Threagile
Agile Threat Modeling

Threat Model Report
Innovera Payment System

14 May 2022

Khalegh Salehi Aghdam

https://innovera.ir

Table of Contents

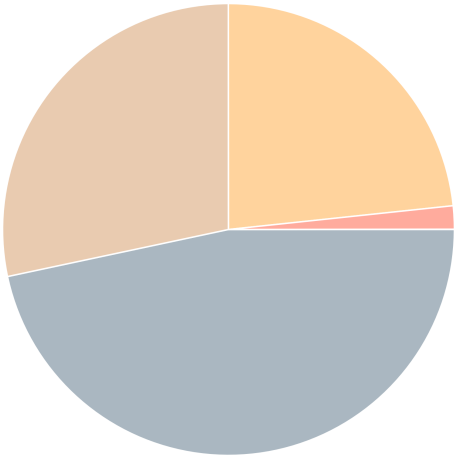
Management Summary

Threagile toolkit was used to model the architecture of "Innovera Payment System" 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 "Innovera Payment System" whether the mitigation advices have been applied or not.

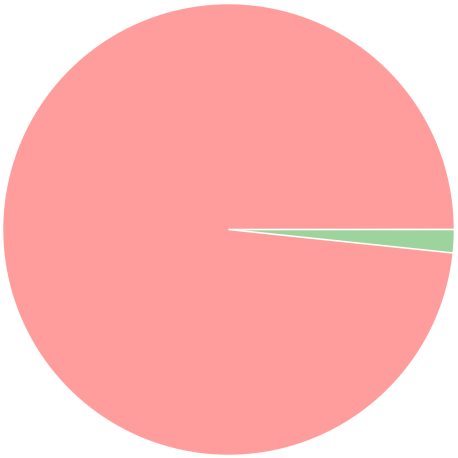
Each risk finding references a chapter of the OWASP ASVS (Application Security Verification Standard) audit checklist. The OWASP ASVS checklist should be considered as an inspiration by architects and developers to further harden the application in a Defense-in-Depth approach. Additionally, for each 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 **60 initial risks** in **21 categories** have been identified during the threat modeling process:

1 critical risk
0 high risk
14 elevated risk
17 medium risk
28 low risk



59 unchecked
0 in discussion
0 accepted
0 in progress
1 *mitigated*
0 *false positive*



Innovera Payment System Threat Modeling

Impact Analysis of 60 Initial Risks in 21 Categories

The most prevalent impacts of the **60 initial risks** (distributed over **21 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.

Critical: **Service Disaster**: 1 Initial Risk - Exploitation likelihood is *Likely* with *High* impact.
QoS

Elevated: **Cross-Site Scripting (XSS)**: 1 Initial Risk - Exploitation likelihood is *Likely* with *Medium* impact.
If this risk remains unmitigated, attackers might be able to access individual victim sessions and steal or modify user data.

Elevated: **SQL/NoSQL-Injection**: 1 Initial Risk - Exploitation likelihood is *Very Likely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to modify SQL/NoSQL queries to steal and modify data and eventually further escalate towards a deeper system penetration via code executions.

Elevated: **Unguarded Access From Internet**: 3 Initial Risks - Exploitation likelihood is *Very Likely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to directly attack sensitive systems without any hardening components in-between due to them being directly exposed on the internet.

Elevated: **Untrusted Deserialization**: 6 Initial Risks - Exploitation likelihood is *Likely* with *High* impact.
If this risk is unmitigated, attackers might be able to execute code on target systems by exploiting untrusted deserialization endpoints.

Elevated: **XML External Entity (XXE)**: 4 Initial Risks - Exploitation likelihood is *Very Likely* with *Medium* 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.

Medium: **Cross-Site Request Forgery (CSRF)**: 1 Initial Risk - 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 Cloud Hardening**: 2 Initial Risks - Exploitation likelihood is *Unlikely* with *High* impact.
If this risk is unmitigated, attackers might access cloud components in an unintended way.

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

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

Medium: **Missing Two-Factor Authentication (2FA)**: 2 Initial Risks - 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: **Server-Side Request Forgery (SSRF)**: 4 Initial Risks - Exploitation likelihood is *Likely* with *Low* 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.

Low: **DoS-risky Access Across Trust-Boundary**: 5 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.

Low: **Missing Identity Propagation**: 3 Initial Risks - Exploitation likelihood is *Unlikely* with *Low* 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.

Low: **Missing Network Segmentation**: 2 Initial Risks - Exploitation likelihood is *Unlikely* with *Low* 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 not separated by network segmentation.

Low: **Unnecessary Communication Link**: 3 Initial Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
If this risk is unmitigated, attackers might be able to target unnecessary communication links.

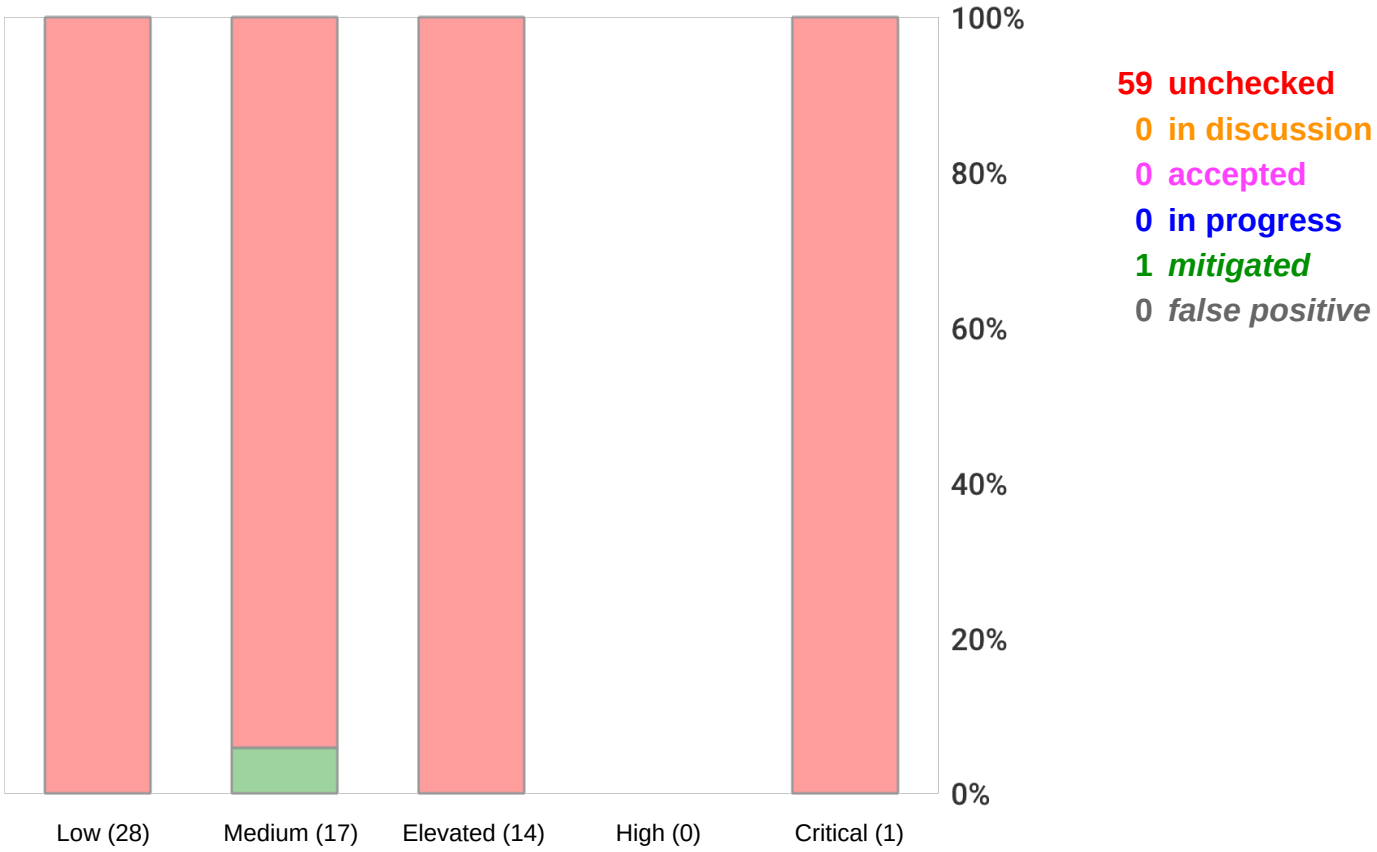
Low: **Unnecessary Data Transfer**: 8 Initial Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
If this risk is unmitigated, attackers might be able to target unnecessarily transferred data.

Low: **Unnecessary Technical Asset**: 4 Initial Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
If this risk is unmitigated, attackers might be able to target unnecessary technical assets.

Low: **Wrong Communication Link Content**: 3 Initial Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
If this potential model error is not fixed, some risks might not be visible.

