Threagile
Agile Threat Modeling

Threat Model Report

IAC Infrastructure

4 January 2024

Shashank Sanap

https://github.com/Shashanksanap99/

Table of Contents

Management Summary

Threagile toolkit was used to model the architecture of "IAC Infrastructure" 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 "IAC Infrastructure" 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 **53 initial risks** in **20 categories** have been identified during the threat modeling process:

0 critical risk		**53 unchecked**
2 high risk		**0 in discussion**
16 elevated risk		**0 accepted**
29 medium risk		**0 in progress**
6 low risk		**0 *mitigated***
		0 *false positive*
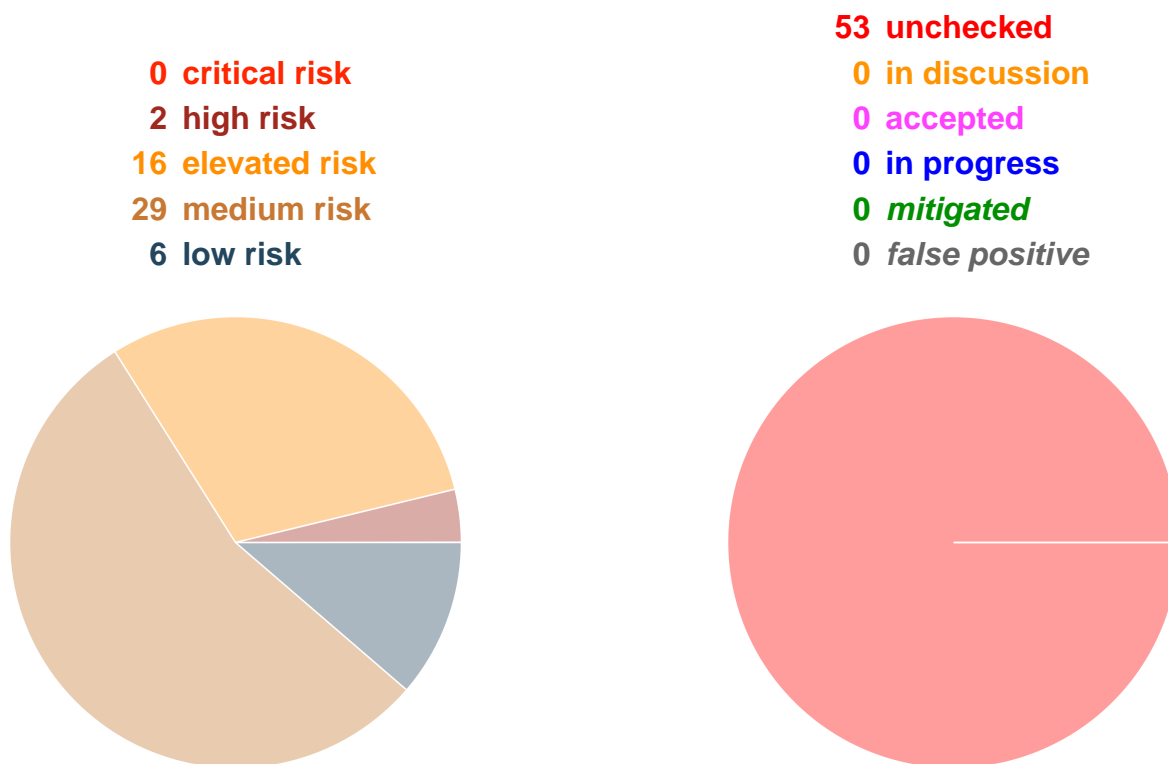
IAC CloudFormation facilitates the creation of a AWS architecture consist of VPC with defined public and private subnets across multiple availability zones.

Impact Analysis of 53 Initial Risks in 20 Categories

The most prevalent impacts of the **53 initial risks** (distributed over **20 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.

High: **SQL/NoSQL-Injection**: 2 Initial Risks - Exploitation likelihood is *Very 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.

High: **XML External Entity (XXE)**: 1 Initial Risk - Exploitation likelihood is *Very Likely* with *High* impact.
If this risk is unmitigated, attackers might be able to read sensitive files (configuration data, key/credential files, deployment files, business data files, etc.) form the filesystem of affected components and/or access sensitive services or files of other components.

Elevated: **Cross-Site Scripting (XSS)**: 5 Initial Risks - Exploitation likelihood is *Likely* with *High* impact.
If this risk remains unmitigated, attackers might be able to access individual victim sessions and steal or modify user data.

Elevated: **Missing Authentication**: 1 Initial Risk - Exploitation likelihood is *Likely* with *High* impact.
If this risk is unmitigated, attackers might be able to access or modify sensitive data in an unauthenticated way.

Elevated: **Missing Cloud Hardening**: 5 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 File Validation**: 1 Initial Risk - Exploitation likelihood is *Very Likely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to provide malicious files to the application.

Elevated: **Missing Hardening**: 1 Initial Risk - Exploitation likelihood is *Likely* with *Medium* impact.
If this risk remains unmitigated, attackers might be able to easier attack high-value targets.

Elevated: **Server-Side Request Forgery (SSRF)**: 3 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.

Medium: **Cross-Site Request Forgery (CSRF)**: 5 Initial Risks - Exploitation likelihood is *Very Likely* with *Low* impact.
If this risk remains unmitigated, attackers might be able to trick logged-in victim users into unwanted actions within the web application by visiting an attacker controlled web site.

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 Propagation**: 1 Initial Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to access or modify foreign data after a successful compromise of a component within the system due to missing resource-based authorization checks.

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: **Missing Web Application Firewall (WAF)**: 3 Initial Risks - Exploitation likelihood is *Unlikely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to apply standard attack pattern tests at great speed without any filtering.

Medium: **Mixed Targets on Shared Runtime**: 1 Initial Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
If this risk is unmitigated, attackers successfully attacking other components of the system might have an easy path towards more valuable targets, as they are running on the same shared runtime.

Medium: **Unencrypted Communication**: 2 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**: 7 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: **Unguarded Access From Internet**: 1 Initial Risk - Exploitation likelihood is *Very Likely* with *Low* 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: **Unnecessary Data Transfer**: 8 Initial Risks - Exploitation likelihood is *Unlikely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to target unnecessarily transferred data.

Low: **DoS-risky Access Across Trust-Boundary**: 3 Initial Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
If this risk remains unmitigated, attackers might be able to disturb the availability of important parts of the system.

Risk Mitigation

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

53 unchecked
 0 in discussion
 0 accepted
 0 in progress
 0 *mitigated*
 0 *false positive*
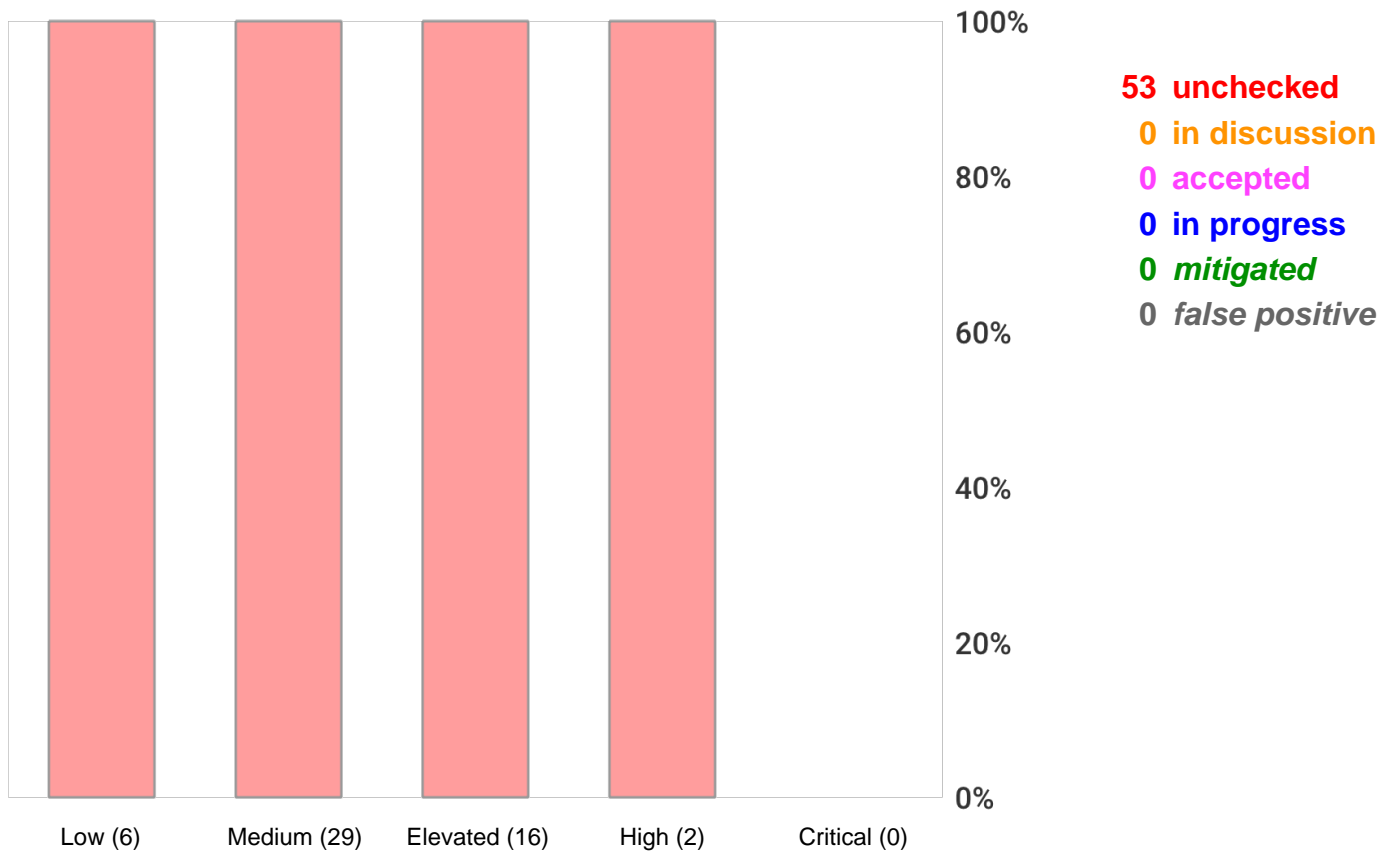
After removal of risks with status *mitigated* and *false positive* the following **53 remain unmitigated**:

