAST</li> <li>&gt; DAST</li> <li>&gt; ENTERPRISE</li> <li>&gt; 231027 dcta</li> <li>&gt; client</li> <li>&gt; eclipse</li> </ul>	
V 🖿 intellij	
<ul> <li>enterprise_ij_plugin-0.1.202403050001.zip</li> <li>runtime-agent</li> <li>server</li> <li>SparrowEnterprise_EventClipboard</li> <li>task-agent</li> <li>tso</li> </ul>	
Prag and drop a file into the space above to quickly locate it OK	Cancel

5. Choose Plugin File 창이 표시되면 경로에서 다운로드한 IntelliJ 플러그인 설치 파일을 선택하고 OK 버튼을 클릭하세요.



6. IntelliJ 플러그인 설치가 완료되었습니다.

Tip: 플러그인을 생성한 주체를 확인하는 Third-Party Plugins Notice 창이 표시되는 경우 Accept 버튼을 클릭하세요. 플러그인의 인증서를 확인하는 Untrusted Server's Certificate 창이 표시되면 Accept 버튼을 클릭하여 플러그인을 실행하세요.





IntelliJ 플러그인: 로그인하기

Sparrow Enterprise 웹에 한 번도 로그인하지 않은 사용자 계정은 올바른 사용자 ID와 비밀번호를 입력하더 라도 IntelliJ 플러그인과 같은 클라이언트에 로그인할 수 없습니다. 따라서 Sparrow Enterprise 웹에 먼저 로 그인하여 비밀번호를 변경한 후, 변경한 비밀번호로 플러그인에 로그인해야 합니다.

1. sparrow-plugin의 설정하러 가기 버튼을 클릭하세요.



2. 혹은 File 메뉴에서 Settings를 클릭하고 Settings 창의 Tools > SPARROW\_Enterprise 메뉴를 클릭 하세요.

Settings				×
Qr.	Tools > SPARROW_Enterprise =		← -	÷
Version Control	인종			
<ul> <li>Build, Execution, Deployment</li> <li>Languages &amp; Frameworks</li> </ul>	서비 주소			
/ Tools Space	사용자 ID			
Qodana Actions on Save	비일번호	879		
Web Browsers and Preview		215		
Terminal III	설정			
Android Device File Explorer Android Emulator	Sparrow 경로	要7		
Code With Me Database inspector				
> Diff & Merge				
Features Trainer				
Logcat Server Certificates				
Shared Indexes				
SPARROW_Enterprise				
Startup Tasks 🖂				
XPath Viewer				
2		K Cancel	Annha	

3. 서버 주소, 사용자 ID, 비밀번호를 입력하고 로그인 버튼을 클릭하세요.

Tip: 설정에서 자동 로그인 체크 박스를 선택하면 IntelliJ를 실행할 때 자동으로 로그인하게 됩니다.

4. SPARROW 경로에서 찾기 버튼을 클릭하세요.

Sparrow Pa	th	×
찾는 위치()):	🖬 sparro240222 🔻 🛋 音 📴 🔡	:
bin conf jre logs output sbuild	☐ sparrow ⊡ sparrow.bak	
물더 이름(N): 파악 요형(TD):	C:#Sparrow#ENTERPRISE#client#sparrow-enterprise-client-windows-r233-20240222	
파일 유영(U):	열기 취	* *

5. 로컬에 설치된 Sparrow Enterprise 클라이언트 경로를 선택하고 열기를 클릭하세요.

Settings				×
Q.		Tools > SPARROW_Enterprise = Reset	÷	$\rightarrow$
Plugins	14	0.5		
> Version Control	8	L 8		
> Build, Execution, Deployment		서비 주소 https://192.168.100.98:10880		
Languages & Frameworks				
		사용자 admin (Superadmin)		
Space				
Qodana		로그아웃		
Actions on Save	*			
Web Browsers and Preview		설정		
External Tools		☑ 재시작 시 자동 로그인		
Terminal	ж.	Snamnw 3 E ISnamnw#ENTERDRISE#client#cnamnw.enternise.client.windows.c240.20240220		
Android Device File Explorer		abarrow Size _ abarrow and a second state and a		
Android Emulator				
Code With Me				
Database Inspector				
> Diff & Merge				
Features Suggester				
Features Trainer				
Logcat				
Server Certificates				
Shared indexes				
SPARROW_Enterprise				
Startup Tasks	Ξ			
> Tasks	н			
?		OK Cancel	Apply	

6. **OK** 버튼을 클릭하세요.

7. 이제 IntelliJ 플러그인에서 Sparrow Enterprise에 로그인되었습니다.

IntelliJ 플러그인: 프로젝트 추가하기

먼저 분석을 수행할 프로젝트를 추가하겠습니다.

1. sparrow-plugin 창의 프로젝트 목록에서 더하기 아이콘을 클릭하세요.

2. 프로젝트 키, 프로젝트 이름을 입력하세요.

3. 추가하기 버튼을 클릭하세요.

IntelliJ 플러그인: 분석하기

이제 Sparrow Enterprise 클라이언트에 연결된 IntelliJ 플러그인을 사용하여 소스코드 이슈 및 컴포넌트 이슈 를 분석할 수 있습니다. 분석할 때 프로젝트, 패키지, 파일 등 사용자가 원하는 분석 대상을 선택하여 분석할 수 있습니다.

1. sparrow-plugin 창의 프로젝트 목록에서 앞서 추가한 프로젝트를 선택하세요.

2. Project 창에서 분석할 대상을 선택하세요.

3. 마우스 오른쪽 버튼을 클릭하세요.



4. Run SPARROW을 클릭하세요.

🔛 새 작업 시작		×
작업 유형	전수 분석	-
작업 프로파일	모든 작업과 검출 규칙	-
	취소하기	시작하기

5. 작업 유형에서 전수 분석 또는 수시 분석을 선택하세요.

Tip: 전수 분석과 수시 분석에 대한 설명은 분석을 참고하세요.

6. 작업 프로파일을 선택하세요.

**Tip**: **작업 프로파일**은 이슈 검출 규칙과 작업 옵션 등 작업에 필요한 정보를 모아둔 데이터입니다. 자 세한 내용은 작업 프로파일을 참고하세요.

7. 시작하기 버튼을 클릭하세요.

8. 이제 분석이 시작됩니다.

Tip: 분석이 수행되면 로그 창에 분석 로그가 표시됩니다.

IntelliJ 플러그인: 결과 확인

분석이 끝나고 결과를 확인하려면 sparrow-plugin 창의 프로젝트 목록에서 분석을 수행한 프로젝트를 클 릭하세요. 해당 분석의 **이슈 목록**이 표시됩니다. 여기서 이슈에 대한 다양한 정보를 확인할 수 있습니다.

✔ 이슈 목록

sparrow-	plugin			\$ −
(J)	o, ↓,	۲		
«	TestProj	iect	전체 78,618 이슈 + 3시간	2 전 5
이슈	목록		전체 78,543 이슈 < 1	>
Q	검색어를 입력	력하세요.		
	#3434311	#pragma 지시자 사용	C:\Testcode\SAST\testcode\c\a	•
	#3434310	#pragma 지시자 사용	C:\Testcode\SAST\testcode\c\a	•
	#7530061	* 및 & 토큰 규칙 위반	c-simple/sample.c	•
	#7530060	* 및 & 토큰 규칙 위반	c-simple/sample.c	•
	#7530059	* 및 & 토큰 규칙 위반	c-simple/sample.c	•
100	#7530058	* 및 & 토큰 규칙 위반	c-simple/sample.c	•
	#7530057	* 및 & 토큰 규칙 위반	c-simple/sample.c	•
1000	#7530056	* 및 & 토큰 규칙 위반	c-simple/sample.c	•
••••	#7530055	* 및 & 토큰 규칙 위반	c-simple/sample.c	•
••••	#7530054	* 및 & 토큰 규칙 위반	c-simple/sample.c	•
••••	#7530053	* 및 & 토큰 규칙 위반	c-simple/sample.c	•
••••	#7530052	* 및 & 토큰 규칙 위반	c-simple/sample.c	•
•	#7530051	* 및 & 토큰 규칙 위반	c-simple/sample.c	•
••••	#7530050	* 및 & 토큰 규칙 위반	c-simple/sample.c	•
••••	#7530049	* 및 & 토큰 규칙 위반	c-simple/sample.c	•
•	#7530048	* 및 & 토큰 규칙 위반	c-simple/sample.c	•
••••	#7530047	* 및 & 토큰 규칙 위반	c-simple/sample.c	•
•••••	#7530046	* 및 & 토큰 규칙 위반	c-simple/sample.c	•
••••	#7530045	* 및 & 토큰 규칙 위반	c-simple/sample.c	•
	#7530044	* 및 & 토큰 규칙 위반	c-simple/sample.c	<b>(</b> )

이슈 목록에서는 프로젝트의 최근 이슈 목록을 확인할 수 있습니다. 여기에는 이슈의 **ID**, **유형**, **이슈 이름**, 이슈가 검출된 **자산**, **위험도**, 이슈 상태가 표시됩니다.

## ✔ 소스코드 이슈 상세 정보

검출한 이슈에 대한 정보를 표시합니다.

sparrow-plugin	☆ —
G + ©, ↓, ⊗	
TestProject	전체 78,618 이슈 , 3시간 전 😒
# 7530331 XQuery 삽입	×
기본정보 내비게이터 위험한 예시	안전한 예시
태해해 배우높음  ASP	:48:41
XQuery 삽입 체커는 검증되지 않은 외부 입력값	t이 포함된 XQuery 구문을 검출합니
XQuery를 사용하여 XML 데이터에 대한 동적 쿠 값에 대해 적절한 검증 절차가 존재하지 않으면 킁 경할 수 있게 됩니다. 이로 인해 허가되지 않은 데 할 수 있습니다. 예를 들어 XQuery 문은 userna 옴표를 사용하여 username과 비교할 문자열을 위해 삽입된 문자열에 작은 따옴표가 허용되는 걸 있습니다. " admin' or "=' " 위 문자열을 사용한 username = 'admin' or "=" "="은 언제나 tru 회할 수 있습니다. XQuery에 사용되는 외부 입력 데이터에 대하여 야 합니다.	워리를 생성할 때 사용되는 외부 입력 공격자가 쿼리문의 구조를 임의로 변 l이터를 조회하거나 인증 절차를 우회 ame='local_user1' 과 같이 작은 따 구분합니다. 만약 외부에서 비교를 경우 다음과 같은 문자열을 입력할 수 · 쿼리의 조건문은 다음과 같습니다. e이므로 username 비교 자체를 우 특수문자 및 쿼리 예약어를 필터링해
이슈 의견을 입력하세요.	
사용자 선택 이전	<b>미확인</b> 확인 해결 <b>다음 이슈</b>

소스코드 이슈 상세 정보에는 이슈 검출 규칙에 대한 기본 정보, 검출된 이슈의 소스코드 라인에 대한 설 명인 내비게이터, 해당 이슈에 대한 위험한 예시 및 안전한 예시가 탭으로 표시됩니다.
sparrow-plugin	\$ −
ଓ + ବ୍ା୍ ଭ	
TestProject	전체 78,618 이슈 🔹 3시간 전 🔭
# 7530331 XQuery 삽입	×
기본 정보 내비게이터 위험한 예시	안전한 예시
분기 표시	
추적 규칙 옵션에 따라 클래스 HiddenField 적하기 시작합니다. (XQueryInjectionASPNETText.cs:64)	l의 속성 Value을 검출하였으므로 추
추적 중인 값이 pass에 지정되었습니다. (XQueryInjectionASPNETText.cs:64)	
추적 중인 값이 문자열 연결에 사용되었으므 (XQueryInjectionASPNETText.cs:66)	로 해당 결과값을 추적합니다.
추적 중인 값이 squery에 지정되었습니다. (XQueryInjectionASPNETText.cs:66)	
중적 중인 값 squery이 클래스 StreamRea 용되었으므로 초기화되는 객체 new System (XQueryInjectionASPNETText.cs:74)	ider 생성자의 1번째 매개변수에 사 m.IO.StreamReader을 추적합니다.
추적 중인 값이 query에 지정되었습니다. (XQueryInjectionASPNETText.cs:74)	
추적 중인 값 query이 메소드 StreamRead 사용되었으므로 해당 반환값을 추적합니다. (XQueryInjectionASPNETText.cs:77)	ler.ReadToEnd()의 베이스 객체에
<ul> <li>추적 중인 값이 메소드 XQueryCompiler.C 되었으므로 추적 규칙을 위반했습니다. (XQueryInjectionASPNETText.cs:77)</li> </ul>	compile()의 1번째 매개변수로 사용
이슈 의견을 입력하세요.	
사용자 선택 이전	<b>미확인</b> 확인 해결 <b>다음이슈</b>

## √ 이슈 상태

이슈 상세 정보의 맨 아래에 있는 이슈 톡에서 이슈 담당자를 지정하거나 이슈 상태를 변경할 수 있습니다. 이슈 담당자를 지정하거나 이슈 상태를 변경하려면 1) 프로젝트의 프로젝트 구성원으로써 프로젝트 권한 중 2) 이슈 참여 권한을 포함한 프로젝트 역할을 가져야 합니다.

## 이슈 담당자

해당 이슈를 검토할 담당자를 표시합니다. 권한 있는 사용자 혹은 사용자 그룹 중에서 선택할 수 있으며 담당자를 지정하기 전에는 아무 것도 표시되지 않습니다.

#### 이슈 상태

이슈가 검출되면 해당 이슈를 확인하고 해결하거나, 오탐 또는 다른 원인으로 인해 이슈에서 제외하도록 처리해야 합니다. 이슈를 어떻게 처리했는지 표시하기 위해서 이슈마다 **이슈 상태**를 다음과 같이 표시합니 다.

- 미확인 : 담당자가 검출된 이슈를 아직 검토하지 않음
- 확인 : 담당자가 해당 이슈를 확인함
- 해결 : 담당자가 해당 이슈에서 발견된 문제를 해결함

## IntelliJ 플러그인: 삭제하기

1. IntelliJ의 File 메뉴에서 Settings를 클릭하세요.

<u>N</u> ew >	LdapInjectionTest.m				<u>토</u> - <	Current File 💌 🕨 🕸 🖏 🖊	- 1
Open	🕸 — 🍭 CNF	S_004.cpp × 🗯 FormatString.m × 🗯 LdapinjectionTest.m ×	:	sparrow-p	plugin		
Close Project	^.m file	s are supported in other JetBrains IDEs	Try CLion Try IntelliJ IDEA Ultimate Dismiss	0 +	0, ₹, 8		
Settings Ctrl+Alt+S	53	if (err == LDAP_SUCCESS)	<b>≈</b> 10 ^ ~		TestDesiset	700 70 000 004	
Project Structure Ctrl+Alt+Shift+S	54	{		~	restProject	신제 78,018 이유 + 3	340.0
File Properties >	55	NSLog(@" TLS established");					_
Local History	56	} else {		이슈 문	목록	전체 78,543 이슈 〈	1
Save All Ctrl+S	57	<pre>ldap_get_option( ld, LDAP_OPT_DIAGNOSTIC_MESSAGE, (v</pre>	oid*)&msg);				
Reload All from Disk Ctrl+Alt+Y	58	NSLog(@" ldap_start_tls_s(): %s", ldap_err2string(	err));	Q 2	넘색어를 입력하세요.		
Repair IDE		NSLog(@" ssl/tls: %s", msg);					
Invalidate Caches	60	ldap_memfree(msg);			= 7538373 사용되지 많은 시	,역 민수 aspnet/CheckerUnitTest/XPi	Pat
Manage IDE Settings >				( m	= 7530372 안전하지 않은 로	경 aspnet/CheckerUnitTest/XPathin	njec
New Projects Setup >	62	r,					
Save File as rempjate	64	NSLog(@" Bind Data:"):			#7530371 예외 정보 노출 :	aspnet/CheckerUnitTest/XPathInjectic	ion
Export /		NSLog(@" Mech: Simple"):			#7530370 지나치게 일반적(	?! 예외 처리 aspnet/CheckerUnitTer	est/.
Power Save Mede		NSLog(@" DN: %s", bindDN ? bindDN : "(NULL)");					
rowel save moue	67	NSLog(@" Passwd: %s", bindPW ? bindPW : "(NULL)");		( <b></b>	#7530369 사용되지 않은 지	역 변수 aspnet/CheckerUnitTest/XP	Pat
Qui	68				= 7538368 아저하지 아유 큰	21 asnnet/Checkerl InitTest/XPathin	nier
	69	NSLog(@" binding to LDAP server");			1.220200 15/20141 18/2 12	B ashietoneoverontrestiveating	ile.
	70	cred.bv_val = bindPW ? <u>strdup(bindPW)</u> : NULL;			#7530367 <b>예외 정보 노출</b> :	aspnet/CheckerUnitTest/XPathInjectic	tion
	71	<pre>cred.bv_len = bindPW ? (size_t) strlen("drowssap") : 0;</pre>					
		err = ldap_sasl_bind_s(ld, bindDN, LDAP_SASL_SIMPLE, &cre	d, NULL, NULL, &servercredp);		# /538366 시나시게 일반적당	진 예외 서리 aspnet/UneckerUnities	.st/.
		if (err != LDAP_SUCCESS)		(† <b>1</b> 00 - 2	#7530365 사용되지 않은 지	역 변수 aspnet/CheckerUnitTest/We	/eal
	75	NSLog(@" ldap_sasl_bind_s(): %s", ldap_err2string(err	));		#7530364 빈 catch 블록 #	aspnet/CheckerUnitTest/WeakPasswo	VOFC
		<pre>cdap_undind_ext_s(id, NULL, NULL);</pre>			= 7538363 사용되지 않은 지	역 변수 aspnet/CheckerUnitTest/Wr	leal
	77	recom a;					
		r,			= 7530362 빈 catch 블록 :	aspnet/CheckerUnitTest/WeakPasswc	IOR
	80	NSLog(@" initiating lookup"):			+7520261 ILBCITI 0/9 TL	DINEL scoot/Chacked InitTert/Lin	0784
	81	if ((err = ldap_search_ext_s(ld, baseDN, scope. filter. N	ULL, 0, NULL, NULL, NULL, -1, &res))) //@violation		- / / / / / / / / / / / / / / / / / / /	elelel ashard accelenting the	in wei
	82	{		- mii -	#7530360 사용되지 않은 파	라이터 aspnet/CheckerUnitTest/Unr	1re:
	83	NSLog(@" ldap_search_ext_s(): %s", ldap_err2string(er	r));				
	84	<pre>ldap_unbind_ext_s(ld, NULL, NULL);</pre>			= /538359 사용되지 않은 시	.왜 법수 aspnet/CheckerUnitTest/Sar	and
	85	return 0;		1 mil 2	= 7538358 변수에 대해 Equ	als 사용 aspnet/CheckerUnitTest/Re	Reli
	86	};					
	87				= 7538357 HttpOnly가 아닌	] 꾸키 aspnet/CheckerUnitTest/Pers	sis
	88	return 0;		100	= 7538356 HttpOnly7+ 0H-	· · · · · · · · · · · · · · · · · · ·	rsis
	89	8					
					= 7538355 HttpOnly가 아닌	년 쿠키 aspnet/CheckerUnitTest/Pers	rsis

- 2. Settings 창이 표시되면 Plugin > SPARROW Enterprise로 이동하세요.
- 3. 오른쪽 위에 있는 토글을 클릭한 후 Uninstall 버튼을 클릭하세요.



4. Plugin Uninstall 창에서 Yes 버튼을 클릭하세요.

•	Uninstall Plugin	×
	Are you sure you want to uninstall the plugin	
	'SPARROW_ENTERPRISE'?	
	Yes No	

- 5. **OK** 버튼을 클릭하여 IntelliJ 플러그인을 삭제하세요.
- 6. 이제 삭제가 완료되었습니다.

## Visual Stuido Code 플러그인

개발 단계에서 Visual Stuido Code를 주로 사용하신다면 Visual Stuido Code 플러그인을 설치해서 간단하게 분석을 수행할 수 있습니다. Visual Stuido Code 플러그인은 클라이언트를 사용하는 분석 방법이기 때문에 먼저 클라이언트를 설치해야 합니다. 클라이언트를 설치하는 방법은 <mark>클라이언트 설치하기를</mark> 참고하세요.

Visual Stuido Code 플러그인: 설치하기

- 1. Visual Stuido Code를 실행하세요.
- 2. 왼쪽 사이드 메뉴에서 확장 아이콘을 클릭하세요.

3. 더보기 아이콘을 클릭하고 VSIX에서 설치를 클릭하세요.

∢	파일(F) 핀	편집(E) 선택 영역(S) 보기(V) ···· ← →		٦Q	Testcode	
þ	확장		ა	C <sup>e</sup> Author	rizationBypassSqlASPNE	TTest.cs ×
	마켓플	플레이스에서 확장 검색	=×	보기	>	Test > C AuthorizationBypassSqIASPNETTest.cs
Q				확장 업데이트	트 확인	WETCODY: ASD NET Convorton modulo */
	~ 길지금			확장 자동 업!	데이트 >	14-18-06 20:19:25 */
୍ବର		Korean Language Pack for Visual Studio Code 하국어			0	(*************************************
	Y	Microsoft		보는 확장 시대		C:\Users\fasoo-ybj\Desktop\aspnet\benchmark\b
æ		· · · · · · · · · · · · · · · · · · ·		설지된 모든 4	확장 사용 안 암	code with additional engine options white o
_		Markdown All in One All you need to write Markdown (keyboard shortcuts, table of so	onton	실행 중인 확	장 표시	owers */
		Yu Zhang	Jitten	확장 이동분 /	시작	
				VSIX에서 설치	tl	
	(M+)	Markdown PDF Convert Markdown to PDF		12	using System	Dilections.Generic;
	PDF	vzane	8	13	using System.	Ling;
		,		14	using System.	Net;
	9	Pylance		15	using System.	Web;
		A performant, feature-rich language server for Python in VS Cod	de	16	using System.	Web.Helpers;
	-	Microsoft	63	17	using System.	Web.Security;
		Python		18	using System.	Web.UI;
		Python language support with extension access points for Intelli	iSense (	19	using System.	Web.WebPages;
		Microsoft	-	20	using System.	Web.Mvc.Aiax:
				22	using System.	Web.Mvc.Html:
		Python Debugger		23	using System.	Web.Routing;
		Python Debugger extension using debugpy.	<b>C</b> 2	24	using System.	Data.Odbc;
		WICTOSOTC	-634	25	using System.	Data.SqlClient;
	∨ 권장		4	26		
	*	<b>P</b> 1		27	public class	SqlInjectionTest : Account.Login {
	ي الله	Docker 0 33	3.2M ★ 4.5	28	Utta	at Baswatt
	docker	Makes it easy to create, manage, and debug containenzed applic	cations.	29	HttpRespo	st Request;
	_	WICIOSOT	[ 2신 ]	31	neepkespo	nse kesponse,
Ø		GitLens — Git supercharged 🛛 🗘	31.5M ★ 4	32	public Sq	<pre>lInjectionTest() {</pre>
Ø		Supercharge Git within VS Code — Visualize code authorship at	a glanc	33	}	
572		SitKraken	[설치 ] 🗸	34		
503	*	markdownlint 🗠 6	18M 🛨 45	35	void Butte	onClickBad(object sender, string connect, Event
× -	⊗ 0 ∆ 0	% 0		26		줄 1, 열 1 공백:4 UTF-8 CRLF C# 💭

4. Sparrow Enterprise 플러그인 파일을 선택하세요.

X Install from VSIX			×
← → ✓ ↑ 🧾 « 로컬 디스크 (C:) > Sparrow > ENTERPRIS	E > vscode ~ ⊘	vscode 검색	,
구성 👻 새 물더		<b>1</b> 11 •	• 🔳 🔞
및 내 PC 이를	수정한 날짜	유형	크기
🧊 3D 개제 📓 vscode-plugin-0.0.6.vsix	2024-05-01 오후 3:15	Microsoft Visual	14,608KB
Downloads			
📓 동영상			
🔁 문서			
🔜 바탕 화면			
📰 사진			
> 음악			
_ 로컬 디스크 (C:)			
🔜 로컬 디스크 (D:			
- HE03 Y			
파일 이름(N):	~	VSIX Extensions (*.v	six) 🗸
		install	취소

- 5. 플러그인이 설치되면 Visual Stuido Code를 다시 시작하세요
- 6. 설치가 완료되었습니다.

Visual Stuido Code 플러그인: 로그인하기

Sparrow Enterprise 웹에 한 번도 로그인하지 않은 사용자 계정은 올바른 사용자 ID와 비밀번호를 입력하더 라도 Visual Stuido Code 플러그인과 같은 클라이언트에 로그인할 수 없습니다. 따라서 Sparrow Enterprise 웹에 먼저 로그인하여 비밀번호를 변경한 후, 변경한 비밀번호로 플러그인에 로그인해야 합니다.

1. **파일 탐색기** 창에서 가장 아래에 있는 SPARROW ENTERPRISE 섹션을 펼치세요.



2. SPARROW ENTERPRISE 섹션에서 설정하러 가기를 클릭하세요.

•	() + დ ∳ (მ) >
《 설정	
서버 주소 *	
서버 주소를 입력하세요.	
사용자 ID *	
사용자 ID를 입력하세요.	
비밀번호 *	
비밀번호를 입력하세요.	
📄 재시작 시 자동 로그인	로그인
Sparrow 클라이언트 설치 경로	
경로를 입력하세요.	찾아보기

3. 서버 주소, 사용자 ID, 비밀번호를 입력하고 로그인 버튼을 클릭하세요.

**Tip**: **재시작 시 자동 로그인** 체크 박스를 선택하면 Visual Stuido Code를 실행할 때 자동으로 로그인 하게 됩니다.

4. Sparrow 클라이언트 설치 경로에서 찾아보기 버튼을 클릭하세요.

🗙 폴더 선택						Х
← → • ↑ 📙 « Sp	parrow > ENTERPRISE > client > sparrow-enter	prise-client-windows-r263-2	20240430	✓ Ö sparrow-enterprise-	client-win	Q
구성 ▼ 새 폴더						?
TW-106 ^	이름 ^	수정한 날짜	유형	크기		
- vscode	bin	2024-05-01 오후 3:39	파일 쫄더			
작업 메시지	🔄 conf	2024-05-01 오후 3:39	파일 폴더			
	📙 jre	2024-05-01 오후 3:39	파일 폴더			
Onebine	📙 sbuild	2024-05-01 오후 3:39	파일 폴더			
OneDrive						
💻 LII PC						
🧊 3D 개체						
🕹 Downloads						
📕 동영상						
🔮 문서						
🔜 바탕 화면						
▶ 사진						
▶ 음악						
🔜 로컬 디스크 (C:) 🗸						
폴더	sparrow-enterprise-client-windows-r263-202404	30				
= 1.	· · · · · · · · · · · · · · · · · · ·			Coloct Coorrow Directory	치스	-
			2	select sparrow Directory	41 <u>-</u> 2	

5. 로컬에 설치된 Sparrow Enterprise 클라이언트 경로를 선택하고 Sparrow 경로 선택을 클릭하세요.

6. 이제 Visual Stuido Code 플러그인에서 Sparrow Enterprise에 로그인되었습니다.

Visual Stuido Code 플러그인: 프로젝트 추가하기

먼저 분석을 수행할 프로젝트를 추가하겠습니다.

1. SPARROW ENTERPRISE 섹션의 프로젝트 목록에서 더하기 아이콘을 클릭하세요.

2. **프로젝트 키**, **프로젝트 이름**을 입력하세요.

$\sim$ spar	ROW ENTERPRISE	G	+	•	↓F	۲
~	프로젝트 추가					
프로젝	트 키 •					
프로	젝트 키를 입력하세요.					
프로젝	트 이름					
프로	젝트 이름을 입력하세요.					
프로 <sup>8</sup> 다	!트 이름을 입력하지 않으면 프로젝트 키가 자동으로 프로젝. 추	트 이름	1	은 사용 추기	응됩니	-1

3. 추가하기 버튼을 클릭하세요.

Visual Stuido Code 플러그인: 분석하기

이제 Sparrow Enterprise 클라이언트에 연결된 Visual Stuido Code 플러그인을 사용하여 소스코드 이슈 및 컴포넌트 이슈를 분석할 수 있습니다. 분석할 때 프로젝트, 패키지, 파일 등 사용자가 원하는 분석 대상을 선 택하여 분석할 수 있습니다.

1. SPARROW ENTERPRISE 섹션의 프로젝트 목록에서 앞서 추가한 프로젝트를 선택하세요.

<pre>C sample x  Trengrine c imple &gt; C sample.&gt; 00 double_free_complex_sublist ') 280 void double_free_main() { 280 free(head); /* BUG:DOUBLE_FREE */ 281 } 282 283 void double_free_complex_subl(list *p) { 286 free(c-&gt;ptr) { 287 } 288 void double_free_complex_subl(list *p) { 289 void double_free_complex_main() { 291     List *head; 292     head - (List *palloc(sizeof(List)); 293     if (lnead) { 294</pre>			●           ●       ● <th>값 + ● 분 분 ● &gt;           전체 78,618 여승 · 3×1건 건 · ·           전체 78,643 여승 · 3×1건 건 · ·           전체 78,643 여승 · (1)           전체 78,643 여승 · (1)           값은 지역 변수 appret/DeckerUnitest/0781binged           값은 지역 변수 appret/DeckerUnitest/0781binged           값은 지역 변수 appret/DeckerUnitest/0781binged           값 2 3 appret/DeckerUnitest/0781binged           값 2 3</th>	값 + ● 분 분 ● >           전체 78,618 여승 · 3×1건 건 · ·           전체 78,643 여승 · 3×1건 건 · ·           전체 78,643 여승 · (1)           전체 78,643 여승 · (1)           값은 지역 변수 appret/DeckerUnitest/0781binged           값은 지역 변수 appret/DeckerUnitest/0781binged           값은 지역 변수 appret/DeckerUnitest/0781binged           값 2 3 appret/DeckerUnitest/0781binged           값 2 3
<pre>chapters &gt; C sample &gt; C double_free_complex_subdist ') 288 vold double_free_main() { 280 281 } 282 282 284 vold double_free_complex_sub(list *p) } 285 285 //free(rowship) /* BUG:DOUBLE_FREE */ 286 vold double_free_complex_sub(list *p) } 287 //free(rowship) //  288 vold double_free_complex_sub(list *p) } 289 vold double_free_complex_main() { 290 vold double_free_complex_main() { 291 //  292 //free(rowship) //  293 //f (head) ( 293 //f (head) //  294 //  294 //  294 //  295 //f (head) //f (hea</pre>		Nggananan Mgananan Sanan Sananan Sanan Sanan Sanan Sanan Sanan Sanan Sanan Sanan Sanan Sanan Sanan Sanan Sanan Sanan S	《 TestProject 이슈 목록 Q 김네이를 입력하셔요. 비비 #753877 사용되지 ( 비비 #753877 예정 정보 100 # 753877 예정 정보	원제 78,618 여승 - 3시간 전 - 원제 78,543 여승 < 1 > 전원 78,543 여승 < 1 > 전원 포킹 aspnet/DieckerUniTest/XPathinged @ 전원 포킹 aspnet/DieckerUniTest/XPathingedIon(1 @ 도움 aspnet/DieckerUniTest/XPathingedIon(1 @
<pre>281 } 282 283 284 void double_free_complex_sub(List *p) [] 285 if (universe) 286 if (universe) 287 [ free(p-); 287 [ free(p); ] 289 void double_free_complex_main() { 291 List *head; 292 head + (List *)malloc(sizeof(List)); 293 if (lnead) { 294 [ exit(1); 294 ] </pre>			이슈 목록 Q. 검색이를 인덕하세요. ()) = 7538373 사용되지 { ()) = 7538372 안전하지 { ()) = 7538371 예외 정보	전체 78,543 이슈 《 1 》 같은 지역 변수 aspret(DirectorUniTest/Path) 응 ( 같은 포깅 aspret(DirectorUniTest/Pathispect) 응 ( 노출 aspret(DirectorUniTest/Pathispect) 유 ( )
<pre>295</pre>			비비         #73050         사용되지           비비         #73050         연단하지           비비         #750806         여에 정보           비비         #750806         지나지케           비비         #750806         신요지지           비비         #750806         신요지지           비비         #750806         신요지지	월입학원 역에 치리 appretCheckerUnitTestX07 6 ( 응은 지원 년 수 appretCheckerUnitTestX078th) 6 ( 응은 포원 appretCheckerUnitTestX078th) 6 ( 일양원원 역에 치리 appretCheckerUnitTestX078th) 6 ( 양양원원 역에 치리 appretCheckerUnitTestX0484P 6 ( 응용 지역 변수 appretCheckerUnitTestWeakP 6 ( 응용 지역 변수 appretCheckerUnitTestWeakP 6 ( 응용 지역 변수 appretCheckerUnitTestWeakP 6 ( 응용 appretCheckerUnitTestWeakPappresson) 6 ( 용용 appretCheckerUnitTestWeakPappresso
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS	C#	× ≡ A … ^ × i	#####################################	않은 파라미너 aspnet/CheckerUnitTest/Unrestr 🧐
Installing parkage - nazor Language Server (elemetry (windows / x04) Finished			·····································	않은 시역 변수 aspnet/CheckerUnitTest/Sanitiz @
Using dotnet configured on PATH			######################################	/가 아닌 쿠키 aspnet/CheckerUnitTest/Persiste 🧑 🗌
Dotnet path: C:\Program Files\dotnet\dotnet.exe Activating C# + C# Dev Kit			=7538356 HttpOnly	<b>/가 아닌 쿠키</b> aspnet/CheckerUnitTest/Persiste 🐽 🗌
waiting for named pipe information from server [stdout] {"pipeName":"\\\.\pipe\\5db3eae9"}			######################################	/가 아닌 쿠키 aspnet/CheckerUnitTest/Persiste 💩 🗌
received named pipe information from server attempting to connect client to server client has connected to server life of 4:53:29 PM] [Program] Language server initialized			···· = 7530354 사용되지 (	않은 파라미터 aspnet/CheckerUnitTest/HitpRe: 🛞 🗌
	<pre>index_iptr = (int *)walloc(sizeof(int) * 10); if (free(head); if (ree(head); if (ree(head);</pre>	<pre>idead-ptr = (it *)malloc(sizeof(int) * 10); if (itea-ptr); if</pre>	Jack-Str:       (free(head);         Jing (dead-Str:)       (free(head); <td>image: pice (-pice -)pice (</td>	image: pice (-pice -)pice (

- 2. Visual Stuido Code의 **탐색기** 창에서 분석할 대상을 선택하세요.
- 3. 마우스 오른쪽 버튼을 클릭하세요.

ile Edit Selection View Go	o Run Terminal Help	$\leftrightarrow \rightarrow$	,⊘ Testcode			0	
EXPLORER ····	C sample.c ×			•⊳~ © □ …			ც + • № მ :
TESTCODE     idea	Enterprise > c-simple > C sample.c > 🖓 double 268 void double_free_main() { 280 free(bead): /* BUG:DOUBLE E	free_complex_sub(List *)			« TestPr	oject	전체 78,618 이슈 + 3시간 전 🐂
Jos     Enterprise     java     osca_hash_testset     SAST	281 } New File New Folder Pauval in Eile Evolgener Shift+ Alt+P	//////////////////////////////////////			<b>이슈 목록</b> 〇, 검색어를 입	역하세요.	전체 78,543 이슈 〈 1 ›
> SCA > sparrow	Open in Integrated Terminal			TErturnen.	#111 #3434311	#pragma 지시자 사용 Criti	estcode\SAST\testcode\c\all_ 😐 🕘
> util_testcode-main Enterprise.zip	Find in Folder Shift+Alt+F	1			# 7538961	* 및 & 토크 규칙 위반 c-sim	rstcode\SAST\testcode\c\all_ 00 (
<ul> <li>osca_hash_testset.zip</li> <li>sparrow.zip</li> </ul>	Cut Ctrl+X Copy Ctrl+C	f(List));			#7530066	*및&토콘규칙위반 c-sim	pie/sample.c
util_testcode-main.zip	Paste Ctrl+V			The reader	#7530059	* 및 & 토큰 규칙 위반 c-sim	ple/sample.c
	Copy Path Shift+Alt+C Copy Relative Path Ctrl+K Ctrl+Shift+C	<pre>izeof(int) * 10);</pre>		Column Column	#7530058	* 및 & 토콘 규칙 위반 o-sim	ple/sample.c
	Run Tests			<u>.</u>	#7530057	* 및 & 토큰 규칙 위반 c-sim	ple/sample.c
	Rename F2	d); REE */		Northan an Northann Martine Martine	#7530055	· 및 & 토큰 규칙 위반 c-sim	ple/sample.c
	Delete Delete			Tools	#7530054	* 및 & 토콘 규칙 위반 c-sim	ple/sample.c
	Run SPARROW Analysis			Weiner Weiner	#7530053	* 및 & 토큰 규칙 위반 c-sim	ple/sample.c 💿
	308 free(p->ptr); /* BUG:USE_AP 309 }	TER_FREE */		No. of Concession, No. of Conces	#7530052	* 및 & 토큰 규칙 위반 c-sim	ple/sample.c
	310 311 ///////////////////////////////////			Mineral Minera	#7530051	*및&도근 규칙 위반 o-sim	ple/sample.c 00
	PROBLEMS OUTPUT DEBUG CONSOLE TERMI INSCALLING PACKAGE RAZOF LANGUAGE SE	NAL PORTS IVEF TELEMEETY (WINDOWS / X04)	C# ~	≡ A … ^ ×	#7538049	* 및 & 토큰 규칙 위반 c-sim	ple/sample.c
	Finished				<b> </b>      #7538048	* 및 & 토큰 규칙 위반 c-sim	ple/sample.c
> OUTLINE	Using dotnet configured on PATH	datnat ava			#7538047	* 및 & 토콘 규칙 위반 c-sim	ple/sample.c 💿 🗌
> TIMELINE V SOLUTION EXPLORER	Activating C# + C# Dev Kit waiting for named pipe information fr	om server			# 7530046	* 및 & 토큰 규칙 위반 c-sim	ple/sample.c 00
<ul> <li>ConsoleApp1</li> <li>ConsoleApp1 (not su</li> </ul>	<pre>[stdout] {"pipeName":"\\\.\pipe\\5d received named pipe information from attempting to connect client to server client has connected to server</pre>	b3eae9"} server r			**************************************	· · x & 또는 규칙 위반 c-sim	ple/sample.c 0

4. Run SPARROW Analysis를 클릭하세요.

•	(3 ≠ 40 ≠ 50 ×
TestProject	전체 78,618 이슈 🔹 3시간 전 🔭
새 작업 시작	×
직업 유형 *	
전수 분석	~
작업 프로파일 •	
모든 작업과 검출 규칙	~
	취소하기 시작하기

5. 작업 유형에서 전수 분석 또는 수시 분석을 선택하세요.