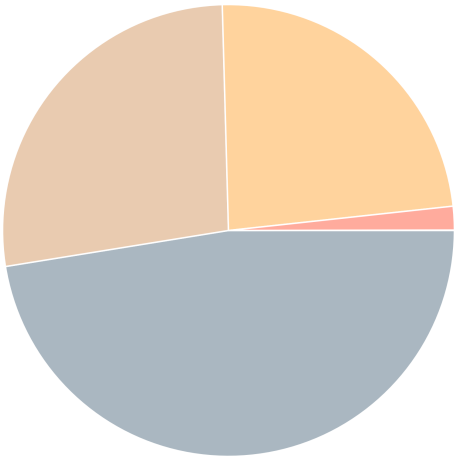
Risk Mitigation

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

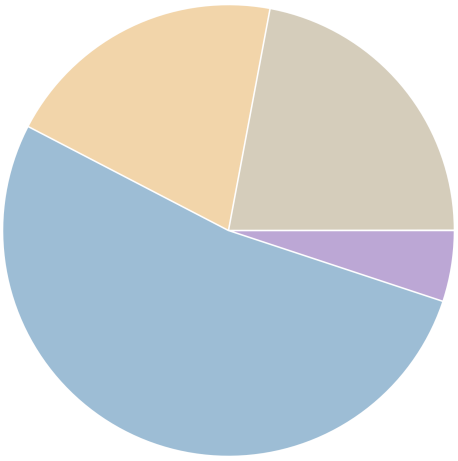


After removal of risks with status *mitigated* and *false positive* the following **59 remain unmitigated**:

1 unmitigated critical risk
0 unmitigated high risk
14 unmitigated elevated risk
16 unmitigated medium risk
28 unmitigated low risk



3 business side related
31 architecture related
12 development related
13 operations related



Impact Analysis of 59 Remaining Risks in 20 Categories

The most prevalent impacts of the **59 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.

Critical: **Service Disaster**: 1 Remaining Risk - Exploitation likelihood is *Likely* with *High* impact.
QoS

Elevated: **Cross-Site Scripting (XSS)**: 1 Remaining Risk - Exploitation likelihood is *Likely* with *Medium* impact.
If this risk remains unmitigated, attackers might be able to access individual victim sessions and steal or modify user data.

Elevated: **SQL/NoSQL-Injection**: 1 Remaining Risk - Exploitation likelihood is *Very Likely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to modify SQL/NoSQL queries to steal and modify data and eventually further escalate towards a deeper system penetration via code executions.

Elevated: **Unguarded Access From Internet**: 3 Remaining Risks - Exploitation likelihood is *Very Likely* with *Medium* impact.
If this risk is unmitigated, attackers might be able to directly attack sensitive systems without any hardening components in-between due to them being directly exposed on the internet.

Elevated: **Untrusted Deserialization**: 6 Remaining Risks - Exploitation likelihood is *Likely* with *High* impact.
If this risk is unmitigated, attackers might be able to execute code on target systems by exploiting untrusted deserialization endpoints.

Elevated: **XML External Entity (XXE)**: 4 Remaining Risks - Exploitation likelihood is *Very Likely* with *Medium* 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.

Medium: **Cross-Site Request Forgery (CSRF)**: 1 Remaining Risk - 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 Cloud Hardening**: 2 Remaining Risks - Exploitation likelihood is *Unlikely* with *High* impact.
If this risk is unmitigated, attackers might access cloud components in an unintended way.

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

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

Medium: **Missing Two-Factor Authentication (2FA)**: 2 Remaining Risks - 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: **Server-Side Request Forgery (SSRF)**: 4 Remaining Risks - Exploitation likelihood is *Likely* with *Low* 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.

Low: **DoS-risky Access Across Trust-Boundary**: 5 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.

Low: **Missing Identity Propagation**: 3 Remaining Risks - Exploitation likelihood is *Unlikely* with *Low* 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.

Low: **Missing Network Segmentation**: 2 Remaining Risks - Exploitation likelihood is *Unlikely* with *Low* 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 not separated by network segmentation.

Low: **Unnecessary Communication Link**: 3 Remaining Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
If this risk is unmitigated, attackers might be able to target unnecessary communication links.

Low: **Unnecessary Data Transfer**: 8 Remaining Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
If this risk is unmitigated, attackers might be able to target unnecessarily transferred data.

Low: **Unnecessary Technical Asset**: 4 Remaining Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
If this risk is unmitigated, attackers might be able to target unnecessary technical assets.

Low: **Wrong Communication Link Content**: 3 Remaining Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
If this potential model error is not fixed, some risks might not be visible.

Application Overview

Business Criticality

The overall business criticality of "Innovera Payment System" was rated as:

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

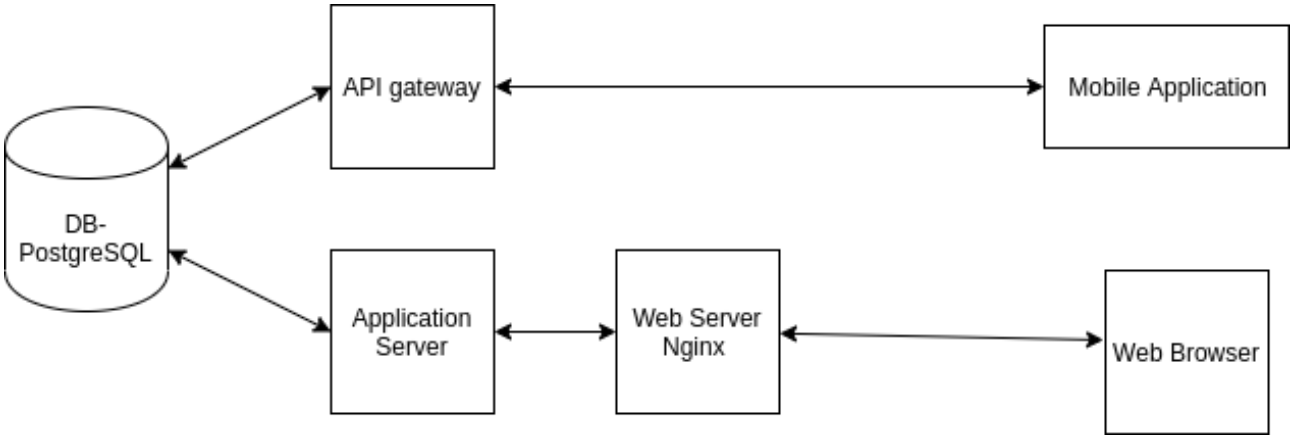
Business Overview

Innovera Payment System

Technical Overview

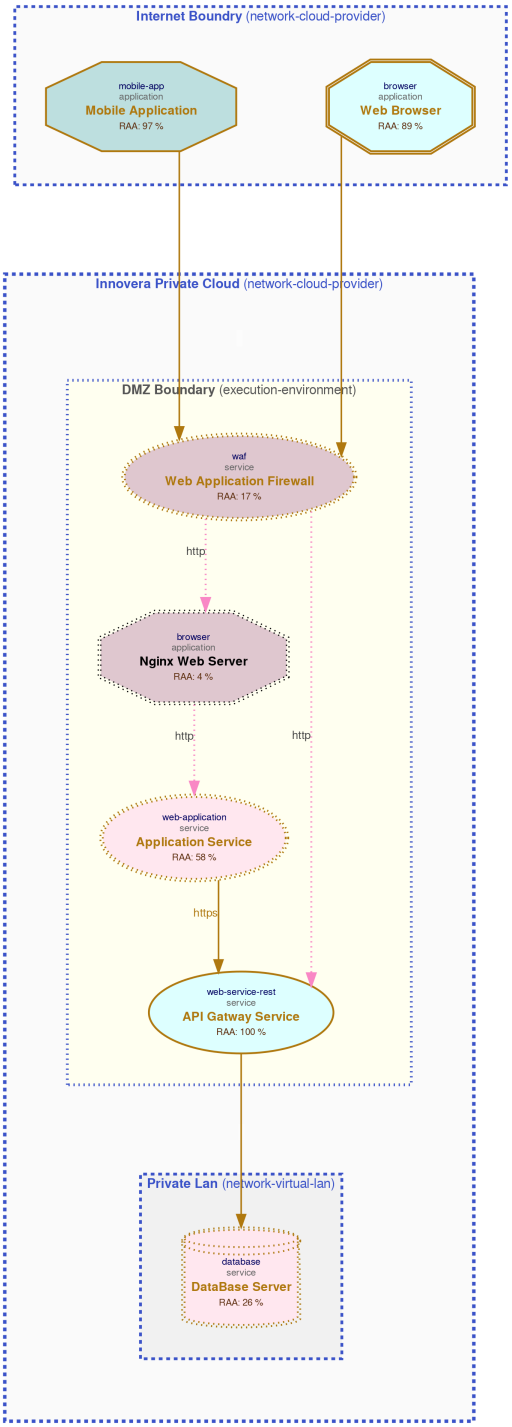
Payment System technical overview

Technical Overview:



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.

BOT activites detection and protection
The server side must detect and block robot activity

Input validation
The API must verify all input files (MIME type) from the client, only PDF format is acceptable.

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.

BOT activity and DDoS attack
As a hacker, I want to destroy the QoS and I also want to call the API by the robot.

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.

vmware
WebApp and REST API Virtualization

STRIDE Classification of Identified Risks

This chapter clusters and classifies the risks by STRIDE categories: In total **60 potential risks** have been identified during the threat modeling process of which **2 in the Spoofing** category, **15 in the Tampering** category, **0 in the Repudiation** category, **12 in the Information Disclosure** category, **6 in the Denial of Service** category, and **25 in the Elevation of Privilege** category.

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

Spoofing

Medium: **Cross-Site Request Forgery (CSRF)**: 1 / 1 Risk - 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.

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

Tampering

Elevated: **Cross-Site Scripting (XSS)**: 1 / 1 Risk - Exploitation likelihood is *Likely* with *Medium* 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: **SQL/NoSQL-Injection**: 1 / 1 Risk - Exploitation likelihood is *Very Likely* with *Medium* 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: **Untrusted Deserialization**: 6 / 6 Risks - Exploitation likelihood is *Likely* with *High* impact.
When a technical asset accepts data in a specific serialized form (like Java or .NET serialization), Untrusted Deserialization risks might arise.

Medium: **Missing Build Infrastructure**: 0 / 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 Cloud Hardening**: 2 / 2 Risks - Exploitation likelihood is *Unlikely* with *High* impact.
Cloud components should be hardened according to the cloud vendor best practices. This affects their configuration, auditing, and further areas.

Medium: **Missing Hardening**: 4 / 4 Risks - Exploitation likelihood is *Likely* with *Low* 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.

