Threat Model and Risk Assessment Report

Executive Summary

This report presents the results of an automated threat modeling and risk assessment for the architecture diagram "test_diagram.svg". The analysis identified 9 potential security threats that should be addressed.

Generated: 2025-07-21 21:10:19

Architecture Overview

The analyzed architecture consists of 2 components and 1 connections.

Components

ID	Name	Type
comp1	Component 1	service
comp2	Component 2	database

Threat Summary

Risk Level	Count	Percentage
High	4	44.4%
Medium	5	55.6%
Low	0	0.0%
Total	9	100%

Identified Threats

Detailed Threat Analysis

Spoofing Threats

Unauthenticated API Access (T001-comp1)

Description: API endpoints without proper authentication can be accessed by unauthorized users

Category: Spoofing

Risk Level: HIGH

Impact: high

Likelihood: likely

Affected Component: comp1

Recommended Mitigation:

1. Implement proper authentication mechanisms such as API keys, OAuth, or JWT
2. Implement OAuth 2.0 or OpenID Connect for authentication
3. Use strong, properly implemented JWT tokens with appropriate expiration
4. Implement IP-based rate limiting to prevent brute force attacks
5. Consider using an API gateway with built-in authentication capabilities

Additional Information:

Spoofing attacks involve attackers pretending to be someone or something else. These attacks can lead to unauthorized access to systems or data. Common spoofing techniques include IP spoofing, email spoofing, and website spoofing.

References:

- OWASP Top 10 2021: A07 - Identification and Authentication Failures
- NIST SP 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management
- CWE-287: Improper Authentication
- OWASP API Security Top 10 2023

Denial of Service Threats

Denial of Service Vulnerability (T004-comp1)

Description: Services without rate limiting or load balancing are vulnerable to DoS attacks

Category: Denial of Service

Risk Level: MEDIUM

Impact: medium

Likelihood: possible

Affected Component: comp1

Recommended Mitigation:

1. Implement rate limiting, load balancing, and DoS protection

2. Implement rate limiting

3. Use a CDN for static content

4. Implement auto-scaling for dynamic resources

5. Use a DDoS protection service

Additional Information:

Denial of Service (DoS) attacks aim to make a system or resource unavailable to its intended users. This can be achieved by overwhelming the system with traffic, exploiting vulnerabilities, or exhausting system resources.

References:

• OWASP Top 10 2021: A05 - Security Misconfiguration

• CWE-400: Uncontrolled Resource Consumption

• NIST SP 800-53: SC-5 Denial of Service Protection

Single Point of Failure (T006-arch)

Description: Architecture has components that represent single points of failure

Category: Denial of Service

Risk Level: HIGH

Impact: high

Likelihood: likely

Affected Component: overall_architecture

Recommended Mitigation:

1. Implement redundancy and high availability patterns

2. Implement rate limiting

3. Use a CDN for static content

4. Implement auto-scaling for dynamic resources

5. Use a DDoS protection service

Additional Information:

Denial of Service (DoS) attacks aim to make a system or resource unavailable to its intended users. This can be achieved by overwhelming the system with traffic, exploiting vulnerabilities, or exhausting system resources.

References:

• OWASP Top 10 2021: A05 - Security Misconfiguration

• CWE-400: Uncontrolled Resource Consumption

• NIST SP 800-53: SC-5 Denial of Service Protection

Repudiation Threats

Insufficient Logging (T005-comp1)

Description: Lack of proper logging makes it difficult to track security incidents

Category: Repudiation

Risk Level: MEDIUM

Impact: medium

Likelihood: possible

Affected Component: comp1

Recommended Mitigation:

1. Implement comprehensive logging and monitoring
2. Implement centralized logging with tamper-evident logs
3. Use a SIEM solution for log analysis
4. Ensure all security-relevant events are logged
5. Include unique request IDs in logs for traceability

Additional Information:

Repudiation threats involve users denying that they performed an action, and the system lacking the ability to prove otherwise. Proper logging and auditing are essential to mitigate repudiation threats.

