Semgrep SAST Scan Report for Repository: nnayar-r2c/new-vulnado

Report Generated at 2024-02-28 09:28

SAST Scan Summary

Vulnerability Severity	Vulnerability Count
Findings- SAST High Severity	7
Findings- SAST Medium Severity	25
Findings- SAST Low Severity	0

Findings Summary- HIGH Severity

Finding Title	Finding Description & Remediation	severity	state	ref	location
detected-jwt-token	JWT token detected	high	unresolved	master	exercises/02-xss.md#L65
command-injection-process-builder	A formatted or concatenated string was detected as input to a ProcessBuilder call. This is dangerous if a variable is controlled by user input and could result in a command injection. Ensure your variables are not controlled by users or sufficiently sanitized.	high	unresolved	master	src/main/java/com/scalesec/vulnado/Cowsay.java#L11
formatted-sql-string	Detected a formatted string in a SQL statement. This could lead to SQL injection if variables in the SQL statement are not properly sanitized. Use a prepared statements (java.sql.PreparedStatement) instead. You can obtain a PreparedStatement using 'connection.prepareStatement'.	high	unresolved	master	src/main/java/com/scalesec/vulnado/User.java#L49
var-in-script-tag	Detected a template variable used in a script tag. Although template variables are HTML escaped, HTML escaping does not always prevent cross-site scripting (XSS) attacks when used directly in JavaScript. If you need this data on the rendered page, consider placing it in the HTML portion (outside of a script tag). Alternatively, use a JavaScript-specific encoder, such as the one available in OWASP ESAPI. For Django, you may also consider using the 'json_script' template tag and retrieving the data in your script by using the element ID (e.g., `document.getElementById`).	high	unresolved	master	client/index.html#L63
var-in-script-tag	Detected a template variable used in a script tag. Although template variables are HTML escaped, HTML escaping does not always prevent cross-site scripting (XSS) attacks when used directly in JavaScript. If you need this data on the rendered page, consider placing it in the HTML portion (outside of a script tag). Alternatively, use a JavaScript-specific encoder, such as the one available in OWASP ESAPI. For Django, you may also consider using the 'json_script' template tag and retrieving the data in your script by using the element ID (e.g., `document.getElementById`).	high	unresolved	master	client/index.html#L67

Finding Title	Finding Description & Remediation	severity	state	ref	location
var-in-script-tag	Detected a template variable used in a script tag. Although template variables are HTML escaped, HTML escaping does not always prevent cross-site scripting (XSS) attacks when used directly in JavaScript. If you need this data on the rendered page, consider placing it in the HTML portion (outside of a script tag). Alternatively, use a JavaScript-specific encoder, such as the one available in OWASP ESAPI. For Django, you may also consider using the 'json_script' template tag and retrieving the data in your script by using the element ID (e.g., `document.getElementById`).	high	unresolved	master	client/index.html#L67
var-in-script-tag	Detected a template variable used in a script tag. Although template variables are HTML escaped, HTML escaping does not always prevent cross-site scripting (XSS) attacks when used directly in JavaScript. If you need this data on the rendered page, consider placing it in the HTML portion (outside of a script tag). Alternatively, use a JavaScript-specific encoder, such as the one available in OWASP ESAPI. For Django, you may also consider using the 'json_script' template tag and retrieving the data in your script by using the element ID (e.g., `document.getElementById`).	high	unresolved	master	client/index.html#L73

Findings Summary- MEDIUM Severity

Finding Title	Finding Description & Remediation	severity	state	ref	location
aws-subnet-has-public-ip-address	Resources in the AWS subnet are assigned a public IP address. Resources should not be exposed on the public internet, but should have access limited to consumers required for the function of your application. Set `map_public_ip_on_launch` to false so that resources are not publicly-accessible.	medium	unresolved	master	reverse_shell/main.tf#L33
var-in-script-tag	Detected a template variable used in a script tag. Although template variables are HTML escaped, HTML escaping does not always prevent cross-site scripting (XSS) attacks when used directly in JavaScript. If you need this data on the rendered page, consider placing it in the HTML portion (outside of a script tag). Alternatively, use a JavaScript-specific encoder, such as the one available in OWASP ESAPI. For Django, you may also consider using the 'json_script' template tag and retrieving the data in your script by using the element ID (e.g., `document.getElementById`).	medium	unresolved	master	client/index.html#L63
var-in-script-tag	Detected a template variable used in a script tag. Although template variables are HTML escaped, HTML escaping does not always prevent cross-site scripting (XSS) attacks when used directly in JavaScript. If you need this data on the rendered page, consider placing it in the HTML portion (outside of a script tag). Alternatively, use a JavaScript-specific encoder, such as the one available in OWASP ESAPI. For Django, you may also consider using the 'json_script' template tag and retrieving the data in your script by using the element ID (e.g., `document.getElementById`).	medium	unresolved	master	client/index.html#L67