 0 unmitigated critical risk
 2 unmitigated high risk   **1 business side related**
16 unmitigated elevated risk   **13 architecture related**
29 unmitigated medium risk   **17 development related**
 6 unmitigated low risk   **22 operations related**
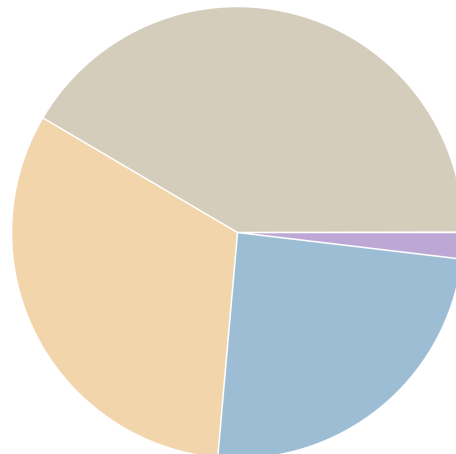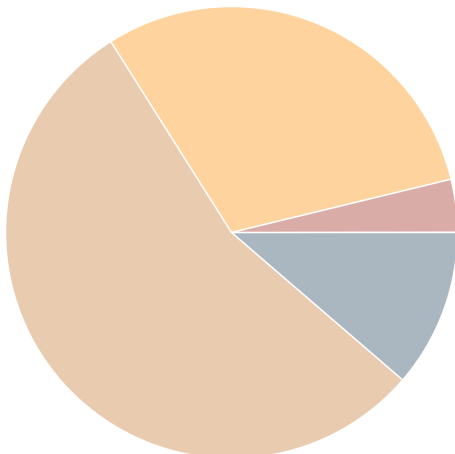
Impact Analysis of 53 Remaining Risks in 20 Categories

The most prevalent impacts of the **53 remaining risks** (distributed over **20 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.

High: **SQL/NoSQL-Injection**: 2 Remaining Risks - Exploitation likelihood is *Very 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.

High: **XML External Entity (XXE)**: 1 Remaining Risk - Exploitation likelihood is *Very Likely* with *High* impact.
If this risk is unmitigated, attackers might be able to read sensitive files (configuration data, key/credential files, deployment files, business data files, etc.) form the filesystem of affected components and/or access sensitive services or files of other components.

Elevated: **Cross-Site Scripting (XSS)**: 5 Remaining Risks - Exploitation likelihood is *Likely* with *High* impact.
If this risk remains unmitigated, attackers might be able to access individual victim sessions and steal or modify user data.

Elevated: **Missing Authentication**: 1 Remaining Risk - Exploitation likelihood is *Likely* with *High* impact.
If this risk is unmitigated, attackers might be able to access or modify sensitive data in an unauthenticated way.

Elevated: **Missing Cloud Hardening**: 5 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 File Validation**: 1 Remaining Risk - Exploitation likelihood is *Very Likely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to provide malicious files to the application.

Elevated: **Missing Hardening**: 1 Remaining Risk - Exploitation likelihood is *Likely* with *Medium* impact.
If this risk remains unmitigated, attackers might be able to easier attack high-value targets.

Elevated: **Server-Side Request Forgery (SSRF)**: 3 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.

Medium: **Cross-Site Request Forgery (CSRF)**: 5 Remaining Risks - Exploitation likelihood is *Very Likely* with *Low* impact.
If this risk remains unmitigated, attackers might be able to trick logged-in victim users into unwanted actions within the web application by visiting an attacker controlled web site.

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 Propagation**: 1 Remaining Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to access or modify foreign data after a successful compromise of a component within the system due to missing resource-based authorization checks.

Medium: **Missing Two-Factor Authentication (2FA)**: 1 Remaining 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 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: **Missing Web Application Firewall (WAF)**: 3 Remaining Risks - Exploitation likelihood is *Unlikely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to apply standard attack pattern tests at great speed without any filtering.

Medium: **Mixed Targets on Shared Runtime**: 1 Remaining Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
If this risk is unmitigated, attackers successfully attacking other components of the system might have an easy path towards more valuable targets, as they are running on the same shared runtime.

Medium: **Unencrypted Communication**: 2 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**: 7 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: **Unguarded Access From Internet**: 1 Remaining Risk - Exploitation likelihood is *Very Likely* with *Low* 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: **Unnecessary Data Transfer**: 8 Remaining Risks - Exploitation likelihood is *Unlikely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to target unnecessarily transferred data.

Low: **DoS-risky Access Across Trust-Boundary**: 3 Remaining Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
If this risk remains unmitigated, attackers might be able to disturb the availability of important parts of the system.

Application Overview

Business Criticality

The overall business criticality of "IAC Infrastructure" was rated as:

(archive | operational | **IMPORTANT** | critical | mission-critical)

Business Overview

A scalable and secure network is offered by AWS infrastructure on Amazon Web Services (AWS).It guarantees a robust architecture strong enough to support important parts like databases and application servers. This architecture serves companies looking for a stable, flexible, and secure cloud-based environment to support their operations by enabling dependable application hosting and effective database management.

Technical Overview

AWS network infrastructure configures a Virtual Private Cloud (VPC) with defined CIDR blocks, enabling DNS support and hostnames. The setup includes public and private subnets across multiple availability zones for high availability and fault tolerance.Key components of this setup include an internet gateway for external connectivity, route tables to manage traffic flow within the VPC,and security groups to control access to instances. The infrastructure comprises various instances a Linux bastion host in the public subnet for secure SSH access,an application server in the private subnet, and a database instance with security group.

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.
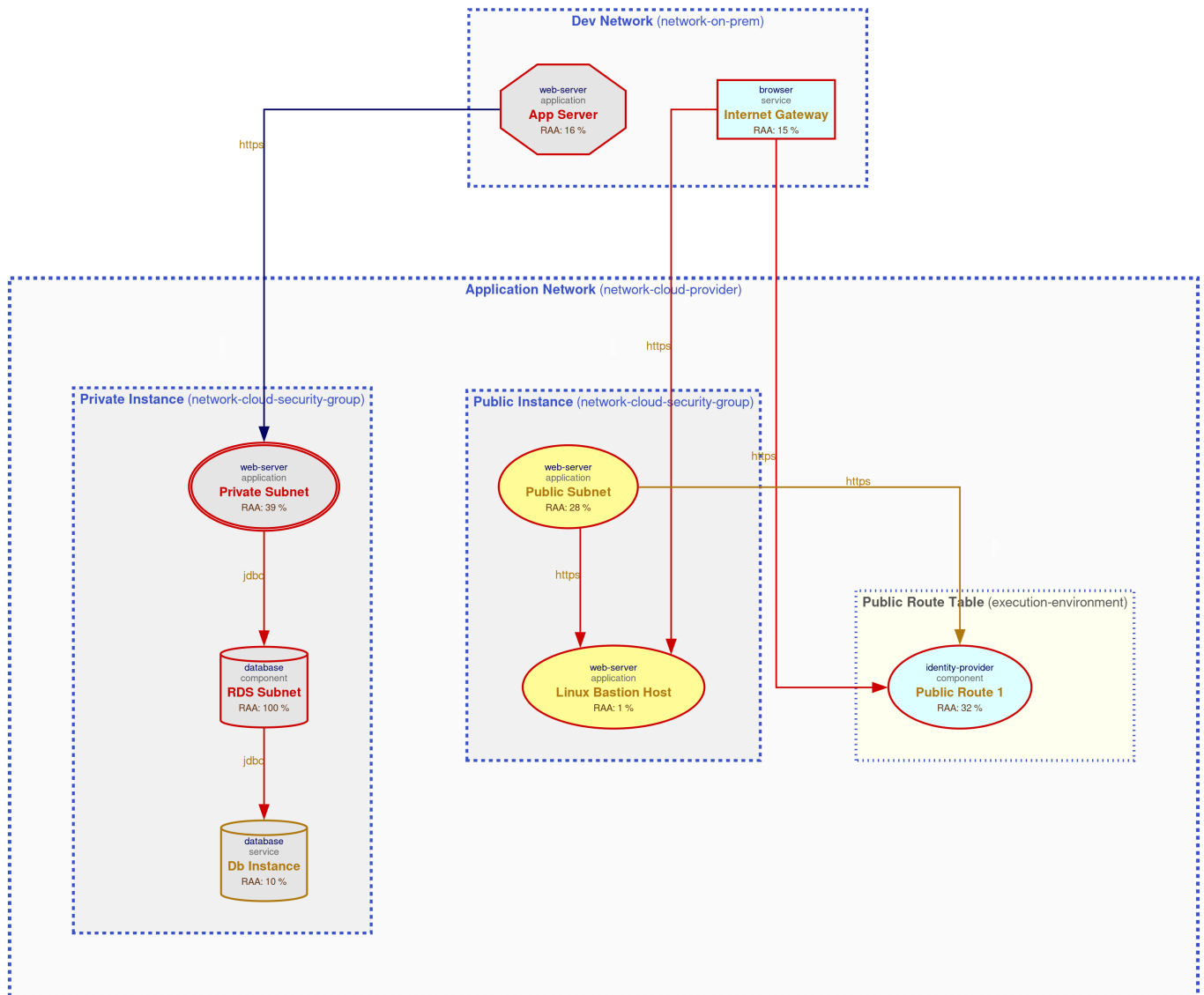
Security Requirements

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

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

Securing Administrative Access
Administrative access must be secured with strong encryption and multi-factor authentication.

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.

AWS-System Compromise
As a hacker I want to access the VPC System in order to steal/modify sensitive business data.

Cross-Site Scripting Attacks
As a hacker I want to execute Cross-Site Scripting (XSS) and similar attacks in order to takeover victim sessions and cause reputational damage.

Database Compromise
As a hacker I want to access the database backend of the rds-Subnet in order to steal/modify sensitive business data.

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 DB Functionality
As a hacker I want to disturb the functionality of the Database system to cause indirect financial damage.

Denial-of-Service of Enduser Functionality
As a hacker I want to disturb the functionality of the enduser parts of the application in order to cause direct financial damage.

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.

PII 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.

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

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:ec2
Internal Access, Public Subnet, Private Instance, Public Instance

aws:rds
Db Instance

aws:vpc
Application Network

linux
Db Instance, Linux Bastion Host, Private Subnet, Public Subnet, RDS Subnet

mysql
RDS Subnet, Database Customizing and Dumps

vmware
Subnet and Instance Virtualization

STRIDE Classification of Identified Risks

This chapter clusters and classifies the risks by STRIDE categories: In total **53 potential risks** have been identified during the threat modeling process of which **6 in the Spoofing** category, **17 in the Tampering** category, **0 in the Repudiation** category, **14 in the Information Disclosure** category, **3 in the Denial of Service** category, and **13 in the Elevation of Privilege** category.