Repudiation

n/a

Information Disclosure

Elevated: **XML External Entity (XXE)**: 4 / 4 Risks - Exploitation likelihood is *Very Likely* with *Medium* impact.
When a technical asset accepts data in XML format, XML External Entity (XXE) 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: **Server-Side Request Forgery (SSRF)**: 4 / 4 Risks - Exploitation likelihood is *Likely* with *Low* 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.

Low: **Wrong Communication Link Content**: 3 / 3 Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
When a communication link is defined as readonly, but does not receive any data asset, or when it is defined as not readonly, but does not send any data asset, it is likely to be a model failure.

Denial of Service

Critical: **Service Disaster**: 1 / 1 Risk - Exploitation likelihood is *Likely* with *High* impact.
Service disater in the case of force module incident

Low: **DoS-risky Access Across Trust-Boundary**: 5 / 5 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: **Unguarded Access From Internet**: 3 / 3 Risks - Exploitation likelihood is *Very Likely* with *Medium* impact.
Internet-exposed assets must be guarded by a protecting service, application, or reverse-proxy.

Medium: **Missing Two-Factor Authentication (2FA)**: 2 / 2 Risks - 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.

Low: **Missing Identity Propagation**: 3 / 3 Risks - Exploitation likelihood is *Unlikely* with *Low* 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.

Low: **Missing Network Segmentation**: 2 / 2 Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
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.

Low: **Unnecessary Communication Link**: 3 / 3 Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
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).

Low: **Unnecessary Data Transfer**: 8 / 8 Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
When a technical asset sends or receives data assets, which it neither processes or stores this is an indicator for unnecessarily transferred data (or for an incomplete model). When the unnecessarily transferred data assets are sensitive, this poses an unnecessary risk of an increased attack surface.

Low: **Unnecessary Technical Asset**: 4 / 4 Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
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).

Assignment by Function

This chapter clusters and assigns the risks by functions which are most likely able to check and mitigate them: In total **60 potential risks** have been identified during the threat modeling process of which **3 should be checked by Business Side**, **32 should be checked by Architecture**, **12 should be checked by Development**, and **13 should be checked by Operations**.
Risk finding paragraphs are clickable and link to the corresponding chapter.

Business Side

Critical: **Service Disaster**: 1 / 1 Risk - Exploitation likelihood is *Likely* with *High* impact.
Service HA

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

Architecture

Elevated: **Unguarded Access From Internet**: 3 / 3 Risks - Exploitation likelihood is *Very Likely* with *Medium* impact.
Encapsulate the asset behind a guarding service, application, or reverse-proxy. For admin maintenance a bastion-host should be used as a jump-server. For file transfer a store-and-forward-host should be used as an indirect file exchange platform.

Elevated: **Untrusted Deserialization**: 6 / 6 Risks - Exploitation likelihood is *Likely* with *High* impact.
Try to avoid the deserialization of untrusted data (even of data within the same trust-boundary as long as it is sent across a remote connection) in order to stay safe from Untrusted Deserialization vulnerabilities. Alternatively a strict whitelisting approach of the classes/types/values to deserialize might help as well. 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: **Missing Build Infrastructure**: 0 / 1 Risk - Exploitation likelihood is *Unlikely* with *Medium* impact.
Include the build infrastructure in the model.

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.).

Low: **Missing Identity Propagation**: 3 / 3 Risks - Exploitation likelihood is *Unlikely* with *Low* 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.

Low: **Unnecessary Communication Link**: 3 / 3 Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
Try to avoid using technical communication links that do not send or receive anything.

Low: **Unnecessary Data Transfer**: 8 / 8 Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
Try to avoid sending or receiving sensitive data assets which are not required (i.e. neither processed or stored) by the involved technical asset.

Low: **Unnecessary Technical Asset**: 4 / 4 Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
Try to avoid using technical assets that do not process or store anything.

Low: **Wrong Communication Link Content**: 3 / 3 Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
Try to model the correct readonly flag and/or data sent/received of communication links. Also try to use communication link types matching the target technology/machine types.

Development

Elevated: **Cross-Site Scripting (XSS)**: 1 / 1 Risk - Exploitation likelihood is *Likely* with *Medium* 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: **SQL/NoSQL-Injection**: 1 / 1 Risk - Exploitation likelihood is *Very Likely* with *Medium* impact.
Try to use parameter binding to be safe from injection vulnerabilities. When a third-party product is used instead of custom developed software, check if the product applies the proper mitigation and ensure a reasonable patch-level.

Elevated: **XML External Entity (XXE)**: 4 / 4 Risks - Exploitation likelihood is *Very Likely* with *Medium* 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.

Medium: **Cross-Site Request Forgery (CSRF)**: 1 / 1 Risk - 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.

Medium: **Missing File Validation**: 1 / 1 Risk - Exploitation likelihood is *Very Likely* with *Low* 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.

Medium: **Server-Side Request Forgery (SSRF)**: 4 / 4 Risks - Exploitation likelihood is *Likely* with *Low* impact.
Try to avoid constructing the outgoing target URL with caller controllable values. Alternatively use a mapping (whitelist) when accessing outgoing URLs instead of creating them including caller controllable values. When a third-party product is used instead of custom developed software, check if the product applies the proper mitigation and ensure a reasonable patch-level.

Operations

Medium: **Missing Cloud Hardening**: 2 / 2 Risks - Exploitation likelihood is *Unlikely* with *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).

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

Low: **DoS-risky Access Across Trust-Boundary**: 5 / 5 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.

Low: **Missing Network Segmentation**: 2 / 2 Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
Apply a network segmentation trust-boundary around the highly sensitive assets and/or datastores.

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.

API Gatway Service: RAA 100%
innovera api gatway service developed by java (spring boot framework)

Mobile Application: RAA 97%
Innovera mobile application

Web Browser: RAA 89%
Web broser that used by customers

Application Service: RAA 58%
Innovera Application Service (MVC / Spring boot)

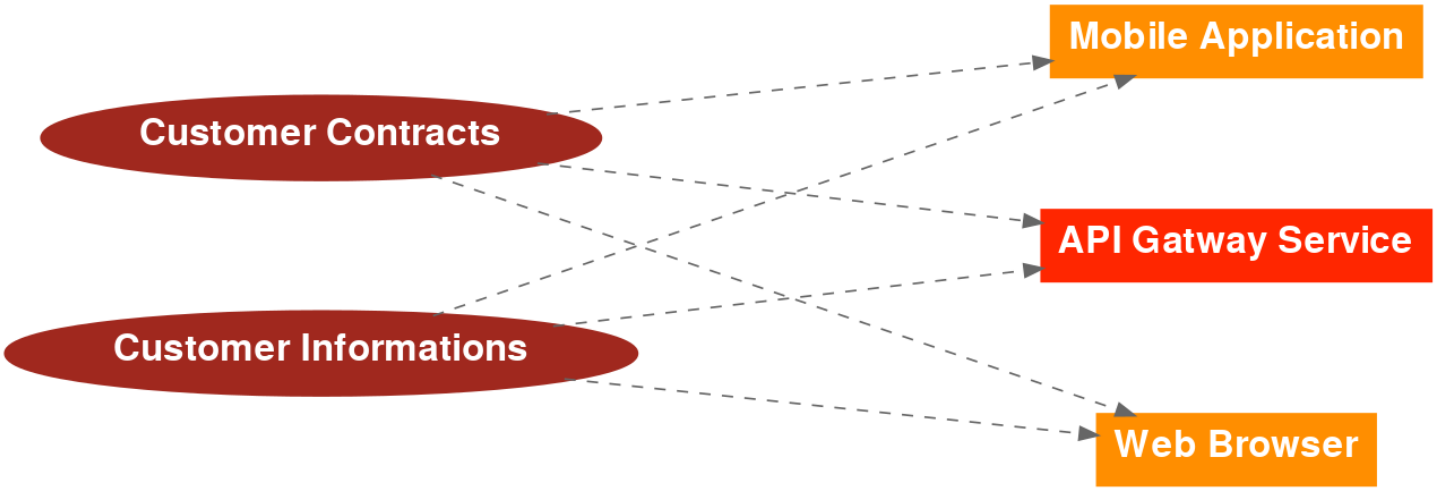
DataBase Server: RAA 26%
Innovera Databse Server

Web Application Firewall: RAA 17%
Web Application Firewall (Barracuda)

Nginx Web Server: RAA 4%
Web Server (Reverse Proxy)

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: 19 / 20 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**: 0 / 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.

Low: **Unnecessary Communication Link**: 3 / 3 Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
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).

Low: **Unnecessary Data Transfer**: 8 / 8 Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
When a technical asset sends or receives data assets, which it neither processes or stores this is an indicator for unnecessarily transferred data (or for an incomplete model). When the unnecessarily transferred data assets are sensitive, this poses an unnecessary risk of an increased attack surface.

Low: **Unnecessary Technical Asset**: 4 / 4 Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
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).

Low: **Wrong Communication Link Content**: 3 / 3 Risks - Exploitation likelihood is *Unlikely* with *Low* impact.
When a communication link is defined as readonly, but does not receive any data asset, or when it is defined as not readonly, but does not send any data asset, it is likely to be a model failure.

Questions: 0 / 2 Questions

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

Are there bot-based attacks and the possibility of abusing the service? ?
No. It is not easily possible. But an attacker can spend time. By using fourth-generation bots like headless chrome to simulate real user behavior (browser).

MiTM Attack?
Can an attacker detect and manipulate traffic between the user and the inside of the API innovera (in mobile applications)?

Identified Risks by Vulnerability Category

In total **60 potential risks** have been identified during the threat modeling process of which **1 are rated as critical**, **0 as high**, **14 as elevated**, **17 as medium**, and **28 as low**.

