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

Report Generated at 2024-02-22 18:18

SAST Scan Summary

Vulnerability Severity	Vulnerability Count
Findings- SAST High Severity	8
Findings- SAST Medium Severity	36
Findings- SAST Low Severity	11

Findings Summary- HIGH Severity

Finding Title	Finding Description & Remediation	severity	state	ref	location
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	unresolved	refs/heads/main	src/main/java/hawk/service/UserSearchService.java#L30
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	fixed	refs/heads/main	src/main/java/hawk/service/UserSearchService.java#L30
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	unresolved	refs/heads/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	fixed	refs/heads/main	src/main/java/hawk/service/UserSearchService.java#L30
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	unresolved	refs/heads/main	src/main/java/hawk/api/jwt/JwtLog4jController.java#L24

Finding Title	Finding Description & Remediation	severity	state	ref	location
detected-generic-secret	Generic Secret detected	high	fixed	refs/heads/main	src/main/java/hawk/api/jwt/JwtTokenProvider.java#L21
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	unresolved	refs/heads/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	unresolved	refs/heads/main	src/main/resources/application-postgresql.properties#L36

Findings Summary- MEDIUM Severity

Finding Title	Finding Description & Remediation	severity	state	ref	location
django-no-csrf-token	Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks	medium	unresolved	refs/heads/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	unresolved	refs/heads/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	unresolved	refs/heads/main	src/main/resources/templates/login.html#L15
django-no-csrf-token	Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks	medium	unresolved	refs/heads/main	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	unresolved	refs/heads/main	src/main/resources/templates/user-search.html#L14
django-no-csrf-token	Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks	medium	fixed	refs/heads/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	fixed	refs/heads/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	fixed	refs/heads/main	src/main/resources/templates/login.html#L15
django-no-csrf-token	Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks	medium	fixed	refs/heads/main	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	fixed	refs/heads/main	src/main/resources/templates/user-search.html#L14
django-no-csrf-token	Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks	medium	fixed	refs/heads/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	fixed	refs/heads/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	fixed	refs/heads/main	src/main/resources/templates/login.html#L15
django-no-csrf-token	Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks	medium	fixed	refs/heads/main	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	fixed	refs/heads/main	src/main/resources/templates/user-search.html#L14

Finding Title	Finding Description & Remediation	severity	state	ref	location
django-no-csrf-token	Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks	medium	fixed	refs/heads/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	fixed	refs/heads/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	fixed	refs/heads/main	src/main/resources/templates/login.html#L15
django-no-csrf-token	Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks	medium	fixed	refs/heads/main	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	fixed	refs/heads/main	src/main/resources/templates/user-search.html#L14
third-party-action-not-pinned-to-commit-sha	An action sourced from a third-party repository on GitHub is not pinned to a full length commit SHA. Pinning an action to a full length commit SHA is currently the only way to use an action as an immutable release. Pinning to a particular SHA helps mitigate the risk of a bad actor adding a backdoor to the action's repository, as they would need to generate a SHA-1 collision for a valid Git object payload.	medium	unresolved	refs/heads/main	.github/workflows/hawkscan.yml#L23
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	unresolved	refs/heads/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-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)	medium	unresolved	refs/heads/main	src/main/java/hawk/controller/LoginController.java#L57

Finding Title	Finding Description & Remediation	severity	state	ref	location
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	unresolved	refs/heads/main	src/main/java/hawk/controller/LoginController.java#L57
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	unresolved	refs/heads/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	unresolved	refs/heads/main	docker-compose.yml#L12
jsch-hardcoded-secret	A secret is hard-coded in the application. Secrets stored in source code, such as credentials, identifiers, and other types of sensitive data, can be leaked and used by internal or external malicious actors. Use environment variables to securely provide credentials and other secrets or retrieve them from a secure vault or Hardware Security Module (HSM).	medium	unresolved	refs/pull/3/merge	src/main/java/hawk/api/vuln1.java#L19
jsch-hardcoded-secret	A secret is hard-coded in the application. Secrets stored in source code, such as credentials, identifiers, and other types of sensitive data, can be leaked and used by internal or external malicious actors. Use environment variables to securely provide credentials and other secrets or retrieve them from a secure vault or Hardware Security Module (HSM).	medium	unresolved	refs/pull/3/merge	src/main/java/hawk/api/vuln1.java#L23
spring-csrf-disabled	CSRF protection is disabled for this configuration. This is a security risk.	medium	unresolved	refs/heads/main	src/main/java/hawk/MultiHttpSecurityConfig.java#L47
spring-csrf-disabled	CSRF protection is disabled for this configuration. This is a security risk.	medium	unresolved	refs/heads/main	src/main/java/hawk/MultiHttpSecurityConfig.java#L88
spring-csrf-disabled	CSRF protection is disabled for this configuration. This is a security risk.	medium	unresolved	refs/heads/main	src/main/java/hawk/MultiHttpSecurityConfig.java#L110
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	fixed	refs/heads/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	fixed	refs/heads/main	docker-compose.yml#L12

Finding Title	Finding Description & Remediation	severity	state	ref	location
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	unresolved	refs/heads/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	unresolved	refs/heads/main	docker-compose.yml#L12
third-party-action-not-pinned-to-commit-sha	An action sourced from a third-party repository on GitHub is not pinned to a full length commit SHA. Pinning an action to a full length commit SHA is currently the only way to use an action as an immutable release. Pinning to a particular SHA helps mitigate the risk of a bad actor adding a backdoor to the action's repository, as they would need to generate a SHA-1 collision for a valid Git object payload.	medium	fixed	refs/heads/main	.github/workflows/hawkscan.yml#L23

