

IT BANK - ITA DAILYBANKING API

Dynamic Pentest Report

CISO/ASM/CYBER OFFSEC COE

A. Document Information

<i>Responsible department</i>	CISO/ASM/CYBER OFFSEC COE
<i>Report owner</i>	Pompa, A. (Andrea) (LX03ND)
<i>Pentesters</i>	Pompa, A. (Andrea) (andrea.pompa.ext@ing.com) (LX03ND)
<i>External party</i>	SECURITY REPLY
<i>Last update date</i>	27.10.2025
<i>Version</i>	1.3
<i>Version status</i>	Draft

1. Version History

Version	Date	Author	Status	Note
0.1	05.09.2025	Pompa, A. (Andrea) (andrea.pompa.ext@ing.com)	Statement of Work	—
0.2	08.09.2025	Pompa, A. (Andrea) (andrea.pompa.ext@ing.com)	Statement of Work	—
1.0	22.09.2025	Pompa, A. (Andrea) (andrea.pompa.ext@ing.com)	Draft	—
1.1	22.09.2025	Forte, V. (Valentina) (valentina.forte.ext@ing.com)	QA	—
1.2	26.09.2025	Forte, V. (Valentina) (valentina.forte.ext@ing.com)	Draft	Integration of missing APIs to BuBA PT scope
1.3	27.10.2025	Forte, V. (Valentina) (valentina.forte.ext@ing.com)	QA	—

B. Table of Contents

A. Document Information	2
1. Version History	2
B. Table of Contents	3
C. Executive Summary	4
1. Overview	4
2. Dynamic Pentest Scope	5
3. Customer Contact Information	12
4. Vulnerabilities chart	13
5. Report Status	13
6. Disclosed Vulnerabilities for legacy findings	13
7. Disclosed Vulnerabilities	14
D. Introduction	15
1. Terminology	15
2. Dynamic Scanning (DAST) Approach	15
3. Vulnerabilities and Report Classification	16
E. Testing Methodology	20
1. Description	20
2. Generic Testing Approach	21
3. API Testing	21
4. Test Phases	26
F. Findings, Recommendations and Retests	27
1. Critical Risk Vulnerabilities	27
2. High Risk Vulnerabilities	28
3. Medium Risk Vulnerabilities	29
4. Low Risk Vulnerabilities	30
4.1. Improper input validation (30612)	30
4.2. Verbose Error Messages (23703)	35
5. Informational Findings	41
5.1. Missing HTTP Strict-Transport-Security Header (23704)	41
5.2. Missing HTTP X-Content-Type-Options Header (29537)	43
5.3. Missing HTTP Content-Security-Policy Header (29538)	45
G. Appendixes	47
1. Testing Limitation - Missing Data	47
2. Rules of Engagement	50
3. Original request	51

C. Executive Summary

1. Overview

This document is a result of Dynamic Pentest process, which is required by CIRM Monitoring Minimum Standard. Dynamic Pentest process is a part of Secure Code Review approach, which contain following elements:

- Source Code Review
- Dynamic Scan (DAST)
- Penetration Testing

Dynamic Pentest is joined exercise of consecutive Dynamic Scan along with Penetration Test.

A goal of Dynamic Scan (DAST) process is to detect and analyze any security vulnerability, misconfiguration or design flaw in web application by using of semi-automated tooling.

Offensive Cyber Security team was tasked to perform Dynamic Pentest against IT BANK - ITA DAILYBANKING API. The security assessment was conducted remotely over the period 02.09.2025 - 08.09.2025.

During the assessment following risks were identified:

- Critical: 0
- High: 0
- Medium: 0
- Low: 1
- Informational: 2

Following risks were identified during previous assesments:

- Critical: 0
- High: 0
- Medium: 0
- Low: 1
- Informational: 1

Vulnerabilities summary chart provides qualitative, graphical representation of the risk profile of the targets mentioned in scope section.

As part of due care related to Strict Change Regime announced by MT CTO, starting from 14 September 2023 for every pentest we are introducing change to pentest methodology. Dynamic Scanning (DAST), enumeration, active fingerprinting, and scripts usage is discouraged. Where necessary, use of throttling is required. All methodology steps that may affect LDAP and DBaaS performance must be performed with caution. In such case throttling must be applied.

This pentest was conducted by SECURITY REPLY, an independent external party. Third party penetration tester(s) have freedom in tooling selection as well as in approach, as long as it is aligned with industry and ING Technical Standard on Security Validation and Testing.

During the assessment, it was not possible to perform security testing on the several APIs due to the absence of data required for execution, as detailed in Appendix section. As agreed with ING CISO team, these APIs will be included in the next round of Penetration Testing on ITA Web Secure Site – WebPortal.

2. Dynamic Pentest Scope

Asset	Date	Details	CIA Rating		
			C	I	A
IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	<p>Target:</p> <ul style="list-style-type: none"> • https://localhost:1234/v2/debit-card/request/start-flow • https://localhost:1234/v2/debit-card/request/end-flow • https://localhost:1234/v1/debit-card/suspension • https://localhost:1234/v1/debit-card/suspension/approved • https://localhost:1234/v1/debit-card/restricted-detail • https://localhost:1234/v1/debit-card/restricted-detail/approved • https://localhost:1234/v1/debit-card/replacement/end-flow • https://localhost:1234/v1/debit-card/reactivation • https://localhost:1234/v1/debit-card/reactivation/approved • https://localhost:1234/v1/debit-card/pin-pad/create • https://localhost:1234/v1/debit-card/mastercard/3ds • https://localhost:1234/v1/debit-card/mastercard/3ds/approved • https://localhost:1234/v1/debit-card/limits/manage • https://localhost:1234/v1/debit-card/limits/approved • https://localhost:1234/v1/debit-card/geo-blocking/area/validation • https://localhost:1234/v1/debit-card/geo-blocking/area/enable • https://localhost:1234/v1/debit-card/geo-blocking/area/enable/approved <p>Methodology: GRAYBOX Facing: INTERNAL</p>	3	4	4

IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	<p>Target:</p> <ul style="list-style-type: none"> • https://localhost:1234/v1/debit-card/geo-blocking/area/disable • https://localhost:1234/v1/debit-card/geo-blocking/area/disable/approved • https://localhost:1234/v1/debit-card/change-pin • https://localhost:1234/v1/debit-card/change-pin/approved • https://localhost:1234/v1/debit-card/activation/end-flow • https://localhost:1234/v1/debit-card/tech-services/health/check • https://localhost:1234/v1/debit-card/restricted-detail/status-data • https://localhost:1234/v1/debit-card/request/{UUID} • https://localhost:1234/v1/debit-card/replacement/start-flow • https://localhost:1234/v1/debit-card/overview • https://localhost:1234/v1/debit-card/mastercard/3ds/info • https://localhost:1234/v1/debit-card/limits • https://localhost:1234/v1/debit-card/geo-blocking • https://localhost:1234/v1/debit-card/geo-blocking/pricing/info • https://localhost:1234/v1/debit-card/details • https://localhost:1234/v1/debit-card/assisted/{productUUID}/details • https://localhost:1234/v1/debit-card/activation/start-flow <p>Methodology: GRAYBOX Facing: INTERNAL</p>	3	4	4

IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	<p>Target:</p> <ul style="list-style-type: none"> • https://localhost:1234/v1/debit-card/action/{UUID}/status <p>Methodology: GRAYBOX Facing: INTERNAL</p>	3	4	4
IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	<p>Target:</p> <ul style="list-style-type: none"> • https://sd80tsssad12:8095/v1/oracle-card/req_request/insert • https://sd80tsssad12:8095/v1/oracle-card/mobile_tvn • https://sd80tsssad12:8095/v1/oracle-card/mobile_token • https://sd80tsssad12:8095/v1/oracle-card/mobile_tcn • https://sd80tsssad12:8095/v1/oracle-card/contract/insert • https://sd80tsssad12:8095/v1/oracle-card/ba_cards_property/update_property_value • https://sd80tsssad12:8095/v1/oracle-card/ba_cards/prepaid/recharge/insert • https://sd80tsssad12:8095/v1/oracle-card/ba_cards/lookup • https://sd80tsssad12:8095/v1/oracle-card/ba_cards/insert • https://sd80tsssad12:8095/v1/oracle-card/req_request/update • https://sd80tsssad12:8095/v1/oracle-card/products/{productId}/update • https://sd80tsssad12:8095/v1/oracle-card/mobile_token/{correlationId} • https://sd80tsssad12:8095/v1/oracle-card/coownership • https://sd80tsssad12:8095/v1/oracle-card/cdc_installment_plans_name • https://sd80tsssad12:8095/v1/oracle-card/ba_cards_services/{cardId} • https://sd80tsssad12:8095/v1/oracle-card/ba_cards/{cardId}/update • https://sd80tsssad12:8095/v1/oracle-card/scoring <p>Methodology: GRAYBOX Facing: INTERNAL</p>	3	4	4

IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	<p>Target:</p> <ul style="list-style-type: none"> • https://sd80tssad12:8095/v1/oracle-card/scoring/{scoringId} • https://sd80tssad12:8095/v1/oracle-card/req_request • https://sd80tssad12:8095/v1/oracle-card/req_request/{requestId}/req_item_kits • https://sd80tssad12:8095/v1/oracle-card/req_request/{requestId}/req_item_cards • https://sd80tssad12:8095/v1/oracle-card/mobile_tar • https://sd80tssad12:8095/v1/oracle-card/health/check • https://sd80tssad12:8095/v1/oracle-card/cdc_installment_plans • https://sd80tssad12:8095/v1/oracle-card/ba_overdraft_blocks • https://sd80tssad12:8095/v1/oracle-card/ba_cards_property/{cardId} • https://sd80tssad12:8095/v1/oracle-card/ba_cards • https://sd80tssad12:8095/v1/oracle-card/ba_cards/{productId}/read • https://sd80tssad12:8095/v1/oracle-card/ba_cards/{personId}/search • https://sd80tssad12:8095/v1/oracle-card/ba_cards/prepaid/recharge/{cardId} <p>Methodology: GRAYBOX Facing: INTERNAL</p>	3	4	4

IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	<p>Target:</p> <ul style="list-style-type: none"> • https://localhost:1234/v1/current-account/solution-selling/onboarding/{onboardingUUID}/{action}/init • https://localhost:1234/v1/current-account/solution-selling/onboarding/tracking-code • https://localhost:1234/v1/current-account/solution-selling/onboarding/digital-signature • https://localhost:1234/v1/current-account/solution-selling/onboarding/commercial-offer/save • https://localhost:1234/v1/current-account/solution-selling/account-portability/digital-signature • https://localhost:1234/v1/current-account/solution-selling/techServices/healthCheck • https://localhost:1234/v1/current-account/solution-selling/onboarding/{onboardingUUID}/{action}/status • https://localhost:1234/v1/current-account/solution-selling/onboarding/context • https://localhost:1234/v1/current-account/solution-selling/onboarding/commercial-offer/cca • https://localhost:1234/v1/current-account/solution-selling/account-portability/static-offers • https://localhost:1234/v1/current-account/solution-selling/account-portability/documents • https://localhost:1234/v1/current-account/solution-selling/account-portability/contract-template <p>Methodology: GRAYBOX Facing: INTERNAL</p>	3	4	4

IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	<p>Target:</p> <ul style="list-style-type: none"> • https://localhost:1234/v1/current-account/solution-selling/account-portability/check-supplementary-products • https://localhost:1234/v1/current-account/solution-selling/account-portability/active-customers • https://localhost:1234/v1/current-account/solution-selling/onboarding/{onboardingUUID} <p>Methodology: GRAYBOX Facing: INTERNAL</p>	3	4	4	
IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	<p>Target:</p> <ul style="list-style-type: none"> • /v1/riba-admin/tech-services/health/check <p>Methodology: GRAYBOX Facing: INTERNAL</p>	3	4	4	
IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	<p>Target:</p> <ul style="list-style-type: none"> • /v1/riba-admin/passive/archive • /v1/riba-admin/passive/payment/document • /v1/riba-admin/passive/to-pay • /v1/riba-admin/riba/action • /v1/riba-admin/tech-services/health/check • /v1/riba-admin/passive/cancel/confirm • /v1/riba-admin/passive/cancel • /v1/riba-admin/passive/pay/confirm • /v1/riba-admin/passive/pay • /v1/riba-admin/passive/reject/confirm • /v1/riba-admin/passive/reject • /v1/riba-admin/passive/to-pay/export <p>Methodology: GRAYBOX Facing: INTERNAL</p>	3	4	4	

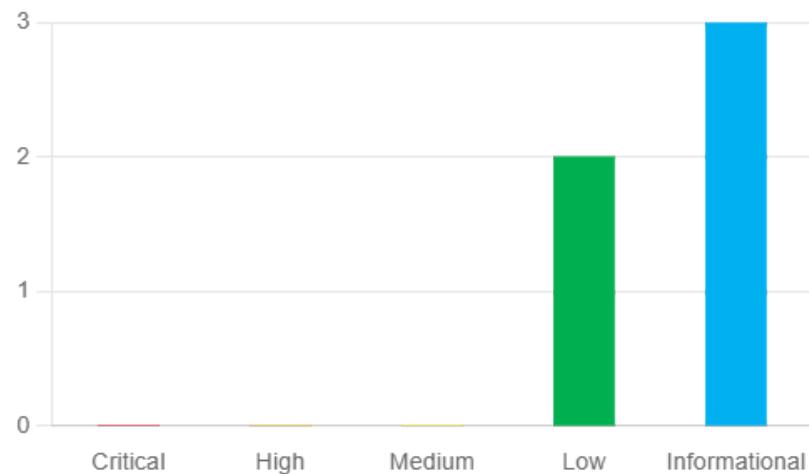
IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	<p>Target:</p> <ul style="list-style-type: none"> • /adapter05/card/phonenumber/{party-uuid} • /adapter05/card/{digitizedCardId} • /adapter05/tech-services/health/check • /adapter05/tech-services/keepalive • /v2/adapter05/card/list • /adapter05/card/details • /adapter05/card/digitizable • /adapter05/card/notify • /adapter05/card/partyinfo <p>Methodology: GRAYBOX Facing: INTERNAL</p>	3	4	4	
IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	<p>Target:</p> <ul style="list-style-type: none"> • /adapter06/card/phonenumber/{party-uuid} • /v1/ita-wallet-debit-card-api/tech-services/health/check/keepalive • /v1/ita-wallet-debit-card-api/tech-services/health/check • /v2/adapter06/card/list • /adapter06/card/details • /adapter06/card/digitizable • /adapter06/card/notify • /adapter06/card/partyinfo <p>Methodology: GRAYBOX Facing: INTERNAL</p>	3	4	4	
IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	<p>Target:</p> <ul style="list-style-type: none"> • /v1/domestic-payments/technical-services/health/check <p>Methodology: GRAYBOX Facing: INTERNAL</p>	3	4	4	

IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	<p>Target:</p> <ul style="list-style-type: none"> • /v1/payments/delete/giro/{paymentId} • /v1/payments/delete/sepa • /v1/payments/delete/operations • /v1/internal/payments/{accountNumber}/receipt • /v1/internal/payments/order-preview • /v1/payments/iban/validation <p>Methodology: GRAYBOX Facing: INTERNAL</p>	3	4	4
IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	<p>Target:</p> <ul style="list-style-type: none"> • /v1/current-accounts/portability/accounts • /v1/current-accounts/{globalProductId}/portability/document • /v1/current-accounts/{globalProductId}/portability/digital-signature • /v1/current-accounts/{globalProductId}/portability (PATCH) • /v1/current-accounts/{globalProductId}/portability (POST) • /v1/current-accounts/{globalProductId}/portability (PUT) • /v1/current-accounts/{globalProductId}/portability (GET) <p>Methodology: GRAYBOX Facing: INTERNAL</p>	3	4	4

3. Customer Contact Information

Name	Role	Asset	Contact information
Neuner, M. (Matthias)	Asset Owner	IT BANK - ITA DAILYBANKING API	Matthias.Neuner@ing.com
Esposito, G. (Gaetano)	IT Custodian	IT BANK - ITA DAILYBANKING API	Gaetano.Esposito@ing.com
Jazaj, E. (Edvin)	Security Officer	IT BANK - ITA DAILYBANKING API	edvin.jazaj@ing.com
Cascella, S. (Stefano)	SPOC	IT BANK - ITA DAILYBANKING API	stefano.cascella@ing.com
Giuseffi, T. (Teresa)	SPOC	IT BANK - ITA DAILYBANKING API	teresa.giuseffi@ing.com

4. Vulnerabilities chart



5. Report Status

Report date	Status
08.09.2025	GREEN

6. Disclosed Vulnerabilities for legacy findings

The findings below are leftovers from previous tests and were automatically pulled for the current test.

Ref	Severity	Assets	Vulnerability	Description	Recommendation	Status
F 4.1 Offsec: 23703	LOW 3.1	/adapter06/car d/details; /adapter05/car d/details; /v1/payments/ delete/sepa... and 1 more assets See full list is in section F.	Verbose Error Messages	Server/Application verbose errors often with stack traces are being presented to end users. Those might reveal sensitive data, application structure and parts of the code.	Verbose errors should not be provided to end users. Friendly static error pages should be provided instead. Error cause should be investigated within the code.	New

F 5.1 Offsec: 23704	INFO	https://localhos t:1234/v1/; https://sd80tsss ad12:8095/v1/	Missing HTTP Strict- Transport- Security Header	HTTP Strict- Transport- Security header was not found in HTTP responses.	Include HTTP Strict-Transport- Security-Header into each server's HTTP response.	Not To Be Fixed
---------------------------	------	--	---	---	---	-----------------

7. Disclosed Vulnerabilities

Ref	Severity	Assets	Vulnerability	Description	Recommendati on	Status
F 4.1 Offsec: 30612	LOW 3.7	/adapter05/car d/phonenumbe r/{party-uuid}; /adapter06/car d/phonenumbe r/{party-uuid}; /v1/payments/i ban/validation	Improper input validation	Input validation is a frequently- used technique for checking potentially dangerous inputs in order to ensure that the inputs are safe for processing within the code, or when communicating with other components.	There are multiple approaches to input validation. However, an effective way is to ensure that you know what data you want, and to reject all other forms of data.	New
F 5.1 Offsec: 29537	INFO 0.0	https://localhos t:1234/v1/; https://sd80tsss ad12:8095/v1/	Missing HTTP X- Content-Type- Options Header	HTTP X-Content- Type-Options header was not found in HTTP responses.	Include HTTP X- Content-Type- Options Header into each server's HTTP response.	Not To Be Fixed
F 5.2 Offsec: 29538	INFO 0.0	https://localhos t:1234/v1/*; https://sd80tsss ad12:8095/v1/*	Missing HTTP Content- Security-Policy Header	HTTP Content- Security-Policy header was not found in HTTP responses.	Include HTTP Content- Security-Policy Header into each server's HTTP response.	Not To Be Fixed

D. Introduction

1. Terminology

The goal of this document is to describe the results of Dynamic Pentest.

Concept	Description
Dynamic Scan (DAST)	Method of evaluating asset security by simulating a semi-automated attack
Vulnerability	A weakness which allows an attacker to reduce a system's information assurance
Severity / Classification	A severity level indicates the security risk posed by exploitation of the vulnerability and its degree of difficulty
Risk	Risk is defined as the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.
Likelihood	Likelihood is defined as the probability of a given threat exploiting vulnerability. This incorporates ease of exploitation and determination and capability of the given threat agent.
Impact	Possible impact of an occurrence of a risk

2. Dynamic Scanning (DAST) Approach

Based on industry standards (OWASP/OSSTMM/ISSAF) and best practices, Offensive Cyber Security team developed its own methodology of conducting Dynamic Scan (DAST) activities. This methodology is based on GrayBox or WhiteBox approach.

