Threat Model Report
E-Commerce Platform

6 January 2025

Kshitija Kulkarni

Table of Contents

Results Overview

Risks by Vulnerability Category

Risks by Technical Asset

Data Breach Probabilities by Data Asset

Trust Boundaries

About Threagile

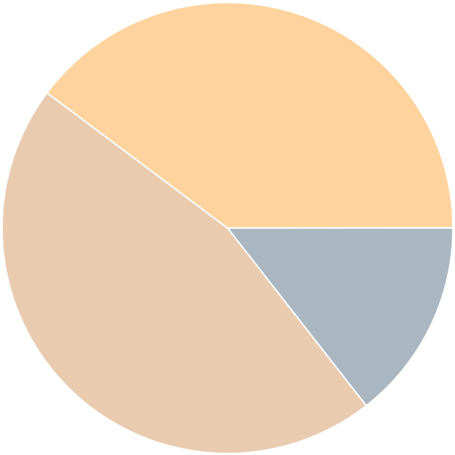
Management Summary

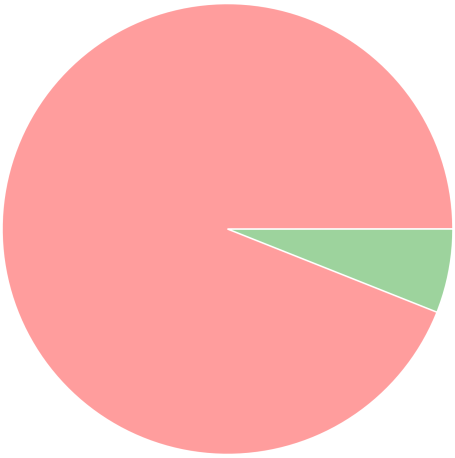
Threagile toolkit was used to model the architecture of "E-Commerce Platform" and derive risks by analyzing the components and data flows. The risks identified during this analysis are shown in the following chapters. Identified risks during threat modeling do not necessarily mean that the vulnerability associated with this risk actually exists: it is more to be seen as a list of potential risks and threats, which should be individually reviewed and reduced by removing false positives. For the remaining risks it should be checked in the design and implementation of "E-Commerce Platform" whether the mitigation advices have been applied or not.

Each risk finding references a chapter of the OWASP ASVS (Application Security Verification Standard) audit checklist. The OWASP ASVS checklist should be considered as an inspiration by architects and developers to further harden the application in a Defense-in-Depth approach. Additionally, for each risk finding a link towards a matching OWASP Cheat Sheet or similar with technical details about how to implement a mitigation is given.

In total **83 initial risks** in **17 categories** have been identified during the threat modeling process:

		78	**unchecked**
0	**critical risk**	**0**	**in discussion**
0	**high risk**	**0**	**accepted**
33	**elevated risk**	**0**	**in progress**
38	**medium risk**	**5**	***mitigated***
12	**low risk**	**0**	***false positive***





an e-commerce platform that allows customers to browse products, add items to their cart, place orders, and process payments.

Impact Analysis of 83 Initial Risks in 17 Categories

The most prevalent impacts of the **83 initial risks** (distributed over **17 risk categories**) are (taking the severity ratings into account and using the highest for each category):
Risk finding paragraphs are clickable and link to the corresponding chapter.

Elevated: **Missing Cloud Hardening**: 7 Initial Risks - Exploitation likelihood is *Unlikely* with *Very High* impact.
If this risk is unmitigated, attackers might access cloud components in an unintended way.

Elevated: **Missing Hardening**: 4 Initial Risks - Exploitation likelihood is *Likely* with *Medium* impact.
If this risk remains unmitigated, attackers might be able to easier attack high-value targets.

Elevated: **SQL/NoSQL-Injection**: 2 Initial Risks - Exploitation likelihood is *Likely* with *High* impact.
If this risk is unmitigated, attackers might be able to modify SQL/NoSQL queries to steal and modify data and eventually further escalate towards a deeper system penetration via code executions.

Elevated: **Server-Side Request Forgery (SSRF)**: 19 Initial Risks - Exploitation likelihood is *Likely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to access sensitive services or files of network-reachable components by modifying outgoing calls of affected components.

Elevated: **Unguarded Access From Internet**: 6 Initial Risks - Exploitation likelihood is *Very Likely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to directly attack sensitive systems without any hardening components in-between due to them being directly exposed on the internet.

Medium: **Container Base Image Backdooring**: 5 Initial Risks - Exploitation likelihood is *Unlikely* with *High* impact.
If this risk is unmitigated, attackers might be able to deeply persist in the target system by executing code in deployed containers.

Medium: **Container Platform Escape**: 4 Initial Risks - Exploitation likelihood is *Unlikely* with *High* impact.
If this risk is unmitigated, attackers which have successfully compromised a container (via other vulnerabilities) might be able to deeply persist in the target system by executing code in many deployed containers and the container platform itself.

Medium: **DoS-risky Access Across Trust-Boundary**: 4 Initial Risks - Exploitation likelihood is *Unlikely* with *Medium* impact.
If this risk remains unmitigated, attackers might be able to disturb the availability of important parts of the system.

Medium: **Missing Build Infrastructure**: 1 Initial Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to exploit risks unseen in this threat model due to critical build infrastructure components missing in the model.

Medium: **Missing Identity Store**: 1 Initial Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to exploit risks unseen in this threat model in the identity provider/store that is currently missing in the model.

Medium: **Missing Two-Factor Authentication (2FA)**: 1 Initial Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to access or modify highly sensitive data without strong authentication.

Medium: **Missing Vault (Secret Storage)**: 1 Initial Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to easier steal config secrets (like credentials, private keys, client certificates, etc.) once a vulnerability to access files is present and exploited.

Medium: **Unencrypted Communication**: 8 Initial Risks - Exploitation likelihood is *Unlikely* with *High* impact.
If this risk is unmitigated, network attackers might be able to to eavesdrop on unencrypted sensitive data sent between components.

Medium: **Unencrypted Technical Assets**: 5 Initial Risks - Exploitation likelihood is *Unlikely* with *High* impact.
If this risk is unmitigated, attackers might be able to access unencrypted data when successfully compromising sensitive components.

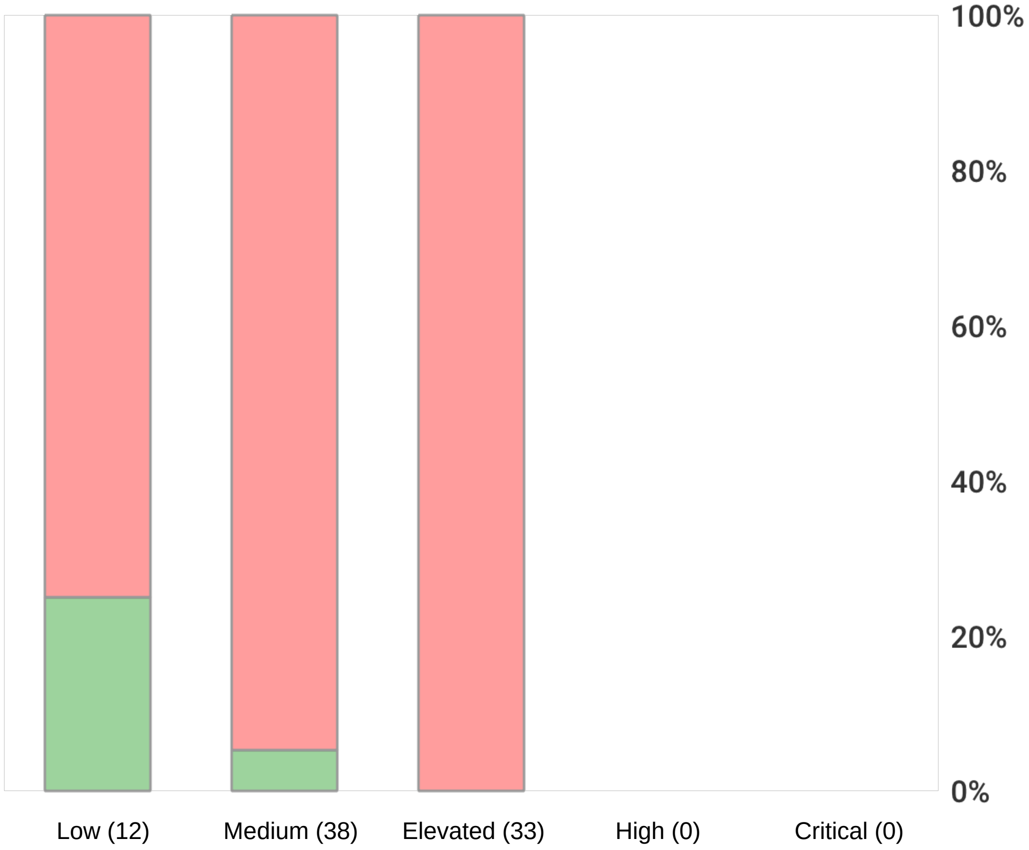
Medium: **Unnecessary Data Transfer**: 7 Initial Risks - Exploitation likelihood is *Unlikely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to target unnecessarily transferred data.

Low: **Unnecessary Data Asset**: 1 Initial Risk - Exploitation likelihood is *Unlikely* with *Low* impact.
If this risk is unmitigated, attackers might be able to access unnecessary data assets using other vulnerabilities.

Low: **Wrong Communication Link Content**: 7 Initial Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
If this potential model error is not fixed, some risks might not be visible.

Risk Mitigation

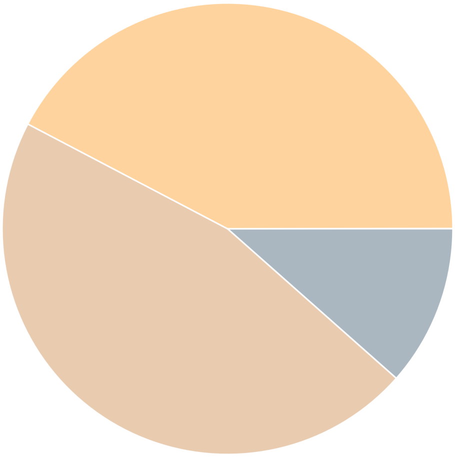
The following chart gives a high-level overview of the risk tracking status (including mitigated risks):



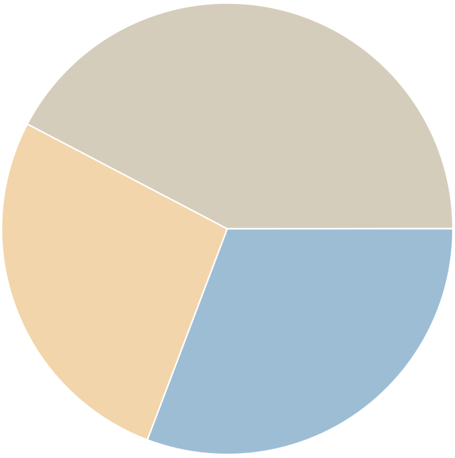
78 unchecked
0 in discussion
0 accepted
0 in progress
5 *mitigated*
0 *false positive*

After removal of risks with status *mitigated* and *false positive* the following **78 remain unmitigated**:

0 unmitigated critical risk
0 unmitigated high risk
33 unmitigated elevated risk
36 unmitigated medium risk
9 unmitigated low risk



0 business side related
24 architecture related
21 development related
33 operations related



Impact Analysis of 78 Remaining Risks in 15 Categories

The most prevalent impacts of the **78 remaining risks** (distributed over **15 risk categories**) are (taking the severity ratings into account and using the highest for each category):

Risk finding paragraphs are clickable and link to the corresponding chapter.

Elevated: **Missing Cloud Hardening**: 7 Remaining Risks - Exploitation likelihood is *Unlikely* with *Very High* impact.
If this risk is unmitigated, attackers might access cloud components in an unintended way.

Elevated: **Missing Hardening**: 4 Remaining Risks - Exploitation likelihood is *Likely* with *Medium* impact.
If this risk remains unmitigated, attackers might be able to easier attack high-value targets.

Elevated: **SQL/NoSQL-Injection**: 2 Remaining Risks - Exploitation likelihood is *Likely* with *High* impact.
If this risk is unmitigated, attackers might be able to modify SQL/NoSQL queries to steal and modify data and eventually further escalate towards a deeper system penetration via code executions.

Elevated: **Server-Side Request Forgery (SSRF)**: 19 Remaining Risks - Exploitation likelihood is *Likely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to access sensitive services or files of network-reachable components by modifying outgoing calls of affected components.

Elevated: **Unguarded Access From Internet**: 6 Remaining Risks - Exploitation likelihood is *Very Likely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to directly attack sensitive systems without any hardening components in-between due to them being directly exposed on the internet.

Medium: **Container Base Image Backdooring**: 5 Remaining Risks - Exploitation likelihood is *Unlikely* with *High* impact.
If this risk is unmitigated, attackers might be able to deeply persist in the target system by executing code in deployed containers.

Medium: **Container Platform Escape**: 4 Remaining Risks - Exploitation likelihood is *Unlikely* with *High* impact.
If this risk is unmitigated, attackers which have successfully compromised a container (via other vulnerabilities) might be able to deeply persist in the target system by executing code in many deployed containers and the container platform itself.

Medium: **Missing Build Infrastructure**: 1 Remaining Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to exploit risks unseen in this threat model due to critical build infrastructure components missing in the model.

Medium: **Missing Identity Store**: 1 Remaining Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to exploit risks unseen in this threat model in the identity provider/store that is currently missing in the model.

Medium: **Missing Vault (Secret Storage)**: 1 Remaining Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to easier steal config secrets (like credentials, private keys, client certificates, etc.) once a vulnerability to access files is present and exploited.

Medium: **Unencrypted Communication**: 8 Remaining Risks - Exploitation likelihood is *Unlikely* with *High* impact.
If this risk is unmitigated, network attackers might be able to to eavesdrop on unencrypted sensitive data sent between components.

Medium: **Unencrypted Technical Assets**: 5 Remaining Risks - Exploitation likelihood is *Unlikely* with *High* impact.
If this risk is unmitigated, attackers might be able to access unencrypted data when successfully compromising sensitive components.

Medium: **Unnecessary Data Transfer**: 7 Remaining Risks - Exploitation likelihood is *Unlikely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to target unnecessarily transferred data.

Low: **Unnecessary Data Asset**: 1 Remaining Risk - Exploitation likelihood is *Unlikely* with *Low* impact.
If this risk is unmitigated, attackers might be able to access unnecessary data assets using other vulnerabilities.

Low: **Wrong Communication Link Content**: 7 Remaining Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
If this potential model error is not fixed, some risks might not be visible.

Application Overview

Business Criticality

The overall business criticality of "E-Commerce Platform" was rated as:

(archive | operational | important | **CRITICAL** | mission-critical)

Business Overview

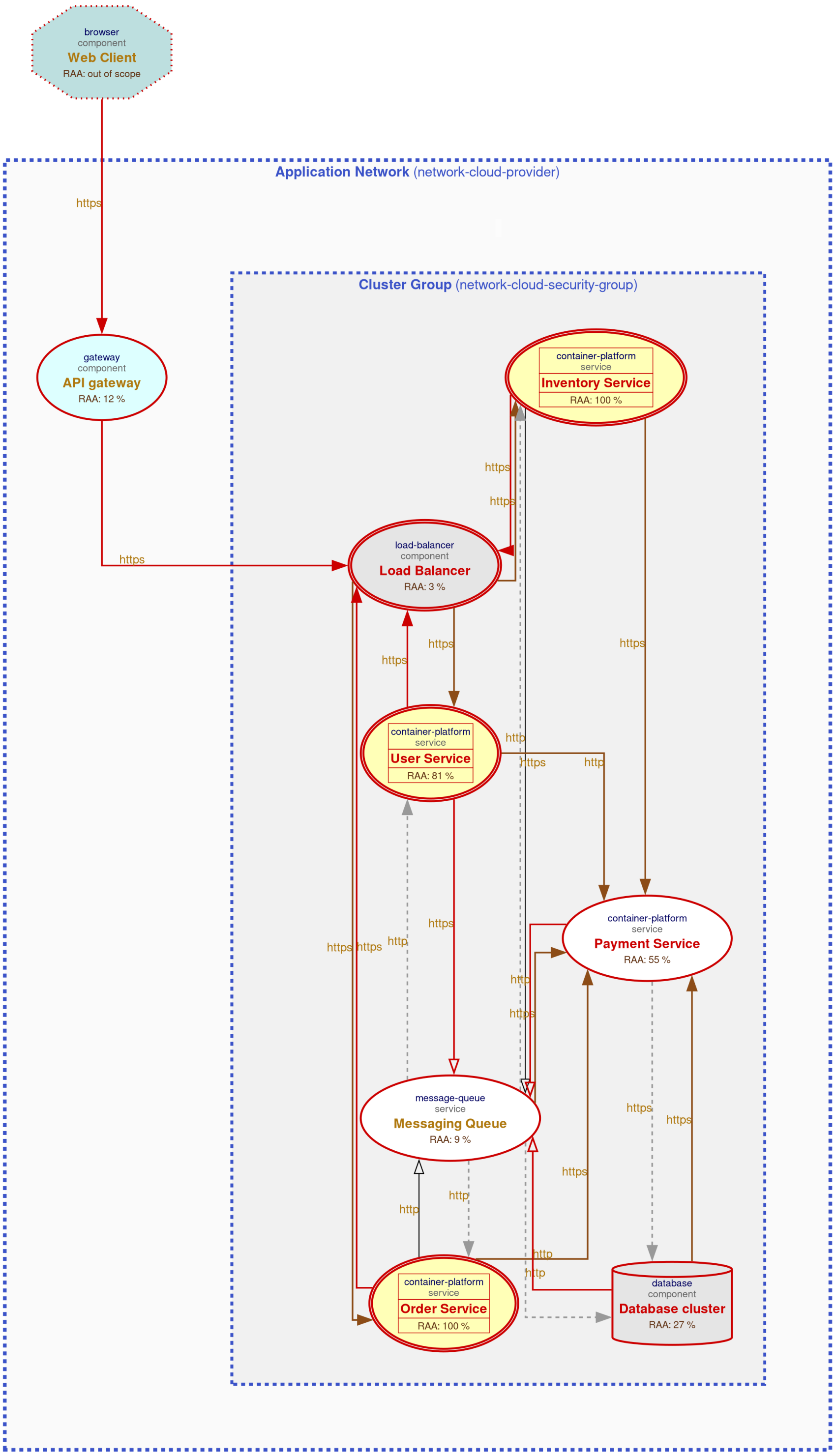
an e-commerce platform that allows customers to browse products, add items to their cart, place orders, and process payments.

Technical Overview

The platform uses a distributed, clustered infrastructure for high availability, scalability, and fault tolerance. It also includes multiple microservices like user management, inventory management, order processing, and payment gateways.

Data-Flow Diagram

The following diagram was generated by Threagile based on the model input and gives a high-level overview of the data-flow between technical assets. The RAA value is the calculated *Relative Attacker Attractiveness* in percent. For a full high-resolution version of this diagram please refer to the PNG image file alongside this report.



Security Requirements

This chapter lists the custom security requirements which have been defined for the modeled target.

Data encryption
Custumer PCI data should be encrypted using strong encryption in transit ans rest.

Input Validation
Strict input validation is required to reduce the overall attack surface.

This list is not complete and regulatory or law relevant security requirements have to be taken into account as well. Also custom individual security requirements might exist for the project.

Abuse Cases

This chapter lists the custom abuse cases which have been defined for the modeled target.

CPU-Cycle Theft
As a hacker I want to steal CPU cycles in order to transform them into money via installed crypto currency miners.

Cross-Site Scripting Attacks
Malicious scripts injected into user input fields (e.g., search, reviews) to steal session cookies.

Database Compromise
Attackers exploiting SQL injection vulnerabilities to extract sensitive information.

Denial-of-Service
As a hacker I want to disturb the functionality of the backend system in order to cause indirect financial damage via unusable features.

Denial-of-Service of Enduser Functionality
Attackers overwhelming the web servers, API Gateway, or backend services with excessive traffic.

Identity Theft
As a hacker I want to steal identity data in order to reuse credentials and/or keys on other targets of the same company or outside.

PCI Theft
As a hacker I want to steal PII (Personally Identifiable Information) data in order to blackmail the company and/or damage their repudiation by publishing them.

Privilege Escalation
Attackers exploiting misconfigurations or vulnerabilities to gain elevated privileges on backend services or databases.

Ransomware
As a hacker I want to encrypt the storage and file systems in order to demand ransom.

Session Hijacking
Attackers stealing or hijacking valid session cookies to impersonate users.

This list is not complete and regulatory or law relevant abuse cases have to be taken into account as well. Also custom individual abuse cases might exist for the project.

Tag Listing

This chapter lists what tags are used by which elements.

aws
Application Network

aws:ec2
Payment Service Traffic, Messaging Queue, Inventory Service, Payment Service Traffic, Messaging Queue, User Service Traffic, Order Service Traffic, Inventory Service Traffic, Messaging Queue, User Service Traffic, Payment Service Traffic, Order Service Traffic, Inventory Service Traffic, Order Service, Payment Service Traffic, Messaging Queue, Payment Service, Messaging Queue, User Service, Payment Service Traffic, Messaging Queue

aws:rds
Database cluster, Database Customizing and Dumps

linux
Database cluster, Inventory Service, Messaging Queue, Order Service, Payment Service, User Service

mysql
Database cluster

STRIDE Classification of Identified Risks

This chapter clusters and classifies the risks by STRIDE categories: In total **83 potential risks** have been identified during the threat modeling process of which **1 in the Spoofing** category, **19 in the Tampering** category, **0 in the Repudiation** category, **40 in the Information Disclosure** category, **4 in the Denial of Service** category, and **19 in the Elevation of Privilege** category.

