DevOps Shack

100 Real Time DevOps Security Errors, Solutions and Root Cause Analysis

Trivy Errors

1. **Error:** `FATAL: unable to authenticate to Docker Hub`
   - **Cause**: Docker Hub authentication credentials are not provided or expired.
   - **Solution**: Log in to Docker Hub using `docker login`.
   - **RCA**: Trivy requires Docker Hub authentication for private images.

2. **Error**: `Error: failed to scan image: timeout while fetching layers`
   - **Cause**: Network latency or connectivity issues.
   - **Solution**: Increase the scan timeout using `--timeout` flag.
   - **RCA**: Slow network connections or server-side delays.

3. **Error**: `Failed to scan image: unsupported media type`
   - **Cause**: The image format is not supported by Trivy.
   - **Solution**: Use `docker save` to convert the image into a supported tar format.
   - **RCA**: Trivy works only with specific media types (e.g., Docker layers).

4. **Error**: `Trivy scan results show "UNKNOWN" severity`
   - **Cause**: Missing or outdated vulnerability database.
   - **Solution**: Update the database using `trivy --update`.
   - **RCA**: Trivy relies on an up-to-date database for accurate vulnerability severity classification.

5. **Error**: `Error: insufficient permissions to scan directories`
    - **Cause**: Lack of read permissions for files or directories.
    - **Solution**: Ensure the user running Trivy has sufficient file permissions.
    - **RCA**: Scanning restricted files without proper permissions results in errors.

OWASP ZAP Errors

6. **Error**: `ZAP unable to start proxy server`
    - **Cause**: Port conflict with another service using the same proxy port.
    - **Solution**: Change the proxy port in ZAP settings.
    - **RCA**: Default port (8080) is often used by other services.

7. **Error**: `ZAP crashes during large-scale scan`
    - **Cause**: Insufficient memory allocated to the JVM.
    - **Solution:** Increase JVM heap size.
    - **RCA**: Large scans consume significant memory.

8. **Error**: `ZapProxy Timeout on Selenium Integration`
    - **Cause**: Selenium WebDriver fails to communicate with ZAP proxy.
    - **Solution**: Increase the timeout in WebDriver settings.
    - **RCA**: Slow network conditions or misconfigured proxy settings disrupt communication.

9. **Error**: `Active scan hangs at 0% progress`
    - **Cause**: Server-side protections blocking ZAP's requests.
    - **Solution**: Add headers or user-agent strings to mimic legitimate traffic.
    - **RCA**: Web servers identify and block ZAP traffic as potentially malicious.

10. Error: `ZAP reports incorrect vulnerabilities`
    - Cause: False positives due to misconfigured contexts or baselines.
    - Solution: Adjust scan rules and verify results manually.
    - RCA: Misconfigured baselines may flag benign issues.

Prowler Errors

11. **Error**: `Access Denied on AWS API calls`
    - **Cause**: Insufficient IAM permissions.
    - **Solution**: Attach the `SecurityAudit` AWS managed policy.
    - **RCA**: Prowler needs extensive permissions to perform checks.

12. **Error**: `Check skipped: Missing AWS CLI or credentials`
    - **Cause**: AWS CLI is not installed or credentials are not configured.
    - **Solution**: Install AWS CLI and configure credentials using `aws configure`.
    - **RCA**: Prowler relies on AWS CLI to interact with AWS services.

13. **Error**: `Failed to execute check: invalid region`
    - **Cause**: AWS region is not valid or not specified.
    - **Solution**: Use `--region` to specify a valid region.
    - **RCA**: Incorrect region values lead to API errors.

14. **Error**: `S3 Bucket encryption check reports incorrect status`
    - **Cause**: Prowler uses cached data from AWS CLI.
    - **Solution**: Clear cache and re-run the check.
    - **RCA**: AWS CLI caching can return stale information.

15. **Error**: `Prowler scan takes too long`
    - **Cause**: Large AWS environments with numerous services.
    - **Solution**: Use `--check` to limit checks to specific services.
    - **RCA**: Checking all resources in large environments is time-consuming.

HashiCorp Vault Errors

16. **Error**: `Error initializing Vault: connection refused`
    - **Cause:** Vault service is not running or incorrectly configured.

- **Solution**: Start the Vault server and verify the configuration.
- **RCA**: Vault initialization requires a running service.

17. **Error**: `Permission denied for secret access`
    - **Cause**: The token does not have appropriate policies attached.
    - **Solution**: Update the policy using `vault policy write`.
    - **RCA**: Vault enforces strict access controls.