Tip: 전수 분석과 수시 분석에 대한 설명은 분석을 참고하세요.

6. 작업 프로파일을 선택하세요.

**Tip**: **작업 프로파일**은 이슈 검출 규칙과 작업 옵션 등 작업에 필요한 정보를 모아둔 데이터입니다. 자 세한 내용은 작업 프로파일을 참고하세요.

7. 시작하기 버튼을 클릭하세요.

8. 이제 분석이 시작됩니다.

Tip: 분석이 수행되면 출력 창에 분석 로그가 표시됩니다.

Visual Stuido Code 플러그인: 결과 확인

분석이 끝나고 결과를 확인하려면 **SPARROW ENTERPRISE** 섹션의 **프로젝트 목록**에서 분석을 수행한 프로 젝트를 클릭하세요. 해당 분석의 **이슈 목록**이 표시됩니다. 여기서 이슈에 대한 다양한 정보를 확인할 수 있 습니다.

✓ 이슈 목록

۲		() ₹ Φ + 5	$\times$
«	TestPro	ject 전체 78,618 이슈 - 3시간 전	r.
이슈	목록	전체 78,543 이슈 < 1	>
Q	검색어를 입호	벽하세요.	
	#7530373	사용되지 않은 지역 변수 aspnet/CheckerUnitTest/XPathli @	
n in	#7530372	안전하지 않은 로깅 aspnet/CheckerUnitTest/XPathInjecti 🥑	!
	#7530371	예외 정보 노출 aspnet/CheckerUnitTest/XPathInjectionA5 @	
	#7530370	지나치게 일반적인 예외 처리 aspnet/CheckerUnitTest/XF 🧔	
	#7530369	사용되지 않은 지역 변수 aspnet/CheckerUnitTest/XPathlr 🥝	
1111	#7530368	안전하지 않은 로깅 aspnet/CheckerUnitTest/XPathInjecti 🤷	
	#7530367	예외 정보 노출 aspnet/CheckerUnitTest/XPathInjectionAs 🧑	
	#7530366	지나치게 일반적인 예외 처리 aspnet/CheckerUnitTest/XF @	
	#7530365	사용되지 않은 지역 변수 aspnet/CheckerUnitTest/WeakP 🧑	
	#7530364	빈 catch 블록 aspnet/CheckerUnitTest/WeakPasswordR @	
	#7530363	사용되지 않은 지역 변수 aspnet/CheckerUnitTest/WeakP 🤫	
	#7530362	빈 catch 블록 aspnet/CheckerUnitTest/WeakPasswordR	
	#7530361	사용되지 않은 파라미터 aspnet/CheckerUnitTest/Unrestr @	
	#7530360	사용되지 않은 파라미터 aspnet/CheckerUnitTest/Unrestr 🤷	
	#7530359	사용되지 않은 지역 변수 aspnet/CheckerUnitTest/Sanitiz @	
	#7530358	변수에 대해 Equals 사용 aspnet/CheckerUnitTest/Relian 🧓	
	#7530357	HttpOnly가 아닌 쿠키 aspnet/CheckerUnitTest/Persiste 🧑	
	#7530356	HttpOnly가 아닌 쿠키 aspnet/CheckerUnitTest/Persiste 🥑	
	#7530355	HttpOnly가 아닌 쿠키 aspnet/CheckerUnitTest/Persiste 🥑	
	#7530354	사용되지 않은 파라미터 aspnet/CheckerUnitTest/HttpRe:	

이슈 목록에서는 프로젝트의 최근 이슈 목록을 확인할 수 있습니다. 여기에는 이슈의 **ID**, **유형**, **이슈 이름**, 이슈가 검출된 **자산**, **위험도**, 이슈 상태가 표시됩니다.

## √ 소스코드 이슈 상세 정보

검출한 이슈에 대한 정보를 표시합니다.

	(3 + 40 ₽ (8) ×
TestProject	전체 78,618 이슈 + 3시간 전 ***
🧑 # 7530331 XQuery 삽입	×
기본정보 내비게이터 위험한 예시	안전한 예시
₩₩₩ 매우 높음 〈/〉 ASP 芭 2024-06-04 10	:48:41
XQuery 삽입 체커는 검증되지 않은 외부 입력긻 다.	)이 포함된 XQuery 구문을 검출합니
지. XQuery를 사용하여 XML 데이터에 대한 동적 류 값에 대해 적절한 검증 절차가 존재하지 않으면 문 경할 수 있습니다. 예를 들어 XQuery 문은 userna 홈표를 사용하여 username과 비교할 문자열을 위해 삽입된 문자열에 작은 따옴표가 허용되는 경 있습니다. " admin' or "=" "위 문자열을 사용한 username = 'admin' or "=" "="은 언제나 tru 회할 수 있습니다. XQuery에 사용되는 외부 입력 데이터에 대하여 야 합니다.	리리를 생성할 때 사용되는 외부 입력 공격자가 쿼리문의 구조를 임의로 변 ll이터를 조회하거나 인증 절차를 우회 ame='local_user1' 과 같이 작은 따 구분합니다. 만약 외부에서 비교를 경우 다음과 같은 문자열을 입력할 수 러리의 조건문은 다음과 같습니다. we이므로 username 비교 자체를 우
이슈 의견을 입력하세요.	
사용자 선택 이전	미확인 확인 해결 다음이슈

소스코드 이슈 상세 정보에는 이슈 검출 규칙에 대한 기본 정보, 검출된 이슈의 소스코드 라인에 대한 설명인 내비게이터, 해당 이슈에 대한 위험한 예시 및 안전한 예시가 탭으로 표시됩니다.

()         ()
≪ TestProject 전체 78,618 이슈 · 3시간 전 →
# 7530331 XQuery 삽입 ×
기본 정보 내비계이터 위험한 예시 안전한 예시
분기표시
<ul> <li>추적 규칙 옵션에 따라 클래스 HiddenField의 속성 Value을 검출하였으므로 추 적하기 시작합니다. (XQueryInjectionASPNETText.cs:64)</li> </ul>
중적 중인 값이 pass에 지정되었습니다. (XQueryInjectionASPNETText.cs:64)
추적 중인 값이 문자열 연결에 사용되었으므로 해당 결과값을 추적합니다. (XQueryInjectionASPNETText.cs:66)
<ul> <li>추적 중인 값이 squery에 지정되었습니다.</li> <li>(XQueryInjectionASPNETText.cs:66)</li> </ul>
★적 중인 값 squery이 클래스 StreamReader 생성자의 1번째 매개변수에 사용되었으므로 초기화되는 객체 new System.IO.StreamReader을 추적합니다. (XQueryInjectionASPNETText.cs:74)
<ul> <li>추적 중인 값이 query에 지정되었습니다.</li> <li>(XQueryInjectionASPNETText.cs:74)</li> </ul>
추적 중인 값 query이 메소드 StreamReader.ReadToEnd()의 베이스 객체에 사용되었으므로 해당 반환값을 추적합니다. (XQueryInjectionASPNETText.cs:77)
<ul> <li>추적 중인 값이 메소드 XQueryCompiler.Compile()의 1번째 매개변수로 사용 되었으므로 추적 규칙을 위반했습니다. (XQueryInjectionASPNETText.cs:77)</li> </ul>
이슈 의견을 입력하세요.
사용자 선택 이전 <b>미확인</b> 확인 해결 <b>다음 이슈</b>

## √ 이슈 상태

이슈 상세 정보의 맨 아래에 있는 이슈 톡에서 이슈 담당자를 지정하거나 이슈 상태를 변경할 수 있습니다. 이슈 담당자를 지정하거나 이슈 상태를 변경하려면 1) 프로젝트의 프로젝트 구성원으로써 프로젝트 권한 중 2) 이슈 참여 권한을 포함한 프로젝트 역할을 가져야 합니다.

## 이슈 담당자

해당 이슈를 검토할 담당자를 표시합니다. 권한 있는 사용자 혹은 사용자 그룹 중에서 선택할 수 있으며 담당자를 지정하기 전에는 아무 것도 표시되지 않습니다.

#### 이슈 상태

이슈가 검출되면 해당 이슈를 확인하고 해결하거나, 오탐 또는 다른 원인으로 인해 이슈에서 제외하도록 처리해야 합니다. 이슈를 어떻게 처리했는지 표시하기 위해서 이슈마다 **이슈 상태**를 다음과 같이 표시합니 다.

- 미확인 : 담당자가 검출된 이슈를 아직 검토하지 않음
- 확인 : 담당자가 해당 이슈를 확인함
- 해결 : 담당자가 해당 이슈에서 발견된 문제를 해결함

Visual Stuido Code 플러그인: 삭제하기

- 1. 왼쪽 사이드 메뉴에서 확장 아이콘을 클릭하세요.
- 2. Sparrow Enterprise를 클릭하세요.



3. 오른쪽 창에서 제거 버튼을 클릭하세요.

4. 이제 삭제가 완료되었습니다.

## 분석 중지하기

수행 중인 분석을 종료하려면 1) 프로젝트의 **프로젝트 구성원**으로써 프로젝트 권한 중 2) **작업 관리** 권한을 포함한 프로젝트 역할을 가져야 합니다. 자세한 내용은 다음을 참고하세요.

1. 프로젝트 상세 정보의 오른쪽 위에 있는 작업 이력 보기 버튼을 클릭하세요.

			^
🖀 🛗 🛗 🛗	상제 정보 💽 🔅	Q, 검색아를 두 글자 이상 입력하세요. 웹터 🗸	목록 내보내기 식지하기 20개씩 보기 > 일편집 >
프로젝트 키 <u>TestProject</u> 한 · 런타임 에이전	전드 javaAgent · 마지막문석 <u>2분전 %</u> · 방어 <u>3시간전</u> %	직업ID \$ 유형 \$	작업 상태 💲 작업자 💲 작업 시작 일시 🤟
· 영 · · · · · · · · · · · · · · · · · ·	이슈 또는 컴포넌트 정보가 변경될 수 있습니다.	1620 (% 수시 분석	<b>52%</b> a 2024-06-04 13:29:37
<u>eo0</u>		1613 ① 자가방어	수행중 a 2024-06-04 10:16:54
문 Q, 검색어를 입력하세요	응 프로젝트 홈	전체 2 작업 1 - 2 표시됨	1         페이지 이동         →
	위험도별 이슈 수 (78,613) 비해 대우 표 1.3% (0.04) (78,613) 비해 모두 표 1.3% (0.04) (19,15) 변화 1.5% (7.473) (19,119) 면화 1.5% (7.473) (19,119		

2. 진행 중인 분석을 선택하세요.

Sparrow Enterprise	작업 이력	중 수시분석 1620	×
A       SS TestProject () () () () () () () () () () () () ()	Q. 김색이를 두 글라, 이상 입기         핵감비 :       유명         1020 %         1013 %         전백 2 책업 1 - 2 프셔트	한번 정말         확업 여시기           지국 제품         지도 M         지도 M <t< th=""><th>원 ¥</th></t<>	원 ¥

## 3. 슬라이드 아래에서 중지하기 버튼을 클릭하세요.

**Tip**: 프로젝트의 **작업 관리** 권한이 있는 사용자는 **작업 이력** 슬라이드에서 분석을 삭제할 수도 있습니다. 자세한 내용은 분석 삭제하기를 참고하세요.

# 결과 확인

앞에서 수행한 분석 결과를 확인하기 위해서는 브라우저를 통해 Sparrow Enterprise 서버로 이동해야 합니 다. CLI 명령어로도 프로젝트 결과를 간단히 확인할 수 있습니다. 자세한 내용은 <mark>클라이언트 CLI로 프로젝트</mark> 확인을 참고하세요.

## 마이페이지 확인하기

Sparrow Enterprise에 로그인하면 가장 먼저 표시되는 페이지가 마이페이지입니다. 마이페이지에서는 내 계정과 관련된 프로젝트 및 이슈에 대한 정보를 확인할 수 있습니다. 화면 왼쪽 위에 있는 Sparrow Enterprise 로고나 사이드 바에 있는 마이페이지 아이콘을 클릭하여 마이페이지로 이동하세요. 마이페이지 는 다음과 같은 내용을 표시합니다.

۱	Sparrow Enterprise							🔒 🔗 admin 🗸			
<b>&amp;</b>	환영합니다, admin님! 🔗	지금 Smart & Secure DevSecOps를 시작하세요				프로젝트 추가하기 새 작업 시작하기					
8 영	88 ···· 참여한 프로젝트 12	••• • • • • • • • • • • • • • • • • •	···· 최근 연료된 작업 58	() 진행 중인 결재 O		[] 처리할 결재 1	•••	 최근 치리한 결재 1			
Ð Ø	88 취약한 프로젝트		*** 모든 프로젝트 보7	A 처리할 이슈				*** 처리할 이슈 모두 보기			
	TestProject @ ① 篇 ① 322,806		2024-07-03 16:52:53에 마지막으로 작업할	2024-07-03 18-52-53에 미지막으로 작업동							
	<u>파란젝트 역할 테스트</u> @ 🕽 듣 (): 85,314		2024-06-04 14:30:57에 마지막으로 작업할 (전문) +10	총 이슈 22	_	_	59.1% (13) 1 31.8% (7) 9.1% (2)				
	TestProject vscode @ ① 目 ① 3,076		2024-05-04 22:18:16에 마지막으로 작업함	③ 최근에 수행된 작업 -	101			*** 수행된 작업 모두 보기			
	240620_tw		2024-06-20 18:09:48에 마지막으로 작업함	SS TestProject			2024-07-03 18:52:53에 사작됨 ⓒ 2시간 32분 28초 알료				
	Ø		0	· · · · · · · · · · · · · · · · · · ·							
	<u>240325 tw</u> ⑧ ① Ⅲ ① 290		2024-03-25 15:08:10에 마지막으로 작업함 (3	<ul> <li>중 수시 분석 <u>1860</u> 년 적</li> <li>88 <u>240620.tw</u></li> </ul>	되었			2024-06-20 18:09:48에 시작힘 ⓒ 12초 완료			

### √ 내 요약 정보

#### 참여한 프로젝트

사용자 계정이 구성원으로 포함된 프로젝트의 개수입니다. 더보기 아이콘을 클릭하면 **프로젝트 목록**으로 이동합니다.

#### 진행 중인 작업

사용자 계정이 프로젝트에서 수행한 작업 중에서 현재 **준비** 중이거나 **진행 중**인 작업의 개수입니다. 더보 기 아이콘을 클릭하면 **수행한 작업 목록**으로 이동합니다.

### 최근 완료된 작업

사용자 계정이 프로젝트에서 수행한 작업 중에서 최근 30일 동안 **완료**된 작업의 개수입니다. 더보기 아이 콘을 클릭하면 **수행한 작업 목록**으로 이동합니다.

#### 진행 중인 결재

사용자 계정이 요청한 결재 중에서 현재 진행 중인 결재의 개수입니다. 더보기 아이콘을 클릭하면 요청한 결재 목록으로 이동합니다.

#### 처리할 결재

사용자 계정이 처리할 수 있는 결재의 개수입니다. 더보기 아이콘을 클릭하면 **처리할 결재 목록**으로 이동 합니다.

#### 최근 처리한 결재

사용자 계정이 최근 30일 동안 처리한 결재의 개수입니다. 더보기 아이콘을 클릭하면 **처리한 결재 목록**으 로 이동합니다.

**Tip**: **결재**에 대한 설명은 이슈 제외하기를 참고하세요.

#### √ 취약한 프로젝트

사용자 계정이 구성원으로 포함된 프로젝트 중 이슈를 기준으로 가장 많은 이슈가 검출된 5개 프로젝트 를 카드로 표시합니다. 카드 오른쪽 위에 있는 **모든 프로젝트 보기**를 클릭하면 **전체 프로젝트 목록**으로 이동 합니다.

#### √ 처리할 이슈

사용자 계정이 담당자로 지정된 이슈의 상태 및 개수를 그래프로 표시합니다. 그래프 오른쪽 위에 있는 처리할 이슈 모두 보기를 클릭하면 처리할 이슈 목록으로 이동합니다.

#### √ 최근에 수행된 작업

사용자 계정이 구성원으로 포함된 프로젝트에서 수행된 작업 중 최근 3개 작업을 카드로 표시합니다. 카 드를 클릭하면 해당 작업의 요약 정보 페이지로 이동합니다. 카드 오른쪽 위에 있는 **수행된 작업 모두 보기** 를 클릭하면 **수행한 작업 목록**으로 이동합니다.

## 프로젝트 확인하기

이제 본격적으로 Sparrow Enterprise에서 만든 프로젝트와 수행한 분석에 대한 결과를 확인하고 이슈가 무 엇인지 알아보도록 하겠습니다.

#### 웹 서버에서 프로젝트 확인

프로젝트를 확인하기 위해서는 다음을 참고하세요.

## 1. 사이드 바에서 프로젝트 목록 아이콘을 클릭하세요.

😵 Sp	sarrow Enterprise								🗘 🚷 admin ~
*	전체 프로젝트 목록							프로젝트 추기	<mark>가하기</mark> 목록 내보내기
œ	Q. 검색어를 두 글자 이상 입적하세요 필터 ✓				<b>=</b>	로젝트 수정하기	삭제하기	20개씩 보기	> 일편집 >
000	프로젝트 이름 💲	테스트 케이스 수 🔅	총 이슈 🔅	매우 높음 \Rightarrow	높음 ::	보통 🔅	낮음 🗇	매우 낮음 💲	최근 작업 일시 🔸
8	TestProject	0	248	171	44	32	1	0	2023-06-14 16:48:31
Ð	mypage_test_02	0	40,603	195	1,151	6,086	2,004	9,999+	2023-06-14 15:22:03
۲	mypage_test_01	0	371	10	124	188	22	27	2023-06-14 14:53:16
	only-rasp	0	6	4	0	0	0	2	2023-06-14 14:37:08
	knj_sast	0	40,558	193	1,126	6,085	2,009	9,999+	2023-06-14 14:03:37
	다인 개인화 테스트	0	37	2	4	7	10	14	2023-06-14 13:58:39
	2023-06-14-기본동작	0	544	8	29	103	22	382	2023-06-14 13:54:50
	empty-2023-06-12	0	18	6	0	12	0	0	2023-06-14 13:38:40
	□ 시나리오 테스트 2305.1-2	2	384	58	117	179	12	18	2023-06-14 13:30:21
	2023-05-25	2	558	13	29	108	22	386	2023-06-14 11:10:36
	test	1	86	28	12	21	11	14	2023-06-14 10:03:25
	2023-06-23_yoon	0	0	0	0	0	0	0	2023-06-13 22:58:52
	2023-06-05	0	16	5	0	11	0	0	2023-06-13 19:06:06
	빌드 실패 무시	0	34	0	0	4	14	16	2023-06-13 18:44:35
	sparrow-1810	0	40,585	193	1,147	6,083	1,995	9,999+	2023-06-13 14:53:20
	C분석 뽀개기	0	4,746	0	96	688	1,794	2,168	2023-06-13 09:31:22
	request-11	1	55	12	4	19	10	10	2023-06-13 08:25:20

- 2. 전체 프로젝트 목록 페이지에서 확인하려는 프로젝트 이름을 클릭하세요.
- 3. 그러면 해당 프로젝트의 프로젝트 상세 정보로 이동합니다.

응왕 TestProject 《( 프로제도 키 TestProject 이 · 한타왕 이다	실색 정보 <b>● ③</b> 전드 javaAgent · 미지역 분석 <u>24분 2</u> ~ · 정어 <u>15분 2</u> √		48497 ~	수 💽 - 분석 결과 비교하기 작업 아직 보기 <mark>세 작업</mark>
진행 중인 작업의 결과에 따라 자신	; 이슈 또는 컴포넌트 정보가 변경될 수 있습니다.			진행 중인 직
Q. 검색어를 입력하세요	88 프로젝트 홈			요약 이슈 자산 컴포넌!
C         C	위험도별 이슈 수 6 000 78,615 111 연우 1	HE         1.3%         (1,004)           5.3%         (4,152)         12.3%         (8,032)           9.5%         (7,473)         (8,034)	상태별 이슈 수	1월 100.0% (78.613) 1 0.0% (1) 2 0.0% (1)
표 에스토 케이스	유형별 이슈 수	· · · · · · · · · · · · · · · · · · ·	フび増 이슈 추이 80000 20000 0 05-05 00-11 05-15 00-19	(1) 11 11 11 11 11 11 11 11 11 11 11 11 1

Tip: 작업을 수행하기 전에는 다음과 같이 결과가 표시되지 않습니다.

응 TestProject_T\ 프로젝트 키 TestProject_TW D	N 💿 상세 정보 💽 😕 한타일 에이전트 프로 · 미지역 분석 프로 · 방어 미인명		시오내기 > 분석 클라 비교하기 작업 아직 보기 <mark>세</mark>	작업 시작
Q. 검색이를 입력하세요 급 파일	88 프로젝트 홈	요약 이슈 자산 컴크	포넌트	
● URL 금 데스트 케이스	위험도별 이슈 수 * 이슈 0		상태별 이슈 수 8 영승 0 1 1111 0.05 (0) 1 111 0.05 (0) 1 111 0.05 (0)	
	유형별 이슈 수		フン培り合本の 100 100 100 100 100 100 100 10	<u>전별</u> 5-04

프로젝트 상세 정보 페이지에 표시되는 항목은 아래 내용을 참고하세요.

#### ✓ SBOM

오른쪽 위에 있는 **SBOM 내보내기** 버튼을 클릭해서 프로젝트에서 수집한 SBOM을 출력할 수 있습니다. 자세한 내용은 SBOM 내보내기를 참고하세요.

#### √ 프로젝트 기본 정보, 구성원, 작업 프로파일, 웹훅

권한 있는 사용자는 오른쪽 위에 있는 **프로젝트 수정하기** 버튼을 클릭해서 프로젝트에 대한 정보를 확인 하고 변경할 수 있습니다. 자세한 내용은 프로젝트 수정하기를 참고하세요.

#### √ 작업 이력

오른쪽 위에 있는 **작업 이력 보기**를 클릭하면 프로젝트에서 수행한 모든 작업에 대한 정보를 확인할 수 있습니다. 자세한 내용은 작업 이력 확인하기를 참고하세요.

#### √ 자산 트리

왼쪽에는 분석 작업에서 사용된 분석 대상인 **파일**, **URL**을 **자산**이라는 정보가 표시됩니다. **자산**에 표시된 파일이나 URL을 클릭하면 클릭한 자산에서 검출된 이슈가 **이슈** 목록에 표시됩니다. 프로젝트 상세 정보의 탭에도 **자산** 탭이 추가되었습니다.

#### √ 요약

요약 탭에서는 프로젝트에서 검출한 최근 이슈를 다음과 같은 네 개의 그래프로 표시합니다. 단, Sparrow TSO 제품 라이선스만 소유한 경우에는 테스트 케이스에 대한 데이터를 테이블로 표시합니다.

#### 위험도별 이슈 수

프로젝트에서 검출된 최근 이슈의 개수를 **매우 높음**, **높음**, **보통**, **낮음**, **매우 낮음**이라는 위험도에 따라 5 단계로 구분합니다.

#### 상태별 이슈 수

프로젝트에서 검출된 최근 이슈의 개수를 미확인, 확인, 해결이라는 상태에 따라 3개로 구분합니다.

#### 유형별 이슈 수

프로젝트에서 검출된 최근 이슈의 개수를 **소스코드**, **컴포넌트**, 웹 취약점, 자가 방어라는 분석 도구에 따 라 4개로 구분합니다.

#### 기간별 이슈 추이

프로젝트에서 검출된 최근 이슈가 검출된 날짜와 이슈의 개수를 그래프로 표시합니다.

**Tip**: 프로젝트 상세 정보에 표시되는 이슈는 모두 **최근 이슈**입니다. **최근 이슈**에 대한 자세한 내용은 최근 이슈 확인하기를 참고하세요.

#### √ 이슈

이슈 탭에서는 프로젝트에서 검출한 최근 이슈를 목록으로 표시합니다. 자세한 내용은 최근 이슈 확인하 기를 참고하세요.

#### √ 자산

자산 탭에서는 분석에 사용한 분석 대상인 **파일**과 **URL**을 목록으로 표시합니다. 자세한 내용은 최근 자산 확인하기를 참고하세요.

#### √ 컴포넌트

컴포넌트 탭에서는 프로젝트에서 검출한 최근 컴포넌트를 목록으로 표시합니다. 자세한 내용은 최근 컴 포넌트 확인하기를 참고하세요.

#### 프로젝트 수정하기

프로젝트에서는 **프로젝트 키**, **프로젝트 이름**, **프로젝트 설명**과 같은 **기본 정보**를 변경할 수 있습니다. 또한 프로젝트에서 사용할 **작업 프로파일**을 활성화하거나 프로젝트의 **구성원**, 웹**훅**을 추가하고 삭제할 수 있습 니다.

프로젝트 설정을 수정하려면 1) 프로젝트의 **프로젝트 구성원**으로써 프로젝트 권한 중 2) **프로젝트 수정** 권 한을 포함한 프로젝트 역할을 가져야 합니다. 혹은 시스템의 **프로젝트 관리** 권한이 있는 관리자도 프로젝트 설정을 수정할 수 있습니다. 자세한 내용은 다음을 참고하세요.

1. 프로젝트 상세 정보 페이지로 이동하세요.

2. 오른쪽 위에 있는 프로젝트 수정하기 버튼을 클릭하세요.

🧊 sp	barrow Enterprise		프로젝트 수정			×					
æ	# TestProject	હના છાટ 💶 😨	글 기본 정보								
88	프로젝트 키 <u>TestProject</u> 🖸 🐳 현타임 예	이전트 일음 - 마지막 분석 일음 - 방어 미진행	프로젝트 키 •	<u>=</u> 2	제트 이름						
*	Q, 검색어를 입력하세요		TestProject TestProject								
<u>eo0</u>	<ul> <li>मध</li> </ul>	88 프로젝트 용	설명 서머은 인러하네요								
1			202 0 4 6 4 2								
Q	URL	위험도별 이슈 수									
۲	)는 테스트케이스		추. 구성원								
		* 000 O	Q 검색어를 두 글자 이상 입력하세요.	필터 🗸		추가하기 20개씩 보기 🗸 열편집 🗸					
			□ 유형 \$ 이름 ↑	역말 ::)							
			사용자 admin (admin)	PROJECT-ADMIN							
			전체 1 구성원 1 - 1 표시됨			1 페이지 이동 →					
		유형별 이슈 수	금 작업 프루파일								
			· · · · · · · · · · · · · · · · · · ·								
			Q, 검색어를 두 글자 이상 입력하세요.	필터 🗸		20개씩 보기 🗸 열편집 🗸					
			프로파일 이름 🛧	허용된 작업	역할	검출 규칙 수 💠 활성화 🔅					
			모든 작업과 검출 규칙	전수 분석, 수시 분석, 자가 방어, 테스트 케이스 최	적화 -	2,711					
			소프트웨어 보안약점 진단가이드 검출 규칙	전수 분석, 수시 분석		532					
			자가 방어 검출 규칙	자가 방어		30					
			주요정보통신기반시설 취약점 분석·평가 기준 검출 규	전수 분석, 수시 분석		15 💽					
			럼포넌트 분석 검출 규칙	전수 분석, 수시 분석		520					
			전체 5 프로파일 1 - 5 표시원			1 페이지 이동 →					
			ふ <b>전</b> 호								
			Q. 검색어를 두 글자 이상 입력하세요.	월터 🗸		추가하기 20개씩 보기 🗸 열편집 🗸					
			대상 이벤트 🛧 HT	TP 메소드 ① 대상 URL ①							
				등록 대기 중이거나 내용이	기 없습니다.						
						취소하기 <b>삭제하기 수정하기</b>					

3. 슬라이드에서 프로젝트 키나 프로젝트 이름을 수정하세요.

4. 아래에 있는 수정하기 버튼을 클릭하세요.

#### 프로젝트 구성원 추가하기

- 1. 프로젝트 수정 슬라이드로 이동하세요.
- 2. 구성원에 있는 추가하기 버튼을 클릭하세요.

🧊 s	parrow Enterprise			프로젝트 수정			구성원 추가		×
2	# TestProject 🔘	상세 정보 💽 🛞		기본 정보	구성원 * 구성원을 선택하세요.		~		
88	프로젝트 카 <u>TestProject</u> 🙆 🐳 전타임 에이전	현료 입음 · 마지막 분석 입음 · 방어 미진행		프로젝트 키 •	<u>=</u>	2제트 이용	이함 *		
æ	Q, 검색어를 입력하세요			TestProject	т	estProject	역할을 선택하세요.		~
000	<ul> <li>파일</li> </ul>	88 프로젝트 홈		설명 설명을 입력하세요.			<b>114 1131</b>	-	***
R D	URL	위험도별 이슈 수					취소아기	제속 추가하기	주가하기
۲	는 배수트 케이스			冬 구성원					
			송 이슈 0	Q. 검색어를 두 글자 이상 입력하세요.	필터 🗸				
				유형 : 이를 수	역할 :::				
				다 사용자 admin (admin)	PROJECT-ADMIN				
		유형별 이슈 수		전체 1 구성원 1 - 1 프시원					
				Q, 검색이를 두 글자 이상 입백하세요.	필터 🗸				
				프로파일 이름 🛧	하용된 작업	역말			
				모든 작업과 검출 규칙	전수 분석, 수시 분석, 자가 방어, 테스트 케이스 최	[적화 -			
				소프트웨어 보안약점 진단가이드 경출 규칙	전수 분석, 수시 분석				
				자가 방어 검출 규칙	자가 방어				
				주요정보통신기반시설 취약점 분석-평가 기준 검출 규	전수 분석, 수시 분석				
				컴포넌트 분석 검출 규칙	전수 분석, 수시 분석				

3. 아래를 참고하여 구성원 정보를 입력하세요.

4. 추가하기 버튼을 클릭하세요.

5. 프로젝트 수정 슬라이드에서 수정하기 버튼을 클릭하세요.