Risk finding paragraphs are clickable and link to the corresponding chapter.

Spoofing

Medium: **Missing Identity Store**: 1 / 1 Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
The modeled architecture does not contain an identity store, which might be the risk of a model missing critical assets (and thus not seeing their risks).

Tampering

Elevated: **Missing Cloud Hardening**: 7 / 7 Risks - Exploitation likelihood is *Unlikely* with *Very High* impact.
Cloud components should be hardened according to the cloud vendor best practices. This affects their configuration, auditing, and further areas.

Elevated: **Missing Hardening**: 4 / 4 Risks - Exploitation likelihood is *Likely* with *Medium* impact.
Technical assets with a Relative Attacker Attractiveness (RAA) value of 55 % or higher should be explicitly hardened taking best practices and vendor hardening guides into account.

Elevated: **SQL/NoSQL-Injection**: 2 / 2 Risks - Exploitation likelihood is *Likely* with *High* impact.
When a database is accessed via database access protocols SQL/NoSQL-Injection risks might arise. The risk rating depends on the sensitivity technical asset itself and of the data assets processed or stored.

Medium: **Container Base Image Backdooring**: 5 / 5 Risks - Exploitation likelihood is *Unlikely* with *High* impact.
When a technical asset is built using container technologies, Base Image Backdooring risks might arise where base images and other layers used contain vulnerable components or backdoors.

Medium: **Missing Build Infrastructure**: 1 / 1 Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
The modeled architecture does not contain a build infrastructure (devops-client, sourcecode-repo, build-pipeline, etc.), which might be the risk of a model missing critical assets (and thus not seeing their risks). If the architecture contains custom-developed parts, the pipeline where code gets developed and built needs to be part of the model.

Repudiation

n/a

Information Disclosure

Elevated: **Server-Side Request Forgery (SSRF)**: 19 / 19 Risks - Exploitation likelihood is *Likely* with *Medium* impact.
When a server system (i.e. not a client) is accessing other server systems via typical web protocols Server-Side Request Forgery (SSRF) or Local-File-Inclusion (LFI) or Remote-File-Inclusion (RFI) risks might arise.

Medium: **Missing Vault (Secret Storage)**: 1 / 1 Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
In order to avoid the risk of secret leakage via config files (when attacked through vulnerabilities being able to read files like Path-Traversal and others), it is best practice to use a separate hardened process with proper authentication, authorization, and audit logging to access config secrets (like credentials, private keys, client certificates, etc.). This component is usually some kind of Vault.

Medium: **Unencrypted Communication**: 8 / 8 Risks - Exploitation likelihood is *Unlikely* with *High* impact.
Due to the confidentiality and/or integrity rating of the data assets transferred over the communication link this connection must be encrypted.

Medium: **Unencrypted Technical Assets**: 5 / 5 Risks - Exploitation likelihood is *Unlikely* with *High* impact.
Due to the confidentiality rating of the technical asset itself and/or the processed data assets this technical asset must be encrypted. The risk rating depends on the sensitivity technical asset itself and of the data assets stored.

Low: **Wrong Communication Link Content**: 7 / 7 Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
When a communication link is defined as readonly, but does not receive any data asset, or when it is defined as not readonly, but does not send any data asset, it is likely to be a model failure.

Denial of Service

Medium: **DoS-risky Access Across Trust-Boundary**: 0 / 4 Risks - Exploitation likelihood is *Unlikely* with *Medium* impact.
Assets accessed across trust boundaries with critical or mission-critical availability rating are more prone to Denial-of-Service (DoS) risks.

Elevation of Privilege

Elevated: **Unguarded Access From Internet**: 6 / 6 Risks - Exploitation likelihood is *Very Likely* with *Medium* impact.
Internet-exposed assets must be guarded by a protecting service, application, or reverse-proxy.

Medium: **Container Platform Escape**: 4 / 4 Risks - Exploitation likelihood is *Unlikely* with *High* impact.
Container platforms are especially interesting targets for attackers as they host big parts of a containerized runtime infrastructure. When not configured and operated with security best practices in mind, attackers might exploit a vulnerability inside an container and escape towards the platform as highly privileged users. These scenarios might give attackers capabilities to attack every other container as owning the container platform (via container escape attacks) equals to owning every container.

Medium: **Missing Two-Factor Authentication (2FA)**: 0 / 1 Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
Technical assets (especially multi-tenant systems) should authenticate incoming requests with two-factor (2FA) authentication when the asset processes or stores highly sensitive data (in terms of confidentiality, integrity, and availability) and is accessed by humans.

Medium: **Unnecessary Data Transfer**: 7 / 7 Risks - Exploitation likelihood is *Unlikely* with *Medium* impact.
When a technical asset sends or receives data assets, which it neither processes or stores this is an indicator for unnecessarily transferred data (or for an incomplete model). When the unnecessarily transferred data assets are sensitive, this poses an unnecessary risk of an increased attack surface.

Low: **Unnecessary Data Asset**: 1 / 1 Risk - Exploitation likelihood is *Unlikely* with *Low* impact.
When a data asset is not processed or stored by any data assets and also not transferred by any communication links, this is an indicator for an unnecessary data asset (or for an incomplete model).

Assignment by Function

This chapter clusters and assigns the risks by functions which are most likely able to check and mitigate them: In total **83 potential risks** have been identified during the threat modeling process of which **1 should be checked by Business Side**, **24 should be checked by Architecture**, **21 should be checked by Development**, and **37 should be checked by Operations**.

Risk finding paragraphs are clickable and link to the corresponding chapter.

Business Side

Medium: **Missing Two-Factor Authentication (2FA)**: 0 / 1 Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
Apply an authentication method to the technical asset protecting highly sensitive data via two-factor authentication for human users.

Architecture

Elevated: **Unguarded Access From Internet**: 6 / 6 Risks - Exploitation likelihood is *Very Likely* with *Medium* impact.
Encapsulate the asset behind a guarding service, application, or reverse-proxy. For admin maintenance a bastion-host should be used as a jump-server. For file transfer a store-and-forward-host should be used as an indirect file exchange platform.

Medium: **Missing Build Infrastructure**: 1 / 1 Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
Include the build infrastructure in the model.

Medium: **Missing Identity Store**: 1 / 1 Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
Include an identity store in the model if the application has a login.

Medium: **Missing Vault (Secret Storage)**: 1 / 1 Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
Consider using a Vault (Secret Storage) to securely store and access config secrets (like credentials, private keys, client certificates, etc.).

Medium: **Unnecessary Data Transfer**: 7 / 7 Risks - Exploitation likelihood is *Unlikely* with *Medium* impact.
Try to avoid sending or receiving sensitive data assets which are not required (i.e. neither processed or stored) by the involved technical asset.

Low: **Unnecessary Data Asset**: 1 / 1 Risk - Exploitation likelihood is *Unlikely* with *Low* impact.
Try to avoid having data assets that are not required/used.

Low: **Wrong Communication Link Content**: 7 / 7 Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
Try to model the correct readonly flag and/or data sent/received of communication links. Also try to use communication link types matching the target technology/machine types.

Development

Elevated: **SQL/NoSQL-Injection**: 2 / 2 Risks - Exploitation likelihood is *Likely* with *High* impact.
Try to use parameter binding to be safe from injection vulnerabilities. When a third-party product is used instead of custom developed software, check if the product applies the proper mitigation and ensure a reasonable patch-level.

Elevated: **Server-Side Request Forgery (SSRF)**: 19 / 19 Risks - Exploitation likelihood is *Likely* with *Medium* impact.
Try to avoid constructing the outgoing target URL with caller controllable values. Alternatively use a mapping (whitelist) when accessing outgoing URLs instead of creating them including caller controllable values. When a third-party product is used instead of custom developed software, check if the product applies the proper mitigation and ensure a reasonable patch-level.

Operations

Elevated: **Missing Cloud Hardening**: 7 / 7 Risks - Exploitation likelihood is *Unlikely* with *Very High* impact.
Apply hardening of all cloud components and services, taking special care to follow the individual risk descriptions (which depend on the cloud provider tags in the model).

Elevated: **Missing Hardening**: 4 / 4 Risks - Exploitation likelihood is *Likely* with *Medium* impact.
Try to apply all hardening best practices (like CIS benchmarks, OWASP recommendations, vendor recommendations, DevSec Hardening Framework, DBSAT for Oracle databases, and others).

Medium: **Container Base Image Backdooring**: 5 / 5 Risks - Exploitation likelihood is *Unlikely* with *High* impact.
Apply hardening of all container infrastructures (see for example the *CIS-Benchmarks for Docker and Kubernetes* and the *Docker Bench for Security*). Use only trusted base images of the original vendors, verify digital signatures and apply image creation best practices. Also consider using Google's *Distroless* base images or otherwise very small base images. Regularly execute container image scans with tools checking the layers for vulnerable components.

Medium: **Container Platform Escape**: 4 / 4 Risks - Exploitation likelihood is *Unlikely* with *High* impact.
Apply hardening of all container infrastructures.

Medium: **DoS-risky Access Across Trust-Boundary**: 0 / 4 Risks - Exploitation likelihood is *Unlikely* with *Medium* impact.
Apply anti-DoS techniques like throttling and/or per-client load blocking with quotas. Also for maintenance access routes consider applying a VPN instead of public reachable interfaces. Generally applying redundancy on the targeted technical asset reduces the risk of DoS.

Medium: **Unencrypted Communication**: 8 / 8 Risks - Exploitation likelihood is *Unlikely* with *High* impact.
Apply transport layer encryption to the communication link.

Medium: **Unencrypted Technical Assets**: 5 / 5 Risks - Exploitation likelihood is *Unlikely* with *High* impact.
Apply encryption to the technical asset.

RAA Analysis

For each technical asset the **"Relative Attacker Attractiveness"** (RAA) value was calculated in percent. The higher the RAA, the more interesting it is for an attacker to compromise the asset. The calculation algorithm takes the sensitivity ratings and quantities of stored and processed data into account as well as the communication links of the technical asset. Neighbouring assets to high-value RAA targets might receive an increase in their RAA value when they have a communication link towards that target ("Pivoting-Factor").

The following lists all technical assets sorted by their RAA value from highest (most attacker attractive) to lowest. This list can be used to prioritize on efforts relevant for the most attacker-attractive technical assets:
Technical asset paragraphs are clickable and link to the corresponding chapter.

Order Service: RAA 100%
Manages order creation, status, and tracking.

Inventory Service: RAA 100%
Handles product catalog, stock levels, and pricing.

User Service: RAA 81%
Manages user authentication, profile, and session management.

Payment Service: RAA 55%
Integrates with external payment gateways (e.g., Stripe, PayPal) for payment processing.

Database cluster: RAA 27%
The database

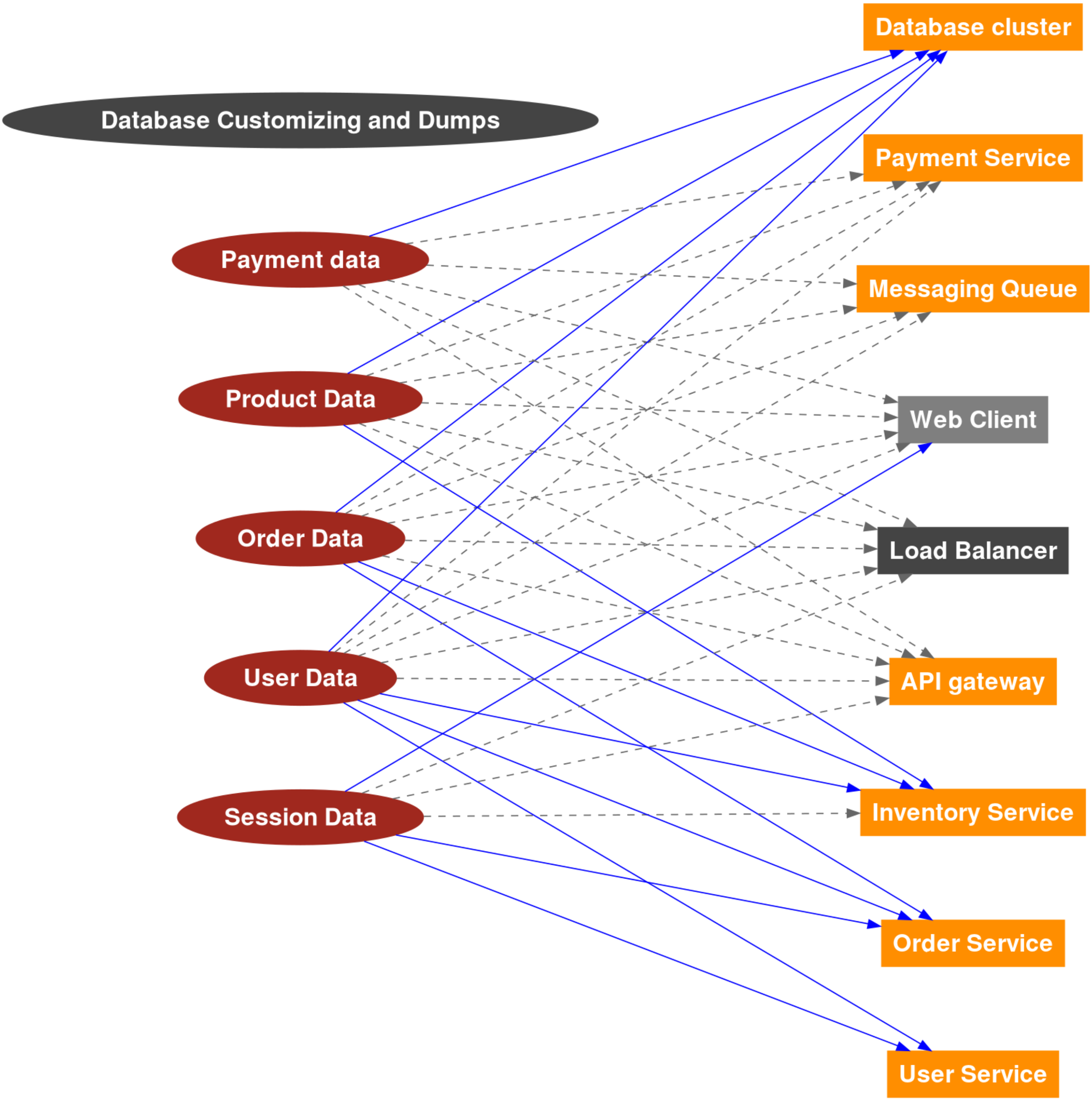
API gateway: RAA 12%
API gateway

Messaging Queue: RAA 9%
Used for communication between microservices

Load Balancer: RAA 3%
Load Balancer

Data Mapping

The following diagram was generated by Threagile based on the model input and gives a high-level distribution of data assets across technical assets. The color matches the identified data breach probability and risk level (see the "Data Breach Probabilities" chapter for more details). A solid line stands for *data is stored by the asset* and a dashed one means *data is processed by the asset*. For a full high-resolution version of this diagram please refer to the PNG image file alongside this report.



Out-of-Scope Assets: 1 Asset

This chapter lists all technical assets that have been defined as out-of-scope. Each one should be checked in the model whether it should better be included in the overall risk analysis:

Technical asset paragraphs are clickable and link to the corresponding chapter.

Web Client: out-of-scope
Owned and managed by enduser customer

Potential Model Failures: 18 / 18 Risks

This chapter lists potential model failures where not all relevant assets have been modeled or the model might itself contain inconsistencies. Each potential model failure should be checked in the model against the architecture design:

Risk finding paragraphs are clickable and link to the corresponding chapter.

Medium: **Missing Build Infrastructure**: 1 / 1 Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.

The modeled architecture does not contain a build infrastructure (devops-client, sourcecode-repo, build-pipeline, etc.), which might be the risk of a model missing critical assets (and thus not seeing their risks). If the architecture contains custom-developed parts, the pipeline where code gets developed and built needs to be part of the model.

Medium: **Missing Identity Store**: 1 / 1 Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.

The modeled architecture does not contain an identity store, which might be the risk of a model missing critical assets (and thus not seeing their risks).

Medium: **Missing Vault (Secret Storage)**: 1 / 1 Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.

In order to avoid the risk of secret leakage via config files (when attacked through vulnerabilities being able to read files like Path-Traversal and others), it is best practice to use a separate hardened process with proper authentication, authorization, and audit logging to access config secrets (like credentials, private keys, client certificates, etc.). This component is usually some kind of Vault.

Medium: **Unnecessary Data Transfer**: 7 / 7 Risks - Exploitation likelihood is *Unlikely* with *Medium* impact.

When a technical asset sends or receives data assets, which it neither processes or stores this is an indicator for unnecessarily transferred data (or for an incomplete model). When the unnecessarily transferred data assets are sensitive, this poses an unnecessary risk of an increased attack surface.

Low: **Unnecessary Data Asset**: 1 / 1 Risk - Exploitation likelihood is *Unlikely* with *Low* impact.

When a data asset is not processed or stored by any data assets and also not transferred by any communication links, this is an indicator for an unnecessary data asset (or for an incomplete model).

Low: **Wrong Communication Link Content**: 7 / 7 Risks - Exploitation likelihood is *Unlikely* with *Low* impact.

When a communication link is defined as readonly, but does not receive any data asset, or when it is defined as not readonly, but does not send any data asset, it is likely to be a model failure.

Questions: 1 / 3 Questions

This chapter lists custom questions that arose during the threat modeling process.

How are the admin clients managed/protected against compromise?
- answer pending -

How are the build pipeline components managed/protected against compromise?
Managed by XYZ

How are the development clients managed/protected against compromise?
Managed by XYZ

Identified Risks by Vulnerability Category

In total **83 potential risks** have been identified during the threat modeling process of which **0 are rated as critical**, **0 as high**, **33 as elevated**, **38 as medium**, and **12 as low**.

These risks are distributed across **17 vulnerability categories**. The following sub-chapters of this section describe each identified risk category.

Missing Cloud Hardening: 7 / 7 Risks

Description (Tampering): CWE 1008

Cloud components should be hardened according to the cloud vendor best practices. This affects their configuration, auditing, and further areas.

Impact

If this risk is unmitigated, attackers might access cloud components in an unintended way.

Detection Logic

In-scope cloud components (either residing in cloud trust boundaries or more specifically tagged with cloud provider types).

Risk Rating

The risk rating depends on the sensitivity of the technical asset itself and of the data assets processed and stored.

False Positives

Cloud components not running parts of the target architecture can be considered as false positives after individual review.

Mitigation (Operations): Cloud Hardening

Apply hardening of all cloud components and services, taking special care to follow the individual risk descriptions (which depend on the cloud provider tags in the model).

For **Amazon Web Services (AWS)**: Follow the *CIS Benchmark for Amazon Web Services* (see also the automated checks of cloud audit tools like *"PacBot", "CloudSploit", "CloudMapper", "ScoutSuite", or "Prowler AWS CIS Benchmark Tool"*).
For EC2 and other servers running Amazon Linux, follow the *CIS Benchmark for Amazon Linux* and switch to IMDSv2.
For S3 buckets follow the *Security Best Practices for Amazon S3* at https://docs.aws.amazon.com/AmazonS3/latest/dev/security-best-practices.html to avoid accidental leakage.
Also take a look at some of these tools: https://github.com/toniblyx/my-arsenal-of-aws-security-tools

For **Microsoft Azure**: Follow the *CIS Benchmark for Microsoft Azure* (see also the automated checks of cloud audit tools like *"CloudSploit" or "ScoutSuite"*).

For **Google Cloud Platform**: Follow the *CIS Benchmark for Google Cloud Computing Platform* (see also the automated checks of cloud audit tools like *"CloudSploit" or "ScoutSuite"*).

For **Oracle Cloud Platform**: Follow the hardening best practices (see also the automated checks of cloud audit tools like *"CloudSploit"*).

ASVS Chapter: V1 - Architecture, Design and Threat Modeling Requirements
Cheat Sheet: Attack_Surface_Analysis_Cheat_Sheet

Check

Are recommendations from the linked cheat sheet and referenced ASVS chapter applied?

Risk Findings

The risk **Missing Cloud Hardening** was found **7 times** in the analyzed architecture to be potentially possible. Each spot should be checked individually by reviewing the implementation whether all controls have been applied properly in order to mitigate each risk.

Risk finding paragraphs are clickable and link to the corresponding chapter.