GrayBox approach is used when some additional information is provided by customer including unprivileged account access to application or asset, information about system types, service versions, network devices details, databases, network segments and so forth. Typically, the goal of methodology, is to simulate possible internal threats like malicious/fraudulent user actions or Advanced Persistent Threats (APT) activities. This also includes privilege escalation as well as further exploration of affected environment.

WhiteBox Methodology (a.k.a CrystalBox) refers to full review of system with all possible information delivered by customer. In case of applications - it's possible to perform Static Code Review, if application source code is available to customer and/or pentester.

All findings discovered by scanner are manually reviewed.

3. Vulnerabilities and Report Classification

Classification methodology is based on Common Vulnerability Scoring System. CVSS consists of three metric groups: Base, Temporal, and Environmental.

The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments, the Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment.

The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

Following factors describe Base metrics group:

- Exploitability metrics reflect the ease and technical means by which the vulnerability can be exploited. That is, they represent characteristics of the thing that is vulnerable, which we refer to formally as the vulnerable component. Attack Vector (AV). This metric value (and consequently the Base Score) will be larger the more remote (logically, and physically) an attacker can be in order to exploit the vulnerable component. Values: Network (N), Adjacent (A), Local (L), Physical (P).
 - Attack Complexity (AC). The Base Score is greatest for the least complex attacks. If a successful attack requires either knowledge about the environment (such as configuration settings, sequence numbers, or shared secrets), modification of the environment to improve exploit reliability, or usage of a man in the middle attack, then the complexity is High. Values: Low (L), High (H).
 - Attack Vector (AV). This metric value (and consequently the Base Score) will be larger the more remote (logically, and physically) an attacker can be in order to exploit the vulnerable component. Values: Network (N), Adjacent (A), Local (L), Physical (P).
 - Privileges Required (PR). This metric describes the level of an attacker must possess before successfully exploiting the vulnerability. The Base Score is greatest if no privileges are required. Low value is set when basic user capabilities are needed, high - if significant role (e.g. administrative) is required. Values: None (N), Low (L), High (H).
 - User Interaction (UI). This metric captures the requirement for a human user, other than the attacker, to participate in the successful compromise of the vulnerable component. This metric determines whether the vulnerability can be exploited solely at the will of the attacker, or whether a separate user (or user initiated process) must participate in some manner. Values: None (N), Required (R).
- Scope metric captures whether a vulnerability in one vulnerable component impacts resources in components beyond its security scope. The scope metric is set to Changed if an exploited vulnerability can affect resources beyond the security scope managed by the security authority of the vulnerable component. Values: Unchanged (U), Changed (C).
- Impact metrics reflect the direct consequence of a successful exploit, and represent the consequence to the thing that suffers the impact, which we refer to formally as the impacted component.
 - Confidentiality (C). This metric measures the impact to the confidentiality of the information resources managed by a software component due to a successfully exploited vulnerability. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized ones. The Base Score is greatest when the loss to the impacted component is highest. Values: None (N), Low(L), High (H).
 - Integrity (I). This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of information. The Base Score is greatest when the consequence to the impacted component is highest. Values: None (N), Low (L), High (H).

- Availability (A). This metric measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability. While the Confidentiality and Integrity impact metrics apply to the loss of confidentiality or integrity of data (e.g., information, files) used by the impacted component, this metric refers to the loss of availability of the impacted component itself, such as a networked service (e.g., web, database, email). Since availability refers to the accessibility of information resources, attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of an impacted component. The Base Score is greatest when the consequence to the impacted component is highest. Values: None (N), Low (L), High (H).

Following factors describe the optional Temporal metrics group:

- Exploit Code Maturity (E). This metric measures the likelihood of the vulnerability being attacked, and is typically based on the current state of exploit techniques, exploit code availability, or active, "in-the-wild" exploitation. Public availability of easy-to-use exploit code increases the number of potential attackers by including those who are unskilled, thereby increasing the severity of the vulnerability. Initially, real-world exploitation may only be theoretical. Publication of proof-of-concept code, functional exploit code, or sufficient technical details necessary to exploit the vulnerability may follow. Furthermore, the exploit code available may progress from a proof-of-concept demonstration to exploit code that is successful in exploiting the vulnerability consistently. In severe cases, it may be delivered as the payload of a network-based worm or virus or other automated attack tools. Values: Not Defined (X), High (H), Functional (F), Proof-of-Concept (P), Unproven (U).
- Remediation Level (RL). The typical vulnerability is unpatched when initially published. Workarounds or hotfixes may offer interim remediation until an official patch or upgrade is issued. Each of these respective stages adjusts the Temporal Score downwards, reflecting the decreasing urgency as remediation becomes final. The less official and permanent a fix, the higher the vulnerability score. Values: Not Defined (X), Unavailable (U), Workaround (W), Temporary Fix (T), Official Fix (O).
- Report Confidence (RC). This metric measures the degree of confidence in the existence of the vulnerability and the credibility of the known technical details. Sometimes only the existence of vulnerabilities is publicized, but without specific details. For example, an impact may be recognized as undesirable, but the root cause may not be known. The vulnerability may later be corroborated by research which suggests where the vulnerability may lie, though the research may not be certain. Finally, a vulnerability may be confirmed through acknowledgment by the author or vendor of the affected technology. The urgency of a vulnerability is higher when a vulnerability is known to exist with certainty. Values: Not Defined (X), Confirmed (C), Reasonable (R), Unknown (U).

Environmental metrics group reflects the CIA triad of the asset in the following fashion:

- Score set to 1 and 2 of [Confidentiality (CR) | Integrity (IR) | Availability (AR)] is likely to have only a limited adverse effect on the organization or individuals associated with the organization (e.g., employees, customers). Therefore the value is set to Low (L), which lowers the base score.
- Score set to 3 of [Confidentiality (CR) | Integrity (IR) | Availability (AR)] is likely to have a serious adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).Therefore the value is set to Medium (M), which does not affect the base score.
- Score set to 4 of [Confidentiality (CR) | Integrity (IR) | Availability (AR)] is likely to have a catastrophic adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).Therefore the value is set to High (H), which raises the base score.

The following table is taken from Global Security Incident Management (Memo titled "New vulnerability classification and remediation timelines" from 21/12/2022). If it is not possible to address given finding within recommended closure date, a remediation action plan should be prepared to that date.

Classification	Description	Time to fix online flag is true	Time to fix online flag is false	CVSS Score
INFO	Informational only	Not required	Not required	0.0
LOW	A low risk vulnerability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	12 weeks	16 weeks	0.1 - 3.9
MEDIUM	Medium risk vulnerability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	8 weeks	12 weeks	4.0 - 6.9
HIGH	High risk vulnerability could be expected to have a severe adverse effect on organizational operations, organizational assets, or individuals.	2 weeks	6 weeks	7.0 - 8.9
CRITICAL	Critical risk vulnerability could be expected to have catastrophic adverse effect on organizational operations, organizational assets, or individuals.	24 hours	2 weeks	9.0 - 10.0

Real severe critical vulnerabilities on offline assets can be promoted to immediate remediation (P1 threat).

Asset classification is described in CORM Foundation Minimum Standard and has following criteria:

Asset Criticality	Criteria
Critical	One or more of either C, I or A have been assessed at level 4.
High	One or more of either C, I or A have been assessed at level 3.
Medium	One or more of either C, I or A have been assessed at level 2.
Low	Other assets that do not fall into the above categories.

According to this information, our best practices and experience allow to assess a criticality of vulnerabilities, this approach is described in process description. If asset has findings classified as below, report should have Red Status, which means that findings should be solved before going to production environment.

General findings criticalities: There are thresholds to decline portals from going past the tollgate. A zero-tolerance approach to SQL injection and Cross-Site Scripting. In addition the following approach should be used:

Business criticality	Application type	Flaw severities not allowed
Critical	External	critical, high
	Internal	critical, high
High	External	critical, high
	Internal	critical, high
Medium	External	critical, high
	Internal	critical, high
Low	External	critical, high
	Internal	critical

Report statuses

Report status	Description
Red	Vulnerabilities in application should be solved before go to the production.
Green	The application can go to the production.

E. Testing Methodology

1. Description

Methodologies vary depending on goals, scope and specific requirements set by the Customer. Offensive Cyber Security team adopted the best industry standards of testing like OWASP and worked out own techniques and methodologies based on own experiences from other penetration testing services delivered already to other ING Business Units.