References:

- OWASP Top 10 2021: A09 - Security Logging and Monitoring Failures
- CWE-778: Insufficient Logging
- NIST SP 800-53: AU-2 Audit Events

Insufficient Logging (T005-comp2)

Description: Lack of proper logging makes it difficult to track security incidents

Category: Repudiation

Risk Level: MEDIUM

Impact: medium

Likelihood: possible

Affected Component: comp2

Recommended Mitigation:

1. Implement comprehensive logging and monitoring
2. Implement centralized logging with tamper-evident logs
3. Use a SIEM solution for log analysis
4. Ensure all security-relevant events are logged

5. Include unique request IDs in logs for traceability

Additional Information:

Repudiation threats involve users denying that they performed an action, and the system lacking the ability to prove otherwise. Proper logging and auditing are essential to mitigate repudiation threats.

References:

- OWASP Top 10 2021: A09 - Security Logging and Monitoring Failures
- CWE-778: Insufficient Logging
- NIST SP 800-53: AU-2 Audit Events

Insufficient Logging (T005-conn1)

Description: Lack of proper logging makes it difficult to track security incidents

Category: Repudiation

Risk Level: MEDIUM

Impact: medium

Likelihood: possible

Affected Component: comp1-comp2

Recommended Mitigation:

1. Implement comprehensive logging and monitoring
2. Implement centralized logging with tamper-evident logs
3. Use a SIEM solution for log analysis
4. Ensure all security-relevant events are logged
5. Include unique request IDs in logs for traceability

Additional Information:

Repudiation threats involve users denying that they performed an action, and the system lacking the ability to prove otherwise. Proper logging and auditing are essential to mitigate repudiation threats.

References:

- OWASP Top 10 2021: A09 - Security Logging and Monitoring Failures
- CWE-778: Insufficient Logging
- NIST SP 800-53: AU-2 Audit Events

Insufficient Logging (T005-arch)

Description: Lack of proper logging makes it difficult to track security incidents

Category: Repudiation

Risk Level: MEDIUM

Impact: medium

Likelihood: possible

Affected Component: overall_architecture

Recommended Mitigation:

1. Implement comprehensive logging and monitoring

2. Implement centralized logging with tamper-evident logs

3. Use a SIEM solution for log analysis

4. Ensure all security-relevant events are logged

5. Include unique request IDs in logs for traceability

Additional Information:

Repudiation threats involve users denying that they performed an action, and the system lacking the ability to prove otherwise. Proper logging and auditing are essential to mitigate repudiation threats.

References:

• OWASP Top 10 2021: A09 - Security Logging and Monitoring Failures

• CWE-778: Insufficient Logging

• NIST SP 800-53: AU-2 Audit Events

Tampering Threats

Insecure Data Storage (T003-comp2)

Description: Data stored without encryption can be accessed or modified by unauthorized users

Category: Tampering

Risk Level: HIGH

Impact: high

Likelihood: likely

Affected Component: comp2

Recommended Mitigation:

1. Implement data encryption at rest

2. Use AES-256 encryption for sensitive data

3. Implement proper key management

4. Use digital signatures to detect tampering

5. Implement data integrity checks

Additional Information:

Tampering involves the unauthorized modification of data or code. This can lead to data corruption, system compromise, or unauthorized actions being performed. Tampering can occur during storage, transmission, or processing of data.

References:

- OWASP Top 10 2021: A03 - Injection
- CWE-89: SQL Injection
- NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity
- CWE-311: Missing Encryption of Sensitive Data

Information Disclosure Threats

Unencrypted Data Transfer (T002-conn1)

Description: Data transferred over unencrypted connections can be intercepted

Category: Information Disclosure

Risk Level: HIGH

Impact: high

Likelihood: likely

Affected Component: comp1-comp2

Recommended Mitigation:

1. Use TLS/SSL for all data transfers
2. Use TLS 1.3 for all data transfers
3. Implement proper certificate validation
4. Use strong cipher suites
5. Implement HSTS to prevent downgrade attacks

Additional Information:

Information disclosure threats involve the exposure of sensitive information to unauthorized parties. This can include data breaches, unencrypted communications, or improper access controls leading to data leakage.

References:

- OWASP Top 10 2021: A02 - Cryptographic Failures
- CWE-311: Missing Encryption of Sensitive Data
- NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity
- NIST SP 800-57: Recommendation for Key Management