Finding Title	Finding Description & Remediation	severity	state	ref	location
var-in-script-tag	Detected a template variable used in a script tag. Although template variables are HTML escaped, HTML escaping does not always prevent cross-site scripting (XSS) attacks when used directly in JavaScript. If you need this data on the rendered page, consider placing it in the HTML portion (outside of a script tag). Alternatively, use a JavaScript-specific encoder, such as the one available in OWASP ESAPI. For Django, you may also consider using the 'json_script' template tag and retrieving the data in your script by using the element ID (e.g., `document.getElementById`).	medium	unresolved	master	client/index.html#L67
var-in-script-tag	Detected a template variable used in a script tag. Although template variables are HTML escaped, HTML escaping does not always prevent cross-site scripting (XSS) attacks when used directly in JavaScript. If you need this data on the rendered page, consider placing it in the HTML portion (outside of a script tag). Alternatively, use a JavaScript-specific encoder, such as the one available in OWASP ESAPI. For Django, you may also consider using the 'json_script' template tag and retrieving the data in your script by using the element ID (e.g., `document.getElementById`).	medium	unresolved	master	client/index.html#L73
missing-integrity	This tag is missing an 'integrity' subresource integrity attribute. The 'integrity' attribute allows for the browser to verify that externally hosted files (for example from a CDN) are delivered without unexpected manipulation. Without this attribute, if an attacker can modify the externally hosted resource, this could lead to XSS and other types of attacks. To prevent this, include the base64-encoded cryptographic hash of the resource (file) youâ€™re telling the browser to fetch in the 'integrity' attribute for all externally hosted files.	medium	unresolved	master	client/index.html#L57

Finding Title	Finding Description & Remediation	severity	state	ref	location
missing-integrity	This tag is missing an 'integrity' subresource integrity attribute. The 'integrity' attribute allows for the browser to verify that externally hosted files (for example from a CDN) are delivered without unexpected manipulation. Without this attribute, if an attacker can modify the externally hosted resource, this could lead to XSS and other types of attacks. To prevent this, include the base64-encoded cryptographic hash of the resource (file) youâ€™re telling the browser to fetch in the 'integrity' attribute for all externally hosted files.	medium	unresolved	master	client/index.html#L60
missing-integrity	This tag is missing an 'integrity' subresource integrity attribute. The 'integrity' attribute allows for the browser to verify that externally hosted files (for example from a CDN) are delivered without unexpected manipulation. Without this attribute, if an attacker can modify the externally hosted resource, this could lead to XSS and other types of attacks. To prevent this, include the base64-encoded cryptographic hash of the resource (file) youâ€™re telling the browser to fetch in the 'integrity' attribute for all externally hosted files.	medium	unresolved	master	client/login.html#L40
missing-integrity	This tag is missing an 'integrity' subresource integrity attribute. The 'integrity' attribute allows for the browser to verify that externally hosted files (for example from a CDN) are delivered without unexpected manipulation. Without this attribute, if an attacker can modify the externally hosted resource, this could lead to XSS and other types of attacks. To prevent this, include the base64-encoded cryptographic hash of the resource (file) youâ€™re telling the browser to fetch in the 'integrity' attribute for all externally hosted files.	medium	unresolved	master	client/login.html#L43
active-debug-code-printstacktrace	Possible active debug code detected. Deploying an application with debug code can create unintended entry points or expose sensitive information.	medium	unresolved	master	src/main/java/com/scalesec/vulnado/Comment.java#L55