These risks are distributed across **21 vulnerability categories**. The following sub-chapters of this section describe each identified risk category.

Service Disaster: 1 / 1 Risk

Description (Denial of Service): CWE 1234

Service disater in the case of force module incident

Impact

QoS

Detection Logic

by pinging service

Risk Rating

identifed by Innovera red team during local benchmark

False Positives

no, agents are dirstbuted in multi location

Mitigation (Business Side): Some text describing the action...

Service HA

ASVS Chapter: V0 - Denial of Service
Cheat Sheet: Denial_of_Service_Cheat_Sheet

Check

distribute tiny agent ping

Risk Findings

The risk **Service Disaster** 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.

Critical Risk Severity

Service Disater at **Innovera API gateway**: Exploitation likelihood is *Likely* with *High* impact.

Innovera-Service-Disater@innovera-api-gatway-service

Unchecked

Cross-Site Scripting (XSS): 1 / 1 Risk

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 **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

Cross-Site Scripting (XSS) risk at **Application Service**: Exploitation likelihood is *Likely* with *Medium* impact.

cross-site-scripting@Innovera-Application-Service

Unchecked

SQL/NoSQL-Injection: 1 / 1 Risk

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 **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

SQL/NoSQL-Injection risk at **API Gatway Service** against database **DataBase Server** via **Public Internet Traffic**: Exploitation likelihood is *Very Likely* with *Medium* impact.

sql-nosql-injection@innovera-api-gatway-service@Innovera-Database-Server@innovera-api-gatway-service>public-internet-traffic

Unchecked

Unguarded Access From Internet: 3 / 3 Risks

Description (Elevation of Privilege): CWE 501

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

Impact

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

Detection Logic

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

Risk Rating

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

False Positives

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

Mitigation (Architecture): Encapsulation of Technical Asset

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

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

Check

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

Risk Findings

The risk **Unguarded Access From Internet** was found **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

Unguarded Access from Internet of **API Gatway Service** by **Application Service** via **Local Network Area**: Exploitation likelihood is *Very Likely* with *Medium* impact.

unguarded-access-from-internet@innovera-api-gatway-service@Innovera-Application-Service@Innovera-Application-Service>local-network-area

Unchecked

Unguarded Access from Internet of **API Gatway Service** by **Web Application Firewall** via **Linke to API gateway**: Exploitation likelihood is *Very Likely* with *Medium* impact.

unguarded-access-from-internet@innovera-api-gatway-service@Innovera-WAF@Innovera-WAF>linke-to-api-gateway

Unchecked

Medium Risk Severity

Unguarded Access from Internet of **DataBase Server** by **API Gatway Service** via **Public Internet Traffic**: Exploitation likelihood is *Very Likely* with *Low* impact.

unguarded-access-from-internet@Innovera-Database-Server@innovera-api-gatway-service@innovera-api-gatway-service>public-internet-traffic

Unchecked

Untrusted Deserialization: 6 / 6 Risks

Description (Tampering): CWE 502

When a technical asset accepts data in a specific serialized form (like Java or .NET serialization), Untrusted Deserialization risks might arise.

See https://christian-schneider.net/JavaDeserializationSecurityFAQ.html for more details.

Impact

If this risk is unmitigated, attackers might be able to execute code on target systems by exploiting untrusted deserialization endpoints.

Detection Logic

In-scope technical assets accepting serialization data formats (including EJB and RMI protocols).

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) data deserialized can be considered as false positives after individual review.

Mitigation (Architecture): Prevention of Deserialization of Untrusted Data

Try to avoid the deserialization of untrusted data (even of data within the same trust-boundary as long as it is sent across a remote connection) in order to stay safe from Untrusted Deserialization vulnerabilities. Alternatively a strict whitelisting approach of the classes/types/values to deserialize might help as well. 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: Deserialization_Cheat_Sheet

Check

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

Risk Findings

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

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

Elevated Risk Severity

Untrusted Deserialization risk at **API Gatway Service**: Exploitation likelihood is *Likely* with *High* impact.

untrusted-deserialization@innovera-api-gatway-service

Unchecked

Untrusted Deserialization risk at **Application Service**: Exploitation likelihood is *Likely* with *High* impact.

untrusted-deserialization@Innovera-Application-Service

Unchecked

Untrusted Deserialization risk at **DataBase Server**: Exploitation likelihood is *Likely* with *High* impact.

untrusted-deserialization@Innovera-Database-Server

Unchecked

Untrusted Deserialization risk at **Mobile Application**: Exploitation likelihood is *Likely* with *High* impact.

untrusted-deserialization@innovera-mobile-application

Unchecked

Untrusted Deserialization risk at **Nginx Web Server**: Exploitation likelihood is *Likely* with *High* impact.

untrusted-deserialization@Innovera-Web-Server-Nginx

Unchecked

Untrusted Deserialization risk at **Web Browser**: Exploitation likelihood is *Likely* with *High* impact.

untrusted-deserialization@Web-browser

Unchecked

XML External Entity (XXE): 4 / 4 Risks

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

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

Elevated Risk Severity

XML External Entity (XXE) risk at **Application Service**: Exploitation likelihood is *Very Likely* with *Medium* impact.

xml-external-entity@Innovera-Application-Service

Unchecked

XML External Entity (XXE) risk at **DataBase Server**: Exploitation likelihood is *Very Likely* with *Medium* impact.

xml-external-entity@Innovera-Database-Server

Unchecked

XML External Entity (XXE) risk at **Nginx Web Server**: Exploitation likelihood is *Very Likely* with *Medium* impact.

xml-external-entity@Innovera-Web-Server-Nginx

Unchecked

XML External Entity (XXE) risk at **Web Browser**: Exploitation likelihood is *Very Likely* with *Medium* impact.

xml-external-entity@Web-browser

Unchecked

Cross-Site Request Forgery (CSRF): 1 / 1 Risk

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 **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

Cross-Site Request Forgery (CSRF) risk at **Application Service** via **Public Internet Link** from **Nginx Web Server**: Exploitation likelihood is *Very Likely* with *Low* impact.

cross-site-request-forgery@Innovera-Application-Service@Innovera-Web-Server-Nginx>public-internet-link

Unchecked

Missing Cloud Hardening: 2 / 2 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 **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

Missing Cloud Hardening risk at **Innovera Private Cloud**: Exploitation likelihood is *Unlikely* with *High* impact.

missing-cloud-hardening@Innovera-Private-Cloud

Unchecked

Missing Cloud Hardening risk at **Internet Boundry**: Exploitation likelihood is *Unlikely* with *High* impact.

missing-cloud-hardening@Internet-Boundry

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.

Medium Risk Severity

Missing File Validation risk at **API Gatway Service**: Exploitation likelihood is *Very Likely* with *Low* impact.

missing-file-validation@innovera-api-gatway-service

Unchecked

Missing Hardening: 4 / 4 Risks

Description (Tampering): CWE 16

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

Impact

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

Detection Logic

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

Risk Rating

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

False Positives

Usually no false positives.

Mitigation (Operations): System Hardening

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

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

Check

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

Risk Findings

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

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

Medium Risk Severity

Missing Hardening risk at **API Gatway Service**: Exploitation likelihood is *Likely* with *Low* impact.

missing-hardening@innovera-api-gatway-service

Unchecked

Missing Hardening risk at **Application Service**: Exploitation likelihood is *Likely* with *Low* impact.

missing-hardening@Innovera-Application-Service

Unchecked

Missing Hardening risk at **Mobile Application**: Exploitation likelihood is *Likely* with *Low* impact.

missing-hardening@innovera-mobile-application

Unchecked

Missing Hardening risk at **Web Browser**: Exploitation likelihood is *Likely* with *Low* impact.

missing-hardening@Web-browser

Unchecked

Missing Two-Factor Authentication (2FA): 2 / 2 Risks

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 **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

Missing Two-Factor Authentication covering communication link **Linke to API gateway** from **Mobile Application** forwarded via **Web Application Firewall** to **API Gatway Service**: Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-authentication-second-factor@Innovera-WAF>linke-to-api-gateway@Innovera-WAF@innovera-api-gatway-service

Unchecked

Missing Two-Factor Authentication covering communication link **Linke to API gateway** from **Web Browser** forwarded via **Web Application Firewall** to **API Gatway Service**: Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-authentication-second-factor@Innovera-WAF>linke-to-api-gateway@Innovera-WAF@innovera-api-gatway-service

Unchecked

Missing Vault (Secret Storage): 1 / 1 Risk

Description (Information Disclosure): CWE 522

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

Impact

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

Detection Logic

Models without a Vault (Secret Storage).

Risk Rating

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

False Positives

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

Mitigation (Architecture): Vault (Secret Storage)

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

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

Check

Is a Vault (Secret Storage) in place?

Risk Findings

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

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

Medium Risk Severity

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

missing-vault@Innovera-Application-Service

Unchecked

Server-Side Request Forgery (SSRF): 4 / 4 Risks

Description (Information Disclosure): CWE 918

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

Impact

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

Detection Logic

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

Risk Rating

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

False Positives

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

Mitigation (Development): SSRF Prevention

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

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

Check

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

Risk Findings

The risk **Server-Side Request Forgery (SSRF)** was found **4 times** in the analyzed architecture to be potentially possible. Each spot should be checked individually by reviewing the implementation whether all controls have been applied properly in order to mitigate each risk.

