AccuKnox

Application Security Posture Management Report (ASPM)

Report Period **30 Days** - **Feb 12, 2025 12:00:00** to **Mar 12, 2025 12:00:00 (IST)**

Prepared for
Acme Corp

Prepared by
AccuKnox
support@accuknox.com

Report Summary

Across all application security scans - **SAST**, **DAST**, **SCA**, **Container Scanning**, and **Secret Scanning** - a total of **1.5k** security issues were identified. This includes **1,500 High**, **500 Medium**, and **100 Low** severity findings. The most significant concentration of high-risk issues was observed in **SAST** which requires immediate prioritisation for remediation.

Secret Scan Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**

Report Summary

The Secret scan revealed **6.5k** hardcoded or exposed secrets, classified into **5.2k High**, **2.5k Medium**, and **3k Low** severity across **20 repositories**. *http://lengtheri/design/wireframes* had the highest exposure with **6.28k findings**. These issues pose a critical risk of unauthorized access to sensitive systems if not addressed promptly.

Secret Scan Findings

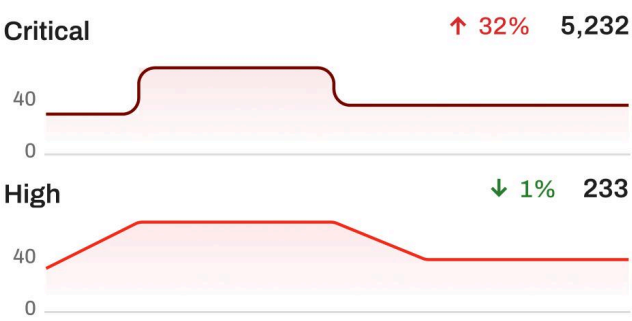
7
Critical Findings

198
High Findings

28
Medium Findings

2
Low Findings

Secret Exposure Trend



Highlights exposed credentials, tokens, and keys categorized by severity. It helps users prioritize and remediate high-risk secrets that could lead to unauthorized access or data breaches.

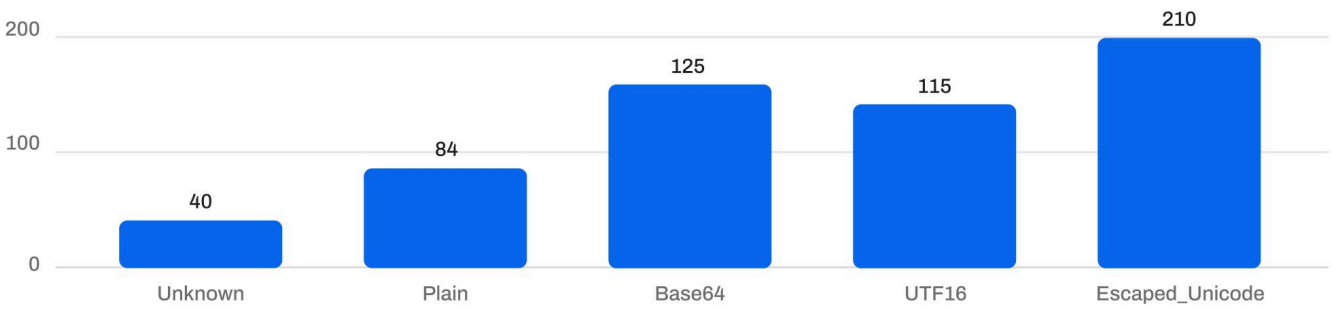
Shows how secret-related risks (like leaked API keys or credentials) change over time.

Top 5 Repositories with Secrets

Repository	Count	Verified	Unverified
lengtheri/design/mockups	120	20	100
lengtheri/design/wireframes	80	33	47
lengtheri/design/styleguide	75	5	70
gitlab.org/lengtheri-team/frontend/dashboard	30	21	9
bitbucket.org/lengtheri-team/design/ui-mockups	20	9	11

Lists the code repositories containing the highest number of exposed secrets. It helps security teams quickly identify high-risk projects that require immediate attention and policy enforcement.