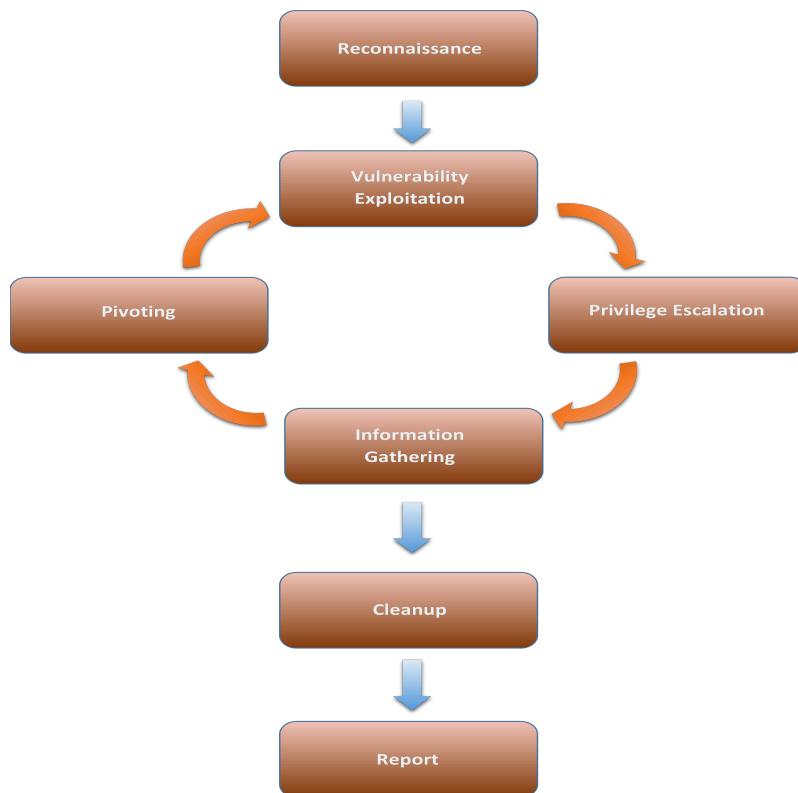
Offensive Cyber Security team uses the following main methodologies depending on the requirements:

- **BlackBox** having the following characteristics
 - Offensive Cyber Security team does not possess any initial knowledge about tested environment,
 - Usually the customer delivers IP address pools, URL or domain addresses as a starting point for the test,
 - The Offensive Cyber Security team emulates typical attacker's actions who do not know the environment (operating systems, network services and applications operating, network topology etc.)
 - Black Box testing is the most common methodology for the tests of external facing systems and applications (like DMZ network and internet applications,
 - One of the key factors in this methodology is gathering of any available information about tested environment. The Offensive Cyber Security team is using passive techniques such as:
 - passive intelligence gathering, collecting an information about an application, used technologies and frameworks and/or APIs,
 - active environment analysis: DNS enumeration, network scanning, port/service probing, port scanning, application scanning, OS fingerprinting, or website spidering.
 - Offensive Cyber Security team can use socio-technical attacks if the Customer approves.
 - Next stage of the test is identification and analysis of possible vector attacks against tested system or application if enough information is already available. The Offensive Cyber Security team uses fuzzing, analysis or requests and responses to/from tested system, and performs manual testing.
 - Offensive Cyber Security team verifies detected vulnerabilities to eliminate false positives,
 - Offensive Cyber Security team can attempt to exploit vulnerabilities, elevate privileges and attack other part of tested system if Customer approves and contractual provisions allow.
 - The last part is reporting consisting of detailed report and presentation prepared for the target audience (management, business owners or technicians).
- **WhiteBox (CrystalBox)** having the following characteristics:
 - The customer delivers detailed information about tested system, usually as documentation or interview with employees having a required knowledge (developers, system/application administrators or IT architects)
 - The test emulates possible actions performed by an attacker having deep knowledge about target (i.e. Advanced Persistent Threat, attacks perpetrated by current or former employees/contractors),
 - Reconnaissance and intelligence gathering is reduced comparing to Black Box or Gray Box methodologies,
 - False positives could be confirmed after review of a part of the source code (when source code is available for the Offensive Cyber Security team)
 - Other phases of the testing are common in Black Box and White box (main difference is the amount of knowledge about tested system)
- **GrayBox** having the following characteristics:

- This is a concatenation of WhiteBox and BlackBox
- The Offensive Cyber Security team is provided with basic authorization in tested system (the goal is to test internals of the system and elevate the privileges if possible),
- The testers can be provided with additional information about tested environment (high level design, services, protocols etc.)
- This methodology is the most common for the emulation of attacks against systems where non-privileged credentials or limited knowledge are available for an attacker,
- Usually this method is being used in order to assess a security and effectiveness of controls of third-party applications,
- This methodology provides additional advantage which is providing information about findings to a vendor. Such sort of cooperation enables to performing additional verification of findings and publishing security patches for the tested system (better than alternative workaround solutions mitigating existing risks).

2. Generic Testing Approach

The generic approach utilizes cyclic activities following Deming's Plan-Do-Check-Act schema and is common for all methodologies regardless of level of knowledge (Black/Gray/ Whitebox) and type of tested asset (Web/Infra/Mobile/ThickClient).



3. API Testing

This methodology is focused on testing API services which should disclose any potential misconfigurations and vulnerabilities.

- Scoping

- Gathering of requirements, scope and additional information from the customer before test start
- Information Gathering
 - Conduct Search Engine Discovery and Reconnaissance for Information Leakage
 - Fingerprint Web
 - Review Webserver Metafiles for Information Leakage
 - Enumerate Applications on Webserver
 - Review Webpage Comments and Metadata for Information Leakage
 - Identify application entry points
 - Enumerate and map all the documented and potentially hidden API endpoints
 - Identify publicly available API (SwaggerUI, OpenAPI etc.)
 - Fingerprint Web Application Framework
 - Fingerprint Web Application
 - Map Network and Application Architecture
- Additional API Reconnaissance
 - API architecture discovery (REST, GraphQL, SOAP etc.)
 - API version discovery
 - API version discovery
 - API documentations discovery
 - HTTP methods discovery
 - Endpoints gathering through local documents (e.g. WADL / WSDL)
 - API endpoints fuzzing and discovery
 - API actions fuzzing and discovery
 - API objects fuzzing and discovery
- Configuration and Deploy Management Testing
 - Test Network/Infrastructure Configuration
 - Test Application Platform Configuration
 - Test File Extensions Handling for Sensitive Information
 - Review Old, Backup and Unreferenced Files for Sensitive Information
 - Enumerate Infrastructure and Application Admin Interfaces
 - Test HTTP Methods
 - Test HTTP Strict Transport Security
 - Test RIA cross domain policy
- Identity Management Testing
 - Test Role Definitions
 - Test User Registration Process
 - Test Account Provisioning Process
 - Testing for Account Enumeration and Guessable User Account
 - Testing for Weak or unenforced username policy
- Authentication Testing
 - Testing for Credentials Transported over an Encrypted Channel
 - Testing for default credentials

- Testing for Weak lock out mechanism
- Testing for bypassing authentication schema
- Test remember password functionality
- Testing for Browser cache weakness
- Testing for Weak password policy
- Testing for Weak security question/answer
- Testing for Weak password change or reset functionalities
- Testing for Weaker authentication in alternative channel
- Two-factor Authentication Testing (MFA)
- Authorization Testing
 - Testing Directory traversal/file include
 - Testing for bypassing authorization schema
 - Testing for Privilege Escalation
 - Testing for Insecure Direct Object References
- Session Management Testing
 - Testing for Bypassing Session Management Schema
 - Testing for Cookies attributes
 - Testing for Session Fixation
 - Testing for Exposed Session Variables
 - Testing for Cross Site Request Forgery (CSRF)
 - Testing for logout functionality
 - Test Session Timeout
 - Testing for Session puzzling
- Data Validation Testing
 - Testing for Reflected Cross Site Scripting
 - Testing for Stored Cross Site Scripting
 - Testing for HTTP Verb Tampering
 - Testing for HTTP Parameter pollution
 - Testing for SQL Injection
 - Oracle Testing
 - MySQL Testing
 - SQL Server Testing
 - Testing PostgreSQL
 - MS Access Testing
 - Testing for NoSQL injection
 - Testing for LDAP Injection
 - Testing for ORM Injection
 - Testing for XML Injection
 - Testing for SSI Injection
 - Testing for XPath Injection
 - Testing for IMAP/SMTP Injection

- Testing for Code Injection
- Testing for Local File Inclusion
- Testing for Remote File Inclusion
- Testing for Command Injection
- Testing for Buffer overflow
- Testing for Heap overflow
- Testing for Stack overflow
- Testing for Format string
- Testing for incubated vulnerabilities
- Testing for HTTP Splitting/Smuggling
- Testing for Error Handling
 - Testing for improper error handling
 - Testing for Stack Traces
- Testing for weak Cryptography
 - ~~Testing for Weak Transport Layer Security~~ - covered by TLS Grade service
 - Testing for Padding Oracle
 - Testing for Sensitive information sent via unencrypted channels
- Business Logic Testing
 - Test Business Logic Data Validation
 - Test Ability to Forge Requests
 - Test Integrity Checks
 - Test for Process Timing
 - Test Number of Times a Function Can be Used Limits
 - Testing for the Circumvention of Work Flows
 - Test Defenses Against Application Mis-use
 - Test Upload of Unexpected File Types
 - Test Upload of Malicious Files
- API Testing
 - Testing GraphQL
- OWASP API Top 10 2023
 - Broken Object Level Authorization (BOLA / IDOR)
 - Broken Authentication
 - Broken Object Property Level Authorization
 - Unrestricted Resource Consumption
 - Broken Function Level Authorization
 - Unrestricted Access to Sensitive Business Flows
 - Server Side Request Forgery
 - Security Misconfiguration
 - Improper Inventory Management
 - Unsafe Consumption of APIs
- Reporting and presentation

- Announcing detected vulnerabilities to the Customer accordingly to contractual provisions and SLA.

Web-api tests

Test ID	Name	Results
WSTG-INFO	Information gathering	✓
API-REC	Additional API Reconnaissance	✓
WSTG-CONF	Config and deploy management testing	🔍 F 5.1,F 5.2,F 5.3
WSTG-IDNT	Identity management testing	✓
WSTG-ATHN	Authentication testing	✓
WSTG-ATHZ	Authorization testing	✓
WSTG-SESS	Session management testing	✓
WSTG-INPVAL	Input validation testing	🔍 F 4.1
WSTG-ERR	Error handling	🔍 F 4.2
WSTG-CRYP	Testing for Weak Cryptography (partially covered by TLS Grade service)	✓
WSTG-BUSL	Business Logic Testing	✓
WSTG-APIT	API Testing	✓
API-TOP-10	OWASP API Top 10 2023	✓

4. Test Phases

Phase	Description
Preparation	<ul style="list-style-type: none"> Initial calls with the Customer Initial exchange of required information
Testing	<ul style="list-style-type: none"> Information gathering Scanning, vulnerability assessment Manual testing of components Exploitation of findings
Reporting (Draft)	<ul style="list-style-type: none"> Draft report Draft presentation
Finalization of the report	<ul style="list-style-type: none"> Amendments Retesting if required (in case of errors or Customer's remarks)
Final report	<ul style="list-style-type: none"> Final report and presentation
Remediation support	<ul style="list-style-type: none"> Support with remediation process
Retesting	<ul style="list-style-type: none"> Retesting of remediated vulnerabilities (might be expanded in time) Conference calls with Customer's representatives

F. Findings, Recommendations and Retests

1. Critical Risk Vulnerabilities

Critical risk vulnerability could be expected to have a catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is no able to perform one or more of its primary functions;
- Result in major damage to organizational assets
- Result in major financial loss
- Result in severe harm to individuals involving loss of life or serious life threatening injuries.