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

Medium Risk Severity

Server-Side Request Forgery (SSRF) risk at **API Gatway Service** server-side web-requesting the target **DataBase Server** via **Public Internet Traffic**: Exploitation likelihood is *Likely* with *Low* impact.

server-side-request-forgery@innovera-api-gatway-service@Innovera-Database-Server@innovera-api-gatway-service>public-internet-traffic

Unchecked

Server-Side Request Forgery (SSRF) risk at **Application Service** server-side web-requesting the target **API Gatway Service** via **Local Network Area**: Exploitation likelihood is *Likely* with *Low* impact.

server-side-request-forgery@Innovera-Application-Service@innovera-api-gatway-service@Innovera-Application-Service>local-network-area

Unchecked

Server-Side Request Forgery (SSRF) risk at **Web Application Firewall** server-side web-requesting the target **API Gatway Service** via **Linke to API gateway**: Exploitation likelihood is *Likely* with *Low* impact.

server-side-request-forgery@Innovera-WAF@innovera-api-gatway-service@Innovera-WAF>linke-to-api-gateway

Unchecked

Server-Side Request Forgery (SSRF) risk at **Web Application Firewall** server-side web-requesting the target **Nginx Web Server** via **Link to Nginx**: Exploitation likelihood is *Likely* with *Low* impact.

server-side-request-forgery@Innovera-WAF@Innovera-Web-Server-Nginx@Innovera-WAF>link-to-nginx

Unchecked

DoS-risky Access Across Trust-Boundary: 5 / 5 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 **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.

Low Risk Severity

Denial-of-Service risky access of **API Gatway Service** by **Mobile Application** via **Internet Public Traffic** forwarded via **Web Application Firewall**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@innovera-api-gatway-service@innovera-mobile-application@innovera-mobile-application>internet-public-traffic

Unchecked

Denial-of-Service risky access of **API Gatway Service** by **Web Browser** via **Public Internet Link** forwarded via **Web Application Firewall**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@innovera-api-gatway-service@Web-browser@Web-browser>public-internet-link

Unchecked

Denial-of-Service risky access of **DataBase Server** by **API Gatway Service** via **Public Internet Traffic**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@Innovera-Database-Server@innovera-api-gatway-service@innovera-api-gatway-service>public-internet-traffic

Unchecked

Denial-of-Service risky access of **Web Application Firewall** by **Mobile Application** via **Internet Public Traffic**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@Innovera-WAF@innovera-mobile-application@innovera-mobile-application>internet-public-traffic

Unchecked

Denial-of-Service risky access of **Web Application Firewall** by **Web Browser** via **Public Internet Link**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@Innovera-WAF@Web-browser@Web-browser>public-internet-link

Unchecked

Missing Identity Propagation: 3 / 3 Risks

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 **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

Missing Enduser Identity Propagation over communication link **Linke to API gateway** from **Web Application Firewall** to **API Gatway Service**: Exploitation likelihood is *Unlikely* with *Low* impact.

missing-identity-propagation@Innovera-WAF>linke-to-api-gateway@Innovera-WAF@innovera-api-gatway-service

Unchecked

Missing Enduser Identity Propagation over communication link **Local Network Area** from **Application Service** to **API Gatway Service**: Exploitation likelihood is *Unlikely* with *Low* impact.

missing-identity-propagation@Innovera-Application-Service>local-network-area@Innovera-Application-Service@innovera-api-gatway-service

Unchecked

Missing Enduser Identity Propagation over communication link **Public Internet Link** from **Nginx Web Server** to **Application Service**: Exploitation likelihood is *Unlikely* with *Low* impact.

missing-identity-propagation@Innovera-Web-Server-Nginx>public-internet-link@Innovera-Web-Server-Nginx@Innovera-Application-Service

Unchecked

Missing Network Segmentation: 2 / 2 Risks

Description (Elevation of Privilege): CWE 1008

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.

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 not separated by network segmentation.

Detection Logic

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).

Risk 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.

False Positives

When all assets within the network segmentation trust-boundary are hardened and protected to the same extend as if all were containing/processing highly sensitive data.

Mitigation (Operations): Network Segmentation

Apply a network segmentation trust-boundary around the highly sensitive assets and/or datastores.

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 Network Segmentation** 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.

Low Risk Severity

Missing Network Segmentation to further encapsulate and protect **API Gatway Service** against unrelated lower protected assets in the same network segment, which might be easier to compromise by attackers: Exploitation likelihood is *Unlikely* with *Low* impact.

missing-network-segmentation@innovera-api-gatway-service

Unchecked

Missing Network Segmentation to further encapsulate and protect **Mobile Application** against unrelated lower protected assets in the same network segment, which might be easier to compromise by attackers: Exploitation likelihood is *Unlikely* with *Low* impact.

missing-network-segmentation@innovera-mobile-application

Unchecked

Unnecessary Communication Link: 3 / 3 Risks

Description (Elevation of Privilege): CWE 1008

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).

Impact

If this risk is unmitigated, attackers might be able to target unnecessary communication links.

Detection Logic

In-scope technical assets' technical communication links not sending or receiving any data assets.

Risk Rating

low

False Positives

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

Mitigation (Architecture): Attack Surface Reduction

Try to avoid using technical communication links that do not send or receive anything.

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 Communication Link** 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

Unnecessary Communication Link titled **Link to Nginx** at technical asset **Web Application Firewall**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-communication-link@Innovera-WAF>link-to-nginx@Innovera-WAF

Unchecked

Unnecessary Communication Link titled **Linke to API gateway** at technical asset **Web Application Firewall**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-communication-link@Innovera-WAF>linke-to-api-gateway@Innovera-WAF

Unchecked

Unnecessary Communication Link titled **Public Internet Link** at technical asset **Nginx Web Server**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-communication-link@Innovera-Web-Server-Nginx>public-internet-link@Innovera-Web-Server-Nginx

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.

Low Risk Severity

Unnecessary Data Transfer of **Customer Contracts** data at **Application Service** from/to **API Gatway Service**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@innovera-customer-contracts@Innovera-Application-Service@innovera-api-gatway-service

Unchecked

Unnecessary Data Transfer of **Customer Contracts** data at **DataBase Server** from/to **API Gatway Service**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@innovera-customer-contracts@Innovera-Database-Server@innovera-api-gatway-service

Unchecked

Unnecessary Data Transfer of **Customer Contracts** data at **Web Application Firewall** from/to **Mobile Application**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@innovera-customer-contracts@Innovera-WAF@innovera-mobile-application

Unchecked

Unnecessary Data Transfer of **Customer Contracts** data at **Web Application Firewall** from/to **Web Browser**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@innovera-customer-contracts@Innovera-WAF@Web-browser

Unchecked

Unnecessary Data Transfer of **Customer Informations** data at **Application Service** from/to **API Gatway Service**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@innovera-customer-information@Innovera-Application-Service@innovera-api-gatway-service

Unchecked

Unnecessary Data Transfer of **Customer Informations** data at **DataBase Server** from/to **API Gatway Service**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@innovera-customer-information@Innovera-Database-Server@innovera-api-gatway-service

Unchecked

Unnecessary Data Transfer of **Customer Informations** data at **Web Application Firewall** from/to **Mobile Application**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@innovera-customer-information@Innovera-WAF@innovera-mobile-application

Unchecked

Unnecessary Data Transfer of **Customer Informations** data at **Web Application Firewall** from/to **Web Browser**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@innovera-customer-information@Innovera-WAF@Web-browser

Unchecked

Unnecessary Technical Asset: 4 / 4 Risks

Description (Elevation of Privilege): CWE 1008

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).

Impact

If this risk is unmitigated, attackers might be able to target unnecessary technical assets.

Detection Logic

Technical assets not processing or storing any data assets.

Risk Rating

low

False Positives

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

Mitigation (Architecture): Attack Surface Reduction

Try to avoid using technical assets that do not process or store anything.

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

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

Low Risk Severity

Unnecessary Technical Asset named **Application Service**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-technical-asset@Innovera-Application-Service

Unchecked

Unnecessary Technical Asset named **DataBase Server**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-technical-asset@Innovera-Database-Server

Unchecked

Unnecessary Technical Asset named **Nginx Web Server**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-technical-asset@Innovera-Web-Server-Nginx

Unchecked

Unnecessary Technical Asset named **Web Application Firewall**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-technical-asset@Innovera-WAF

Unchecked

Wrong Communication Link Content: 3 / 3 Risks

Description (Information Disclosure): CWE 1008

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

Impact

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

Detection Logic

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

Risk Rating

low

False Positives

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

Mitigation (Architecture): Model Consistency

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

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

Check

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

Risk Findings

The risk **Wrong Communication Link Content** was found **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

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **Nginx Web Server** regarding communication link **Public Internet Link**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@Innovera-Web-Server-Nginx@Innovera-Web-Server-Nginx>public-internet-link

Unchecked

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **Web Application Firewall** regarding communication link **Link to Nginx**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@Innovera-WAF@Innovera-WAF>link-to-nginx

Unchecked

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **Web Application Firewall** regarding communication link **Linke to API gateway**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@Innovera-WAF@Innovera-WAF>linke-to-api-gateway

Unchecked

Missing Build Infrastructure: 0 / 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 **API Gatway Service** as an example): Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-build-infrastructure@innovera-api-gatway-service

Mitigated 2022-05-12 Khalegh Salehi INRM-1000-1

The hardening measures were implemented and checked

Identified Risks by Technical Asset

In total **60 potential risks** have been identified during the threat modeling process of which **1 are rated as critical**, **0 as high**, **14 as elevated**, **17 as medium**, and **28 as low**.

These risks are distributed across **7 in-scope technical assets**. The following sub-chapters of this section describe each identified risk grouped by technical asset. The RAA value of a technical asset is the calculated "Relative Attacker Attractiveness" value in percent.

API Gatway Service: 15 / 16 Risks

Description

innovera api gatway service developed by java (spring boot framework)

Identified Risks of Asset

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

Critical Risk Severity

Service Disater at **Innovera API gateway**: Exploitation likelihood is *Likely* with *High* impact.