Finding Title	Finding Description & Remediation	severity	state	ref	location
active-debug-code-printstacktrace	Possible active debug code detected. Deploying an application with debug code can create unintended entry points or expose sensitive information.	medium	unresolved	master	src/main/java/com/scalesec/vulnado/Comment.java#L70
active-debug-code-printstacktrace	Possible active debug code detected. Deploying an application with debug code can create unintended entry points or expose sensitive information.	medium	unresolved	master	src/main/java/com/scalesec/vulnado/Cowsay.java#L24
active-debug-code-printstacktrace	Possible active debug code detected. Deploying an application with debug code can create unintended entry points or expose sensitive information.	medium	unresolved	master	src/main/java/com/scalesec/vulnado/Postgres.java#L25
active-debug-code-printstacktrace	Possible active debug code detected. Deploying an application with debug code can create unintended entry points or expose sensitive information.	medium	unresolved	master	src/main/java/com/scalesec/vulnado/Postgres.java#L100
active-debug-code-printstacktrace	Possible active debug code detected. Deploying an application with debug code can create unintended entry points or expose sensitive information.	medium	unresolved	master	src/main/java/com/scalesec/vulnado/Postgres.java#L114
active-debug-code-printstacktrace	Possible active debug code detected. Deploying an application with debug code can create unintended entry points or expose sensitive information.	medium	unresolved	master	src/main/java/com/scalesec/vulnado/User.java#L34
active-debug-code-printstacktrace	Possible active debug code detected. Deploying an application with debug code can create unintended entry points or expose sensitive information.	medium	unresolved	master	src/main/java/com/scalesec/vulnado/User.java#L58
use-of-md5	Detected MD5 hash algorithm which is considered insecure. MD5 is not collision resistant and is therefore not suitable as a cryptographic signature. Use HMAC instead.	medium	unresolved	master	src/main/java/com/scalesec/vulnado/Postgres.java#L67

Finding Title	Finding Description & Remediation	severity	state	ref	location
jdbc-sqli	Detected a formatted string in a SQL statement. This could lead to SQL injection if variables in the SQL statement are not properly sanitized. Use a prepared statements (java.sql.PreparedStatement) instead. You can obtain a PreparedStatement using 'connection.prepareStatement'.	medium	unresolved	master	src/main/java/com/scalesec/vulnado/User.java#L49
unrestricted-request-mapping	Detected a method annotated with 'RequestMapping' that does not specify the HTTP method. CSRF protections are not enabled for GET, HEAD, TRACE, or OPTIONS, and by default all HTTP methods are allowed when the HTTP method is not explicitly specified. This means that a method that performs state changes could be vulnerable to CSRF attacks. To mitigate, add the 'method' field and specify the HTTP method (such as 'RequestMethod.POST').	medium	unresolved	master	src/main/java/com/scalesec/vulnado/CowController.java#L11
unrestricted-request-mapping	Detected a method annotated with 'RequestMapping' that does not specify the HTTP method. CSRF protections are not enabled for GET, HEAD, TRACE, or OPTIONS, and by default all HTTP methods are allowed when the HTTP method is not explicitly specified. This means that a method that performs state changes could be vulnerable to CSRF attacks. To mitigate, add the 'method' field and specify the HTTP method (such as 'RequestMethod.POST').	medium	unresolved	master	src/main/java/com/scalesec/vulnado/LinksController.java#L15
unrestricted-request-mapping	Detected a method annotated with 'RequestMapping' that does not specify the HTTP method. CSRF protections are not enabled for GET, HEAD, TRACE, or OPTIONS, and by default all HTTP methods are allowed when the HTTP method is not explicitly specified. This means that a method that performs state changes could be vulnerable to CSRF attacks. To mitigate, add the 'method' field and specify the HTTP method (such as 'RequestMethod.POST').	medium	unresolved	master	src/main/java/com/scalesec/vulnado/LinksController.java#L19

Finding Title	Finding Description & Remediation	severity	state	ref	location
template-explicit-unescape	Detected an explicit unescape in a Mustache template, using triple braces '{{{...}}}' or ampersand '&'. If external data can reach these locations, your application is exposed to a cross-site scripting (XSS) vulnerability. If you must do this, ensure no external data can reach this location.	medium	unresolved	master	client/index.html#L73
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	master	docker-compose.yml#L23
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	master	docker-compose.yml#L23

Findings Summary- LOW Severity

Finding Title	Finding Description & Remediation	severity	state	ref	location