18. **Error**: `Vault unseal operation failed`
    - **Cause**: Incorrect unseal keys provided.
    - **Solution**: Use valid unseal keys generated during initialization.
    - **RCA**: Incorrect keys prevent access to Vault.

19. Error: `Unable to renew token: permission denied`
    - Cause: Token lacks `renew-self` capability.
    - Solution: Attach a policy with `renew-self` permissions.
    - RCA: Restricted token capabilities prevent renewal.

20. **Error**: `Audit logs not being generated`
    - **Cause**: Audit device not enabled or configured incorrectly.
    - **Solution**: Enable audit devices using `vault audit enable`.
    - **RCA**: Audit devices must be explicitly enabled in Vault.

OWASP ZAP Errors

21. **Error**: `API scan fails with "Invalid JSON Response"`
    - **Cause**: API endpoints return non-standard responses.
    - **Solution**: Validate and format JSON responses before scanning.
    - **RCA**: ZAP expects JSON-compliant data for API scans.

22. **Error**: `Unable to authenticate via API key`
    - **Cause**: Incorrect API key provided in ZAP configuration.
    - **Solution**: Update the API key in the ZAP settings.
    - **RCA**: API access requires matching keys for authentication.

23. **Error**: `Passive scan results are incomplete`
    - **Cause**: ZAP is not properly intercepting traffic.
    - **Solution**: Verify proxy settings and ensure traffic passes through ZAP.
    - **RCA**: Misconfigured proxies prevent passive scans.

Trivy Errors

24. **Error:** `Error parsing image manifest: unsupported schema version`

- **Cause:** Trivy encountered an image manifest with a schema version it does not support.
- **Solution:**
    1. Ensure the Docker image uses a supported schema (e.g., Schema 2).
    2. Rebuild the image using `docker build` and push it again to the registry.
- **RCA:** Trivy requires images to adhere to specific standards, and outdated or incompatible manifests result in parsing errors.

25. **Error:** `Cannot scan local files: no vulnerabilities detected, but warnings present`

- **Cause:** The directory being scanned lacks sufficient permissions, or critical libraries are missing.
- **Solution:**
    1. Run the scan as a user with read access to all files in the directory.
    2. Ensure that critical files such as `package.json` (for Node.js) or `requirements.txt` (for Python) exist.
- **RCA:** Trivy depends on specific metadata and library files to detect vulnerabilities in local projects. Missing files lead to incomplete scans.

26. **Error:** `Error fetching vulnerability database: failed to update database`

- **Cause:** Network restrictions or a failure in the Trivy update mechanism.
- **Solution:**
    1. Ensure you have internet access.
    2. Use a proxy by setting the `HTTP_PROXY` or `HTTPS_PROXY` environment variable if behind a firewall.
    3. Manually update the database with `trivy db update`.
- **RCA:** Trivy uses an online database to identify vulnerabilities. Network connectivity issues or proxy misconfigurations block access.

27. **Error:** `High CPU usage during Trivy scan`

- **Cause:** Trivy processes large Docker images or extensive file directories, consuming significant CPU resources.
- **Solution:**
    1. Limit resource usage with container tools like Docker's `--cpus` or `--memory` flags.
    2. Break down scans into smaller parts or exclude unnecessary directories.
- **RCA:** Trivy scans large files comprehensively, which can overwhelm system resources, especially on underpowered machines.

28. **Error:** `Empty results despite confirmed vulnerabilities`

- **Cause:** The vulnerability database is outdated or the wrong scan mode is used.
- **Solution:**
    1. Update the database using `trivy --update`.
    2. Use the correct scan mode, such as `trivy fs` for file systems or `trivy image` for Docker images.
- **RCA:** Incorrect configurations or database sync issues lead to incomplete or inaccurate results.

OWASP ZAP Errors

29. **Error:** `Authentication script not working`

- **Cause:** Incorrect scripting format or unsupported scripting language used for authentication scripts.
- **Solution:**
    1. Use ZAP's Script Console to debug the authentication script.
    2. Refer to ZAP documentation to use supported languages (e.g., JavaScript or Python).
- **RCA:** ZAP's authentication module depends on properly configured scripts. Errors in syntax or unsupported features cause authentication failures.

30. **Error:** `ZAP returns empty scan reports`

- **Cause:** Incorrect inclusion/exclusion rules or missing context configuration.
- **Solution:**
    1. Add proper inclusion rules to target the application domain.
    2. Ensure the target application is within ZAP's active scan context.
- **RCA:** ZAP scans only the URLs within its configured context. Misconfigurations lead to empty or incomplete reports.