구성원\*

프로젝트에 구성원으로 추가할 사용자 또는 사용자 그룹입니다.

#### 역할\*

프로젝트 구성원으로 추가할 사용자 또는 사용자 그룹의 역할입니다. 프로젝트 역할을 추가하는 방법은 프로젝트 역할를 참고하세요.

#### 프로젝트 작업 프로파일 설정하기

1. 프로젝트 수정 슬라이드로 이동하세요.

2. 작업 프로파일 목록에는 사용 가능한 모든 작업 프로파일이 있습니다.

- <b>(</b> )	Sparrow Enterprise					프로젝트 수정	작업 프로파일 모	든 작업과 검출	규칙						×
<i>P</i> 22	🏭 TestProject 🌑	성세 정보 🛑 🛞				Q, 검색어를 두 글자 이상 입네	📄 기본 정보								
88	프로젝트 키 <u>TestProject</u> () · 전타임 여	이전트 업음 - 마지막 분석 업음 - 방어 미진영				- #8 :	사용 가능한 역할				허용함 작업 저슈 분석, 슈시 분석, 파	가 바이 테스트 ㅋ	비미스 치저히		
-00 W	Q, 검색어를 입력하세요	※ 프로젝트 홈				□ 사용자	<ol> <li>건출규칙</li> </ol>				2129,1429,4		1+1		
200	<u>ि</u> महि 												103681 H3	1	ofmixi
9	URL .	위험도별 이슈 수				응 작업 프로파일	Q 김역너물 두 날사 이상 입역하세요. 썰더 🗸			2-1 V			10/14 ±2		800 V
۲	臣 테스트 케이스		중 이슈		0.0%	Q. 검색어를 두 글자 이상 입태	88 3	언어 :	위험도 ()	규칙이름 ↑ # 효유 ## 여사자 사유					
					0.0%	프로파일 이름 🛧	S 2475	C++	<ul> <li>&gt; 낮음</li> </ul>	#if 지시자 사용					
			0		0.0%	모든 작업과 검출 규칙	S 24.75	C++	• ¥8	#pragma 지시자 사용					
					0.0%	소프트웨어 보안약점 진단가이	5 소스코드	C++	<ul> <li>&gt; 낮음</li> </ul>	#undef 지시자 사용					
					자가 방어 검출 규칙	S 4435	C++	○ 매우 낮음	* 및 & 토콘 규칙 위반						
		으형벽 이스 스				주요정보통신기반시설 취약점	S ****	Java	이 매우 낮음	+ 및 += 연산자로 더해진 문	자열				
		1102-1111				컴포넌트 분석 검출 규칙	S 4435	C#	• 18	+ 연산에 사용된 빈 문자열					
						전체 5 프로파일 1 - 5 표시됨	S 4435	C#	<del>•</del> 보통	+= 연산자로 더해진 문자열					
							S ****	C++	• ¥8	, 면산자 사용					
						.S. 웹혹	€ 험포년트	35	○ 매우 낮음	OBSD 라이선스 컴포넌트 시	18				
						Q, 검색어를 두 글자 이상 입어	전체 2,711 점을 규칙 1	- 10 표시됨		1 2 3	4 5 6 7 8	9 10	× ×	페이지 이동	$\rightarrow$
						대상 이번트 🛧	<♪ 소스코드 분·	넉 옵션							
							분석 제외 경로 -								
					웹 취약점 분	석 옵션									

3. 선택 토글 버튼을 활성화하거나 비활성화하세요.

4. 이제 작업을 시작하세요.

#### 작업 프로파일\*

**작업 프로파일**은 이슈 검출 규칙과 작업 옵션 등 작업에 필요한 정보를 모아둔 데이터입니다. 작업 프로 파일을 추가하는 방법은 작업 프로파일 추가하기를 참고하세요. **프로젝트 수정** 페이지의 **작업 프로파일**에서는 분석 작업에서 이슈를 검출하는 이슈 검출 규칙의 상세 정보 를 확인할 수도 있습니다. 다음을 참고하세요.

1. 프로젝트 수정 슬라이드로 이동하세요.

2. 작업 프로파일 목록에서 분석 작업에 사용한 항목을 클릭하세요.

3. 검출 규칙 목록에서 확인하려는 이슈 검출 규칙을 클릭하세요.

🧐 s	parrow Enterprise					프로젝트 수정	작업 프로파일 5	든 작업과 검출	규칙			이슈 검출 규칙 상세 ×			
*	# TestProject O	क्षम छन्न 💿 🛞				Q. 검색어를 두 글자 이상 압	🖹 기본 정보					금치 아름 #undef 지시자 사용			
*	프로젝트 키 <u>TestProject</u> 0 · 현타임 예(					- #8 :	사용 가능한 역할 -				허용할 지입 <sup>상 ()</sup> 전수 분석, 수시 <u>소스코드</u>	~ 10 · · · · · · · · · · · · · · · · · ·			
<u>e00</u>	Q 김역어를 입역하세요 : 파일	88 프로젝트 <b>흥</b>					① 검출규칙					이었도 · · · · · · · · · · · · · · · · · · ·			
22 0	URL	이허드병 이스 스				CALIFORNIA	Q, 검색어를 두	글자 이상 입력하	세요.	필터 🗸		C++ 48			
2		지침도를 이유 구				◎ 작업 프로파일	#8 ¢	언어 🗇	위험도 🔅	규칙이름 수		#undef 지시자 사용 체커는 undef 전치리 구문을 사용한 경우를 검출합니다.			
Ý						Q 검색어를 두 글자 이상 입태	<u>3544</u>	C++	이 매우 낮음	# 혹은 ## 연산자 사용		undef 전처리 구문을 사용한 헤더 파일을 include 하는 경우, 이 전에 define 전처리 구문으로 정의한 매크로 변수의 값이 달라져			
			종 이슈 0			프로파일 이름 🛧	5 소스코드	C++	◎ 낮음	#if 지시자 사용		에너 파월이 비장장역으로 포함될 수 있습니다. 악하기 힘든 오류가 발생할 수 있습니다. undef 제처리 구문을 취대한 사용하지 않도록 한니다.			
			U	() 낮음 () () 매우 낮음 ()		모든 작업과 검출 규칙	모든 작업과 검출 규칙 S 소스코드 C++ · · · · · · · · · · · · · · · · · ·	#pragma 지시자 사용		62					
						소프트웨어 보안약점 진단가이	S &ARE	C++	<ul> <li>&gt; 것음</li> </ul>	#undef 지시자 사용		C++ 252			
						자가 방어 검출 규칙	S ****	C++	○ 매우 낮용	* 및 & 토큰 규칙 위반					
		유형별 이슈 수		주요정보통신기반시설 취약정	S 2525	Java	○ 매우 낮음	+ 및 += 연산자로 더해진 문	자열						
						컴포넌트 분석 검출 규칙	<u>3544</u>	C#	* MB	+ 면산에 사용된 빈 문자열					
						전체 5 프로파일 1 - 5 표시됨	<u>3644</u>	C#	<ul> <li>보통</li> </ul>	+= 연산자로 더해진 문자열					
							S 2025	C++	• ¥8	, 면산자 사용					
						69 <b>1</b> 44	€ 컴포넌트	35	○ 매우 낮음	0BSD 라이선스 업포넌트 사	8				
						Q 검색어를 두 글자 이상 입지	전체 2,711 검출 규칙	I - 10 표시됨		1 2 3	4 5 6				
						대상 이벤트 🛧		석 옵션							
					_	분석 제의 경로 -									
							웹 취약정 눈	석옵션							

4. 이슈 검출 규칙의 정보를 확인하세요.

Tip: 이슈 검출 규칙을 수정하거나 추가하려면 이슈 검출 규칙 관리하기를 참고하세요.

프로젝트 웹훅 설정하기

**프로젝트 수정** 슬라이드에서는 프로젝트의 특정 이벤트에 **웹훅**을 설정하는 것도 가능합니다. 다음 내용을 참고하세요.

1. 프로젝트 수정 슬라이드로 이동하세요.

2. 웹훅에 있는 추가하기 버튼을 클릭하세요.

🦻 si	arrow Enterprise				프로젝트 수정		웹훅 추가		
	🎛 TestProject 🔘	상제 정보 🔼 😟			Q, 검색어를 두 글자 이상 입력하세요.		대상 이벤트 * 대상 이벤트를 선택하세요.	~	HTTP 에스드 * GET
	프로젝트 키 <u>TestProject</u> 🙆 🐳 현타임 에이전	표 없음 - 마지막 분석 없음 - 방어 미			□ 유형 ᠅ 이름 ↑		대상 URL *		
	Q, 검색어를 입력하세요	··· 프콘제트 호			사용자 admin (admin)		대상 URL을 입력하세요.		
	<u>ه</u> ۳۲	*****			저원1그사회 1.1프시외		HTTP NCI		
	URL	위험도별 이슈 수			광 작업 프로파일		<ul> <li>이 키를 입력하세요.</li> <li>+ 추가하기</li> </ul>		같을 입력하세요.
	T (1) E 101						요청 HTTP 분문		
	10 000 1010			0.0%	Q, 검색어를 두 글자 이상 입력하세요.		요청으로 전달할 HTTP 본문을 입력하세요.		
			종 이슈	0.0%	프로파일 이름 🛧	허용된			
			0	0.0%	모든 작업과 검출 규칙	전수 통			
				0.0%	소프트웨어 보안약점 진단가이드 검출 규칙	전수 8			
					자가 방어 검壺 규칙	자가 병			
		으형병 이스 스			주요정보통신기반시설 취약점 분석·평가 기준 검출 규	전수 8	프로젝트나 작업과 관련된 값을 접목을 통해 선물아/ 한 원혹 변수를 확인하세요.	1위해 사선에	성외된 접국 변수를 사용할 수 있습니다. 아래 버튼을 클릭하여 사용
		1102 -111 1			컴포넌트 분석 검출 규칙	전수 8	행혹 변수 보기		
					전체 5 프로파일 1 - 5 표시됨				취소하기 추기
					. · · · · · · · · · · · · · · · · · · ·				
					Q, 검색어를 두 글자 이상 입력하세요.				
					대상이벤트 수 HT	TP 메소드			

3. 아래를 참고하여 웹훅 정보를 입력하세요.

4. 추가하기 버튼을 클릭하세요.

5. 프로젝트 수정 슬라이드에서 수정하기 버튼을 클릭하세요.

#### 대상 이벤트\*

웹훅을 실행할 프로젝트의 이벤트입니다. **작업 시작**, **작업 실패**, **작업 완료** 중에서 하나 이상을 선택할 수 있습니다.

#### HTTP 메소드\*

실행할 웹훅 요청에서 사용할 HTTP 메소드입니다. GET, HEAD, POST, PUT, DELETE, OPTIONS, TRACE, PATCH 중에 하나를 선택할 수 있습니다.(기본값: GET)

#### 대상 URL\*

웹훅을 실행할 대상 URL입니다. 이 옵션은 http:// 혹은 https://로 시작하는 URL 형식으로 입력해야 합니다.

#### HTTP 헤더

웹훅을 실행할 때 대상 URL로 보내는 HTTP 요청에 추가할 헤더의 키와 값 목록입니다. 키와 값의 쌍으로 되어있으며 목록의 아래에 있는 **+ 추가하기** 버튼을 클릭하여 하나 이상의 키값을 입력할 수 있습니다.

#### 요청 HTTP 본문

웹훅을 실행할 때 대상 URL에 대한 요청으로 전송할 HTTP 본문입니다. 값이 존재하지 않는 경우 별도의 본문을 전달하지 않습니다. **웹훅 변수 보기**에 있는 변수를 이 옵션에 입력할 수 있습니다.

#### 웹훅 변수 보기

웹훅을 실행할 때 요청 HTTP 본문에 사용할 수 있는 변수의 목록입니다. 프로젝트 키, 작업 ID, 작업 유형, 작업 시작 일시, 작업 완료 일시, 작업 수행자 ID, 작업 수행자 이름, 총 이슈 수, 위험도별 이슈 수와 같은 정 보를 사용할 수 있습니다.

#### 작업 이력 확인하기

사용자가 가진 제품 라이선스에 따라 Sparrow Enterprise에서 수행한 동작 중 **분석**, **자가 방어**, **테스트 케이 스 최적화**를 작업이라고 부릅니다. **작업 이력**에서는 프로젝트에서 수행한 모든 작업의 목록에 표시됩니다. 여기서 작업에 대한 주요 정보를 확인하실 수 있습니다.

작업 이력에서는 분석 로그를 다운로드 받거나 완료된 분석의 분석 보고서를 다운로드 받을 수도 있습니다. 자세한 내용은 분석 로그 다운로드 및 분석 보고서를 참고하세요.

분석을 중지하거나 삭제하는 것도 **작업 이력** 페이지에서 하실 수 있습니다. 만약 분석을 중지하면 다시 해당 분석을 시작할 수 없습니다. 또한 분석을 삭제하는 경우에도 분석 결과를 복구할 수 없다는 점에 유의하세 요. 자세한 내용은 분석 중지하기 및 분석 삭제하기를 참고하세요.

#### 분석 로그 다운로드

1. 작업 이력에서 로그를 다운로드하려는 분석을 선택하세요.

2. 분석 슬라이드로 이동합니다.

Sparrow Ent	terprise				작업 (	이력		③ 수시 분석 16	514					>
88 1	TestProject 🔘	정세 정보 💽 😟			٩	검색어를 두 글;	자 이상 입태	일반 정보	작업 메시기	4				
프로젝트 카	비 <u>TestProject</u> 🖸 🐳 편타입에이	N전드 javaAgent · 마지막분석 <u>24분전</u> / · 방어 <u>3시간</u>	<u>1 8</u> ."			직업 ID 🔅	유행	프로젝트			3	각업 프로파일		
0	진행 중인 작업의 결과에 따라 자신	t, 이슈 또는 컴포넌트 정보가 변경될 수 있습니다.				1620	6	TestProject 진행 상황			5	리는 작업과 경울 규칙 1요 시간		
						1614	6	<ul> <li>완료</li> </ul>			1	0분 28초		
Q 2	색어를 입력하세요	88 프로젝트 홈				1613	0	분석 시작 일시 2024-06-04 10:44	4:03			문석자 admin(Supera	dmin)	
in 199						1612	0	분석 대상						
> Eo : > Eo :	apache-maven-3.3.9.zip aspnet/CheckerUnitTest	1개의 예약된 작업이 있습니다.				1611	6	Enterprise.zip						
> 60	c-simple					1401	6	다 작업 프로피 1	파일은 이전 작업	법에 적용된 내용	응을 표시하므로 현재	프로젝트 설정과 다를	수 있습니다.	
> Eo (	C-\Testcode isp	위험도별 이슈 수				1280	6	① 건축 그치						
> 20 0	objc/parse_error					1254	0							
> E <mark>o</mark> :	sca_all_version.zip		비비비 매우 높음	1.3% (1,004)		1253	0	Q. 검색어를 두 글	자 이상 입력히	세요.	핖	EI 🗸	10개씩 보기 🗸	열편집 🗸
😜 URL		충이슈 <b>70,010</b>		<b>12.3%</b> (9,632)		1050		유형 ::	언어 🗇	위험도 💲	규칙 이름 🛧			
> 🚳 (	http://dastapp.fasoo.com:9090/W	78,018	IIII ya	<b>9.5%</b> (7,473)		1202	•	🛷 소스코드	C++		# 혹은 ## 연산지	ት 사용		
등 데스트	트 케이스		매우 낮음	<b>71.7%</b> (56,355)		1235	•		C++		#if 지시자 사용			
						1230		0 소스코드	C++		#pragma 지시지	ት 사용		
						1227	6	00 AARC	C++		#undef TIAITE			
		유영멀 이슈 수				1141		() AABE	C++		* 0 2 63 34	910		
						1139	6	· · · · · ·			- X & EE #9	1122		
				······································		1138	0	(*) 소스코드	Java		+ 및 += 연산자5	리더해진 문자열		
		•				1080	۲	🥗 소스코드	C#		+ 연산에 사용된	빈 문자열		
		•		0 x		1079	٢					কমাক	기 로그 다운로드	보고서 내보내기

3. 아래쪽에 있는 로그 다운로드 버튼을 클릭하세요.

Tip: 자가 방어 및 최적화의 경우 분석 로그를 다운로드할 수 없습니다.

분석 작업의 경우, 가장 최근의 분석에서 검출한 이슈를 비롯한 분석 결과는 프로젝트의 탭에서 자세하게 확 인할 수 있습니다. 하지만 이전에 수행한 분석 결과 중 이슈나 자산, 컴포넌트와 같은 상세 결과의 내용은 표 시되지 않습니다.

따라서 만약 이전 작업과 관련된 결과를 자세히 확인하려면 해당 작업의 이후에 수행한 동일한 유형의 작업 을 모두 삭제해야 합니다. 단, 방어의 경우 이미 수행된 작업을 삭제하는 것이 불가능합니다.

Warning: 삭제된 데이터는 복구할 수 없다는 점에 유의하세요.

수행이 종료된 분석을 삭제하려면 1) 프로젝트의 **프로젝트 구성원**으로써 프로젝트 권한 중 2) **작업 관리** 권 한을 포함한 프로젝트 역할을 가져야 합니다. 자세한 내용은 다음을 참고하세요.

1. 프로젝트 상세 정보 페이지로 이동하세요.

2. 오른쪽 위에 있는 작업 이력 보기 버튼을 클릭하세요.

3. 삭제할 분석의 체크박스를 선택하고 목록 오른쪽 위에 있는 **삭제하기** 버튼을 클릭하세요.

4. 혹은 삭제하려는 분석의 상세 정보 슬라이드에서 아래에 있는 삭제하기 버튼을 클릭하세요.



Tip: 자가 방어 및 최적화의 경우 작업을 삭제할 수 없습니다.

#### 작업 메시지 확인하기

작업을 진행하는 과정에서 사용자가 알아야 할 중요한 문제가 발생하는 경우 작업 이력에 알림이 표시됩니 다. 이 알림에서 **작업 메시지 보기**를 클릭하면 해당 메시지 목록으로 이동할 수 있습니다.

1. **작업 이력**에서 작업 메시지를 확인하려는 분석을 선택하세요.

2. 분석 슬라이드로 이동합니다.

🥵 s	parrow Enterprise				작업 (	이력		③ 수시 분석 7	92						×
A.	器 TestProject 🔘	상세 정보 🌑 🔅			٩	검색어를 두 글지	다 이상 입 <sup>4</sup>	일반 정보	작업 메시기	지 2					
	프로젝트 키 TestProject 🖸 🕜 컨타입에이	I전드 없음 → 마지막 문석 <u>2시간 전</u> <sup>™</sup> → 방어 <u>5시간 전</u> ■			0	직업 ID 💲	유행	<ol> <li>작업 도량</li> </ol>	통 주의 메시지가	발생했습니다. 3	박업 메시지를 8	확인하세요.			작업 메시지 보기
<del>.</del>	진행 중인 작업의 결과에 따라 자신	, 이슈 또는 컴포넌트 정보가 변경될 수 있습니다.				1620	<b></b>								
000					0	1614	6	프로젝트 작업 메시지				작업 프로파일 모든 작업과 검	출 규칙		
8	Q, 검색어를 입력하세요	88 프로젝트 홈			0	1613	0	진행 상황				소요 시간 20초			
Q	🐻 मध				0	1612	0	· 근표 분석 시작 임시				분석자			
0	Co apache-maven-3.3.9.zip     Co aspnet/CheckerUnitTest	1개의 예약된 작업이 있습니다.				1611	6	2024-04-19 09:	24:12			🛃 김다인김	다인김다인길	님다인김다인김다인경	I다인김다인(dain)
	> Eo c-simple					1401	6	분석 대상 😝 sast+sca.zip							
	> E C:\Testcode	위험도볔 이슈 수				1000	0								
	> Eo jsp					1280	()	⑦ 검출 규칙							
	> Co sca_all_version.zip		태태 매우 높음	<b>1.3%</b> (1,004)		1254	<b>(</b>	0							
			IIII 높음	<b>5.3%</b> (4,154)		1253	6	Q 검색어를 두	글자 이상 입력히	하세요.		필터 🗸		10개씩 보기 🗸	열편집 🗸
		78,618	11111 ±5	<b>12.3%</b> (9,632)	0	1252	6	유형 💲	언어 💲	위험도 💲	규칙 이름 1	ħ			
	> eo nitp://dastapp.tasoo.com.auau/w			<b>9.5%</b> (7,473)		1235	<b>(</b>	🤒 소스코드	C++	1111	# 혹은 ##	연산자 사용			
	經 테스트케이스		비미미 매우 낮음	<b>71.7%</b> (56,355,		1230	6	🤣 소스코드	C++		#if 지시자	사용			
						1227	6	🧼 소스코드	C++		#pragma	지시자 사용			
		유형별 이슈 수				1141	3	🧼 소스코드	C++		#undef 지	시자 사용			
					0	1139	6	🧼 소스코드	C++	1111	* 및 & 토큰	큰 규칙 위반			
			_		0	1138	0	🧼 소스코드	Java	1111	+ 및 += 연	년산자로 더해진 문자!	열		
		•				1080	۲	🧼 소스코드	C#		+ 연산에 시	나용된 빈 문자열			
		•				1079	0						삭제하기	로그 다운로드	보고서 내보내기
					_										

3. 알림에서 **작업 메시지 보기**를 클릭하거나 **작업 메시지** 탭을 클릭하세요.

Sparrow Enterprise			작업 이력		ᢙ 수시 분석 792	작업 메시지 조회	×
# TestProject	હમા સપ્ર 💽 🔞		Q 검색어를	두 글자 이상 입	일반 정보 적업 미	제목 이슈 업로드 실패	
프로젝트 키 TestProject 🗅 · 런타임 에	이전트 앞음 · 마지막 분석 <u>2시간 전 <sup></sup> · 방어 5시간 전</u> ■		- 작업	D 🗘 유행	Q, 검색어를 두 글자 이상 입행	50 0 주의	
진행 중인 작업의 결과에 따라 자신	난, 이슈 또는 컴포넌트 정보가 변경될 수 있습니다.		162	•	등급 🗘 제목 🗘	발생 일시	
			1614	u 🚳	주의 이슈 업로드	2024-04-19 09:24:47	
Q, 검색어를 입력하세요	※ 프로젝트 홈		1613	0	주의 로그 다운로	이슈 업로드 실패	
ि <mark>0</mark> मध			1612	0			
> E apache-maven-3.3.9.zip     > E aspnet/CheckerUnitTest	🚺 1개의 예약된 작업이 있습니다.		1611	6	전체 2 메시지 1 - 2 표시됨	792 문학회 이유 접도드가 실패었습니다. SAST 지미스 도그를 확인해야 합니다. 792	
> Eo c-simple			140			- 0±	
> Eo C:\Testcode	위험도별 이슈 수		128	) @		logs/sast/sast.log	
> E objc/parse_error			- 125	1 @			
> Co sca_all_version.zip		IIIII 매우높음 1.3% (1,004	0 125			SASI OP MH DEL	
🚳 URL	충이슈	·····································					
> 🚯 http://dastapp.fasoo.com:9090/W	78,618	태배 낮음 9.5% (7,473					
狂 페스트 케이스		┃     매우닟읍 <b>71.7%</b> (56,33	5)	5 6			
			123	) (6			
			122	° ©			
	유형별 이슈 수		1141	6			
			1139				
			4 🗌 1138	. 0			
	•		g 108	) @			
	•		x 1079	. 0			

4. 목록에서 확인할 항목을 클릭하세요.

😵 Sp	arrow Enterprise			- 40	작업 0	이력		중 수시 분석 792	작업 메시지 조회	×
æ		상세 정보 💽 🛞 1도 영웅 - 미지막분석 <u>2시간 전 <sup>10</sup> -</u> 영어 <u>5시간 전</u> =			۹	검색어를 두 글지 직업 ID 💲	는 이상 입태 유형	일반 정보 작업 여 Q. 검색어를 두 글자 이상 입태	제작 아슈 업로드 실패 등급 •	
- <u>00</u>	진행 중인 작업의 결과에 따라 자산,	이슈 또는 컴포넌트 정보가 변경될 수 있습니다.				1620 1614	© ©	동급 () 제목 ()	발생 일시 2024-04-19 09:24:47	
e.	Q. 검색이를 입력하세요	응 프로젝트 홈				1613	0	주의 로그 다운로	<sup>48</sup> 이슈 업로드 실패	
۲	Co apache-maven-3.3.9.zip     Co aspnet/CheckerUnitTest	● 1개의 예약된 작업이 있습니다.				1612	6	전체 2 메시지 1 - 2 표시됨	792 분석의 이슈 업로드가 실패했습니다. SAST 서비스 로그를 확인해야 합니다. <b>경로</b>	
	Concentration     Concentration     Concentration     Concentration     Concentration	위험도별 이슈 수				1401 1280	© ©		logs/sast/sast.log	
	<ul> <li>Coopc/parse_error</li> <li>Coopc.all_version.zip</li> </ul>		11111 매우높음 11111 녹음	<b>1.3%</b> (1,004)		1254	6		해고 SAST 이슈 실제 업코드	
	♥ URL > ♥ http://dastapp.fasoo.com:9090/W	<sup>⊗ 0 </sup> ⊕ 78,618	11111 보통 11111 보통	<b>12.3%</b> (9,632) <b>9.5%</b> (7,473)		1252	6			
	응금 테스트 케이스		┃     매우 낮음	<b>71.7%</b> (56,355)		1235 1230	© ©			
		으혀벼 이스 스				1227	6			
		ㅠ경골에ㅠㅜ				1141	©			
						1138	0			
		•		0 1 () X		1079	0			

#### 제목

표시된 작업 메시지의 제목입니다.

#### 등급

표시된 작업 메시지는 **주의** 혹은 **경고**라는 등급으로 분류됩니다. **주의**는 작업에 포함된 일부 분석 결과에 이상이 있을 수 있는 경우이고 **경고**는 작업이 정상적으로 진행되지 않고 전체 분석 결과를 확인할 수 없는 경우를 의미합니다.

#### 발생 일시

표시된 작업 메시지가 발생한 일시입니다.

#### 내용

표시된 작업 메시지의 내용입니다. 여기에는 작업 메시지에 대한 설명이나 더 자세한 로그를 확인할 수 있는 위치 등 구체적인 정보가 포함됩니다.

#### 태그

표시된 작업 메시지와 관련된 태그입니다.

#### 분석 결과 비교하기

1. 비교할 분석의 프로젝트 상세 정보 페이지로 이동하세요.

2. 오른쪽 위에 있는 분석 결과 비교하기 버튼을 클릭하세요.

아래 내용을 참고하여 분석 결과 비교 슬라이드에서 비교 기준 분석 및 비교 대상 분석을 선택하세요.
 (\*는 필수 입력 항목)

🧐 S	parrow Enterprise			분석 결과 비교	×
æ 88	<b>양 TestProject ()</b> 프로젝트 키 <u>TestProject</u> 이 · 한타임 여야전	상세 전상 🌑 ⑧ 프 JavaAgent - 미지역분석 <u>19분 전 5 - 18억 34/0 전 5</u>	내보내기 🗸	선택한 분석에서 검출한 이슈, 자산, 킹 다. 기준 분석이 시작된 후에 수행한 분 수 있습니다.	1포넌트의 목록을 비교합니 4석만 대상 분석으로 선택할
	진행 중인 작업의 결과에 따라 자산,	가수 또는 철보선은 정보가 변경될 수 있습니다.		프로젝트 TestProject	
8	Q, 검색어를 입력하세요	응 프로젝트 홈		비교 기준 분석 *	~
Ð	ि <mark>०</mark> मध			비교 대상 분석 •	
0	Co apache-maven-3.3.9.zip     Da asonet/CheckerLinitTest	1개의 예약된 작업이 있습니다.		비교 대상 분석을 선택하세요.	~
	> Cg Simple           > Cg Clivescool           > Cg. Directool           > Cg. Solid/pres.error           > Cg. solid/pres.error <td>위험도별 이슈 수 상태별 이슈 수</td> <td><ul> <li>미하인</li> <li>1 하인</li> <li>2 해결</li> </ul></td> <td></td> <td>취소하기 <b>비교하기</b></td>	위험도별 이슈 수 상태별 이슈 수	<ul> <li>미하인</li> <li>1 하인</li> <li>2 해결</li> </ul>		취소하기 <b>비교하기</b>
		유형별 이슈 수 기간별 이슈 추이			
		◆ 소스프트         77,425         80000           ● 일본년트         1,118         40000           ● 일위적월         38         20000           ● 경위적월         37         0			

4. 비교하기 버튼을 클릭하세요.

Sparrow Enterprise				분석 결	라비교									×
器 TestProject 🔘	) 상세 정보 💽 😥			↔ 비	교 결과 요약									
프로젝트 키 <u>TestProject</u> 🗘 · 런타임 에이	전트 javaAgent - 마지막분석 <u>22분전</u> ~ - 방어 <u>3시간 3</u>	<u>u</u> ~		6	수시 분석 <u>5</u>	271	202	4-05-30 13:56:41		🚱 수시 분석	5280	2024	-05-30 15:57	:41
진행 중인 작업의 결과에 따라 자산	, 이슈 또는 컴포넌트 정보가 변경될 수 있습니다.			이슈				3,115 🕕		이슈		+ 559	3,674	0
Q. 검색어를 입력하세요	응 프로젝트 홈			자산 컴포(	de			141 📄 45 🐨	$\rightarrow$	자산 컴포넌트		+ 375 + 63	516 ( 108 §	8
다 비원 > 단습 apache-maven-3.3.9.zip > 단습 aspnet/CheckerUnitTest > 단고 c-simple	1개의 예약된 작업이 있습니다.			= ні:	교 결과 상세									
<ul> <li>E C:\Testcode</li> <li>E jsp</li> <li>E objc/parse_error</li> </ul>	위험도별 이슈 수			이슈	ম	산 점크	E년트							
> Co sca_all_version.zip		배해 매우 높음	<b>1.3%</b> (1,004)	Q 3	색어를 두 글자	이상 입력하세요		필터 🗸			목록 내보내기 2	20개씩 보기 🗸 🗸	열편집	~
🏀 URL	종이슈 <b>78 61</b> 8	11111 높음 11111 보통	5.3% (4,154) 12.3% (9,632)		기준 분석 个	대상 문석 💲	유형 🗘	위험도 💲 이	슈이용 💲		자산 💲			
> 🚳 http://dastapp.fasoo.com:9090/W	70,010	₩111 낮음	<b>9.5%</b> (7,473)	0	있음	있음	😑 웹 취약점	7	본 언어 표시	누락	http://21	11.39.141.177:80	80/benchma	ar
狂 테스트 케이스		매우 낮음	<b>71.7%</b> (56,355)		있음	있음	😑 웹 취약점	1111 Q	못된 HTML		http://21	11.39.141.177:80	80/benchma	ar
					있음	있음	😑 웹 취약점	ш	SRF 토큰이	없는 폼 태그	http://21	11.39.141.177:80	80/benchma	ar
				0	있음	있음	😑 웹 취약점	।।।। थ	이블 누락		http://21	11.39.141.177:80	80/benchma	ar
	유영일 이유 주			0	있음	있음	😑 웹 취약점	IIII 2	못된 HTML		http://21	11.39.141.177:80	80/benchma	ər
					있음	있음	😑 웹 취약점	1111 a	이블 누락		http://21	11.39.141.177:80	80/benchma	ar
			0 2 0 2		있음	있음	😑 웹 취약점	e e	이블 누락		http://21	11.39.141.177:80	80/benchma	ar
	•		e e م ا										다른 분석 비금	2하기
	SB         TestProject         CC           RCME 7         TestProject         CC           RCME 7         TestProject         CC           C         TestProject         CC           C	Signed Statepsise     Signed Statepsise <th>SP TestProject Co   A d d d e Co   C Control TestProject Co   C</th> <th>Se TestProject Co verse verse javagent - andre 2 222 ° + tot 2022 * A data 1 Instituted C + data data data data data data data da</th> <th>Spence Enterprise       Ket 421         Spence Enterprise       Color Article Co</th> <th>By Department         Ext d a d a d a           66         T Cest DProject         Co         A d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a d a d a d a d a d a d a d a</th> <th>Spectrow         Media index         Spectrow         Spectrow</th> <th>by prove heterprise PS TestProject</th> <th>by prove future future</th> <th>by prove heterprise PS TestProject</th> <th>Arrend Marrendia Set TestProject () units () u</th> <th>by experience between the server of the ser</th> <th>Per de la d</th> <th>by the field of t</th>	SP TestProject Co   A d d d e Co   C Control TestProject Co   C	Se TestProject Co verse verse javagent - andre 2 222 ° + tot 2022 * A data 1 Instituted C + data data data data data data data da	Spence Enterprise       Ket 421         Spence Enterprise       Color Article Co	By Department         Ext d a d a d a           66         T Cest DProject         Co         A d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a         →         B a d a d a d a d a d a d a d a d a d a	Spectrow         Media index         Spectrow         Spectrow	by prove heterprise PS TestProject	by prove future	by prove heterprise PS TestProject	Arrend Marrendia Set TestProject () units () u	by experience between the server of the ser	Per de la d	by the field of t

#### 비교 기준 분석\*

분석 결과를 비교할 기준으로써 해당 프로젝트의 분석 중 **진행 중**, **중지**, **완료**된 분석을 선택할 수 있습니 다.

### 비교 대상 분석\*

분석 결과를 비교할 대상으로써 해당 프로젝트의 분석 중 **비교 기준 분석** 이후에 수행한 **진행 중**, **중지**, **완** 료된 분석을 선택할 수 있습니다.

Warning: 진행 중인 분석을 선택하는 경우 진행 정도에 따라 비교 결과가 다를 수 있다는 점에 유의 하세요.

## 클라이언트 CLI로 프로젝트 확인

### 클라이언트 CLI: 프로젝트 목록 확인하기

Sparrow Enterprise 클라이언트 CLI에서 프로젝트 목록을 확인하는 방법은 다음과 같습니다.

1. 명령 프롬프트를 실행하세요.

2. \*\*{Sparrow Enterprise 클라이언트 설치 디렉토리}\*\*로 이동하세요.