Findings Summary- LOW Severity

Finding Title	Finding Description & Remediation	severity	state	ref	location
hashicorp-tf-password	A gitleaks hashicorp-tf-password was detected which attempts to identify hard-coded credentials. It is not recommended to store credentials in source-code, as this risks secrets being leaked and used by either an internal or external malicious adversary. It is recommended to use environment variables to securely provide credentials or retrieve credentials from a secure vault or HSM (Hardware Security Module).	low	unresolved	refs/heads/main	integration_tests/conf_files/stackhawk-jsv-json-token.yml#L20
hashicorp-tf-password	A gitleaks hashicorp-tf-password was detected which attempts to identify hard-coded credentials. It is not recommended to store credentials in source-code, as this risks secrets being leaked and used by either an internal or external malicious adversary. It is recommended to use environment variables to securely provide credentials or retrieve credentials from a secure vault or HSM (Hardware Security Module).	low	unresolved	refs/heads/main	stackhawk-actions.yml#L22
hashicorp-tf-password	A gitleaks hashicorp-tf-password was detected which attempts to identify hard-coded credentials. It is not recommended to store credentials in source-code, as this risks secrets being leaked and used by either an internal or external malicious adversary. It is recommended to use environment variables to securely provide credentials or retrieve credentials from a secure vault or HSM (Hardware Security Module).	low	unresolved	refs/heads/main	stackhawk.d/stackhawk-auth-form-cookie.yml#L14
hashicorp-tf-password	A gitleaks hashicorp-tf-password was detected which attempts to identify hard-coded credentials. It is not recommended to store credentials in source-code, as this risks secrets being leaked and used by either an internal or external malicious adversary. It is recommended to use environment variables to securely provide credentials or retrieve credentials from a secure vault or HSM (Hardware Security Module).	low	unresolved	refs/heads/main	stackhawk.d/stackhawk-auth-json-token.yml#L14

Finding Title	Finding Description & Remediation	severity	state	ref	location
hashicorp-tf-password	A gitleaks hashicorp-tf-password was detected which attempts to identify hard-coded credentials. It is not recommended to store credentials in source-code, as this risks secrets being leaked and used by either an internal or external malicious adversary. It is recommended to use environment variables to securely provide credentials or retrieve credentials from a secure vault or HSM (Hardware Security Module).	low	unresolved	refs/heads/main	stackhawk.d/stackhawk-custom-spider-curl.yml#L20
hashicorp-tf-password	A gitleaks hashicorp-tf-password was detected which attempts to identify hard-coded credentials. It is not recommended to store credentials in source-code, as this risks secrets being leaked and used by either an internal or external malicious adversary. It is recommended to use environment variables to securely provide credentials or retrieve credentials from a secure vault or HSM (Hardware Security Module).	low	unresolved	refs/heads/main	stackhawk.d/stackhawk-custom-spider-newman.yml#L20
hashicorp-tf-password	A gitleaks hashicorp-tf-password was detected which attempts to identify hard-coded credentials. It is not recommended to store credentials in source-code, as this risks secrets being leaked and used by either an internal or external malicious adversary. It is recommended to use environment variables to securely provide credentials or retrieve credentials from a secure vault or HSM (Hardware Security Module).	low	unresolved	refs/heads/main	stackhawk.d/stackhawk-jsv-form-cookie.yml#L22
hashicorp-tf-password	A gitleaks hashicorp-tf-password was detected which attempts to identify hard-coded credentials. It is not recommended to store credentials in source-code, as this risks secrets being leaked and used by either an internal or external malicious adversary. It is recommended to use environment variables to securely provide credentials or retrieve credentials from a secure vault or HSM (Hardware Security Module).	low	unresolved	refs/heads/main	stackhawk.d/stackhawk-jsv-json-token.yml#L19

Finding Title	Finding Description & Remediation	severity	state	ref	location
hashicorp-tf-password	A gitleaks hashicorp-tf-password was detected which attempts to identify hard-coded credentials. It is not recommended to store credentials in source-code, as this risks secrets being leaked and used by either an internal or external malicious adversary. It is recommended to use environment variables to securely provide credentials or retrieve credentials from a secure vault or HSM (Hardware Security Module).	low	unresolved	refs/heads/main	stackhawk.d/stackhawk-openapi.yml#L17
hashicorp-tf-password	A gitleaks hashicorp-tf-password was detected which attempts to identify hard-coded credentials. It is not recommended to store credentials in source-code, as this risks secrets being leaked and used by either an internal or external malicious adversary. It is recommended to use environment variables to securely provide credentials or retrieve credentials from a secure vault or HSM (Hardware Security Module).	low	unresolved	refs/heads/main	stackhawk.yml#L20
private-key	A gitleaks private-key was detected which attempts to identify hard-coded credentials. It is not recommended to store credentials in source-code, as this risks secrets being leaked and used by either an internal or external malicious adversary. It is recommended to use environment variables to securely provide credentials or retrieve credentials from a secure vault or HSM (Hardware Security Module).	low	unresolved	refs/heads/main	src/main/resources/keyStore.pem#L5