Innovera-Service-Disater@innovera-api-gatway-service

Unchecked

Elevated Risk Severity

Untrusted Deserialization risk at **API Gatway Service**: Exploitation likelihood is *Likely* with *High* impact.

untrusted-deserialization@innovera-api-gatway-service

Unchecked

SQL/NoSQL-Injection risk at **API Gatway Service** against database **DataBase Server** via **Public Internet Traffic**: Exploitation likelihood is *Very Likely* with *Medium* impact.

sql-nosql-injection@innovera-api-gatway-service@Innovera-Database-Server@innovera-api-gatway-service>public-internet-traffic

Unchecked

Unguarded Access from Internet of **API Gatway Service** by **Application Service** via **Local Network Area**: Exploitation likelihood is *Very Likely* with *Medium* impact.

unguarded-access-from-internet@innovera-api-gatway-service@Innovera-Application-Service@Innovera-Application-Service>local-network-area

Unchecked

Unguarded Access from Internet of **API Gatway Service** by **Web Application Firewall** via **Linke to API gateway**: Exploitation likelihood is *Very Likely* with *Medium* impact.

unguarded-access-from-internet@innovera-api-gatway-service@Innovera-WAF@Innovera-WAF>linke-to-api-gateway

Unchecked

Medium Risk Severity

Missing Two-Factor Authentication covering communication link **Linke to API gateway** from **Mobile Application** forwarded via **Web Application Firewall** to **API Gatway Service**: Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-authentication-second-factor@Innovera-WAF>linke-to-api-gateway@Innovera-WAF@innovera-api-gatway-service

Unchecked

Missing Two-Factor Authentication covering communication link **Linke to API gateway** from **Web Browser** forwarded via **Web Application Firewall** to **API Gatway Service**: Exploitation likelihood is *Unlikely* with *Medium* impact.

missing-authentication-second-factor@Innovera-WAF>linke-to-api-gateway@Innovera-WAF@innovera-api-gatway-service

Unchecked

Missing File Validation risk at **API Gatway Service**: Exploitation likelihood is *Very Likely* with *Low* impact.

missing-file-validation@innovera-api-gatway-service

Unchecked

Missing Hardening risk at **API Gatway Service**: Exploitation likelihood is *Likely* with *Low* impact.

missing-hardening@innovera-api-gatway-service

Unchecked

Server-Side Request Forgery (SSRF) risk at **API Gatway Service** server-side web-requesting the target **DataBase Server** via **Public Internet Traffic**: Exploitation likelihood is *Likely* with *Low* impact.

server-side-request-forgery@innovera-api-gatway-service@Innovera-Database-Server@innovera-api-gatway-service>public-internet-traffic

Unchecked

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

missing-build-infrastructure@innovera-api-gatway-service

Mitigated 2022-05-12 Khalegh Salehi INRM-1000-1
The hardening measures were implemented and checked

Low Risk Severity

Denial-of-Service risky access of **API Gatway Service** by **Mobile Application** via **Internet Public Traffic** forwarded via **Web Application Firewall**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@innovera-api-gatway-service@innovera-mobile-application@innovera-mobile-application>internet-public-traffic

Unchecked

Denial-of-Service risky access of **API Gatway Service** by **Web Browser** via **Public Internet Link** forwarded via **Web Application Firewall**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@innovera-api-gatway-service@Web-browser@Web-browser>public-internet-link

Unchecked

Missing Enduser Identity Propagation over communication link **Linke to API gateway** from **Web Application Firewall** to **API Gatway Service**: Exploitation likelihood is *Unlikely* with *Low* impact.

missing-identity-propagation@Innovera-WAF>linke-to-api-gateway@Innovera-WAF@innovera-api-gatway-service

Unchecked

Missing Enduser Identity Propagation over communication link **Local Network Area** from **Application Service** to **API Gatway Service**: Exploitation likelihood is *Unlikely* with *Low* impact.

missing-identity-propagation@Innovera-Application-Service>local-network-area@Innovera-Application-Service@innovera-api-gatway-service

Unchecked

Missing Network Segmentation to further encapsulate and protect **API Gatway Service** against unrelated lower protected assets in the same network segment, which might be easier to compromise by attackers: Exploitation likelihood is *Unlikely* with *Low* impact.

missing-network-segmentation@innovera-api-gatway-service

Unchecked

Asset Information

ID:	innovera-api-gatway-service
Type:	process
Usage:	devops
RAA:	100 %
Size:	service
Technology:	web-service-rest
Tags:	none
Internet:	true
Machine:	virtual
Encryption:	data-with-asymmetric-shared-key
Multi-Tenant:	false
Redundant:	false
Custom-Developed:	true
Client by Human:	false
Data Processed:	Customer Contracts, Customer Informations
Data Stored:	none
Formats Accepted:	File, JSON, Serialization

Asset Rating

Owner:	Innovera Development Team	
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:		

Outgoing Communication Links: 1

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

Public Internet Traffic (outgoing)

Some Description

Target:	DataBase Server
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	none
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Sent:	Customer Contracts, Customer Informations
Data Received:	Customer Contracts, Customer Informations

Incoming Communication Links: 2

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

Linke to API gateway (incoming)

Internet Link

Source:	Web Application Firewall
Protocol:	http
Encrypted:	false
Authentication:	session-id
Authorization:	none
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Received:	none
Data Sent:	none

Local Network Area (incoming)

Local Area Network

Source:	Application Service
Protocol:	https
Encrypted:	true
Authentication:	session-id
Authorization:	none
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Received:	Customer Contracts, Customer Informations
Data Sent:	Customer Contracts, Customer Informations

Application Service: 11 / 11 Risks

Description

Innovera Application Service (MVC / Spring boot)

Identified Risks of Asset

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

Elevated Risk Severity

Untrusted Deserialization risk at **Application Service**: Exploitation likelihood is *Likely* with *High* impact.

untrusted-deserialization@Innovera-Application-Service

Unchecked

XML External Entity (XXE) risk at **Application Service**: Exploitation likelihood is *Very Likely* with *Medium* impact.

xml-external-entity@Innovera-Application-Service

Unchecked

Cross-Site Scripting (XSS) risk at **Application Service**: Exploitation likelihood is *Likely* with *Medium* impact.

cross-site-scripting@Innovera-Application-Service

Unchecked

Medium Risk Severity

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

missing-vault@Innovera-Application-Service

Unchecked

Cross-Site Request Forgery (CSRF) risk at **Application Service** via **Public Internet Link** from **Nginx Web Server**: Exploitation likelihood is *Very Likely* with *Low* impact.

cross-site-request-forgery@Innovera-Application-Service@Innovera-Web-Server-Nginx>public-internet-link

Unchecked

Missing Hardening risk at **Application Service**: Exploitation likelihood is *Likely* with *Low* impact.

missing-hardening@Innovera-Application-Service

Unchecked

Server-Side Request Forgery (SSRF) risk at **Application Service** server-side web-requesting the target **API Gatway Service** via **Local Network Area**: Exploitation likelihood is *Likely* with *Low* impact.

server-side-request-forgery@Innovera-Application-Service@innovera-api-gatway-service@Innovera-Application-Service>local-network-area

Unchecked

Low Risk Severity

Missing Enduser Identity Propagation over communication link **Public Internet Link** from **Nginx Web Server** to **Application Service**: Exploitation likelihood is *Unlikely* with *Low* impact.

missing-identity-propagation@Innovera-Web-Server-Nginx>public-internet-link@Innovera-Web-Server-Nginx@Innovera-Application-Service

Unchecked

Unnecessary Data Transfer of **Customer Contracts** data at **Application Service** from/to **API Gatway Service**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@innovera-customer-contracts@Innovera-Application-Service@innovera-api-gatway-service

Unchecked

Unnecessary Data Transfer of **Customer Informations** data at **Application Service** from/to **API Gatway Service**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@innovera-customer-information@Innovera-Application-Service@innovera-api-gatway-service

Unchecked

Unnecessary Technical Asset named **Application Service**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-technical-asset@Innovera-Application-Service

Unchecked

Asset Information

ID:	Innovera-Application-Service
Type:	process
Usage:	business
RAA:	58 %
Size:	service
Technology:	web-application
Tags:	none
Internet:	true
Machine:	virtual
Encryption:	data-with-symmetric-shared-key
Multi-Tenant:	false
Redundant:	true
Custom-Developed:	false
Client by Human:	false

Data Processed: none
Data Stored: none
Formats Accepted: CSV, File, JSON, Serialization, XML

Asset Rating

Owner: Innovera Developemnt Team
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:

Outgoing Communication Links: 1

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

Local Network Area (outgoing)
Local Area Network

Target: API Gatway Service
Protocol: https
Encrypted: true
Authentication: session-id
Authorization: none
Read-Only: false
Usage: business
Tags: none
VPN: false
IP-Filtered: false
Data Sent: Customer Contracts, Customer Informations
Data Received: Customer Contracts, Customer Informations

Incoming Communication Links: 1

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

Public Internet Link (incoming)
Internet Link

Source: Nginx Web Server

Protocol:	http
Encrypted:	false
Authentication:	session-id
Authorization:	none
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Received:	none
Data Sent:	none

DataBase Server: 7 / 7 Risks

Description

Innovera Databse Server

Identified Risks of Asset

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

Elevated Risk Severity

Untrusted Deserialization risk at **DataBase Server**: Exploitation likelihood is *Likely* with *High* impact.

untrusted-deserialization@Innovera-Database-Server

Unchecked

XML External Entity (XXE) risk at **DataBase Server**: Exploitation likelihood is *Very Likely* with *Medium* impact.

xml-external-entity@Innovera-Database-Server

Unchecked

Medium Risk Severity

Unguarded Access from Internet of **DataBase Server** by **API Gatway Service** via **Public Internet Traffic**: Exploitation likelihood is *Very Likely* with *Low* impact.