No critical severity findings have been found.

2. High Risk Vulnerabilities

A high risk vulnerability could be expected to have a severe adverse effect on organizational operations, organizational assets, or individuals. A severe adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
- Result in major damage to organizational assets;
- Result in major financial loss; or
- Result in severe harm to individuals involving loss of life or serious life threatening injuries.

No high severity findings have been found.

3. Medium Risk Vulnerabilities

A medium risk vulnerability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
- Result in significant damage to organizational assets;
- Result in significant financial loss; or
- Result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

No medium severity findings have been found.

4. Low Risk Vulnerabilities

A low risk vulnerability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- Cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
- Result in minor damage to organizational assets;
- Result in minor financial loss; or
- Result in minor harm to individuals.

4.1. Improper input validation (30612)

LOW 3.7	Attack Vector: NETWORK	Scope: UNCHANGED
	Attack Complexity: HIGH	Confidentiality: LOW
	Privileges Required: NONE	Integrity: NONE
	User Interaction: NONE	Availability: NONE
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/CR:M/IR:H/AR:H		

4.1.1. Assets

```
/adapter05/card/phonenumer/{party-uuid};  
/adapter06/card/phonenumer/{party-uuid};  
/v1/payments/iban/validation;
```

4.1.2. Description

Input validation is a frequently-used technique for checking potentially dangerous inputs in order to ensure that the inputs are safe for processing within the code, or when communicating with other components. When software does not validate input properly, an attacker is able to craft the input in a form that is not expected by the rest of the application. This will lead to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.

4.1.3. Recommendation

There are multiple approaches to input validation. However, an effective way is to ensure that you know what data you want, and to reject all other forms of data.

4.1.4. Additional Information

CWE-200

<https://cwe.mitre.org/data/definitions/20.html>

4.1.5. Evidence

The tested endpoints do not enforce proper input validation on several parameters.

For example, it was possible to submit unexpected values, such as JavaScript code, in field named *iban*. Despite containing invalid or potentially malicious input, the API accepted the requests and returned a 200 response, indicating that the payload was processed without error.

Please note that when injecting specific characters (such as '<'), the API returns a Bad request error message.

```
POST /v1/payments/iban/validation HTTP/1.1
Host: localhost:1234
Cookie: JSESSIONID=DD57AB3D80BE6EF0602C9D5893B820C5
Content-Length: 38
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: it-IT,it;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Content-Type: application/json
Sec-Ch-UA-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/140.0.0.0 Safari/537.36
Origin: https://localhost:1234
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://localhost:1234/swagger-ui/index.html
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

{
    "iban": "alert(document.cookie)"
}
```

Improper input validation (/v1/payments/iban/validation)

Request	Response
Pretty	Pretty
Raw	Raw
Hex	Render
<pre>1 POST /v1/payments/iban/validation HTTP/1.1 2 Host: localhost:1234 3 Cookie: JSESSIONID=DD57AB3D80BE6EF0602C9D5893B820C5 4 Content-Length: 38 5 Sec-Ch-Ua-Platform: "Windows" 6 Accept-Language: it-IT,it;q=0.9 7 Accept: application/json 8 Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140" 9 Content-Type: application/json 10 Sec-Ch-UA-Mobile: ?0 11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36 12 Origin: https://localhost:1234 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Dest: empty 16 Referer: https://localhost:1234/swagger-ui/index.html 17 Accept-Encoding: gzip, deflate, br 18 Priority: u=1, i 19 Connection: keep-alive 20 21 { 22 "iban": "alert(document.cookie)" 23 }</pre>	<pre>1 HTTP/1.1 200 2 traceparent: 00-e89eba576dacl15dacecf8d8699ca8cc-a07bb68a5421e37-01 3 Set-Cookie: JSESSIONID=ED1A1A254CF053079B05B121A7D83E1E; Path=/; Secure; HttpOnly 4 Content-Type: application/json 5 Date: Fri, 28 Sep 2023 10:44:26 GMT 6 Keep-Alive: timeout=60 7 Connection: keep-alive 8 Content-Length: 141 9 10 { 11 "iban": "alert(document.cookie)", 12 "sepaReachable": null, 13 "bankDetails": null, 14 "validFormat": false, 15 "internalAccountClosed": null, 16 "blacklisted": null 17 }</pre>

In addition, in some requests required headers are not validated. As an example, please consider the following figure shows the X-ING-Request-Id is a required header to perform reques to /adapter06/card/phonenumber/{party-uuid}.

Required header X-ING-Request-Id

The screenshot shows a Swagger UI interface for a GET request. The URL is `/adapter06/card/phonenumber/{party-uuid}`. The description is "Retrieve customer phone-number". Below the URL, it says "Given party-uuid retrieves customer phone-number". Under the "Parameters" section, there are two entries:

- X-ING-Request-Id** * required string (header) - The input field is empty.
- party-uuid** * required string (path) - The input field contains "party-uuid".

A "Try it out" button is visible in the top right corner of the parameters section.

Even if the header is marked as required value, it is possible to perform the request leaving the header empty.

```
GET /adapter06/card/phonenumber/727e027a-bca1-445b-9308-2f4f90aae2eb HTTP/1.1
Host: localhost:1234
Cookie: JSESSIONID=C9C0123637671359C894825E2FE5C469
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: it-IT,it;q=0.9
Accept: application/json
X-Ing-Request-Id:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/140.0.0.0 Safari/537.36
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Sec-Ch-Ua-Mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://localhost:1234/swagger-ui/index.html
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Improper input validation - X-ING-Request-Id (/adapter06/card/phonenumber/{party-uuid})

Request		Response	
Pretty	Raw	Hex	Render
<pre> 1 GET /adapter06/card/phonenumber/727e027a-bcal-445b-9308-2f4f90aae 2b HTTP/1.1 3 Host: localhost:1234 4 Cookie: JSESSIONID=C9C0123637671359C894825E2FE5C469 5 Sec-Ch-Ua-Platform: "Windows" 6 Accept-Language: it-IT,it;q=0.9 7 Accept: application/json 7 X-Ing-Request-Id: 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36 9 Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140" .0 Sec-Ch-Ua-Mobile: ?0 .1 Sec-Fetch-Site: same-origin .2 Sec-Fetch-Mode: cors .3 Sec-Fetch-Dest: empty .4 Referer: https://localhost:1234/swagger-ui/index.html .5 Accept-Encoding: gzip, deflate, br .6 Priority: u=1, i .7 Connection: keep-alive .8 .9 </pre>		<pre> 1 HTTP/1.1 404 2 traceparent: 00-f907071403e4573d00b56e68ddde29dd-97bfabeb7eb40c1-01 3 Content-Type: application/json 4 Content-Length: 101 5 Date: Wed, 22 Oct 2025 07:04:56 GMT 6 Keep-Alive: timeout=20 7 Connection: keep-alive 8 9 { "error": { "code": "INVOLVED_PARTY_NOT_FOUND", "message": "involved party not found", "severity": "error" } } </pre>	

4.2. Verbose Error Messages (23703)

LOW 3.1	Attack Vector: NETWORK	Scope: UNCHANGED
	Attack Complexity: HIGH	Confidentiality: LOW
	Privileges Required: LOW	Integrity: NONE
	User Interaction: NONE	Availability: NONE
CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/CR:M/IR:H/AR:H		

4.2.1. Assets