Elevated Risk Severity

Missing Cloud Hardening (AWS) risk at **Application Network**: CIS Benchmark for AWS: Exploitation likelihood is *Unlikely* with *Very High* impact.

missing-cloud-hardening@application-network

Unchecked

Missing Cloud Hardening (EC2) risk at **Inventory Service**: CIS Benchmark for Amazon Linux: Exploitation likelihood is *Unlikely* with *Very High* impact.

missing-cloud-hardening@inventory-service

Unchecked

Missing Cloud Hardening (EC2) risk at **Messaging Queue**: CIS Benchmark for Amazon Linux: Exploitation likelihood is *Unlikely* with *Very High* impact.

missing-cloud-hardening@message-queue

Unchecked

Missing Cloud Hardening (EC2) risk at **Order Service**: CIS Benchmark for Amazon Linux: Exploitation likelihood is *Unlikely* with *Very High* impact.

missing-cloud-hardening@order-service

Unchecked

Missing Cloud Hardening (EC2) risk at **Payment Service**: CIS Benchmark for Amazon Linux : Exploitation likelihood is *Unlikely* with *Very High* impact.

missing-cloud-hardening@payment-service

Unchecked

Missing Cloud Hardening (EC2) risk at **User Service**: CIS Benchmark for Amazon Linux: Exploitation likelihood is *Unlikely* with *Very High* impact.

missing-cloud-hardening@user-service

Unchecked

Missing Cloud Hardening risk at **Cluster Group**: Exploitation likelihood is *Unlikely* with *Very High* impact.

missing-cloud-hardening@cluster-group

Unchecked

Missing Hardening: 4 / 4 Risks

Description (Tampering): CWE 16

Technical assets with a Relative Attacker Attractiveness (RAA) value of 55 % or higher should be explicitly hardened taking best practices and vendor hardening guides into account.

Impact

If this risk remains unmitigated, attackers might be able to easier attack high-value targets.

Detection Logic

In-scope technical assets with RAA values of 55 % or higher. Generally for high-value targets like datastores, application servers, identity providers and ERP systems this limit is reduced to 40 %

Risk Rating

The risk rating depends on the sensitivity of the data processed or stored in the technical asset.

False Positives

Usually no false positives.

Mitigation (Operations): System Hardening

Try to apply all hardening best practices (like CIS benchmarks, OWASP recommendations, vendor recommendations, DevSec Hardening Framework, DBSAT for Oracle databases, and others).

ASVS Chapter: V14 - Configuration Verification Requirements
Cheat Sheet: Attack_Surface_Analysis_Cheat_Sheet

Check

Are recommendations from the linked cheat sheet and referenced ASVS chapter applied?

Risk Findings

The risk **Missing Hardening** was found **4 times** in the analyzed architecture to be potentially possible. Each spot should be checked individually by reviewing the implementation whether all controls have been applied properly in order to mitigate each risk.

Risk finding paragraphs are clickable and link to the corresponding chapter.

Elevated Risk Severity

Missing Hardening risk at **Inventory Service**: Exploitation likelihood is *Likely* with *Medium* impact.

missing-hardening@inventory-service

Unchecked

Missing Hardening risk at **Order Service**: Exploitation likelihood is *Likely* with *Medium* impact.

missing-hardening@order-service

Unchecked

Missing Hardening risk at **Payment Service**: Exploitation likelihood is *Likely* with *Medium* impact.

missing-hardening@payment-service

Unchecked

Missing Hardening risk at **User Service**: Exploitation likelihood is *Likely* with *Medium* impact.

missing-hardening@user-service

Unchecked

SQL/NoSQL-Injection: 2 / 2 Risks

Description (Tampering): CWE 89

When a database is accessed via database access protocols SQL/NoSQL-Injection risks might arise. The risk rating depends on the sensitivity technical asset itself and of the data assets processed or stored.

Impact

If this risk is unmitigated, attackers might be able to modify SQL/NoSQL queries to steal and modify data and eventually further escalate towards a deeper system penetration via code executions.

Detection Logic

Database accessed via typical database access protocols by in-scope clients.

Risk Rating

The risk rating depends on the sensitivity of the data stored inside the database.

False Positives

Database accesses by queries not consisting of parts controllable by the caller can be considered as false positives after individual review.

Mitigation (Development): SQL/NoSQL-Injection Prevention

Try to use parameter binding to be safe from injection vulnerabilities. When a third-party product is used instead of custom developed software, check if the product applies the proper mitigation and ensure a reasonable patch-level.

ASVS Chapter: V5 - Validation, Sanitization and Encoding Verification Requirements
Cheat Sheet: SQL_Injection_Prevention_Cheat_Sheet

Check

Are recommendations from the linked cheat sheet and referenced ASVS chapter applied?

Risk Findings

The risk **SQL/NoSQL-Injection** was found **2 times** in the analyzed architecture to be potentially possible. Each spot should be checked individually by reviewing the implementation whether all controls have been applied properly in order to mitigate each risk.

Risk finding paragraphs are clickable and link to the corresponding chapter.

Elevated Risk Severity

SQL/NoSQL-Injection risk at **Messaging Queue** against database **Database cluster** via **Database communication**: Exploitation likelihood is *Likely* with *High* impact.

sql-nosql-injection@message-queue@sql-database@message-queue>database-communication

Unchecked

SQL/NoSQL-Injection risk at **Payment Service** against database **Database cluster** via **Database communication**: Exploitation likelihood is *Likely* with *High* impact.

sql-nosql-injection@payment-service@sql-database@payment-service>database-communication

Unchecked

Server-Side Request Forgery (SSRF): 19 / 19 Risks

Description (Information Disclosure): CWE 918

When a server system (i.e. not a client) is accessing other server systems via typical web protocols Server-Side Request Forgery (SSRF) or Local-File-Inclusion (LFI) or Remote-File-Inclusion (RFI) risks might arise.

Impact

If this risk is unmitigated, attackers might be able to access sensitive services or files of network-reachable components by modifying outgoing calls of affected components.

Detection Logic

In-scope non-client systems accessing (using outgoing communication links) targets with either HTTP or HTTPS protocol.

Risk Rating

The risk rating (low or medium) depends on the sensitivity of the data assets receivable via web protocols from targets within the same network trust-boundary as well on the sensitivity of the data assets receivable via web protocols from the target asset itself. Also for cloud-based environments the exploitation impact is at least medium, as cloud backend services can be attacked via SSRF.

False Positives

Servers not sending outgoing web requests can be considered as false positives after review.

Mitigation (Development): SSRF Prevention

Try to avoid constructing the outgoing target URL with caller controllable values. Alternatively use a mapping (whitelist) when accessing outgoing URLs instead of creating them including caller controllable values. When a third-party product is used instead of custom developed software, check if the product applies the proper mitigation and ensure a reasonable patch-level.

ASVS Chapter: V12 - File and Resources Verification Requirements
Cheat Sheet: Server_Side_Request_Forgery_Prevention_Cheat_Sheet

Check

Are recommendations from the linked cheat sheet and referenced ASVS chapter applied?

Risk Findings

The risk **Server-Side Request Forgery (SSRF)** was found **19 times** in the analyzed architecture to be potentially possible. Each spot should be checked individually by reviewing the implementation whether all controls have been applied properly in order to mitigate each risk.

Risk finding paragraphs are clickable and link to the corresponding chapter.

Elevated Risk Severity

Server-Side Request Forgery (SSRF) risk at **API gateway** server-side web-requesting the target **Load Balancer** via **Customer Traffic**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@api-gateway@load-balancer@api-gateway>customer-traffic

Unchecked

Server-Side Request Forgery (SSRF) risk at **Database cluster** server-side web-requesting the target **Messaging Queue** via **Messaging Queue**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@sql-database@message-queue@sql-database>messaging-queue

Unchecked

Server-Side Request Forgery (SSRF) risk at **Database cluster** server-side web-requesting the target **Payment Service** via **Payment Service Traffic**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@sql-database@payment-service@sql-database>payment-service-traffic

Unchecked

Server-Side Request Forgery (SSRF) risk at **Inventory Service** server-side web-requesting the target **Load Balancer** via **Inventory Traffic**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@inventory-service@load-balancer@inventory-service>inventory-traffic

Unchecked

Server-Side Request Forgery (SSRF) risk at **Inventory Service** server-side web-requesting the target **Messaging Queue** via **Messaging Queue**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@inventory-service@message-queue@inventory-service>messaging-queue

Unchecked

Server-Side Request Forgery (SSRF) risk at **Inventory Service** server-side web-requesting the target **Payment Service** via **Payment Service Traffic**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@inventory-service@payment-service@inventory-service>payment-service-traffic

Unchecked

Server-Side Request Forgery (SSRF) risk at **Messaging Queue** server-side web-requesting the target **Payment Service** via **Payment Service Traffic**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@message-queue@payment-service@message-queue>payment-service-traffic

Unchecked

Server-Side Request Forgery (SSRF) risk at **Order Service** server-side web-requesting the target **Load Balancer** via **Order Traffic**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@order-service@load-balancer@order-service>order-traffic

Unchecked

Server-Side Request Forgery (SSRF) risk at **Order Service** server-side web-requesting the target **Messaging Queue** via **Messaging Queue**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@order-service@message-queue@order-service>messaging-queue

Unchecked

Server-Side Request Forgery (SSRF) risk at **Order Service** server-side web-requesting the target **Payment Service** via **Payment Service Traffic**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@order-service@payment-service@order-service>payment-service-traffic

Unchecked

Server-Side Request Forgery (SSRF) risk at **Payment Service** server-side web-requesting the target **Messaging Queue** via **Messaging Queue**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@payment-service@message-queue@payment-service>messaging-queue

Unchecked

Server-Side Request Forgery (SSRF) risk at **User Service** server-side web-requesting the target **Load Balancer** via **User Traffic**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@user-service@load-balancer@user-service>user-traffic

Unchecked

Server-Side Request Forgery (SSRF) risk at **User Service** server-side web-requesting the target **Messaging Queue** via **Messaging Queue**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@user-service@message-queue@user-service>messaging-queue

Unchecked

Server-Side Request Forgery (SSRF) risk at **User Service** server-side web-requesting the target **Payment Service** via **Payment Service Traffic**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@user-service@payment-service@user-service>payment-service-traffic

Unchecked

Medium Risk Severity

Server-Side Request Forgery (SSRF) risk at **Messaging Queue** server-side web-requesting the target **Database cluster** via **Database communication**: Exploitation likelihood is *Unlikely* with *Medium* impact.

server-side-request-forgery@message-queue@sql-database@message-queue>database-communication

Unchecked

Server-Side Request Forgery (SSRF) risk at **Messaging Queue** server-side web-requesting the target **Inventory Service** via **Inventory Service Traffic**: Exploitation likelihood is *Unlikely* with *Medium* impact.

server-side-request-forgery@message-queue@inventory-service@message-queue>inventory-service-traffic

Unchecked

Server-Side Request Forgery (SSRF) risk at **Messaging Queue** server-side web-requesting the target **Order Service** via **Order Service Traffic**: Exploitation likelihood is *Unlikely* with *Medium* impact.

server-side-request-forgery@message-queue@order-service@message-queue>order-service-traffic

Unchecked

Server-Side Request Forgery (SSRF) risk at **Messaging Queue** server-side web-requesting the target **User Service** via **User Service Traffic**: Exploitation likelihood is *Unlikely* with *Medium* impact.

server-side-request-forgery@message-queue@user-service@message-queue>user-service-traffic

Unchecked

Server-Side Request Forgery (SSRF) risk at **Payment Service** server-side web-requesting the target **Database cluster** via **Database communication**: Exploitation likelihood is *Unlikely* with *Medium* impact.

server-side-request-forgery@payment-service@sql-database@payment-service>database-communication

Unchecked

Unguarded Access From Internet: 6 / 6 Risks

Description (Elevation of Privilege): CWE 501

Internet-exposed assets must be guarded by a protecting service, application, or reverse-proxy.

Impact

If this risk is unmitigated, attackers might be able to directly attack sensitive systems without any hardening components in-between due to them being directly exposed on the internet.

Detection Logic

In-scope technical assets (excluding load-balancer) with confidentiality rating of confidential (or higher) or with integrity rating of critical (or higher) when accessed directly from the internet. All web-server, web-application, reverse-proxy, waf, and gateway assets are exempted from this risk when they do not consist of custom developed code and the data-flow only consists of HTTP or FTP protocols. Access from monitoring systems as well as VPN-protected connections are exempted.

Risk Rating

The matching technical assets are at low risk. When either the confidentiality rating is strictly-confidential or the integrity rating is mission-critical, the risk-rating is considered medium. For assets with RAA values higher than 40 % the risk-rating increases.

False Positives

When other means of filtering client requests are applied equivalent of reverse-proxy, waf, or gateway components.

Mitigation (Architecture): Encapsulation of Technical Asset

Encapsulate the asset behind a guarding service, application, or reverse-proxy. For admin maintenance a bastion-host should be used as a jump-server. For file transfer a store-and-forward-host should be used as an indirect file exchange platform.

ASVS Chapter: V1 - Architecture, Design and Threat Modeling Requirements
Cheat Sheet: Attack_Surface_Analysis_Cheat_Sheet

Check

Are recommendations from the linked cheat sheet and referenced ASVS chapter applied?

Risk Findings

The risk **Unguarded Access From Internet** was found **6 times** in the analyzed architecture to be potentially possible. Each spot should be checked individually by reviewing the implementation whether all controls have been applied properly in order to mitigate each risk.

Risk finding paragraphs are clickable and link to the corresponding chapter.

Elevated Risk Severity

Unguarded Access from Internet of **Database cluster** by **Messaging Queue** via **Database communication**: Exploitation likelihood is *Very Likely* with *Medium* impact.

unguarded-access-from-internet@sql-database@message-queue@message-queue>database-communication

Unchecked

Unguarded Access from Internet of **Database cluster** by **Payment Service** via **Database communication**: Exploitation likelihood is *Very Likely* with *Medium* impact.

unguarded-access-from-internet@sql-database@payment-service@payment-service>database-communication

Unchecked

Unguarded Access from Internet of **Inventory Service** by **Messaging Queue** via **Inventory Service Traffic**: Exploitation likelihood is *Very Likely* with *Medium* impact.

unguarded-access-from-internet@inventory-service@message-queue@message-queue>inventory-service-traffic

Unchecked

Unguarded Access from Internet of **Order Service** by **Messaging Queue** via **Order Service Traffic**: Exploitation likelihood is *Very Likely* with *Medium* impact.

unguarded-access-from-internet@order-service@message-queue@message-queue>order-service-traffic

Unchecked

Unguarded Access from Internet of **Payment Service** by **Messaging Queue** via **Payment Service Traffic**: Exploitation likelihood is *Very Likely* with *Medium* impact.

unguarded-access-from-internet@payment-service@message-queue@message-queue>payment-service-traffic

Unchecked

Unguarded Access from Internet of **User Service** by **Messaging Queue** via **User Service Traffic**: Exploitation likelihood is *Very Likely* with *Medium* impact.

unguarded-access-from-internet@user-service@message-queue@message-queue>user-service-traffic

Unchecked

Container Base Image Backdooring: 5 / 5 Risks

Description (Tampering): CWE 912

When a technical asset is built using container technologies, Base Image Backdooring risks might arise where base images and other layers used contain vulnerable components or backdoors.

See for example:
https://techcrunch.com/2018/06/15/tainted-crypto-mining-containers-pulled-from-docker-hub/

Impact

If this risk is unmitigated, attackers might be able to deeply persist in the target system by executing code in deployed containers.

Detection Logic

In-scope technical assets running as containers.

Risk Rating

The risk rating depends on the sensitivity of the technical asset itself and of the data assets.

False Positives

Fully trusted (i.e. reviewed and cryptographically signed or similar) base images of containers can be considered as false positives after individual review.

Mitigation (Operations): Container Infrastructure Hardening

Apply hardening of all container infrastructures (see for example the *CIS-Benchmarks for Docker and Kubernetes* and the *Docker Bench for Security*). Use only trusted base images of the original vendors, verify digital signatures and apply image creation best practices. Also consider using Google's *Distroless* base images or otherwise very small base images. Regularly execute container image scans with tools checking the layers for vulnerable components.

ASVS Chapter: V10 - Malicious Code Verification Requirements
Cheat Sheet: Docker_Security_Cheat_Sheet

Check

Are recommendations from the linked cheat sheet and referenced ASVS/CSVS applied?

Risk Findings

The risk **Container Base Image Backdooring** was found **5 times** in the analyzed architecture to be potentially possible. Each spot should be checked individually by reviewing the implementation whether all controls have been applied properly in order to mitigate each risk.

Risk finding paragraphs are clickable and link to the corresponding chapter.

Medium Risk Severity

Container Base Image Backdooring risk at **Inventory Service**: Exploitation likelihood is *Unlikely* with *High* impact.

container-baseimage-backdooring@inventory-service

Unchecked

Container Base Image Backdooring risk at **Messaging Queue**: Exploitation likelihood is *Unlikely* with *High* impact.

container-baseimage-backdooring@message-queue

Unchecked

Container Base Image Backdooring risk at **Order Service**: Exploitation likelihood is *Unlikely* with *High* impact.

container-baseimage-backdooring@order-service

Unchecked

Container Base Image Backdooring risk at **Payment Service**: Exploitation likelihood is *Unlikely* with *High* impact.

container-baseimage-backdooring@payment-service

Unchecked

Container Base Image Backdooring risk at **User Service**: Exploitation likelihood is *Unlikely* with *High* impact.

container-baseimage-backdooring@user-service

Unchecked

Container Platform Escape: 4 / 4 Risks

Description (Elevation of Privilege): CWE 1008

Container platforms are especially interesting targets for attackers as they host big parts of a containerized runtime infrastructure. When not configured and operated with security best practices in mind, attackers might exploit a vulnerability inside an container and escape towards the platform as highly privileged users. These scenarios might give attackers capabilities to attack every other container as owning the container platform (via container escape attacks) equals to owning every container.

Impact

If this risk is unmitigated, attackers which have successfully compromised a container (via other vulnerabilities) might be able to deeply persist in the target system by executing code in many deployed containers and the container platform itself.

Detection Logic

In-scope container platforms.

Risk Rating

The risk rating depends on the sensitivity of the technical asset itself and of the data assets processed and stored.

False Positives

Container platforms not running parts of the target architecture can be considered as false positives after individual review.

Mitigation (Operations): Container Infrastructure Hardening

Apply hardening of all container infrastructures. See for example the *CIS-Benchmarks for Docker and Kubernetes* as well as the *Docker Bench for Security* (https://github.com/docker/docker-bench-security) or *InSpec Checks for Docker and Kubernetes* (https://github.com/dev-sec/cis-docker-benchmark and https://github.com/dev-sec/cis-kubernetes-benchmark). Use only trusted base images, verify digital signatures and apply image creation best practices. Also consider using Google's **Distroless base images or otherwise very small base images. Apply namespace isolation and nod affinity to separate pods from each other in terms of access and nodes the same style as you separate data.**

ASVS Chapter: V14 - Configuration Verification Requirements
Cheat Sheet: Docker_Security_Cheat_Sheet

Check

Are recommendations from the linked cheat sheet and referenced ASVS or CSVS chapter applied?

Risk Findings

The risk **Container Platform Escape** was found **4 times** in the analyzed architecture to be potentially possible. Each spot should be checked individually by reviewing the implementation whether all controls have been applied properly in order to mitigate each risk.

Risk finding paragraphs are clickable and link to the corresponding chapter.

Medium Risk Severity

Container Platform Escape risk at **Inventory Service**: Exploitation likelihood is *Unlikely* with *High* impact.

container-platform-escape@inventory-service

Unchecked

Container Platform Escape risk at **Order Service**: Exploitation likelihood is *Unlikely* with *High* impact.

container-platform-escape@order-service

Unchecked

Container Platform Escape risk at **Payment Service**: Exploitation likelihood is *Unlikely* with *High* impact.

container-platform-escape@payment-service

Unchecked

Container Platform Escape risk at **User Service**: Exploitation likelihood is *Unlikely* with *High* impact.

container-platform-escape@user-service

Unchecked

Missing Build Infrastructure: 1 / 1 Risk

Description (Tampering): CWE 1127

The modeled architecture does not contain a build infrastructure (devops-client, sourcecode-repo, build-pipeline, etc.), which might be the risk of a model missing critical assets (and thus not seeing their risks). If the architecture contains custom-developed parts, the pipeline where code gets developed and built needs to be part of the model.

Impact

If this risk is unmitigated, attackers might be able to exploit risks unseen in this threat model due to critical build infrastructure components missing in the model.

Detection Logic

Models with in-scope custom-developed parts missing in-scope development (code creation) and build infrastructure components (devops-client, sourcecode-repo, build-pipeline, etc.).

Risk Rating

The risk rating depends on the highest sensitivity of the in-scope assets running custom-developed parts.

False Positives

Models not having any custom-developed parts can be considered as false positives after individual review.

Mitigation (Architecture): Build Pipeline Hardening

Include the build infrastructure in the model.

ASVS Chapter: V1 - Architecture, Design and Threat Modeling Requirements
Cheat Sheet: Attack_Surface_Analysis_Cheat_Sheet

Check

Are recommendations from the linked cheat sheet and referenced ASVS chapter applied?

Risk Findings

The risk **Missing Build Infrastructure** was found **1 time** in the analyzed architecture to be potentially possible. Each spot should be checked individually by reviewing the implementation whether all controls have been applied properly in order to mitigate each risk.

Risk finding paragraphs are clickable and link to the corresponding chapter.

Medium Risk Severity

Missing Build Infrastructure in the threat model (referencing asset **Order Service** as an example): Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-build-infrastructure@order-service

Unchecked

Missing Identity Store: 1 / 1 Risk

Description (Spoofing): CWE 287

The modeled architecture does not contain an identity store, which might be the risk of a model missing critical assets (and thus not seeing their risks).