Secrets by Decoder Type



Lists the code repositories containing the highest number of exposed secrets. It helps security teams quickly identify high-risk projects that require immediate attention and policy enforcement.

Secret Scan Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**

Secrets by Contributor

Name	Total
thomasknoll@mail.com	120
jones.nell@company.com	90
admin@mail.com	75
admin+username 9238498	12
admin+username 9238498	8

Highlights which developers or contributors have committed secrets into repositories.

Verified vs Unverified Secrets

Verified	35
Unverified	15

Compares the number of secrets confirmed as active (verified) against those that are unvalidated or inactive (unverified).

Verified Secrets Breakdown

AWS	100
Mockaroo	75
URI	20
Azure	5

Categorizes secrets that have been validated as active or exploitable, grouped by type (e.g., API keys, tokens, credentials) or source.

Secret Assets

Serverless	18.5k
Software	1.5k
Database	1.5k
Object Storage	500
Others	300

Gives users a clear view of how secret-related issues are being tracked and managed across teams.

Ticket Status

Created	30
To-Do	54
In Progress	25
Closed	10
Cancelled	25

Gives users a clear view of how secret-related issues are being tracked and managed across teams.

SAST Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**

Report Summary

The SAST scan revealed **6.5k** secrets, classified into **5.2k High**, **2.5k Medium**, and **3k Low** severity across multiple repositories. *http://lengtheri/design/wireframes* had the highest number of **6.28k findings**. These issues pose a critical risk of unauthorised access to sensitive systems if not addressed promptly.

SAST Findings

7
Critical Findings

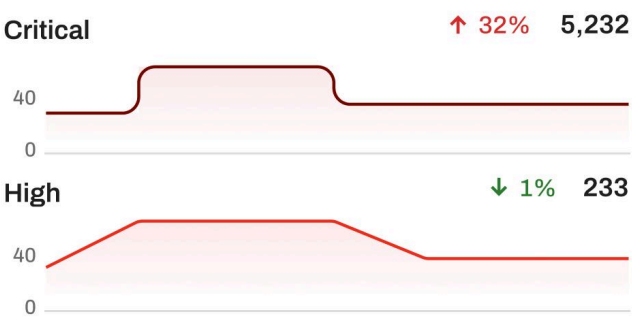
198
High Findings

28
Medium Findings

2
Low Findings

Highlights exposed credentials, tokens, and keys categorized by severity. It helps users prioritize and remediate high-risk secrets that could lead to unauthorized access or data breaches.

SAST Findings Trend



Shows how secret-related risks (like leaked API keys or credentials) change over time.

Top 10 SAST Findings

Finding	Severity	Findings
Client Hardcoded Domain	Critical	8
Stored XSS	Critical	98
SQL Injection	High	2,788
Parameter Tampering	Medium	23
Authentication Gaps & Bypass Risks	Low	2

Reflects common vulnerabilities in the code that can be automatically detected by SAST tools during development.

Top 10 SAST Findings by Count

Finding	Severity	Findings
SQL Injection	High	2,788
Stored XSS	Critical	98
Parameter Tampering	Medium	23
Client Hardcoded Domain	Critical	8
Authentication Gaps & Bypass Risks	Low	2

Widget ranks the most frequently detected security vulnerabilities during static application security testing (SAST), providing a clear overview of the most common issues in the codebase.

SAST Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**

SAST Findings by Types

Finding Type	Findings	Severity
Code Smell	120	20 C, 10 H, 60 M, 60 L
Bug	8	2 C, 1 H, 3 M, 2 L
Security Hotspot	10	7 C, 1 H, 1 M, 1 L
Vulnerability	8	8 C, 0 H, 0 M, 0 L

Security teams prioritize remediation by focusing on the most prevalent or severe vulnerability types within the codebase.

Top 5 SAST Findings by Security Category

Category	Severity	Findings
Auth	Critical	98
Insecure-Conf	Critical	8
Weak-cryptography	High	2,788
Encrypt-data	Medium	23
Dos	Low	2

Widget categorizes static application security testing results based on types of vulnerabilities, such as Injection, Access Control, Cryptographic Issues, and Data Protection.