```
/adapter06/card/details;
/adapter05/card/details;
/v1/payments/delete/sepa;
https://sd80tsssd12:8095/v1/oracle-card/scoring;
```

4.2.2. Description

During the test it has been revealed that in case of some requests, server throws out an error exception. The exception message may contain a lot of detailed technical information, including filenames, absolute paths, but also libraries, classes and methods used. This information might be crucial in conducting other, critical attacks (like Arbitrary File Read, Code Execution or platform specific attacks). Such detailed information should be available only to application developers and system administrators and should never be revealed to the end user.

4.2.3. Recommendation

Verbose errors should not be provided to end users. Friendly static error pages should be provided instead. Error cause should be investigated within the code.

4.2.4. Additional Information

4.2.5. Evidence

In the example below, it is possible to observe that the error message informed us that an Integer for the parameter ScoringType is required. Even though the information retrieved is not very relevant, it is recommended to always return generic error messages.

Verbose Error Messages (<https://sd80tsssad12:8095/v1/oracle-card/scoring>)

Request		Response	
Pretty	Raw	Hex	Render
<pre> 1 GET /v1/oracle-card/scoring?coownId=0002014121& 2 scoringType=HTTP/1.1 3 Host: sd80tsssad12:8095 4 Sec-Ch-Ua-Platform: "Windows" 5 Accept-Language: en-US,en;q=0.9 6 Accept: application/json 7 Sec-Ch-Ua: "Chromium";v="139", "Not;A=Brand";v="99" 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) 9 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 10 Safari/537.36 11 Sec-Ch-Ua-Mobile: ? 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: https://sd80tsssad12:8095/swagger-ui/index.html 16 Accept-Encoding: gzip, deflate, br 17 Priority: u=1, i 18 Connection: keep-alive 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 159 160 161 162 163 164 165 166 167 168 169 169 170 171 172 173 174 175 176 177 178 179 179 180 181 182 183 184 185 186 187 188 189 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 209 210 211 212 213 214 215 216 217 218 219 219 220 221 222 223 224 225 226 227 228 229 229 230 231 232 233 234 235 236 237 237 238 239 239 240 241 242 243 244 245 246 247 247 248 249 249 250 251 252 253 254 255 256 257 257 258 259 259 260 261 262 263 264 265 266 267 267 268 269 269 270 271 272 273 274 275 276 277 277 278 279 279 280 281 282 283 284 285 286 287 287 288 289 289 290 291 292 293 294 295 296 297 297 298 299 299 300 301 302 303 304 305 306 307 308 309 309 310 311 312 313 314 315 316 317 318 319 319 320 321 322 323 324 325 326 327 328 329 329 330 331 332 333 334 335 336 337 338 339 339 340 341 342 343 344 345 346 347 347 348 349 349 350 351 352 353 354 355 356 357 357 358 359 359 360 361 362 363 364 365 366 367 367 368 369 369 370 371 372 373 374 375 376 377 377 378 379 379 380 381 382 383 384 385 386 387 387 388 389 389 390 391 392 393 394 395 396 397 397 398 399 399 400 401 402 403 404 405 406 407 408 409 409 410 411 412 413 414 415 416 417 417 418 419 419 420 421 422 423 424 425 426 427 427 428 429 429 430 431 432 433 434 435 436 437 437 438 439 439 440 441 442 443 444 445 446 447 447 448 449 449 450 451 452 453 454 455 456 457 457 458 459 459 460 461 462 463 464 465 466 467 467 468 469 469 470 471 472 473 474 475 476 477 477 478 479 479 480 481 482 483 484 485 486 487 487 488 489 489 490 491 492 493 494 495 496 497 497 498 499 499 500 501 502 503 504 505 506 507 508 509 509 510 511 512 513 514 515 516 517 517 518 519 519 520 521 522 523 524 525 526 527 527 528 529 529 530 531 532 533 534 535 536 537 537 538 539 539 540 541 542 543 544 545 546 547 547 548 549 549 550 551 552 553 554 555 556 557 557 558 559 559 560 561 562 563 564 565 566 567 567 568 569 569 570 571 572 573 574 575 576 577 577 578 579 579 580 581 582 583 584 585 586 587 587 588 589 589 590 591 592 593 594 595 596 597 597 598 599 599 600 601 602 603 604 605 606 607 607 608 609 609 610 611 612 613 614 615 616 617 617 618 619 619 620 621 622 623 624 625 626 627 627 628 629 629 630 631 632 633 634 635 636 637 637 638 639 639 640 641 642 643 644 645 646 647 647 648 649 649 650 651 652 653 654 655 656 657 657 658 659 659 660 661 662 663 664 665 666 667 667 668 669 669 670 671 672 673 674 675 676 677 677 678 679 679 680 681 682 683 684 685 686 687 687 688 689 689 690 691 692 693 694 695 696 697 697 698 699 699 700 701 702 703 704 705 706 707 707 708 709 709 710 711 712 713 714 715 715 716 717 717 718 719 719 720 721 722 723 724 725 726 727 727 728 729 729 730 731 732 733 734 735 736 737 737 738 739 739 740 741 742 743 744 745 746 747 747 748 749 749 750 751 752 753 754 755 756 757 757 758 759 759 760 761 762 763 764 765 766 767 767 768 769 769 770 771 772 773 774 775 776 777 777 778 779 779 780 781 782 783 784 785 786 787 787 788 789 789 790 791 792 793 794 795 796 797 797 798 799 799 800 801 802 803 804 805 806 807 807 808 809 809 810 811 812 813 814 815 816 817 817 818 819 819 820 821 822 823 824 825 826 827 827 828 829 829 830 831 832 833 834 835 836 837 837 838 839 839 840 841 842 843 844 845 846 847 847 848 849 849 850 851 852 853 854 855 856 857 857 858 859 859 860 861 862 863 864 865 866 867 867 868 869 869 870 871 872 873 874 875 876 877 877 878 879 879 880 881 882 883 884 885 886 887 887 888 889 889 890 891 892 893 894 895 896 897 897 898 899 899 900 901 902 903 904 905 906 907 907 908 909 909 910 911 912 913 914 915 916 916 917 918 918 919 920 921 922 923 924 925 926 927 927 928 929 929 930 931 932 933 934 935 936 937 937 938 939 939 940 941 942 943 944 945 946 947 947 948 949 949 950 951 952 953 954 955 956 957 957 958 959 959 960 961 962 963 964 965 966 967 967 968 969 969 970 971 972 973 974 975 976 977 977 978 979 979 980 981 982 983 984 985 986 987 987 988 989 989 990 991 992 993 994 995 996 997 998 999 999 1000 1001 1002 1003 1004 1005 1006 1007 1007 1008 1009 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1029 1030 1031 1032 1033 1034 1035 1036 1037 1037 1038 1039 1039 1040 1041 1042 1043 1044 1045 1046 1047 1047 1048 1049 1049 1050 1051 1052 1053 1054 1055 1056 1057 1057 1058 1059 1059 1060 1061 1062 1063 1064 1065 1066 1067 1067 1068 1069 1069 1070 1071 1072 1073 1074 1075 1076 1077 1077 1078 1079 1079 1080 1081 1082 1083 1084 1085 1086 1087 1087 1088 1089 1089 1090 1091 1092 1093 1094 1095 1096 1097 1097 1098 1099 1099 1100 1101 1102 1103 1104 1105 1106 1107 1107 1108 1109 1109 1110 1111 1112 1113 1114 1115 1116 1117 1117 1118 1119 1119 1120 1121 1122 1123 1124 1125 1126 1127 1127 1128 1129 1129 1130 1131 1132 1133 1134 1135 1136 1137 1137 1138 1139 1139 1140 1141 1142 1143 1144 1145 1146 1147 1147 1148 1149 1149 1150 1151 1152 1153 1154 1155 1156 1157 1157 1158 1159 1159 1160 1161 1162 1163 1164 1165 1166 1167 1167 1168 1169 1169 1170 1171 1172 1173 1174 1175 1176 1177 1177 1178 1179 1179 1180 1181 1182 1183 1184 1185 1186 1187 1187 1188 1189 1189 1190 1191 1192 1193 1194 1195 1196 1197 1197 1198 1199 1199 1200 1201 1202 1203 1204 1205 1206 1207 1207 1208 1209 1209 1210 1211 1212 1213 1214 1215 1216 1217 1217 1218 1219 1219 1220 1221 1222 1223 1224 1225 1226 1227 1227 1228 1229 1229 1230 1231 1232 1233 1234 1235 1236 1237 1237 1238 1239 1239 1240 1241 1242 1243 1244 1245 1246 1247 1247 1248 1249 1249 1250 1251 1252 1253 1254 1255 1256 1257 1257 1258 1259 1259 1260 1261 1262 1263 1264 1265 1266 1267 1267 1268 1269 1269 1270 1271 1272 1273 1274 1275 1276 1277 1277 1278 1279 1279 1280 1281 1282 1283 1284 1285 1286 1287 1287 1288 1289 1289 1290 1291 1292 1293 1294 1295 1296 1297 1297 1298 1299 1299 1300 1301 1302 1303 1304 1305 1306 1307 1307 1308 1309 1309 1310 1311 1312 1313 1314 1315 1316 1317 1317 1318 1319 1319 1320 1321 1322 1323 1324 1325 1326 1327 1327 1328 1329 1329 1330 1331 1332 1333 1334 1335 1336 1337 1337 1338 1339 1339 1340 1341 1342 1343 1344 1345 1346 1347 1347 1348 1349 1349 1350 1351 1352 1353 1354 1355 1356 1357 1357 1358 1359 1359 1360 1361 1362 1363 1364 1365 1366 1367 1367 1368 1369 1369 1370 1371 1372 1373 1374 1375 1376 1377 1377 1378 1379 1379 1380 1381 1382 1383 1384 1385 1386 1387 1387 1388 1389 1389 1390 1391 1392 1393 1394 1395 1396 1397 1397 1398 1399 1399 1400 1401 1402 1403 1404 1405 1405 1406 1407 1407 1408 1409 1409 1410 1411 1412 1413 1414 1415 1416 1417 1417 1418 1419 1419 1420 1421 1422 1423 1424 1425 1426 1427 1427 1428 1429 1429 1430 1431 1432 1433 1434 1435 1436 1437 1437 1438 1439 1439 1440 1441 1442 1443 1444 1445 1446 1447 1447 1448 1449 1449 1450 1451 1452 1453 1454 1455 1456 1457 1457 1458 1459 1459 1460 1461 1462 1463 1464 1465 1466 1467 1467 1468 1469 1469 1470 1471 1472 1473 1474 1475 1476 1477 1477 1478 1479 1479 1480 1481 1482 1483 1484 1485 1486 1487 1487 1488 1489 1489 1490 1491 1492 1493 1494 1495 1496 1497 1497 1498 1499 1499 1500 1501 1502 1503 1504 1505 1506 1507 1507 1508 1509 1509 1510 1511 1512 1513 1514 1515 1516 1517 1517 1518 1519 1519 1520 1521 1522 1523 1524 1525 1526 1527 1527 1528 1529 1529 1530 1531 1532 1533 1534 1535 1536 1537 1537 1538 1539 1539 1540 1541 1542 1543 1544 1545 1546 1547 1547 1548 1549 1549 1550 1551 1552 1553 1554 1555 1556 1557 1557 1558 1559 1559 1560 1561 1562 1563 1564 1565 1566 1567 1567 1568 1569 1569 1570 1571 1572 1573 1574 1575 1576 1577 1577 1578 1579 1579 1580 1581 1582 1583 1584 1585 1586 1587 1587 1588 1589 1589 1590 1591 1592 1593 1594 1595 1596 1597 1597 1598 1599 1599 1600 1601 1602 1603 1604 1605 1606 1607 1607 1608 1609 1609 1610 1611 1612 1613 1614 1615 1616 1617 1617 1618 1619 1619 1620 1621 1622 1623 1624 1625 1626 1627 1627 1628 1629 1629 1630 1631 1632 1633 1634 1635 1636 1637 1637 1638 1639 1639 1640 1641 1642 1643 1644 1645 1646 1647 1647 1648 1649 1649 1650 1651 1652 1653 1654 1655 1656 1657 1657 1658 1659 1659 1660 1661 1662 1663 1664 1665 1666 1667 1667 1668 1669 1669 1670 1671 1672 1673 1674 1675 1676 1677 1677 1678 1679 1679 1680 1681 1682 1683 1684 1685 1686 1687 1687 1688 1689 1689 1690 1691 1692 1693 1694 1695 1696 1697 1697 1698 1699 1699 1700 1701 1702 1703 1704 1705 1706 1707 1707 1708 1709 1709 1710 1711 1712 1713 1714 1715 1716 1717 1717 1718 1719 1719 1720 1721 1722 1723 1724 1725 1726 1727 1727 1728 1729 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1738 1739 1739 1740 1741 1741 1742 1743 1743 1744 1745 1745 1746 1747 1747 1748 1749 1749 1750 1751 1752 1753 1754 1755 1756 1757 1757 1758 1759 1759 1760 1761 1762 1763 1764 1765 1766 1767 1767 1768 1769 1769 1770 1771 1772 1773 1774 1775 1776 1777 1777 1778 1779 1779 1780 1781 1782 1783 1784 1785 1786 1787 1787 1788 1789 1789 1790 1791 1792 1793 1794 1795 1796 1797 1797 1798 1799 1799 1800 1801 1802 1803 1804 1805 1806 1807 1807 1808 1809 1809 1810 1811 1812 1813 1814 1815 1816 1817 1817 1818 1819 1819 1820 1821 1822 1823 1824 1825 1826 1827 1827 1828 1829 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1838 1839 1840 1840 1841 1842 1842 1843 1844 1844 1845 1846 1846 1847 1848 1848 1849 1850 1851 1852 1853 1854 1855 1856 1857 1857 1858 1859 1859 1860 1861 1862 1863 1864 1865 1866 1867 1867 1868 1869 1869 1870 1871 1872 1873 1874 1875 1876 1877 1877 1878 1879 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1889 1889 1890 1891 1892 1893 1894 1895 1896 1897 1897 1898 1899 1899 1900 1901 1902 1903 1904 1905 1906 1907 1907 1908 1909 1909 1910 1911 1912 1913 1914 1915 1916 1917 1917 1918 1919 1919 1920 1921 1922 1923 1924 1925 1926 1927 1927 1928 1929 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1938 1939 1940 1940 1941 1942 1942 1943 1944 1944 1945 1946 1946 1947 1948 1948 1949 1950 1951 1952 1953 1954 1955 1956 1957 1957 1958 1959 1959 1960 1961 1962 1963 1964 1965 1966 1967 1967 1968 1969 1969 1970 1971 1972 1973 1974 1975 1976 1977 1977 1978 1979 1979 1980 1981 19</pre>			