Impact

If this risk is unmitigated, attackers might be able to exploit risks unseen in this threat model in the identity provider/store that is currently missing in the model.

Detection Logic

Models with authenticated data-flows authorized via enduser-identity missing an in-scope identity store.

Risk Rating

The risk rating depends on the sensitivity of the enduser-identity authorized technical assets and their data assets processed and stored.

False Positives

Models only offering data/services without any real authentication need can be considered as false positives after individual review.

Mitigation (Architecture): Identity Store

Include an identity store in the model if the application has a login.

ASVS Chapter: V2 - Authentication Verification Requirements
Cheat Sheet: Authentication_Cheat_Sheet

Check

Are recommendations from the linked cheat sheet and referenced ASVS chapter applied?

Risk Findings

The risk **Missing Identity Store** was found **1 time** in the analyzed architecture to be potentially possible. Each spot should be checked individually by reviewing the implementation whether all controls have been applied properly in order to mitigate each risk.

Risk finding paragraphs are clickable and link to the corresponding chapter.

Medium Risk Severity

Missing Identity Store in the threat model (referencing asset **Order Service** as an example): Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-identity-store@order-service

Unchecked

Missing Vault (Secret Storage): 1 / 1 Risk

Description (Information Disclosure): CWE 522

In order to avoid the risk of secret leakage via config files (when attacked through vulnerabilities being able to read files like Path-Traversal and others), it is best practice to use a separate hardened process with proper authentication, authorization, and audit logging to access config secrets (like credentials, private keys, client certificates, etc.). This component is usually some kind of Vault.

Impact

If this risk is unmitigated, attackers might be able to easier steal config secrets (like credentials, private keys, client certificates, etc.) once a vulnerability to access files is present and exploited.

Detection Logic

Models without a Vault (Secret Storage).

Risk Rating

The risk rating depends on the sensitivity of the technical asset itself and of the data assets processed and stored.

False Positives

Models where no technical assets have any kind of sensitive config data to protect can be considered as false positives after individual review.

Mitigation (Architecture): Vault (Secret Storage)

Consider using a Vault (Secret Storage) to securely store and access config secrets (like credentials, private keys, client certificates, etc.).

ASVS Chapter: V6 - Stored Cryptography Verification Requirements
Cheat Sheet: Cryptographic_Storage_Cheat_Sheet

Check

Is a Vault (Secret Storage) in place?

Risk Findings

The risk **Missing Vault (Secret Storage)** was found **1 time** in the analyzed architecture to be potentially possible. Each spot should be checked individually by reviewing the implementation whether all controls have been applied properly in order to mitigate each risk.

Risk finding paragraphs are clickable and link to the corresponding chapter.

Medium Risk Severity

Missing Vault (Secret Storage) in the threat model (referencing asset **Database cluster** as an example): Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-vault@sql-database

Unchecked

Unencrypted Communication: 8 / 8 Risks

Description (Information Disclosure): CWE 319

Due to the confidentiality and/or integrity rating of the data assets transferred over the communication link this connection must be encrypted.

Impact

If this risk is unmitigated, network attackers might be able to to eavesdrop on unencrypted sensitive data sent between components.

Detection Logic

Unencrypted technical communication links of in-scope technical assets (excluding monitoring traffic as well as local-file-access and in-process-library-call) transferring sensitive data.

Risk Rating

Depending on the confidentiality rating of the transferred data-assets either medium or high risk.

False Positives

When all sensitive data sent over the communication link is already fully encrypted on document or data level. Also intra-container/pod communication can be considered false positive when container orchestration platform handles encryption.

Mitigation (Operations): Encryption of Communication Links

Apply transport layer encryption to the communication link.

ASVS Chapter: V9 - Communication Verification Requirements
Cheat Sheet: Transport_Layer_Protection_Cheat_Sheet

Check

Are recommendations from the linked cheat sheet and referenced ASVS chapter applied?

Risk Findings

The risk **Unencrypted Communication** was found **8 times** in the analyzed architecture to be potentially possible. Each spot should be checked individually by reviewing the implementation whether all controls have been applied properly in order to mitigate each risk.

Risk finding paragraphs are clickable and link to the corresponding chapter.

Medium Risk Severity

Unencrypted Communication named **Database communication** between **Messaging Queue** and **Database cluster** transferring authentication data (like credentials, token, session-id, etc.): Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-communication@message-queue>database-communication@message-queue@sql-database

Unchecked

Unencrypted Communication named **Messaging Queue** between **Database cluster** and **Messaging Queue** transferring authentication data (like credentials, token, session-id, etc.): Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-communication@sql-database>messaging-queue@sql-database@message-queue

Unchecked

Unencrypted Communication named **Messaging Queue** between **Inventory Service** and **Messaging Queue** transferring authentication data (like credentials, token, session-id, etc.): Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-communication@inventory-service>messaging-queue@inventory-service@message-queue

Unchecked

Unencrypted Communication named **Messaging Queue** between **Order Service** and **Messaging Queue** transferring authentication data (like credentials, token, session-id, etc.): Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-communication@order-service>messaging-queue@order-service@message-queue

Unchecked

Unencrypted Communication named **Messaging Queue** between **Payment Service** and **Messaging Queue** transferring authentication data (like credentials, token, session-id, etc.): Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-communication@payment-service>messaging-queue@payment-service@message-queue

Unchecked

Unencrypted Communication named **Order Service Traffic** between **Messaging Queue** and **Order Service** transferring authentication data (like credentials, token, session-id, etc.): Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-communication@message-queue>order-service-traffic@message-queue@order-service

Unchecked

Unencrypted Communication named **Payment Service Traffic** between **User Service** and **Payment Service** transferring authentication data (like credentials, token, session-id, etc.): Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-communication@user-service>payment-service-traffic@user-service@payment-service

Unchecked

Unencrypted Communication named **User Service Traffic** between **Messaging Queue** and **User Service** transferring authentication data (like credentials, token, session-id, etc.): Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-communication@message-queue>user-service-traffic@message-queue@user-service

Unchecked

Unencrypted Technical Assets: 5 / 5 Risks

Description (Information Disclosure): CWE 311

Due to the confidentiality rating of the technical asset itself and/or the processed data assets this technical asset must be encrypted. The risk rating depends on the sensitivity technical asset itself and of the data assets stored.

Impact

If this risk is unmitigated, attackers might be able to access unencrypted data when successfully compromising sensitive components.

Detection Logic

In-scope unencrypted technical assets (excluding reverse-proxy, load-balancer, waf, ids, ips and embedded components like library) storing data assets rated at least as confidential or critical. For technical assets storing data assets rated as strictly-confidential or mission-critical the encryption must be of type data-with-enduser-individual-key.

Risk Rating

Depending on the confidentiality rating of the stored data-assets either medium or high risk.

False Positives

When all sensitive data stored within the asset is already fully encrypted on document or data level.

Mitigation (Operations): Encryption of Technical Asset

Apply encryption to the technical asset.

ASVS Chapter: V6 - Stored Cryptography Verification Requirements
Cheat Sheet: Cryptographic_Storage_Cheat_Sheet

Check

Are recommendations from the linked cheat sheet and referenced ASVS chapter applied?

Risk Findings

The risk **Unencrypted Technical Assets** was found **5 times** in the analyzed architecture to be potentially possible. Each spot should be checked individually by reviewing the implementation whether all controls have been applied properly in order to mitigate each risk.

Risk finding paragraphs are clickable and link to the corresponding chapter.

Medium Risk Severity

Unencrypted Technical Asset named **Inventory Service**: Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-asset@inventory-service

Unchecked

Unencrypted Technical Asset named **Order Service**: Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-asset@order-service

Unchecked

Unencrypted Technical Asset named **User Service**: Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-asset@user-service

Unchecked

Unencrypted Technical Asset named **Database cluster** missing enduser-individual encryption with data-with-enduser-individual-key: Exploitation likelihood is *Unlikely* with *Medium* impact.

unencrypted-asset@sql-database

Unchecked

Unencrypted Technical Asset named **Messaging Queue** missing enduser-individual encryption with data-with-enduser-individual-key: Exploitation likelihood is *Unlikely* with *Medium* impact.

unencrypted-asset@message-queue

Unchecked

Unnecessary Data Transfer: 7 / 7 Risks

Description (Elevation of Privilege): CWE 1008

When a technical asset sends or receives data assets, which it neither processes or stores this is an indicator for unnecessarily transferred data (or for an incomplete model). When the unnecessarily transferred data assets are sensitive, this poses an unnecessary risk of an increased attack surface.

Impact

If this risk is unmitigated, attackers might be able to target unnecessarily transferred data.

Detection Logic

In-scope technical assets sending or receiving sensitive data assets which are neither processed nor stored by the technical asset are flagged with this risk. The risk rating (low or medium) depends on the confidentiality, integrity, and availability rating of the technical asset. Monitoring data is exempted from this risk.

Risk Rating

The risk assessment is depending on the confidentiality and integrity rating of the transferred data asset either low or medium.

False Positives

Technical assets missing the model entries of either processing or storing the mentioned data assets can be considered as false positives (incomplete models) after individual review. These should then be addressed by completing the model so that all necessary data assets are processed and/or stored by the technical asset involved.

Mitigation (Architecture): Attack Surface Reduction

Try to avoid sending or receiving sensitive data assets which are not required (i.e. neither processed or stored) by the involved technical asset.

ASVS Chapter: V1 - Architecture, Design and Threat Modeling Requirements
Cheat Sheet: Attack_Surface_Analysis_Cheat_Sheet

Check

Are recommendations from the linked cheat sheet and referenced ASVS chapter applied?

Risk Findings

The risk **Unnecessary Data Transfer** was found **7 times** in the analyzed architecture to be potentially possible. Each spot should be checked individually by reviewing the implementation whether all controls have been applied properly in order to mitigate each risk.
Risk finding paragraphs are clickable and link to the corresponding chapter.

Medium Risk Severity

Unnecessary Data Transfer of **Payment data** data at **Inventory Service** from/to **Payment Service**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@payment-data@inventory-service@payment-service

Unchecked

Unnecessary Data Transfer of **Payment data** data at **Order Service** from/to **Payment Service**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@payment-data@order-service@payment-service

Unchecked

Unnecessary Data Transfer of **Payment data** data at **User Service** from/to **Messaging Queue**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@payment-data@user-service@message-queue

Unchecked

Unnecessary Data Transfer of **Payment data** data at **User Service** from/to **Payment Service**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@payment-data@user-service@payment-service

Unchecked

Unnecessary Data Transfer of **Session Data** data at **Database cluster** from/to **Payment Service**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@session-data@sql-database@payment-service

Unchecked

Unnecessary Data Transfer of **Session Data** data at **Payment Service** from/to **Database cluster**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@session-data@payment-service@sql-database

Unchecked

Low Risk Severity

Unnecessary Data Transfer of **Product Data** data at **Order Service** from/to **Load Balancer**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@product-data@order-service@load-balancer

Unchecked

Unnecessary Data Asset: 1 / 1 Risk

Description (Elevation of Privilege): CWE 1008

When a data asset is not processed or stored by any data assets and also not transferred by any communication links, this is an indicator for an unnecessary data asset (or for an incomplete model).

Impact

If this risk is unmitigated, attackers might be able to access unnecessary data assets using other vulnerabilities.

Detection Logic

Modelled data assets not processed or stored by any data assets and also not transferred by any communication links.

Risk Rating

low

False Positives

Usually no false positives as this looks like an incomplete model.

Mitigation (Architecture): Attack Surface Reduction

Try to avoid having data assets that are not required/used.

ASVS Chapter: V1 - Architecture, Design and Threat Modeling Requirements
Cheat Sheet: Attack_Surface_Analysis_Cheat_Sheet

Check

Are recommendations from the linked cheat sheet and referenced ASVS chapter applied?

Risk Findings

The risk **Unnecessary Data Asset** was found **1 time** in the analyzed architecture to be potentially possible. Each spot should be checked individually by reviewing the implementation whether all controls have been applied properly in order to mitigate each risk.

Risk finding paragraphs are clickable and link to the corresponding chapter.

Low Risk Severity

Unnecessary Data Asset named **Database Customizing and Dumps**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-asset@db-dumps

Unchecked

Wrong Communication Link Content: 7 / 7 Risks

Description (Information Disclosure): CWE 1008

When a communication link is defined as readonly, but does not receive any data asset, or when it is defined as not readonly, but does not send any data asset, it is likely to be a model failure.

Impact

If this potential model error is not fixed, some risks might not be visible.

Detection Logic

Communication links with inconsistent data assets being sent/received not matching their readonly flag or otherwise inconsistent protocols not matching the target technology type.

Risk Rating

low

False Positives

Usually no false positives as this looks like an incomplete model.

Mitigation (Architecture): Model Consistency

Try to model the correct readonly flag and/or data sent/received of communication links. Also try to use communication link types matching the target technology/machine types.

ASVS Chapter: V1 - Architecture, Design and Threat Modeling Requirements
Cheat Sheet: Threat_Modeling_Cheat_Sheet

Check

Are recommendations from the linked cheat sheet and referenced ASVS chapter applied?

Risk Findings

The risk **Wrong Communication Link Content** was found **7 times** in the analyzed architecture to be potentially possible. Each spot should be checked individually by reviewing the implementation whether all controls have been applied properly in order to mitigate each risk.
Risk finding paragraphs are clickable and link to the corresponding chapter.

Low Risk Severity

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **Inventory Service** regarding communication link **Payment Service Traffic**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@inventory-service@inventory-service>payment-service-traffic

Unchecked

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **Messaging Queue** regarding communication link **Inventory Service Traffic**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@message-queue@message-queue>inventory-service-traffic

Unchecked

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **Messaging Queue** regarding communication link **Order Service Traffic**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@message-queue@message-queue>order-service-traffic

Unchecked

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **Messaging Queue** regarding communication link **Payment Service Traffic**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@message-queue@message-queue>payment-service-traffic

Unchecked

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **Messaging Queue** regarding communication link **User Service Traffic**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@message-queue@message-queue>user-service-traffic

Unchecked

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **Order Service** regarding communication link **Payment Service Traffic**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@order-service@order-service>payment-service-traffic

Unchecked

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **User Service** regarding communication link **Payment Service Traffic**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@user-service@user-service>payment-service-traffic

Unchecked

DoS-risky Access Across Trust-Boundary: 0 / 4 Risks

Description (Denial of Service): CWE 400

Assets accessed across trust boundaries with critical or mission-critical availability rating are more prone to Denial-of-Service (DoS) risks.

Impact

If this risk remains unmitigated, attackers might be able to disturb the availability of important parts of the system.

Detection Logic

In-scope technical assets (excluding load-balancer) with availability rating of critical or higher which have incoming data-flows across a network trust-boundary (excluding devops usage).

Risk Rating

Matching technical assets with availability rating of critical or higher are at low risk. When the availability rating is mission-critical and neither a VPN nor IP filter for the incoming data-flow nor redundancy for the asset is applied, the risk-rating is considered medium.

False Positives

When the accessed target operations are not time- or resource-consuming.

Mitigation (Operations): Anti-DoS Measures

Apply anti-DoS techniques like throttling and/or per-client load blocking with quotas. Also for maintenance access routes consider applying a VPN instead of public reachable interfaces. Generally applying redundancy on the targeted technical asset reduces the risk of DoS.

ASVS Chapter: V1 - Architecture, Design and Threat Modeling Requirements
Cheat Sheet: Denial_of_Service_Cheat_Sheet

Check

Are recommendations from the linked cheat sheet and referenced ASVS chapter applied?

Risk Findings

The risk **DoS-risky Access Across Trust-Boundary** was found **4 times** in the analyzed architecture to be potentially possible. Each spot should be checked individually by reviewing the implementation whether all controls have been applied properly in order to mitigate each risk.
Risk finding paragraphs are clickable and link to the corresponding chapter.

Medium Risk Severity

Denial-of-Service risky access of **API gateway** by **Web Client** via **API gateway Traffic**: Exploitation likelihood is *Unlikely* with *Medium* impact.

dos-risky-access-across-trust-boundary@api-gateway@web-client@web-client>api-gateway-traffic

Mitigated 2025-01-04 John Doe XYZ-1234
The hardening measures are being implemented and checked. Used AWS DOS mitigation

Low Risk Severity

Denial-of-Service risky access of **Inventory Service** by **API gateway** via **Customer Traffic** forwarded via **Load Balancer**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@inventory-service@api-gateway@api-gateway>customer-traffic

Mitigated 2025-01-04 John Doe XYZ-1234
The hardening measures are being implemented and checked. Used AWS DOS mitigation

Denial-of-Service risky access of **Order Service** by **API gateway** via **Customer Traffic** forwarded via **Load Balancer**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@order-service@api-gateway@api-gateway>customer-traffic

Mitigated 2025-01-04 John Doe XYZ-1234
The hardening measures are being implemented and checked. Used AWS DOS mitigation

Denial-of-Service risky access of **User Service** by **API gateway** via **Customer Traffic** forwarded via **Load Balancer**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@user-service@api-gateway@api-gateway>customer-traffic

Mitigated 2025-01-04 John Doe XYZ-1234
The hardening measures are being implemented and checked. Used AWS DOS mitigation

Missing Two-Factor Authentication (2FA): 0 / 1 Risk

Description (Elevation of Privilege): CWE 308

Technical assets (especially multi-tenant systems) should authenticate incoming requests with two-factor (2FA) authentication when the asset processes or stores highly sensitive data (in terms of confidentiality, integrity, and availability) and is accessed by humans.

Impact

If this risk is unmitigated, attackers might be able to access or modify highly sensitive data without strong authentication.

Detection Logic

In-scope technical assets (except load-balancer, reverse-proxy, waf, ids, and ips) should authenticate incoming requests via two-factor authentication (2FA) when the asset processes or stores highly sensitive data (in terms of confidentiality, integrity, and availability) and is accessed by a client used by a human user.

Risk Rating

medium

False Positives

Technical assets which do not process requests regarding functionality or data linked to end-users (customers) can be considered as false positives after individual review.

Mitigation (Business Side): Authentication with Second Factor (2FA)

Apply an authentication method to the technical asset protecting highly sensitive data via two-factor authentication for human users.

ASVS Chapter: V2 - Authentication Verification Requirements
Cheat Sheet: Multifactor_Authentication_Cheat_Sheet

Check

Are recommendations from the linked cheat sheet and referenced ASVS chapter applied?

Risk Findings

The risk **Missing Two-Factor Authentication (2FA)** was found **1 time** in the analyzed architecture to be potentially possible. Each spot should be checked individually by reviewing the implementation whether all controls have been applied properly in order to mitigate each risk.

Risk finding paragraphs are clickable and link to the corresponding chapter.

Medium Risk Severity

Missing Two-Factor Authentication covering communication link **API gateway Traffic** from **Web Client** to **API gateway**: Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-authentication-second-factor@web-client>api-gateway-traffic@web-client@api-gateway

Mitigated 2025-01-04 John Doe XYZ-1234

The hardening measures were implemented and checked

Identified Risks by Technical Asset

In total **83 potential risks** have been identified during the threat modeling process of which **0 are rated as critical**, **0 as high**, **33 as elevated**, **38 as medium**, and **12 as low**.

These risks are distributed across **8 in-scope technical assets**. The following sub-chapters of this section describe each identified risk grouped by technical asset. The RAA value of a technical asset is the calculated "Relative Attacker Attractiveness" value in percent.

API gateway: 1 / 3 Risks

Description

API gateway

Identified Risks of Asset

Risk finding paragraphs are clickable and link to the corresponding chapter.

Elevated Risk Severity

Server-Side Request Forgery (SSRF) risk at **API gateway** server-side web-requesting the target **Load Balancer** via **Customer Traffic**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@api-gateway@load-balancer@api-gateway>customer-traffic

Unchecked

Medium Risk Severity

Denial-of-Service risky access of **API gateway** by **Web Client** via **API gateway Traffic**: Exploitation likelihood is *Unlikely* with *Medium* impact.

dos-risky-access-across-trust-boundary@api-gateway@web-client@web-client>api-gateway-traffic

Mitigated 2025-01-04 John Doe XYZ-1234
The hardening measures are being implemented and checked. Used AWS DOS mitigation

Missing Two-Factor Authentication covering communication link **API gateway Traffic** from **Web Client** to **API gateway**: Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-authentication-second-factor@web-client>api-gateway-traffic@web-client@api-gateway

Mitigated 2025-01-04 John Doe XYZ-1234
The hardening measures were implemented and checked

Asset Information

ID:	api-gateway
Type:	process
Usage:	business
RAA:	12 %
Size:	component
Technology:	gateway
Tags:	none
Internet:	true
Machine:	virtual
Encryption:	data-with-asymmetric-shared-key

Multi-Tenant:	false
Redundant:	false
Custom-Developed:	false
Client by Human:	false
Data Processed:	Order Data, Payment data, Product Data, Session Data, User Data
Data Stored:	none
Formats Accepted:	JSON

Asset Rating

Owner:	Company XYZ	
Confidentiality:	public	(rated 1 in scale of 5)
Integrity:	critical	(rated 4 in scale of 5)
Availability:	mission-critical	(rated 5 in scale of 5)
CIA-Justification:	API gateway connects to client	

Outgoing Communication Links: 1

Target technical asset names are clickable and link to the corresponding chapter.