31. **Error:** `ZAP proxy requests blocked by firewall`

- **Cause:** The target application or network has firewall rules blocking ZAP's IP or requests.
- **Solution:**
    1. Whitelist ZAP's IP address or configure the firewall to allow its requests.
    2. Use stealth techniques, such as modifying headers or using a different user-agent string.
- **RCA:** Security mechanisms often block automated scanners to prevent penetration testing.

32. **Error:** `Persistent XSS checks not detected during scan`

- **Cause:** ZAP is not configured to detect persistent vulnerabilities by default.
- **Solution:**
    1. Enable ZAP's advanced passive scan rules.
    2. Use ZAP extensions like "Retest Add-On" to enhance XSS detection.
- **RCA:** Persistent vulnerabilities require deeper inspection and tailored scan rules to detect effectively.

Prowler Errors

33. **Error:** `Multiple failed checks: "KMS keys are not rotated"`

- **Cause:** Customer-managed KMS keys have exceeded the recommended rotation period.
- **Solution:**
    1. Manually rotate KMS keys using the AWS Management Console or CLI.
    2. Set automatic rotation policies for future compliance.
- **RCA:** AWS recommends rotating KMS keys every 365 days. Failure to comply leads to non-compliance alerts in tools like Prowler.

34. **Error:** `Root user access detected`

- **Cause:** Root credentials have been used for AWS actions.
- **Solution:**
    1. Create and use IAM users with specific permissions.
    2. Lock down root user access and enable MFA (Multi-Factor Authentication).
- **RCA:** AWS advises against using the root account for day-to-day operations. Detection tools flag such usage as a security risk.

35. **Error:** `IAM policy with "FullAccess" found`

- **Cause:** Overly permissive policies attached to users or roles.
- **Solution:**
    1. Review and update the IAM policies to follow the principle of least privilege.

2. Replace `FullAccess` policies with more granular permissions.

- **RCA:** Overly broad permissions increase the attack surface, violating security best practices.

36. **Error:** `S3 bucket publicly accessible`

- **Cause:** Bucket policies or ACLs (Access Control Lists) allow public read/write access.
- **Solution:**
    1. Use the AWS S3 Block Public Access feature to restrict public access.
    2. Review and update bucket policies to ensure access is limited to required entities.
- **RCA:** Misconfigured bucket policies expose sensitive data, a common vulnerability in cloud environments.

37. **Error:** `Prowler reports "Unencrypted EBS volumes"`

- **Cause:** EBS volumes are created without specifying encryption.
- **Solution:**
    1. Enable encryption during volume creation or re-enable encryption for existing volumes.
    2. Use AWS Config rules to enforce encryption by default.
- **RCA:** AWS does not encrypt volumes by default unless explicitly configured, leading to compliance issues.

HashiCorp Vault Errors

38. **Error:** `Vault login failed: "invalid token"`

- **Cause:** The token used is expired or revoked.
- **Solution:**
    1. Generate a new token using a valid root or admin token.
    2. Configure a longer TTL for tokens that require extended usage.
- **RCA:** Vault tokens are time-sensitive and must be refreshed regularly.

39. **Error:** `Vault performance backend unreachable`

- **Cause:** The configured backend (e.g., Consul, DynamoDB) is not reachable due to network issues or misconfiguration.
- **Solution:**
    1. Verify the backend service's health and network connectivity.
    2. Update Vault's configuration with the correct backend address.
- **RCA:** Vault relies on external storage backends for persistence. Disruptions in these services affect Vault's performance.

40. **Error:** `TLS handshake failed`

- **Cause:** SSL/TLS certificates are invalid or misconfigured.
- **Solution:**
    1. Verify and replace expired or incorrect certificates.
    2. Use a valid CA-signed certificate or configure self-signed certificates correctly.
- **RCA:** Secure communication between Vault and clients depends on valid SSL/TLS configurations.

HashiCorp Vault Errors

41. **Error:** `Vault cluster nodes fail to join`

- **Cause:** Incorrect cluster configuration or network connectivity issues between nodes.
- **Solution:**
    1. Verify the `api_addr` and `cluster_addr` settings in the Vault configuration file.
    2. Ensure that all nodes can communicate over the specified ports (e.g., 8200 and 8201 by default).
- **RCA:** Vault uses specific addresses and ports for cluster communication. Misconfigurations or blocked ports prevent nodes from joining the cluster.

42. **Error:** `Vault high availability mode not working`

- **Cause:** Incorrect backend configuration for HA (e.g., Consul or DynamoDB not properly set up).
- **Solution:**
    1. Confirm that the storage backend supports high availability.
    2. Verify the backend health and network settings.
- **RCA:** HA in Vault depends on the storage backend's ability to manage leader elections and state synchronization.