unguarded-access-from-internet@Innovera-Database-Server@innovera-api-gatway-service@innovera-api-gatway-service>public-internet-traffic

Unchecked

Low Risk Severity

Denial-of-Service risky access of **DataBase Server** by **API Gatway Service** via **Public Internet Traffic**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@Innovera-Database-Server@innovera-api-gatway-service@innovera-api-gatway-service>public-internet-traffic

Unchecked

Unnecessary Data Transfer of **Customer Contracts** data at **DataBase Server** from/to **API Gatway Service**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@innovera-customer-contracts@Innovera-Database-Server@innovera-api-gatway-service

Unchecked

Unnecessary Data Transfer of **Customer Informations** data at **DataBase Server** from/to **API Gatway Service**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@innovera-customer-information@Innovera-Database-Server@innovera-api-gatway-service

Unchecked

Unnecessary Technical Asset named **DataBase Server**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-technical-asset@Innovera-Database-Server

Unchecked

Asset Information

ID:	Innovera-Database-Server
Type:	datastore
Usage:	devops
RAA:	26 %
Size:	service
Technology:	database
Tags:	none
Internet:	false
Machine:	virtual
Encryption:	data-with-symmetric-shared-key
Multi-Tenant:	false
Redundant:	true
Custom-Developed:	false
Client by Human:	false
Data Processed:	none
Data Stored:	none
Formats Accepted:	CSV, File, JSON, Serialization, XML

Asset Rating

Owner:	Innovera SRE Team	
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:		

Incoming Communication Links: 1

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

Public Internet Traffic (incoming)

Some Description

Source:	API Gatway Service
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	none
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Received:	Customer Contracts, Customer Informations
Data Sent:	Customer Contracts, Customer Informations

Mobile Application: 3 / 3 Risks

Description

Innovera mobile application

Identified Risks of Asset

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

Elevated Risk Severity

Untrusted Deserialization risk at **Mobile Application**: Exploitation likelihood is *Likely* with *High* impact.

untrusted-deserialization@innovera-mobile-application

Unchecked

Medium Risk Severity

Missing Hardening risk at **Mobile Application**: Exploitation likelihood is *Likely* with *Low* impact.

missing-hardening@innovera-mobile-application

Unchecked

Low Risk Severity

Missing Network Segmentation to further encapsulate and protect **Mobile Application** against unrelated lower protected assets in the same network segment, which might be easier to compromise by attackers: Exploitation likelihood is *Unlikely* with *Low* impact.

missing-network-segmentation@innovera-mobile-application

Unchecked

Asset Information

ID:	innovera-mobile-application
Type:	process
Usage:	business
RAA:	97 %
Size:	application
Technology:	mobile-app
Tags:	none
Internet:	true

Machine:	physical
Encryption:	data-with-asymmetric-shared-key
Multi-Tenant:	false
Redundant:	false
Custom-Developed:	false
Client by Human:	true
Data Processed:	Customer Contracts, Customer Informations
Data Stored:	none
Formats Accepted:	File, JSON, Serialization

Asset Rating

Owner:	Development Team	
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:		

Outgoing Communication Links: 1

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

Internet Public Traffic (outgoing)

mobile app connection to innovera api gatway

Target:	Web Application Firewall
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	none
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Sent:	Customer Contracts, Customer Informations
Data Received:	Customer Contracts, Customer Informations

Nginx Web Server: 5 / 5 Risks

Description

Web Server (Reverse Proxy)

Identified Risks of Asset

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

Elevated Risk Severity

Untrusted Deserialization risk at **Nginx Web Server**: Exploitation likelihood is *Likely* with *High* impact.

untrusted-deserialization@Innovera-Web-Server-Nginx

Unchecked

XML External Entity (XXE) risk at **Nginx Web Server**: Exploitation likelihood is *Very Likely* with *Medium* impact.

xml-external-entity@Innovera-Web-Server-Nginx

Unchecked

Low Risk Severity

Unnecessary Communication Link titled **Public Internet Link** at technical asset **Nginx Web Server**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-communication-link@Innovera-Web-Server-Nginx>public-internet-link@Innovera-Web-Server-Nginx

Unchecked

Unnecessary Technical Asset named **Nginx Web Server**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-technical-asset@Innovera-Web-Server-Nginx

Unchecked

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **Nginx Web Server** regarding communication link **Public Internet Link**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@Innovera-Web-Server-Nginx@Innovera-Web-Server-Nginx>public-internet-link

Unchecked

Asset Information

ID:	Innovera-Web-Server-Nginx
Type:	process
Usage:	devops

RAA:	4 %
Size:	application
Technology:	browser
Tags:	none
Internet:	true
Machine:	physical
Encryption:	data-with-symmetric-shared-key
Multi-Tenant:	false
Redundant:	true
Custom-Developed:	false
Client by Human:	true
Data Processed:	none
Data Stored:	none
Formats Accepted:	CSV, File, JSON, Serialization, XML

Asset Rating

Owner:	Innovera SRE team	
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:		

Outgoing Communication Links: 1

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

Public Internet Link (outgoing)

Internet Link

Target:	Application Service
Protocol:	http
Encrypted:	false
Authentication:	session-id
Authorization:	none
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false

IP-Filtered: false
Data Sent: none
Data Received: none

Incoming Communication Links: 1

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

Link to Nginx (incoming)

Internet Link

Source: Web Application Firewall
Protocol: http
Encrypted: false
Authentication: session-id
Authorization: none
Read-Only: false
Usage: business
Tags: none
VPN: false
IP-Filtered: false
Data Received: none
Data Sent: none

Web Browser: 3 / 3 Risks

Description

Web broser that used by customers

Identified Risks of Asset

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

Elevated Risk Severity

Untrusted Deserialization risk at **Web Browser**: Exploitation likelihood is *Likely* with *High* impact.

untrusted-deserialization@Web-browser

Unchecked

XML External Entity (XXE) risk at **Web Browser**: Exploitation likelihood is *Very Likely* with *Medium* impact.

xml-external-entity@Web-browser

Unchecked

Medium Risk Severity

Missing Hardening risk at **Web Browser**: Exploitation likelihood is *Likely* with *Low* impact.

missing-hardening@Web-browser

Unchecked

Asset Information

ID:	Web-browser
Type:	process
Usage:	business
RAA:	89 %
Size:	application
Technology:	browser
Tags:	none
Internet:	true
Machine:	virtual
Encryption:	data-with-symmetric-shared-key
Multi-Tenant:	false
Redundant:	true
Custom-Developed:	false

Client by Human:	true
Data Processed:	Customer Contracts, Customer Informations
Data Stored:	none
Formats Accepted:	CSV, File, JSON, Serialization, XML

Asset Rating

Owner:	End user	
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:		

Outgoing Communication Links: 1

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

Public Internet Link (outgoing)

Internet Link

Target:	Web Application Firewall
Protocol:	https
Encrypted:	true
Authentication:	session-id
Authorization:	none
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Sent:	Customer Contracts, Customer Informations
Data Received:	Customer Contracts, Customer Informations

Web Application Firewall: 13 / 13 Risks

Description

Web Application Firewall (Barracuda)

Identified Risks of Asset

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

Medium Risk Severity

Server-Side Request Forgery (SSRF) risk at **Web Application Firewall** server-side web-requesting the target **API Gatway Service** via **Linke to API gateway**: Exploitation likelihood is *Likely* with *Low* impact.

server-side-request-forgery@Innovera-WAF@innovera-api-gatway-service@Innovera-WAF>linke-to-api-gateway

Unchecked

Server-Side Request Forgery (SSRF) risk at **Web Application Firewall** server-side web-requesting the target **Nginx Web Server** via **Link to Nginx**: Exploitation likelihood is *Likely* with *Low* impact.

server-side-request-forgery@Innovera-WAF@Innovera-Web-Server-Nginx@Innovera-WAF>link-to-nginx

Unchecked

Low Risk Severity

Denial-of-Service risky access of **Web Application Firewall** by **Mobile Application** via **Internet Public Traffic**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@Innovera-WAF@innovera-mobile-application@innovera-mobile-application>internet-public-traffic

Unchecked

Denial-of-Service risky access of **Web Application Firewall** by **Web Browser** via **Public Internet Link**: Exploitation likelihood is *Unlikely* with *Low* impact.

dos-risky-access-across-trust-boundary@Innovera-WAF@Web-browser@Web-browser>public-internet-link

Unchecked

Unnecessary Communication Link titled **Link to Nginx** at technical asset **Web Application Firewall**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-communication-link@Innovera-WAF>link-to-nginx@Innovera-WAF

Unchecked

Unnecessary Communication Link titled **Linke to API gateway** at technical asset **Web Application Firewall**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-communication-link@Innovera-WAF>linke-to-api-gateway@Innovera-WAF

Unchecked

Unnecessary Data Transfer of **Customer Contracts** data at **Web Application Firewall** from/to **Mobile Application**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@innovera-customer-contracts@Innovera-WAF@innovera-mobile-application

Unchecked

Unnecessary Data Transfer of **Customer Contracts** data at **Web Application Firewall** from/to **Web Browser**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@innovera-customer-contracts@Innovera-WAF@Web-browser

Unchecked

Unnecessary Data Transfer of **Customer Informations** data at **Web Application Firewall** from/to **Mobile Application**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@innovera-customer-information@Innovera-WAF@innovera-mobile-application

Unchecked

Unnecessary Data Transfer of **Customer Informations** data at **Web Application Firewall** from/to **Web Browser**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-data-transfer@innovera-customer-information@Innovera-WAF@Web-browser

Unchecked

Unnecessary Technical Asset named **Web Application Firewall**: Exploitation likelihood is *Unlikely* with *Low* impact.

unnecessary-technical-asset@Innovera-WAF

Unchecked

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **Web Application Firewall** regarding communication link **Link to Nginx**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@Innovera-WAF@Innovera-WAF>link-to-nginx