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

Spoofing

Elevated: **Missing File Validation**: 1 / 1 Risk - Exploitation likelihood is *Very Likely* with *Medium* impact.
When a technical asset accepts files, these input files should be strictly validated about filename and type.

Medium: **Cross-Site Request Forgery (CSRF)**: 5 / 5 Risks - Exploitation likelihood is *Very Likely* with *Low* impact.
When a web application is accessed via web protocols Cross-Site Request Forgery (CSRF) risks might arise.

Tampering

High: **SQL/NoSQL-Injection**: 2 / 2 Risks - Exploitation likelihood is *Very 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.

Elevated: **Cross-Site Scripting (XSS)**: 5 / 5 Risks - Exploitation likelihood is *Likely* with *High* impact.
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.

Elevated: **Missing Cloud Hardening**: 5 / 5 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**: 1 / 1 Risk - 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.

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 Web Application Firewall (WAF)**: 3 / 3 Risks - Exploitation likelihood is *Unlikely* with *Medium* impact.
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.

Repudiation

n/a

Information Disclosure

High: **XML External Entity (XXE)**: 1 / 1 Risk - Exploitation likelihood is *Very Likely* with *High* impact.
When a technical asset accepts data in XML format, XML External Entity (XXE) risks might arise.

Elevated: **Server-Side Request Forgery (SSRF)**: 3 / 3 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**: 2 / 2 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**: 7 / 7 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.

Denial of Service

Low: **DoS-risky Access Across Trust-Boundary**: 3 / 3 Risks - Exploitation likelihood is *Unlikely* with *Low* 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: **Missing Authentication**: 1 / 1 Risk - Exploitation likelihood is *Likely* with *High* impact.
Technical assets (especially multi-tenant systems) should authenticate incoming requests when the asset processes or stores sensitive data.

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

Medium: **Missing Two-Factor Authentication (2FA)**: 1 / 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: **Mixed Targets on Shared Runtime**: 1 / 1 Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
Different attacker targets (like frontend and backend/datastore components) should not be running on the same shared (underlying) runtime.

Medium: **Unguarded Access From Internet**: 1 / 1 Risk - Exploitation likelihood is *Very Likely* with *Low* impact.
Internet-exposed assets must be guarded by a protecting service, application, or reverse-proxy.

Medium: **Unnecessary Data Transfer**: 8 / 8 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.

Assignment by Function

This chapter clusters and assigns the risks by functions which are most likely able to check and mitigate them: In total **53 potential risks** have been identified during the threat modeling process of which **1 should be checked by Business Side**, **13 should be checked by Architecture**, **17 should be checked by Development**, and **22 should be checked by Operations**.

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

Business Side

Medium: **Missing Two-Factor Authentication (2FA)**: 1 / 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: **Missing Authentication**: 1 / 1 Risk - Exploitation likelihood is *Likely* with *High* impact.
Apply an authentication method to the technical asset. To protect highly sensitive data consider the use of two-factor authentication for human users.

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

Medium: **Missing Identity Propagation**: 1 / 1 Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
When processing requests for endusers if possible authorize in the backend against the propagated identity of the enduser. This can be achieved in passing JWTs or similar tokens and checking them in the backend services. For DevOps usages apply at least a technical-user authorization.

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: **Unguarded Access From Internet**: 1 / 1 Risk - Exploitation likelihood is *Very Likely* with *Low* 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: **Unnecessary Data Transfer**: 8 / 8 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.

Development

High: **SQL/NoSQL-Injection**: 2 / 2 Risks - Exploitation likelihood is *Very 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.

High: **XML External Entity (XXE)**: 1 / 1 Risk - Exploitation likelihood is *Very Likely* with *High* impact.
Apply hardening of all XML parser instances in order to stay safe from XML External Entity (XXE) 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: **Cross-Site Scripting (XSS)**: 5 / 5 Risks - Exploitation likelihood is *Likely* with *High* impact.
Try to encode all values sent back to the browser and also handle DOM-manipulations in a safe way to avoid DOM-based XSS. 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: **Missing File Validation**: 1 / 1 Risk - Exploitation likelihood is *Very Likely* with *Medium* impact.
Filter by file extension and discard (if feasible) the name provided. Whitelist the accepted file types and determine the mime-type on the server-side (for example via "Apache Tika" or similar checks). If the file is retrievable by endusers and/or backoffice employees, consider performing scans for popular malware (if the files can be retrieved much later than they were uploaded, also apply a fresh malware scan during retrieval to scan with newer signatures of popular malware). Also enforce limits on maximum file size to avoid denial-of-service like scenarios.

Elevated: **Server-Side Request Forgery (SSRF)**: 3 / 3 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.

Medium: **Cross-Site Request Forgery (CSRF)**: 5 / 5 Risks - Exploitation likelihood is *Very Likely* with *Low* impact.
Try to use anti-CSRF tokens ot the double-submit patterns (at least for logged-in requests). When your authentication scheme depends on cookies (like session or token cookies), consider marking them with the same-site flag. 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**: 5 / 5 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**: 1 / 1 Risk - 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: **Missing Web Application Firewall (WAF)**: 3 / 3 Risks - Exploitation likelihood is *Unlikely* with *Medium* impact.
Consider placing a Web Application Firewall (WAF) in front of the web-services and/or web-applications. For cloud environments many cloud providers offer pre-configured WAFs. Even reverse proxies can be enhances by a WAF component via ModSecurity plugins.

Medium: **Mixed Targets on Shared Runtime**: 1 / 1 Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
Use separate runtime environments for running different target components or apply similar separation styles to prevent load- or breach-related problems originating from one more attacker-facing asset impacts also the other more critical rated backend/datastore assets.

Medium: **Unencrypted Communication**: 2 / 2 Risks - Exploitation likelihood is *Unlikely* with *High* impact.
Apply transport layer encryption to the communication link.

Medium: **Unencrypted Technical Assets**: 7 / 7 Risks - Exploitation likelihood is *Unlikely* with *High* impact.
Apply encryption to the technical asset.

Low: **DoS-risky Access Across Trust-Boundary**: 3 / 3 Risks - Exploitation likelihood is *Unlikely* with *Low* 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.

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.

RDS Subnet: RAA 100%
The database behind the private subnet

Private Subnet: RAA 39%
Used for database and app server

Public Route 1: RAA 32%
Public Route 1

Public Subnet: RAA 28%
Public Subnet hosting the client-side code

App Server: RAA 16%
App Server

Internet Gateway: RAA 15%
Internet Gateway

Db Instance: RAA 10%
db instance for storing the application data in mysql database

Linux Bastion Host: RAA 1%
Linux bastion host for hosting the application

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.
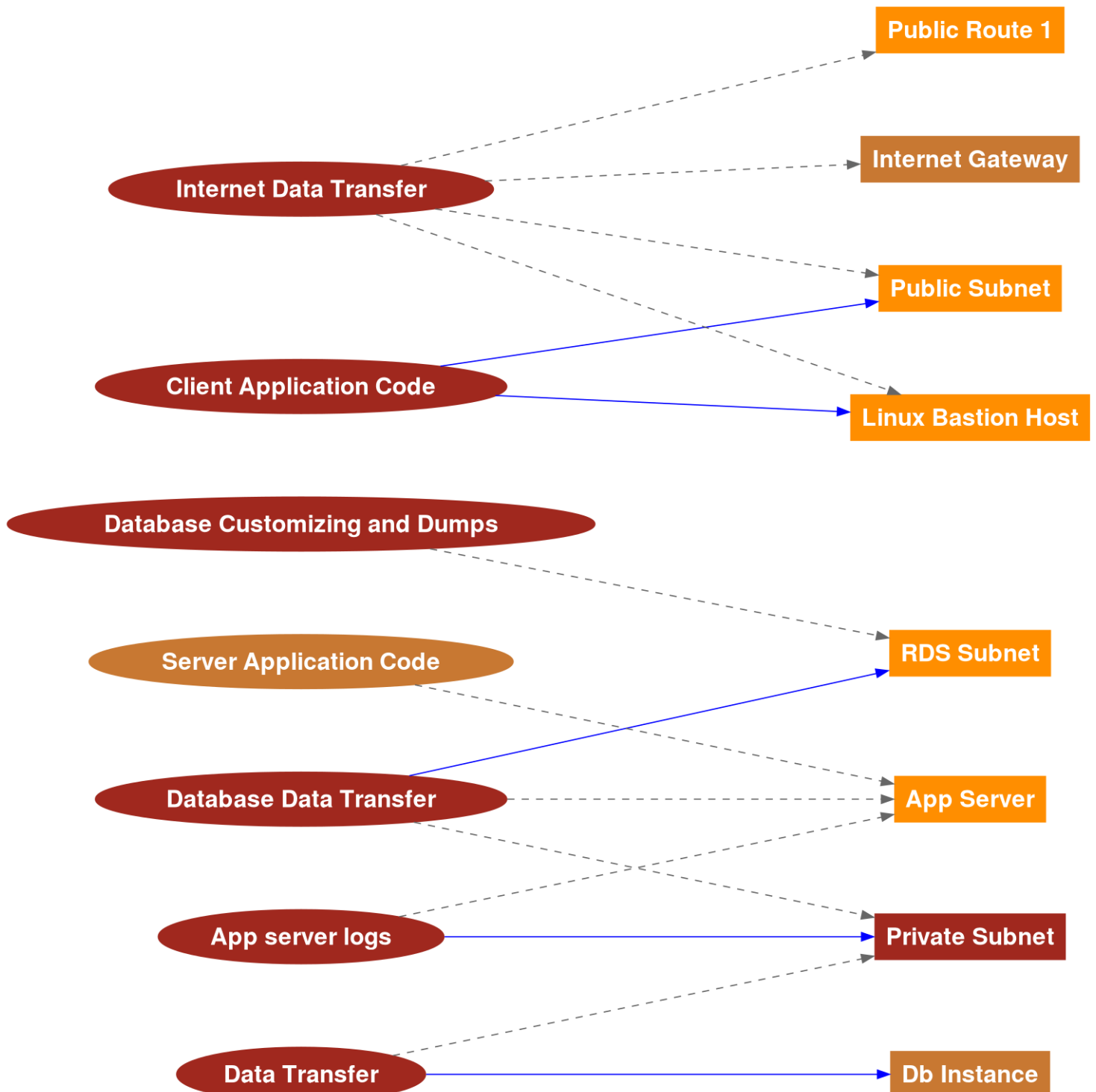
Out-of-Scope Assets: 0 Assets

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.

No technical assets have been defined as out-of-scope.

Potential Model Failures: 10 / 10 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 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**: 8 / 8 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.

Questions: 0 / 0 Questions

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

No custom questions arose during the threat modeling process.