43. **Error:** `Seal/Unseal keys lost`

- **Cause:** The original keys from the initialization process are not securely stored or have been misplaced.
- **Solution:**
    1. Restore the keys from a secure backup, if available.
    2. Reinitialize Vault and restore secrets if the keys cannot be recovered.
- **RCA:** Vault relies on these keys for secure access. Loss of these keys renders the Vault inaccessible.

44. **Error:** `Error: "max_lease_ttl exceeded"`

- **Cause:** A lease duration exceeds the maximum TTL configured for Vault.
- **Solution:**
    1. Update the `max_lease_ttl` configuration in Vault's settings.
    2. Ensure requested leases comply with the maximum allowed TTL.
- **RCA:** Lease TTL restrictions are set to enforce security policies. Requests exceeding these limits are rejected.

45. **Error:** `Error: "no route to backend"`

- **Cause:** The backend storage service is unavailable or unreachable.
- **Solution:**
    1. Restart the backend storage service (e.g., Consul, DynamoDB).
    2. Verify the network settings and DNS resolution for the backend's address.
- **RCA:** Vault depends on the backend storage for persistence. Backend downtime directly affects Vault's availability.

OWASP ZAP Errors

46. **Error:** `Unable to detect CSRF vulnerabilities`

- **Cause:** Anti-CSRF tokens or incorrect scanner configuration.
- **Solution:**
    1. Add the appropriate anti-CSRF token configuration in ZAP.
    2. Use ZAP's Anti-CSRF add-on to improve detection.
- **RCA:** Applications with CSRF protection mechanisms require specific configurations for ZAP to detect vulnerabilities effectively.

47. **Error:** `Scan results include duplicate vulnerabilities`

- **Cause:** Multiple similar endpoints or payloads return the same vulnerability.
- **Solution:**
    1. Consolidate the results manually or use deduplication scripts.
    2. Limit the scan scope to unique endpoints.
- **RCA:** ZAP scans every endpoint individually, which can result in duplicate findings for similar payloads.

48. **Error:** `AJAX Spider fails to discover all endpoints`

- **Cause:** Dynamic JavaScript rendering or client-side routing not handled by ZAP.
- **Solution:**
    1. Use ZAP's Headless Browser or Selenium integration for enhanced endpoint discovery.
    2. Enable debugging to identify skipped endpoints.
- **RCA:** AJAX-based applications rely heavily on client-side rendering, requiring advanced tools for full coverage.

49. **Error:** `Invalid SSL certificate error during scan`

- **Cause:** ZAP's self-signed certificate is not trusted by the browser or application.
- **Solution:**
    1. Import ZAP's certificate into the browser or application.

2. Use `zap.sh` to generate and trust a custom certificate.

- **RCA:** Applications require trusted certificates to accept HTTPS traffic. ZAP's default self-signed certificate is flagged as untrusted.

50. **Error:** `Scan results missing key vulnerabilities`

- **Cause:** Incorrect scan rule set or insufficient privileges to access endpoints.
- **Solution:**
    1. Enable all scan rules in the Scan Policy Manager.
    2. Ensure proper authentication is configured to access protected endpoints.
- **RCA:** Restricted endpoints or disabled scan rules can lead to incomplete vulnerability detection.

Prowler Errors

51. **Error:** `No MFA enabled for IAM users`

- **Cause:** IAM users are created without enabling MFA.
- **Solution:**
    1. Enable MFA for all IAM users via the AWS Management Console or CLI.
    2. Use a policy to enforce MFA requirements.
- **RCA:** MFA adds an extra layer of security for IAM users, and lack of it violates AWS best practices.

52. **Error:** `VPC Flow Logs not enabled`

- **Cause:** VPC Flow Logs are not configured for monitoring network traffic.
- **Solution:**
    1. Enable Flow Logs for all VPCs using the AWS Management Console or CLI.
    2. Store the logs in an S3 bucket or CloudWatch for analysis.
- **RCA:** VPC Flow Logs provide essential data for network monitoring and troubleshooting. Their absence leads to blind spots in security audits.

53. **Error:** `Unrestricted inbound traffic on security groups`

- **Cause:** Security groups allow unrestricted inbound traffic on critical ports (e.g., 22, 3389).
- **Solution:**
    1. Restrict inbound traffic to specific IPs or CIDR blocks.
    2. Use AWS Config rules to enforce stricter security group settings.
- **RCA:** Open ports increase the risk of unauthorized access and potential attacks.