3. Linux 환경에서는 sparrow-cli 파일과 list project 명령어 및 옵션을 입력하세요.

```
./sparrow-cli list project -s https://localhost:10880 -u admin -p
/home/user/workspace/password.txt
```

4. Windows 환경에서는 sparrow-cli.cmd 파일과 list project 명령어 및 옵션을 입력하세요.

sparrow-cli.cmd list project -s https://localhost:10880 -u admin -p
C:\workspace\password.txt

5. 아래 내용을 참고하여 옵션을 입력하고 실행하세요.(\*는 필수 입력 항목)

#### -s 또는 --server\*

연결하려는 Sparrow Enterprise 서버의 IP 주소 및 포트 번호입니다.(예시: -s {Sparrow Enterprise 서 버 IP 주소}:{포트 번호})

#### -u 또는 -–user\*

프로젝트 목록을 확인하려는 사용자 계정의 ID입니다.(예시: -u {사용자 ID})

#### -p 또는 --password

분석을 수행하려는 사용자 계정의 비밀번호를 저장한 txt 파일의 위치입니다. 이 옵션에 값을 입력하지 않은 경우 사용자 계정의 비밀번호를 입력하라는 메시지가 추가로 표시되며 해당 메시지에 비밀번호를 입력하면 됩니다.(예시: -p {txt 파일 경로})

그러면 프로젝트 이름, 프로젝트 키, 마지막 작업, 마지막 작업의 작업 시작 일시, 프로젝트 생성 일시가 표시 됩니다.

#### 클라이언트 CLI: 프로젝트 상세 정보 확인하기

Sparrow Enterprise 클라이언트 CLI에서 프로젝트 상세 정보를 확인하는 방법은 다음과 같습니다.

1. 명령 프롬프트를 실행하세요.

2. \*\*{Sparrow Enterprise 클라이언트 설치 디렉토리}\*\*로 이동하세요.

3. Linux 환경에서는 sparrow-cli 파일과 get project 명령어 및 옵션을 입력하세요.

./sparrow-cli get project -s https://localhost:10880 -u admin -p
/home/user/workspace/password.txt -k myapp

4. Windows 환경에서는 sparrow-cli.cmd 파일과 get project 명령어 및 옵션을 입력하세요.

sparrow-cli.cmd get project -s https://localhost:10880 -u admin -p C:\workspace\password.txt -k myapp

5. 아래 내용을 참고하여 **옵션**을 입력하고 실행하세요.(\*는 필수 입력 항목)

#### -s 또는 --server\*

연결하려는 Sparrow Enterprise 서버의 IP 주소 및 포트 번호입니다.(예시: -s {Sparrow Enterprise 서 버 IP 주소}:{포트 번호})

#### -u 또는 -–user\*

프로젝트 상세 정보를 확인하려는 사용자 계정의 ID입니다.(예시: -u {사용자 ID})

#### -p 또는 --password

분석을 수행하려는 사용자 계정의 비밀번호를 저장한 txt 파일의 위치입니다. 이 옵션에 값을 입력하지 않은 경우 사용자 계정의 비밀번호를 입력하라는 메시지가 추가로 표시되며 해당 메시지에 비밀번호를 입력하면 됩니다.(예시: -p {txt 파일 경로})

#### -k 또는 --key\*

확인할 프로젝트의 프로젝트 키입니다.(예시: -k {프로젝트 키})

그러면 프로젝트 키, 프로젝트 이름, 생성 시간, 마지막 작업, 마지막 작업의 작업 ID, 작업 유형, 작업 시작 일 시, 작업 완료 일시, 작업 상태, 총 이슈 수, 분석을 수행한 사용자 ID, 사용자 이름이 표시됩니다.

'클라이언트 CLI로 작업 확인

## 클라이언트 CLI: 작업 이력 확인하기

Sparrow Enterprise 클라이언트 CLI에서 최근 작업 이력을 확인하는 방법은 다음과 같습니다.

1. 명령 프롬프트를 실행하세요.

2. \*\*{Sparrow Enterprise 클라이언트 설치 디렉토리}\*\*로 이동하세요.

3. Linux 환경에서는 sparrow-cli 파일과 list analysis 명령어 및 옵션을 입력하세요.

./sparrow-cli list analysis -s https://localhost:10880 -u admin -p
/home/user/workspace/password.txt -k myapp

4. Windows 환경에서는 sparrow-cli.cmd 파일과 list analysis 명령어 및 옵션을 입력하세요.

sparrow-cli.cmd list analysis -s https://localhost:10880 -u admin -p C:\workspace\password.txt -k myapp

5. 아래 내용을 참고하여 옵션을 입력하고 실행하세요.(\*는 필수 입력 항목)

#### -s 또는 --server\*

연결하려는 Sparrow Enterprise 서버의 IP 주소 및 포트 번호입니다.(예시: -s {Sparrow Enterprise 서 버 IP 주소}:{포트 번호})

#### -u 또는 -–user\*

작업 이력을 확인하려는 사용자 계정의 ID입니다.(예시: -u {사용자 ID})

#### -p 또는 --password

분석을 수행하려는 사용자 계정의 비밀번호를 저장한 txt 파일의 위치입니다. 이 옵션에 값을 입력하지 않은 경우 사용자 계정의 비밀번호를 입력하라는 메시지가 추가로 표시되며 해당 메시지에 비밀번호를 입력하면 됩니다.(예시: -p {txt 파일 경로})

#### -k 또는 --key

분석 작업을 수행할 프로젝트의 프로젝트 키입니다. 이 옵션을 입력하면 해당 프로젝트에서 수행된 최근 작업을 표시합니다. 이 옵션에 값을 입력하지 않으면 모든 프로젝트에서 수행된 최근 작업을 표시합니다.(예 시: -k {프로젝트 키})

그러면 작업 ID, 프로젝트 키, 작업의 작업 유형, 작업 상태, 진행률, 작업에서 검출된 총 이슈 수, 작업 시작 일시, 작업 완료 일시가 표시됩니다.

#### 클라이언트 CLI: 작업 상세 정보 확인하기

Sparrow Enterprise 클라이언트 CLI에서 작업 상세 정보를 확인하는 방법은 다음과 같습니다.

- 1. 명령 프롬프트를 실행하세요.
- 2. \*\*{Sparrow Enterprise 클라이언트 설치 디렉토리}\*\*로 이동하세요.
- 3. Linux 환경에서는 sparrow-cli 파일과 get analysis 명령어 및 옵션을 입력하세요.

```
./sparrow-cli get analysis -i 49 -s https://localhost:10880 -u admin -p
/home/user/workspace/password.txt
```

4. Windows 환경에서는 sparrow-cli.cmd 파일과 get analysis 명령어 및 옵션을 입력하세요.

```
sparrow-cli.cmd get analysis -i 49 -s https://localhost:10880 -u admin -p
C:\workspace\password.txt
```

5. 아래 내용을 참고하여 옵션을 입력하고 실행하세요.(\*는 필수 입력 항목)

#### -i 또는 --id\*

확인할 작업의 고유한 ID입니다.(예시: -i {작업 ID})

#### -s 또는 --server\*

연결하려는 Sparrow Enterprise 서버의 IP 주소 및 포트 번호입니다.(예시: -s {Sparrow Enterprise 서 버 IP 주소}:{포트 번호})

#### -u 또는 -–user\*

작업 상세 정보를 확인하려는 사용자 계정의 ID입니다.(예시: -u {사용자 ID})

#### -p 또는 ---password

분석을 수행하려는 사용자 계정의 비밀번호를 저장한 txt 파일의 위치입니다. 이 옵션에 값을 입력하지 않은 경우 사용자 계정의 비밀번호를 입력하라는 메시지가 추가로 표시되며 해당 메시지에 비밀번호를 입력하면 됩니다.(예시: -p {txt 파일 경로})

그러면 프로젝트 키, 프로젝트 이름, 마지막 작업의 작업 ID, 작업 유형, 작업 시작 일시, 작업 완료 일시, 작업 상태, 총 이슈 수, 분석을 수행한 사용자 ID, 사용자 이름이 표시됩니다.

## 최근 이슈 확인하기

**이슈 목록**에는 Sparrow Enterprise에서 1) 마지막으로 시작한 전수 분석 및 해당 전수 분석의 수시 분석 2) 마 지막으로 완료되거나 수행 중인 방어 작업에서 검출된 이슈가 표시됩니다.

**Tip**: 전수 분석의 이전에 수행된 분석의 상세 데이터를 확인하는 방법은 작업 이력 확인하기를 참고 하세요.

따라서 이슈 목록을 확인할 때 주의해야 할 점이 있습니다. 먼저, 이슈 목록에는 하나 이상의 작업, 즉, 하나 의 전수 분석과 다수의 수시 분석의 결과가 포함될 수 있습니다. 앞서 분석에서 설명한 것처럼 **수시 분석**이 이전에 수행한 **전수 분석**의 결과를 업데이트하기 때문입니다. 또한, 여러 분석에서 동일한 이슈 검출 규칙으로 특정 자산을 분석한 경우 검출되는 이슈의 구분자가 동일한 상황이 발생할 수 있습니다. 이 경우에 이전 분석에서 발견한 이슈가 새로 시작한 분석에서도 발견된다면 하 나의 이슈로 표시합니다. 하지만 이전 분석의 이슈가 새로운 분석에서 발견되지 않는다면 해당 이슈가 사라 졌다고 판단하고 이슈 목록에 표시하지 않습니다.

**Tip**: 만약 프로젝트를 진행하는 도중 파일의 이름을 변경하거나 파일을 삭제했다면 전수 분석을 수행 하는 것이 정확한 결과를 확인하는데 도움이 됩니다.

소스코드 이슈

문 <b>TestProject ()</b> · 한타임에이?	상세 정보 🂽 🚱	1 <u>시간 전</u> <sup>***</sup> · 방어 <u>44</u>	시간 전		내보내기 🗸 분석 플라 비교하기 작업 아제	코기 새
<ol> <li>진행 중인 작업의 결과에 따라 자산,</li> </ol>	이슈 또는 컴포넌트 정보가	변경될 수 있습니다.				진행 링
Q, 검색어를 입력하세요	88 프로젝트 홈				요약 이슈 자	난 컴
<mark>는</mark> 파일						
Po apache-maven-3.3.9.zip     Po aspnet/CheckerUnitTest	Q, 검색어를 두 글자	이상 입력하세요.		필터 😢 🗸	목록 내보내기 이슈 처리하기 🗸 20개씩 보기	~ 열편
> Eo c-simple	제외 여부: 신청, 해당 답	없음 ✔ 유형: 소	▶스코드 ✔			
> 📴 C-\Testcode	이슈 ID 🗸	유형 💲	위험도 💲 이	슈이를 💲	자산 💲 이슈상태	담당지
> Po objc/parse_error	7530373	🥺 소스코드	HIII 사	용되지 않은 지역 변수	aspnet/CheckerUnitTest/XPathInjectionASPNETTest.cs 이확인	-
> Po sca_all_version.zip	7530372	🤒 소스코드	····· 안	전하지 않은 로깅	aspnet/CheckerUnitTest/XPathInjectionASPNETTest.cs 육인	-
URL	7530371	🥺 소스코드	iiii q	외 정보 노출	aspnet/CheckerUnitTest/XPathInjectionASPNETTest.cs 이희인	-
http://dastapp.fasoo.com:9090/W	7530370	😐 소스코드	<b>।।</b> ।। त	나치게 일반적인 예외 처리	aspnet/CheckerUnitTest/XPathInjectionASPNETTest.cs 미원인	-
테스트 케이스	7530369	🐵 소스코드	1111 사	용되지 않은 지역 변수	aspnet/CheckerUnitTest/XPathInjectionASPNETTest.cs 미확인	-
	7530368	0 소스코드	····· 안	전하지 않은 로깅	aspnet/CheckerUnitTest/XPathInjectionASPNETTest.cs 미테인	-
	7530367	😕 소스코드	<b>III</b> 0	외 정보 노출	aspnet/CheckerUnitTest/XPathInjectionASPNETTest.cs 미웨인	-
	7530366	🥺 소스코드	মা ম	나치게 일반적인 예외 처리	aspnet/CheckerUnitTest/XPathInjectionASPNETTest.cs 미테인	-
	7530365	🤒 소스코드	사	용되지 않은 지역 변수	aspnet/CheckerUnitTest/WeakPasswordRequirementsASPNETTest.cs 미웨인	-
	7530364	🤕 소스코드	비비빈	catch 블록	aspnet/CheckerUnitTest/WeakPasswordRequirementsASPNETTest.cs 미리인	-
	7530363	🤒 소스코드	사	용되지 않은 지역 변수	aspnet/CheckerUnitTest/WeakPasswordRequirementsASPNETTest.cs 미웨인	-
	7530362	🧼 소스코드	빈	catch 블록	aspnet/CheckerUnitTest/WeakPasswordRequirementsASPNETTest.cs 미리아인	-
	7530361	😕 소스코드		용되지 않은 파라미터	aspnet/CheckerUnitTest/UnrestrictedFileUploadASPNETTest.cs 미웨인	-
	7530360	🐵 소스코드	배비사	용되지 않은 파라미터	aspnet/CheckerUnitTest/UnrestrictedFileUploadASPNETTest.cs ାଣ୍ଟାତ୍ରା	-
	7530359	🐵 소스코드	배비사	용되지 않은 지역 변수	aspnet/CheckerUnitTest/SanitizeUntrustedRegexASPNETTest.cs ାଣାହା	-
	7530358	👳 소스코드	1111 B	수에 대해 Equals 사용	aspnet/CheckerUnitTest/RelianceOnUntrustedInputsASPNETTest.cs ାୟାତ୍ର	-
	7530357	0 소스코드	IIII H	ttpOnly가 아닌 쿠키	aspnet/CheckerUnitTest/PersistentCookleASPNETTest.cs 미페인	-
	7530356	😕 소스코드	н	ttpOnly가 아닌 쿠키	aspnet/CheckerUnitTest/PersistentCookieASPNETTest.cs 미페인	-
	7530355	00 소스코드	н	ttpOnly가 아닌 쿠키	aspnet/CheckerUnitTest/PersistentCookieASPNETTest.cs 미파인	-
	-					

Sparrow SAST/SAQT를 통해 소스코드를 검사하면 이슈 검출 규칙에 따라 잠재적인 취약점이나 품질 관련 문제를 찾아낼 수 있습니다. 이 이슈를 **소스코드 이슈**라고 하고 이슈 탭에서 확인할 수 있습니다. **최근 이슈** 에서 **소스코드 이슈**에 표시되는 내용은 다음과 같습니다.

#### 이슈 ID

이슈의 고유한 구분 ID입니다.

이슈 유형

이슈를 검출한 분석 방법을 검출한 도구별로 구분하여 **소스코드**, **컴포넌트**, 웹 취약점, 자가 방어 중에 하 나로 표시합니다. 여기서는 소스코드 이슈이므로 **소스코드**로 표시됩니다.

#### 위험도

소스코드에서 검출된 이슈의 위험도이며 **매우 높음**, **높음**, **보통**, **낮음**, **매우 낮음**이라는 5단계로 구분합니 다.

#### 이슈 이름

소스코드에서 검출된 이슈의 이름입니다. 이슈 이름은 이슈를 검출한 이슈 검출 규칙의 이름을 그대로 사용합니다. 따라서 같은 이슈 검출 규칙으로 찾아낸 이슈의 이름이 동일하게 표시됩니다.

#### 자산

이슈가 검출된 분석 대상이며 **파일** 또는 URL의 형태로 표시됩니다. **파일** 자산을 표시할 때 웹 분석의 경 우 분석 대상으로 선택한 zip 파일의 이름을 제외한 상대 경로로 표시되고, 클라이언트 GUI 및 CLI 분석의 경 우 해당 파일의 절대 경로로 표시됩니다.

#### 이슈 상태

해당 이슈의 검토 상태를 미확인, 확인, 해결 중 하나로 표시됩니다.(기본값: 미확인)

#### 담당자

해당 이슈를 검토할 담당자를 표시합니다. 담당자를 지정하기 전에는 아무 것도 표시되지 않습니다.

#### 이슈 검출 일시

소스코드 분석에서 해당 이슈를 검출한 일시입니다.

#### 제외 여부

해당 이슈가 이슈 목록에서 제외되었는지 표시합니다. 제외하도록 신청된 경우 **신청**으로 표시되고 신청 이 승인된 경우 **제외**로 표시됩니다. 이슈를 제외하는 방법은 이슈 제외하기를 참고하세요.

#### 소스코드 이슈 상세 정보

소스코드 이슈 목록에서 이슈를 클릭하면 해당 이슈의 상세 정보 페이지로 이동합니다. 여기에는 소스코드 를 검출한 이슈 검출 규칙에 대한 정보, 이슈의 발생 원인을 찾아가는 내비게이터, 이슈가 검출된 파일의 소 스코드가 표시됩니다. 자세한 내용은 아래를 참고해주세요.

parrow Enterprise					이슈 경로 조작 🧑	
# TestProject	) 상세 정보 💽 🔅			ID Z	2335 D · 언어 ASP · 건물 일시 2024-06-04 10:48:41	
				PathT	versalAS	위험한 예시 안?
프로젝트 키 TestProject 🚺 · 런타임 에이	I전드 없음 · 마지막 분석 ]	<u>56분전</u> ** · 방어 <u>4시</u>	<u>간전</u> ~	aspnet	neckerUnitTest/PathTraversalASPNETTtest.cs	
					using System.Web.UI;	
신영 양인 작업의 결과에 따라 사진	r, 이유 또는 침포턴트 정보가	헌경철 수 있습니다.			using System.web.01.webControis;	
Q、 검색어를 입력하세요				1	//NOTE: To run test code with additional engine options, write options like the below. /* OPT : -show_followers */	
	88 프로젝트 봄			1:	namespace WebFormTest	
▶ 타일 > Ea apache-maven-3.3.9.zip	7530346	🕐 소스코드	m	지나? 1	<pre>public partial class PathTraversal : System.Web.UI.Page </pre>	
> Eo aspnet/CheckerUnitTest	7530345	🧼 소스코드		잘못된 <sup>11</sup> 10	<pre>protected void Page_Load(object sender, EventArgs e) {</pre>	
> Concerning Concernin	7530344		m	지나카 11	}	
> E <sub>0</sub> jsp	7530343	🥝 소스코드	m	사용5 <sup>15</sup> 20	<pre>protected void TextBox1_TextChanged(object sender, EventArgs e)</pre>	
Co objc/parse_error     Co sca_all_version.zip	7530342	🥺 소스코드	m	HTTI 2:	✓ { 원인··추적 규칙 옵션에 따라 클레스 TextBox의 속성 Text을 감출하였으므로 추적하기 시작합니다.	
	7530341	🐠 소스코드	mu –	신뢰 [← 2:	원인·주석 중인 값이 arg에 시상되었습니다. string arg = TextBox1.Text;	
CURL C	7530340	🐠 소스코드	m	에러 0 2	이슈··주적 중인 값이 메소드 File.Delete()의 1번째 매기번수로 사용되었으므로 추적 규칙을 위변했습니다. File.Delete(arg); /* BUG: PATH TRAVERSAL ASPNET */	
http://dastapp.fasoo.com:9090/W	7530339	0 소스코드		24	}	
狂 테스트 케이스				2	<pre>protected void TextBox2_TextChanged(object sender, EventArgs e)</pre>	
	7530338	🐠 소스코드		제한5 21	<pre>     {       string arg = TextBox2.Text:     </pre>	
	7530337	🥝 소스코드	m	명속전 21 34	<pre>if (arg.IndexOf('\\') &gt; -1    arg.IndexOf('/') &gt; -1) {</pre>	
	7530336	🥺 소스코드	m	명속? 32	<pre>Response.Write("Bad File Name"); }</pre>	
	7530335	🕐 소스코드	m	33 경로 : 34	else (	
	7530334	🥹 소스코드	m	31 신뢰함 31	<pre>File.Delete(arg); // not bug }</pre>	
	전체 77,425 건 21 - 40 표	E시됨		3	}	
					사용자 선택 이전 미환인 확인 해결	이슈 제외

#### ✓ 이슈 검출 규칙

이슈 검출 규칙의 이름과 위험도, 언어 및 설명이 표시됩니다. 이슈 검출 규칙에 대한 더 자세한 설명은 **프** 로젝트 설정의 작업 프로파일에서 확인할 수 있습니다. 자세한 내용은 이슈 검출 규칙 확인하기를 참고하세 요.

#### √ 소스코드 파일

이슈가 검출된 파일의 실제 소스코드가 표시됩니다. 하나의 파일당 하나의 탭으로 구성되어 이슈가 여러 파일에 걸쳐서 발생하는 경우 여러 개의 탭이 표시됩니다.

여기서는 소스코드 상에 이슈와 관련된 내용을 메시지로 확인할 수 있습니다. 또한 오른쪽에 있는 **내비게** 이터와 연결되어 내비게이터에 표시된 특정 아이콘을 클릭하면 소스코드의 해당하는 라인으로 이동합니다. 내비게이터와 동일하게 이슈는 빨강색, 원인은 파랑색, 분기는 회색, 프레임워크는 녹색으로 표시됩니다. 각 정보에 대한 자세한 내용은 아래를 참고하세요.

#### 이슈

소스코드에서 이슈가 발생하는 결정적인 지점이며 **빨강색** 메시지가 표시됩니다. 내비게이터에서는 빨강 색 경고 아이콘으로 표시됩니다.

#### 원인

이슈가 발생하는 원인이며 **파랑색** 메시지가 표시됩니다. 내비게이터에서는 파랑색 삽입 아이콘으로 표시 됩니다.

#### 분기

이슈와 연관된 부분 실행 코드가 있는 부분이며 **회색** 메시지가 표시됩니다. 내비게이터에서는 회색 분기 아이콘으로 표시됩니다.

#### 프레임워크

이슈의 원인에서 발생 지점으로 전개되는 과정이며 **녹색** 메시지가 표시됩니다. 내비게이터에서는 녹색 프레임워크 아이콘으로 표시됩니다.

#### ✔ 예시 및 수정 방법

#### 위험한 예시

**위험한 예시** 버튼을 클릭하면 이슈 검출 규칙에서 검출하는 소스코드 예시와 함께 해당하는 라인에 대한 설명을 표시합니다.

#### 안전한 예시

**안전한 예시** 버튼을 클릭하면 **위험한 예시**를 수정한 소스코드 예시와 함께 해당하는 라인에 대한 설명을 표시합니다.

#### 수정 방법

**수정 방법** 버튼이 있는 경우 해당 버튼을 클릭하면 이슈를 수정할 수 있는 방법과 함께 설명을 표시합니 다.

#### √ 내비게이터

소스코드 오른쪽에 있는 바에 이슈가 발생한 원인부터 이슈가 발생한 지점까지의 과정을 소스코드 라인 및 아이콘으로 표시합니다. 아이콘에 마우스를 이동하면 해당하는 메시지가 표시되고, 아이콘을 클릭하면 왼쪽에 있는 **소스코드**에서 해당하는 라인으로 이동하게 됩니다.

#### √ 이슈 톡

발견된 이슈를 어떻게 처리했는지를 확인하기 위해 사용하며 **이슈 의견**, **이슈 담당자**, **이슈 상태**, **이슈 제 외**가 표시됩니다.

이슈 담당자를 지정하거나 이슈 상태를 변경하려면 1) 프로젝트의 프로젝트 구성원으로써 프로젝트 권한 중 2) 이슈 참여 권한을 포함한 프로젝트 역할을 가져야 합니다.

#### 이슈 의견

해당 이슈에 대한 검토 의견을 입력하거나 입력된 의견을 표시합니다.

#### 이슈 담당자

해당 이슈를 검토할 담당자를 표시합니다. 권한 있는 사용자 혹은 사용자 그룹 중에서 선택할 수 있으며 담당자를 지정하기 전에는 아무 것도 표시되지 않습니다.

#### 이슈 상태

이슈가 검출되면 해당 이슈를 확인하고 해결하거나, 오탐 또는 다른 원인으로 인해 이슈에서 제외하도록 처리해야 합니다. 이슈를 어떻게 처리했는지 표시하기 위해서 이슈마다 **이슈 상태**를 다음과 같이 표시합니 다.

- 미확인 : 담당자가 검출된 이슈를 아직 검토하지 않음
- 확인 : 담당자가 해당 이슈를 확인함
• 해결 : 담당자가 해당 이슈에서 발견된 문제를 해결함

#### 이슈 제외

해당 이슈가 오탐이거나 다른 이유로 인해 이슈 목록에서 제외하려는 경우 이슈 제외 버튼을 클릭하여 이 슈를 제외하도록 신청하거나 신청을 수락 또는 거절할 수 있습니다. 자세한 내용은 이슈 제외하기를 참고하 세요.

Warning: 이슈 목록에서는 제외된 이슈를 표시하지 않도록 기본값으로 필터링합니다. 이슈 목록에 서 제외된 이슈를 확인하려면 해당 필터를 제거하세요.

## 이전 및 다음 이슈

이슈 목록에 표시된 이전 이슈 또는 다음 이슈로 이동합니다.

이슈 제외 | 결재

Sparrow Enterprise에서는 소스코드 이슈, 컴포넌트 이슈, 웹 취약점 이슈 및 자가 방어 이슈를 검출합니다. 하지만 이슈 중에는 잠재적으로 문제가 될 가능성이 있을 뿐 실제로 보안 취약점 혹은 품질 문제라고 볼 수 없는 경우가 있습니다. 이러한 경우 보안 진단원 혹은 동일한 자격의 전문가라고 할 수 있는 사용자가 특정 이슈를 문제에서 제외시킬 수 있도록 만든 기능이 **이슈 제외**입니다.

이 기능을 통해 제외된 이슈는 기본적으로 이슈 목록에 표시되지 않도록 설계되어 있습니다. 또한 프로젝트 나 작업의 이슈 수에도 포함되지 않습니다. 작업 보고서를 출력할 때도 이슈 목록에는 포함되지 않고 제외된 이슈라는 별도 목록에만 표시됩니다.

이슈 제외는 문제가 되지 않는 이슈를 발견했을 때 해당 이슈를 제외하도록 결재를 요청한 후 요청된 결재를 처리하는 방식으로 동작합니다. 만약 제외가 요청된 이슈에 여전히 문제의 소지가 있다고 판단하는 경우 이 슈 제외를 반려할 수도 있습니다. 이렇게 결재를 요청하고 처리하려면 먼저 결재선을 설정해야 합니다. 결재 선을 설정하지 않는 경우 사용자가 이슈 제외를 요청하는 즉시 이슈가 목록에서 제외됩니다. 자세한 내용은 결재선 관리하기를 참고하세요.

Warning: 일단 이슈 제외 결재가 완료된 이슈는 제외된 이슈에서 제외되지 않은 이슈로 변경될 수 없다는 점에 유의하세요.

#### 이슈 제외 요청하기

이슈 목록에서 이슈 제외를 요청하려는 사용자는, 해당 이슈가 포함된 1) 프로젝트의 **프로젝트 구성원**으로 써 **결재선**에서 설정한 2) **요청 가능 역할** 옵션에 포함된 프로젝트 역할을 가져야 합니다.

1. 이슈 목록에서 이슈 제외를 요청할 이슈를 선택하세요.

2. 오른쪽 아래에 있는 이슈 제외 버튼을 클릭하세요.

🜍 Spa	arrow Enterprise				🔢 이슈 주석문에 비밀번호 노출 🝻	결재 요청 이슈 제외	×
2	器 TestProject 🔘	상세 정보 🔵 😥			ID <u>433896</u> 🜔 · 언어 기타 · 전품 일시 2024-07-10 18:23:24	요청 유형 프로젝트 이슈 제외 <u>TestProject</u> 단	
88 99	Q 검색어를 입력하세요	88 프로젝트 홈		1	WeakPasswordR           aspnet/CheckerUnitTest/WeakPasswordReq.irementsASPNETTest.cs           12         * {	아슈 ID 이슈 유형 13198 IČ 소스코드 이슈 이름	
8 Ø R	Call space-inversion 3.3.9 (p)     Call space-	<ul> <li>○ ♥♠ ID ↓</li> <li>433910</li> <li>433909</li> <li>433908</li> <li>433907</li> <li>433906</li> <li>433905</li> </ul>	89 0 2544 0 2544 0 2544 0 2544 0 2544 0 2544 0	이슈 이 주석 :	<pre>pair t public void CreateUser_Onlick(adject sender, EventArgs args)  v</pre>	수진원에 비밀한 도움 ● 결재 단계 미원보기 ● 추유 PROJECT-USER 의 1개 역할 ● 추유 PROJECT-ADMIN 의 2개 역할	함의 전제
	> @ http://testagp.fecos.com/S990/W 문 14△도 199△	<ul> <li>433903</li> <li>433901</li> <li>433901</li> <li>433901</li> <li>433901</li> <li>433900</li> <li>433899</li> <li>433898</li> <li>433897</li> </ul>	25.44 0 27.44 0 27.44 0 27.44 0 27.44 0 27.44 0 27.44 0	<ul> <li>하구</li> <li>하수</li> <li>하수</li> <li>하수</li> <li>·</li> <li>·<!--</td--><th><pre></pre></th><td>ম মন্দ এই গশুন্দ গুলাগন্য.</td><td></td></li></ul>	<pre></pre>	ম মন্দ এই গশুন্দ গুলাগন্য.	
		<u> </u>	···· 소스코드	 주석문	· 사용자 선택	50	[기기] <mark>요청하기</mark>

3. 결재 단계를 확인하고 이슈를 제외해야 하는 요청 의견을 작성하세요.

Tip: 요청 의견을 입력하지 않아도 결재를 요청할 수 있습니다.

4. 요청하기 버튼을 클릭하세요.

## 이슈 제외 요청 취소하기

이슈 제외 결재를 요청한 사용자는 이슈의 처리 내역 슬라이드에서 신청한 결재를 취소할 수도 있습니다.

1. 이슈 목록에서 이슈 제외 요청을 취소할 이슈를 선택하세요.

2. 오른쪽 아래에 있는 처리 내역 버튼을 클릭하세요.

Sparrow Enterprise					₩Ⅱ 이슈 4	주석문에 비밀번호 노출 🐠	D	결재 요청 <b>195</b>		>
🐁 🏦 TestProject 🔘	3 상세 정보 🔵 🕄	3			ID <u>433896</u> 🖸	· 안이 기타 · 검출 일시 2024-07-10 18:23:24	요청 유 이슈 자	<sup>2</sup> 영 테외	프로젝트 <u>TestProject</u> 년	
38 Q. 검색어를 입력하세요	않 프로젝트 홈				•• 이슈	제외가 요청되어 처리 중입니다.	이슈 ID <u>13198</u>	2 C	이슈 유형 소스코드	
al 다 비원 > Co apache-maven-3.3.9.zip	433904	@ 소스코드	1	함수·	WeakPass aspnet/Checker	wordR UniTest/WeakPasswordRequirementsASPNETTest.cs	이슈 이 주석문	등 에 비밀번호 노출		
	433903	@ 소스코드		함수	12 ~ { 14 ~	ł	0	처리 현황		
D) > C <sub>0</sub> java > C <sub>0</sub> java > C <sub>0</sub> java	433902	@ 소스코드	m	파일	20 21 ~	<pre>public void CreateUser_OnClick(object sender, EventArgs args) {     try</pre>	0	admin(Suport dmin)		이체, 트루크
> En jap	433901	@ 소스코드		주석	23 ¥ 24	{     HembershipUser newUser - Membership.CreateUser(UserName.	.	이슈 제외 요청합니다.		T.O B.M :
<ul> <li>Eo obje/parse_error</li> <li>Eo sca_all_version.zip</li> </ul>	433900	··· 소스코드		함수	25 26 27	Response.Redirect("login.aspx"); } catch (MembershipCreateUserException e)				2024-07-15 18:36
CURL	433898	· 소스코드		클래스	28 29	( )		🍂 PROJECT-USER 의 1개 역할		합의 · 대기 중 ()
<ul> <li>         Intp://211.39.141.177:8080     </li> <li>         Intp://dastapp.fasoo.com:9090/W     </li> </ul>	433897	@ 소스코드	m	파일	31 32	<pre>, public void CreateUser_OnClick2(object sender, EventArgs args)</pre>	•			
經 테스트케이스	433896	🕜 소스코드	mu	주석	33 ¥ 34	{ try		2월 PROJECT-ADMIN 의 4개 역할		[đ재 · 대기 중 (3
	433895	Ø 소스코드		누락된	36 37	<pre>string pass = Password.Text; if (pass.Length &gt;= 8) // Length constraint</pre>				
	433894	④ 소스코드		외부	38 ~	{ 이슈 · 주석문내에 비밀번호 정보가 있습니다.				
	433893	0 소스코드		외부	40 V	if (Regex.IsMatch(pass, ".*[!@w\\\$%\\^\\&\*\\(\))\\ {				
	433892	0 소스코드		외부	41 42 42	<pre>nembershipuser newoser = nembership.createuser(u Response.Redirect("login.aspx"); }</pre>	1			
	<u>433891</u> 전체 21,334 건 18,441 -	<ul> <li> 소스코드</li> <li>- 18,460 표시됨</li> </ul>		외부	44 45 46 47	<pre>// / / / catch (MembershipCreateUserException e) {</pre>				
					다 사용	자선택			5	B아가기 요청 취소하기

3. 요청 취소하기 버튼을 클릭하세요.

이슈 제외 요청 처리하기

이슈 제외를 승인하거나 반려하려면 해당 이슈가 포함된 1) 프로젝트의 **프로젝트 구성원**으로써 **결재선**에서 설정한 2) **처리 가능 역할** 옵션에 포함된 프로젝트 역할을 가져야 합니다.

1. 이슈 목록에서 이미 이슈 제외가 신청된 이슈를 클릭하세요.

2. 오른쪽 아래에 있는 처리 내역 버튼을 클릭하세요.

