Semgrep SAST Scan Report for Repository: Semgrep-Demo/ JavaLog4J

Report Generated at 2024-09-04 21:52

SAST Scan Summary

Vulnerability Severity	Vulnerability Count
Findings- SAST High Severity	7
Findings- SAST Medium Severity	0
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	vulnerable-application/src/main/java/com/example/log4shell/LoginServlet.java#L34
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	vulnerable-application/src/main/java/com/example/log4shell/LoginServlet.java#L35
dangerous-subprocess-use-audit	Detected subprocess function 'run' without a static string. If this data can be controlled by a malicious actor, it may be an instance of command injection. Audit the use of this call to ensure it is not controllable by an external resource. You may consider using 'shlex.escape()'.	high	open	main	poc.py#L62
dangerous-subprocess-use-audit	Detected subprocess function 'call' without a static string. If this data can be controlled by a malicious actor, it may be an instance of command injection. Audit the use of this call to ensure it is not controllable by an external resource. You may consider using 'shlex.escape()'.	high	open	main	poc.py#L86
dangerous-subprocess-use-audit	Detected subprocess function 'run' without a static string. If this data can be controlled by a malicious actor, it may be an instance of command injection. Audit the use of this call to ensure it is not controllable by an external	high	open	main	poc.py#L98

Finding Title	Finding Description & Remediation	severity	status	ref	location
	resource. You may consider using 'shlex.escape()'.				
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	reviewing	main	vulnerable-application/src/main/java/com/example/log4shell/LoginServlet.java#L34
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	vulnerable-application/src/main/java/com/example/log4shell/LoginServlet.java#L35

Findings Summary- Medium Severity

Finding Title	Finding Description & Remediation	severity	status	ref	location

Findings Summary- Low Severity

Finding Title	Finding Description & Remediation	severity	status	ref	location