Top 5 Most Vulnerable Files

File	Findings
aurora-client.yaml	120
main.tf	90
storageaccount.tf	75
main.tf	12
restore.tf	8

Highlights the specific files in the codebase that contain the highest number of critical security vulnerabilities.

OWASP Top 10 (2021) SAST

OWASP Risk	Name	Findings
A01:2021	Broken Access Control	10
A02:2021	Cryptographic Failures	12
A03:2021	Injection	22
A04:2021	Insecure Design	23
A05:2021	Security Misconfiguration	2

Widget highlights the most critical vulnerabilities found in code during static application security testing.

SAST Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**

Top 5 Vulnerable Code Repos

Repository	Findings				Severity
lengtheri/design/mockups	120	20 C	10 H	60 M	60 L
lengtheri/design/wireframes	80	2 C	1 H	3 M	2 L
lengtheri/design/styleguide	75	7 C	1 H	1 M	1 L
gitlab.org/lengtheri-team/frontend/dashboard	30	8 C	0 H	0 M	0 L
bitbucket.org/lengtheri-team/design/ui-mockups	30	8 C	0 H	0 M	0 L

Widget displays the repositories with the highest number of critical security vulnerabilities detected during static application security testing (SAST).

SAST Assets

Gives users a clear view of how secret-related issues are being tracked and managed across teams.

Ticket Status

Gives users a clear view of how secret-related issues are being tracked and managed across teams.

DAST Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**

Report Summary

The DAST scan uncovered **4.5k runtime vulnerabilities**, with **900 High**, **500 Medium**, and **3.1k Low** severity findings across 45 applications. **Serverless** was the most impacted, accounting for **900 issues**. These findings may indicate real-time threats such as exposed endpoints, authentication bypasses, or injection vulnerabilities.

DAST Findings

7
Critical Findings

198
High Findings

28
Medium Findings

2
Low Findings

Highlights exposed credentials, tokens, and keys categorized by severity. It helps users prioritize and remediate high-risk secrets that could lead to unauthorized access or data breaches.

DAST Findings Trend

Shows how secret-related risks (like leaked API keys or credentials) change over time.

Top 10 DAST Findings

Finding	Severity	Assets
Public Buckets Access	Critical	120
Publicly Available Database	Critical	8
Access Keys Older than 180 Days	High	10
Misconfigured Identity and Access Management (IAM)...	Medium	8
All/Custom Ports Publicly Available	Low	88

Lists the code repositories containing the highest number of exposed secrets. It helps security teams quickly identify high-risk projects that require immediate attention and policy enforcement.

Top 10 DAST Findings by Count

Finding	Severity	Findings
SQL Injection	High	2,788
Stored XSS	Critical	98
Parameter Tampering	Medium	23
Client Hardcoded Domain	Critical	8
Authentication Gaps & Bypass Risks	Low	2

Widget showcases the most prevalent security vulnerabilities discovered during dynamic application scans.

DAST Findings

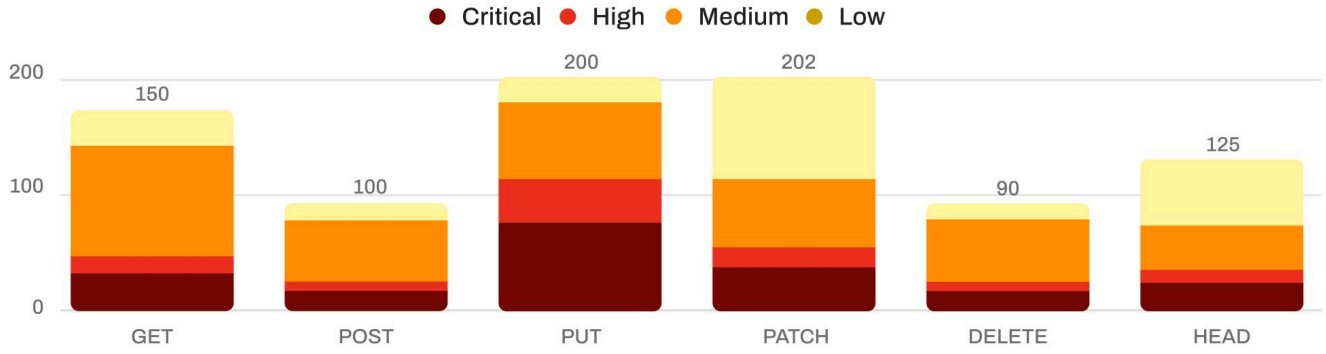
Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**