54. **Error:** `CloudTrail not enabled in all regions`

- **Cause:** CloudTrail is not configured for logging activity in specific AWS regions.
- **Solution:**
    1. Enable CloudTrail in all AWS regions.
    2. Configure centralized logging for improved visibility.
- **RCA:** CloudTrail monitors API activity across regions. Disabling it leads to gaps in activity logs.

55. **Error:** `AWS Config rules non-compliant`

- **Cause:** Misconfigured or missing AWS Config rules for resource compliance.
- **Solution:**
    1. Review and correct non-compliant rules in AWS Config.
    2. Use Prowler's recommendations to implement compliant configurations.
- **RCA:** AWS Config enforces compliance. Misconfigured rules result in failed checks during audits.

Trivy Errors

56. **Error:** `Container image scan fails due to missing manifest.json`

- **Cause:** The image does not include a valid `manifest.json` file.
- **Solution:**
    1. Rebuild the Docker image to ensure it includes the manifest.
    2. Use `docker save` to create a tarball that includes all necessary metadata.

- **RCA:** Trivy requires `manifest.json` to understand image layers and dependencies.

57. **Error:** `Error: scan limit exceeded`
- **Cause:** Trivy exceeds the API rate limit of the Docker registry.
- **Solution:**
    1. Authenticate with Docker Hub using `docker login`.
    2. Increase API limits for enterprise-grade accounts if using a private registry.
- **RCA:** Trivy makes multiple API calls to retrieve image metadata, which can hit rate limits on free-tier accounts.

58. **Error:** `Outdated CVE information in scan results`
- **Cause:** Trivy's vulnerability database is not updated regularly.
- **Solution:** Run `trivy db update` before each scan to ensure up-to-date CVE data.
- **RCA:** Trivy relies on the latest CVE database to identify vulnerabilities accurately.

HashiCorp Vault Errors

59. **Error:** `Vault replication issues in performance standby mode`
- **Cause:** Network latency or misconfigured replication settings between primary and secondary Vault instances.
- **Solution:**
    1. Check the `primary_cluster_addr` and `cluster_addr` settings in the Vault configuration.
    2. Verify network connectivity and ensure required ports (e.g., 8201) are open.
- **RCA:** Replication in Vault requires low latency and properly synchronized configuration. Network interruptions or incorrect settings disrupt data synchronization.

60. **Error:** `Vault transit secret engine encryption failure`
- **Cause:** Missing encryption keys or invalid key settings in the transit engine.
- **Solution:**
    1. Ensure encryption keys are created and properly initialized using `vault write transit/keys/<key-name>`.
    2. Verify that the key name matches the one used during encryption operations.
- **RCA:** The transit engine relies on properly initialized keys for encryption/decryption. Missing or misconfigured keys result in failures.

61. **Error:** `Error: "invalid backend configuration"`
- **Cause:** Incorrect storage backend settings in the Vault configuration file.
- **Solution:**
    1. Review the backend block in the Vault configuration file.
    2. Correct any typos or missing parameters.
- **RCA:** Vault depends on correctly configured storage backends (e.g., Consul, DynamoDB). Misconfigurations prevent it from operating correctly.

62. **Error:** `Error enabling dynamic secrets: "plugin not found"`
- **Cause:** The specified plugin for dynamic secrets is not installed or registered.
- **Solution:**
    1. Verify that the plugin binary exists in the plugin directory.
    2. Register the plugin using `vault write sys/plugins/catalog/...`.
- **RCA:** Vault requires plugins to be registered and accessible. Missing or unregistered plugins prevent dynamic secret generation.

63. **Error:** `Vault failed to authenticate with Kubernetes`
- **Cause:** Incorrect Kubernetes service account configuration or missing JWT tokens.
- **Solution:**
    1. Verify the service account's role binding and ensure it has the necessary permissions.

2. Check the JWT token used for authentication.

- **RCA:** Vault uses Kubernetes tokens for authentication. Misconfigured service accounts or invalid tokens disrupt this process.

OWASP ZAP Errors

64. **Error:** `Active scan detects fewer vulnerabilities than expected`

- **Cause:** Default scan rules do not cover all potential vulnerabilities.
- **Solution:**
    1. Add additional scan rules or use third-party plugins to enhance ZAP's detection capabilities.
    2. Review the Scan Policy Manager to ensure all rules are enabled.
- **RCA:** The default ZAP configuration may not cover specialized or rare vulnerabilities.

65. **Error:** `Error while importing HAR file`

- **Cause:** HAR file is corrupted or generated in an unsupported format.
- **Solution:**
    1. Regenerate the HAR file using a supported browser or tool.
    2. Verify that the file adheres to the HAR specification.
- **RCA:** ZAP requires HAR files to conform to standards. Corruption or unsupported formats lead to import failures.