```

Sec-Ch-Ua-Platform: "Windows"
Accept-Language: it-IT,it;q=0.9
X-Ing-AccessToken:
eyJhbGciOiJSUzI1NiIsIngldCI6IjhfQUZD0EQxMjBDRjVFQzLBMTBDQkNENkQ20EJEQTFDRTA5RDYyNzM
iLCJraWQiOjI4RUFGQzhEMTIwQ0Y1RUM5QTEwQ0JDrdZENjhCREExQ0UwOUQ2MjczIn0.eyJjaWQiOjIjbG
llbnRJZCIsInNreSI6ImI1MTIwM2NhZGQ00Tg4MTU0MzNkMzJhNzFkMTAxYTE4MDdkM2EyMzhmMmQ1MzM50
GVkZjVjNmM1MTU5NjUwYjciLCJ0cmMiOnRydWUsInNjb3BLIjoicGVyc29uYWxfZGF0YSIsImluYSI6MCwi
Y3NvIjoiQ1NPX3ZhHVlIiwiZXhlijp7InBlcnNvbI6Ijg40DMwYTc1LTJk0GYtNGEzZS04NDfLLTg5ZDh
lOTI50GMyYiIsInByb2ZpbGUiOjJmY2M0YmNlNC040DljLTrhNTctYjIwMS1h0WY2N2FhYzA3NjciLCJtZW
FucyI6W3sidHlwIjoiwWhbnNUeXBlIiwiwQoijtZWfuc0lkIn1dLCJsb2Ei0jUsInR5cCI6ImN1c3Rvb
wVyiIn0sInB0eSI6ImNvb2tpZSIIsInB2ZSI6InNly3VyZV9yYW5kb21fdmFsdwUiLCJzaWQoijkZTc3ZjY3
ZC00Y2U5LTQ4ZmYt0DVizS1j0WjkYmVkJzWMiLCJ2ZXi0iIxLjQilCJqdGkiOii4NzI4MTYwMi1lZDN
mLTrjNDAt0Tg5Zi05YwvjZDA3YTZjMzcilCJ0eXAi0iJhY2Nlc3MiLCJleHAi0jE3NTkzNjg2NzYsIm5iZi
I6MTc10TMw0DY3NiwiawF0IjoxNzU5MzA4Njg1LCJpc3Mi0iJhcGkuZG9tYWluLmNbSJ9.Jgx5zH6Pc85P
U_u657hS-mt6P0zk729WPxerxxtMCYkQxm20XiPlrMVSq9WBaHZNRR2HdTbVHPYdJM-
J7hBCgjdQ5i0xBFFdfsWLmn0PM9ZzMLvebzGFwfNOMXpr3r-
FfIcfJaFemd_bYbYief3x9mS2RANEqN03RNnzsC75d75U0VZ0_VRCV65__GKHYzMuBHY2j0Go3uPriWEUhT
b2weGaVJ5JPPT80p7CFW0Xf6oxw0AV-_7z0wUT7wCMRHRMvUPLYQUt-6bFummLGeG_LCM9-
velWzLRoHWuG48mu_g00hhTxYkY0U4zHlpXezNgi3P9Rb7gFRbNIRnPv2rf7g
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
X-Ing-Request-Id: 11
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept: application/json
Content-Type: application/json
Origin: https://localhost:1234
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://localhost:1234/swagger-ui/index.html
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
  "ingEntity": "string",
  "productType": "string",
  "cardPointerId": "string"
}

```

Verbose Error Messages (/adapter05/card/details): UUID type missing

Request	Response
<pre> 1 POST /adapter05/card/details HTTP/2 2 Host: localhost:1234 3 Cookie: JSESSIONID=F82DB3E0E4B22DE56BB4F2C5AACBDED2 4 Content-Length: 83 5 Sec-Ch-Ua-Platform: "Windows" 6 Accept-Language: it-IT,it;q=0.9 7 X-Ing-Accesstoken: eyJhbGciOiJSUzI1NiIsIngldCI6IjhFQUZD0EqxMjBDRjVFQzLBMTBDQkNENkQ20EJEQTFRAT5RDYyNzM iLCJraWQiOiI4RUFGQzhEMTIwQ0Y1RUM5QTEwQ0JDRDZENjhCREExQ0UwOUQ2MjczIn0..eyJjaWQiOiJjbG llbnRJZCIsInNreSI6ImI1MTIwM2NhZGQ00Tg4MTU0MzNkMzJhNzfKMTAxYTE4MDdkM2EyMzhmMmQ1MzM50 GVkZjVjNmM1MTU5NjUwYjciLCJ0cmMiOnRydWUsInNb3BlIjoicGVyc29uYWxfZGF0YSIsImluYSI6MCwi Y3NvIjoiQ1NPX3ZhbHVlIiwiZXhlIjp7InBlcnNvbii6Ijg40DMwYTc1LTJk0GYtNGEzZS04NDfLLTg5Zdh 10TI50GMYiIsInByb2ZpbGUoIjMjY2M0YmNlNC040DljLTRhNTctYjIwMS1h0WY2N2FhYzA3NjciLCJtZW FucyI6W3sidHlwIjoiwVhbnNUeXBIIiwiaWQiOiJtzWFuc0lkIn1dLCJsb2Ei0jUsInR5cI6ImN1cRvb WVyiIn0sInB0eSI6ImNvb2tpZSIsInB2ZSI6InNly3VyZV9yYW5kb21fdmFsdWLmPZM2EwvzbGFNFNCpr3r-F1c ZC00Y2U5LTQ4ZmYtODViZS1j0WjkYmVkmDljZWMiLCJ2ZXi0iIxlj0iLCJqdGkiOiI4NzI4MTYwMii1ZDN mLTrjNDAt0Tg5Zi05YwvjZDA3YTzjMzcilCJ0eXAi0iJhY2Nlc3MiLCJleHAi0jE3NTkzNjg2NzYsIm5iZi I6MTc10TMw0DY3NiwiawF0IjoxNzU5MzA4Njg1LCJpc3Mi0iJhcGkuZG9tYwluLmNvbSJ9.Jgx5zH6Pc85P U_u657hS-mt6P0zk729WPixerxxtMCYkQxm20XiPlrMVSq9WBaHZNRR2HdTbVHPYdJM- J7hBCgjdQ5i0xBFFdfsWLmn0PM9ZzMLvebzGFwfNOMXpr3r- FfIcfJaFemd_bYbYief3x9mS2RANEqN03RnNzsC75d75U0Vz0_VRCV65__GKHYzMuBHY2j0Go3uPriWEUhT b2weGaVJ5JPPT80p7CFW0Xf6oxwOAV-_7z0wUT7wCMRHRMvUPLYQut-6bfummLGeG_LCM9- velWzLRoHWuG48mu_g00hhTxYkY0U4zHlpXezNgi3P9Rb7gFRbNIRnPv2rf7g Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140" X-Ing-Request-Id: 11 Sec-Ch-Ua-Mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36 Accept: application/json Content-Type: application/json Origin: https://localhost:1234 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: https://localhost:1234/swagger-ui/index.html Accept-Encoding: gzip, deflate, br </pre>	<pre> 1 HTTP/2 400 Bad Request 2 Traceparent: 00-132d8383fe7b63ca75clee24b570fa58-4063097e722d73b7-01 3 Content-Type: application/json 4 Content-Length: 173 5 Date: Wed, 01 Oct 2025 08:52:04 GMT 6 7 { "error": { "code": "400", "message": "Invalid UUID", "severity": "error", "source": "API", "innerErrors": [{ "code": "400", "message": "Invalid UUID", "severity": "error", "source": "API" }] } } </pre>