Unchecked

Wrong Communication Link Content (data assets sent/received not matching the communication link's readonly flag) at **Web Application Firewall** regarding communication link **Linke to API gateway**: Exploitation likelihood is *Unlikely* with *Low* impact.

wrong-communication-link-content@Innovera-WAF@Innovera-WAF>linke-to-api-gateway

Unchecked

Asset Information

ID:	Innovera-WAF
Type:	process
Usage:	devops
RAA:	17 %
Size:	service
Technology:	waf
Tags:	none

Internet:	true
Machine:	physical
Encryption:	data-with-symmetric-shared-key
Multi-Tenant:	false
Redundant:	true
Custom-Developed:	false
Client by Human:	false
Data Processed:	none
Data Stored:	none
Formats Accepted:	none of the special data formats accepted

Asset Rating

Owner:	Innovera Security team	
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:		

Outgoing Communication Links: 2

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

Linke to API gateway (outgoing)

Internet Link

Target:	API Gatway Service
Protocol:	http
Encrypted:	false
Authentication:	session-id
Authorization:	none
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Sent:	none
Data Received:	none

Link to Nginx (outgoing)
Internet Link

Target:	Nginx Web Server
Protocol:	http
Encrypted:	false
Authentication:	session-id
Authorization:	none
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Sent:	none
Data Received:	none

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

Internet Public Traffic (incoming)
mobile app connection to innovera api gatway

Source:	Mobile Application
Protocol:	https
Encrypted:	true
Authentication:	token
Authorization:	none
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Received:	Customer Contracts, Customer Informations
Data Sent:	Customer Contracts, Customer Informations

Public Internet Link (incoming)
Internet Link

Source:	Web Browser

Protocol:	https
Encrypted:	true
Authentication:	session-id
Authorization:	none
Read-Only:	false
Usage:	business
Tags:	none
VPN:	false
IP-Filtered:	false
Data Received:	Customer Contracts, Customer Informations
Data Sent:	Customer Contracts, Customer Informations

Identified Data Breach Probabilities by Data Asset

In total **60 potential risks** have been identified during the threat modeling process of which **1 are rated as critical**, **0 as high**, **14 as elevated**, **17 as medium**, and **28 as low**.

These risks are distributed across **2 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.

Customer Contracts: 23 / 23 Risks

customer contract (PDF)

ID:	innovera-customer-contracts	
Usage:	business	
Quantity:	many	
Tags:	none	
Origin:	Some Origin	
Owner:	Innovera Contract Manager	
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:	contartc data contain customers information	
Processed by:	API Gatway Service, Mobile Application, Web Browser	
Stored by:	none	
Sent via:	Public Internet Traffic, Public Internet Link, Local Network Area, Internet Public Traffic	
Received via:	Public Internet Traffic, Public Internet Link, Local Network Area, Internet Public Traffic	
Data Breach:	**probable**	
Data Breach Risks:	This data asset has data breach potential because of 23 remaining risks:	

Probable: missing-cloud-hardening@Innovera-Private-Cloud

Probable: missing-cloud-hardening@Internet-Boundry

Probable: missing-file-validation@innovera-api-gatway-service

Probable: Innovera-Service-Disater@innovera-api-gatway-service

Probable: untrusted-deserialization@innovera-api-gatway-service

Probable: untrusted-deserialization@innovera-mobile-application

Probable: untrusted-deserialization@Web-browser

Probable: xml-external-entity@Web-browser

Possible: missing-authentication-second-factor@Innovera-WAF>linke-to-api-gateway@Innovera-WAF@innovera-api-gatway-service

Possible: missing-authentication-second-factor@Innovera-WAF>linke-to-api-gateway@Innovera-WAF@innovera-api-gatway-service

Possible: server-side-request-forgery@innovera-api-gatway-service@Innovera-Database-Server@innovera-api-gatway-service>public-internet-traffic

Possible: server-side-request-forgery@Innovera-Application-Service@innovera-api-gatway-service@Innovera-Application-Service>local-network-area

Possible: server-side-request-forgery@Innovera-WAF@innovera-api-gatway-service@Innovera-WAF>linke-to-api-gateway

Possible: server-side-request-forgery@Innovera-WAF@Innovera-Web-Server-Nginx@Innovera-WAF>link-to-nginx

Possible: unguarded-access-from-internet@innovera-api-gatway-service@Innovera-Application-Service@Innovera-Application-Service>local-network-area

Possible: unguarded-access-from-internet@innovera-api-gatway-service@Innovera-WAF@Innovera-WAF>linke-to-api-gateway

Improbable: missing-identity-propagation@Innovera-WAF>linke-to-api-gateway@Innovera-WAF@innovera-api-gatway-service

Improbable: missing-identity-propagation@Innovera-Application-Service>local-network-area@Innovera-Application-Service@innovera-api-gatway-service

Improbable: missing-hardening@innovera-api-gatway-service

Improbable: missing-hardening@innovera-mobile-application

Improbable: missing-hardening@Web-browser

Improbable: missing-network-segmentation@innovera-api-gatway-service

Improbable: missing-network-segmentation@innovera-mobile-application

Customer Informations: 23 / 23 Risks

customer information

ID:	innovera-customer-information	
Usage:	business	
Quantity:	many	
Tags:	none	
Origin:		
Owner:	Innovera CRM team	
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:		
Processed by:	API Gatway Service, Mobile Application, Web Browser	
Stored by:	none	
Sent via:	Public Internet Traffic, Public Internet Link, Local Network Area, Internet Public Traffic	
Received via:	Public Internet Traffic, Public Internet Link, Local Network Area, Internet Public Traffic	
Data Breach:	**probable**	
Data Breach Risks:	This data asset has data breach potential because of 23 remaining risks:	

Probable: missing-cloud-hardening@Innovera-Private-Cloud

Probable: missing-cloud-hardening@Internet-Boundry

Probable: missing-file-validation@innovera-api-gatway-service

Probable: Innovera-Service-Disater@innovera-api-gatway-service

Probable: untrusted-deserialization@innovera-api-gatway-service

Probable: untrusted-deserialization@innovera-mobile-application

Probable: untrusted-deserialization@Web-browser

Probable: xml-external-entity@Web-browser

Possible: missing-authentication-second-factor@Innovera-WAF>linke-to-api-gateway@Innovera-WAF@innovera-api-gatway-service

Possible: missing-authentication-second-factor@Innovera-WAF>linke-to-api-gateway@Innovera-WAF@innovera-api-gatway-service

Possible: server-side-request-forgery@innovera-api-gatway-service@Innovera-Database-Server@innovera-api-gatway-service>public-internet-traffic

Possible: server-side-request-forgery@Innovera-Application-Service@innovera-api-gatway-service@Innovera-Application-Service>local-network-area

Possible: server-side-request-forgery@Innovera-WAF@innovera-api-gatway-service@Innovera-WAF>linke-to-api-gateway

Possible: server-side-request-forgery@Innovera-WAF@Innovera-Web-Server-Nginx@Innovera-WAF>link-to-nginx

Possible: unguarded-access-from-internet@innovera-api-gatway-service@Innovera-Application-Service@Innovera-Application-Service>local-network-area

Possible: unguarded-access-from-internet@innovera-api-gatway-service@Innovera-WAF@Innovera-WAF>linke-to-api-gateway

Improbable: missing-identity-propagation@Innovera-WAF>linke-to-api-gateway@Innovera-WAF@innovera-api-gatway-service

Improbable: missing-identity-propagation@Innovera-Application-Service>local-network-area@Innovera-Application-Service@innovera-api-gatway-service

Improbable: missing-hardening@innovera-api-gatway-service

Improbable: missing-hardening@innovera-mobile-application

Improbable: missing-hardening@Web-browser

Improbable: missing-network-segmentation@innovera-api-gatway-service

Improbable: missing-network-segmentation@innovera-mobile-application

Trust Boundaries

In total **4 trust boundaries** have been modeled during the threat modeling process.

DMZ Boundary
Internet network

ID:	public-internet
Type:	execution-environment
Tags:	none
Assets inside:	Application Service, Web Application Firewall, Nginx Web Server, API Gatway Service
Boundaries nested:	none

Innovera Private Cloud
Innovera Private Cloud

ID:	Innovera-Private-Cloud
Type:	network-cloud-provider
Tags:	none
Assets inside:	none
Boundaries nested:	Private Lan, DMZ Boundary

Internet Boundry
Intrnet Link

ID:	Internet-Boundry
Type:	network-cloud-provider
Tags:	none
Assets inside:	Web Browser, Mobile Application
Boundaries nested:	none

Private Lan
innovera private network

ID:	private-network

Type: network-virtual-lan
Tags: none
Assets inside: DataBase Server
Boundaries nested: none

Shared Runtimes

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

WebApp and REST API Virtualization
WebApp ans REST API Virtualization

ID:	Webapp-ResetApi-Virtualization
Tags:	vmware
Assets running:	API Gatway Service

Risk Rules Checked by Threagile

Threagile Version: 1.0.0
Threagile Build Timestamp: 20211121124511
Threagile Execution Timestamp: 20220314141348
Model Filename: /dev/shm/threagile-input-1021253137/threagile-sample/threagile.yaml
Model Hash (SHA256): d72f287f2c4f93bc5ff5bc701a833f6453394dfd17b241485b9d20e4547ac9bd

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:

Service Disaster
Innovera-Service-Disater

Individual Risk Category

STRIDE: Denial of Service
Description: Service disater in the case of force module incident
Detection: by pinging service
Rating: identifed by Innovera red team during local benchmark

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

Khalegh Salehi Aghdam 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. Khalegh Salehi Aghdam 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 Khalegh Salehi Aghdam 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.