Top 10 Vulnerable Endpoints

Endpoint	Count				Severity
https://api.lengtheri.com/v1/auth/login	120	20 C	10 H	60 M	60 L
https://api.lengtheri.com/v1/users/12345/profile	8	2 C	1 H	3 M	2 L
https://api.lengtheri.com/v1/documents/7890/download	10	7 C	1 H	1 M	1 L
https://api.lengtheri.com/v1/comments	8	8 C	0 H	0 M	0 L
https://api.lengtheri.com/v1/comments	8	8 C	0 H	0 M	0 L

Widget lists the most frequently affected API or web endpoints identified during dynamic scans.

High Risk Endpoints by HTTP Methods



Helps teams understand which request types are most frequently associated with high-risk findings and prioritize securing those methods accordingly.

OWASP Top 10 (2021) DAST

OWASP Risk	Name	Findings
A01:2021	Broken Access Control	10
A02:2021	Cryptographic Failures	12
A03:2021	Injection	22
A04:2021	Insecure Design	23
A05:2021	Security Misconfiguration	2

Helps users understand which vulnerabilities can be effectively discovered during runtime scanning and where additional security measures may be required.

DAST Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**

Top Vulnerable Domains

Domain	Count				Severity
https://testaspnet.vuln.web.com	120	20 C	10 H	60 M	60 L
https://dummy.com	8	2 C	1 H	3 M	2 L
https://www.wikipedia.org	10	7 C	1 H	1 M	1 L
https://astoria.apikeys.com	8	8 C	0 H	0 M	0 L
https://vulnmgt.com	8	8 C	0 H	0 M	0 L

Displays the top domains with the highest count of vulnerabilities, categorized by severity levels.

DAST Assets

Serverless	18.5k
Software	1.5k
Database	1.5k
Object Storage	500
Others	300

Gives users a clear view of how secret-related issues are being tracked and managed across teams.

Ticket Status

Created	30
To-Do	54
In Progress	25
Closed	10
Cancelled	25

Gives users a clear view of how secret-related issues are being tracked and managed across teams.

Container Image Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**

Report Summary

Container scanning detected **3.2k vulnerabilities** within **82 container images**, with **1.2k High**, **800 Medium**, and **2k Low** severity levels. The container image with the most issues was *frontend-app:latest*, contributing **1.2k findings**. These risks are commonly linked to outdated base images or misconfigured packages.

Container Image Findings

7
Critical Findings

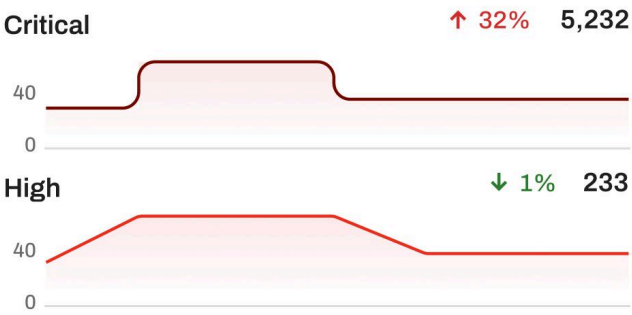
198
High Findings

28
Medium Findings

2
Low Findings

Highlights exposed credentials, tokens, and keys categorized by severity. It helps users prioritize and remediate high-risk secrets that could lead to unauthorized access or data breaches.

Container Image Findings Trend



Shows how secret-related risks (like leaked API keys or credentials) change over time.