🧐 s	parrow Enterprise					₩Ⅱ 이슈	주석문에 비밀번호 노출 🛷	0	결재 요청 <b>195</b>		×
2	器 TestProject 🔘	) 상세정보 🔵 🥹				ID <u>433896</u> O	· 언이 기타 · 검출 입시 2024-07-10 18:23:24	요청 유럽 이슈 제	8	프로젝트 TestProject [2]	
**	Q. 검색어를 입력하세요	응 프로젝트 홈				··· 이슈	제외가 요청되어 처리 중입니다.	이슈 ID <u>13198</u>	Ľ	이슈 유형 소스코드	
<u></u>	ि मध > ि apache-maven-3.3.9.zip > C aspnet/CheckerUnitTest	433904	0 소스코드	100	함수	WeakPass aspnet/Checke 12 ~ {	wordR U/UniTest/WeakPasswordRequirementsASPNETTest.cs	이슈 이름 주석문(	: 에 비밀번호 노출 <b>너리 현황</b>		
Q	> Eo c-simple > Eo java > Eo javascript/rule	433902	· 소스코드	m	파일	14 × 20 21 × 22	<pre>{     public void CreateUser_OnClick(object sender, EventArgs args)     {         try         try         try     } }</pre>	0	admin(Superådmin)		이제 . 드로 +
×.	> E jsp > E objc/parse_error	<ul><li>433901</li><li>433900</li></ul>	<ul> <li> 소스코드</li> <li> 소스코드</li> </ul>	1000 1000	주석   함수 -	23 ¥ 24 25	<pre>{     HembershipUser newUser = Membership.CreateUser(UserName.'     Response.Redirect("login.espx");</pre>		이슈 제외 요청합니다.		2024-07-15 18:36:19
	> Lo sca_al_version.zip	433899	소스코드		함수 :	26 27 28 29	} catch (MembershipCreateUserException e) { }	$\odot$	유 PROJECT-USER 의 1개 역할		합의 · 대기 중 0
	<ul> <li>http://211.39.141.177-8080</li> <li>http://dastapp.fasoo.com:9090/W</li> </ul>	433897	@ 소스코드		파일	30 31 32 33 ¥	<pre>} public void CreateUser_OnClick2(object sender, EventArgs args) {</pre>	•	은유 PROJECT-ADMIN 외 4개 역할		결재 · 대기 중 0
	征 테스트 케이스	433896	<ul> <li> 소스코드</li> <li> 소스코드</li> </ul>		주석된 누락된	34 35 🗸 36	try ( string pass - Password.Text;				
		433894	<ul> <li>소스코드</li> <li>소스코드</li> </ul>		외부 : 외부 :	37 38 V 9 39	if (pass.length >= 8) // Length constraint ( <u>이슈 · 주석문내에 비밀번호 정보가 있습니다.</u> if (Regex.ls/Match(pass, "[1@#\/\$\$\\^\\&\\*\\(\))\\;				
		433892	④ 소스코드	m	외부	40 ∨ 41 42 43	<pre>{     HembershipUser newUser = Hembership.CreateUser(U     Response.Redirect("login.aspx"); }</pre>	admin	님은 PROJECT-ADMIN 역할로 결제 단계를	처리할 수 있습니다.	
		전체 21,334 건 18,441 -	<ul> <li>         소스코드     </li> <li>18,460 표시됨</li> </ul>		외부	44 45 46 47	<pre>} } catch (MembershipCreateUserException e) {</pre>	결재	처리 의견을 입력하세요.		
						<b>\</b>	자 선택			돌아가기	반려하기 승인하기

3. 결재 단계를 확인하고 이슈를 제외해야 하는 처리 의견을 작성하세요.

Tip: 처리 의견을 입력하지 않아도 결재를 처리할 수 있습니다.

4. 결재 단계인 경우 이슈 제외를 허락하려면 승인하기 버튼을 클릭하고 이슈 제외를 거절하려면 반려 하기 버튼을 클릭하세요. 합의 단계인 경우 이슈 제외에 찬성하려면 동의하기 버튼을 클릭하고 이슈 제외에 반대하려면 반대하기 버튼을 클릭하세요.

					외된 이슈 우익문에 비밀면호 노발 🥝	☑ 일세	1.0 100	×
器 TestProject 🔘	· 상세 정보 🔵 🔅			ID <u>13198</u>	○ · 안이 기타 · 검출 일시 2024-07-15 17:36:47	요청 유행 이슈 제외	프로젝트 <u>TestProject</u> 12	
Q 검색어를 입력하세요	※ 프로젝트 홈			0	이슈 제외 요청이 승인되었습니다. 제외된 이슈는 이슈 수에 포함되지 않습니다.	이슈 ID <u>13198</u> [소	이슈 유형 소스코드	
ि मध				Weak	PasswordR	이슈 이름 주석문에 비	일번호 노출	
> Pa aspet/CheckerUnitTest	Q, 검색어를 두 글자	가 이상 입력하세요.		aspnet/Cl	eckerUnitTest/WeakPasswordRequirementsASPNETTest.cs			
> Co c-simple	제외 여부: 신청, 해당	없음 🗸		12 ~	1	③ 처리	현황	
> E jsp > E objc/parse_error	↓ QI ♠!0	유형 💲	위험도 💲	19 20 21 ~	<pre>public void CreateUser_OnClick(object sender, EventArgs args) {</pre>	0	admin(SuperAdmin)	요청 - 등록 1
> Eo sca_all_version.zip	13198	🕐 소스코드		주석원 22 23 V	try (		요청	
URL	13197	😡 소스코드		<sup>24</sup> 초기호 <sub>25</sub>	<pre>HembershipUser newUser = Membership.CreateUser(UserName. Response.Redirect("login.aspx");</pre>			2024-07-15 17:43:5
	13196	④ 소스코드		실모E 27	<pre>} catch (MembershipCreateUserException e)</pre>		-	
狂 테스트케이스	13195	@ 소스코드		28 도달: 29	{ }		proView(Viewer)	합의 · 반대 ×
	13194	@ 소스코드		30 쓸모t 31 32	<pre>} public void Createllser Op(lick2(object sender, Eventages ares)</pre>			2024-07-15 17:47:4
	13193	@ 소스코드	ш	0으로 <sup>33</sup> ~ 34	{ { try		admin(SuperAdmin)	결재 - 승인 🗸
	13192	🕐 소스코드	100	한빈. 35 ~	{     string mass = Passund Taxt-		SPA-15639으로 인해 이슈 제의 승인합니다.	
	13191	@ 소스코드		한번. 37 38 V	if (pass.Length >= 8) // Length constraint {			2024-07-15 18:27:3
	13190	Ø 소스코드	1111	한번 🚺 39	이슈 · 주석문내에 비밀번호 정보가 있습니다.           1f (Regex.IsHatch(pass, ".*(!@#\\\$%\\^\\&\\*\\(\\)\\)			
	13189	@ 소스코드	m	40 ~ 잘못한 41	{ HembershipUser newUser - Membership.CreateUser(U	a		
	13188	@ 소스코드		42 한번. 43 44	<pre>kesponse.kedirect('login.aspx'); }</pre>			
	13187	@ 소스코드	IIII	잘못된 <sup>45</sup> 46	} catch (MembershipCreateUserException e)			
	12196			21 H				

5. 결재 단계가 모두 완료되면 이슈가 제외됩니다.

Tip: 단, 합의의 경우 반대하기를 선택한 경우에도 다음 단계로 결재를 계속 진행합니다.

최근 자산 확인하기

# TestProject 🜑	상세 정보	e 🛑 e	3			L	내보내기 🗸	분석 결과 비교	하기 작업	이력 보기 새 작업 시
프로젝트 키 <u>TestProject</u> 🖒 · 런타임 에이전:	드 없음 ·	마지막 분석	<u>49분 전 <sup></sup> · 방어 4시간 전 <sup></sup></u>							
진행 중인 작업의 결과에 따라 자산, 0	이슈 또는 킹	넘포넌트 정보	가 변경될 수 있습니다.							진행 중인 작업
Q. 검색어를 입력하세요	88 프로 <sup>8</sup>	医音						요약	이슈	자산 컴포넌트
• मध									-	
> Co apache-maven-3.3.9.zip	Q Z	색어를 두 글	자 이상 입력하세요. 필터 🖌					목록 내보내기	20개씩 보	기 🗸 열편집 -
<ul> <li>Complete control and a complete control and a complete</li></ul>	0	유형 💲	식별자 💲	총 이슈 💲	매우 높음 \Rightarrow	높음 🛈	보통 💲	낮음 💲	매우 낮음 💲	최근 작업 일시 🔸
> Pa iso	$\bigcirc$	파일	apache-maven-3.3.9.zip	-	-		-	-	-	2024-06-04 10:44:03
> E objc/parse_error		파일	apache-maven-3.3.9.zip/bin/m2.conf					-	-	2024-06-04 10:44:03
> Co sca_all_version.zip	$\Box$	파일	apache-maven-3.3.9.zip/bin/mvn	-	-	-	-	-	-	2024-06-04 10:44:03
n URL	0	파일	apache-maven-3.3.9.zip/bin/mvn.cmd	-				-	-	2024-06-04 10:44:03
http://dastapp.fasoo.com:9090/W 테스트 케이스		파일	apache-maven-3.3.9.zip/bin/mvnDebug	-	-	-	-	-	-	2024-06-04 10:44:03
征 테스트 케이스		파일	apache-maven-3.3.9.zip/bin/mvnDebug.cmd	-	-	-	-	-	-	2024-06-04 10:44:03
		파일	apache-maven-3.3.9.zip/bin/mvnyjp		-			-	-	2024-06-04 10:44:03
		파일	apache-maven-3.3.9.zip/boot/plexus-classworlds-2.5.2.jar	-	-	-	-	-	-	2024-06-04 10:44:03
	0	파일	apache-maven-3.3.9.zip/conf/settings.xml	-				-	-	2024-06-04 10:44:03
		파일	apache-maven-3.3.9.zip/conf/toolchains.xml	-	-			-	-	2024-06-04 10:44:03
	0	파일	apache-maven-3.3.9.zip/lib/aether-api-1.0.2.v20150114.jar	1		-	1	-	-	2024-06-04 10:44:03
		파일	apache-maven-3.3.9.zip/lib/aether-connector-basic-1.0.2.v20150114.jar	1			1			2024-06-04 10:44:03
		파일	apache-maven-3.3.9.zip/lib/aether-impl-1.0.2.v20150114.jar	1	-	-	1	-	-	2024-06-04 10:44:03
		파일	apache-maven-3.3.9.zip/lib/aether-spi-1.0.2.v20150114.jar	1	-	-	1	-	-	2024-06-04 10:44:03
		파일	apache-maven-3.3.9.zip/lib/aether-transport-wagon-1.0.2.v20150114.jar	1			1		-	2024-06-04 10:44:03
		파일	apache-maven-3.3.9.zip/lib/aether-util-1.0.2.v20150114.jar	1	-	-	1	-	-	2024-06-04 10:44:03
		파일	apache-maven-3.3.9.zip/lib/aopalliance-1.0.jar						-	2024-06-04 10:44:03
		파일	apache-maven-3.3.9.zip/lib/cdi-api-1.0.jar			-	-	-	-	2024-06-04 10:44:03
	0	파일	apache-maven-3.3.9.zip/lib/commons-cli-1.2.jar	-	-	-	-	-	-	2024-06-04 10:44:03
		파일	apache-maven-3.3.9.zip/lib/commons-io-2.2.jar	1	1				-	2024-06-04 10:44:03
					_					

**자산 목록**에는 Sparrow Enterprise에서 마지막으로 시작한 전수 분석 및 해당 전수 분석의 수시 분석에서 검 출된 자산이 표시됩니다.

**Tip**: 전수 분석의 이전에 수행된 분석의 상세 데이터를 확인하는 방법은 작업 이력 확인하기를 참고 하세요.

자산 트리 혹은 자산 목록을 확인할 때 주의해야 할 점이 있습니다. 먼저, 자산 목록에는 하나 이상의 작업, 즉, 하나의 전수 분석과 다수의 수시 분석의 결과가 포함될 수 있습니다. 앞서 <mark>분석</mark>에서 설명한 것처럼 **수시** 분석이 이전에 수행한 **전수 분석**의 결과에 변경된 결과를 업데이트하기 때문입니다.

이전 분석에서 식별한 자산이 새로 시작한 분석의 동일한 경로에서도 발견된다면 하나의 자산으로 표시합 니다. 하지만, **이슈**와 달리 한 번 발견한 자산은 목록에서 제거되지 않습니다.

Warning: 단, 웹 분석의 경우에는 자산의 절대 경로를 파악할 수 없기 때문에 이전 분석과 동일한 경 로에 있는 자산을 분석하더도 다른 자산으로 식별합니다.

자산을 식별하는 기준인 식별자는 파일인 경우 상대 혹은 절대 경로이고, 웹 사이트인 경우 리소스가 위치한 URL입니다. 따라서, 만약 프로젝트를 진행하는 도중 대상 파일의 이름을 변경하거나 파일을 삭제했다면 전 수 분석을 수행하는 것이 정확한 결과를 확인하는데 도움이 됩니다.

## 유형

이슈가 검출된 분석 대상을 **파일** 또는 **URL** 중에 하나로 구분합니다. 소스코드 분석과 컴포넌트 분석에서 는 자산이 파일로 표시되고, 웹 취약점 분석에서는 자산이 URL로 표시됩니다. 자가 방어의 경우 명확한 자산 이 표시되지 않습니다.

## 식별자

자산을 식별하는데 사용하는 고유한 문자열이며, 보통 자산의 경로 혹은 URL로 표시됩니다. 같은 프로젝 트 안에서 식별자가 동일하다면 해당 자산은 동일한 자산입니다.

**파일** 자산을 표시할 때 웹 분석의 경우 자산이 분석 대상으로 선택한 zip 파일 이름을 제외한 상대 경로로 표시되고, 클라이언트 GUI 및 CLI 분석의 경우 자산이 절대 경로로 표시됩니다.

#### 총 이슈

검출된 자산에 포함된 전체 이슈의 개수입니다.

## 매우 높음/높음/보통/낮음/매우 낮음

자산에서 검출된 위험도별 이슈의 개수이며 위험도를 **매우 높음**, **높음**, **보통**, **낮음**, **매우 낮음**이라는 5단계 로 구분합니다.

## 마지막 작업 일시

자산이 발견된 마지막 작업의 시작 일시를 표시합니다.

# 작업 보고서

사용자는 프로젝트에서 수행한 소스코드 분석, 컴포넌트 분석, 웹 취약점 분석, 자가 방어의 결과를 공유하 고 검출된 이슈를 처리한 상태를 확인하기 위해서 **작업 보고서**를 출력할 수 있습니다.

작업 보고서에는 작업 요약 정보, 위험도별 이슈 수, 레퍼런스별 이슈 수, 검출 결과 상세 및 제외된 이슈 목 록이 포함됩니다. 특히, 이슈 목록에서 제외된 이슈는 분석 보고서의 다른 내용에 포함되지 않고 제외된 이 슈 목록에서만 별도로 확인할 수 있습니다. 보고서 템플릿에 대한 자세한 내용은 보고서 템플릿 관리하기를 참고하세요.

Warning: 작업 보고서는 완료된 분석이나 중지된 자가 방어에서만 출력할 수 있습니다. 분석이 완료 되지 않거나 실행 중인 자가 방어에서는 보고서 내보내기를 실행할 수 없습니다.

1. 프로젝트의 상세 정보 페이지로 이동하세요.

2. 오른쪽 위에 있는 작업 이력 보기 버튼을 클릭하세요.

🧊 s	parrow Enterprise			작업 이	력					×
&	# TestProject 🔘	상세 정보 💽 🔅		٩ 3	검색어를 두 글자 이	이상 입력하세요.	필터 🗸	목록 내보내기 작제하	20개씩 보	기 🗸 열편집 🗸
<b>60</b>	프로젝트키 TestProject 🗅 🐳 런타입에야	1전드 javaAgent · 마지막문석 1분전 - 방어 3시간전 ·	*	0	직업 ID 💲	유형 🗘		작업 상태 💲	작업자 💲	작업 시작 일시 🔸
88	진행 중인 작업의 결과에 따라 자신	t, 이슈 또는 컴포넌트 정보가 변경될 수 있습니다.			1620	🚱 수시 분석		52%	٥	2024-06-04 13:29:37
000				0	1614	🚱 수시 분석		완료	٥	2024-06-04 10:44:03
8	Q, 검색어를 입력하세요	88 프로젝트 홈		0	1613	자가 방어		수행 중	٥	2024-06-04 10:16:54
Q	B <mark>o</mark> 파일			0	1612	③ 자가 방어		중지	0	2024-06-04 09:59:48
۲	<ul> <li>Eo apache-maven-3.3.9.zip</li> <li>Eo aspnet/CheckerUnitTest</li> </ul>	위험도별 이슈 수		0	1611	🚱 수시 문석		완료	0	2024-06-04 09:57:00
	> E c-simple				1401	🚱 수시 분석		완료	•	2024-05-28 10:44:02
	> E Chrestcode		대해 매우높음 <b>1.3%</b> (1,004)	0	1280	🚱 수시 분석		완료		2024-05-2110:44:02
	> Coopic/parse_error	초 이슈	·····································		1254	🚱 수시 분석		완료	0	2024-05-17 10:25:40
	> Co sca_all_version.zip	78,618	ⅠⅠ□□ 낮음 9.5% (7,473)	0	1253	🚱 수시 분석		완료	a	2024-05-17 10:10:39
	URL     Meter//dastage_faces_com/0000/M		┃       매우 낮음 <b>71.7%</b> (56,355)	0	1252	ⓒ 수시 문석		완료	8	2024-05-17 10:07:16
				0	1235	🚱 수시 분석		완료	8	2024-05-16 19:45:34
	經 테스트 케이스	유형별 이슈 수			1230	ⓒ 수시 분석		완료	•	2024-05-16 19:32:09
					1227	🚱 수시 분석		완료	•	2024-05-16 19:11:29
				0	1141	📀 수시 분석		완료	•	2024-05-14 11:27:32
				0	1139	🚱 수시 분석		완료	٥	2024-05-14 10:44:01
		•	0 2 0 X	0	1138	전수 분석		완료	٥	2024-05-14 10:35:03
					1080	④ 전수 분석		완료	3	2024-05-08 17:52:18
					1079	<ul> <li>전수 분석</li> </ul>		완료	8	2024-05-08 16:58:00
									-	

3. 보고서를 생성할 작업을 선택하세요.

Sparrow Enterprise				작업 0	이력		ⓒ 수시 분석 16	14					×
器 TestProject 📧	상세 정보 💽 🚱			Q	검색어를 두 글기	다 이상 입태	일반 정보	작업 메시지	1				
프로젝트 키 TestProject 🖸 🕤 런타임 에이	전트 javaAgent - 마지막분석 <u>24분원</u> 2 - 방어 <u>3시간</u>	<u>स</u> ."			작업 ID 💲	유형	프로젝트			작업 프로파	2		
진행 중인 작업의 결과에 따라 자신	, 이슈 또는 컴포넌트 정보가 변경될 수 있습니다.				1620	6	TestProject 진행 상황			모든 작업교 소요 시간	P 검출 규직		
					1614	<b></b>	◎ 완료			10분 28초			
Q, 검색어를 입력하세요	88 프로젝트 홈				1613	0	분석 시작 일시 2024-06-04 10:44	:03		문석자 adm	nin(Superadm	in)	
E <mark>o</mark> मध					1612	0	분석 대상						
Po apache-maven-3.3.9.zip     Pa aspnet/CheckerUnitTest	이 1개의 예약된 작업이 있습니다.				1611	6	if Enterprise.zip						
> Eo c-simple					1401	<b></b>	• 작업 프로피	일은 이전 작업	넘에 적용된 내용	응을 표시하므로 현재 프로젝트	설정과 다를 수	있습니다.	
> E C:\Testcode	위험도별 이슈 수				1280	Q	0.000						
> Co pp					1054	•	(!) 검출 규직						
> Co sca_all_version.zip		┃┃┃┃ 매우 높음	<b>1.3%</b> (1,004)		1254		Q, 검색어를 두 글	자 이상 입력히	세요.	필터 🗸		10개씩 보기 🗸	열편집 🗸
🚱 URL	종이슈		5.3% (4,154)		1253	6	011	olol (		711012			
> @ http://dastapp.fasoo.com:9090/W	78,618		9.5% (7,473)		1252	6	***	201	182 0	#9998 T			
		매우 낮음	<b>71.7%</b> (56,355)		1235	6	0 TOPE	0.44		# 독은 ## 인신사 사용			
\$E 테스트 케이스					1230	6	0 소스코드	C++		#if 지시자 사용			
					1227	6	👳 소스코드	C++		#pragma 지시자 사용			
	유형별 이슈 수				1141	6	🥺 소스코드	C++	1111	#undef 지시자 사용			
					1139	6	🥴 소스코드	C++	1111	* 및 & 토큰 규칙 위반			
		_			1138	۲	🧼 소스코드	Java		+ 및 += 연산자로 더해진 (	문자열		
					1080	0	🧼 소스코드	C#		+ 연산에 사용된 빈 문자열			
	•		0 7		1079	Ø					삭제하기	로그 다운로드	보고서 내보내기

4. 아래쪽에 있는 **보고서 내보내기** 버튼을 클릭하세요.



5. 아래 내용을 참고하여 원하는 템플릿, 파일 이름, 형식을 선택하세요.

6. 내보내기 버튼을 클릭하세요.

Tip: 내보낸 작업 보고서는 사용자의 로컬 다운로드 디렉토리에 저장됩니다.

#### 프로젝트

내보낼 작업 보고서가 포함된 작업의 프로젝트입니다.

## 작업 ID

내보낼 작업 보고서가 포함된 작업의 ID입니다.

## 작업 유형

내보낼 작업 보고서가 포함된 작업의 유형이며 전수 분석, 수시 분석, 자가 방어 중 하나로 표시됩니다.

## 템플릿\*

내보낼 작업 보고서의 템플릿을 선택할 수 있습니다. 다른 보고서 템플릿을 추가하려면 보고서 템플릿 추 가하기를 참고하세요.

## 파일 이름\*

내보낼 작업 보고서의 파일 이름이며 250자 이하의 한글, 영문, 숫자, 특수 문자를 입력할 수 있습니다.

#### 형식\*

내보낼 작업 보고서의 파일 형식입니다. 작업 보고서의 파일 형식은 현재 **Portable Document Format** (.pdf), Microsoft Word Open XML (.docx), \*\*Microsoft Excel Open XML (.xlsx)\*\*과 \*\*한글 문서 (.hwp)\*\*를 지원합니다.

# 워크플로

DevSecOps를 구현하기 위해서 사용자는 여러 가지 툴에서 다양한 작업을 수행해야 합니다. 버전 관리 시스 템에서 소스코드를 당겨와서, 소스코드 분석을 수행하고, 분석 결과 발견한 이슈가 몇 개인지 확인하고, 다 시 이것을 패키징하여 배포하고, 웹 취약점을 다시 확인하는 등 복잡한 과정이 수반됩니다.

워크플로란 이렇게 **복잡한 개발-보안-운영 관리를 하나의 플랫폼에서 수행할 수 있도록 돕는** 기능입니다. 사용자는 워크플로 기능을 통해 이 과정을 평소에 실행해왔던 것보다 더 쉽고 빠르게 진행할 수 있게 됩니 다. 또한 워크플로를 Sparrow Enterprise라는 플랫폼에서 수행함으로써 데이터가 쌓이게 됩니다. 따라서 현 재 진행 중인 워크플로뿐만 아니라 지금까지 완료된 모든 워크플로의 히스토리를 확인할 수 있다는 장점이 있습니다.

# 워크플로 만들기

시스템의 **워크플로 관리** 권한이 있는 관리자는 새로운 워크플로를 추가할 수 있습니다. 워크플로에는 태스 크라는 주머니와 액션이라는 돌이 있어서 워크플로에서 실제 실행할 작업을 액션에서 설정하고 다수의 작 업을 태스크에 저장할 수 있도록 설계되었습니다. 워크플로, 태스크, 액션을 모두 설정해야 워크플로를 실행 할 수 있습니다. 먼저 다음과 같이 워크플로의 이름을 정합니다.

1. 전체 워크플로 목록에서 워크플로 추가하기 버튼을 클릭하세요.

유 RE 전체 워크플로 목록 전체 워크플로 목록 원 전체 워크플로 목록 원 전체 워크플로 목록 원 전체 위크플로 이용을 입역하세요.	
· Q. 전역어를 두 교자 이상 안석하세요. 표면 · · · · · · · · · · · · · · · · · ·	<b>4</b> Ω.
····································	
	취소하기 추가하기
U .	

2. 아래 내용을 참고하여 워크플로 이름을 입력하세요.(\*는 필수 입력 항목)

3. 추가하기 버튼을 클릭하세요.

## 워크플로 이름\*

추가할 워크플로의 이름이며 최대 50자까지 입력할 수 있습니다.

추가할 워크플로의 설명이며 최대 500자까지 입력할 수 있습니다.

이제 워크플로가 추가되었습니다.

## 워크플로 변수 추가하기

커맨드라인 명령어를 실행하거나 REST API를 호출하는데 필요한 변수가 있다면 워크플로에서 해당 액션을 수행하기 전에 워크플로에 변수를 미리 저장해두세요. 그러면 액션에 입력한 값에 변수의 \${키} 형식이 포 함되는 경우 해당 형식을 입력한 값으로 바꾸어 줍니다. 하지만 \${키} 형식이더라도 해당하는 키가 워크플 로 변수에 포함되지 않는다면 바꾸지 않고 그대로 둡니다.

다음과 같은 내용을 참고하여 사용하려는 변수를 저장하세요.

1. 워크플로 상세 정보 페이지로 이동하세요.

2. 오른쪽 위에 있는 변수 수정하기 버튼을 클릭하세요.

🧊 s	Darrow Enterprise > <u>에이트로 무해</u> > TestWorkflow		워크플로 변수 수정	×
<i>♣</i> ₩	문 워크플로 TestWorkflow		작성된 워크프로 변수는 액션 옵션에서 사용됩니다. 액션 옵션 중 길에 \$(변수 키) 형식 단, 형식은 \$(변수 키) 이나 해당 변수 키가 존재하지 않는다면 값을 치한하지 않고 그다	이 포함된다면 해당 형식을 변수 값으로 치환합니다. 로 둡니다.
œ	영성자 🚺 admin (admin)	생성 열시	치환은 단 한번만 수행합니다. 빈수 키 형식을 중첩되어 사용한 경우에도 한 번만 치환을	irici.
000	성명 -		N workflow.id 위크플로 ID	
			ର workflow.exe.id 위크플로 실행	
	😵 사용할 수 있는 테스크 에이전트가 없어 워크플로를 실행할 수 없습니다.		S task.id 태스크 ID	
**		태스크 목록	및 action.id 액션 ID	
	실행 횟수 <b>0회</b> 태스크 수 <b>2개</b>		N action.exe.id 액션 실행 ID	
		1 45	이 기름 입력하세요. 값을 입력하세	<u>a</u> .
	위크플로 실행 목록 제3# 2 성명에게	전체 0 액션	+ 추가하기	
	Q. 검색어플 두 글자 이상 입력하세요.         필터 ❤         20개백 보기. ♥         열환집. ♥			
	실행ID ○ 실행시작입시 ↓	<ol> <li>자동</li> </ol>		
	등록 대가 중이거나 내용이 없습니다.	전체 0 액션		
				취소하기 <mark>수정하기</mark>

3. 변수에 사용할 키와 값을 입력하세요.

**Tip**: 목록의 아래에 있는 + **추가하기** 버튼을 클릭하여 키값 쌍을 추가로 입력할 수 있습니다.

4. 모든 변수를 입력하고 수정하기 버튼을 클릭하세요.

워크플로를 실행할 때 여기에 입력한 변수의 키나 값을 변경하거나 추가로 다른 변수를 입력할 수 있습니다. 자세한 내용은 태스크와 액션을 모두 만든 후에 워크플로 실행하기를 참고하세요.

태스크 추가하기

태스크는 워크플로에서 여러 개의 액션을 하나로 모아두는 역할을 하고 있습니다. 여러 개의 액션을 태스크 단위로 구분하여 어떤 것을 먼저 실행할지 우선순위를 결정합니다. 따라서 태스크의 순서에 유의해서 정렬 하는 것이 좋습니다.

1. 워크플로 상세 정보 페이지에서 **태스크 추가하기** 버튼을 클릭하세요.

S 😵	parrow Enterprise > 910002.55 > TestWoodflow	태스크 추가	×
2 88 89 80	응 워크플로 TestWorkflow (1917년 - 1917년 - 1917	위크플로 TestWorkflow 테스크 이름 * 테스크 이름을 입력하세요. 시작 방식 *	
8		자동	~
Q &	중 포함한 테스크가 없어 위크로운동 실행할 수 없습니다. 테스크를 먼저 추가하세요.	▲ 선택 입력 항목 숨기기 선행 테스크 ●	
	○         사용원 수 있는 목스크 에어컨트가 없어 체크용공을 실행된 수 없습니다.           ····································	인저 앞료되어야 하는 선행 태스크를 선택하세요. 지정 태스크 에이컨트 ● 에이컨트를 지정하세요.	~
		취소하기 🤻	추가하기
	워크플로 실행 목록 태교 분 성태에 관		
	Q, 전세어표 두 글자 이상 인력하세요. 월버 ✔ 204백 보기 ✔ 열린 입 ✔ 역스크가 존재하지 않습니다.		
	실행 Ø : 실행 사직 열시 ↓ 동쪽 대기 중이거나 내용이 없습니다.		

2. 태스크 이름을 입력하고 시작 방식을 선택하세요.

3. 아래 내용을 참고하여 다른 항목을 입력하세요.(\*는 필수 입력 항목)

4. **추가하기** 버튼을 클릭하세요.

## 워크플로

태스크를 추가할 워크플로의 이름이며 변경할 수 없습니다.

## 태스크 이름\*

추가할 태스크의 이름이며 최대 50자까지 입력할 수 있습니다.

#### 시작 방식\*

추가할 태스크의 시작 방식이며 자동과 수동 중에 하나를 선택할 수 있습니다. 자동으로 설정된 태스크는 선행 태스크가 없거나 모든 선행 태스크가 완료된 경우 자동으로 실행됩니다. 수동으로 설정된 태스크는 선 행 태스크가 없거나 모든 선행 태스크가 완료된 경우 사용자가 **시작하기**를 클릭하여 실행시키게 됩니다.(기 본값: 자동)

#### 선행 태스크

추가할 태스크를 실행하기 전에 먼저 완료되어야 하는 태스크입니다. 동일한 워크플로에 포함된 태스크 중에서 하나 이상의 태스크를 선택할 수 있습니다.

Tip: 선행 태스크가 없는 태스크는 알파벳 순으로 나열됩니다.

## 지정 태스크 에이전트

추가할 태스크의 액션을 수행하도록 명령을 전달할 태스크 에이전트입니다. 에이전트를 지정하는 경우 태스크에 포함된 모든 액션은 해당 에이전트에서 수행됩니다. 하지만 지정된 에이전트를 사용할 수 없다면 태스크가 실패하게 됩니다. 에이전트를 지정하지 않는 경우 임의의 에이전트에서 태스크에 포함된 액션이 수행됩니다.

Tip: 태스크 에이전트에 대한 설명이나 설치 방법은 태스크 에이전트 설치하기를 참고하세요.

액션 추가하기

이제 태스크에 액션을 추가하겠습니다. 현재 태스크에서 수행할 수 있는 액션은 **커맨드라인 실행**과 **REST API 호출** 두 가지입니다.

Warning: 하나의 태스크에서는 한 개의 에이전트를 사용하도록 설계되었습니다. 에이전트는 사용자 가 설치한 머신에서 동작하며 Sparrow Enterprise 서버와 통신합니다. 따라서 태스크에 여러 액션을 추가할 때 모두 동일한 IP의 머신에서 수행되도록 설정해야 합니다.

1. 태스크에서 액션 추가하기 버튼을 클릭하세요

S S	parrow Enterprise > (1) III (			액션 추가			×
*	22 워크플로 TestWorkflow		생성 양시	위크플로 TestWorkflow 예산 유상 • REST API 호출	~	태스크 Task02 역선 이름 • 역선 이름을 입력하세요.	
<u></u>	en -			REST API 호출 정보			
Ð	사용할 수 있는 테스크 아이전트가 없어 위크홈모를 실행할 수 없습니다.			HTTP 메소드 * GET 대상 URL *	~		
	실명 맞수 <b>0회</b> 태스크 수	2개	태스크 목록	대상 URL을 입력하세요. HTTP 헤디 및, 키를 입력하세요.		값을 입력하세요.	
	워크플로 실행 목록		전체 0 액션	+ 추가하기 요청 HTTP 분문			
	Q. 검색이별두글자 이상 업색하세요.         범터 >         20개백 5/7 >           SWEID :         SWEID :         SWEID :         SWEID :	일편집 ✓	<b>2</b> 45	요청으로 진담할 HTTP 본문을 입력하세요.			
			24042				
							취소하기 <b>추가하기</b>

Tip: 캡쳐된 화면은 액션 유형이 REST API 호출 정보인 경우에 입력할 슬라이드입니다.

- 2. 액션 유형을 입력하고 액션 이름을 입력하세요.
- 아래 내용을 참고하여 커맨드라인 실행 정보나 REST API 호출 정보를 입력하세요.(\*는 필수 입력 항 목)

4. 추가하기 버튼을 클릭하세요.

워크플로

액션을 추가할 워크플로의 이름이며 변경할 수 없습니다.

태스크

액션을 추가할 태스크의 이름이며 변경할 수 없습니다.

#### 액션 유형\*

추가할 액션의 유형이며 **커맨드라인 실행**과 REST API 호출 중에 하나를 선택할 수 있습니다.

#### 액션 이름\*

추가할 액션의 이름이며 최대 50자까지 입력할 수 있습니다.

#### ✓ 커맨드라인 실행 정보

## 실행 명령어 내용\*

커맨드라인으로 실행할 명령어입니다. 워크플로에서 설정한 변수를 이 옵션에 입력할 수 있습니다.

## 작업 디렉토리

위 옵션에 입력한 커맨드라인을 실행할 작업 디렉토리 경로입니다.

**Tip**: **커맨드라인 실행**에는 명령어를 실행할 머신의 IP를 입력하지 않기 때문에 특정 머신을 지정할 수 없다는 사실에 유의하세요. 여러 머신으로부터 사용 가능한 에이전트가 연결된 경우 그중에 **작업 디렉토리가 일치하는 머신에서** 옵션에 입력한 실행 명령어를 실행합니다.

다만, 태스크를 만들 때 **지정 태스크 에이전트**를 선택하여 태스크 에이전트가 작동 중인 머신에서 커 맨드라인을 실행하도록 하는 방법이 있습니다. 태스크 에이전트를 지정하는 방법은 <mark>태스크 추가하기</mark> 에서 **지정 태스크 에이전트** 옵션을 참고하세요.

## √ REST API 호출 정보

## HTTP 메소드\*

REST API를 호출하는데 사용할 HTTP 메소드입니다. GET, HEAD, POST, PUT, DELETE, CONNECT, OPTIONS, TRACE, PATCH 중에 하나를 선택할 수 있습니다.(기본값: GET)

#### 대상 URL\*

REST API 호출을 수행할 대상 URL입니다. 이 옵션은 https://로 시작하는 URL 형식으로 입력해야 합니다.

