

Semgrep SAST Scan Report for Repository: leaky-repo

Report Generated at 2024-09-04 21:52

SAST Scan Summary

Vulnerability Severity	Vulnerability Count				
Findings- SAST High Severity	18				
Findings- SAST Medium Severity	5				
Findings- SAST Low Severity	0				

Findings Summary- High Severity

Finding Title	Finding Description & Remediation	severity	status	ref	location
detected-etc- shadow	linux shadow file detected	high	open	master	etc/shadow#L1
detected- bcrypt-hash	bcrypt hash detected	high	open	master	db/dump.sql#L32
detected- bcrypt-hash	bcrypt hash detected	high	open	master	db/dump.sql#L33
detected- bcrypt-hash	bcrypt hash detected	high	open	master	db/dump.sql#L34
detected- bcrypt-hash	bcrypt hash detected	high	open	master	db/dump.sql#L35
detected- bcrypt-hash	bcrypt hash detected	high	open	master	db/dump.sql#L36
detected- bcrypt-hash	bcrypt hash detected	high	open	master	db/dump.sql#L37
detected- bcrypt-hash	bcrypt hash detected	high	open	master	db/dump.sql#L38
detected- bcrypt-hash	bcrypt hash detected	high	open	master	db/dump.sql#L39
detected- bcrypt-hash	bcrypt hash detected	high	open	master	db/dump.sql#L40
	bcrypt hash detected	high	open	master	db/dump.sql#L41

Finding Title	Finding Description & Remediation	severity	status	ref	location
detected- bcrypt-hash					
detected-etc- shadow	linux shadow file detected	high	fixed	master	etc/shadow#L1
detected- generic-api- key	Generic API Key detected	high	open	master	.bashrc#L106
detected- generic-api- key	Generic API Key detected	high	open	master	cloud/.tugboat#L4
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	master	.ssh/id_rsa#L1
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	master	misc-keys/cert- key.pem#L1
detected-slack- token	Slack Token detected	high	open	master	.bash_profile#L23
dangerous- subprocess- use-audit	Detected subprocess function 'Popen' 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	master	.leaky-meta/ benchmark.py#L27

Findings Summary- Medium Severity

Finding Title	Finding Description & Remediation	severity	status	ref	location
unspecified- open-encoding	Missing 'encoding' parameter. 'open()' uses device locale encodings by default, corrupting files with special characters. Specify the encoding to ensure cross-platform support when opening files in text mode (e.g. encoding="utf-8").	medium	open	master	.leaky-meta/ benchmark.py#L16
unspecified- open-encoding	Missing 'encoding' parameter. 'open()' uses device locale encodings by default, corrupting files with special characters. Specify the encoding to ensure cross-platform support when opening files in text mode (e.g. encoding="utf-8").	medium	open	master	.leaky-meta/ benchmark.py#L45
unspecified- open-encoding	Missing 'encoding' parameter. 'open()' uses device locale encodings by default, corrupting files with special characters. Specify the encoding to ensure cross-platform support when opening files in text mode (e.g. encoding="utf-8").	medium	open	master	.leaky-meta/ benchmark.py#L161
unspecified- open-encoding	Missing 'encoding' parameter. 'open()' uses device locale encodings by default, corrupting files with special characters. Specify the encoding to ensure cross-platform support when opening files in text mode (e.g. encoding="utf-8").	medium	open	master	.leaky-meta/ benchmark.py#L163
unspecified- open-encoding	Missing 'encoding' parameter. 'open()' uses device locale encodings by default, corrupting files with special characters. Specify the encoding to ensure cross-platform support when opening files in text mode (e.g. encoding="utf-8").	medium	open	master	.leaky-meta/ benchmark.py#L165

Findings Summary- Low Severity