Identified Risks by Vulnerability Category

In total **53 potential risks** have been identified during the threat modeling process of which **0 are rated as critical**, **2 as high**, **16 as elevated**, **29 as medium**, and **6 as low**.

These risks are distributed across **20 vulnerability categories**. The following sub-chapters of this section describe each identified risk category.

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.

High Risk Severity

SQL/NoSQL-Injection risk at **Private Subnet** against database **RDS Subnet** via **Database Traffic**: Exploitation likelihood is *Very Likely* with *High* impact.

sql-nosql-injection@Private-Subnet@sql-database@Private-Subnet>database-traffic

Unchecked

Elevated Risk Severity

SQL/NoSQL-Injection risk at **RDS Subnet** against database **Db Instance** via **Database Traffic**: Exploitation likelihood is *Very Likely* with *Medium* impact.

sql-nosql-injection@sql-database@db-instance@sql-database>database-traffic

Unchecked

XML External Entity (XXE): 1 / 1 Risk

Description (Information Disclosure): CWE 611

When a technical asset accepts data in XML format, XML External Entity (XXE) risks might arise.

Impact

If this risk is unmitigated, attackers might be able to read sensitive files (configuration data, key/credential files, deployment files, business data files, etc.) form the filesystem of affected components and/or access sensitive services or files of other components.

Detection Logic

In-scope technical assets accepting XML data formats.

Risk 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).

False Positives

Fully trusted (i.e. cryptographically signed or similar) XML data can be considered as false positives after individual review.

Mitigation (Development): XML Parser Hardening

Apply hardening of all XML parser instances in order to stay safe from XML External Entity (XXE) 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: V14 - Configuration Verification Requirements
Cheat Sheet: XML_External_Entity_Prevention_Cheat_Sheet

Check

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

Risk Findings

The risk **XML External Entity (XXE)** 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.

High Risk Severity

XML External Entity (XXE) risk at **Private Subnet**: Exploitation likelihood is *Very Likely* with *High* impact.

xml-external-entity@Private-Subnet

Unchecked

Cross-Site Scripting (XSS): 5 / 5 Risks

Description (Tampering): CWE 79

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.

Impact

If this risk remains unmitigated, attackers might be able to access individual victim sessions and steal or modify user data.

Detection Logic

In-scope web applications.

Risk Rating

The risk rating depends on the sensitivity of the data processed or stored in the web application.

False Positives

When the technical asset is not accessed via a browser-like component (i.e not by a human user initiating the request that gets passed through all components until it reaches the web application) this can be considered a false positive.

Mitigation (Development): XSS Prevention

Try to encode all values sent back to the browser and also handle DOM-manipulations in a safe way to avoid DOM-based XSS. 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: Cross_Site_Scripting_Prevention_Cheat_Sheet

Check

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

Risk Findings

The risk **Cross-Site Scripting (XSS)** 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.

Elevated Risk Severity

Cross-Site Scripting (XSS) risk at **App Server**: Exploitation likelihood is *Likely* with *High* impact.

cross-site-scripting@app-server

Unchecked

Cross-Site Scripting (XSS) risk at **Linux Bastion Host**: Exploitation likelihood is *Likely* with *High* impact.

cross-site-scripting@Linux-Bastion-Host

Unchecked

Cross-Site Scripting (XSS) risk at **Private Subnet**: Exploitation likelihood is *Likely* with *High* impact.

cross-site-scripting@Private-Subnet

Unchecked

Cross-Site Scripting (XSS) risk at **Public Route 1**: Exploitation likelihood is *Likely* with *High* impact.

cross-site-scripting@public-route-1

Unchecked

Cross-Site Scripting (XSS) risk at **Public Subnet**: Exploitation likelihood is *Likely* with *High* impact.

cross-site-scripting@Public-Subnet

Unchecked

Missing Authentication: 1 / 1 Risk

Description (Elevation of Privilege): CWE 306

Technical assets (especially multi-tenant systems) should authenticate incoming requests when the asset processes or stores sensitive data.

Impact

If this risk is unmitigated, attackers might be able to access or modify sensitive data in an unauthenticated way.

Detection Logic

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).

Risk 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.

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 (Architecture): Authentication of Incoming Requests

Apply an authentication method to the technical asset. To protect highly sensitive data consider the use of two-factor authentication for human users.

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 Authentication** 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.

Elevated Risk Severity

Missing Authentication covering communication link **Bastion Host Access** from **Internet Gateway** to **Linux Bastion Host**: Exploitation likelihood is *Likely* with *High* impact.

missing-authentication@internet-gateway>bastion-host-access@internet-gateway@Linux-Bastion-Host

Unchecked

Missing Cloud Hardening: 5 / 5 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 **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.

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 (AWS) risk at **Private Instance**: CIS Benchmark for AWS: Exploitation likelihood is *Unlikely* with *Very High* impact.

missing-cloud-hardening@Private-Instance

Unchecked

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

missing-cloud-hardening@Public-Instance

Unchecked

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

missing-cloud-hardening@Public-Subnet

Unchecked

Medium Risk Severity

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

missing-cloud-hardening@db-instance

Unchecked

Missing File Validation: 1 / 1 Risk

Description (Spoofing): CWE 434

When a technical asset accepts files, these input files should be strictly validated about filename and type.

Impact

If this risk is unmitigated, attackers might be able to provide malicious files to the application.

Detection Logic

In-scope technical assets with custom-developed code accepting file data formats.

Risk Rating

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

False Positives

Fully trusted (i.e. cryptographically signed or similar) files can be considered as false positives after individual review.

Mitigation (Development): File Validation

Filter by file extension and discard (if feasible) the name provided. Whitelist the accepted file types and determine the mime-type on the server-side (for example via "Apache Tika" or similar checks). If the file is retrievable by endusers and/or backoffice employees, consider performing scans for popular malware (if the files can be retrieved much later than they were uploaded, also apply a fresh malware scan during retrieval to scan with newer signatures of popular malware). Also enforce limits on maximum file size to avoid denial-of-service like scenarios.

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

Check

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

Risk Findings

The risk **Missing File Validation** 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.

Elevated Risk Severity

> **Missing File Validation** risk at **Public Subnet**: Exploitation likelihood is *Very Likely* with *Medium* impact.
>
> missing-file-validation@Public-Subnet
>
> **Unchecked**

Missing Hardening: 1 / 1 Risk

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 **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.

Elevated Risk Severity

Missing Hardening risk at **RDS Subnet**: Exploitation likelihood is *Likely* with *Medium* impact.

missing-hardening@sql-database

Unchecked

Server-Side Request Forgery (SSRF): 3 / 3 Risks

Description (Information Disclosure): <u>CWE 918</u>

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: <u>V12 - File and Resources Verification Requirements</u>
Cheat Sheet: <u>Server_Side_Request_Forgery_Prevention_Cheat_Sheet</u>

Check

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

Risk Findings

The risk **Server-Side Request Forgery (SSRF)** was found **3 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 **App Server** server-side web-requesting the target **Private Subnet** via **Internal Access**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@app-server@Private-Subnet@app-server>internal-access

Unchecked

Server-Side Request Forgery (SSRF) risk at **Public Subnet** server-side web-requesting the target **Linux Bastion Host** via **Public Subnet Include Bastion Host**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@Public-Subnet@Linux-Bastion-Host@Public-Subnet>public-subnet-include-bastion-host

Unchecked

Server-Side Request Forgery (SSRF) risk at **Public Subnet** server-side web-requesting the target **Public Route 1** via **Subnet to Route table connection**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@Public-Subnet@public-route-1@Public-Subnet>subnet-to-route-table-connection

Unchecked

Cross-Site Request Forgery (CSRF): 5 / 5 Risks

Description (Spoofing): CWE 352

When a web application is accessed via web protocols Cross-Site Request Forgery (CSRF) risks might arise.

Impact

If this risk remains unmitigated, attackers might be able to trick logged-in victim users into unwanted actions within the web application by visiting an attacker controlled web site.

Detection Logic

In-scope web applications accessed via typical web access protocols.

Risk Rating

The risk rating depends on the integrity rating of the data sent across the communication link.

False Positives

Web applications passing the authentication sate via custom headers instead of cookies can eventually be false positives. Also when the web application is not accessed via a browser-like component (i.e not by a human user initiating the request that gets passed through all components until it reaches the web application) this can be considered a false positive.

Mitigation (Development): CSRF Prevention

Try to use anti-CSRF tokens ot the double-submit patterns (at least for logged-in requests). When your authentication scheme depends on cookies (like session or token cookies), consider marking them with the same-site flag. 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: V4 - Access Control Verification Requirements
Cheat Sheet: Cross-Site_Request_Forgery_Prevention_Cheat_Sheet

Check

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

Risk Findings

The risk **Cross-Site Request Forgery (CSRF)** 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

Cross-Site Request Forgery (CSRF) risk at **Linux Bastion Host** via **Bastion Host Access** from **Internet Gateway**: Exploitation likelihood is *Very Likely* with *Low* impact.

cross-site-request-forgery@Linux-Bastion-Host@internet-gateway>bastion-host-access

Unchecked

Cross-Site Request Forgery (CSRF) risk at **Linux Bastion Host** via **Public Subnet Include Bastion Host** from **Public Subnet**: Exploitation likelihood is *Very Likely* with *Low* impact.

cross-site-request-forgery@Linux-Bastion-Host@Public-Subnet>public-subnet-include-bastion-host

Unchecked

Cross-Site Request Forgery (CSRF) risk at **Private Subnet** via **Internal Access** from **App Server**: Exploitation likelihood is *Very Likely* with *Low* impact.

cross-site-request-forgery@Private-Subnet@app-server>internal-access

Unchecked

Cross-Site Request Forgery (CSRF) risk at **Public Route 1** via **Route Table Access** from **Internet Gateway**: Exploitation likelihood is *Very Likely* with *Low* impact.

cross-site-request-forgery@public-route-1@internet-gateway>route-table-access

Unchecked

Cross-Site Request Forgery (CSRF) risk at **Public Route 1** via **Subnet to Route table connection** from **Public Subnet**: Exploitation likelihood is *Very Likely* with *Low* impact.

cross-site-request-forgery@public-route-1@Public-Subnet>subnet-to-route-table-connection

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 **Public Subnet** as an example): Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-build-infrastructure@Public-Subnet

Unchecked

Missing Identity Propagation: 1 / 1 Risk

Description (Elevation of Privilege): CWE 284

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.

Impact

If this risk is unmitigated, attackers might be able to access or modify foreign data after a successful compromise of a component within the system due to missing resource-based authorization checks.