## HTTP 헤더

REST API 호출을 수행할 때 대상 URL로 보내는 HTTP 요청에 추가할 헤더의 키와 값 목록입니다. 키와 값 의 쌍으로 되어있으며 목록의 아래에 있는 **+ 추가하기** 버튼을 클릭하여 하나 이상의 키값을 입력할 수 있습 니다.

## 요청 HTTP 본문

REST API 호출을 수행할 때 대상 URL에 대한 요청으로 전송할 HTTP 본문입니다. 값이 존재하지 않는 경우 별도의 본문을 전달하지 않습니다. 워크플로에서 설정한 변수를 이 옵션에 입력할 수 있습니다. **Tip**: 태스크를 만들 때 **지정 태스크 에이전트**를 선택하지 않은 경우 대상 URL에 해당하는 머신으로부 터 사용 가능한 에이전트를 사용합니다. 해당 머신에서 하나 이상의 에이전트가 연결되어 있다면 임 의의 에이전트를 사용하게 됩니다.

# 워크플로 실행하기

이제 워크플로를 실행하겠습니다. 다음과 같은 동작을 수행하세요.

1. 워크플로 상세 정보 페이지로 이동하세요.

2. 워크플로 실행하기 버튼을 클릭하세요.

3. 워크플로 실행 슬라이드에서 미리 설정한 워크플로 변수의 키와 값을 변경하거나 새로 입력하세요.

Tip: 워크플로 변수 추가하기에서 입력한 변수가 기본값으로 표시됩니다.

4. 실행하기 버튼을 클릭하세요.

이제 워크플로가 실행됩니다.

워크플로 실행 확인하기

실행한 워크플로는 워크플로 상세 정보 페이지의 워크플로 실행 목록에 표시됩니다. 목록을 클릭하면 태스 크나 액션과 관련된 정보와 실행된 워크플로에서 검출한 이슈를 포함하는 **워크플로 실행 상세 정보** 페이지 를 확인할 수 있습니다.

ទি Sparrow Enterprise > <u>মানারর বল্ল</u> > TestProtect > মানারর এউ বল্ল > মানারর এউ চচ		🔒 🙆 admin 🗸
<sup>♣</sup> ◎ 워크플로 실행 <b>55</b>		<b>삭제하기</b> 변수 보기
89 소요시간 21	<b>초</b> 실행 상황	완료
관         제대표교         TestProject           역         시전 웹사         2024-05-20 10-26-12           응         ····································	수행자 😵 admin(SuperAdmin) 관표 11시 2024-05-20 10:26:15	
위험도별 이슈 수 응어수 12 12 14 14 14 14 14 14 14 14 14 14		및 dain_book_agent 역선 육록 습기기 ▲ 1호
검출된 이슈         목록 내보내기           Q. 김석아들 두 글자 이상 입력하세요.         필터 >         20개백 보기 >         열린 3	● 兆音 Task02 전체 0 1111 0 1111 0 1111 0 1111 0 전체 1억년 1 0余 中和五匹	묘 dain_tocat_agent 역전 목록 송기기 ▲ 1호 ⊘
위원도 ② 이슈 이동 ③ 이슈 김홍 목사 ↓		
····································		
ⅠⅠⅡⅠ 취약한 컴포넌트 사용 2023-04-211E00-52		
취약한 컴포넌트 사용         2023-04-2111:00:52		
이미 취약한 급보던트 사용         2023-04-21 1100-52           VQuery 삼업         2023-04-21 1100-52		
IIIII         workflow issue2         2023-04-21 11:00:52		
workflow issue2 2023-04-21 11:00:52		
workflow issue2 2023-04-2111:00:52		
XSS         2023-04-211100:52		
worknow issue2 2023-04-211100-52		
전체 12 아슈 1 - 12 프시핑		

## √ 워크플로 실행 정보

워크플로 실행에 대한 정보입니다. 워크플로 실행 정보에는 워크플로의 **실행 상황**과 **소요 시간**이 표시됩 니다.

워크플로 실행을 수행 중인 경우 **중지하기** 버튼을 클릭하여 워크플로를 중지할 수 있습니다. 워크플로 실 행이 실패하거나 완료된 경우 **삭제하기** 버튼을 클릭하여 워크플로 실행을 삭제할 수 있습니다. **변수 보기** 버 튼을 클릭하면 해당 워크플로 실행에 사용한 변수를 확인할 수 있습니다.

## √ 위험도별 이슈 수

워크플로 실행에서 검출된 이슈의 개수를 **매우 높음**, **높음**, **보통**, **낮음**, **매우 낮음**이라는 위험도에 따라 5 단계로 구분하여 그래프로 표시합니다.

## √ 검출된 이슈

워크플로 실행에서 검출한 이슈의 목록입니다. 검출된 이슈 목록에는 검출된 이슈의 **위험도**, **이슈 이름**, **이슈 검출 일시**가 표시됩니다.

여기서 **목록 내보내기**를 클릭하고 **파일 이름**을 입력하여 **.csv**, **.xlsx**, **.cell** 형식의 파일을 다운로드할 수 있 습니다. 이 파일에는 검출된 모든 이슈 중에서 목록에 나열된 이슈가 포함됩니다.

## √ 태스크 실행 목록

페이지의 오른쪽에 있는 태스크 실행 목록은 실제 실행된 태스크와 액션에 대한 정보를 표시합니다. 태스 크와 관련된 정보에는 **태스크 상태, 태스크 시작 방식, 태스크 이름, 선행 태스크 목록, 지정 태스크 에이전 트**, 태스크에서 검출된 **이슈 수**가 포함되고, 액션과 관련된 정보에는 **액션 이름, 액션 실행 소요 시간, 액션** 실행 상황이 포함됩니다.

액션을 클릭하면 수행된 액션에 대한 좀 더 자세한 내용을 확인할 수 있습니다. 여기에는 **액션 실행 ID**, 액 션의 **유형**, **진행 상황**, 액션이 포함된 **워크플로**, **워크플로 실행 ID**, **태스크 이름**이 표시됩니다. 또한 로그 다 운로드하기 버튼을 클릭하여 실행된 액션의 분석 로그를 다운로드할 수 있습니다.

관리

시스템 권한이 있는 관리자의 경우 기본 메뉴에서 관리 아이콘을 클릭하면 다음과 같은 메뉴를 확인할 수 있 습니다. 관리 메뉴에서는 Sparrow Enterprise 시스템의 여러 가지 기능을 확인하고 변경할 수 있습니다.

Sparrow Enterprise				🔓 😩 admin 🗸
A	역할 및 권한           전형을 조합하여 시스템 역할 및 프로젝트 역할을 추가하거나 검정할 수 있습니다. 또한, 특징 기능에 결제산을 지정할 수 있 습니다.           시스템 역할         프로젝트 역할         질재건	안중 및 사용자     사망자 그들을 추가하거나 등록된 사용자     사망자 그들의 정보를 변경할 수 있습니다. 또한, LDAP을 해 고유한 안용 금급자를 사용적도록 설정할 수 있습니다.     사망자     사망자     사망자 제품 인종 급급자	작업 및 규칙           사용함 이슈 검을 규칙을 확인하고 선택할 수 있습니다. 또한 적업 수행을 위한 작업 프로파일을 분질할 수 있습니다.           관         여슈 감을 규칙           여슈 감을 규칙         적업 프로파일	
0	((우)) 에이전트 작업 대상에 환격으로 연결된 에이전트의 상대를 확인하고 관 리컬 수 있습니다. 태스크 에이전트	보고서 적업 상세 보고서에 사용되는 보고서 행용것을 서통계 추가: 기나 기존에 흔져하는 명몰것을 편집할 수 있습니다. 보고서 행동3	양         컴포넌트           사용자의 립트먼트를 추가하고 관리할 수 있습니다.         사용자 협포먼트를 추가하고 관리할 수 있습니다.	
	응 정보 제품과 서비, 사용 연형 정보를 초 제품 라이스스 형보를 초회하 신험 수 있습니다. 사스템 7	5회할 수 있습니다. 또한 책용 고 사람은 제품 리이선스로 경 명말 제품 리이선스 정보	+ 데이터의 발생 아력 등 로그 정보를 조 감사 기록	

## √ 역할 및 권한

## 시스템 역할

시스템 역할 탭에서는 시스템 역할 정보를 확인하고 변경할 수 있으며 역할 및 권한 관리 권한이 있는 관 리자만 해당 탭에 접근할 수 있습니다. 자세한 내용은 시스템 역할 관리하기를 참고하세요.

## 프로젝트 역할

**프로젝트 역할** 탭에서는 프로젝트 역할 정보를 확인하고 변경할 수 있으며 **역할 및 권한 관리** 권한이 있는 관리자만 해당 탭에 접근할 수 있습니다. 자세한 내용은 프로젝트 역할 관리하기를 참고하세요.

## 결재선

**결재선** 탭에서는 특정 기능에 결재선을 지정할 수 있으며 **역할 및 권한 관리** 권한이 있는 관리자만 해당 탭에 접근할 수 있습니다. 자세한 내용은 결재선 관리하기를 참고하세요.

#### √ 인증 및 사용자

#### 사용자

**사용자** 탭에서는 등록된 사용자 목록 및 사용자 정보를 확인하고 변경할 수 있으며 **인증 및 사용자 관리** 권한이 있는 관리자만 해당 탭에 접근할 수 있습니다. 자세한 내용은 사용자 관리하기를 참고하세요.

#### 사용자 그룹

**사용자 그룹** 탭에서는 등록된 사용자를 사용자 그룹에 추가하고 변경할 수 있으며 **인증 및 사용자 관리** 권한이 있는 관리자만 해당 탭에 접근할 수 있습니다. 자세한 내용은 사용자 그룹 관리하기를 참고하세요.

#### 인증 공급자

**인증 공급자** 탭에서는 LDAP을 사용하는 사용자의 외부 인증 공급자 정보를 등록할 수 있습니다. 자세한 내용은 인증 공급자 관리하기를 참고하세요.

#### √ 작업 및 규칙

#### 이슈 검출 규칙

**이슈 검출 규칙** 탭에서는 등록된 이슈 검출 규칙을 확인하고 활성화할 수 있습니다. 자세한 내용은 이슈 검출 규칙 관리하기를 참고하세요.

#### 작업 프로파일

**작업 프로파일** 탭에서는 이슈 검출 규칙과 작업 옵션과 같이 작업에 필요한 정보를 묶어서 프로젝트의 특 정 작업을 수행할 때 사용할 수 있도록 설정할 수 있습니다. 자세한 내용은 작업 프로파일 관리하기를 참고 하세요.

#### √ 에이전트

#### 태스크 에이전트

**태스크 에이전트** 탭에서는 워크플로에서 태스크를 실행할 때 사용하는 태스크 에이전트 등록 정보 및 실 행 상황을 확인할 수 있습니다. 자세한 내용은 태스크 에이전트 관리하기를 참고하세요.

#### √ 보고서

#### 보고서 템플릿

**보고서 템플릿** 탭에서는 수행한 작업에 대한 보고서를 출력할 때 사용할 보고서의 형식을 새롭게 추가하 거나 기존 형식을 수정할 수 있습니다. 자세한 내용은 보고서 템플릿 관리하기를 참고하세요.

## √ 컴포넌트

#### 사용자 컴포넌트

**사용자 컴포넌트** 탭에서는 Sparrow 데이터 웨어하우스에서 검출하지 않는 특정 파일을 컴포넌트로 추가 함으로써 컴포넌트 분석에서 해당 파일을 컴포넌트로 식별하도록 설정할 수 있습니다. 자세한 내용은 사용 자 컴포넌트 관리하기를 참고하세요.

#### √ 정보

#### 시스템 정보

시스템 정보 페이지에서는 시스템 정보를 확인할 수 있으며 시스템 관리 권한이 있는 관리자만 해당 페이 지에 접근할 수 있습니다. 자세한 내용은 시스템 정보 확인을 참고하세요.

#### 제품 라이선스 정보

제품 라이선스 정보 페이지에서는 Sparrow Enterprise를 사용할 수 있는 권한인 제품 라이선스 정보를 확 인하고 변경할 수 있습니다. 이 페이지는 시스템 관리 권한이 있는 관리자만 해당 페이지에 접근할 수 있습 니다. 자세한 내용은 제품 라이선스 정보 확인을 참고하세요.

#### √ 로그

## 감사 기록

**감사 기록** 페이지에서는 Sparrow Enterprise에서 발생한 이벤트를 확인할 수 있으며 **시스템 관리** 권한이 있는 관리자만 해당 페이지에 접근할 수 있습니다. 자세한 내용은 <mark>감사 기록 확인을</mark> 참고하세요.

# 역할 및 권한

시스템 역할 관리하기

시스템 역할은 시스템을 사용하기 위해 부여되는 권한을 모은 정보입니다. **시스템 역할** 메뉴에서는 등록된 역할의 목록 및 역할 정보를 확인하고 변경할 수 있습니다.

1. 왼쪽 사이드 바에서 **관리**를 클릭하세요.

2. 사용자 메뉴에서 시스템 역할을 클릭하세요.

#### 시스템 역할 추가하기

시스템의 **역할 및 권한 관리** 권한이 있는 관리자는 **관리** 메뉴의 **시스템 역할** 페이지에서 다음과 같은 방법으 로 새 시스템 역할을 추가할 수 있습니다.

Tip: 시스템 역할에는 모든 시스템 권한을 가진 SPARROW-ADMIN과 아무 시스템 권한이 없는 SPARROW-USER라는 역할이 기본적으로 설정되어 있습니다. 기본 설정된 두 역할은 수정하거나 삭제 할 수 없습니다. 다른 역할을 추가하여 시스템 역할을 커스터마이징하세요.

1. 시스템 역할 페이지에서 오른쪽 위에 있는 시스템 역할 추가하기 버튼을 클릭하세요.

۲	Sparrow Enterprise » 관리	› 여행 및 관한	시스템 역할 추가	×
æ.	역할 및 권한		역할 이름 •	
00	시스템 역할	시스템 역할 목록	시스템 역할 이름을 입력하세	8.
800	프로젝트 역할		권한 *	
w	결재선	Q, 검색어를 두 글자 이상 입력하세요. 필터 🗸	- 프로젝트 관리	이 역할 및 권한 관리
000	인증 및 사용자	역할 아름 🛧	이 이글프로 과기	○ 시스템 관리
2	사용자	SPARROW-ADMIN	지 정포넌트 관리	· 포고지 편리
Q	사용자 그룹	SPARROW-USER		
8	인종 공급자		✓ 선택 입력 항목 보기	
-	작업 및 규칙	전체 2 시스템 역할 1 - 2 표시된	オレムネルフリ	제소 초기치기 초기치기
	이슈 검출 규칙		HEORY	All designed as a second
	작업 프로파일			
	에이전트			
	태스크 에이전트			
	보고서			
	보고서 템플릿			
	컴포넌트			
	사용자 컴포넌트			
	정보			
	시스템 전보			
	제풍 라이선스 정보			
	27			
	2)11 21 22			
	원석 시 <del>작</del>			

2. 아래의 내용을 참고하여 역할에 부여할 정보를 입력하세요.(\*는 필수 입력 항목)

3. 추가하기 버튼을 클릭하세요.

4. 역할이 성공적으로 추가되면 왼쪽 아래에 성공 메시지가 출력됩니다.

#### 역할 이름\*

시스템 역할의 이름이며 50자 이하의 한글, 영문, 숫자, 특수 문자, 공백을 입력할 수 있습니다.

## 권한\*

역할에 부여할 권한이며 다음 중 하나 이상의 권한을 선택할 수 있습니다.

 프로젝트 관리 : 프로젝트를 추가하거나, 이미 생성된 프로젝트의 정보를 수정하고 프로젝트를 삭제할 수 있습니다.

**Tip**: 프로젝트 관리 권한이 있는 시스템 역할의 사용자라도 프로젝트에서 작업을 수행하기 위해서는 작업 수행 권한이 있는 프로젝트 역할이 필요합니다.

• 역할 및 권한 관리 : 시스템 역할과 프로젝트 역할을 생성하거나 수정할 수 있습니다.

**Tip**: 역할 및 권한 관리는 Sparrow Enterprise의 시스템 전체에서 사용할 역할을 관리합니다. 특정 사용자에게 역할을 부여하려면 아래의 인증 및 사용자 관리 권한이 필요합니다.

- 인증 및 사용자 관리 : 사용자 및 사용자 그룹을 추가하거나 사용자에 관련된 정보, 예를 들어 비밀번 호나 사용자 역할을 변경할 수 있습니다. Sparrow Enterprise에 LDAP을 사용하는 인증 방법을 설정하 는 권한도 포함되어 있습니다.
- 시스템 관리 : 시스템 정보, 제품 라이선스 정보, 로그를 확인할 수 있습니다. 제품 라이선스 를 갱신할 수 있는 권한이기도 합니다.
- 워크플로 관리 : 워크플로를 관리하거나 사용하기 위해 필요합니다.
- 보고서 관리 : 보고서 템플릿을 생성하거나 수정하고 삭제할 수 있습니다.

**Tip**: 보고서 관리는 보고서 템플릿과 관련된 관리 기능에 접근할 수 있는 권한입니다. 프로젝트에서 작업 보고서를 출력하려면 프로젝트 구성원이어야 합니다. 프로젝트에서 PROJECT-VIEWER와 같은 낮은 권한이 있는 사용자도 보고서를 출력할 수 있습니다.

 컴포넌트 관리 : 컴포넌트 분석에서 사용할 수 있는 사용자 컴포넌트를 추가하고 수정할 수 있 습니다.

**Tip**: 사용자 컴포넌트는 Sparrow 데이터 웨어하우스에서 제공하지 않는 사용자가 지정한 컴포넌트 를 의미합니다. 자세한 내용은 사용자 컴포넌트 관리를 참고하세요.

 작업 및 규칙 관리 : 작업 중 분석 및 자가 방어에 사용할 이슈 검출 규칙 목록을 가져오거나 이슈 검출 규칙을 추가할 수 있습니다. 또한, 작업에 사용할 작업 프로파일을 생성하고 수정할 수도 있습니다.

## 설명

시스템 역할에 대한 설명을 입력하세요.

#### 시스템 역할 변경하기

이제 앞에서 추가한 역할로 사용자의 시스템 역할을 변경하려는 경우 다음을 참고하세요.

1. 관리 메뉴의 **사용자** 페이지로 이동하세요.

2. 사용자 목록에서 역할을 변경할 사용자의 체크박스를 선택하세요.

3. 오른쪽에 있는 수정하기 버튼을 클릭하세요.

**Tip**: 새로운 사용자에게 역할을 주려는 경우 사용자 목록에서 **사용자 추가하기** 버튼을 클릭하고 새로 운 사용자를 추가하세요. 자세한 내용은 <u>사용자 추가하기를</u> 참고하세요.

4. 새로운 역할을 선택하세요.

5. 수정하기 버튼을 클릭하세요.

## 프로젝트 역할 관리하기

프로젝트 역할은 프로젝트에 대해 부여되는 권한을 모은 정보입니다. **프로젝트 역할** 메뉴에서는 등록된 역 할의 목록 및 역할 정보를 확인하고 변경할 수 있습니다.

1. 왼쪽 사이드 바에서 **관리**를 클릭하세요.

2. **사용자** 메뉴에서 프로젝트 역할 탭을 클릭하세요.

## 프로젝트 역할 추가하기

시스템의 **역할 및 권한 관리** 권한이 있는 관리자는 **관리** 메뉴의 **프로젝트 역할** 페이지에서 다음과 같은 방법 으로 새 프로젝트 역할을 추가할 수 있습니다. Tip: 프로젝트 역할에는 프로젝트를 마음껏 수정할 수 있는 권한을 가진 PROJECT-ADMIN과 프로젝트 에서 분석을 수행할 사용할 수 있는 일부 권한이 있는 PROJECT-USER, 프로젝트의 구성원으로서 조 회 이외에는 다른 권한이 없는 PROJECT-VIEWER라는 역할이 기본적으로 설정되어 있습니다. 기본 설 정된 세 역할은 수정하거나 삭제할 수 없습니다. 다른 역할을 추가하여 프로젝트 역할을 커스터마이 징하세요.

S 🔊	iparrow Enterprise » 관립 :	· 여행 및 관련	프로젝트 역할 추가	×
æ.	역할 및 권한		역할 이동 *	
88	시스템 역할	프로젝트 역할 목록	프로젝트 역할 이름을 입력하시	iΩ.
80	프로젝트 역할			
ø	결재선	Q 검색어를 두 글자 이상 입력하세요. 웹터 🗸	🗌 작업 수행	🗌 작업 관리
<u>00o</u>	인증 및 사용자	역할 이름 🛧	🗌 이슈 참여	📄 이슈 제외 승인
2	사용자	PROJECT-ADMIN	✓ 선택 입력 항목 보기	
	사용자 그룹	PROJECT-USER		
8	인종 공급자	PROJECT-VIEWER	취소하기	계속 추가하기 추가하기
_	작업 및 규칙			
	이슈 검출 규칙	전체 3 프로젝트 역할 1 - 3 프시핑		
	작업 프로파일			
	에이전트			
	태스크 에이전트			
	보고서			
	보고서 뜀플릿			
	컴포넌트			
	사용자 컴포넌트			
	정보			
	시스템 정보			
	제품 라이선스 정보			
	22			
	감사 기록			

1. 프로젝트 역할 페이지에서 오른쪽 위에 있는 프로젝트 역할 추가하기 버튼을 클릭하세요.

2. 아래의 내용을 참고하여 역할에 부여할 정보를 입력하세요.(\*는 필수 입력 항목)

3. 추가하기 버튼을 클릭하세요.

4. 역할이 성공적으로 추가되면 왼쪽 아래에 성공 메시지가 출력됩니다.

## 역할 이름\*

프로젝트 역할의 이름이며 50자 이하의 한글, 영문, 숫자, 특수 문자, 공백을 입력할 수 있습니다.

## 권한

역할에 부여할 권한이며 하나 이상의 권한을 선택할 수 있습니다.

- 프로젝트 수정 : 권한이 있는 프로젝트의 기본 정보, 구성원, 작업 프로파일 활성화, 웹훅 등 프로젝 트 설정에 포함된 정보를 수정할 수 있습니다.
- 프로젝트 삭제 : 권한이 있는 프로젝트 및 해당 프로젝트에 포함된 모든 정보를 삭제할 수 있습니다.
- 작업 수행 : 권한이 있는 프로젝트에서 작업을 수행할 수 있습니다.
- 작업 관리 : 권한이 있는 프로젝트에서 작업을 중지하거나 삭제할 수 있습니다.
- 이슈 참여 : 권한이 있는 프로젝트에서 이슈의 상태를 변경하거나, 이슈의 담당자 중 한 명으로 써 담당자를 지정할 수 있습니다.

Tip: 프로젝트 권한은 모두 독립적이며 다른 권한의 상위 권한으로 동작하지 않습니다. 예를 들어, 작 업 관리 권한이 작업 수행 권한을 포함하고 있지 않다는 것에 유의하세요.

## 설명

프로젝트 역할에 대한 설명을 입력하세요.

#### 프로젝트 역할 변경하기

이제 앞에서 추가한 역할로 사용자의 프로젝트 역할을 변경하려는 경우 다음을 참고하세요.

1. 프로젝트 역할을 변경하려는 프로젝트의 **프로젝트 상세 정보** 페이지로 이동하세요.

2. 오른쪽 위에 있는 프로젝트 수정하기 버튼을 클릭하세요.

3. **구성원** 목록에서 역할을 변경할 사용자의 체크박스를 선택하세요.

4. 구성원 목록에 있는 수정하기 버튼을 클릭하세요.

Tip: 다른 사용자를 구성원으로 추가하려는 경우 구성원 목록에서 추가하기 버튼을 클릭하고 새로운 구성원을 선택하세요.

5. 새로운 **역할**을 선택하세요.

6. 수정하기 버튼을 클릭하세요.

결재선 관리하기

결재선은 특정 동작에 대해 승인을 요청하고 이 요청을 승인하거나 반려하는 절차를 추가하는 기능입니다. **결재선** 메뉴에서는 결재선을 만들 수 있는 동작이 무엇인지 확인할 수 있습니다.

1. 왼쪽 사이드 바에서 **관리**를 클릭하세요.

2. 역할 및 권한 메뉴에서 결재선 탭을 클릭하세요.

## 결재선 변경하기

시스템의 **역할 및 권한 관리** 권한이 있는 관리자는 **관리** 메뉴의 **결재선** 페이지에서 다음과 같은 방법으로 결 재선의 세부 내용을 변경할 수 있습니다.

1. 관리 메뉴의 결재선 페이지로 이동하세요.

2. 결재선 목록에서 변경할 항목을 선택하세요.

iparrow Enterprise »	<u>관리</u> > 역할 및 권한	결재선 관리 이슈 제외
역할 및 권한		요청 유성 범위 경제 단계 사용
시스템 역할	결재선 목록	이슈 제외 프로젝트
프로젝트 역할		요청 가능 역할 🕥
견재선	Q. 검색어를 두 글자 이상 입력하세요. 필터 🂙	PROJECT-ADMIN X PROJECT-USER X PROJECT-VIEWER X
인증 및 사용자	요청유형 个	결제 단계 목록
사용자	이슈 제의	걸제 ~
사용자 그룹		태 지리 가능 예할 *
인증 공급자	전체 1 결제선 1 - 1 표시팀	역할을 선택하세요.
작업 및 규칙		
이슈 검출 규칙		+ 주기하기
작업 프로파일		
에이전트		
태스크 에이전트		
보고서		
보고서 팬플릭		
911UE		
LOT NUITE		
Mon Balle		
성모		
시스템 정보		
제품 라이선스 정보		
로그		
감사 기록		
		취소하기 2

3. 결재 단계 사용을 활성화하고 단계를 추가하세요.

4. 아래를 참고하여 옵션을 선택하고 저장하기 버튼을 클릭하세요.

## 요청 유형

결재를 요청하는 목적입니다. 요청 유형은 기본 설정되어 있으며 사용자가 수정할 수 없습니다.

범위

결재가 미치는 영향의 범위를 의미합니다. 범위는 기본 설정되어 있으며 사용자가 수정할 수 없습니다. 이 슈 제외 요청은 프로젝트 범위의 결재로 설정되어 있습니다.

## 결재 단계 사용

결재 단계를 사용하는 경우 이 옵션을 활성화해야 합니다. 이 옵션을 사용하지 않는 경우 결재를 요청하 는 즉시 승인하게 됩니다.

#### 요청 가능 역할

결재선 기능에서는 역할에 따라 결재를 요청할 수 있는 사용자를 구분합니다. 따라서 여기에 선택된 역할 을 가진 사용자가 결재를 요청할 수 있습니다. 결재의 범위가 시스템인 경우, 시스템 역할 중에서 역할을 선 택해야 합니다. 결재의 범위가 프로젝트인 경우, 프로젝트 역할 중에서 역할을 선택해야 합니다.

역할을 선택하지 않는 경우 기본값은 **모든 역할**로 설정됩니다. 기본 설정된 역할 이외에 새로운 역할을 추가하려는 경우 시스템 역할 추가하기 또는 프로젝트 역할 추가하기를 참고하세요.

## 결재 단계 목록

결재 단계는 결재를 승인 받는 절차이며 결재 유형과 처리 가능 역할을 포함합니다. 결재선에는 최대 5 개의 결재 단계를 설정할 수 있습니다. 단, 이 옵션은 결재 단계 사용 옵션을 비활성화하는 경우 표시되지 않습니다.

#### 결재 유형

결재 방법을 결재와 합의로 구분합니다. 결재를 선택하는 경우 결재 요청을 승인하거나 반려하게 됩니다. 합의를 선택하는 경우 결재 요청에 동의하거나 반대하게 됩니다.

결재를 승인하는 경우, 다음 결재 단계가 시작됩니다. 만약 다음 단계가 없다면 결재가 완료됩니다. 결재 를 반려하는 경우, 다음 결재 단계가 시작되지 않고 결재 요청 이전으로 돌아갑니다. 합의의 경우, 결재에 동 의 혹은 반대가 선택되기만 하면 다음 결재 단계가 시작됩니다.

Tip: 가장 마지막 결재 단계의 유형은 결재여야 합니다.

## 처리 가능 역할\*

결재 단계를 처리할 수 있는 역할을 의미합니다. 여기에 선택된 역할을 가진 사용자가 해당 결재 단계를 처리할 수 있습니다. 결재의 범위가 시스템인 경우, 시스템 역할 중에서 역할을, 결재의 범위가 프로젝트인 경우, 프로젝트 역할 중에서 역할을 선택해야 합니다. 또한, 적어도 하나 이상의 역할을 선택해야 합니다.

**Tip**: 이슈 제외 결재선의 경우 범위가 프로젝트이므로 프로젝트 역할 중에서 역할을 선택해야 합니다.

# 인증 및 사용자

사용자 관리하기

시스템의 **인증 및 사용자 관리** 권한이 있는 관리자는 **사용자** 메뉴에서 등록된 사용자 목록 및 사용자 정보를 확인하고 변경할 수 있습니다. 사용자 목록을 확인하는 방법은 다음과 같습니다.

1. 왼쪽 사이드 바에서 관리를 클릭하세요.

2. **사용자** 메뉴에서 **사용자**를 클릭하세요.

사용자 목록에 표시되는 각 항목에 대한 설명은 아래의 내용을 참고하세요.

#### ID

사용자 계정의 ID입니다.

## 이름

사용자 계정의 이름입니다.

#### 아바타

사용자 계정의 아바타 이미지입니다.

#### 활성화

사용자 계정의 활성화 상태입니다. **활성**이나 **비활성** 중 하나로 표시되며 권한 있는 사용자는 비활성화 상 태의 계정을 활성화시킬 수 있습니다.

## 역할

사용자 계정에 부여된 시스템 역할입니다. 시스템 역할에 대한 자세한 내용은 시스템 역할 관리하기를 참 고하세요.

## 이메일

사용자 계정의 이메일입니다.

## 인증 공급자

사용자 계정의 인증 공급자입니다.

## 사용자 그룹

사용자 계정이 포함되어 있는 사용자 그룹입니다.

## 최근 수정 일시

최근에 사용자 계정을 수정한 일시입니다.

## 최근 접속 일시

사용자 계정의 권한으로 최근에 접속한 일시입니다.

## 만료 일시

사용자 계정이 만료되는 일시입니다.

## 사용자 추가하기

시스템의 **인증 및 사용자 관리** 권한이 있는 관리자는 **관리**의 **사용자** 메뉴에서 아래 방법으로 새 사용자를 추 가할 수 있습니다.

1. 사용자 페이지에서 오른쪽 위에 있는 사용자 추가하기 버튼을 클릭하세요.

🔊 s	iparrow Enterprise >> 관리 >	인증 및 사용자				А	용자 추가	×
2	역할 및 권한					ID		
	시스템 역할	사용자 목록					사용자 ID를 입력하세요.	
00	프로젝트 역할					01	e •	
68	결재선	Q, 검색어를 두 글자 이상 입력하세요.	필터 🗸			수정하	사용자 이름을 입력하세요.	
000	인증 및 사용자	1 al 🗌	이름 💲	아비타 활성화 🗘 역할	사용자 그룹	ы	일번호 •	
22	사용자	admin	admin	a 習る SPARROW-ADMIN		1	비밀번호를 입력하세요.	
Ð	사용자 그룹					UI UI	일번호 확인 •	
	인증 공급자	전체 1 사용자 1 - 1 표시됨					쇠밀번호를 다시 한 번 입력하세요.	
<b>•</b>	작업 및 규칙					언	બ •	
	이슈 검출 규칙						한국어	~
	작업 프로파일					9		
	에이전트						지료를 전력에서표. 조 고급해 ·	· ·
	태스크 에이전트						내부 인증 공급자	~
	보고서					2	<b>4</b> 章••	
	보고서 팬플리						D	
	NUC							
	URT NTHE					`	/ 선택 입력 항목 보기	
	사용사 업보인트							at a let a l
	정보						위소이기 세탁주기이기	주기에기
	시스템 정보							
	제품 라이선스 정보							
	22							
	감사 기록							

2. 아래의 내용을 참고하여 사용자 정보를 입력하세요.(\*는 필수 입력 항목)

3. 추가하기 버튼을 클릭하세요.

4. 사용자가 성공적으로 추가되면 왼쪽 아래에 성공 메시지가 출력됩니다.

#### ID\*

추가할 사용자 계정의 ID이며 4~32자 사이의 영문, 숫자를 입력할 수 있습니다.

## 이름\*

추가할 사용자 계정의 이름이며 1~50자 사이의 한글, 영문, 공백을 입력할 수 있습니다.

## 비밀번호\*

추가할 사용자 계정의 비밀번호이며 8~32자 사이의 영문, 숫자, 특수 문자의 조합으로 입력해야 합니다. 이 옵션은 **인증 공급자** 옵션에서 LDAP을 선택하는 경우 표시되지 않습니다.

**Tip**: Sparrow Enterprise에서는 Bcrypt, SHA-512를 사용하여 백엔드 데이터에 저장되는 비밀번호를 암호화합니다.

#### 비밀번호 확인\*

추가할 사용자 계정의 비밀번호를 다시 입력합니다. 위의 비밀번호 항목과 일치해야 합니다. 이 옵션은 인 증 공급자 옵션에서 LDAP을 선택하는 경우 표시되지 않습니다.

## 언어\*

추가할 사용자 계정에 표시할 언어입니다. 한국어, 영어 중에 하나를 선택할 수 있습니다.

**Tip**: 이미 등록된 사용자의 언어를 변경하려는 경우 목록에서 해당 사용자를 클릭하거나 변경하려는 다수의 사용자를 선택하세요. **수정하기** 버튼을 클릭한 다음 다른 **언어**를 선택하고 **수정하기** 버튼을 클릭하세요.

## 역할\*

추가할 사용자 계정의 시스템 역할이며 적어도 하나 이상의 역할을 선택해야 합니다. 사용자의 역할을 추 가하는 방법은 시스템 역할 추가하기를 참고하세요.

## 인증 공급자

추가할 사용자 계정을 인증할 공급자를 선택하세요. 별도의 외부 인증 공급자를 사용하지 않는 경우 **내부** 인증 공급자를 선택하면 됩니다. 인증 공급자 탭에서 LDAP 서버를 미리 설정한 경우 LDAP을 선택하여 인 증 정보를 가져올 수 있습니다.