Top Vulnerable Packages

Package	Findings					Severity
openssl 1.1.1w	100	50 C	75 H	15 M	10 L	
libcurl 7.87.0	350	250 C	50 H	25 M	25 L	
log4j-core 2.14.1	100	30 C	20 H	50 M	5 L	
express 4.18.2	1	1 C	0 H	0 M	0 L	
lodash 4.17.21	2	2 C	0 H	0 M	0 L	

Helps security teams identify and prioritize the most critical packages that need immediate updates or patches to prevent exploitation and strengthen the overall security of the application.

Top 25 CWEs

Rank	CWE ID	Name	Findings
1	CWE-79	Improper Neutralization of Input During Web Page Generation (Cross-site Scripting)	10
2	CWE-787	Out-of-bounds Write	12
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command (SQL Inje...	22
4	CWE-352	Cross-Site Request Forgery (CSRF)	23
5	CWE-22	Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)	2

Lists the code repositories containing the highest number of exposed secrets. It helps security teams quickly identify high-risk projects that require immediate attention and policy enforcement.

Container Image Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**

Top Insecure Registries

Registry	Findings					Severity
us-docker.pkg.dev/project-id/backend-service	100	50 C	75 H	15 M	10 L	
asia.gcr.io/test-env/ai-model-api	350	250 C	50 H	25 M	25 L	
europe-west2-docker.pkg.dev/org/security-tools	100	30 C	20 H	50 M	5 L	
gcr.io/lab-env/container-tools	1	1 C	0 H	0 M	0 L	
gcr.io/demo-env/container-tools	2	2 C	0 H	0 M	0 L	

Lists the code repositories containing the highest number of exposed secrets. It helps security teams quickly identify high-risk projects that require immediate attention and policy enforcement.

Top 20 CVEs' FIndings with CVSS Score vs Severity

CVE	Severity	CVSS Score	Count
CVE-2023-45853	Critical	10	8
CVE-2023-31484	Critical	9.8	5,540
CVE-2023-2953	High	9.8	2,788
CVE-2023-56171	Medium	8.1	23
CVE-2023-6345	Low	7	159

Lists the code repositories containing the highest number of exposed secrets. It helps security teams quickly identify high-risk projects that require immediate attention and policy enforcement.

Top 10 Container Images by Finding

Image	Findings
frontend-app:latest	450
backend-service:v1.4.2	200
auth-api:stable	105
nginx-proxy:v2.1	15
postgres-db:13.3-alpine	2

Widget ranks container images based on the number of security vulnerabilities or misconfigurations detected during scans.

Top CVEs by Severity and Affected Images

CVE ID	Severity	Images
CVE-2023-45853	Critical	100
CVE-2023-31484	Critical	70
CVE-2023-2953	High	30
CVE-2024-56171	Medium	23
CVE-2024-6345	Low	2

Ranks the most critical Common Vulnerabilities and Exposures (CVEs) based on their severity, along with the affected container images.

To view detailed data, visit dashboard

Container Image Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**

Top Container Images with Secrets

Image	Count
frontend-app:latest	100
backend-service:v1.4.2	70
auth-api:stable	30
nginx-proxy:v2.1	23
postgres-db:13.3-alpine	2

Identifies the container images that contain the highest number of exposed secrets, such as API keys, credentials, or tokens.

Image Findings by Fix Status

Fix Available	35
Fix Unavailable	15

Tracks the remediation status of container images containing vulnerabilities. It categorizes images as either Unavailable (fix not yet implemented or unavailable) or Available (fix or patch is available), helping teams prioritize and act on images that require immediate updates or secure configurations.

Image Assets

Serverless	18.5k
Software	1.5k
Database	1.5k
Object Storage	500
Others	300

Gives users a clear view of how secret-related issues are being tracked and managed across teams.

Ticket Status

Created	30
To-Do	54
In Progress	25
Closed	10
Cancelled	25

Gives users a clear view of how secret-related issues are being tracked and managed across teams.

IaC Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**

Report Summary

The Secret scan revealed **6.5k** hardcoded or exposed secrets, classified into **5.2k High**, **2.5k Medium**, and **3k Low** severity across **20 repositories**. *http://lengtheri/design/wireframes* had the highest exposure with **6.28k findings**. These issues pose a critical risk of unauthorized access to sensitive systems if not addressed promptly.