Detection Logic

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.

Risk Rating

The risk rating (medium or high) depends on the confidentiality, integrity, and availability rating of the technical asset.

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 (Architecture): Identity Propagation and Resource-based Authorization

When processing requests for endusers if possible authorize in the backend against the propagated identity of the enduser. This can be achieved in passing JWTs or similar tokens and checking them in the backend services. For DevOps usages apply at least a technical-user authorization.

ASVS Chapter: V4 - Access Control Verification Requirements
Cheat Sheet: Access_Control_Cheat_Sheet

Check

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

Risk Findings

The risk **Missing Identity Propagation** 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 Enduser Identity Propagation over communication link **Internal Access** from **App Server** to **Private Subnet**: Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-identity-propagation@app-server>internal-access@app-server@Private-Subnet

Unchecked

Missing Two-Factor Authentication (2FA): 1 / 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 **Internal Access** from **App Server** to **Private Subnet**: Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-authentication-second-factor@app-server>internal-access@app-server@Private-Subnet

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 **Private Subnet** as an example): Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-vault@Private-Subnet

Unchecked

Missing Web Application Firewall (WAF): 3 / 3 Risks

Description (Tampering): CWE 1008

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.

Impact

If this risk is unmitigated, attackers might be able to apply standard attack pattern tests at great speed without any filtering.

Detection Logic

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.

Risk Rating

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

False Positives

Targets only accessible via WAFs or reverse proxies containing a WAF component (like ModSecurity) can be considered as false positives after individual review.

Mitigation (Operations): Web Application Firewall (WAF)

Consider placing a Web Application Firewall (WAF) in front of the web-services and/or web-applications. For cloud environments many cloud providers offer pre-configured WAFs. Even reverse proxies can be enhances by a WAF component via ModSecurity plugins.

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

Check

Is a Web Application Firewall (WAF) in place?

Risk Findings

The risk **Missing Web Application Firewall (WAF)** was found **3 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

Missing Web Application Firewall (WAF) risk at **Linux Bastion Host**: Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-waf@Linux-Bastion-Host

Unchecked

Missing Web Application Firewall (WAF) risk at **Private Subnet**: Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-waf@Private-Subnet

Unchecked

Missing Web Application Firewall (WAF) risk at **Public Route 1**: Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-waf@public-route-1

Unchecked

Mixed Targets on Shared Runtime: 1 / 1 Risk

Description (Elevation of Privilege): CWE 1008

Different attacker targets (like frontend and backend/datastore components) should not be running on the same shared (underlying) runtime.

Impact

If this risk is unmitigated, attackers successfully attacking other components of the system might have an easy path towards more valuable targets, as they are running on the same shared runtime.

Detection Logic

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.

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.

False Positives

When all assets running on the shared runtime are hardened and protected to the same extend as if all were containing/processing highly sensitive data.

Mitigation (Operations): Runtime Separation

Use separate runtime environments for running different target components or apply similar separation styles to prevent load- or breach-related problems originating from one more attacker-facing asset impacts also the other more critical rated backend/datastore assets.

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 **Mixed Targets on Shared Runtime** 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

Mixed Targets on Shared Runtime named **Subnet and Instance Virtualization** might enable attackers moving from one less valuable target to a more valuable one: Exploitation likelihood is *Unlikely* with *Medium* impact.

mixed-targets-on-shared-runtime@Instance-virtualization

Unchecked

Unencrypted Communication: 2 / 2 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 **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.

Medium Risk Severity

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

unencrypted-communication@Private-Subnet>database-traffic@Private-Subnet@sql-database

Unchecked

Unencrypted Communication named **Database Traffic** between **RDS Subnet** and **Db Instance** transferring authentication data (like credentials, token, session-id, etc.): Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-communication@sql-database>database-traffic@sql-database@db-instance

Unchecked

Unencrypted Technical Assets: 7 / 7 Risks

Description (Information Disclosure): <u>CWE 311</u>

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: <u>V6 - Stored Cryptography Verification Requirements</u>
Cheat Sheet: <u>Cryptographic_Storage_Cheat_Sheet</u>

Check

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

Risk Findings

The risk **Unencrypted Technical Assets** 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

Unencrypted Technical Asset named **App Server**: Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-asset@app-server

Unchecked

Unencrypted Technical Asset named **Internet Gateway**: Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-asset@internet-gateway

Unchecked

Unencrypted Technical Asset named **Linux Bastion Host**: Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-asset@Linux-Bastion-Host

Unchecked

Unencrypted Technical Asset named **Private Subnet**: Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-asset@Private-Subnet

Unchecked

Unencrypted Technical Asset named **Public Route 1**: Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-asset@public-route-1

Unchecked

Unencrypted Technical Asset named **Public Subnet**: Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-asset@Public-Subnet

Unchecked

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

unencrypted-asset@sql-database

Unchecked

Unguarded Access From Internet: 1 / 1 Risk

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 **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

Unguarded Access from Internet of **Public Route 1** by **Internet Gateway** via **Route Table Access**: Exploitation likelihood is *Very Likely* with *Low* impact.

unguarded-access-from-internet@public-route-1@internet-gateway@internet-gateway>route-table-access

Unchecked

Unnecessary Data Transfer: 8 / 8 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 **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

Unnecessary Data Transfer of **Database Data Transfer** data at **Db Instance** from/to **RDS Subnet**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@database-data-transfer@db-instance@sql-database

Unchecked

Unnecessary Data Transfer of **Internet Data Transfer** data at **Db Instance** from/to **RDS Subnet**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@internet-data-transfer@db-instance@sql-database

Unchecked

Unnecessary Data Transfer of **Internet Data Transfer** data at **Private Subnet** from/to **RDS Subnet**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@internet-data-transfer@Private-Subnet@sql-database

Unchecked

Unnecessary Data Transfer of **Internet Data Transfer** data at **RDS Subnet** from/to **Db Instance**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@internet-data-transfer@sql-database@db-instance

Unchecked

Unnecessary Data Transfer of **Internet Data Transfer** data at **RDS Subnet** from/to **Private Subnet**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@internet-data-transfer@sql-database@Private-Subnet

Unchecked

Low Risk Severity

Unnecessary Data Transfer of **Data Transfer** data at **App Server** from/to **Private Subnet**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@data-transfer@app-server@Private-Subnet

Unchecked

Unnecessary Data Transfer of **Data Transfer** data at **Public Route 1** from/to **Public Subnet**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@data-transfer@public-route-1@Public-Subnet

Unchecked

Unnecessary Data Transfer of **Data Transfer** data at **Public Subnet** from/to **Public Route 1**:
Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@data-transfer@Public-Subnet@public-route-1

Unchecked

DoS-risky Access Across Trust-Boundary: 3 / 3 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 **3 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

Denial-of-Service risky access of **Private Subnet** by **App Server** via **Internal Access**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@Private-Subnet@app-server@app-server>internal-access

Unchecked

Denial-of-Service risky access of **Public Route 1** by **Internet Gateway** via **Route Table Access**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@public-route-1@internet-gateway@internet-gateway>route-table-access

Unchecked

Denial-of-Service risky access of **Public Route 1** by **Public Subnet** via **Subnet to Route table connection**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@public-route-1@Public-Subnet@Public-Subnet>subnet-to-route-table-connection

Unchecked

Identified Risks by Technical Asset

In total **53 potential risks** have been identified during the threat modeling process of which **0 are rated as critical**, **2 as high**, **16 as elevated**, **29 as medium**, and **6 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.

Private Subnet: 12 / 12 Risks

Description

Used for database and app server

Identified Risks of Asset

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

High Risk Severity

SQL/NoSQL-Injection risk at **Private Subnet** against database **RDS Subnet** via **Database Traffic**: Exploitation likelihood is *Very Likely* with *High* impact.

sql-nosql-injection@Private-Subnet@sql-database@Private-Subnet>database-traffic

Unchecked

XML External Entity (XXE) risk at **Private Subnet**: Exploitation likelihood is *Very Likely* with *High* impact.

xml-external-entity@Private-Subnet

Unchecked

Elevated Risk Severity

Cross-Site Scripting (XSS) risk at **Private Subnet**: Exploitation likelihood is *Likely* with *High* impact.

cross-site-scripting@Private-Subnet

Unchecked

Medium Risk Severity

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

unencrypted-communication@Private-Subnet>database-traffic@Private-Subnet@sql-database

Unchecked

Unencrypted Technical Asset named **Private Subnet**: Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-asset@Private-Subnet

Unchecked

Missing Enduser Identity Propagation over communication link **Internal Access** from **App Server** to **Private Subnet**: Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-identity-propagation@app-server>internal-access@app-server@Private-Subnet

Unchecked

Missing Two-Factor Authentication covering communication link **Internal Access** from **App Server** to **Private Subnet**: Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-authentication-second-factor@app-server>internal-access@app-server@Private-Subnet

Unchecked

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

missing-vault@Private-Subnet

Unchecked

Missing Web Application Firewall (WAF) risk at **Private Subnet**: Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-waf@Private-Subnet

Unchecked

Unnecessary Data Transfer of **Internet Data Transfer** data at **Private Subnet** from/to **RDS Subnet**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@internet-data-transfer@Private-Subnet@sql-database

Unchecked

Cross-Site Request Forgery (CSRF) risk at **Private Subnet** via **Internal Access** from **App Server**: Exploitation likelihood is *Very Likely* with *Low* impact.

cross-site-request-forgery@Private-Subnet@app-server>internal-access

Unchecked

Low Risk Severity

Denial-of-Service risky access of **Private Subnet** by **App Server** via **Internal Access**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@Private-Subnet@app-server@app-server>internal-access

Unchecked

Asset Information

ID:	Private-Subnet
Type:	process
Usage:	business
RAA:	39 %
Size:	application
Technology:	web-server
Tags:	linux

Internet:	false
Machine:	virtual
Encryption:	none
Multi-Tenant:	false
Redundant:	true
Custom-Developed:	false
Client by Human:	false
Data Processed:	Data Transfer, Database Data Transfer
Data Stored:	App server logs
Formats Accepted:	File, XML

Asset Rating

Owner:	shashank	
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 private instance contains sensitive data of application	

Outgoing Communication Links: 1

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

Database Traffic (outgoing)

Link to the RDS Subnet Instance

Target:	RDS Subnet
Protocol:	jdbc
Encrypted:	false
Authentication:	credentials
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Sent:	Database Data Transfer, Internet Data Transfer
Data Received:	Database Data Transfer, Internet Data Transfer

Incoming Communication Links: 1

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

Internal Access (incoming)

Link to the Private system

Source:	App Server
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	aws:ec2
VPN:	true
IP-Filtered:	false
Data Received:	Database Data Transfer
Data Sent:	Data Transfer, Database Data Transfer