Tip: LDAP 서버를 설정하는 방법은 인증 공급자 관리하기를 참고하세요.

## 활성화

추가할 사용자 계정의 활성화 상태이며 **활성**이나 **비활성** 중 하나로 표시되며 권한 있는 사용자는 비활성 화 상태의 계정을 활성화시킬 수 있습니다.

#### 아바타

추가할 사용자 계정의 아바타를 설정할 수 있습니다. **찾아보기**를 클릭하여 .avif, .gif, .pjp, .jpg, .pjpeg, .jpeg, .pfif, .png, .svgz, .svg, .webp 형식의 이미지 파일을 업로드하세요.

**Tip**: 이미지 파일의 크기는 5MB 이하여야 합니다.

## 이메일

추가할 사용자 계정의 이메일 주소를 입력할 수 있습니다.

#### 사용자 그룹

추가할 사용자 계정이 포함될 사용자 그룹을 선택할 수 있습니다.

## 만료 일시

추가할 사용자 계정의 권한을 종료할 일시를 선택할 수 있습니다.

## 사용자 삭제하기

Sparrow Enterprise에서는 어떤 사용자를 삭제하기 전에 먼저 그 사용자가 시스템 혹은 특정 프로젝트에서 수행하고 있던 역할을 다른 사용자에게 넘겨주도록 강제하고 있습니다. 만약 해당 사용자가 PROJECT-VIEWER와 같은 낮은 권한의 역할을 가지고 있더라도 해당 역할을 다른 사용자로 대체해야만 합니다.

1. 사용자 목록에서 삭제할 사용자의 체크박스를 선택하세요.

사용자 목록					사용자 추가하기	목록 가져오기 목록 내보내기
Q 검색어를 두 글자 이상 입력하세요	요. 필터 🗸			4	수정하기 <b>삭제하기</b> 207	배씩 보기 🗸 열편집 🗸
🚍 ID 🛧	이름 ①	아바타 활성화	☆ 역할	사용자 그룹	최근 접속 일시 🔹	만료 일시
admin	admin	a 활성	SPARROW-ADMIN	-	2024-02-22 10:48	17 -
SuperAdmin	admin	a 활성	SPARROW-ADMIN	-	-	-

## 2. 오른쪽 위에 있는 **삭제하기** 버튼을 클릭하세요.

1	Sparrow Enterprise » 22	> 인증 및 사용자							사용자 삭제	×
	옥, 역할 및 권한 100 시스템 역할 프로팩트 역할	사용자 목록							삭제할 사용자가 시스템 혹은 프로젝트에서 맡은 역 다른 사용자를 지정해야 합니다. 대체 사용자에 대해 더 앞아보기 💿	할을 대체할
٩	양 결재선	Q 검색어를 두 글자 이상 입력하세요.	필터 🗸					수정하	대체 사용자 *	
0	<u>00</u> 인증 및 사용자		이름 ()	아바타	탐성화 💲	역할	사용자 그룹		삭제될 사용자를 대체할 사용자를 선택하세요.	~
ĉ	요 사용자	admin	admin	0	발성	SPARROW-ADMIN	-			
Ģ	라 사용자 그룹	SuperAdmin	admin	0	발성	SPARROW-ADMIN	-		취소하기	삭제하기
	인종 공급자									
	작업 및 규칙	전체 2 사용자 1 - 2 표시됨 1 선택됨								
	이슈 검출 규칙									
	작업 프로파일									
	에이전트									
	태스크 에이전트									
	보고서									
	보고서 됌플릿									
	컴포넌트									
	사용자 컴포넌트									
	정보									
	시스템 정보									
	제품 라이선스 정보									
	22									
	감사 기록									

Warning: 기본 설정된 최고 관리자 계정의 ID인 admin은 삭제할 수 없습니다.

3. 아래를 참고하여 대체 사용자를 지정하세요.

4. 삭제하기 버튼을 클릭하세요.

## 대체 사용자\*

삭제할 사용자가 시스템 혹은 프로젝트에서 맡은 역할을 넘겨 받을 다른 사용자입니다. 사용자 목록에 미 리 추가된 사용자 중에 하나의 사용자를 선택할 수 있습니다.

대체 사용자는 삭제되는 사용자의 1) 시스템 역할, 2) 프로젝트 역할, 3) 이슈 담당자로 지정된 이슈를 넘 겨 받게 됩니다. 그 외에 삭제되는 사용자가 생성한 프로젝트나 수행한 작업 등에는 해당 시점의 데이터가 그대로 저장됩니다.

사용자 그룹 관리하기

시스템의 **인증 및 사용자 관리** 권한이 있는 관리자는 **사용자 그룹** 메뉴에서 등록된 사용자 그룹 목록 및 사용자 그룹 정보를 확인하고 변경할 수 있습니다. 사용자 그룹 목록을 확인하는 방법은 다음과 같습니다.

1. 왼쪽 사이드 바에서 관리를 클릭하세요.

2. 사용자 메뉴에서 사용자 그룹을 클릭하세요.

사용자 그룹 목록에 표시되는 각 항목에 대한 설명은 아래의 내용을 참고하세요.

## 이름

사용자 그룹의 이름입니다.

#### 사용자 수

사용자 그룹에 포함된 사용자 계정의 개수입니다.

## 사용자 그룹 추가하기

시스템의 **인증 및 사용자 관리** 권한이 있는 관리자는 **관리**의 **사용자 그룹**에서 아래 방법으로 새 사용자 그룹 을 추가할 수 있습니다.

1. 사용자 그룹 페이지에서 오른쪽 위에 있는 사용자 그룹 추가하기 버튼을 클릭하세요.

S 🔊	Sparrow Enterprise » 관리	> 인증 및 사용자	4	용자 그룹 추가								×
<i>e</i> ,	역할 및 권한 시스템 역할	사용자 그룹 목록		응자 그룹 이름 • 나용자 그룹 이름을 입력ㅎ	내요.							
ege col	프로젝트 역할 결재선	Q 검색어를 두 글자 이상 입력하세요.	관 필	<sup>물자</sup> Q, 검색어를 두 글자 이	남 입력하세요.		필터 🗸			선택하기 해제하기	20개씩 보	1 ~ 열편집 ~
100 100	인종 및 사용자 사용자	사용자 그룹 이름 🛧			이름 ()	아바타	활성화 💲	역할	사용자 그룹	최근 접속 일시 💲	만료 일시	선택 0
Ð	사용자 그룹			SuperAdmin	admin	0	월 50 활성	SPARROW-ADMIN	-	-	-	
8	인종 공급자 작업 및 규칙		2	제 <b>2 사용자 1</b> - 2 표시됨								페이지 이동 🔶
	이슈 검출 규칙										_	
	작업 프로파일 에이전트											
	태스크 에이전트											
	보고서 보고서 웹플렛											
	컴포넌트											
	사용자 컴포넌트											
	<sup>8 또</sup> 시스템 정보											
	제품 라이선스 정보											
	감사 기록											
											취소하기	계속 추가하기 추가하기

2. 아래의 내용을 참고하여 사용자 그룹 정보를 입력하세요.(\*는 필수 입력 항목)

3. 추가하기 버튼을 클릭하세요.

4. 사용자 그룹이 성공적으로 추가되면 왼쪽 아래에 성공 메시지가 출력됩니다.

## 사용자 그룹 이름\*

사용자 그룹의 이름이며 50자 이하의 한글, 영문, 숫자, 특수 문자, 공백을 입력할 수 있습니다.

사용자

새 사용자 그룹에 포함할 사용자의 목록으로 사용자 관리하기에서 확인할 수 있는 사용자가 표시됩니다. 목록의 오른쪽에 있는 **선택** 항목을 활성화하여 사용자를 사용자 그룹에 추가할 수 있습니다. 하나 이상의 사 용자를 변경하려는 경우 목록에서 추가할 사용자의 체크박스를 선택하고 **선택하기** 혹은 **해제하기** 버튼을 클릭하여 사용자를 사용자 그룹에 포함하거나 제외할 수 있습니다.

Tip: 사용자를 사용자 그룹에 추가하는 동작으로 인해 선택된 사용자의 다른 정보가 변경되지 않습니다.

인증 공급자 관리하기

기존의 인증 정보를 사용하여 다수의 사용자를 추가하려는 경우 시스템의 **인증 및 사용자 관리** 권한이 있는 관리자는 **인증 공급자** 메뉴에서 등록한 LDAP 서버의 정보를 사용할 수 있습니다. 다음과 같이 LDAP 서버를 등록하세요.

1. 인증 공급자 페이지에서 오른쪽 위에 있는 수정하기 버튼을 클릭하세요.

2. **활성화** 버튼을 토글하여 활성화세요.

- 😻 s	Sparrow Enterprise » 관리 >	만중 및 사용자	LDAP 서버 수정	×
æ.	역할 및 권한		왕성화 *	
90	시스템 역할	LDAP		
	프로젝트 역할		URL *	
÷	결재선	활성화 여부 아니요	URL을 입력하세요.	
000	인증 및 사용자			연결 테스트
2	사용자		기본 DN •	
Ð	사용자 그룹		기본 DN을 입력하세요.	
	인증 공급자		ID 속성 *	
	작업 및 규칙		ID 속성을 입력하세요.	
	이슈 검출 규칙		동적 사용자 생성 *	
	작업 프로파일			
	에이전트		✔ 선택 입력 항목 보기	
	태스크 에이전트			
	보고서			
	보고서 템플릿			
	컴포넌트			
	사용자 컴포넌트			
	정보			
	시스템 정보			
	제품 라이선스 정보			
	22			
	감사 기록			
				취소하기 <mark>수정하기</mark>

3. 아래의 내용을 참고하여 인증 공급자 정보를 입력하세요.(\*는 필수 입력 항목)

4. 수정하기 버튼을 클릭하세요.

5. 인증 공급자가 성공적으로 추가되면 왼쪽 아래에 성공 메시지가 출력됩니다.

## 활성화\*

LDAP 서버 정보의 사용 여부를 의미합니다. 이 정보를 사용자 인증에 사용하려면 이 옵션의 토글 버튼을 활성화해야 합니다.(기본값: 비활성)

Tip: LDAP 서버를 설정한 후 활성화 버튼을 비활성화한 경우에도 이미 저장된 정보는 사라지지 않습 니다.

#### URL\*

LDAP 서버의 URL이며 URL 형식으로 입력해야 합니다. URL을 입력한 후 **연결 테스트** 버튼을 클릭하여 LDAP 서버에 정상적으로 연결되는지 확인하세요.

## 기본 DN\*

LDAP 서버의 기본 DN이며 최대 200자까지 입력할 수 있습니다.

## ID 속성\*

LDAP 인증 공급자를 사용할 때 사용자 ID로 사용할 속성이며 최대 500자까지 입력할 수 있습니다.

## 동적 사용자 생성\*

활성화하는 경우 인증 공급자에 등록된 사용자 정보를 사용하여 Sparrow Enterprise 서버에 등록되지 않은 사용자를 자동으로 추가합니다. 비활성화하는 경우 동적 사용자를 생성하지 않으므로 서버에 등록되지 않은 사용자를 자동으로 추가하지 않습니다.(기본값: 활성)

## 사용자 DN

LDAP 서버 인증에 사용할 사용자 DN이며 최대 200자까지 입력할 수 있습니다.

#### 비밀번호

사용자 DN과 함께 LDAP 서버 인증에 사용할 비밀번호입니다.

#### 타임아웃

LDAP 서버에 연결을 시도하는 경우 사용하는 제한 시간이며 최대 600을 입력할 수 있습니다.(단위: 초)

#### 이름 속성

사용자 계정의 이름으로 사용될 속성 이름이며 최대 500자까지 입력할 수 있습니다. 값이 존재하지 않는 경우 사용자 계정의 이름을 입력하지 않습니다.

## 이메일 속성

사용자 계정의 이메일로 사용될 속성 이름이며 최대 500자까지 입력할 수 있습니다. 값이 존재하지 않는 경우 사용자 계정의 메일을 입력하지 않습니다.

## 작업 및 규칙

이슈 검출 규칙 관리하기

시스템의 **작업 및 규칙 관리** 권한이 있는 관리자는 **이슈 검출 규칙** 메뉴에서 등록된 이슈 검출 규칙을 확인 하고 사용 여부를 결정할 수 있습니다. 이슈 검출 규칙 목록을 확인하는 방법은 다음과 같습니다.

1. 왼쪽 사이드 바에서 **관리**를 클릭하세요.

2. 이슈 메뉴에서 이슈 검출 규칙을 클릭하세요.

Tip: 이슈 검출 규칙 목록의 위에 표시되는 알림 메시지에서 이슈 검출 규칙이 업데이트된 시각을 확 인할 수 있습니다.

이슈 검출 규칙 목록에 표시되는 각 항목에 대한 설명은 아래의 내용을 참고하세요.

## 유형

이슈 검출 규칙을 적용하는 작업을 기준으로 이슈 검출 규칙의 유형을 구분합니다. 이 옵션은 작업에 따 라 **소스코드**, 웹 취약점, 컴포넌트, 자가 방어로 나눠집니다.

## 이슈 검출 규칙 제공자

이슈 검출 규칙을 생성한 주체를 표시합니다. **기본**으로 표시된 경우 Sparrow Enterprise에서 기본으로 제 공하는 이슈 검출 규칙을 의미합니다. 사용자가 직접 이슈 검출 규칙을 추가한 경우 **사용자 정의**로 표시됩니 다. 사용자 지정 이슈 검출 규칙을 추가하는 방법은 사용자 지정 이슈 검출 규칙 추가하기를 참고하세요.

## 언어

이슈 검출 규칙이 지원하는 언어를 표시합니다.

Tip: 웹 취약점 및 컴포넌트 관련 이슈 검출 규칙의 경우 언어가 공통으로 표시됩니다.

## 위험도

이슈 검출 규칙의 위험도이며 매우 높음, 높음, 보통, 낮음, 매우 낮음이라는 5단계로 구분합니다.

## 규칙 이름

이슈 검출 규칙의 이름입니다.

## 레퍼런스

이슈 검출 규칙이 포함되어 있는 국내외 소스코드 취약점 혹은 품질 관련 기준입니다. 레퍼런스에 해당하 는 이슈 검출 규칙의 경우 다음과 같은 레퍼런스 중 하나 이상이 표시될 수 있습니다. .NET framework design guideline, Code conventions for the Java Programming Language(Oracle), CWE 658 4.14, CWE 658 4.7, CWE 659 4.14, CWE 659 4.7, CWE 660 4.14, CWE 660 4.7, JavaScript 시큐어코딩 가이드 2022, MISRA-C 2004, MISRA-C 2012, MISRA-C 2012 Amendment 2, MISRA-C 2012 Amendment 3, MISRA-C++ 2008, OWASP 2017, OWASP 2021, Python 시큐어코딩 가이드 2022, Rust ANSSI guide v1.0, 무기체계 소프트웨어 보안약점 점검 목록, 방위사업청 코딩규칙, 소프트웨어 보안약점 진단가이드 2021, 주요정보통신기반시설 취약점 분석·평가 기준.

## 활성화

이슈 검출 규칙의 활성화 상태이며 활성, 비활성 중 하나로 표시됩니다.

## 이슈 검출 규칙 수정하기

이슈 검출 규칙은 이미 정해진 보안 또는 품질 관련 지침이므로 주요 사항을 변경할 수는 없습니다. 하지만 이슈 검출 규칙의 **상세 정보**가 포함되어 있는 경우 허용하는 범위 안에서 세부적인 규칙을 조정할 수 있습니 다. 자세한 내용은 다음을 참고하세요.

<b>S</b>	Sparrow Enterprise » <u>관리</u> >	이슈 검출 규칙							이슈 검출 규칙 수정 X
~	역할 및 원한 시스템 역할	<b>9</b> 2	024-06-03 21:15	:48에 마지막으로 업데이트 되었	규칙 이름 AccessController.doPrivileged 내 신뢰할 수 없는 입력 유생				
89 <u>0</u>	프로닉트 닉플 <b>결재선</b> 인증 및 사용자	이슈	검출 규칙 목	록					소스코드 언어 Java
8	사용자	Qi	Q. 검색어를 두 글자 이상 입력하세요.		필터 🗸				실명 AccessController.doPrivileged 내 신뢰할 수 없는 입력 체커
Ð	사용자 그룹		유형 💲	이슈 검출 규칙 제공자 🌐	언어 ③	위험도 💲	규칙 이름 🔨	레퍼런스	는 AccessController.doPrivileged() 메소드에서 외부 값이 겸 증 없이 사용되면 검출합니다.
8	인증 공급자		🧀 소스코드	기본	C++	1111	== 및 != 연산자를 사용한 문자열 비교	없음	외부 값에 대해 검증 없이 사용될 경우 공격자가 시스템에 존재하 는 파일에 접근할 수 있습니다.
-	작업 및 규칙		🧀 소스코드	기본	Obj-C	m	@synchronized 지시자에 nil 전달	없음	권한이 부여된 블록에서 유효성이 확인되지 않았거나 신뢰할 수 없는 데이터를 이용해 연산하면 안됩니다.
	이슈 검출 규칙		🛷 소스코드	기본	C++	100	[] 연산자를 통한 배열 접근	없음	162
	작업 프로파일		🐨 컴포넌트	기본	35		AAL 라이선스 컴포넌트 사용	없음	Java 보안 약점 위해도 •
	에이전트		😻 컴포넌트	기본	35		Abstyles 라이선스 컴포넌트 사용	없음	태태 배우높음 ~
	태스크 에이전트		🛷 소스코드	기본	Java		AccessController.doPrivileged 내 신뢰할 수 없는	없음	활성화 •
	보고서		🐨 컴포넌트	기본	35		AdaCore-doc 라이선스 컴포넌트 사용	없음	
	보고서 템플릿		🐨 컴포넌트	기본			Adobe-2006 라이선스 컴포넌트 사용	없음	상세 정보
	신유가 커피네트		🐨 컴포넌트	기본	35		Adobe-Glyph 리이선스 컴포넌트 사용	없음	
	정보		🦁 컴포넌트	기본	공동		ADSL 라이선스 컴포넌트 사용	없음	AccessController 클래스 @ java.security.AccessController
	시스템 정보		🐨 컴포넌트	기본	35		AFL-1.1 라이선스 컴포넌트 사용	없음	AccessController
	재품 라이선스 정보		😴 컴포넌트	71足	공동		AFI -1.2 라이셔스 컴포너트 사용	었음	
	로그		정무너트	218	采奏		ΔFI -2 0 라이서스 컴퓨너트 사용	 N-2	
	감사 기록			71보	25		AEI-21 관이서스 커프너트 사요	어우	dovrtovieged vijoza 💓
			- BILLE	716	75				취소하기 수정하기

1. 이슈 검출 규칙 목록에서 항목을 클릭하세요.

2. 슬라이드에서 아래를 참고하여 수정할 내용을 선택하거나 입력하세요.

3. 수정하기 버튼을 클릭하세요.

## 위험도

이슈 검출 규칙의 **위험도**입니다. 드롭다운 버튼을 클릭하여 **매우 높음**, **높음**, **보통**, **낮음**, **매우 낮음** 중에서 변경하려는 위험도를 선택할 수 있습니다.

Warning: 기본적으로 위험도는 국내외 레퍼런스를 기준으로 구분되어 있습니다. 위험도를 조정하면 검출된 이슈가 얼마나 위험한지에 대해 정확한 판단이 어려울 수 있다는 점에 주의하세요.

## 활성화

규칙을 분석 작업에 적용할 것인지 결정합니다. **활성화** 버튼을 비활성화하면 해당 규칙을 모든 분석에 사 용하지 않게 됩니다. 버튼을 활성화하면 다시 해당 규칙을 적용하여 작업을 실행합니다.

**Tip**: 특정 프로젝트에서 특정 이슈 검출 규칙을 적용하여 작업을 시작하려는 경우 작업 프로파일 관 리하기를 참고하세요.

## 상세 정보

세부적인 **검출 규칙**이나 **제외 규칙**을 표시합니다. 검출 규칙마다 여기에 표시되는 옵션의 내용이 다릅니 다. 권한이 있는 사용자는 이 옵션을 조정하여 규칙이 허용하는 조건 안에서 검출 규칙이나 제외 규칙을 수 정할 수 있습니다.

#### 사용자 지정 이슈 검출 규칙 추가하기

시스템의 **작업 및 규칙 관리** 권한이 있는 관리자는 **사용자 지정 이슈 검출 규칙**을 추가할 수 있습니다. 자세 한 내용은 다음을 참고하세요.

**Tip**: 현재 웹 취약점에 대한 이슈 검출 규칙만 사용자가 추가할 수 있습니다.

1. **이슈 검출 규칙** 페이지에서 오른쪽 위에 있는 **사용자 정의 규칙 추가하기** 버튼을 클릭하세요.

- <b>(</b> )	Sparrow Enterprise » <u>관리</u> >	이슈 검출 규칙						사용자 정의 규칙 추가 🛛 🗙
<i>e</i> ,	역할 및 권한 시스템 역할		5:48에 마지막으로 업데이트 되었	(습니다.				기본 정보
89 00	<b>프로젝트 역할</b> <b>결제선</b> 인중 및 사용자	이슈 검출 규칙 목	<b>극록</b> 1상 인력하세요.	필터 🗸				유형 • 이슈 유항을 선택하세요.
8	사용자 사용자 그룹	여 김석이를 두 물자 이상 감격하세요.           유형 :         아슈 감금 규칙 제공자 :         암석           ····································		언어 :	위험도 🗘	규칙 이름 🛧	레티언스	실명 * 검출된 이슈의 결과에 포함될 설명을 입력하세요.
۲	인종 공급자 작업 및 규칙	····································	기본 사용자 정의	C+++ 공동		# 혹은 ## 연산자 사용 ####	MISRA-C 2004 의 2개 없음	
	이슈 컴출 규칙 작업 프로파일		기분	C++		## 지시자 사용 #braama 지시자 사용	없음 MISRA-C 2004 위 1개	위험도 •
	에이전트 태스크 에이전트	0 ±435	기본	C++		#undef 지시자 사용	MISRA-C 2004 외 2개	환성화 *
	보고서 보고서 행플릿	·····································	기본	C++ Java	1	* 및 & 토큰 규칙 위반 + 및 += 연산자로 더해진 문자열	218 218	이슈 유형을 선택하면 검출 규칙에 해당하는 상세 정보를 추가적 으로 입력할 수 있습니다.
	컴포넌트 사용자 커피너트	· · · · · · · · · · · · · · · · · · ·	기분	C#		+ 연산에 사용된 빈 문자열 += 연산자로 더해진 문자열	없음 없음	
	정보	0 <u>4475</u>	기분	C++		, 연산자 사용	MISRA-C 2004 외 2개	
	시스템 정보 제품 라이선스 정보	····································	기본	공동 C++		0BSD 라이선스 컴포넌트 사용 0으로 나누기	없음 MISRA-C 2004 의 4개	
	로그 감사 기록		기분	C#		0으로 나누기	무기체계 소프트웨어 보안약점 점검 목록 드기체계 소프트웨어 보아야적 정검 목록	
		······································	기본	Obj-C		0으로 나누기	가지에게 프로드레이 프로그램 영업 목록 없음	취소하기 <mark>추가하기</mark>

2. 아래의 내용을 참고하여 이슈 검출 규칙의 정보를 입력하세요.(\*는 필수 입력 항목)

3. 추가하기 버튼을 클릭하세요.

4. 사용자 정의 이슈 검출 규칙이 성공적으로 추가되면 왼쪽 아래에 성공 메시지가 출력됩니다.

## √ 기본 정보

## 유형\*

추가할 이슈 검출 규칙이 Sparrow Enterprise가 지원하는 분석 중 어디에 해당하는지를 구분합니다. 현재 **웹 취약점**만 선택할 수 있습니다.

## 규칙 이름\*

추가할 이슈 검출 규칙의 이름이며 최대 50자까지 입력할 수 있습니다.

## 설명\*

추가할 이슈 검출 규칙에 대한 설명이며 최대 2000자까지 입력할 수 있습니다. 여기에 입력한 내용은 이 규칙으로 검출된 이슈의 결과인 이슈 상세 정보 페이지에 표시됩니다.

## 위험도\*

추가할 이슈 검출 규칙의 위험도이며 **매우 높음**, **높음**, **보통**, **낮음**, **매우 낮음**이라는 5단계로 구분합니다. (기본값: 매우 높음)

## 활성화 여부\*

추가할 이슈 검출 규칙의 사용 여부를 의미합니다. 이 규칙을 분석에 사용하려면 이 옵션의 토글 버튼을 활성화해야 합니다.(기본값: 활성)

## √ 상세 정보

#### 침투 공격 대상

웹 취약점 분석 과정에서 공격 문자열을 배치할 위치입니다. **퀴리 문자열**, **폼 데이터**, **쿠키**, **HTTP 헤더**, **URL 경로** 중에서 하나 이상의 대상을 선택할 수 있습니다.

## RPC 공격 대상

웹 취약점 공격 문자열을 삽입할 데이터 형식입니다. multipart/form-data, XML, JSON, 구글 웹 툴킷, DWR 중에서 하나 이상의 대상을 선택할 수 있습니다.

#### 공격 문자열

웹 취약점 공격 수행 도중 서버로 전송하는 HTTP 요청 내부에 포함시킬 수 있는 문자열입니다. 하나 이상 의 문자열을 엔터와 쉼표(,)로 구분하여 입력할 수 있습니다.

## 검출 정규식

웹 취약점 공격에 대한 서버의 HTTP 응답에서 취약점을 검출하기 위해 사용하는 정규식입니다. 하나 이 상의 정규식을 엔터와 쉼표(,)로 구분하여 입력할 수 있습니다.

## 제외 정규식

웹 취약점 검출에서 제외할 대상을 정의하기 위해 사용하는 정규식입니다. 하나 이상의 정규식을 엔터와 쉼표(,)로 구분하여 입력할 수 있습니다.

#### 작업 프로파일 관리하기

프로젝트에서 **분석, 자가 방어, 테스트 케이스 최적화** 작업을 수행하는 경우 **작업 프로파일**을 선택해야 합니 다. 선택한 **작업 프로파일**을 통해 작업에 사용할 이슈 검출 규칙 및 작업 옵션을 결정합니다.

<b>S</b>	iparrow Enterprise » 관리 >	작업 프로파일		작업 프로파일 수정하기							×			
<i>₹</i>	역할 및 권한 시스템 역할 프로젝트 역할	작업 프로파일 목록		표로제일 이름 - 모든 작업과 경울 규칙										
ଙ୍ଖ <u>ଇ</u> ା	결재선 이즈 이 나오다.	Q 검색어를 두 글자 이상 입력하세요.	필터 🗸	역할을	선택하세요.			~	<ul> <li>⑦ 전수 분석</li> <li>第 테스트 키</li> </ul>	×	분석 × 🚺 지	가방이 ×	```	~
22	사용자 그룹	프로파일 아름 구 모든 작업과 검출 규칙	여용된 석일 전수 분석, 수시 분석, 자가 방어, 테	() 겸	출 규칙									
<b>e</b>	인증 공급자 작업 및 규칙	소프트웨어 모안약점 신단가이드 겸을 규칙 자가 방어 검출 규칙	신수 문식, 수시 문식 ?	০ ব্ৰ	넘색어를 두 글자 이상	} 입력하세요.		필터 🗸		선택하기	해제하기	20개씩 보기 🗸	일편집	~
	이슈 검출 규칙 작업 프로파일	주요정보통신기반시설 취약점 분석·평가 기준 검출 규칙 컴포넌트 분석 검출 규칙	전수 분석, 수시 분석 전수 분석, 수시 분석		유형 🗘	언어 ③ C++	위험도 ()	규칙 이름 ↑ # 혹은 ## 연산자 사용					활성화 (	۵ ۲
	에이전트 태스크 에이전트	전체 5 프로파일 1 - 5 표시팀			<ul> <li>         소스코드     </li> <li>         소스코드     </li> </ul>	C++ C++		#if 지시자 사용 #pragma 지시자 사용						) >
	보고서 보고서 템플릿				<ul> <li>소스코드</li> <li>소스코드</li> </ul>	C++ C++		#undef 지시자 사용 * 및 & 토큰 규칙 위반						) )
	컴포넌트 사용자 컴포넌트				<ul> <li>소스코드</li> <li>소스코드</li> </ul>	Java C#		+ 및 += 연산자로 더해진 + 연산에 사용된 빈 문자(	! 문자열 열					>
	<sup>정보</sup> 시스템 정보			0		C#		+= 연산자로 더해진 문자	열					5
	제품 라이선스 정보 로그			0	<ul> <li>철포넌트</li> </ul>	35		, 근근지 지당 OBSD 라이선스 컴포넌트	사용					5
	강사 기록				🤣 소스코드	C#		0으로 나누기				취소하기 삭제하	·기 수정하	)  7

만약 특정 레퍼런스에 해당하는 이슈만을 검출하려면 1) 먼저 작업 프로파일 추가하기를 참고하여 해당 레 퍼런스의 작업 프로파일을 생성하세요. 여기서 추가한 작업 프로파일은 모든 프로젝트에 공통적으로 적용 되지만 작업 유형 및 프로젝트 역할을 통해 사용할 수 있는 작업과 사용자를 조정할 수 있습니다. 그런 다음, 2) 새 작업 시작하기 슬라이드에서 작업 프로파일을 선택하세요. 앞서 언급한 대로 작업 유형 및 프로젝트 역할에 따라 사용할 수 있는 작업 프로파일이 표시됩니다. 또한 작업 프로파일에 특정 레퍼런스로 매핑된 규 칙이 모두 포함되어 있는 경우, 해당 레퍼런스의 이름을 작업 프로파일에서 바로 확인하실 수 있습니다.

특히, **전수 분석**과 **수시 분석**에서 사용할 수 있는 작업 프로파일을 구분할 수 있도록 설계되었습니다. 따라 서, 관리자가 전수 분석인 경우 특정 작업 프로파일만 사용해서 분석하도록 설정함으로써 전수 분석의 분석 결과를 정확하게 관리할 수 있습니다.

## 작업 프로파일 추가하기

시스템의 **작업 및 규칙 관리** 권한이 있는 관리자는 **작업 프로파일** 페이지에서 작업 프로파일을 추가할 수 있 습니다. 작업 프로파일을 만드는 방법은 다음과 같습니다.

1. 작업 프로파일 페이지에서 오른쪽 위에 있는 프로파일 추가하기 버튼을 클릭하세요.

💱 Sparrow Enterprise > স্থ্র ২ মৃত্র মহলপ্র				작업 프로파일 추가하기					×
2	역할 및 권한 시스템 역할	작업 프로파일 목록		프로파일 이용 - 작업 프로파일 이용을 일찍하세요.					
00	프로젝트 역할			사용 가능한 역할 🥝				히용할 작업 🔘 •	
999 1	결재선	Q, 검색어를 두 글자 이상 입력하세요.	필터 🗸	역할을 선택하세요.			~	허용할 작업 유형을 선택하세요.	~
<u>000</u>	인증 및 사용자	프로파일 이름 个	허용된 작업						
2	사용자	모든 작업과 검출 규칙	전수 분석, 수시 분석, 자가 방어, 테:	① 검출규칙					
Ð	사용자 그룹	소프트웨어 보안약점 진단가이드 검출 규칙	전수 분석, 수시 분석 :						
8	인증 공급자	자가 방어 검출 규칙	자가 방어	Q. 검색어를 누 글사 이상 입력하세요. 웰터 🂙			원리 🗸	신덕이가 에세이가	20개적보기 🗸 일반집 🗸
	작업 및 규칙	주요정보통신기반시설 취약적 분석-평가 기준 검출 규칙	전수 분석 수치 분석	유형 🗘	언어 💲	위험도 💲	규칙 이름 个		<b>팜성화</b> 💲
	이슈 검출 규칙			📄 🧼 소스코드	C++		# 혹은 ## 연산자 사용		
	작업 프로파일	김보인트 군의 김물 규의	신부 문역, 부시 문역	📄 🧼 소스코드	C++	0.00	#if 지시자 사용		
	에이전트	전체 5 프로파일 1 - 5 표시됨		📄 🛛 🥺 소스코드	C++		#pragma 지시자 사용		
	태스크 에이전트			📄 🛛 🧀 소스코드	C++		#undef 지시자 사용		
	보고서			📄 🛷 소스코드	C++		* 및 & 토큰 규칙 위반		
	국고서 남글 X			📄 🧼 소스코드	Java		+ 및 += 연산자로 더해진 [	로자열	
	사용자 컴포넌트			📄 🧼 소스코드	C#		+ 연산에 사용된 빈 문자열		
	정보			📄 🛛 🥺 소스코드	C#		+= 연산자로 더해진 문자열	1	
	시스템 정보			🗌 🛷 소스코드	C++		, 연산자 사용		
	제품 라이선스 정보			💿 😻 컴포넌트	35	1111	OBSD 라이선스 컴포넌트 -	사용	
	로그			🗌 🛷 소스코드	C#		0으로 나누기		
	감사 기록								
									취소하기 <mark>추가하기</mark>

#### 2. 작업 프로파일 이름을 입력하세요.

3. 아래의 내용을 참고하여 사용 가능한 역할과 허용할 작업을 선택하세요.(\*는 필수 입력 항목)

4. 검색이나 필터를 사용하여 작업 프로파일에서 **사용할 이슈 검출 규칙**을 선택하세요.

Tip: 작업 프로파일에서 선택하지 않은 이슈 검출 규칙은 작업에 사용되지 않습니다. 즉, 규칙을 선택 하지 않으면 해당 규칙은 분석, 방어, 최적화에 적용되지 않습니다.

5. 추가하기 버튼을 클릭하세요.

6. 작업 프로파일이 성공적으로 추가되면 왼쪽 아래에 성공 메시지가 출력됩니다.

## √ 기본 정보

작업 프로파일 이름\*
추가할 작업 프로파일의 이름이며 50자 이하의 한글, 영문, 숫자, 특수 문자, 공백을 입력할 수 있습니다.

#### 사용 가능한 역할

추가할 작업 프로파일을 사용할 수 있는 프로젝트 역할을 지정합니다. 프로젝트 역할 관리하기에서 설정 한 역할 중 하나 이상을 선택할 수 있습니다. 이 옵션을 입력하면 선택한 프로젝트 역할의 구성원만 추가할 작업 프로파일을 사용하게 됩니다. 이 옵션을 입력하지 않으면 모든 프로젝트 구성원이 해당 작업 프로파일 을 사용할 수 있습니다.