Customer Traffic (outgoing)

Link to the load balancer

Target:	Load Balancer
Protocol:	https
Encrypted:	true
Authentication:	session-id
Authorization:	enduser-identity-propagation
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Sent:	Order Data, Payment data, Product Data, Session Data, User Data
Data Received:	Order Data, Payment data, Product Data, Session Data, User Data

Incoming Communication Links: 1

Source technical asset names are clickable and link to the corresponding chapter.

API gateway Traffic (incoming)

Link to the API gateway

Source:	Web Client
Protocol:	https
Encrypted:	true
Authentication:	session-id
Authorization:	enduser-identity-propagation
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Received:	Order Data, Payment data, Product Data, Session Data, User Data
Data Sent:	Order Data, Payment data, Product Data, Session Data, User Data

Database cluster: 8 / 8 Risks

Description

The database

Identified Risks of Asset

Risk finding paragraphs are clickable and link to the corresponding chapter.

Elevated Risk Severity

Unguarded Access from Internet of **Database cluster** by **Messaging Queue** via **Database communication**: Exploitation likelihood is *Very Likely* with *Medium* impact.

unguarded-access-from-internet@sql-database@message-queue@message-queue>database-communication

Unchecked

Unguarded Access from Internet of **Database cluster** by **Payment Service** via **Database communication**: Exploitation likelihood is *Very Likely* with *Medium* impact.

unguarded-access-from-internet@sql-database@payment-service@payment-service>database-communication

Unchecked

Server-Side Request Forgery (SSRF) risk at **Database cluster** server-side web-requesting the target **Messaging Queue** via **Messaging Queue**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@sql-database@message-queue@sql-database>messaging-queue

Unchecked

Server-Side Request Forgery (SSRF) risk at **Database cluster** server-side web-requesting the target **Payment Service** via **Payment Service Traffic**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@sql-database@payment-service@sql-database>payment-service-traffic

Unchecked

Medium Risk Severity

Unencrypted Communication named **Messaging Queue** between **Database cluster** and **Messaging Queue** transferring authentication data (like credentials, token, session-id, etc.): Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-communication@sql-database>messaging-queue@sql-database@message-queue

Unchecked

Missing Vault (Secret Storage) in the threat model (referencing asset **Database cluster** as an example): Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-vault@sql-database

Unchecked

Unencrypted Technical Asset named **Database cluster** missing enduser-individual encryption with data-with-enduser-individual-key: Exploitation likelihood is *Unlikely* with *Medium* impact.

unencrypted-asset@sql-database

Unchecked

Unnecessary Data Transfer of **Session Data** data at **Database cluster** from/to **Payment Service**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@session-data@sql-database@payment-service

Unchecked

Asset Information

ID:	sql-database
Type:	datastore
Usage:	business
RAA:	27 %
Size:	component
Technology:	database
Tags:	aws:rds, linux, mysql
Internet:	false
Machine:	virtual
Encryption:	data-with-symmetric-shared-key
Multi-Tenant:	false
Redundant:	false
Custom-Developed:	false
Client by Human:	false
Data Processed:	Order Data, Payment data, Product Data, User Data
Data Stored:	Order Data, Payment data, Product Data, User Data
Formats Accepted:	JSON

Asset Rating

Owner:	Company XYZ	
Confidentiality:	strictly-confidential	(rated 5 in scale of 5)
Integrity:	mission-critical	(rated 5 in scale of 5)
Availability:	mission-critical	(rated 5 in scale of 5)

CIA-Justification:	The database contains business-relevant sensitive data for Company XYZ processes.

Outgoing Communication Links: 2

Target technical asset names are clickable and link to the corresponding chapter.

Payment Service Traffic (outgoing)

Link to the payment service inside cluster

Target:	Payment Service
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Sent:	Payment data
Data Received:	Payment data

Messaging Queue (outgoing)

Link

Target:	Messaging Queue
Protocol:	http
Encrypted:	false
Authentication:	token
Authorization:	technical-user
Read-Only:	true
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	false
Data Sent:	none
Data Received:	Order Data, Payment data, Product Data, User Data

Incoming Communication Links: 2

Source technical asset names are clickable and link to the corresponding chapter.

Database communication (incoming)

Link to the database

Source:	Payment Service
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	devops
Tags:	none
VPN:	false
IP-Filtered:	true
Data Received:	Order Data, Payment data, Product Data, User Data
Data Sent:	Order Data, Payment data, Product Data, Session Data, User Data

Database communication (incoming)

Link to the database (JDBC tunneled via SSH)

Source:	Messaging Queue
Protocol:	http
Encrypted:	false
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	devops
Tags:	none
VPN:	false
IP-Filtered:	true
Data Received:	Order Data, Payment data, Product Data, User Data
Data Sent:	none

Inventory Service: 12 / 13 Risks

Description

Handles product catalog, stock levels, and pricing.

Identified Risks of Asset

Risk finding paragraphs are clickable and link to the corresponding chapter.

Elevated Risk Severity

Missing Cloud Hardening (EC2) risk at **Inventory Service**: CIS Benchmark for Amazon Linux: Exploitation likelihood is *Unlikely* with *Very High* impact.

missing-cloud-hardening@inventory-service

Unchecked

Unguarded Access from Internet of **Inventory Service** by **Messaging Queue** via **Inventory Service Traffic**: Exploitation likelihood is *Very Likely* with *Medium* impact.

unguarded-access-from-internet@inventory-service@message-queue@message-queue>inventory-service-traffic

Unchecked

Missing Hardening risk at **Inventory Service**: Exploitation likelihood is *Likely* with *Medium* impact.

missing-hardening@inventory-service

Unchecked

Server-Side Request Forgery (SSRF) risk at **Inventory Service** server-side web-requesting the target **Load Balancer** via **Inventory Traffic**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@inventory-service@load-balancer@inventory-service>inventory-traffic

Unchecked

Server-Side Request Forgery (SSRF) risk at **Inventory Service** server-side web-requesting the target **Messaging Queue** via **Messaging Queue**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@inventory-service@message-queue@inventory-service>messaging-queue

Unchecked

Server-Side Request Forgery (SSRF) risk at **Inventory Service** server-side web-requesting the target **Payment Service** via **Payment Service Traffic**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@inventory-service@payment-service@inventory-service>payment-service-traffic

Unchecked

Medium Risk Severity

Container Base Image Backdooring risk at **Inventory Service**: Exploitation likelihood is *Unlikely* with *High* impact.

container-baseimage-backdooring@inventory-service

Unchecked

Container Platform Escape risk at **Inventory Service**: Exploitation likelihood is *Unlikely* with *High* impact.

container-platform-escape@inventory-service

Unchecked

Unencrypted Communication named **Messaging Queue** between **Inventory Service** and **Messaging Queue** transferring authentication data (like credentials, token, session-id, etc.): Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-communication@inventory-service>messaging-queue@inventory-service@message-queue

Unchecked

Unencrypted Technical Asset named **Inventory Service**: Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-asset@inventory-service

Unchecked

Unnecessary Data Transfer of **Payment data** data at **Inventory Service** from/to **Payment Service**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@payment-data@inventory-service@payment-service

Unchecked

Low Risk Severity

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **Inventory Service** regarding communication link **Payment Service Traffic**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@inventory-service@inventory-service>payment-service-traffic

Unchecked

Denial-of-Service risky access of **Inventory Service** by **API gateway** via **Customer Traffic** forwarded via **Load Balancer**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@inventory-service@api-gateway@api-gateway>customer-traffic

Mitigated 2025-01-04 John Doe XYZ-1234
The hardening measures are being implemented and checked. Used AWS DOS mitigation

Asset Information

ID:	inventory-service
Type:	process

Usage:	business
RAA:	100 %
Size:	service
Technology:	container-platform
Tags:	aws:ec2, linux
Internet:	false
Machine:	container
Encryption:	none
Multi-Tenant:	true
Redundant:	true
Custom-Developed:	true
Client by Human:	false
Data Processed:	Order Data, Product Data, Session Data, User Data
Data Stored:	Order Data, Product Data, User Data
Formats Accepted:	JSON

Asset Rating

Owner:	Company XYZ	
Confidentiality:	internal	(rated 2 in scale of 5)
Integrity:	mission-critical	(rated 5 in scale of 5)
Availability:	mission-critical	(rated 5 in scale of 5)
CIA-Justification:	The correct configuration and reachability of the service is mandatory for all customer usages of the Platform.	

Outgoing Communication Links: 3

Target technical asset names are clickable and link to the corresponding chapter.

Payment Service Traffic (outgoing)

Link to the payment service inside cluster

Target:	Payment Service
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	business

Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Sent:	none
Data Received:	Order Data, Payment data, Product Data

Messaging Queue (outgoing)

Link

Target:	Messaging Queue
Protocol:	http
Encrypted:	false
Authentication:	token
Authorization:	technical-user
Read-Only:	true
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	false
Data Sent:	none
Data Received:	Product Data

Inventory Traffic (outgoing)

Link to the load balancer

Target:	Load Balancer
Protocol:	https
Encrypted:	true
Authentication:	session-id
Authorization:	enduser-identity-propagation
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Sent:	Order Data, Product Data, Session Data
Data Received:	Order Data, Product Data, Session Data

Incoming Communication Links: 2

Source technical asset names are clickable and link to the corresponding chapter.

Inventory Service Traffic (incoming)

Link to the Inventory service inside cluster

Source:	Messaging Queue
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	devops
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Received:	none
Data Sent:	Product Data

Inventory Service Traffic (incoming)

Link to the Inventory service inside cluster

Source:	Load Balancer
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Received:	Product Data, Session Data, User Data
Data Sent:	Product Data, Session Data, User Data

Messaging Queue: 16 / 16 Risks

Description

Used for communication between microservices

Identified Risks of Asset

Risk finding paragraphs are clickable and link to the corresponding chapter.

Elevated Risk Severity

Missing Cloud Hardening (EC2) risk at **Messaging Queue**: CIS Benchmark for Amazon Linux: Exploitation likelihood is *Unlikely* with *Very High* impact.

missing-cloud-hardening@message-queue

Unchecked

SQL/NoSQL-Injection risk at **Messaging Queue** against database **Database cluster** via **Database communication**: Exploitation likelihood is *Likely* with *High* impact.

sql-nosql-injection@message-queue@sql-database@message-queue>database-communication

Unchecked

Server-Side Request Forgery (SSRF) risk at **Messaging Queue** server-side web-requesting the target **Payment Service** via **Payment Service Traffic**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@message-queue@payment-service@message-queue>payment-service-traffic

Unchecked

Medium Risk Severity

Container Base Image Backdooring risk at **Messaging Queue**: Exploitation likelihood is *Unlikely* with *High* impact.

container-baseimage-backdooring@message-queue

Unchecked

Unencrypted Communication named **Database communication** between **Messaging Queue** and **Database cluster** transferring authentication data (like credentials, token, session-id, etc.): Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-communication@message-queue>database-communication@message-queue@sql-database

Unchecked

Unencrypted Communication named **Order Service Traffic** between **Messaging Queue** and **Order Service** transferring authentication data (like credentials, token, session-id, etc.): Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-communication@message-queue>order-service-traffic@message-queue@order-service

Unchecked

Unencrypted Communication named **User Service Traffic** between **Messaging Queue** and **User Service** transferring authentication data (like credentials, token, session-id, etc.): Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-communication@message-queue>user-service-traffic@message-queue@user-service

Unchecked

Server-Side Request Forgery (SSRF) risk at **Messaging Queue** server-side web-requesting the target **Database cluster** via **Database communication**: Exploitation likelihood is *Unlikely* with *Medium* impact.

server-side-request-forgery@message-queue@sql-database@message-queue>database-communication

Unchecked

Server-Side Request Forgery (SSRF) risk at **Messaging Queue** server-side web-requesting the target **Inventory Service** via **Inventory Service Traffic**: Exploitation likelihood is *Unlikely* with *Medium* impact.

server-side-request-forgery@message-queue@inventory-service@message-queue>inventory-service-traffic

Unchecked

Server-Side Request Forgery (SSRF) risk at **Messaging Queue** server-side web-requesting the target **Order Service** via **Order Service Traffic**: Exploitation likelihood is *Unlikely* with *Medium* impact.

server-side-request-forgery@message-queue@order-service@message-queue>order-service-traffic

Unchecked

Server-Side Request Forgery (SSRF) risk at **Messaging Queue** server-side web-requesting the target **User Service** via **User Service Traffic**: Exploitation likelihood is *Unlikely* with *Medium* impact.

server-side-request-forgery@message-queue@user-service@message-queue>user-service-traffic

Unchecked

Unencrypted Technical Asset named **Messaging Queue** missing enduser-individual encryption with data-with-enduser-individual-key: Exploitation likelihood is *Unlikely* with *Medium* impact.

unencrypted-asset@message-queue

Unchecked

Low Risk Severity

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **Messaging Queue** regarding communication link **Inventory Service Traffic**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@message-queue@message-queue>inventory-service-traffic

Unchecked

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **Messaging Queue** regarding communication link **Order Service Traffic**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@message-queue@message-queue>order-service-traffic

Unchecked

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **Messaging Queue** regarding communication link **Payment Service Traffic**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@message-queue@message-queue>payment-service-traffic

Unchecked

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **Messaging Queue** regarding communication link **User Service Traffic**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@message-queue@message-queue>user-service-traffic

Unchecked

Asset Information

ID:	message-queue
Type:	process
Usage:	devops
RAA:	9 %
Size:	service
Technology:	message-queue
Tags:	aws:ec2, linux
Internet:	true
Machine:	container
Encryption:	data-with-symmetric-shared-key
Multi-Tenant:	false
Redundant:	false
Custom-Developed:	false
Client by Human:	false
Data Processed:	Order Data, Payment data, Product Data, User Data
Data Stored:	none
Formats Accepted:	JSON

Asset Rating

Owner:	Company XYZ	
Confidentiality:	internal	(rated 2 in scale of 5)

Integrity:	operational	(rated 2 in scale of 5)
Availability:	operational	(rated 2 in scale of 5)
CIA-Justification:	Internal	

Outgoing Communication Links: 5

Target technical asset names are clickable and link to the corresponding chapter.

User Service Traffic (outgoing)

Link to the User service inside cluster

Target:	User Service
Protocol:	http
Encrypted:	false
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	devops
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Sent:	none
Data Received:	User Data

Payment Service Traffic (outgoing)

Link to the payment service inside cluster

Target:	Payment Service
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Sent:	none
Data Received:	Payment data

Order Service Traffic (outgoing)

Link to the Order service inside cluster

Target:	Order Service
Protocol:	http
Encrypted:	false
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	devops
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Sent:	none
Data Received:	Order Data

Inventory Service Traffic (outgoing)

Link to the Inventory service inside cluster

Target:	Inventory Service
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	devops
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Sent:	none
Data Received:	Product Data

Database communication (outgoing)

Link to the database (JDBC tunneled via SSH)

Target:	Database cluster
Protocol:	http
Encrypted:	false
Authentication:	token
Authorization:	technical-user

Read-Only:	false
Usage:	devops
Tags:	none
VPN:	false
IP-Filtered:	true
Data Sent:	Order Data, Payment data, Product Data, User Data
Data Received:	none

Incoming Communication Links: 5

Source technical asset names are clickable and link to the corresponding chapter.

Messaging Queue (incoming)

Link

Source:	User Service
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	true
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	false
Data Received:	none
Data Sent:	Payment data, User Data

Messaging Queue (incoming)

Link

Source:	Database cluster
Protocol:	http
Encrypted:	false
Authentication:	token
Authorization:	technical-user
Read-Only:	true
Usage:	business
Tags:	aws:ec2
VPN:	false

IP-Filtered:	false
Data Received:	none
Data Sent:	Order Data, Payment data, Product Data, User Data

Messaging Queue (incoming)

Link

Source:	Payment Service
Protocol:	http
Encrypted:	false
Authentication:	token
Authorization:	technical-user
Read-Only:	true
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	false
Data Received:	none
Data Sent:	Payment data

Messaging Queue (incoming)

Link

Source:	Order Service
Protocol:	http
Encrypted:	false
Authentication:	token
Authorization:	technical-user
Read-Only:	true
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	false
Data Received:	none
Data Sent:	Order Data

Messaging Queue (incoming)

Link

Source:	Inventory Service

Protocol:	http
Encrypted:	false
Authentication:	token
Authorization:	technical-user
Read-Only:	true
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	false
Data Received:	none
Data Sent:	Product Data

Order Service: 15 / 16 Risks

Description

Manages order creation, status, and tracking.

Identified Risks of Asset

Risk finding paragraphs are clickable and link to the corresponding chapter.

Elevated Risk Severity

Missing Cloud Hardening (EC2) risk at **Order Service**: CIS Benchmark for Amazon Linux: Exploitation likelihood is *Unlikely* with *Very High* impact.

missing-cloud-hardening@order-service

Unchecked

Unguarded Access from Internet of **Order Service** by **Messaging Queue** via **Order Service Traffic**: Exploitation likelihood is *Very Likely* with *Medium* impact.

unguarded-access-from-internet@order-service@message-queue@message-queue>order-service-traffic

Unchecked

Missing Hardening risk at **Order Service**: Exploitation likelihood is *Likely* with *Medium* impact.

missing-hardening@order-service

Unchecked

Server-Side Request Forgery (SSRF) risk at **Order Service** server-side web-requesting the target **Load Balancer** via **Order Traffic**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@order-service@load-balancer@order-service>order-traffic

Unchecked

Server-Side Request Forgery (SSRF) risk at **Order Service** server-side web-requesting the target **Messaging Queue** via **Messaging Queue**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@order-service@message-queue@order-service>messaging-queue

Unchecked

Server-Side Request Forgery (SSRF) risk at **Order Service** server-side web-requesting the target **Payment Service** via **Payment Service Traffic**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@order-service@payment-service@order-service>payment-service-traffic

Unchecked

Medium Risk Severity

Container Base Image Backdooring risk at **Order Service**: Exploitation likelihood is *Unlikely* with *High* impact.

container-baseimage-backdooring@order-service

Unchecked

Container Platform Escape risk at **Order Service**: Exploitation likelihood is *Unlikely* with *High* impact.

container-platform-escape@order-service

Unchecked

Unencrypted Communication named **Messaging Queue** between **Order Service** and **Messaging Queue** transferring authentication data (like credentials, token, session-id, etc.): Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-communication@order-service>messaging-queue@order-service@message-queue

Unchecked

Unencrypted Technical Asset named **Order Service**: Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-asset@order-service

Unchecked

Missing Build Infrastructure in the threat model (referencing asset **Order Service** as an example): Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-build-infrastructure@order-service

Unchecked

Missing Identity Store in the threat model (referencing asset **Order Service** as an example): Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-identity-store@order-service

Unchecked

Unnecessary Data Transfer of **Payment data** data at **Order Service** from/to **Payment Service**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@payment-data@order-service@payment-service

Unchecked

Low Risk Severity

Unnecessary Data Transfer of **Product Data** data at **Order Service** from/to **Load Balancer**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@product-data@order-service@load-balancer

Unchecked

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **Order Service** regarding communication link **Payment Service Traffic**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@order-service@order-service>payment-service-traffic

Unchecked

Denial-of-Service risky access of **Order Service** by **API gateway** via **Customer Traffic** forwarded via **Load Balancer**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@order-service@api-gateway@api-gateway>customer-traffic

Mitigated 2025-01-04 John Doe XYZ-1234
The hardening measures are being implemented and checked. Used AWS DOS mitigation

Asset Information

ID:	order-service
Type:	process
Usage:	business
RAA:	100 %
Size:	service
Technology:	container-platform
Tags:	aws:ec2, linux
Internet:	false
Machine:	container
Encryption:	none
Multi-Tenant:	true
Redundant:	true
Custom-Developed:	true
Client by Human:	false
Data Processed:	Order Data, Session Data, User Data
Data Stored:	Order Data, Session Data, User Data
Formats Accepted:	JSON

Asset Rating

Owner:	Company XYZ	
Confidentiality:	restricted	(rated 3 in scale of 5)
Integrity:	mission-critical	(rated 5 in scale of 5)
Availability:	mission-critical	(rated 5 in scale of 5)
CIA-Justification:	The correct configuration and reachability of the service is mandatory for all customer usages of the Platform.	

Outgoing Communication Links: 3

Target technical asset names are clickable and link to the corresponding chapter.

Payment Service Traffic (outgoing)

Link to the payment service inside cluster

Target:	Payment Service
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Sent:	none
Data Received:	Order Data, Payment data, User Data

Order Traffic (outgoing)

Link to the load balancer

Target:	Load Balancer
Protocol:	https
Encrypted:	true
Authentication:	session-id
Authorization:	enduser-identity-propagation
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Sent:	Order Data, User Data
Data Received:	Order Data, Session Data, User Data

Messaging Queue (outgoing)

Link

Target:	Messaging Queue
Protocol:	http

Encrypted:	false
Authentication:	token
Authorization:	technical-user
Read-Only:	true
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	false
Data Sent:	none
Data Received:	Order Data

Incoming Communication Links: 2

Source technical asset names are clickable and link to the corresponding chapter.

Order Service Traffic (incoming)

Link to the Order service inside cluster

Source:	Messaging Queue
Protocol:	http
Encrypted:	false
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	devops
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Received:	none
Data Sent:	Order Data

Order Service Traffic (incoming)

Link to the orders service inside cluster

Source:	Load Balancer
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false

Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Received:	Order Data, Product Data, Session Data, User Data
Data Sent:	Order Data, Product Data, Session Data, User Data

Payment Service: 10 / 10 Risks

Description

Integrates with external payment gateways (e.g., Stripe, PayPal) for payment processing.

