Semgrep SAST Scan Report for Repository: Semgrep-Demo/pro-engine-demo

Report Generated at 2024-09-04 21:52

SAST Scan Summary

Vulnerability Severity	Vulnerability Count
Findings- SAST High Severity	9
Findings- SAST Medium Severity	18
Findings- SAST Low Severity	0

Findings Summary- High Severity

Finding Title	Finding Description & Remediation	severity	status	ref	location
crlf-injection-logs-deepsemgrep	When data from an untrusted source is put into a logger and not neutralized correctly, an attacker could forge log entries or include malicious content.	high	open	main	src/main/java/hawk/api/jwt/JwtLog4jController.java#L24
tainted-sql-string	User data flows into this manually-constructed SQL string. User data can be safely inserted into SQL strings using prepared statements or an object-relational mapper (ORM). Manually-constructed SQL strings is a possible indicator of SQL injection, which could let an attacker steal or manipulate data from the database. Instead, use prepared statements (`connection.PreparedStatement`) or a safe library.	high	open	main	src/main/java/hawk/service/UserSearchService.java#L30
detected-private-key	Private Key detected. This is a sensitive credential and should not be hardcoded here. Instead, store this in a separate, private file.	high	open	main	src/main/resources/keyStore.pem#L5
spring-actuator-fully-enabled	Spring Boot Actuator is fully enabled. This exposes sensitive endpoints such as /actuator/env, /actuator/logfile, /actuator/heapdump and others. Unless you have Spring Security enabled or another means to protect these endpoints, this functionality is available without authentication, causing a significant security risk.	high	open	main	src/main/resources/application-postgresql.properties#L36
crlf-injection-logs-deepsemgrep	When data from an untrusted source is put into a logger and not neutralized correctly, an attacker could forge log entries or include malicious content.	high	open	refs/pull/5/merge	src/assistant-fix-custom-message.java#L14
crlf-injection-logs-	When data from an untrusted source is put into a logger and not neutralized correctly, an attacker could	high	open		src/assistant-fix-custom-message.java#L14

Finding Title	Finding Description & Remediation	severity	status	ref	location
deepsemgrep-javaorg-copy	forge log entries or include malicious content. Please use the Jsoup.clean() function to sanitize data.			refs/pull/5/merge	
tainted-sql-string	Detected user input used to manually construct a SQL string. This is usually bad practice because manual construction could accidentally result in a SQL injection. An attacker could use a SQL injection to steal or modify contents of the database. Instead, use a parameterized query which is available by default in most database engines. Alternatively, consider using an object-relational mapper (ORM) such as Sequelize which will protect your queries.	high	open	refs/pull/4/merge	src/assistant-fix-sqli-sequelize.ts#L5
express-sequelize-injection	Detected a sequelize statement that is tainted by user-input. This could lead to SQL injection if the variable is user-controlled and is not properly sanitized. In order to prevent SQL injection, it is recommended to use parameterized queries or prepared statements.	high	open	refs/pull/4/merge	src/assistant-fix-sqli-sequelize.ts#L5
crlf-injection-logs-deepsemgrep-javaorg-copy	When data from an untrusted source is put into a logger and not neutralized correctly, an attacker could forge log entries or include malicious content. Please use the Jsoup.clean() function to sanitize data.	high	open	main	src/main/java/hawk/api/jwt/JwtLog4jController.java#L24