66. **Error:** `Context import failed: "Invalid configuration"`

- **Cause:** The imported context file contains incorrect or outdated settings.
- **Solution:**
    1. Export a fresh context from a working ZAP instance.
    2. Verify and correct any invalid parameters in the configuration file.
- **RCA:** Contexts store scan parameters and settings. Misconfigured contexts disrupt the scanning process.

67. **Error:** `ZAP's Fuzzer fails to test endpoints`
- **Cause:** Incorrect fuzz payloads or improperly configured attack settings.
- **Solution:**
    1. Use valid payloads and configure the fuzzer's settings for the target endpoint.
    2. Test with smaller payload sets to identify issues incrementally.
- **RCA:** Fuzzers depend on well-formed payloads to interact with endpoints effectively. Incorrect configurations cause failures.

68. **Error:** `Spidering fails to crawl certain pages`
- **Cause:** Pages are dynamically loaded via JavaScript or hidden behind authentication.
- **Solution:**
    1. Use ZAP's AJAX Spider for better coverage of JavaScript-heavy sites.
    2. Authenticate using ZAP's session management features before crawling.
- **RCA:** Traditional crawlers struggle with dynamic content, requiring advanced techniques to discover all pages.

69. **Error:** `Unrestricted outbound traffic detected`
- **Cause:** Security groups allow unrestricted outbound traffic.
- **Solution:**
    1. Restrict outbound traffic to specific IPs, CIDR blocks, or ports.
    2. Use AWS Config rules to enforce stricter security group policies.
- **RCA:** Unrestricted outbound traffic can be exploited by malicious actors to exfiltrate data.

70. **Error:** `Unused IAM roles detected`
- **Cause:** IAM roles have not been used in over 90 days.
- **Solution:**
    1. Identify unused roles using AWS IAM Access Analyzer.
    2. Delete or deactivate roles that are no longer needed.
- **RCA:** Unused IAM roles increase the attack surface and violate AWS best practices.

71. **Error:** `ECS task definition not encrypted`
- **Cause:** The ECS task definition does not specify encryption for sensitive environment variables.
- **Solution:**
    1. Use AWS KMS to encrypt sensitive variables in the task definition.
    2. Update the task definition and redeploy affected services.
- **RCA:** Unencrypted environment variables expose sensitive data to potential leaks.

72. **Error:** `RDS instance not using multi-AZ deployment`
- **Cause:** RDS instance is deployed in a single availability zone.
- **Solution:**
    1. Enable multi-AZ deployment for all critical databases.
    2. Configure backups and replication for high availability.
- **RCA:** Multi-AZ deployments ensure availability during outages. Single-zone setups are less resilient.

73. **Error:** `AWS Lambda function without logging enabled`
- **Cause:** The function does not have logging enabled via CloudWatch.
- **Solution:**
    1. Enable logging in the Lambda function's configuration.
    2. Use AWS Config to ensure all Lambda functions are compliant.
- **RCA:** Logging is critical for monitoring and debugging. Missing logs hinder operational visibility.

74. **Error:** `Scan excludes certain vulnerabilities`
- **Cause:** Default scanning policies exclude low-severity vulnerabilities.
- **Solution:**
    1. Use `--severity` to include low, medium, and high vulnerabilities in scans.
    2. Update the Trivy configuration file to include all severities.
- **RCA:** Default settings often exclude low-priority vulnerabilities to reduce noise.

75. **Error:** `Filesystem scan fails due to symbolic links`
- **Cause:** Trivy cannot resolve broken or recursive symbolic links.
- **Solution:**
    1. Identify and fix broken symbolic links in the scanned directory.
    2. Use the `--skip-dirs` option to exclude problematic directories.
- **RCA:** Symbolic link resolution is critical for file scans. Broken links disrupt the process.

76. **Error:** `Vault HTTP status 500: Internal Server Error`
- **Cause:** Misconfigured backend storage or server-side issue.
- **Solution:**
    1. Check Vault server logs for detailed error messages.
    2. Verify the backend storage configuration (e.g., Consul, DynamoDB) and its availability.
    3. Restart the Vault server after resolving backend issues.
- **RCA:** Vault depends on a stable backend storage system. Server-side issues like misconfiguration or storage unavailability cause internal errors.

77. **Error:** `Vault does not respond after leader election`
- **Cause:** The leader node is unable to communicate with standby nodes due to network issues or incorrect cluster settings.
- **Solution:**
    1. Check and correct `cluster_addr` and `api_addr` configurations.
    2. Ensure firewall rules allow cluster communication on required ports (8200 and 8201 by default).
- **RCA:** Leader election requires seamless communication among cluster nodes. Network disruptions or misconfigurations lead to failure.