Identified Risks of Asset

Risk finding paragraphs are clickable and link to the corresponding chapter.

Elevated Risk Severity

Missing Cloud Hardening (EC2) risk at **Payment Service**: CIS Benchmark for Amazon Linux : Exploitation likelihood is *Unlikely* with *Very High* impact.

missing-cloud-hardening@payment-service

Unchecked

SQL/NoSQL-Injection risk at **Payment Service** against database **Database cluster** via **Database communication**: Exploitation likelihood is *Likely* with *High* impact.

sql-nosql-injection@payment-service@sql-database@payment-service>database-communication

Unchecked

Unguarded Access from Internet of **Payment Service** by **Messaging Queue** via **Payment Service Traffic**: Exploitation likelihood is *Very Likely* with *Medium* impact.

unguarded-access-from-internet@payment-service@message-queue@message-queue>payment-service-traffic

Unchecked

Missing Hardening risk at **Payment Service**: Exploitation likelihood is *Likely* with *Medium* impact.

missing-hardening@payment-service

Unchecked

Server-Side Request Forgery (SSRF) risk at **Payment Service** server-side web-requesting the target **Messaging Queue** via **Messaging Queue**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@payment-service@message-queue@payment-service>messaging-queue

Unchecked

Medium Risk Severity

Container Base Image Backdooring risk at **Payment Service**: Exploitation likelihood is *Unlikely* with *High* impact.

container-baseimage-backdooring@payment-service

Unchecked

Container Platform Escape risk at **Payment Service**: Exploitation likelihood is *Unlikely* with *High* impact.

container-platform-escape@payment-service

Unchecked

Unencrypted Communication named **Messaging Queue** between **Payment Service** and **Messaging Queue** transferring authentication data (like credentials, token, session-id, etc.): Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-communication@payment-service>messaging-queue@payment-service@message-queue

Unchecked

Server-Side Request Forgery (SSRF) risk at **Payment Service** server-side web-requesting the target **Database cluster** via **Database communication**: Exploitation likelihood is *Unlikely* with *Medium* impact.

server-side-request-forgery@payment-service@sql-database@payment-service>database-communication

Unchecked

Unnecessary Data Transfer of **Session Data** data at **Payment Service** from/to **Database cluster**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@session-data@payment-service@sql-database

Unchecked

Asset Information

ID:	payment-service
Type:	process
Usage:	business
RAA:	55 %
Size:	service
Technology:	container-platform
Tags:	aws:ec2, linux
Internet:	true
Machine:	container
Encryption:	data-with-asymmetric-shared-key
Multi-Tenant:	false
Redundant:	false
Custom-Developed:	false
Client by Human:	false
Data Processed:	Order Data, Payment data, Product Data, User Data
Data Stored:	none
Formats Accepted:	JSON

Asset Rating

Owner:	Company XYZ	
Confidentiality:	restricted	(rated 3 in scale of 5)
Integrity:	mission-critical	(rated 5 in scale of 5)
Availability:	mission-critical	(rated 5 in scale of 5)
CIA-Justification:	Payment gateway integration service	

Outgoing Communication Links: 2

Target technical asset names are clickable and link to the corresponding chapter.

Messaging Queue (outgoing)

Link

Target:	Messaging Queue
Protocol:	http
Encrypted:	false
Authentication:	token
Authorization:	technical-user
Read-Only:	true
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	false
Data Sent:	none
Data Received:	Payment data

Database communication (outgoing)

Link to the database

Target:	Database cluster
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	devops
Tags:	none
VPN:	false

IP-Filtered:	true
Data Sent:	Order Data, Payment data, Product Data, User Data
Data Received:	Order Data, Payment data, Product Data, Session Data, User Data

Incoming Communication Links: 5

Source technical asset names are clickable and link to the corresponding chapter.

Payment Service Traffic (incoming)

Link to the payment service inside cluster

Source:	User Service
Protocol:	http
Encrypted:	false
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Received:	none
Data Sent:	Payment data, User Data

Payment Service Traffic (incoming)

Link to the payment service inside cluster

Source:	Database cluster
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Received:	Payment data
Data Sent:	Payment data

Payment Service Traffic (incoming)

Link to the payment service inside cluster

Source:	Order Service
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Received:	none
Data Sent:	Order Data, Payment data, User Data

Payment Service Traffic (incoming)

Link to the payment service inside cluster

Source:	Messaging Queue
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Received:	none
Data Sent:	Payment data

Payment Service Traffic (incoming)

Link to the payment service inside cluster

Source:	Inventory Service
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user

Read-Only:	false
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Received:	none
Data Sent:	Order Data, Payment data, Product Data

User Service: 13 / 14 Risks

Description

Manages user authentication, profile, and session management.

Identified Risks of Asset

Risk finding paragraphs are clickable and link to the corresponding chapter.

Elevated Risk Severity

Missing Cloud Hardening (EC2) risk at **User Service**: CIS Benchmark for Amazon Linux: Exploitation likelihood is *Unlikely* with *Very High* impact.

missing-cloud-hardening@user-service

Unchecked

Unguarded Access from Internet of **User Service** by **Messaging Queue** via **User Service Traffic**: Exploitation likelihood is *Very Likely* with *Medium* impact.

unguarded-access-from-internet@user-service@message-queue@message-queue>user-service-traffic

Unchecked

Missing Hardening risk at **User Service**: Exploitation likelihood is *Likely* with *Medium* impact.

missing-hardening@user-service

Unchecked

Server-Side Request Forgery (SSRF) risk at **User Service** server-side web-requesting the target **Load Balancer** via **User Traffic**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@user-service@load-balancer@user-service>user-traffic

Unchecked

Server-Side Request Forgery (SSRF) risk at **User Service** server-side web-requesting the target **Messaging Queue** via **Messaging Queue**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@user-service@message-queue@user-service>messaging-queue

Unchecked

Server-Side Request Forgery (SSRF) risk at **User Service** server-side web-requesting the target **Payment Service** via **Payment Service Traffic**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@user-service@payment-service@user-service>payment-service-traffic

Unchecked

Medium Risk Severity

Container Base Image Backdooring risk at **User Service**: Exploitation likelihood is *Unlikely* with *High* impact.

container-baseimage-backdooring@user-service

Unchecked

Container Platform Escape risk at **User Service**: Exploitation likelihood is *Unlikely* with *High* impact.

container-platform-escape@user-service

Unchecked

Unencrypted Communication named **Payment Service Traffic** between **User Service** and **Payment Service** transferring authentication data (like credentials, token, session-id, etc.): Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-communication@user-service>payment-service-traffic@user-service@payment-service

Unchecked

Unencrypted Technical Asset named **User Service**: Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-asset@user-service

Unchecked

Unnecessary Data Transfer of **Payment data** data at **User Service** from/to **Messaging Queue**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@payment-data@user-service@message-queue

Unchecked

Unnecessary Data Transfer of **Payment data** data at **User Service** from/to **Payment Service**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@payment-data@user-service@payment-service

Unchecked

Low Risk Severity

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **User Service** regarding communication link **Payment Service Traffic**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@user-service@user-service>payment-service-traffic

Unchecked

Denial-of-Service risky access of **User Service** by **API gateway** via **Customer Traffic** forwarded via **Load Balancer**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@user-service@api-gateway@api-gateway>customer-traffic

Mitigated 2025-01-04 John Doe XYZ-1234
The hardening measures are being implemented and checked. Used AWS DOS mitigation

Asset Information

ID:	user-service
Type:	process

Usage:	business
RAA:	81 %
Size:	service
Technology:	container-platform
Tags:	aws:ec2, linux
Internet:	false
Machine:	container
Encryption:	none
Multi-Tenant:	true
Redundant:	true
Custom-Developed:	true
Client by Human:	false
Data Processed:	Session Data, User Data
Data Stored:	Session Data, User Data
Formats Accepted:	JSON

Asset Rating

Owner:	Company XYZ	
Confidentiality:	restricted	(rated 3 in scale of 5)
Integrity:	mission-critical	(rated 5 in scale of 5)
Availability:	mission-critical	(rated 5 in scale of 5)
CIA-Justification:	The correct configuration and reachability of the service is mandatory for all customer usages of the Platform.	

Outgoing Communication Links: 3

Target technical asset names are clickable and link to the corresponding chapter.

User Traffic (outgoing)

Link to the load balancer

Target:	Load Balancer
Protocol:	https
Encrypted:	true
Authentication:	session-id
Authorization:	enduser-identity-propagation
Read-Only:	false
Usage:	business

Tags:	none
VPN:	false
IP-Filtered:	false
Data Sent:	Session Data, User Data
Data Received:	User Data

Payment Service Traffic (outgoing)

Link to the payment service inside cluster

Target:	Payment Service
Protocol:	http
Encrypted:	false
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Sent:	none
Data Received:	Payment data, User Data

Messaging Queue (outgoing)

Link

Target:	Messaging Queue
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	true
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	false
Data Sent:	none
Data Received:	Payment data, User Data

Incoming Communication Links: 2

Source technical asset names are clickable and link to the corresponding chapter.

User Service Traffic (incoming)

Link to the User service inside cluster

Source:	Messaging Queue
Protocol:	http
Encrypted:	false
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	devops
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Received:	none
Data Sent:	User Data

User Service Traffic (incoming)

Link to the service inside cluster

Source:	Load Balancer
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Received:	User Data
Data Sent:	Session Data, User Data

Load Balancer: 0 / 0 Risks

Description

Load Balancer

Identified Risks of Asset

No risks were identified.

Asset Information

ID:	load-balancer
Type:	process
Usage:	business
RAA:	3 %
Size:	component
Technology:	load-balancer
Tags:	none
Internet:	false
Machine:	virtual
Encryption:	data-with-asymmetric-shared-key
Multi-Tenant:	false
Redundant:	true
Custom-Developed:	false
Client by Human:	false
Data Processed:	Order Data, Payment data, Product Data, Session Data, User Data
Data Stored:	none
Formats Accepted:	none of the special data formats accepted

Asset Rating

Owner:	Company XYZ	
Confidentiality:	internal	(rated 2 in scale of 5)
Integrity:	mission-critical	(rated 5 in scale of 5)
Availability:	mission-critical	(rated 5 in scale of 5)
CIA-Justification:	The correct configuration and reachability of the load balancer is mandatory for all customer and Company XYZ usages of the Platform.	

Outgoing Communication Links: 3

Target technical asset names are clickable and link to the corresponding chapter.

User Service Traffic (outgoing)

Link to the service inside cluster

Target:	User Service
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Sent:	User Data
Data Received:	Session Data, User Data

Order Service Traffic (outgoing)

Link to the orders service inside cluster

Target:	Order Service
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Sent:	Order Data, Product Data, Session Data, User Data
Data Received:	Order Data, Product Data, Session Data, User Data

Inventory Service Traffic (outgoing)

Link to the Inventory service inside cluster

Target:	Inventory Service
Protocol:	https

Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	aws:ec2
VPN:	false
IP-Filtered:	true
Data Sent:	Product Data, Session Data, User Data
Data Received:	Product Data, Session Data, User Data

Incoming Communication Links: 4

Source technical asset names are clickable and link to the corresponding chapter.

User Traffic (incoming)

Link to the load balancer

Source:	User Service
Protocol:	https
Encrypted:	true
Authentication:	session-id
Authorization:	enduser-identity-propagation
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Received:	Session Data, User Data
Data Sent:	User Data

Order Traffic (incoming)

Link to the load balancer

Source:	Order Service
Protocol:	https
Encrypted:	true
Authentication:	session-id
Authorization:	enduser-identity-propagation
Read-Only:	false

Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Received:	Order Data, User Data
Data Sent:	Order Data, Session Data, User Data

Inventory Traffic (incoming)

Link to the load balancer

Source:	Inventory Service
Protocol:	https
Encrypted:	true
Authentication:	session-id
Authorization:	enduser-identity-propagation
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Received:	Order Data, Product Data, Session Data
Data Sent:	Order Data, Product Data, Session Data

Customer Traffic (incoming)

Link to the load balancer

Source:	API gateway
Protocol:	https
Encrypted:	true
Authentication:	session-id
Authorization:	enduser-identity-propagation
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Received:	Order Data, Payment data, Product Data, Session Data, User Data
Data Sent:	Order Data, Payment data, Product Data, Session Data, User Data

Web Client: out-of-scope

Description

Customer Web Client

Identified Risks of Asset

Asset was defined as out-of-scope.

Asset Information

ID:	web-client
Type:	external-entity
Usage:	business
RAA:	out-of-scope
Size:	component
Technology:	browser
Tags:	none
Internet:	true
Machine:	physical
Encryption:	none
Multi-Tenant:	false
Redundant:	false
Custom-Developed:	false
Client by Human:	true
Data Processed:	Order Data, Payment data, Product Data, Session Data, User Data
Data Stored:	Session Data
Formats Accepted:	none of the special data formats accepted

Asset Rating

Owner:	Customer	
Confidentiality:	public	(rated 1 in scale of 5)
Integrity:	critical	(rated 4 in scale of 5)
Availability:	mission-critical	(rated 5 in scale of 5)
CIA-Justification:	The client used by the customers to access the E-commerse platform.	

Asset Out-of-Scope Justification

Owned and managed by enduser customer

Outgoing Communication Links: 1

Target technical asset names are clickable and link to the corresponding chapter.

API gateway Traffic (outgoing)

Link to the API gateway

Target:	API gateway
Protocol:	https
Encrypted:	true
Authentication:	session-id
Authorization:	enduser-identity-propagation
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Sent:	Order Data, Payment data, Product Data, Session Data, User Data
Data Received:	Order Data, Payment data, Product Data, Session Data, User Data

Identified Data Breach Probabilities by Data Asset

In total **83 potential risks** have been identified during the threat modeling process of which **0 are rated as critical**, **0 as high**, **33 as elevated**, **38 as medium**, and **12 as low**.

These risks are distributed across **6 data assets**. The following sub-chapters of this section describe the derived data breach probabilities grouped by data asset.
Technical asset names and risk IDs are clickable and link to the corresponding chapter.

Order Data: 59 / 60 Risks

Details of user orders, order statuses, shipping information.

ID:	order-data	
Usage:	business	
Quantity:	many	
Tags:	none	
Origin:	User	
Owner:	Company XYZ	
Confidentiality:	restricted	(rated 3 in scale of 5)
Integrity:	critical	(rated 4 in scale of 5)
Availability:	mission-critical	(rated 5 in scale of 5)
CIA-Justification:	Order data may contain PCI and user location data. The confidentiality, integrity and availability of order data is required for platform functionality.	
Processed by:	API gateway, Database cluster, Inventory Service, Load Balancer, Messaging Queue, Order Service, Payment Service, Web Client	
Stored by:	Database cluster, Inventory Service, Order Service	
Sent via:	Order Traffic, Order Service Traffic, Inventory Traffic, Database communication, Database communication, Customer Traffic, API gateway Traffic	
Received via:	Payment Service Traffic, Payment Service Traffic, Order Traffic, Order Service Traffic, Order Service Traffic, Messaging Queue, Messaging Queue, Inventory Traffic, Database communication, Customer Traffic, API gateway Traffic	
Data Breach:	**probable**	
Data Breach Risks:	This data asset has data breach potential because of 59 remaining risks:	

Probable: container-baseimage-backdooring@inventory-service

Probable: container-baseimage-backdooring@message-queue

Probable: container-baseimage-backdooring@order-service

Probable: container-baseimage-backdooring@payment-service

Probable: container-platform-escape@inventory-service

Probable: container-platform-escape@order-service

Probable: container-platform-escape@payment-service

Probable: container-platform-escape@user-service

Probable: missing-cloud-hardening@application-network

Probable: missing-cloud-hardening@inventory-service

Probable: missing-cloud-hardening@message-queue

Probable: missing-cloud-hardening@order-service

Probable: missing-cloud-hardening@payment-service

Probable: missing-cloud-hardening@cluster-group

Probable: sql-nosql-injection@message-queue@sql-database@message-queue>database-communication

Probable: sql-nosql-injection@payment-service@sql-database@payment-service>database-communication

Possible: server-side-request-forgery@api-gateway@load-balancer@api-gateway>customer-traffic

Possible: server-side-request-forgery@sql-database@message-queue@sql-database>messaging-queue

Possible: server-side-request-forgery@sql-database@payment-service@sql-database>payment-service-traffic

Possible: server-side-request-forgery@inventory-service@load-balancer@inventory-service>inventory-traffic

Possible: server-side-request-forgery@inventory-service@message-queue@inventory-service>messaging-queue

Possible: server-side-request-forgery@inventory-service@payment-service@inventory-service>payment-service-traffic

Possible: server-side-request-forgery@message-queue@sql-database@message-queue>database-communication

Possible: server-side-request-forgery@message-queue@inventory-service@message-queue>inventory-service-traffic

Possible: server-side-request-forgery@message-queue@order-service@message-queue>order-service-traffic

Possible: server-side-request-forgery@message-queue@payment-service@message-queue>payment-service-traffic

Possible: server-side-request-forgery@message-queue@user-service@message-queue>user-service-traffic

Possible: server-side-request-forgery@order-service@load-balancer@order-service>order-traffic

Possible: server-side-request-forgery@order-service@message-queue@order-service>messaging-queue

Possible: server-side-request-forgery@order-service@payment-service@order-service>payment-service-traffic

Possible: server-side-request-forgery@payment-service@sql-database@payment-service>database-communication

Possible: server-side-request-forgery@payment-service@message-queue@payment-service>messaging-queue

Possible: server-side-request-forgery@user-service@load-balancer@user-service>user-traffic

Possible: server-side-request-forgery@user-service@message-queue@user-service>messaging-queue

Possible: server-side-request-forgery@user-service@payment-service@user-service>payment-service-traffic

Possible: unencrypted-communication@message-queue>database-communication@message-queue@sql-database

Possible: unencrypted-communication@sql-database>messaging-queue@sql-database@message-queue

Possible: unencrypted-communication@inventory-service>messaging-queue@inventory-service@message-queue

Possible: unencrypted-communication@order-service>messaging-queue@order-service@message-queue

Possible: unencrypted-communication@payment-service>messaging-queue@payment-service@message-queue

Possible: unencrypted-communication@message-queue>order-service-traffic@message-queue@order-service

Possible: unencrypted-communication@user-service>payment-service-traffic@user-service@payment-service

Possible: unguarded-access-from-internet@sql-database@message-queue@message-queue>database-communication

Possible: unguarded-access-from-internet@sql-database@payment-service@payment-service>database-communication

Possible: unguarded-access-from-internet@inventory-service@message-queue@message-queue>inventory-service-traffic

Possible: unguarded-access-from-internet@order-service@message-queue@message-queue>order-service-traffic

Possible: unguarded-access-from-internet@payment-service@message-queue@message-queue>payment-service-traffic

Improbable: missing-hardening@inventory-service

Improbable: missing-hardening@order-service

Improbable: missing-hardening@payment-service

Improbable: unencrypted-asset@sql-database

Improbable: unencrypted-asset@inventory-service

Improbable: unencrypted-asset@message-queue

Improbable: unencrypted-asset@order-service

Improbable: unnecessary-data-transfer@payment-data@inventory-service@payment-service

Improbable: unnecessary-data-transfer@payment-data@order-service@payment-service

Improbable: unnecessary-data-transfer@product-data@order-service@load-balancer

Improbable: unnecessary-data-transfer@session-data@sql-database@payment-service

Improbable: unnecessary-data-transfer@session-data@payment-service@sql-database

Payment data: 45 / 46 Risks

Payment transaction details and communication with third-party payment processors.