Findings Summary- Medium Severity

Finding Title	Finding Description & Remediation	severity	status	ref	location
cookie-missing-httponly	A cookie was detected without setting the 'HttpOnly' flag. The 'HttpOnly' flag for cookies instructs the browser to forbid client-side scripts from reading the cookie. Set the 'HttpOnly' flag by calling 'cookie.setHttpOnly(true);'	medium	open	main	src/main/java/hawk/controller/LoginController.java#L57
cookie-missing-secure-flag	A cookie was detected without setting the 'secure' flag. The 'secure' flag for cookies prevents the client from transmitting the cookie over insecure channels such as HTTP. Set the 'secure' flag by calling 'new Cookie("XLOGINID", cookieCode).setSecure(true);'	medium	open	main	src/main/java/hawk/controller/LoginController.java#L57
cookie-missing-httponly	A cookie was detected without setting the 'HttpOnly' flag. The 'HttpOnly' flag for cookies instructs the browser to forbid client-side scripts from reading the cookie. Set the 'HttpOnly' flag by calling 'cookie.setHttpOnly(true);'	medium	open	main	src/main/java/hawk/controller/LoginController.java#L57
cookie-missing-samesite	The application does not appear to verify inbound requests which can lead to a Cross-site request forgery (CSRF) vulnerability. If the application uses cookie-based authentication, an attacker can trick users into sending authenticated HTTP requests without their knowledge from any arbitrary domain they visit. To prevent this vulnerability start by identifying if the framework or library leveraged has built-in features or offers plugins for CSRF protection. CSRF tokens should be unique and securely random. The `Synchronizer Token` or `Double Submit Cookie` patterns with defense-in-	medium	open	main	src/main/java/hawk/controller/LoginController.java#L57

Finding Title	Finding Description & Remediation	severity	status	ref	location
	depth mechanisms such as the `sameSite` cookie flag can help prevent CSRF. For more information, see: [Cross-site request forgery prevention](https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html)				
cookie-missing-secure-flag	A cookie was detected without setting the 'secure' flag. The 'secure' flag for cookies prevents the client from transmitting the cookie over insecure channels such as HTTP. Set the 'secure' flag by calling 'new Cookie("XLOGINID", cookieCode).setSecure(true);'	medium	open	main	src/main/java/hawk/controller/LoginController.java#L57
spring-csrf-disabled	CSRF protection is disabled for this configuration. This is a security risk.	medium	open	main	src/main/java/hawk/MultiHttpSecurityConfig.java#L47
spring-csrf-disabled	CSRF protection is disabled for this configuration. This is a security risk.	medium	open	main	src/main/java/hawk/MultiHttpSecurityConfig.java#L88
spring-csrf-disabled	CSRF protection is disabled for this configuration. This is a security risk.	medium	open	main	src/main/java/hawk/MultiHttpSecurityConfig.java#L110
django-no-csrf-token	Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.	medium	open	main	src/main/resources/templates/general.html#L30
django-no-csrf-token	Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.	medium	open	main	src/main/resources/templates/login-form-multi.html#L15
django-no-csrf-token	Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.	medium	open	main	src/main/resources/templates/login.html#L15
		medium	open	main	

Finding Title	Finding Description & Remediation	severity	status	ref	location
django-no-csrf-token	Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.				src/main/resources/templates/search.html#L14
django-no-csrf-token	Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks.	medium	open	main	src/main/resources/templates/user-search.html#L14
no-new-privileges	Service 'db' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	medium	open	main	docker-compose.yml#L3
no-new-privileges	Service 'javavulny' allows for privilege escalation via setuid or setgid binaries. Add 'no-new-privileges:true' in 'security_opt' to prevent this.	medium	open	main	docker-compose.yml#L12
writable-filesystem-service	Service 'db' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to this service to prevent this.	medium	open	main	docker-compose.yml#L3
writable-filesystem-service	Service 'javavulny' is running with a writable root filesystem. This may allow malicious applications to download and run additional payloads, or modify container files. If an application inside a container has to save something temporarily consider using a tmpfs. Add 'read_only: true' to this service to prevent this.	medium	open	main	docker-compose.yml#L12
crlf-injection-logs	When data from an untrusted source is put into a logger and not neutralized correctly, an attacker could forge log entries or include malicious content.	medium	open	refs/pull/5/merge	src/assistant-fix-custom-message.java#L13

Findings Summary- Low Severity

Finding Title	Finding Description & Remediation	severity	status	ref	location