App Server: 4 / 4 Risks

Description

App Server

Identified Risks of Asset

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

Elevated Risk Severity

Cross-Site Scripting (XSS) risk at **App Server**: Exploitation likelihood is *Likely* with *High* impact.

cross-site-scripting@app-server

Unchecked

Server-Side Request Forgery (SSRF) risk at **App Server** server-side web-requesting the target **Private Subnet** via **Internal Access**: Exploitation likelihood is *Likely* with *Medium* impact.

server-side-request-forgery@app-server@Private-Subnet@app-server>internal-access

Unchecked

Medium Risk Severity

Unencrypted Technical Asset named **App Server**: Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-asset@app-server

Unchecked

Low Risk Severity

Unnecessary Data Transfer of **Data Transfer** data at **App Server** from/to **Private Subnet**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@data-transfer@app-server@Private-Subnet

Unchecked

Asset Information

ID:	app-server
Type:	external-entity
Usage:	business
RAA:	16 %

Size:	application
Technology:	web-server
Tags:	none
Internet:	false
Machine:	virtual
Encryption:	none
Multi-Tenant:	false
Redundant:	false
Custom-Developed:	false
Client by Human:	true
Data Processed:	App server logs, Database Data Transfer, Server Application Code
Data Stored:	none
Formats Accepted:	none of the special data formats accepted

Asset Rating

Owner:	Shashank	
Confidentiality:	confidential	(rated 4 in scale of 5)
Integrity:	important	(rated 3 in scale of 5)
Availability:	important	(rated 3 in scale of 5)
CIA-Justification:	The client used by Shashank to administer and use the system.	

Outgoing Communication Links: 1
Target technical asset names are clickable and link to the corresponding chapter.

Internal Access (outgoing)
Link to the Private system

Target:	Private Subnet
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	aws:ec2
VPN:	true
IP-Filtered:	false

Data Sent: Database Data Transfer
Data Received: Data Transfer, Database Data Transfer

Linux Bastion Host: 6 / 6 Risks

Description

Linux bastion host for hosting the application

Identified Risks of Asset

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

Elevated Risk Severity

Cross-Site Scripting (XSS) risk at **Linux Bastion Host**: Exploitation likelihood is *Likely* with *High* impact.

cross-site-scripting@Linux-Bastion-Host

> **Unchecked**

Missing Authentication covering communication link **Bastion Host Access** from **Internet Gateway** to **Linux Bastion Host**: Exploitation likelihood is *Likely* with *High* impact.

missing-authentication@internet-gateway>bastion-host-access@internet-gateway@Linux-Bastion-Host

> **Unchecked**

Medium Risk Severity

Unencrypted Technical Asset named **Linux Bastion Host**: Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-asset@Linux-Bastion-Host

> **Unchecked**

Missing Web Application Firewall (WAF) risk at **Linux Bastion Host**: Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-waf@Linux-Bastion-Host

> **Unchecked**

Cross-Site Request Forgery (CSRF) risk at **Linux Bastion Host** via **Bastion Host Access** from **Internet Gateway**: Exploitation likelihood is *Very Likely* with *Low* impact.

cross-site-request-forgery@Linux-Bastion-Host@internet-gateway>bastion-host-access

> **Unchecked**

Cross-Site Request Forgery (CSRF) risk at **Linux Bastion Host** via **Public Subnet Include Bastion Host** from **Public Subnet**: Exploitation likelihood is *Very Likely* with *Low* impact.

cross-site-request-forgery@Linux-Bastion-Host@Public-Subnet>public-subnet-include-bastion-host

> **Unchecked**

Asset Information

ID:	Linux-Bastion-Host
Type:	process
Usage:	business
RAA:	1 %
Size:	application
Technology:	web-server
Tags:	linux
Internet:	false
Machine:	virtual
Encryption:	none
Multi-Tenant:	false
Redundant:	false
Custom-Developed:	true
Client by Human:	false
Data Processed:	Client Application Code, Internet Data Transfer
Data Stored:	Client Application Code
Formats Accepted:	none of the special data formats accepted

Asset Rating

Owner:	shashank	
Confidentiality:	internal	(rated 2 in scale of 5)
Integrity:	important	(rated 3 in scale of 5)
Availability:	important	(rated 3 in scale of 5)
CIA-Justification:	The correct configuration and reachability of the web server is mandatory for all customer usages of the portal.	

Incoming Communication Links: 2
Source technical asset names are clickable and link to the corresponding chapter.

Bastion Host Access (incoming)

Link to the Bastion host

Source:	Internet Gateway
Protocol:	https
Encrypted:	true

Authentication:	none
Authorization:	none
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Received:	Internet Data Transfer
Data Sent:	none

Public Subnet Include Bastion Host (incoming)
Link to the bastion host

Source:	Public Subnet
Protocol:	https
Encrypted:	true
Authentication:	session-id
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Received:	Client Application Code, Internet Data Transfer
Data Sent:	Client Application Code, Internet Data Transfer

Public Route 1: 9 / 9 Risks

Description

Public Route 1

Identified Risks of Asset

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

Elevated Risk Severity

Cross-Site Scripting (XSS) risk at **Public Route 1**: Exploitation likelihood is *Likely* with *High* impact.

cross-site-scripting@public-route-1

Unchecked

Medium Risk Severity

Unencrypted Technical Asset named **Public Route 1**: Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-asset@public-route-1

Unchecked

Missing Web Application Firewall (WAF) risk at **Public Route 1**: Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-waf@public-route-1

Unchecked

Cross-Site Request Forgery (CSRF) risk at **Public Route 1** via **Route Table Access** from **Internet Gateway**: Exploitation likelihood is *Very Likely* with *Low* impact.

cross-site-request-forgery@public-route-1@internet-gateway>route-table-access

Unchecked

Cross-Site Request Forgery (CSRF) risk at **Public Route 1** via **Subnet to Route table connection** from **Public Subnet**: Exploitation likelihood is *Very Likely* with *Low* impact.

cross-site-request-forgery@public-route-1@Public-Subnet>subnet-to-route-table-connection

Unchecked

Unguarded Access from Internet of **Public Route 1** by **Internet Gateway** via **Route Table Access**: Exploitation likelihood is *Very Likely* with *Low* impact.

unguarded-access-from-internet@public-route-1@internet-gateway@internet-gateway>route-table-access

Unchecked

Low Risk Severity

Denial-of-Service risky access of **Public Route 1** by **Internet Gateway** via **Route Table Access**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@public-route-1@internet-gateway@internet-gateway>route-table-access

> **Unchecked**

Denial-of-Service risky access of **Public Route 1** by **Public Subnet** via **Subnet to Route table connection**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@public-route-1@Public-Subnet@Public-Subnet>subnet-to-route-table-connection

> **Unchecked**

Unnecessary Data Transfer of **Data Transfer** data at **Public Route 1** from/to **Public Subnet**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@data-transfer@public-route-1@Public-Subnet

> **Unchecked**

Asset Information

ID:	public-route-1
Type:	process
Usage:	business
RAA:	32 %
Size:	component
Technology:	identity-provider
Tags:	none
Internet:	true
Machine:	virtual
Encryption:	none
Multi-Tenant:	false
Redundant:	false
Custom-Developed:	false
Client by Human:	false
Data Processed:	Internet Data Transfer
Data Stored:	none
Formats Accepted:	none of the special data formats accepted

Asset Rating

Owner:	shashank	
Confidentiality:	confidential	(rated 4 in scale of 5)

Integrity: critical   (rated 4 in scale of 5)
Availability: critical   (rated 4 in scale of 5)
CIA-Justification: The auth data of the application

Incoming Communication Links: 2
Source technical asset names are clickable and link to the corresponding chapter.

Route Table Access (incoming)
Link to the public route 1

Source:	Internet Gateway
Protocol:	https
Encrypted:	true
Authentication:	credentials
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Received:	Internet Data Transfer
Data Sent:	Internet Data Transfer

Subnet to Route table connection (incoming)
Link to the Public Route 1

Source:	Public Subnet
Protocol:	https
Encrypted:	true
Authentication:	credentials
Authorization:	none
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Received:	Data Transfer
Data Sent:	Data Transfer

Public Subnet: 8 / 8 Risks

Description

Public Subnet hosting the client-side code

Identified Risks of Asset

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

Elevated Risk Severity

Missing Cloud Hardening (EC2) risk at **Public Subnet**: <u>CIS Benchmark for Amazon Linux</u>:
Exploitation likelihood is *Unlikely* with *Very High* impact.

missing-cloud-hardening@Public-Subnet

> **Unchecked**

Cross-Site Scripting (XSS) risk at **Public Subnet**: Exploitation likelihood is *Likely* with *High*
impact.

cross-site-scripting@Public-Subnet

> **Unchecked**

Missing File Validation risk at **Public Subnet**: Exploitation likelihood is *Very Likely* with
Medium impact.

missing-file-validation@Public-Subnet

> **Unchecked**

Server-Side Request Forgery (SSRF) risk at **Public Subnet** server-side web-requesting the
target **Linux Bastion Host** via **Public Subnet Include Bastion Host**: Exploitation likelihood is
Likely with *Medium* impact.

server-side-request-forgery@Public-Subnet@Linux-Bastion-Host@Public-Subnet>public-subnet-include-bastion-host

> **Unchecked**

Server-Side Request Forgery (SSRF) risk at **Public Subnet** server-side web-requesting the
target **Public Route 1** via **Subnet to Route table connection**: Exploitation likelihood is *Likely*
with *Medium* impact.

server-side-request-forgery@Public-Subnet@public-route-1@Public-Subnet>subnet-to-route-table-connection

> **Unchecked**

Medium Risk Severity

Unencrypted Technical Asset named **Public Subnet**: Exploitation likelihood is *Unlikely* with
High impact.

unencrypted-asset@Public-Subnet

> **Unchecked**

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

missing-build-infrastructure@Public-Subnet

Unchecked

Low Risk Severity

Unnecessary Data Transfer of **Data Transfer** data at **Public Subnet** from/to **Public Route 1**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@data-transfer@Public-Subnet@public-route-1

Unchecked

Asset Information

ID:	Public-Subnet
Type:	process
Usage:	business
RAA:	28 %
Size:	application
Technology:	web-server
Tags:	aws:ec2, linux
Internet:	false
Machine:	virtual
Encryption:	none
Multi-Tenant:	false
Redundant:	false
Custom-Developed:	true
Client by Human:	false
Data Processed:	Client Application Code, Internet Data Transfer
Data Stored:	Client Application Code
Formats Accepted:	File, JSON

Asset Rating

Owner:	shashank	
Confidentiality:	internal	(rated 2 in scale of 5)
Integrity:	critical	(rated 4 in scale of 5)
Availability:	critical	(rated 4 in scale of 5)
CIA-Justification:	The correct configuration and reachability of the Public subnet is mandatory for all resources.	