78. **Error:** `Dynamic secrets are not rotated automatically`
- **Cause:** Rotation policies for dynamic secrets are not configured.
- **Solution:**
    1. Set up a lease with the desired TTL and auto-renewal for dynamic secrets.

2. Use `vault renew` for manual renewal if needed.

- **RCA:** Vault does not rotate secrets automatically unless explicitly configured. Dynamic secrets must adhere to lease policies.

79. **Error:** `Access denied to AWS secrets in Vault`

- **Cause:** IAM role or user does not have sufficient permissions in AWS.
- **Solution:**
  1. Update the IAM policy to include necessary permissions (e.g., `secretsmanager:GetSecretValue`).
  2. Reauthenticate Vault with AWS using a role with the correct permissions.
- **RCA:** Vault integrates with AWS using IAM roles. Incorrect permissions prevent access to secrets.

80. **Error:** `Vault policies not enforced`

- **Cause:** Incorrectly defined or applied policies in the Vault configuration.
- **Solution:**
  1. Verify and correct policy definitions using `vault policy read <policy_name>`.
  2. Reattach policies to tokens or roles that require them.
- **RCA:** Vault policies enforce access control. Misconfigured or missing policies result in unexpected behavior.

81. **Error:** `ZAP does not detect SQL Injection vulnerabilities`

- **Cause:** The application uses non-standard SQL queries or parameterized queries that bypass traditional detection methods.
- **Solution:**
  1. Enable advanced SQL Injection rules in the Scan Policy Manager.
  2. Use manual testing with crafted payloads for complex scenarios.
- **RCA:** ZAP relies on generic SQL payloads for detection. Advanced techniques or parameterized queries require custom testing.

82. **Error:** `ZAP AJAX Spider does not load all JavaScript resources`

- **Cause:** The target website blocks requests from untrusted user agents or scripts are dynamically loaded after specific user actions.
- **Solution:**
    1. Change the user-agent string in ZAP to mimic a real browser.
    2. Use ZAP's browser-based crawler for better coverage.
- **RCA:** AJAX Spider relies on fetching JavaScript resources. Security mechanisms like bot detection prevent this.

83. **Error:** `High false positive rate in ZAP scan results`

- **Cause:** Overly aggressive scan rules or lack of application context.
- **Solution:**
    1. Review and refine the scan rules to reduce noise.
    2. Configure proper contexts and exclusions for the target application.
- **RCA:** Default scan configurations may flag benign issues as vulnerabilities without proper context.

84. **Error:** `Unable to intercept HTTPS traffic`

- **Cause:** ZAP's SSL/TLS certificate is not trusted by the browser or application.
- **Solution:**
    1. Import ZAP’s root certificate into the browser or application.
    2. Verify that ZAP is listening on the correct proxy port.
- **RCA:** HTTPS interception requires trusted certificates. Untrusted certificates are rejected by secure applications.

85. **Error:** `Scan stops unexpectedly`

- **Cause:** Resource exhaustion (e.g., memory or disk space) on the system running ZAP.
- **Solution:**
    1. Increase the system's available memory or disk space.
    2. Limit the scan scope to smaller target areas or use pagination.

- **RCA:** Large-scale scans can overwhelm system resources, leading to abrupt terminations.

86. **Error:** `AWS account missing root account MFA`
- **Cause:** MFA is not enabled for the AWS root account.
- **Solution:**
    1. Enable MFA for the root account in the AWS Management Console.
    2. Use a hardware or virtual MFA device to enhance security.
- **RCA:** AWS strongly recommends MFA for the root account. Lack of MFA increases the risk of unauthorized access.

87. **Error:** `IAM access keys are active for over 90 days`
- **Cause:** Access keys have not been rotated or disabled after the recommended period.
- **Solution:**
    1. Rotate the access keys regularly and update applications using them.
    2. Use IAM Access Analyzer to monitor and enforce key rotation.
- **RCA:** Stale access keys are a security risk and often flagged during compliance checks.

88. **Error:** `Default VPC is not deleted`
- **Cause:** The default VPC still exists and is unused.
- **Solution:**
    1. Delete the default VPC if not in use.
    2. Use custom VPCs with stricter security configurations for workloads.
- **RCA:** Default VPCs often have broad permissions and lack custom security configurations, making them less secure.

89. **Error:** `Elastic IPs found unattached`
- **Cause:** Elastic IPs are allocated but not associated with any instance.

- **Solution:**
    1. Release unused Elastic IPs to avoid unnecessary charges.
    2. Regularly audit the account for unattached resources.
- **RCA:** Unused Elastic IPs incur costs and are often overlooked in resource management.