ID:	payment-data	
Usage:	business	
Quantity:	many	
Tags:	none	
Origin:	User	
Owner:	Company XYZ	
Confidentiality:	strictly-confidential	(rated 5 in scale of 5)
Integrity:	critical	(rated 4 in scale of 5)
Availability:	mission-critical	(rated 5 in scale of 5)
CIA-Justification:	Payment data might contain financial data as well as personally identifiable information (PII). The confidentiality, integrity and availability of payment data is required for preventing financial fraud and identity theft.	
Processed by:	API gateway, Database cluster, Load Balancer, Messaging Queue, Payment Service, Web Client	
Stored by:	Database cluster	
Sent via:	Payment Service Traffic, Database communication, Database communication, Customer Traffic, API gateway Traffic	
Received via:	Payment Service Traffic, Payment Service Traffic, Payment Service Traffic, Payment Service Traffic, Payment Service Traffic, Messaging Queue, Messaging Queue, Messaging Queue, Database communication, Customer Traffic, API gateway Traffic	
Data Breach:	**probable**	
Data Breach Risks:	This data asset has data breach potential because of 45 remaining risks:	

Probable: container-baseimage-backdooring@message-queue

Probable: container-baseimage-backdooring@payment-service

Probable: container-platform-escape@inventory-service

Probable: container-platform-escape@order-service

Probable: container-platform-escape@payment-service

Probable: container-platform-escape@user-service

Probable: missing-cloud-hardening@application-network

Probable: missing-cloud-hardening@message-queue

Probable: missing-cloud-hardening@payment-service

Probable: missing-cloud-hardening@cluster-group

Probable: sql-nosql-injection@message-queue@sql-database@message-queue>database-communication

Probable: sql-nosql-injection@payment-service@sql-database@payment-service>database-communication

Possible: server-side-request-forgery@api-gateway@load-balancer@api-gateway>customer-traffic

Possible: server-side-request-forgery@sql-database@message-queue@sql-database>messaging-queue

Possible: server-side-request-forgery@sql-database@payment-service@sql-database>payment-service-traffic

Possible: server-side-request-forgery@inventory-service@load-balancer@inventory-service>inventory-traffic

Possible: server-side-request-forgery@inventory-service@message-queue@inventory-service>messaging-queue

Possible: server-side-request-forgery@inventory-service@payment-service@inventory-service>payment-service-traffic

Possible: server-side-request-forgery@message-queue@sql-database@message-queue>database-communication

Possible: server-side-request-forgery@message-queue@inventory-service@message-queue>inventory-service-traffic

Possible: server-side-request-forgery@message-queue@order-service@message-queue>order-service-traffic

Possible: server-side-request-forgery@message-queue@payment-service@message-queue>payment-service-traffic

Possible: server-side-request-forgery@message-queue@user-service@message-queue>user-service-traffic

Possible: server-side-request-forgery@order-service@load-balancer@order-service>order-traffic

Possible: server-side-request-forgery@order-service@message-queue@order-service>messaging-queue

Possible: server-side-request-forgery@order-service@payment-service@order-service>payment-service-traffic

Possible: server-side-request-forgery@payment-service@sql-database@payment-service>database-communication

Possible: server-side-request-forgery@payment-service@message-queue@payment-service>messaging-queue

Possible: server-side-request-forgery@user-service@load-balancer@user-service>user-traffic

Possible: server-side-request-forgery@user-service@message-queue@user-service>messaging-queue

Possible: server-side-request-forgery@user-service@payment-service@user-service>payment-service-traffic

Possible: unencrypted-communication@message-queue>database-communication@message-queue@sql-database

Possible: unencrypted-communication@sql-database>messaging-queue@sql-database@message-queue

Possible: unencrypted-communication@inventory-service>messaging-queue@inventory-service@message-queue

Possible: unencrypted-communication@order-service>messaging-queue@order-service@message-queue

Possible: unencrypted-communication@payment-service>messaging-queue@payment-service@message-queue

Possible: unencrypted-communication@user-service>payment-service-traffic@user-service@payment-service

Possible: unguarded-access-from-internet@sql-database@message-queue@message-queue>database-communication

Possible: unguarded-access-from-internet@sql-database@payment-service@payment-service>database-communication

Possible: unguarded-access-from-internet@payment-service@message-queue@message-queue>payment-service-traffic

Improbable: missing-hardening@payment-service

Improbable: unencrypted-asset@sql-database

Improbable: unencrypted-asset@message-queue

Improbable: unnecessary-data-transfer@session-data@sql-database@payment-service

Improbable: unnecessary-data-transfer@session-data@payment-service@sql-database

Product Data: 51 / 52 Risks

Product names, descriptions, prices, and inventory counts.

ID:	product-data	
Usage:	business	
Quantity:	many	
Tags:	none	
Origin:	User	
Owner:	Company XYZ	
Confidentiality:	public	(rated 1 in scale of 5)
Integrity:	critical	(rated 4 in scale of 5)
Availability:	mission-critical	(rated 5 in scale of 5)
CIA-Justification:	The integrity and availability of product data is required for platform functionality.	
Processed by:	API gateway, Database cluster, Inventory Service, Load Balancer, Messaging Queue, Payment Service, Web Client	
Stored by:	Database cluster, Inventory Service	
Sent via:	Order Service Traffic, Inventory Traffic, Inventory Service Traffic, Database communication, Database communication, Customer Traffic, API gateway Traffic	
Received via:	Payment Service Traffic, Order Service Traffic, Messaging Queue, Messaging Queue, Inventory Traffic, Inventory Service Traffic, Inventory Service Traffic, Database communication, Customer Traffic, API gateway Traffic	
Data Breach:	**probable**	
Data Breach Risks:	This data asset has data breach potential because of 51 remaining risks:	

Probable: container-baseimage-backdooring@inventory-service

Probable: container-baseimage-backdooring@message-queue

Probable: container-baseimage-backdooring@payment-service

Probable: container-platform-escape@inventory-service

Probable: container-platform-escape@order-service

Probable: container-platform-escape@payment-service

Probable: container-platform-escape@user-service

Probable: missing-cloud-hardening@application-network

Probable: missing-cloud-hardening@inventory-service

Probable: missing-cloud-hardening@message-queue

Probable: missing-cloud-hardening@payment-service

Probable: missing-cloud-hardening@cluster-group

Probable: sql-nosql-injection@message-queue@sql-database@message-queue>database-communication

Probable: sql-nosql-injection@payment-service@sql-database@payment-service>database-communication

Possible: server-side-request-forgery@api-gateway@load-balancer@api-gateway>customer-traffic

Possible: server-side-request-forgery@sql-database@message-queue@sql-database>messaging-queue

Possible: server-side-request-forgery@sql-database@payment-service@sql-database>payment-service-traffic

Possible: server-side-request-forgery@inventory-service@load-balancer@inventory-service>inventory-traffic

Possible: server-side-request-forgery@inventory-service@message-queue@inventory-service>messaging-queue

Possible: server-side-request-forgery@inventory-service@payment-service@inventory-service>payment-service-traffic

Possible: server-side-request-forgery@message-queue@sql-database@message-queue>database-communication

Possible: server-side-request-forgery@message-queue@inventory-service@message-queue>inventory-service-traffic

Possible: server-side-request-forgery@message-queue@order-service@message-queue>order-service-traffic

Possible: server-side-request-forgery@message-queue@payment-service@message-queue>payment-service-traffic

Possible: server-side-request-forgery@message-queue@user-service@message-queue>user-service-traffic

Possible: server-side-request-forgery@order-service@load-balancer@order-service>order-traffic

Possible: server-side-request-forgery@order-service@message-queue@order-service>messaging-queue

Possible: server-side-request-forgery@order-service@payment-service@order-service>payment-service-traffic

Possible: server-side-request-forgery@payment-service@sql-database@payment-service>database-communication

Possible: server-side-request-forgery@payment-service@message-queue@payment-service>messaging-queue

Possible: server-side-request-forgery@user-service@load-balancer@user-service>user-traffic

Possible: server-side-request-forgery@user-service@message-queue@user-service>messaging-queue

Possible: server-side-request-forgery@user-service@payment-service@user-service>payment-service-traffic

Possible: unencrypted-communication@message-queue>database-communication@message-queue@sql-database

Possible: unencrypted-communication@sql-database>messaging-queue@sql-database@message-queue

Possible: unencrypted-communication@inventory-service>messaging-queue@inventory-service@message-queue

Possible: unencrypted-communication@order-service>messaging-queue@order-service@message-queue

Possible: unencrypted-communication@payment-service>messaging-queue@payment-service@message-queue

Possible: unencrypted-communication@user-service>payment-service-traffic@user-service@payment-service

Possible: unguarded-access-from-internet@sql-database@message-queue@message-queue>database-communication

Possible: unguarded-access-from-internet@sql-database@payment-service@payment-service>database-communication

Possible: unguarded-access-from-internet@inventory-service@message-queue@message-queue>inventory-service-traffic

Possible: unguarded-access-from-internet@payment-service@message-queue@message-queue>payment-service-traffic

Improbable: missing-hardening@inventory-service

Improbable: missing-hardening@payment-service

Improbable: unencrypted-asset@sql-database

Improbable: unencrypted-asset@inventory-service

Improbable: unencrypted-asset@message-queue

Improbable: unnecessary-data-transfer@payment-data@inventory-service@payment-service

Improbable: unnecessary-data-transfer@session-data@sql-database@payment-service

Improbable: unnecessary-data-transfer@session-data@payment-service@sql-database

Session Data: 47 / 48 Risks

User sessions and authentication tokens.

ID: session-data

Usage: devops

Quantity: many

Tags: none

Origin: Company XYZ

Owner: Company XYZ

Confidentiality: strictly-confidential (rated 5 in scale of 5)

Integrity: critical (rated 4 in scale of 5)

Availability: mission-critical (rated 5 in scale of 5)

CIA-Justification: Payment data might contain financial data as well as personally identifiable information (PII). The confidentiality, integrity and availability of payment data is required for preventing financial fraud and identity theft.

Processed by: API gateway, Inventory Service, Load Balancer, Order Service, User Service, Web Client

Stored by: Order Service, User Service, Web Client

Sent via: User Traffic, Order Service Traffic, Inventory Traffic, Inventory Service Traffic, Customer Traffic, API gateway Traffic

Received via: User Service Traffic, Order Traffic, Order Service Traffic, Inventory Traffic, Inventory Service Traffic, Database communication, Customer Traffic, API gateway Traffic

Data Breach: **probable**

Data Breach Risks: This data asset has data breach potential because of 47 remaining risks:

Probable: container-baseimage-backdooring@inventory-service

Probable: container-baseimage-backdooring@order-service

Probable: container-baseimage-backdooring@user-service

Probable: container-platform-escape@inventory-service

Probable: container-platform-escape@order-service

Probable: container-platform-escape@payment-service

Probable: container-platform-escape@user-service

Probable: missing-cloud-hardening@application-network

Probable: missing-cloud-hardening@inventory-service

Probable: missing-cloud-hardening@order-service

Probable: missing-cloud-hardening@user-service

Probable: missing-cloud-hardening@cluster-group

Possible: server-side-request-forgery@api-gateway@load-balancer@api-gateway>customer-traffic

Possible: server-side-request-forgery@sql-database@message-queue@sql-database>messaging-queue

Possible: server-side-request-forgery@sql-database@payment-service@sql-database>payment-service-traffic

Possible: server-side-request-forgery@inventory-service@load-balancer@inventory-service>inventory-traffic

Possible: server-side-request-forgery@inventory-service@message-queue@inventory-service>messaging-queue

Possible: server-side-request-forgery@inventory-service@payment-service@inventory-service>payment-service-traffic

Possible: server-side-request-forgery@message-queue@sql-database@message-queue>database-communication

Possible: server-side-request-forgery@message-queue@inventory-service@message-queue>inventory-service-traffic

Possible: server-side-request-forgery@message-queue@order-service@message-queue>order-service-traffic

Possible: server-side-request-forgery@message-queue@payment-service@message-queue>payment-service-traffic

Possible: server-side-request-forgery@message-queue@user-service@message-queue>user-service-traffic

Possible: server-side-request-forgery@order-service@load-balancer@order-service>order-traffic

Possible: server-side-request-forgery@order-service@message-queue@order-service>messaging-queue

Possible: server-side-request-forgery@order-service@payment-service@order-service>payment-service-traffic

Possible: server-side-request-forgery@payment-service@sql-database@payment-service>database-communication

Possible: server-side-request-forgery@payment-service@message-queue@payment-service>messaging-queue

Possible: server-side-request-forgery@user-service@load-balancer@user-service>user-traffic

Possible: server-side-request-forgery@user-service@message-queue@user-service>messaging-queue

Possible: server-side-request-forgery@user-service@payment-service@user-service>payment-service-traffic

Possible: unencrypted-communication@message-queue>order-service-traffic@message-queue@order-service

Possible: unencrypted-communication@message-queue>user-service-traffic@message-queue@user-service

Possible: unguarded-access-from-internet@inventory-service@message-queue@message-queue>inventory-service-traffic

Possible: unguarded-access-from-internet@order-service@message-queue@message-queue>order-service-traffic

Possible: unguarded-access-from-internet@user-service@message-queue@message-queue>user-service-traffic

Improbable: missing-hardening@inventory-service

Improbable: missing-hardening@order-service

Improbable: missing-hardening@user-service

Improbable: unencrypted-asset@inventory-service

Improbable: unencrypted-asset@order-service

Improbable: unencrypted-asset@user-service

Improbable: unnecessary-data-transfer@payment-data@inventory-service@payment-service

Improbable: unnecessary-data-transfer@payment-data@order-service@payment-service

Improbable: unnecessary-data-transfer@payment-data@user-service@message-queue

Improbable: unnecessary-data-transfer@payment-data@user-service@payment-service

Improbable: unnecessary-data-transfer@product-data@order-service@load-balancer

User Data: 67 / 68 Risks

Personal information (name, email, address), credit card details, purchase history.

ID:	user-data	
Usage:	business	
Quantity:	many	
Tags:	none	
Origin:	User	
Owner:	Company XYZ	
Confidentiality:	confidential	(rated 4 in scale of 5)
Integrity:	critical	(rated 4 in scale of 5)
Availability:	mission-critical	(rated 5 in scale of 5)
CIA-Justification:	User data might contain financial data as well as personally identifiable information (PII). The confidentiality, integrity and availability of user data is required for User data privacy and platform functionality.	
Processed by:	API gateway, Database cluster, Inventory Service, Load Balancer, Messaging Queue, Order Service, Payment Service, User Service, Web Client	
Stored by:	Database cluster, Inventory Service, Order Service, User Service	
Sent via:	User Traffic, User Service Traffic, Order Traffic, Order Service Traffic, Inventory Service Traffic, Database communication, Database communication, Customer Traffic, API gateway Traffic	
Received via:	User Traffic, User Service Traffic, User Service Traffic, Payment Service Traffic, Payment Service Traffic, Order Traffic, Order Service Traffic, Messaging Queue, Messaging Queue, Inventory Service Traffic, Database communication, Customer Traffic, API gateway Traffic	
Data Breach:	**probable**	
Data Breach Risks:	This data asset has data breach potential because of 67 remaining risks:	

Probable: container-baseimage-backdooring@inventory-service

Probable: container-baseimage-backdooring@message-queue

Probable: container-baseimage-backdooring@order-service

Probable: container-baseimage-backdooring@payment-service

Probable: container-baseimage-backdooring@user-service

Probable: container-platform-escape@inventory-service

Probable: container-platform-escape@order-service

Probable: container-platform-escape@payment-service

Probable: container-platform-escape@user-service

Probable: missing-cloud-hardening@application-network

Probable: missing-cloud-hardening@inventory-service

Probable: missing-cloud-hardening@message-queue

Probable: missing-cloud-hardening@order-service

Probable: missing-cloud-hardening@payment-service

Probable: missing-cloud-hardening@user-service

Probable: missing-cloud-hardening@cluster-group

Probable: sql-nosql-injection@message-queue@sql-database@message-queue>database-communication

Probable: sql-nosql-injection@payment-service@sql-database@payment-service>database-communication

Possible: server-side-request-forgery@api-gateway@load-balancer@api-gateway>customer-traffic

Possible: server-side-request-forgery@sql-database@message-queue@sql-database>messaging-queue

Possible: server-side-request-forgery@sql-database@payment-service@sql-database>payment-service-traffic

Possible: server-side-request-forgery@inventory-service@load-balancer@inventory-service>inventory-traffic

Possible: server-side-request-forgery@inventory-service@message-queue@inventory-service>messaging-queue

Possible: server-side-request-forgery@inventory-service@payment-service@inventory-service>payment-service-traffic

Possible: server-side-request-forgery@message-queue@sql-database@message-queue>database-communication

Possible: server-side-request-forgery@message-queue@inventory-service@message-queue>inventory-service-traffic

Possible: server-side-request-forgery@message-queue@order-service@message-queue>order-service-traffic

Possible: server-side-request-forgery@message-queue@payment-service@message-queue>payment-service-traffic

Possible: server-side-request-forgery@message-queue@user-service@message-queue>user-service-traffic

Possible: server-side-request-forgery@order-service@load-balancer@order-service>order-traffic

Possible: server-side-request-forgery@order-service@message-queue@order-service>messaging-queue

Possible: server-side-request-forgery@order-service@payment-service@order-service>payment-service-traffic

Possible: server-side-request-forgery@payment-service@sql-database@payment-service>database-communication

Possible: server-side-request-forgery@payment-service@message-queue@payment-service>messaging-queue

Possible: server-side-request-forgery@user-service@load-balancer@user-service>user-traffic

Possible: server-side-request-forgery@user-service@message-queue@user-service>messaging-queue

Possible: server-side-request-forgery@user-service@payment-service@user-service>payment-service-traffic

Possible: unencrypted-communication@message-queue>database-communication@message-queue@sql-database

Possible: unencrypted-communication@sql-database>messaging-queue@sql-database@message-queue

Possible: unencrypted-communication@inventory-service>messaging-queue@inventory-service@message-queue

Possible: unencrypted-communication@order-service>messaging-queue@order-service@message-queue

Possible: unencrypted-communication@payment-service>messaging-queue@payment-service@message-queue

Possible: unencrypted-communication@message-queue>order-service-traffic@message-queue@order-service

Possible: unencrypted-communication@user-service>payment-service-traffic@user-service@payment-service

Possible: unencrypted-communication@message-queue>user-service-traffic@message-queue@user-service

Possible: unguarded-access-from-internet@sql-database@message-queue@message-queue>database-communication

Possible: unguarded-access-from-internet@sql-database@payment-service@payment-service>database-communication

Possible: unguarded-access-from-internet@inventory-service@message-queue@message-queue>inventory-service-traffic

Possible: unguarded-access-from-internet@order-service@message-queue@message-queue>order-service-traffic

Possible: unguarded-access-from-internet@payment-service@message-queue@message-queue>payment-service-traffic

Possible: unguarded-access-from-internet@user-service@message-queue@message-queue>user-service-traffic

Improbable: missing-hardening@inventory-service

Improbable: missing-hardening@order-service

Improbable: missing-hardening@payment-service

Improbable: missing-hardening@user-service

Improbable: unencrypted-asset@sql-database

Improbable: unencrypted-asset@inventory-service

Improbable: unencrypted-asset@message-queue

Improbable: unencrypted-asset@order-service

Improbable: unencrypted-asset@user-service

Improbable: unnecessary-data-transfer@payment-data@inventory-service@payment-service

Improbable: unnecessary-data-transfer@payment-data@order-service@payment-service

Improbable: unnecessary-data-transfer@payment-data@user-service@message-queue

Improbable: unnecessary-data-transfer@payment-data@user-service@payment-service

Improbable: unnecessary-data-transfer@product-data@order-service@load-balancer

Improbable: unnecessary-data-transfer@session-data@sql-database@payment-service

Improbable: unnecessary-data-transfer@session-data@payment-service@sql-database

Database Customizing and Dumps: 0 / 0 Risks

Data for customizing of the DB system, which might include full database dumps.

ID:	db-dumps	
Usage:	devops	
Quantity:	very-few	
Tags:	aws:rds	
Origin:	Company XYZ	
Owner:	Company XYZ	
Confidentiality:	strictly-confidential	(rated 5 in scale of 5)
Integrity:	critical	(rated 4 in scale of 5)
Availability:	critical	(rated 4 in scale of 5)
CIA-Justification:	Data for customizing of the DB system, which might include full database dumps.	
Processed by:	none	
Stored by:	none	
Sent via:	none	
Received via:	none	
Data Breach:	**none**	
Data Breach Risks:	This data asset has no data breach potential.	

Trust Boundaries

In total **2 trust boundaries** have been modeled during the threat modeling process.

Application Network

Application Network

ID:	application-network
Type:	network-cloud-provider
Tags:	aws
Assets inside:	API gateway
Boundaries nested:	Cluster Group

Cluster Group

Cluster Security group

ID:	cluster-group
Type:	network-cloud-security-group
Tags:	none
Assets inside:	Inventory Service, Load Balancer, Messaging Queue, Order Service, Payment Service, Database cluster, User Service
Boundaries nested:	none

Shared Runtimes

In total **0 shared runtime** has been modeled during the threat modeling process.

Risk Rules Checked by Threagile

Threagile Version: 1.0.0

Threagile Build Timestamp: 20231104141112

Threagile Execution Timestamp: 20250204214242

Model Filename: /dev/shm/threagile-input-1293284366/threagile-model-2879089434

Model Hash (SHA256): b713bdbe68e8c80b6127f15115a4ddcc6168009e6dca3dbaa04c018dcbe5e5ef

Threagile (see https://threagile.io for more details) is an open-source toolkit for agile threat modeling, created by Christian Schneider (https://christian-schneider.net): It allows to model an architecture with its assets in an agile fashion as a YAML file directly inside the IDE. Upon execution of the Threagile toolkit all standard risk rules (as well as individual custom rules if present) are checked against the architecture model. At the time the Threagile toolkit was executed on the model input file the following risk rules were checked:

Accidental Secret Leak

accidental-secret-leak

STRIDE: Information Disclosure

Description: Sourcecode repositories (including their histories) as well as artifact registries can accidentally contain secrets like checked-in or packaged-in passwords, API tokens, certificates, crypto keys, etc.

Detection: In-scope sourcecode repositories and artifact registries.

Rating: The risk rating depends on the sensitivity of the technical asset itself and of the data assets processed and stored.

Code Backdooring

code-backdooring

STRIDE: Tampering

Description: For each build-pipeline component Code Backdooring risks might arise where attackers compromise the build-pipeline in order to let backdoored artifacts be shipped into production. Aside from direct code backdooring this includes backdooring of dependencies and even of more lower-level build infrastructure, like backdooring compilers (similar to what the XcodeGhost malware did) or dependencies.

Detection: In-scope development relevant technical assets which are either accessed by out-of-scope unmanaged developer clients and/or are directly accessed by any kind of internet-located (non-VPN) component or are themselves directly located on the internet.