Outgoing Communication Links: 2
Target technical asset names are clickable and link to the corresponding chapter.

Subnet to Route table connection (outgoing)
Link to the Public Route 1

Target:	Public Route 1
Protocol:	https
Encrypted:	true
Authentication:	credentials
Authorization:	none
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Sent:	Data Transfer
Data Received:	Data Transfer

Public Subnet Include Bastion Host (outgoing)
Link to the bastion host

Target:	Linux Bastion Host
Protocol:	https
Encrypted:	true
Authentication:	session-id
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Sent:	Client Application Code, Internet Data Transfer
Data Received:	Client Application Code, Internet Data Transfer

RDS Subnet: 6 / 6 Risks

Description

The database behind the private subnet

Identified Risks of Asset

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

Elevated Risk Severity

SQL/NoSQL-Injection risk at **RDS Subnet** against database **Db Instance** via **Database Traffic**: Exploitation likelihood is *Very Likely* with *Medium* impact.

sql-nosql-injection@sql-database@db-instance@sql-database>database-traffic

   Unchecked

Missing Hardening risk at **RDS Subnet**: Exploitation likelihood is *Likely* with *Medium* impact.

missing-hardening@sql-database

   Unchecked

Medium Risk Severity

Unencrypted Communication named **Database Traffic** between **RDS Subnet** and **Db Instance** transferring authentication data (like credentials, token, session-id, etc.): Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-communication@sql-database>database-traffic@sql-database@db-instance

   Unchecked

Unencrypted Technical Asset named **RDS Subnet** 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 **Internet Data Transfer** data at **RDS Subnet** from/to **Db Instance**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@internet-data-transfer@sql-database@db-instance

   Unchecked

Unnecessary Data Transfer of **Internet Data Transfer** data at **RDS Subnet** from/to **Private Subnet**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@internet-data-transfer@sql-database@Private-Subnet

   Unchecked

Asset Information

ID:	sql-database
Type:	datastore
Usage:	business
RAA:	100 %
Size:	component
Technology:	database
Tags:	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:	Database Customizing and Dumps, Database Data Transfer
Data Stored:	Database Data Transfer
Formats Accepted:	none of the special data formats accepted

Asset Rating

Owner:	shashank	
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 rds database subnet can host databases	

Outgoing Communication Links: 1

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

Database Traffic (outgoing)

Link to the RDS Subnet Instance

Target:	Db Instance
Protocol:	jdbc
Encrypted:	false
Authentication:	credentials

Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Sent:	Database Data Transfer, Internet Data Transfer
Data Received:	Database Data Transfer, Internet Data Transfer

Incoming Communication Links: 1

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

Database Traffic (incoming)

Link to the RDS Subnet Instance

Source:	Private Subnet
Protocol:	jdbc
Encrypted:	false
Authentication:	credentials
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Received:	Database Data Transfer, Internet Data Transfer
Data Sent:	Database Data Transfer, Internet Data Transfer

Db Instance: 3 / 3 Risks

Description

db instance for storing the application data in mysql database

Identified Risks of Asset

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

Medium Risk Severity

Missing Cloud Hardening (EC2) risk at **Db Instance**: <u>CIS Benchmark for Amazon Linux</u>: Exploitation likelihood is *Unlikely* with *High* impact.

missing-cloud-hardening@db-instance

Unchecked

Unnecessary Data Transfer of **Database Data Transfer** data at **Db Instance** from/to **RDS Subnet**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@database-data-transfer@db-instance@sql-database

Unchecked

Unnecessary Data Transfer of **Internet Data Transfer** data at **Db Instance** from/to **RDS Subnet**: Exploitation likelihood is *Unlikely* with *Medium* impact.

unnecessary-data-transfer@internet-data-transfer@db-instance@sql-database

Unchecked

Asset Information

ID:	db-instance
Type:	datastore
Usage:	business
RAA:	10 %
Size:	service
Technology:	database
Tags:	aws:rds, linux
Internet:	false
Machine:	virtual
Encryption:	data-with-symmetric-shared-key
Multi-Tenant:	false
Redundant:	false
Custom-Developed:	false
Client by Human:	false

Data Processed: none
Data Stored: Data Transfer
Formats Accepted: File

Asset Rating

Owner: shashank
Confidentiality: confidential   (rated 4 in scale of 5)
Integrity: critical   (rated 4 in scale of 5)
Availability: important   (rated 3 in scale of 5)
CIA-Justification: Db Instance might contain database of the application. Database will be the
                     according to the application requirement.

Incoming Communication Links: 1
Source technical asset names are clickable and link to the corresponding chapter.

Database Traffic (incoming)
Link to the RDS Subnet Instance

        Source: RDS Subnet
        Protocol: jdbc
        Encrypted: false
        Authentication: credentials
        Authorization: technical-user
        Read-Only: false
        Usage: business
        Tags: none
        VPN: false
        IP-Filtered: false
        Data Received: Database Data Transfer, Internet Data Transfer
        Data Sent: Database Data Transfer, Internet Data Transfer

Internet Gateway: 1 / 1 Risk

Description

Internet Gateway

Identified Risks of Asset

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

Medium Risk Severity

Unencrypted Technical Asset named **Internet Gateway**: Exploitation likelihood is *Unlikely* with *High* impact.

unencrypted-asset@internet-gateway

Unchecked

Asset Information

ID:	internet-gateway
Type:	external-entity
Usage:	business
RAA:	15 %
Size:	service
Technology:	browser
Tags:	none
Internet:	true
Machine:	virtual
Encryption:	none
Multi-Tenant:	false
Redundant:	false
Custom-Developed:	false
Client by Human:	false
Data Processed:	Internet Data Transfer
Data Stored:	none
Formats Accepted:	none of the special data formats accepted

Asset Rating

Owner:	Shashank	
Confidentiality:	public	(rated 1 in scale of 5)

Integrity: operational   (rated 2 in scale of 5)
Availability: operational   (rated 2 in scale of 5)
CIA-Justification: The client used by Shashank to administer the system.

Outgoing Communication Links: 2

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

Route Table Access (outgoing)
Link to the public route 1

Target:	Public Route 1
Protocol:	https
Encrypted:	true
Authentication:	credentials
Authorization:	technical-user
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Sent:	Internet Data Transfer
Data Received:	Internet Data Transfer

Bastion Host Access (outgoing)
Link to the Bastion host

Target:	Linux Bastion Host
Protocol:	https
Encrypted:	true
Authentication:	none
Authorization:	none
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Sent:	Internet Data Transfer
Data Received:	none

Identified Data Breach Probabilities by Data Asset

In total **53 potential risks** have been identified during the threat modeling process of which **0 are rated as critical**, **2 as high**, **16 as elevated**, **29 as medium**, and **6 as low**.

These risks are distributed across **7 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.

App server logs: 15 / 15 Risks

Logs generated by the ERP system.

ID:	app-server-logs
Usage:	devops
Quantity:	many
Tags:	none
Origin:	Shashank
Owner:	Shashank
Confidentiality:	restricted (rated 3 in scale of 5)
Integrity:	archive (rated 1 in scale of 5)
Availability:	archive (rated 1 in scale of 5)
CIA-Justification:	Logs should not contain PII data and are only required for failure analysis, i.e. they are not considered as hard transactional logs.
Processed by:	App Server
Stored by:	Private Subnet
Sent via:	none
Received via:	none
Data Breach:	**probable**
Data Breach Risks:	This data asset has data breach potential because of 15 remaining risks:

Probable: missing-cloud-hardening@application-network

Probable: missing-cloud-hardening@Private-Instance

Probable: xml-external-entity@Private-Subnet

Possible: cross-site-scripting@app-server

Possible: cross-site-scripting@Private-Subnet

Possible: missing-authentication-second-factor@app-server>internal-access@app-server@Private-Subnet

Possible: server-side-request-forgery@app-server@Private-Subnet@app-server>internal-access

Improbable: cross-site-request-forgery@Private-Subnet@app-server>internal-access

Improbable: missing-identity-propagation@app-server>internal-access@app-server@Private-Subnet

Improbable: missing-waf@Private-Subnet

Improbable: mixed-targets-on-shared-runtime@Instance-virtualization

Improbable: unencrypted-asset@app-server

Improbable: unencrypted-asset@Private-Subnet

Improbable: unnecessary-data-transfer@data-transfer@app-server@Private-Subnet

Improbable: unnecessary-data-transfer@internet-data-transfer@Private-Subnet@sql-database

Client Application Code: 16 / 16 Risks

client-side code delivered by the application.

ID:	client-application-code
Usage:	devops
Quantity:	very-few
Tags:	none
Origin:	shashank
Owner:	shashank
Confidentiality:	public (rated 1 in scale of 5)
Integrity:	critical (rated 4 in scale of 5)
Availability:	important (rated 3 in scale of 5)
CIA-Justification:	The integrity of the public data is critical to avoid reputational damage and the availability is important on the long-term scale (but not critical) to keep the growth rate of the customer base steady.
Processed by:	Linux Bastion Host, Public Subnet
Stored by:	Linux Bastion Host, Public Subnet
Sent via:	Public Subnet Include Bastion Host
Received via:	Public Subnet Include Bastion Host
Data Breach:	**probable**
Data Breach Risks:	This data asset has data breach potential because of 16 remaining risks:

Probable: missing-cloud-hardening@application-network

Probable: missing-cloud-hardening@Public-Instance

Probable: missing-cloud-hardening@Public-Subnet

Probable: missing-file-validation@Public-Subnet

Possible: cross-site-scripting@Linux-Bastion-Host

Possible: cross-site-scripting@Public-Subnet

Possible: missing-authentication@internet-gateway>bastion-host-access@internet-gateway@Linux-Bastion-Host

Possible: server-side-request-forgery@Public-Subnet@Linux-Bastion-Host@Public-Subnet>public-subnet-include-bastion-host

Possible: server-side-request-forgery@Public-Subnet@public-route-1@Public-Subnet>subnet-to-route-table-connection

Improbable: cross-site-request-forgery@Linux-Bastion-Host@internet-gateway>bastion-host-access

Improbable: cross-site-request-forgery@Linux-Bastion-Host@Public-Subnet>public-subnet-include-bastion-host