#### 허용할 작업\*

추가할 작업 프로파일을 사용할 수 있는 작업 유형을 의미합니다. 이 옵션에서 선택한 작업에만 해당 작 업 프로파일을 적용할 수 있습니다. 라이선스에 따라 **전수 분석**, **수시 분석**, **자가 방어**, **테스트 케이스 최적화** 중 하나 이상을 선택할 수 있습니다.

#### ✓ 검출 규칙\*

추가할 작업 프로파일에서 사용할 이슈 검출 규칙의 목록입니다. 목록에서 작업 프로파일에 추가할 규칙 의 **선택** 항목을 활성화하세요. 목록에 표시된 정보에 대한 자세한 내용은 이슈 검출 규칙 관리하기를 참고하 세요.

특정 레퍼런스에 해당하는 이슈 검출 규칙만을 작업 프로파일에서 활성화하려면 **레퍼런스**로 목록을 필터 링하고 표시된 목록을 전체 선택한 다음, 목록의 오른쪽 위에 있는 **선택하기** 버튼을 클릭하세요.

① 검출규칙								
Q, 검색어를 두 글자 이상 입해	박하세요.		필터 🚺 🗸	선택하기	ধ্বমাঞ্চগ	20개씩 보기	~ 98	18 V
레피런스: OWASP 2017 木 🖗	3)							
.NET framework design	n guideline		규칙이름 🛧					254 C
CWE 658 4.7			AJP 서비스 노출					
CWE 659 4.7			CRLF 십입					
CWE 660 4.7			Host NEI					-
Code conventions for th	he Java Progra	mmin	Hoat Ment					-
☐ JavaScript 시큐어코딩 가	이드 2022		HTTP 메소드 위조					-
MISRA-C 2012			HTTP 응답 헤더에 포함된 서버 정보					
MISRA-C 2004			JMX/RMI 서비스 노출					
MISRA-C++ 2008			Snoop 서불릿 정보 노출					
0WASP 2017	U++	10	SQL 삽입					
🗌 🔁 원 사약법	85	배우높음	SSI 삽입					
🗋 📵 웹 취약정	85	• #8	Torncat 예제					
전 법 위역법	28	18	URL 내 세션 ID					
<ul> <li>· · · · · · · · · · · · · · · · · · ·</li></ul>	35	18	URL 접근 제한 실패					
🗋 📵 웹 취약점	85	918	web.xml 노출					
<ul> <li>· · · · · · · · · · · · · · · · · · ·</li></ul>	25	812	Xitami Web Server 정보 유출					
2544 8	Java	18	XPath 십입					
전 법 취약정	85	星辰	개별 주소 노출					
□ 8 ±×95	C++	- ¥8	경로 조작					
<ul> <li>한 법 유익법</li> </ul>	85	N8	관리자 페이지 노출					
🗌 🖸 웹 사익점	85	948	누락된 Content-Security-Policy (6	CSP) 헤디				
전 웹 취약용	38	118	누락된 X 콘텐츠 타입 옵션					
체 52 컴플 규칙 1 - 20 표시된				1 2	3 >	*	이지 이동	<i>→</i>

#### √ 작업 옵션

#### 소스코드 분석

#### 분석 제외 경로

분석 제외 경로는 분석에 포함하지 않을 폴더나 파일의 경로를 의미합니다. 즉, 이 옵션에 값을 입력하면 추가할 작업 프로파일로 분석을 수행할 때 특정 경로를 분석하지 않도록 설정할 수 있습니다. 필요한 경우 하나 이상의 경로를 입력하고 엔터로 구분할 수 있습니다.

분석 제외 경로에 입력한 경로는 소스코드 분석에만 적용된다는 점에 주의하세요. 즉, 이 경로에 해당하는 컴포넌트 분석의 자산과 이슈는 분석 결과에 그대로 표시됩니다.

에이전트

태스크 에이전트 관리하기

۳	Sparrow Enterprise » 관리	에어전트		<b>.</b> e	admir	1 🗸
≪ 88 89 3]	여달 및 관한 시스템 역할 프로젝트 역할 결재선 인증 및 사용자	태스크 에이전트 목록         보터 ✓         24           Q. 검색어표 두글자 이상 입력하세요.         보터 ✓         24           예여전트 D         예여전트 여름 ↑         상태 ☆ 실행 중입 역성 ☆	)개씩 보기 🛛 🗸	열편	g ~	
10 B	사용자 사용자 그룹	등록 대기 중이거나 내용이 없습니다.				
۲	인종 공급자 작업 및 규칙 이슈 검출 규칙					
	작업 프로파일 에이전트					
	태스크 에이전트 보고서 보고서 행플릿					
	컴포넌트 사용자 컴포넌트					
	상모 시스템 정보 제품 라이선스 정보					
	로그 감사 기록					

다음과 같은 방법으로 등록된 Sparrow Enterprise의 태스크 에이전트 정보를 확인할 수 있습니다.

Tip: 태스크 에이전트를 설치하는 방법은 태스크 에이전트 설치하기를 참고하세요.

1. 왼쪽 사이드 바에서 관리를 클릭하세요.

2. 에이전트 메뉴에서 태스크 에이전트를 클릭하세요.

태스크 에이전트 목록에 표시된 항목에 대한 설명은 아래의 내용을 참고하세요.

#### 에이전트 ID

태스크 에이전트의 ID입니다. 고유한 번호로 부여되며 변경할 수 없습니다.

#### 에이전트 이름

태스크 에이전트의 이름이며 64자까지 표시됩니다. 에이전트를 설치할 때 설정할 수 있으며 변경할 수 없 습니다.

#### 상태

현재 에이전트의 상태이며 **사용 가능**과 **사용 중** 중 하나로 표시됩니다. **사용 가능**은 태스크 에이전트가 정상적으로 연결되었으며 액션을 실행하고 있지 않은 상태입니다. **사용 중**은 태스크 에이전트가 정상적으 로 연결되었지만 다른 액션을 실행하기 위해 특정 태스크에 할당되었기 때문에 추가로 액션을 실행할 수 없 는 상태를 의미합니다.

#### 실행 중인 액션

**사용 중**인 에이전트가 현재 액션을 실행하고 있는 경우 해당 액션을 표시합니다. 액션이 빠르게 실행되고 종료된 경우 표시되지 않을 수 있습니다.

## 보고서

보고서 템플릿 관리하기

보고서 템플릿 메뉴에서는 프로젝트에서 수행한 소스코드 분석, 컴포넌트 분석, 웹 취약점 분석, 자가 방어 에 대한 작업 보고서를 출력할 때 사용할 템플릿을 만들 수 있습니다. 또한 추가한 템플릿을 수정할 수도 있 습니다. 단, 보고서 템플릿 목록에 있는 **기본 템플릿**은 사용자가 수정하거나 삭제할 수 없습니다. 보고서 템 플릿을 확인하기 위해서는 다음과 같은 방법을 참고하세요.

1. 왼쪽 사이드 바에서 **관리**를 클릭하세요.

2. 정보 메뉴에서 보고서 템플릿을 클릭하세요.

#### 보고서 템플릿 추가하기

시스템의 **보고서 관리** 권한이 있는 관리자는 **관리** 메뉴의 **보고서 템플릿**에서 이런 방법으로 새 보고서 템플 릿을 추가할 수 있습니다.

1. 보고서 템플릿 페이지에서 오른쪽 위에 있는 보고서 템플릿 추가하기 버튼을 클릭하세요.

- 10	Sparrow Enterprise » 관리	) ¥24	보고서 템플릿 추가하기	×
<ul> <li>* :: : : : : : : : : : : : : : : : : :</li></ul>	Spartnow Enterprise         2         2           예약 및 전문	> 보24 보고서 템플릿 목록 면원 연 후 ↑ 기반 변원 전 관계1보24 명원 1-18.0년	보고서 범용및 추가하기 명문 이용 - 명문 이용 입역하세요. 보고사 제목을 입역하세요. 구성 요료 - 1 작업 요박 정보 2 속태로 일하수 수 3 국제원신 별 하수 수 4 요물 콤 참석 5 국제원신 별 하수 수 6 요물 규 참보 2 전문 400 4 7 × (CME 608 4 7 × ) CME 608 4 7 × (CME 608 4 7 × ) CME 608 4 7 × (CME 608 4 7 × ) (CME 600 4 7 × ) CME 600 4 7 × (CME 608 4 7 × ) 1	
	시스템 정보 제품 라이선스 정보 로그 강사 기록		<ul> <li>약기재가 소프트웨어 보인약점 점검 목록 ×</li> <li>병대사업 프로디카 ×</li> <li>소프트웨어 보인약점 전단가에도 2021 ×</li> <li>산력 입력 정복 보기</li> </ul>	
			취소하기 주가하	

2. 아래의 내용을 참고하여 보고서 템플릿 정보를 입력하세요.(\*는 필수 입력 항목)

3. 추가하기 버튼을 클릭하세요.

4. 보고서 템플릿이 성공적으로 추가되면 왼쪽 아래에 성공 메시지가 출력됩니다.

#### 템플릿 이름\*

보고서 템플릿의 이름이며 50자 이하의 한글, 영문, 숫자, 특수 문자, 공백을 입력할 수 있습니다.

#### 보고서 제목\*

보고서 템플릿으로 출력할 보고서의 제목이며 50자 이하의 모든 문자를 입력할 수 있습니다.(기본값: Sparrow 보고서)

Tip: 보고서 제목은 출력할 보고서의 첫 페이지 및 페이지 헤더에 표시됩니다.

#### 구성 요소

보고서 템플릿에 포함될 요소입니다. 작업 요약 정보, 위험도별 이슈 수, 레퍼런스별 이슈 수, 검출 결과 상 세, 제외된 이슈 정보, 검출 규칙 정보로 구성되어 있습니다.(기본값: 모두 선택)

구성 요소 목록의 오른쪽에 있는 토글 버튼을 선택하여 해당 항목을 보고서 템플릿에 포함하거나 템플릿 에서 제외할 수 있습니다. 또한 구성 요소 목록의 왼쪽에 있는 선택 버튼을 클릭한 채로 드래그하여 항목의 순서를 변경할 수 있습니다.

#### 포함될 레퍼런스

보고서에 출력할 레퍼런스의 목록이며 **구성 요소** 중 **레퍼런스별 이슈 수**에 표시할 레퍼런스를 선택할 수 있습니다. 그러면 작업에서 검출된 이슈를 해당 레퍼런스에 비교하여 레퍼런스 기준에서 벗어나는 이슈의 개수를 확인할 수 있습니다.(기본값: 모두 선택)

만약 선택한 레퍼런스에 해당하는 이슈가 작업에서 검출되지 않은 경우 해당 레퍼런스는 작업 보고서에 표시되지 않습니다.

#### 보고서 로고

보고서의 첫 페이지에 표시할 로고 파일을 선택할 수 있습니다. 이미지 파일은 5MB 이하의 .jpg, .jpeg, .png 형식이어야 합니다.(기본값: Sparrow Enterprise 로고)

## 정보

시스템 정보 확인하기

시스템의 **시스템 관리** 권한이 있는 관리자는 다음과 같은 방법으로 등록된 Sparrow Enterprise의 시스템 정 보를 확인할 수 있습니다.

1. 왼쪽 사이드 바에서 관리를 클릭하세요.

2. 정보 메뉴에서 시스템 정보를 클릭하세요.

시스템 정보의 각 항목에 대한 설명은 아래의 내용을 참고하세요.

#### √ 제품 정보

제품 정보에는 제품명을 비롯하여 버전과 설치 정보가 표시됩니다. 버전에서는 제품 버전, 모듈별 버전, 빌드 일시, 빌드 ID에 대한 정보를 확인할 수 있습니다. 설치 정보에는 프로그램 경로, DB 경로, DB 드라이 버, DB 버전, DB URL이 포함됩니다.

#### √ 서버 정보

서버 정보에는 **운영 체제, CPU, 총 메모리, 사용 가능한 메모리, 총 디스크, 사용 가능한 디스크** 정보가 표 시됩니다.

#### √ 사용 현황

사용 현황에는 Sparrow Enterprise를 사용하는 **사용자 수**, **전체 프로젝트 수**, **전체 분석 수**, **전체 테스트 수**, **전체 이슈 검출 규칙 수**가 표시됩니다.

제품 라이선스 정보 확인하기

시스템의 **시스템 관리** 권한이 있는 관리자는 다음과 같은 방법으로 Sparrow Enterprise에 등록된 제품 라이 선스 정보를 확인할 수 있습니다.

1. 왼쪽 사이드 바에서 관리를 클릭하세요.

2. 정보 메뉴에서 제품 라이선스를 클릭하세요.

제품 라이선스 정보의 각 항목에 대한 설명은 아래의 내용을 참고하세요.

#### √ 제품 라이선스 정보

#### 시스템 ID

시스템을 구분하기 위한 고유의 ID이며 Sparrow Enterprise의 제품 라이선스를 발급하기 위해 사용됩니다.

**Tip**: 제품 라이선스를 갱신하려면 **시스템 ID**를 복사하여 스패로우 엔지니어에게 전달하세요. 엔지니 어에게서 제품 라이선스를 받은 다음, 오른쪽 위에 있는 **갱신하기** 버튼을 클릭하여 제품 라이선스를 입력하고 **갱신하기**를 클릭하면 Sparrow Enterprise의 제품 라이선스가 변경됩니다.

#### 시작일

Sparrow Enterprise의 제품 라이선스가 시작된 날짜입니다.

#### 사용 만료일

Sparrow Enterprise의 제품 라이선스가 만료되는 날짜입니다.

#### 남은 사용일

Sparrow Enterprise의 제품 라이선스를 사용할 수 있는 기간을 일로 표시합니다.

#### 최대 등록 사용자 수

Sparrow Enterprise에 등록할 수 있는 전체 사용자 계정의 개수입니다.

#### 남은 사용자 수

Sparrow Enterprise에 앞으로 등록할 수 있는 사용자 계정의 개수입니다.

#### 활성화된 도구

Sparrow Enterprise에 설치된 제품을 표시합니다. **sast,saqt,dast,rasp,sca,tso**와 같이 총 6개의 제품이 표 시될 수 있습니다.

#### √ SAST

#### 최대 라인 수

Sparrow SAST/SAQT에서 분석할 수 있는 소스코드 라인의 개수를 표시합니다.

#### √ SCA

#### 최대 누적 분석 크기

Sparrow SCA에서는 제품 라이선스를 통해 분석할 수 있는 대상 파일의 누적 크기를 제한하며 여기에 지 정된 용량을 표시합니다.

#### 현재 누적 분석 크기

Sparrow SCA에서 현재까지 분석한 대상 파일의 누적 크기를 표시합니다.

#### 남은 누적 분석 크기

Sparrow SCA에서 앞으로 분석할 수 있는 대상 파일의 크기를 표시합니다.

#### √ DAST

#### 최대 동시 분석 수

Sparrow DAST에서는 제품 라이선스를 통해 같은 시각에 분석할 수 있는 대상 웹 애플리케이션의 개수를 제한하며 여기에 지정된 개수를 표시합니다.

#### 현재 동시 분석 수

Sparrow DAST에서 현재 분석하고 있는 웹 애플리케이션의 개수를 표시합니다.

#### 남은 동시 분석 수

Sparrow DAST에서 현재 추가로 분석할 수 있는 웹 애플리케이션의 개수를 표시합니다.

#### √ RASP

#### 최대 동시 방어 수

Sparrow RASP에서는 제품 라이선스를 통해 같은 시각에 방어할 수 있는 대상 웹 애플리케이션의 개수를 제한하며 여기에 지정된 개수를 표시합니다.

#### 현재 동시 방어 수

Sparrow RASP에서 현재 방어하고 있는 웹 애플리케이션의 개수를 표시합니다.

#### 남은 동시 방어 수

Sparrow RASP에서 현재 추가로 방어할 수 있는 웹 애플리케이션의 개수를 표시합니다.

### 로그

## 감사 기록 확인하기

시스템의 **시스템 관리** 권한이 있는 관리자는 다음과 같은 방법으로 등록된 Sparrow Enterprise의 감사 기록 을 확인할 수 있습니다.

1. 왼쪽 사이드 바에서 관리를 클릭하세요.

2. 로그 메뉴에서 감사 기록을 클릭하세요.

감사 기록의 각 항목에 대한 설명은 아래의 내용을 참고하세요.

#### 사건 유형

Sparrow Enterprise에서 발생한 이벤트의 유형을 감사 시작, 감사 종료, 서비스 시작, 서비스 종료, 로그인, 로그아웃, 설정 변경, 보안 기능 수행, 분석 시작, 분석 종료로 분류합니다.

#### 사건 결과

Sparrow Enterprise에서 발생한 이벤트의 결과를 성공 혹은 실패로 분류합니다.

#### 주체

Sparrow Enterprise에서 발생한 이벤트의 주체를 사용자 정보의 **아바타**로 표시합니다.

#### 발생 IP

Sparrow Enterprise에서 이벤트가 발생한 IP를 표시합니다.

#### 발생 일시

Sparrow Enterprise에서 이벤트가 발생한 일시를 표시합니다.

#### 사건 내역

Sparrow Enterprise에서 이벤트가 발생할 때 서비스가 수행한 구체적인 내용을 문장으로 설명하거나 해 당하는 HTTP 요청을 표시합니다. Sparrow Enterprise에서 로그아웃하려면 Sparrow Enterprise 웹 페이지의 오른쪽 위에 있는 **사용자 이름**을 클릭하고 **로그아웃** 버튼을 클릭하세요.

1. 기본 메뉴의 오른쪽 끝에서 사용자 이름을 클릭하세요.

2. **로그아웃** 버튼을 클릭하세요.

# Windows 환경에서 데이터베이스가 정상적으로 초기화되지 않거나 구동되지 않습니다.

Sparrow Enterprise에 포함된 PostgreSQL Windows 버전의 경우 **Microsoft Visual C++ 2015 Redistributable**을 설치해야 합니다. Sparrow Enterprise 서버를 구동하기 전에 아래의 방법을 참고하여 패 키지에 포함된 Microsoft Visual C++ 2015 Redistributable을 사전에 설치해주세요.

1. \*\*{Sparrow Enterprise 서버 설치 디렉토리}\*\*에 있는 **prerequisite** 디렉토리로 이동하세요.

📑   🕑 📙 🖙   prerequisite			-		×
파일 홈 공유 보기					^ <b>()</b>
★ 나 문어님기 분 이동 위치 고정	<ul> <li>★ 삭제 •</li> <li>■ 이름 바꾸기</li> </ul>	▲ 집· 서 집· 월덕	₽÷ 2 2	문 선택	
클립보드	구성	새로 만들기 🛛 😫	기		_
$\leftarrow \rightarrow \prec \uparrow$ 📙 « spa > prereq	v ð ,2 pr	erequisite 검색			
이름 ^	수정한 날짜	유형	а	71	
🚜 erlang_otp_win64-23.3.4.11.exe	2023-06-02 오후 2:25	응용 프로그램	1	07,386K)	в
₩ vcredist_x64.exe	2023-06-02 오후 2:25	응용 프로그럼		7,034K	8
2개 항목				8	

2. vcredist\_x64.exe(64비트 환경) 혹은 vcredist\_x86.exe(32비트 환경)를 실행하여 Microsoft Visual C++ 2015 Redistributable을 설치하세요.

时 Microsof	t Visual C++ 2015 Redistributable (x64) - 14.0	_		×
	Microsoft Visual C++ 201	15		
	Redistributable (x64) - 14	.0.23	3026	
MICROSO	FT 소프트웨어 사용권 계약서			^
MICROSO 및 C++ 2	FT VISUAL STUDIO 2015 추가 기능, VISUAL 내배포 가능 패키지	STUDIC	) SHELL	
본 사용권	계약은 Microsoft Corporation(또는 거주 지역에 <u>보는 고등 관계가 다는 레이어에</u> 드는 바이우고 있어야 ))	따라 겨 	열사 중 ㅋㅋㅋ -	~
	- -	설치(l)	닫기(	(C)

3. 설치가 완료된 이후 Sparrow Enterprise 서버를 다시 시작하세요.

# ⑦ 분석을 실행한 후에 분석이 제대로 시작되었는지 확인하고 싶습니다.

분석이 정상적으로 수행 중인지를 확인하는 방법은 로그를 확인하는 것이 가장 정확합니다. 로그를 가장 간 단히 확인할 수 있는 방법은 다음과 같습니다.

웹 서버에서 분석 로그 다운로드하기

- 1. 프로젝트의 작업 이력에서 확인하려는 분석을 클릭하세요.
- 2. 그러면 해당 분석 슬라이드로 이동합니다.

🧐 s	parrow Enterprise				작업 0	(역		중 수시 분석 161	4				×
~	器 TestProject 🜑	) 상세 정보 🌑 🕄			Q	검색어를 두 글자	이상 입민	일반 정보	작업 메시지				
88	프로젝트 키 <u>TestProject</u> 🗋 🐳 런타임 에어	전트 javaAgent · 마지막분석 <u>24분전</u> .* · 방어 <u>3시간</u>	<u>8</u> 7			작업 ID 💲	유형	프로젝트			작업 프로파일		
*	진행 중인 작업의 결과에 따라 자신	이슈 또는 컴포넌트 정보가 변경될 수 있습니다.				1620	6	TestProject 진행 상황			모든 작업과 검출 소요시간	규직	
<u>000</u>						1614	6	⊘ 완료			10분 28초		
2	Q. 검색어를 입력하세요	88 프로젝트 홈				1613	0	분석 시작 일시 2024-06-04 10:44:	03		분석자 admin(Su	neradmin)	
Ð	B <mark>o</mark> 파일					1612	0	분석 대상			<b>U</b> uumin(ou	paradaminy	
ø	> E apache-maven-3.3.9.zip	1개의 예약된 작업이 있습니다.				1011		🐖 Enterprise.zip					
	> E aspnet/CheckerUnitTest     > E c-simple					1011	00	다 작업 프로파	일은 이전 작업	에 적용된 내용	을 표시하므로 현재 프로젝트 설정과	다를 수 있습니다.	
	> E C:\Testcode					1401	6						
	> 🗗 jsp	위험노멸 이슈 수				1280	6	⑦ 검출 규칙					
	> Co objc/parse_error			100 (1000)		1254	6						
	> Coscalal version.zip		비구 쇼송	5.3% (4.154)		1253	(	Q, 검색어를 두 글자	다이상 입력하/	<u>ଏ</u> ନ.	필터 🗸	10개씩 보기	~ 열편집 ~
	🍘 URL	중 이슈		<b>12.3%</b> (9.632)			-	SM ()	언어 1	위험도 :	규칙 이름 🛧		
	> 🚯 http://dastapp.fasoo.com:9090/W	78,618		9.5% (7,473)		1252	6		0				
			매우 낮음	71.7% (56,355)		1235	6	W TOLE	0.44		# 옥은 ## 인신사 사용		
	經 테스트 케이스					1230	6	🧼 소스코드	C++		#if 지시자 사용		
						1227	6	🐵 소스코드	C++	0.0	#pragma 지시자 사용		
		유형벽 이슈 수				11/1	0	😕 소스코드	C++		#undef 지시자 사용		
		<b>TO2 111 T</b>				1141	00		C++		* 및 & 도큰 규칙 위반		
						1139	6				A G T C I H H H C		
				<b>• • 4</b>		1138	0	🤣 소스코드	Java		+ 및 += 연산자로 더해진 문자열		
		•		9 2 9 2		1080	0	🤒 소스코드	C#		+ 연산에 사용된 빈 문자열		
		•		0 x		1079	0					<b>낙제하기</b> 로그 다운로드	보고서 내보내기

3. 아래쪽에 있는 로그 다운로드 버튼을 클릭하세요.

다운로드한 analysis-{분석ID}.log 파일을 열면 분석이 진행된 시간이 표시됩니다. 수행한 분석을 더 상세히 확인하시려면 해당 파일을 스패로우 엔지니어에게 전달해주세요.

Tip: 단, 자가 방어의 경우 분석 로그 다운로드 기능이 없습니다.

Sparrow Enterprise					작업 (	기력		0 자가 방어 1613					×
≈.	# TestProject CO	) 상세 정보 💽 🔅			٩	검색어를 두 글기	다 이상 입태	일반 정보	작업 메시기	q			
88	프로젝트 키 TestProject 🚺 🕤 런타임 에이	전드 없음 · 마지막분석 <u>2시간전</u> · · 방어 <u>5시간전</u> ■				작업 ID 💲	유형	프로젝트			작업 프로파일		
**	지행 중인 작업의 격과에 따라 자산	이슈 또는 컴포너트 정보가 변경될 수 있습니다.				1620	6	TestProject 지행 상황			모든 작업과 검출 ·	규직	
<u>000</u>						1614	6	O 중지			4시간 36분 12초		
22	Q, 검색어를 입력하세요	88 프로젝트 홈				1613	0	방어 시작 일시 2024-06-04 10:1	6:54		수행자 admin(Sup	eradmin)	
Ð	💫 मध					1612	0						
8	> Co apache-maven-3.3.9.zip	1개의 예약된 작업이 있습니다.				1611	0	🕛 작업 프로	파일은 이전 작업	겁에 적용된 내용	응을 표시하므로 현재 프로젝트 설정과	가를 수 있습니다.	
	Construction of the second secon	•					•	① 거추 그 치					
	> E C:\Testcode					1401	6	① 김물규역					
	> Eğ jsp	위험도널 이슈 수				1280	6	Q. 검색어를 두	글자 이상 입력히	네요.	필터 🗸	10개씩 보기 🗸	열편집 🗸
	Co objc/parse_error     Co sca.all.version.zip		••••• 매우 높음	<b>1.3%</b> (1,004)		1254	6						
			1111 <del>높</del> 음	<b>5.3%</b> (4,154)		1253	6	유형 💲	언어 💲	위험도 💲	규칙 이름 🔨		
	😜 URL	<sup>書 9</sup> 位 78 618	1111 보통	<b>12.3%</b> (9,632)		1252	6	③ 자가 방어	Java		LDAP 삽입		
	http://dastapp.fasoo.com:9090/W	10,010	₩!!! 낮음	<b>9.5%</b> (7,473)		1235	C	🕕 자가 방어	Java		SQL 삽입		
	狂 테스트 케이스		매우 낮음	<b>71.7%</b> (56,355)				🕕 자가 방어	JS		SQL 삽입		
						1230	(G	③ 자가 방어	Java		XPath 삽입		
						1227	6	③ 자가 방어	C#		개별 주소 노출		
		유형별 이슈 수				1141	6	<ul> <li>T121 HIQ1</li> </ul>	Inun		10		
						1139	6	🕔 사가 방어	Java		개별 주소 노물		
				<b>•••</b>		1138	œ	③ 자가 방어	Java		검증되지 않은 리다이렉션		
				<b>₩</b> 2		1080	Ø	🕕 자가 방어	Java		경로 조작		
				0 X		1079	0						
						10/9							모고시 내모내기

## 클라이언트 CLI에서 분석 로그 다운로드하기

Sparrow Enterprise 클라이언트 CLI에서 분석 로그를 다운로드하려면 다음을 수행하세요.

- 1. 명령 프롬프트를 실행하세요.
- 2. {Sparrow Enterprise 클라이언트 설치 디렉토리}로 이동하세요.
- 3. Linux 환경에서는 sparrow-cli 파일과 log analysis 명령어 및 옵션을 입력하세요.

./sparrow-cli log analysis -i 45 -o filename -s https://localhost:10880 -u
admin -p /home/user/workspace/password.txt

4. Windows 환경에서는 sparrow-cli.cmd 파일과 log analysis 명령어 및 옵션을 입력하세요.

sparrow-cli.cmd log analysis -i 45 -o filename -s https://localhost:10880 -u
admin -p C:\workspace\password.txt

5. 아래 내용을 참고하여 옵션을 입력하고 실행하세요.(\*는 필수 입력 항목)

#### -i 또는 --id\*

로그를 다운로드할 작업의 고유한 ID입니다.(예시: -i {작업 ID})

## -o 또는 --out\*

다운로드할 로그의 파일 이름입니다.(예시: -o {파일 이름})

### -s 또는 --server\*

연결하려는 Sparrow Enterprise 서버의 IP 주소 및 포트 번호입니다.(예시: -s {Sparrow Enterprise 서 버 IP 주소}:{포트 번호})

#### -u 또는 -–user\*

분석 로그를 다운로드하려는 사용자 계정의 ID입니다.(예시: -u {사용자 ID})

#### -p 또는 ---password

분석을 수행하려는 사용자 계정의 비밀번호를 저장한 txt 파일의 위치입니다. 이 옵션에 값을 입력하지 않은 경우 사용자 계정의 비밀번호를 입력하라는 메시지가 추가로 표시되며 해당 메시지에 비밀번호를 입력하면 됩니다.(예시: -p {txt 파일 경로})

# ② 사이드 바에 있는 네 번째 아이콘은 어떤 용도인지 궁금합니다.

사이드 바에 있는 네 번째 아이콘은 **통계** 아이콘입니다. 여기서는 Sparrow Enterprise에서 분석한 데이터를 **프로젝트별** 혹은 **분석자별**로 나누어 확인할 수 있습니다.

각각의 화면에서 **프로젝트 혹은 분석자**, **분석 완료 기간**, **포함할 분석** 및 **기타 조회 기준**을 선택한 다음 **조회 하기** 버튼을 클릭하면 해당하는 데이터가 테이블로 표시됩니다.

: 📎	Sparrow Enterprise » 통계								Ĺ,	admin 🗸
4 ::: 89 🛃 13 🔞 49	동계 대이지 <b>보드레스템</b> 분석가별	프로젝트별 통계 데이터 조회 프로젝트 [TestProject x _ @ain-sca x _ TestProje 보석 72 	기준 1/stoode x ] 코든 기간에 대해서 데이터를 초회합니다.						<u>赤</u> 기되	> = = = = =
		프로젝트별 통계 데이터 조회	결과					목록내	보내기 202	개씩 보기 🗸
		프로젝트 이름 个	완료 분석 수 🔹	컴포넌트 수 💲	총 이슈 💲	매우 높음 💲	높음 🗘	보통 💲	낮음 🗘	매우 낮음 💲
		TestProject	6	0	49,995+	986	4,154	9,621	7,473	9,999+
		TestProject_vscode	1	0	3,076	29	138	311	833	1,765
		dain-sca	4	19,193	23,332	2,205	56	544	9,999+	104
		전체 3 프로젝트 1 - 3 표시됨						1	페이지 아	5 →

# ⑦ Sparrow Enterprise에는 게시판 기능이 있는지 궁금합니다.

사이드 바에 있는 여섯 번째 아이콘을 클릭하면 게시판을 사용할 수 있습니다. 자세한 방법은 다음과 같습니 다.

158 / 160

제목\*

유형\*

작성할 글의 유형이며 시스템의 시스템 관리 권한이 있는 관리자는 일반, 공지사항 중에 하나를 선택할 수 있습니다. 공지사항으로 작성된 글은 게시글의 첫 페이지에 표시됩니다.(기본값: 일반)

작성한 글을 클릭하여 글 본문 아래에 답글을 올릴 수 있습니다.

4. 새 글 작성하기 버튼을 클릭하세요.

3. 아래를 참고하여 글의 유형, 제목, 본문을 입력하세요. (\*는 필수 입력 항목)

Sparrow Enterprise	새 글 작성하기	×
· · · · · · · · · · · · · · · · · · ·	유청 * 이바	
88	제목 *	
*	제목을 입력하세요.	
	본문 *	
2. Contraction of the second	B I & m = Ø 19 Ø () = m = m = m	26   21 <u>x</u> 12
	본문을 압력하세요.	
	철부 파일	
	🚺 하나 이상의 I	i일 여기로 끌어오기
	9	e -
	1192 S	to1587
		취소하기 세 금 작성하기

2. 새 글 작성하기 버튼을 클릭하세요.

💱 Spa	arrow Enterprise Q admin V
æ	및 검색어플 입력하세요         최근 등록손         >         20개택보기         >
88	
ŵ	
000	
22	
R	
~	
	새로운 게시글을 작성하세요.
	아직 작성된 게시쿄에 없습니다. 새로운 게시글을 작성하고 사람들과 다양한 의견을 나누어 보세요!
	사용 학생하기

1. 사이드 바에서 게시판 아이콘을 클릭하세요.

작성할 글의 제목이며 100자 이하의 모든 문자를 입력할 수 있습니다.

#### 본문\*

작성할 글의 본문이며 마크다운 형식으로 5,000자까지 입력할 수 있습니다.

#### 첨부 파일

작성할 글에 첨부하려는 파일이며 최대 5개의 파일을 업로드할 수 있습니다. 파일의 크기는 개당 1,000MB 이하여야 합니다.

# 고객센터

추가적으로 Sparrow Enterprise에 대해 궁금하신 점이나 필요한 정보가 있으신 경우 **스패로우 고객센터**로 문의해주세요.

# 법적 고지

본 문서는 ㈜스패로우에서 제공하는 Sparrow Enterprise 사용 방법 및 서비스 사용과 관련된 제반 사항을 설 명한 문서입니다. 본 문서의 내용과 프로그램은 저작권법의 보호를 받습니다. 본 문서와 본 문서에 설명된 프로그램은 ㈜스패로우와의 사용권 계약 하에서만 사용할 수 있습니다. ㈜스패로우의 사전 서면 동의 없이 본 문서의 전체 또는 일부분을 전자, 기계, 녹음 등의 수단을 사용하여 전송, 복제, 배포하거나 2차적 저작물 을 작성할 수 없습니다. 본 문서에 포함된 내용은 추후 제품의 기능 개선 등에 따라 사전 예고 없이 변경될 수 있습니다. 본 제품은 설치 CD와 가이드로 구성됩니다. 본 제품의 품질보증기간은 제품 구입일로부터 1년 이며 이후 별도 계약을 통해 품질을 유지 보수할 수 있습니다.

Microsoft, MS, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10은 Microsoft의 등록 상표 입니다.

© 2024. Sparrow Co., Ltd. all rights reserved.

# 주식회사 스패로우

- 대표 전화 02-6263-7400
- **팩스** 02-6263-7410
- 이메일 sales@sparrow.im
- 홈페이지 https://sparrow.im
- 주소 서울시 마포구 월드컵북로 396 누리꿈스퀘어 비즈니스타워 13층