IaC Findings

7
Critical Findings

198
High Findings

28
Medium Findings

2
Low Findings

Highlights exposed credentials, tokens, and keys categorized by severity. It helps users prioritize and remediate high-risk secrets that could lead to unauthorized access or data breaches.

IaC Findings Trend

Shows how secret-related risks (like leaked API keys or credentials) change over time.

Top 10 IaC Findings

Finding	Severity	Assets
Public Buckets Access	Critical	120
Publicly Available Database	Critical	8
Access Keys Older than 180 Days	High	10
Misconfigured Identity and Access Management (IAM)...	Medium	8
All/Custom Ports Publicly Available	Low	88

Widget highlights the most critical vulnerabilities and misconfigurations found in Infrastructure as Code (IaC) files.

Top 10 IaC Findings by Count

Finding	Severity	Findings
SQL Injection	High	2,788
Stored XSS	Critical	98
Parameter Tampering	Medium	23
Client Hardcoded Domain	Critical	8
Authentication Gaps & Bypass Risks	Low	2

Widget ranks the most frequently occurring vulnerabilities and misconfigurations in Infrastructure as Code (IaC) files.

IaC Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**

Top 10 IaC Vulnerable Repo

Repository	Count				Severity
lengtheri-iac-insecure	120	20 C	10 H	60 M	60 L
iac-infra-v1-flawed	8	2 C	1 H	3 M	2 L
demo-iac-stack-unsecure	10	7 C	1 H	1 M	1 L
legacy-iac-configs	8	8 C	0 H	0 M	0 L
insecure-iac-bootstrap	8	8 C	0 H	0 M	0 L

Widget highlights the repositories containing the most critical vulnerabilities in infrastructure code.

IaC Files with Highest No of Findings

File	Findings
aurora-client.yaml	120
main.tf	90
storageaccount.tf	75
main.tf	12
restore.tf	8

Widget highlights the specific Infrastructure as Code (IaC) files that contain the most security vulnerabilities

IaC Findings by Framework

Framework	Findings
Terraform	120
Terraform Plan	90
Terraform JSON	75
Helm	12
Dockerfile	8

Widget categorizes security vulnerabilities based on the IaC framework used, such as Terraform, CloudFormation, Kubernetes, Ansible, and Pulumi.

Vulnerable Repos by Source

Github	150
Gitlab	35
Bitbucket	10
Others	5

Widget categorizes repositories based on the source where vulnerabilities were discovered, such as GitHub, GitLab, Bitbucket

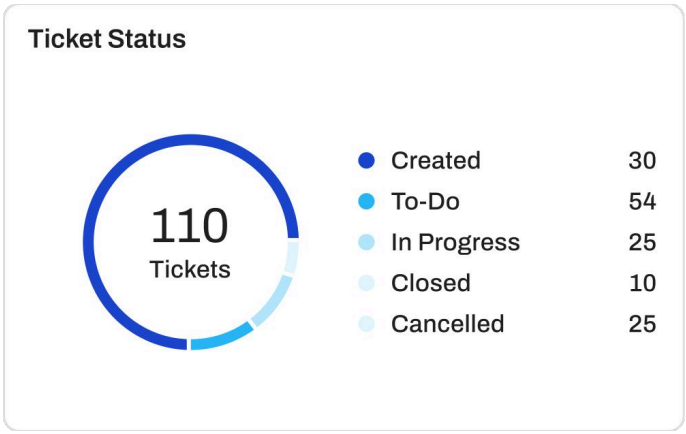
IaC Assets

Serverless	18.5k
Software	1.5k
Database	1.5k
Object Storage	500
Others	300

Gives users a clear view of how secret-related issues are being tracked and managed across teams.

IaC Findings

Feb 12, 2025 12:00:00
to **Mar 12, 2025 12:00:00**



Gives users a clear view of how secret-related issues are being tracked and managed across teams.

ⓘ **Note**: Log in to access data across all widgets.