Improbable: missing-waf@Linux-Bastion-Host

Improbable: mixed-targets-on-shared-runtime@Instance-virtualization

Improbable: unencrypted-asset@Linux-Bastion-Host

Improbable: unencrypted-asset@Public-Subnet

Improbable: unnecessary-data-transfer@data-transfer@Public-Subnet@public-route-1

Data Transfer: 16 / 16 Risks

Data Transfer

ID:	data-transfer
Usage:	business
Quantity:	many
Tags:	none
Origin:	Customer
Owner:	Shashank
Confidentiality:	confidential (rated 4 in scale of 5)
Integrity:	critical (rated 4 in scale of 5)
Availability:	operational (rated 2 in scale of 5)
CIA-Justification:	data transfer might contain financial data as well as personally identifiable information (PII).
Processed by:	Private Subnet
Stored by:	Db Instance
Sent via:	Subnet to Route table connection
Received via:	Subnet to Route table connection, Internal Access
Data Breach:	**probable**
Data Breach Risks:	This data asset has data breach potential because of 16 remaining risks:

Probable: missing-cloud-hardening@application-network

Probable: missing-cloud-hardening@Private-Instance

Probable: missing-cloud-hardening@db-instance

Probable: sql-nosql-injection@sql-database@db-instance@sql-database>database-traffic

Probable: xml-external-entity@Private-Subnet

Possible: cross-site-scripting@Private-Subnet

Possible: missing-authentication-second-factor@app-server>internal-access@app-server@Private-Subnet

Possible: unencrypted-communication@sql-database>database-traffic@sql-database@db-instance

Improbable: cross-site-request-forgery@Private-Subnet@app-server>internal-access

Improbable: missing-identity-propagation@app-server>internal-access@app-server@Private-Subnet

Improbable: missing-waf@Private-Subnet

Improbable: mixed-targets-on-shared-runtime@Instance-virtualization

Improbable: unencrypted-asset@Private-Subnet

Improbable: unnecessary-data-transfer@database-data-transfer@db-instance@sql-database

Improbable: unnecessary-data-transfer@internet-data-transfer@db-instance@sql-database

Improbable: unnecessary-data-transfer@internet-data-transfer@Private-Subnet@sql-database

Database Customizing and Dumps: 9 / 9 Risks

Data for customizing of the DB system, which might include full database dumps.

ID:	db-dumps
Usage:	business
Quantity:	very-few
Tags:	mysql
Origin:	Shashank
Owner:	Shashank
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:	RDS Subnet
Stored by:	none
Sent via:	none
Received via:	none
Data Breach:	**probable**
Data Breach Risks:	This data asset has data breach potential because of 9 remaining risks:

Probable: missing-cloud-hardening@application-network

Probable: missing-cloud-hardening@Private-Instance

Probable: sql-nosql-injection@Private-Subnet@sql-database@Private-Subnet>database-traffic

Possible: unencrypted-communication@Private-Subnet>database-traffic@Private-Subnet@sql-database

Improbable: missing-hardening@sql-database

Improbable: mixed-targets-on-shared-runtime@Instance-virtualization

Improbable: unencrypted-asset@sql-database

Improbable: unnecessary-data-transfer@internet-data-transfer@sql-database@db-instance

Improbable: unnecessary-data-transfer@internet-data-transfer@sql-database@Private-Subnet

Database Data Transfer: 21 / 21 Risks

Database data transfer of the system used to the transfer data between resources.

ID:	database-data-transfer
Usage:	business
Quantity:	few
Tags:	none
Origin:	Shashank
Owner:	Shashank
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 used and/or generated when application running like db-instance - mysql
Processed by:	App Server, Private Subnet, RDS Subnet
Stored by:	RDS Subnet
Sent via:	Internal Access, Database Traffic, Database Traffic
Received via:	Internal Access, Database Traffic, Database Traffic
Data Breach:	**probable**
Data Breach Risks:	This data asset has data breach potential because of 21 remaining risks:

Probable: missing-cloud-hardening@application-network

Probable: missing-cloud-hardening@Private-Instance

Probable: sql-nosql-injection@Private-Subnet@sql-database@Private-Subnet>database-traffic

Probable: xml-external-entity@Private-Subnet

Possible: cross-site-scripting@app-server

Possible: cross-site-scripting@Private-Subnet

Possible: missing-authentication-second-factor@app-server>internal-access@app-server@Private-Subnet

Possible: server-side-request-forgery@app-server@Private-Subnet@app-server>internal-access

Possible: unencrypted-communication@Private-Subnet>database-traffic@Private-Subnet@sql-database

Improbable: cross-site-request-forgery@Private-Subnet@app-server>internal-access

Improbable: missing-identity-propagation@app-server>internal-access@app-server@Private-Subnet

Improbable: missing-hardening@sql-database

Improbable: missing-waf@Private-Subnet

Improbable: mixed-targets-on-shared-runtime@Instance-virtualization

Improbable: unencrypted-asset@app-server

Improbable: unencrypted-asset@Private-Subnet

Improbable: unencrypted-asset@sql-database

Improbable: unnecessary-data-transfer@data-transfer@app-server@Private-Subnet

Improbable: unnecessary-data-transfer@internet-data-transfer@Private-Subnet@sql-database

Improbable: unnecessary-data-transfer@internet-data-transfer@sql-database@db-instance

Improbable: unnecessary-data-transfer@internet-data-transfer@sql-database@Private-Subnet

Internet Data Transfer: 24 / 24 Risks

Internet Data Transfer

ID:	internet-data-transfer
Usage:	business
Quantity:	many
Tags:	none
Origin:	Customer
Owner:	Shashank
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:	Internet data transfer used to be available to offer the internet functionality.
Processed by:	Internet Gateway, Linux Bastion Host, Public Route 1, Public Subnet
Stored by:	none
Sent via:	Route Table Access, Public Subnet Include Bastion Host, Database Traffic, Database Traffic, Bastion Host Access
Received via:	Route Table Access, Public Subnet Include Bastion Host, Database Traffic, Database Traffic
Data Breach:	**probable**
Data Breach Risks:	This data asset has data breach potential because of 24 remaining risks:

Probable: missing-cloud-hardening@application-network

Probable: missing-cloud-hardening@Public-Instance

Probable: missing-cloud-hardening@Public-Subnet

Probable: missing-file-validation@Public-Subnet

Possible: cross-site-scripting@Linux-Bastion-Host

Possible: cross-site-scripting@public-route-1

Possible: cross-site-scripting@Public-Subnet

Possible: missing-authentication@internet-gateway>bastion-host-access@internet-gateway@Linux-Bastion-Host

Possible: server-side-request-forgery@Public-Subnet@Linux-Bastion-Host@Public-Subnet>public-subnet-include-bastion-host

Possible: server-side-request-forgery@Public-Subnet@public-route-1@Public-Subnet>subnet-to-route-table-connection

Possible: unguarded-access-from-internet@public-route-1@internet-gateway@internet-gateway>route-table-access

Improbable: cross-site-request-forgery@Linux-Bastion-Host@internet-gateway>bastion-host-access

Improbable: cross-site-request-forgery@Linux-Bastion-Host@Public-Subnet>public-subnet-include-bastion-host

Improbable: cross-site-request-forgery@public-route-1@internet-gateway>route-table-access

Improbable: cross-site-request-forgery@public-route-1@Public-Subnet>subnet-to-route-table-connection

Improbable: missing-waf@Linux-Bastion-Host

Improbable: missing-waf@public-route-1

Improbable: mixed-targets-on-shared-runtime@Instance-virtualization

Improbable: unencrypted-asset@internet-gateway

Improbable: unencrypted-asset@Linux-Bastion-Host

Improbable: unencrypted-asset@public-route-1

Improbable: unencrypted-asset@Public-Subnet

Improbable: unnecessary-data-transfer@data-transfer@public-route-1@Public-Subnet

Improbable: unnecessary-data-transfer@data-transfer@Public-Subnet@public-route-1

Server Application Code: 5 / 5 Risks

API and other server-side code of the application.

ID:	server-application-code
Usage:	devops
Quantity:	very-few
Tags:	none
Origin:	shashank
Owner:	shashank
Confidentiality:	internal (rated 2 in scale of 5)
Integrity:	mission-critical (rated 5 in scale of 5)
Availability:	important (rated 3 in scale of 5)
CIA-Justification:	The integrity of the API code is critical to avoid reputational damage and the availability is important.
Processed by:	App Server
Stored by:	none
Sent via:	none
Received via:	none
Data Breach:	**possible**
Data Breach Risks:	This data asset has data breach potential because of 5 remaining risks:

Possible: cross-site-scripting@app-server

Possible: server-side-request-forgery@app-server@Private-Subnet@app-server>internal-access

Improbable: mixed-targets-on-shared-runtime@Instance-virtualization

Improbable: unencrypted-asset@app-server

Improbable: unnecessary-data-transfer@data-transfer@app-server@Private-Subnet

Trust Boundaries

In total **5 trust boundaries** have been modeled during the threat modeling process.

Application Network
Virtual-Private-Cloud

ID:	application-network
Type:	network-cloud-provider
Tags:	aws:vpc
Assets inside:	none
Boundaries nested:	Private Instance, Public Instance, Public Route Table

Dev Network
Development Network

ID:	dev-network
Type:	network-on-prem
Tags:	none
Assets inside:	App Server, Internet Gateway
Boundaries nested:	none

Private Instance
Private Instance

ID:	Private-Instance
Type:	network-cloud-security-group
Tags:	aws:ec2
Assets inside:	Private Subnet, Db Instance, RDS Subnet
Boundaries nested:	none

Public Instance
Public Instance

ID:	Public-Instance
Type:	network-cloud-security-group

Tags:	aws:ec2
Assets inside:	Linux Bastion Host, Public Subnet
Boundaries nested:	none

Public Route Table
Public Route Table

ID:	public-route-table
Type:	execution-environment
Tags:	none
Assets inside:	Public Route 1
Boundaries nested:	none

Shared Runtimes

In total **1 shared runtime** has been modeled during the threat modeling process.

Subnet and Instance Virtualization
Instance Virtualization

ID:	Instance-virtualization
Tags:	vmware
Assets running:	Public Subnet, Linux Bastion Host, Private Subnet, Db Instance, RDS Subnet, App Server

Risk Rules Checked by Threagile

Threagile Version: 1.0.0
Threagile Build Timestamp: 20231104141112
Threagile Execution Timestamp: 20240105051829
Model Filename: /github/workspace/threagile.yaml
Model Hash (SHA256): 57bff947cc05d327adacd701d1bb99e3b6b4a29f47d0e018c07b6dfd9a41a92f

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

Shashank Sanap 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. Shashank Sanap 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 Shashank Sanap 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.