Rating: The risk rating depends on the confidentiality and integrity rating of the code being handled and deployed as well as the placement/calling of this technical asset on/from the internet.

Container Base Image Backdooring

container-baseimage-backdooring

STRIDE: Tampering

Description: When a technical asset is built using container technologies, Base Image Backdooring risks might arise where base images and other layers used contain vulnerable components or backdoors.

Detection: In-scope technical assets running as containers.

Rating: The risk rating depends on the sensitivity of the technical asset itself and of the data assets.

Container Platform Escape

container-platform-escape

STRIDE: Elevation of Privilege

Description: Container platforms are especially interesting targets for attackers as they host big parts of a containerized runtime infrastructure. When not configured and operated with security best practices in mind, attackers might exploit a vulnerability inside an container and escape towards the platform as highly privileged users. These scenarios might give attackers capabilities to attack every other container as owning the container platform (via container escape attacks) equals to owning every container.

Detection: In-scope container platforms.

Rating: The risk rating depends on the sensitivity of the technical asset itself and of the data assets processed and stored.

Cross-Site Request Forgery (CSRF)

cross-site-request-forgery

STRIDE: Spoofing

Description: When a web application is accessed via web protocols Cross-Site Request Forgery (CSRF) risks might arise.

Detection: In-scope web applications accessed via typical web access protocols.

Rating: The risk rating depends on the integrity rating of the data sent across the communication link.

Cross-Site Scripting (XSS)

cross-site-scripting

STRIDE: Tampering

Description: For each web application Cross-Site Scripting (XSS) risks might arise. In terms of the overall risk level take other applications running on the same domain into account as well.

Detection: In-scope web applications.

Rating: The risk rating depends on the sensitivity of the data processed or stored in the web application.

DoS-risky Access Across Trust-Boundary

dos-risky-access-across-trust-boundary

STRIDE: Denial of Service

Description: Assets accessed across trust boundaries with critical or mission-critical availability rating are more prone to Denial-of-Service (DoS) risks.

Detection: In-scope technical assets (excluding load-balancer) with availability rating of critical or higher which have incoming data-flows across a network trust-boundary (excluding devops usage).

Rating: Matching technical assets with availability rating of critical or higher are at low risk. When the availability rating is mission-critical and neither a VPN nor IP filter for the incoming data-flow nor redundancy for the asset is applied, the risk-rating is considered medium.

Incomplete Model

incomplete-model

STRIDE: Information Disclosure

Description: When the threat model contains unknown technologies or transfers data over unknown protocols, this is an indicator for an incomplete model.

Detection: All technical assets and communication links with technology type or protocol type specified as unknown.

Rating: low

LDAP-Injection

ldap-injection

STRIDE: Tampering

Description: When an LDAP server is accessed LDAP-Injection risks might arise. The risk rating depends on the sensitivity of the LDAP server itself and of the data assets processed or stored.

Detection: In-scope clients accessing LDAP servers via typical LDAP access protocols.

Rating: The risk rating depends on the sensitivity of the LDAP server itself and of the data assets processed or stored.

Missing Authentication

missing-authentication

STRIDE: Elevation of Privilege

Description: Technical assets (especially multi-tenant systems) should authenticate incoming requests when the asset processes or stores sensitive data.

Detection: In-scope technical assets (except load-balancer, reverse-proxy, service-registry, waf, ids, and ips and in-process calls) should authenticate incoming requests when the asset processes or stores sensitive data. This is especially the case for all multi-tenant assets (there even non-sensitive ones).

Rating: The risk rating (medium or high) depends on the sensitivity of the data sent across the communication link. Monitoring callers are exempted from this risk.

Missing Two-Factor Authentication (2FA)

missing-authentication-second-factor

STRIDE: Elevation of Privilege

Description: Technical assets (especially multi-tenant systems) should authenticate incoming requests with two-factor (2FA) authentication when the asset processes or stores highly sensitive data (in terms of confidentiality, integrity, and availability) and is accessed by humans.

Detection: In-scope technical assets (except load-balancer, reverse-proxy, waf, ids, and ips) should authenticate incoming requests via two-factor authentication (2FA) when the asset processes or stores highly sensitive data (in terms of confidentiality, integrity, and availability) and is accessed by a client used by a human user.

Rating: medium

Missing Build Infrastructure

missing-build-infrastructure

STRIDE: Tampering

Description: The modeled architecture does not contain a build infrastructure (devops-client, sourcecode-repo, build-pipeline, etc.), which might be the risk of a model missing critical assets (and thus not seeing their risks). If the architecture contains custom-developed parts, the pipeline where code gets developed and built needs to be part of the model.

Detection: Models with in-scope custom-developed parts missing in-scope development (code creation) and build infrastructure components (devops-client, sourcecode-repo, build-pipeline, etc.).

Rating: The risk rating depends on the highest sensitivity of the in-scope assets running custom-developed parts.

Missing Cloud Hardening

missing-cloud-hardening

STRIDE: Tampering

Description: Cloud components should be hardened according to the cloud vendor best practices. This affects their configuration, auditing, and further areas.

Detection: In-scope cloud components (either residing in cloud trust boundaries or more specifically tagged with cloud provider types).

Rating: The risk rating depends on the sensitivity of the technical asset itself and of the data assets processed and stored.

Missing File Validation

missing-file-validation

STRIDE: Spoofing

Description: When a technical asset accepts files, these input files should be strictly validated about filename and type.

Detection: In-scope technical assets with custom-developed code accepting file data formats.

Rating: The risk rating depends on the sensitivity of the technical asset itself and of the data assets processed and stored.

Missing Hardening

missing-hardening

STRIDE: Tampering

Description: Technical assets with a Relative Attacker Attractiveness (RAA) value of 55 % or higher should be explicitly hardened taking best practices and vendor hardening guides into account.

Detection: In-scope technical assets with RAA values of 55 % or higher. Generally for high-value targets like datastores, application servers, identity providers and ERP systems this limit is reduced to 40 %

Rating: The risk rating depends on the sensitivity of the data processed or stored in the technical asset.

Missing Identity Propagation

missing-identity-propagation

STRIDE: Elevation of Privilege

Description: Technical assets (especially multi-tenant systems), which usually process data for endusers should authorize every request based on the identity of the enduser when the data flow is authenticated (i.e. non-public). For DevOps usages at least a technical-user authorization is required.

Detection: In-scope service-like technical assets which usually process data based on enduser requests, if authenticated (i.e. non-public), should authorize incoming requests based on the propagated enduser identity when their rating is sensitive. This is especially the case for all multi-tenant assets (there even less-sensitive rated ones). DevOps usages are exempted from this risk.

Rating: The risk rating (medium or high) depends on the confidentiality, integrity, and availability rating of the technical asset.

Missing Identity Provider Isolation

missing-identity-provider-isolation

STRIDE: Elevation of Privilege

Description: Highly sensitive identity provider assets and their identity datastores should be isolated from other assets by their own network segmentation trust-boundary (execution-environment boundaries do not count as network isolation).

Detection: In-scope identity provider assets and their identity datastores when surrounded by other (not identity-related) assets (without a network trust-boundary in-between).

This risk is especially prevalent when other non-identity related assets are within the same execution environment (i.e. same database or same application server).

Rating: Default is high impact. The impact is increased to very-high when the asset missing the trust-boundary protection is rated as strictly-confidential or mission-critical.

Missing Identity Store

missing-identity-store

STRIDE: Spoofing

Description: The modeled architecture does not contain an identity store, which might be the risk of a model missing critical assets (and thus not seeing their risks).

Detection: Models with authenticated data-flows authorized via enduser-identity missing an in-scope identity store.

Rating: The risk rating depends on the sensitivity of the enduser-identity authorized technical assets and their data assets processed and stored.

Missing Network Segmentation

missing-network-segmentation

STRIDE: Elevation of Privilege

Description: Highly sensitive assets and/or datastores residing in the same network segment than other lower sensitive assets (like webservers or content management systems etc.) should be better protected by a network segmentation trust-boundary.

Detection: In-scope technical assets with high sensitivity and RAA values as well as datastores when surrounded by assets (without a network trust-boundary in-between) which are of type client-system, web-server, web-application, cms, web-service-rest, web-service-soap, build-pipeline, sourcecode-repository, monitoring, or similar and there is no direct connection between these (hence no requirement to be so close to each other).

Rating: Default is low risk. The risk is increased to medium when the asset missing the trust-boundary protection is rated as strictly-confidential or mission-critical.

Missing Vault (Secret Storage)

missing-vault

STRIDE: Information Disclosure

Description: In order to avoid the risk of secret leakage via config files (when attacked through vulnerabilities being able to read files like Path-Traversal and others), it is best practice to use a separate hardened process with proper authentication, authorization, and audit logging to access config secrets (like credentials, private keys, client certificates, etc.). This component is usually some kind of Vault.

Detection: Models without a Vault (Secret Storage).

Rating: The risk rating depends on the sensitivity of the technical asset itself and of the data assets processed and stored.

Missing Vault Isolation

missing-vault-isolation

STRIDE: Elevation of Privilege

Description: Highly sensitive vault assets and their datastores should be isolated from other assets by their own network segmentation trust-boundary (execution-environment boundaries do not count as network isolation).

Detection: In-scope vault assets when surrounded by other (not vault-related) assets (without a network trust-boundary in-between). This risk is especially prevalent when other non-vault related assets are within the same execution environment (i.e. same database or same application server).

Rating: Default is medium impact. The impact is increased to high when the asset missing the trust-boundary protection is rated as strictly-confidential or mission-critical.

Missing Web Application Firewall (WAF)

missing-waf

STRIDE: Tampering

Description: To have a first line of filtering defense, security architectures with web-services or web-applications should include a WAF in front of them. Even though a WAF is not a replacement for security (all components must be secure even without a WAF) it adds another layer of defense to the overall system by delaying some attacks and having easier attack alerting through it.

Detection: In-scope web-services and/or web-applications accessed across a network trust boundary not having a Web Application Firewall (WAF) in front of them.

Rating: The risk rating depends on the sensitivity of the technical asset itself and of the data assets processed and stored.

Mixed Targets on Shared Runtime

mixed-targets-on-shared-runtime

STRIDE: Elevation of Privilege

Description: Different attacker targets (like frontend and backend/datastore components) should not be running on the same shared (underlying) runtime.

Detection: Shared runtime running technical assets of different trust-boundaries is at risk. Also mixing backend/datastore with frontend components on the same shared runtime is considered a risk.

Rating: The risk rating (low or medium) depends on the confidentiality, integrity, and availability rating of the technical asset running on the shared runtime.

Path-Traversal

path-traversal

STRIDE: Information Disclosure

Description: When a filesystem is accessed Path-Traversal or Local-File-Inclusion (LFI) risks might arise. The risk rating depends on the sensitivity of the technical asset itself and of the data assets processed or stored.

Detection: Filesystems accessed by in-scope callers.

Rating: The risk rating depends on the sensitivity of the data stored inside the technical asset.

Push instead of Pull Deployment

push-instead-of-pull-deployment

STRIDE: Tampering

Description: When comparing push-based vs. pull-based deployments from a security perspective, pull-based deployments improve the overall security of the deployment targets. Every exposed interface of a production system to accept a deployment increases the attack surface of the production system, thus a pull-based approach exposes less attack surface relevant interfaces.

Detection: Models with build pipeline components accessing in-scope targets of deployment (in a non-readonly way) which are not build-related components themselves.

Rating: The risk rating depends on the highest sensitivity of the deployment targets running custom-developed parts.

Search-Query Injection

search-query-injection

STRIDE: Tampering

Description: When a search engine server is accessed Search-Query Injection risks might arise.

Detection: In-scope clients accessing search engine servers via typical search access protocols.

Rating: The risk rating depends on the sensitivity of the search engine server itself and of the data assets processed or stored.

Server-Side Request Forgery (SSRF)

server-side-request-forgery

STRIDE: Information Disclosure

Description: When a server system (i.e. not a client) is accessing other server systems via typical web protocols Server-Side Request Forgery (SSRF) or Local-File-Inclusion (LFI) or Remote-File-Inclusion (RFI) risks might arise.

Detection: In-scope non-client systems accessing (using outgoing communication links) targets with either HTTP or HTTPS protocol.

Rating: The risk rating (low or medium) depends on the sensitivity of the data assets receivable via web protocols from targets within the same network trust-boundary as well on the sensitivity of the data assets receivable via web protocols from the target asset itself. Also for cloud-based environments the exploitation impact is at least medium, as cloud backend services can be attacked via SSRF.

Service Registry Poisoning

service-registry-poisoning

STRIDE: Spoofing

Description: When a service registry used for discovery of trusted service endpoints Service Registry Poisoning risks might arise.

Detection: In-scope service registries.

Rating: The risk rating depends on the sensitivity of the technical assets accessing the service registry as well as the data assets processed or stored.

SQL/NoSQL-Injection

sql-nosql-injection

STRIDE: Tampering

Description: When a database is accessed via database access protocols SQL/NoSQL-Injection risks might arise. The risk rating depends on the sensitivity technical asset itself and of the data assets processed or stored.

Detection: Database accessed via typical database access protocols by in-scope clients.

Rating: The risk rating depends on the sensitivity of the data stored inside the database.

Unchecked Deployment

unchecked-deployment

STRIDE: Tampering

Description: For each build-pipeline component Unchecked Deployment risks might arise when the build-pipeline does not include established DevSecOps best-practices. DevSecOps best-practices scan as part of CI/CD pipelines for vulnerabilities in source- or byte-code, dependencies, container layers, and dynamically against running test systems. There are several open-source and commercial tools existing in the categories DAST, SAST, and IAST.

Detection: All development-relevant technical assets.

Rating: The risk rating depends on the highest rating of the technical assets and data assets processed by deployment-receiving targets.

Unencrypted Technical Assets

unencrypted-asset

STRIDE: Information Disclosure

Description: Due to the confidentiality rating of the technical asset itself and/or the processed data assets this technical asset must be encrypted. The risk rating depends on the sensitivity technical asset itself and of the data assets stored.

Detection: In-scope unencrypted technical assets (excluding reverse-proxy, load-balancer, waf, ids, ips and embedded components like library) storing data assets rated at least as confidential or critical. For technical assets storing data assets rated as strictly-confidential or mission-critical the encryption must be of type data-with-enduser-individual-key.

Rating: Depending on the confidentiality rating of the stored data-assets either medium or high risk.

Unencrypted Communication

unencrypted-communication

STRIDE: Information Disclosure

Description: Due to the confidentiality and/or integrity rating of the data assets transferred over the communication link this connection must be encrypted.

Detection: Unencrypted technical communication links of in-scope technical assets (excluding monitoring traffic as well as local-file-access and in-process-library-call) transferring sensitive data.

Rating: Depending on the confidentiality rating of the transferred data-assets either medium or high risk.

Unguarded Access From Internet

unguarded-access-from-internet

STRIDE: Elevation of Privilege

Description: Internet-exposed assets must be guarded by a protecting service, application, or reverse-proxy.

Detection: In-scope technical assets (excluding load-balancer) with confidentiality rating of confidential (or higher) or with integrity rating of critical (or higher) when accessed directly from the internet. All web-server, web-application, reverse-proxy, waf, and gateway assets are exempted from this risk when they do not consist of custom developed code and the data-flow only consists of HTTP or FTP protocols. Access from monitoring systems as well as VPN-protected connections are exempted.

Rating: The matching technical assets are at low risk. When either the confidentiality rating is strictly-confidential or the integrity rating is mission-critical, the risk-rating is considered medium. For assets with RAA values higher than 40 % the risk-rating increases.

Unguarded Direct Datastore Access

unguarded-direct-datastore-access

STRIDE: Elevation of Privilege

Description: Datastores accessed across trust boundaries must be guarded by some protecting service or application.

Detection: In-scope technical assets of type datastore (except identity-store-ldap when accessed from identity-provider and file-server when accessed via file transfer protocols) with confidentiality rating of confidential (or higher) or with integrity rating of critical (or higher) which have incoming data-flows from assets outside across a network trust-boundary. DevOps config and deployment access is excluded from this risk.

Rating: The matching technical assets are at low risk. When either the confidentiality rating is strictly-confidential or the integrity rating is mission-critical, the risk-rating is considered medium. For assets with RAA values higher than 40 % the risk-rating increases.

Unnecessary Communication Link

unnecessary-communication-link

STRIDE: Elevation of Privilege

Description: When a technical communication link does not send or receive any data assets, this is an indicator for an unnecessary communication link (or for an incomplete model).

Detection: In-scope technical assets' technical communication links not sending or receiving any data assets.

Rating: low

Unnecessary Data Asset

unnecessary-data-asset

STRIDE: Elevation of Privilege

Description: When a data asset is not processed or stored by any data assets and also not transferred by any communication links, this is an indicator for an unnecessary data asset (or for an incomplete model).

Detection: Modelled data assets not processed or stored by any data assets and also not transferred by any communication links.

Rating: low

Unnecessary Data Transfer

unnecessary-data-transfer

STRIDE: Elevation of Privilege

Description: When a technical asset sends or receives data assets, which it neither processes or stores this is an indicator for unnecessarily transferred data (or for an incomplete model). When the unnecessarily transferred data assets are sensitive, this poses an unnecessary risk of an increased attack surface.

Detection: In-scope technical assets sending or receiving sensitive data assets which are neither processed nor stored by the technical asset are flagged with this risk. The risk rating (low or medium) depends on the confidentiality, integrity, and availability rating of the technical asset. Monitoring data is exempted from this risk.

Rating: The risk assessment is depending on the confidentiality and integrity rating of the transferred data asset either low or medium.

Unnecessary Technical Asset

unnecessary-technical-asset

STRIDE: Elevation of Privilege

Description: When a technical asset does not process or store any data assets, this is an indicator for an unnecessary technical asset (or for an incomplete model). This is also the case if the asset has no communication links (either outgoing or incoming).

Detection: Technical assets not processing or storing any data assets.

Rating: low

Untrusted Deserialization

untrusted-deserialization

STRIDE: Tampering

Description: When a technical asset accepts data in a specific serialized form (like Java or .NET serialization), Untrusted Deserialization risks might arise.

Detection: In-scope technical assets accepting serialization data formats (including EJB and RMI protocols).

Rating: The risk rating depends on the sensitivity of the technical asset itself and of the data assets processed and stored.

Wrong Communication Link Content

wrong-communication-link-content

STRIDE: Information Disclosure

Description: When a communication link is defined as readonly, but does not receive any data asset, or when it is defined as not readonly, but does not send any data asset, it is likely to be a model failure.

Detection: Communication links with inconsistent data assets being sent/received not matching their readonly flag or otherwise inconsistent protocols not matching the target technology type.

Rating: low

Wrong Trust Boundary Content

wrong-trust-boundary-content

STRIDE: Elevation of Privilege

Description: When a trust boundary of type network-policy-namespace-isolation contains non-container assets it is likely to be a model failure.

Detection: Trust boundaries which should only contain containers, but have different assets inside.

Rating: low

XML External Entity (XXE)

xml-external-entity

STRIDE: Information Disclosure

Description: When a technical asset accepts data in XML format, XML External Entity (XXE) risks might arise.

Detection: In-scope technical assets accepting XML data formats.

Rating: The risk rating depends on the sensitivity of the technical asset itself and of the data assets processed and stored. Also for cloud-based environments the exploitation impact is at least medium, as cloud backend services can be attacked via SSRF (and XXE vulnerabilities are often also SSRF vulnerabilities).

Disclaimer

Kshitija Kulkarni conducted this threat analysis using the open-source Threagile toolkit on the applications and systems that were modeled as of this report's date. Information security threats are continually changing, with new vulnerabilities discovered on a daily basis, and no application can ever be 100% secure no matter how much threat modeling is conducted. It is recommended to execute threat modeling and also penetration testing on a regular basis (for example yearly) to ensure a high ongoing level of security and constantly check for new attack vectors.

This report cannot and does not protect against personal or business loss as the result of use of the applications or systems described. Kshitija Kulkarni and the Threagile toolkit offers no warranties, representations or legal certifications concerning the applications or systems it tests. All software includes defects: nothing in this document is intended to represent or warrant that threat modeling was complete and without error, nor does this document represent or warrant that the architecture analyzed is suitable to task, free of other defects than reported, fully compliant with any industry standards, or fully compatible with any operating system, hardware, or other application. Threat modeling tries to analyze the modeled architecture without having access to a real working system and thus cannot and does not test the implementation for defects and vulnerabilities. These kinds of checks would only be possible with a separate code review and penetration test against a working system and not via a threat model.

By using the resulting information you agree that Kshitija Kulkarni and the Threagile toolkit shall be held harmless in any event.

This report is confidential and intended for internal, confidential use by the client. The recipient is obligated to ensure the highly confidential contents are kept secret. The recipient assumes responsibility for further distribution of this document.

In this particular project, a timebox approach was used to define the analysis effort. This means that the author allotted a prearranged amount of time to identify and document threats. Because of this, there is no guarantee that all possible threats and risks are discovered. Furthermore, the analysis applies to a snapshot of the current state of the modeled architecture (based on the architecture information provided by the customer) at the examination time.

Report Distribution

Distribution of this report (in full or in part like diagrams or risk findings) requires that this disclaimer as well as the chapter about the Threagile toolkit and method used is kept intact as part of the distributed report or referenced from the distributed parts.