Semgrep

Semgrep SAST Scan Report for Repository: javaspringvulny

Report Generated at 2024-02-28 09:28

SAST Scan Summary

Vulnerability Severity	Vulnerability Count
Findings- SAST High Severity	2
Findings- SAST Medium Severity	18
Findings- SAST Low Severity	0

Findings Summary- HIGH Severity

Finding Title	Finding Description & Remediation	severity	state	ref	location
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/master	src/main/resources/keyStore.pem#L5
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/master	src/main/java/hawk/api/jwt/JwtLog4jController.java#L24

Findings Summary- MEDIUM Severity

Finding Title	Finding Description & Remediation	severity	state	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	unresolved	refs/heads/master	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	unresolved	refs/heads/master	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	unresolved	refs/heads/master	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/master	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	unresolved	refs/heads/master	src/main/java/hawk/controller/LoginController.java#L57
spring-csrf-disabled	CSRF protection is disabled for this configuration. This is a security risk.	medium	unresolved	refs/heads/master	src/main/java/hawk/MultiHttpSecurityConfig.java#L47

Finding Title	Finding Description & Remediation	severity	state	ref	location
spring-csrf-disabled	CSRF protection is disabled for this configuration. This is a security risk.	medium	unresolved	refs/heads/master	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/master	src/main/java/hawk/MultiHttpSecurityConfig.java#L110
spring-csrf-disabled	CSRF protection is disabled for this configuration. This is a security risk.	medium	unresolved	refs/heads/master	src/main/java/hawk/MultiHttpSecurityConfig.java#L181
django-no-csrf-token	Manually-created forms in django templates should specify a csrf_token to prevent CSRF attacks	medium	unresolved	refs/heads/master	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/master	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/master	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/master	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/master	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	unresolved	refs/heads/master	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/master	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	unresolved	refs/heads/master	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/master	docker-compose.yml#L12

Findings Summary- LOW Severity

Finding Title	Finding Description & Remediation	severity	state	ref	location