90. **Error:** `Unencrypted AMIs detected`
- **Cause:** AMIs are not encrypted during creation.
- **Solution:**
    1. Enable encryption for all AMIs using KMS keys.
    2. Enforce encryption policies via AWS Config rules.
- **RCA:** Unencrypted AMIs expose sensitive data, violating AWS security best practices.

91. **Error:** `Image scan shows missing OS packages`
- **Cause:** The image uses a base layer not supported by Trivy's database.
- **Solution:**
    1. Rebuild the image with a supported base layer.
    2. Ensure that Trivy's vulnerability database is up-to-date.
- **RCA:** Trivy relies on known vulnerabilities for specific OS packages. Unsupported layers lead to incomplete scans.

92. **Error:** `Error analyzing Dockerfile: syntax error detected`
- **Cause:** The Dockerfile contains invalid syntax or unsupported commands.
- **Solution:**
    1. Validate the Dockerfile using `docker build` or linters.
    2. Correct any syntax errors or deprecated commands.
- **RCA:** Trivy's Dockerfile analysis expects proper syntax. Invalid files cannot be processed.

93. **Error:** `No vulnerabilities detected, but outdated dependencies present`

- **Cause:** Trivy does not flag outdated dependencies as vulnerabilities.
- **Solution:**
    1. Use dependency management tools to update to the latest versions.
    2. Combine Trivy with tools like `npm audit` or `pip-audit` for dependency checks.
- **RCA:** Outdated dependencies may not have CVEs but pose a security risk nonetheless.

94. **Error:** `Trivy scan fails for multi-stage builds`

- **Cause:** Trivy scans only the final stage of multi-stage builds by default.
- **Solution:**
    1. Use `docker save` to extract all stages and scan each stage individually.
    2. Build a comprehensive image that includes intermediate layers if necessary.
- **RCA:** Trivy focuses on the final image, potentially missing vulnerabilities in intermediate stages.

95. **Error:** `Trivy reports vulnerabilities for patched CVEs`

- **Cause:** Trivy's database is outdated, or the scanned software uses backported patches that do not update the reported version.
- **Solution:**
    1. Update Trivy’s database using `trivy db update`.
    2. Verify manually if the CVE is fixed through backported patches in the software.
    3. Exclude the specific CVE from the scan results using the `--ignore-unfixed` flag.
- **RCA:** Backported fixes can cause false positives, as the patched version does not always increment its release number.

96. **Error:** `Trivy fails to scan filesystems with special characters`

- **Cause:** Special characters or non-standard filenames in the target directory cause parsing errors.
- **Solution:**
    1. Rename files to standard ASCII characters.
    2. Use `--skip-dirs` or `--skip-files` options to exclude problematic files.
- **RCA:** File parsing issues occur due to non-standard naming conventions or unsupported encoding.

97. **Error:** `Scan of large images crashes with "out of memory"`
- **Cause:** Trivy requires more memory than available on the host system.
- **Solution:**
    1. Increase available memory for the Trivy process by closing unnecessary applications or running it on a system with higher RAM.
    2. Use the `--cache-dir` option to store intermediate scan data on disk instead of memory.
- **RCA:** Trivy's analysis of large images involves loading all image layers into memory, which overwhelms systems with limited resources.

98. **Error:** `Trivy Docker image scan fails: "Cannot connect to Docker daemon"`
- **Cause:** Docker is not running or the user does not have permission to access the Docker socket.
- **Solution:**
    1. Start the Docker daemon using `sudo systemctl start docker`.
    2. Add the current user to the Docker group using `sudo usermod -aG docker $USER`.
    3. Use `sudo` for commands if permissions are not configured.
- **RCA:** Trivy interacts directly with the Docker daemon, requiring it to be running and accessible.

99. **Error:** `Trivy cannot parse SPDX license data`

- **Cause:** The scanned image or project includes malformed SPDX license information.
- **Solution:**
    1. Correct the SPDX license format in the project metadata (e.g., `package.json` or `requirements.txt`).
    2. Rebuild the image or regenerate the metadata.
- **RCA:** SPDX license data needs to adhere to specific formatting standards. Any deviation results in parsing errors.

100. **Error:** `Trivy fails to scan OCI-compliant images`

- **Cause:** The image uses a newer OCI format not fully supported by Trivy.
- **Solution:**
    1. Convert the image to a Docker-compatible format using tools like `docker save`.
    2. Ensure Trivy is updated to the latest version with OCI format support.
- **RCA:** OCI-compliant images introduce features that may not be fully integrated into Trivy's scanning mechanisms.