```

POST /adapter05/card/details HTTP/2
Host: localhost:1234
Cookie: JSESSIONID=F82DB3E0E4B22DE56BB4F2C5AACBDED2
Content-Length: 113
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: it-IT,it;q=0.9
X-Ing-Accesstoken:
eyJhbGciOiJSUzI1NiIsIngldCI6IjhFQUZD0EqxMjBDRjVFQzLBMTBDQkNENkQ20EJEQTFRAT5RDYyNzM
iLCJraWQiOiI4RUFGQzhEMTIwQ0Y1RUM5QTEwQ0JDRDZENjhCREExQ0UwOUQ2MjczIn0..eyJjaWQiOiJjbG
llbnRJZCIsInNreSI6ImI1MTIwM2NhZGQ00Tg4MTU0MzNkMzJhNzfKMTAxYTE4MDdkM2EyMzhmMmQ1MzM50
GVkZjVjNmM1MTU5NjUwYjciLCJ0cmMiOnRydWUsInNb3BlIjoicGVyc29uYWxfZGF0YSIsImluYSI6MCwi
Y3NvIjoiQ1NPX3ZhbHVlIiwiZXhlIjp7InBlcnNvbii6Ijg40DMwYTc1LTJk0GYtNGEzZS04NDfLLTg5Zdh
10TI50GMYiIsInByb2ZpbGUoIjMjY2M0YmNlNC040DljLTRhNTctYjIwMS1h0WY2N2FhYzA3NjciLCJtZW
FucyI6W3sidHlwIjoiwVhbnNUeXBIIiwiaWQiOiJtzWFuc0lkIn1dLCJsb2Ei0jUsInR5cI6ImN1cRvb
WVyiIn0sInB0eSI6ImNvb2tpZSIsInB2ZSI6InNly3VyZV9yYW5kb21fdmFsdWLmPZM2EwvzbGFNFNCpr3r-
ZC00Y2U5LTQ4ZmYtODViZS1j0WjkYmVkmDljZWMiLCJ2ZXi0iIxlj0iLCJqdGkiOiI4NzI4MTYwMii1ZDN
mLTrjNDAt0Tg5Zi05YwvjZDA3YTzjMzcilCJ0eXAi0iJhY2Nlc3MiLCJleHAi0jE3NTkzNjg2NzYsIm5iZi
I6MTc10TMw0DY3NiwiawF0IjoxNzU5MzA4Njg1LCJpc3Mi0iJhcGkuZG9tYwluLmNvbSJ9.Jgx5zH6Pc85P
U_u657hS-mt6P0zk729WPixerxxtMCYkQxm20XiPlrMVSq9WBaHZNRR2HdTbVHPYdJM-
J7hBCgjdQ5i0xBFFdfsWLmn0PM9ZzMLvebzGFwfNOMXpr3r-
FfIcfJaFemd_bYbYief3x9mS2RANEqN03RnNzsC75d75U0Vz0_VRCV65__GKHYzMuBHY2j0Go3uPriWEUhT
b2weGaVJ5JPPT80p7CFW0Xf6oxwOAV-_7z0wUT7wCMRHRMvUPLYQut-6bfummLGeG_LCM9-
velWzLRoHWuG48mu_g00hhTxYkY0U4zHlpXezNgi3P9Rb7gFRbNIRnPv2rf7g
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
X-Ing-Request-Id: 11
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept: application/json
Content-Type: application/json
Origin: https://localhost:1234
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://localhost:1234/swagger-ui/index.html
Accept-Encoding: gzip, deflate, br

```

Priority: u=1, i

```
{
  "ingEntity": "string",
  "productType": "string",
  "cardPointerId": "96fddd70-9052-469f-974a-7421b0e56694"
}
```

Verbose Error Messages (/adapter05/card/details): base64 encoding missing

Request	Response
<pre> 1 POST /adapter05/card/details HTTP/2 2 Host: localhost:1234 3 Cookie: JSESSIONID=F82DB3E0E4B22DE56BB4F2C5AACBDED2 4 Content-Length: 113 5 Sec-Ch-Ua-Platform: "Windows" 6 Accept-Language: it-IT,it;q=0.9 7 X-Ing-Accesstoken: eyJhbGciOiJSUzI1NiIsIngldCI6IjhFQUZD0EQxMjBDRjVFQzbMTBDQkNENkQ20EJEQTFRDRTA5RDYyNzM iLCJraWQiOiI4RUFGQzhEMTIwQ0Y1RUM5QTEwQ0JDRDZENjhCREEExQ0UwOUQ2MjczIn0.eyJjaWQiOiJjbG llbnRJZCIsInNreSI6ImI1MTIwM2NhZGQ00Tg4MTU0MzNkMzJhNzfKMTAxYTE4MDdkM2EyMzhmMmQ1MzM5M0 GVkZjVjNmM1MTU5njUwYjciLCJ0cmMiOnRydWUsInNjb3BljoicGVyc29uYWxfZGF0YSIsImluYSI6MCwi Y3NvIjoiQ1NPX3ZhHVlIiwiZXhlIp7InBlcnNvbii6Ijg40DMwYTc1LTjk0GYtNGEzZS04NDflLTg5ZDh 10TI50GMYiIsInByb2ZpbGUoIjMjY2M0YmNlNC040DljLTRhNTctYjIwMS1h0WY2N2FhYzA3NjciLCJtZW FucyI6W3sidHlwIjoibWvhbnNUeXBliiwiaWQiOjItZWFuc0lkIn1dLCJsb2Ei0jUsInR5cCI6ImN1c3Rvb WVyiOsInB0eSI6ImNvb2tpZSiIsInB2ZSI6InNly3VyZV9yYW5kb21fdmFsdWUiLCJzaWQiOjKzTc3ZjY3 ZC00Y2U5LTQ4ZmYtODViZS1j0WjkYmVkJZWMiLCJ2ZXIiOiIxLjQiLCJqdGkiOjI4NzI4MTYwMi1LZDm mLTrjNDAtOTg5Zi05YVvjZDA3YTjMzcilCJ0eXAiOjJhY2Nlc3MiLCJleHAIoje3NTkzNjg2NzYsIm5iZi I6MTc10TMw0DY3NiwiawF0IjoxNzU5MzA4Njg1LCJpc3Mi0iJhcGkuZG9tYVluLmNvbSJ9.Jgx5zH6Pc85P U_u657hS-mt6P0zk729WPxerxxtMCYkQxm20XiPlrMVSq9WBaHZNRR2HdTbVHPYdJM- J7hbCgjdQ5i0xBFFdfsWLmn0PM9ZzMLvebzGFwfNOMXpr3r- FfcfJaFemd_bYbYief3x9mS2RANEqN03RNnzsC75d75U0VZ0_VRCV65__GKHYzMuBHY2j0Go3uPriWEUhT b2weGaVJ5JPPT80p7CFW0XF6oxW0AV-_7z0wUT7wCMRHRMvUPLYQut-6bFummLGeG_LCM9- velWzLRoHWuG48mu_g00hhTxYkY0U4zHlpXezNgi3P9Rb7gFrbNIRnPv2rf7g Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140" X-Ing-Request-Id: 11 Sec-Ch-Ua-Mobile: ?0 </pre>	<pre> 1 HTTP/2 400 Bad Request 2 Traceparent: 00-abbd18c9c5ba79d3bd37808e1e30b2e-07480053a7af0705-01 3 Content-Type: application/json 4 Content-Length: 268 5 Date: Wed, 01 Oct 2025 08:52:27 GMT 6 7 { "error": { "code": "INVALID_PARAMETERS", "message": "Invalid input parameter", "severity": "error", "source": "ITA WalletCreditCard API", "target": "ITA WalletCreditCard API", "innerErrors": [{ "code": "400", "message": "pointerid can't be decoded as base64", "severity": "error" }] } } </pre>

```

POST /adapter05/card/details HTTP/2
Host: localhost:1234
Cookie: JSESSIONID=F82DB3E0E4B22DE56BB4F2C5AACBDED2
Content-Length: 125
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: it-IT,it;q=0.9
X-Ing-Accesstoken:
eyJhbGciOiJSUzI1NiIsIngldCI6IjhFQUZD0EQxMjBDRjVFQzbMTBDQkNENkQ20EJEQTFRDRTA5RDYyNzM
iLCJraWQiOiI4RUFGQzhEMTIwQ0Y1RUM5QTEwQ0JDRDZENjhCREEExQ0UwOUQ2MjczIn0.eyJjaWQiOiJjbG
llbnRJZCIsInNreSI6ImI1MTIwM2NhZGQ00Tg4MTU0MzNkMzJhNzfKMTAxYTE4MDdkM2EyMzhmMmQ1MzM5M0
GVkZjVjNmM1MTU5njUwYjciLCJ0cmMiOnRydWUsInNjb3BljoicGVyc29uYWxfZGF0YSIsImluYSI6MCwi
Y3NvIjoiQ1NPX3ZhHVlIiwiZXhlIp7InBlcnNvbii6Ijg40DMwYTc1LTjk0GYtNGEzZS04NDflLTg5ZDh
10TI50GMYiIsInByb2ZpbGUoIjMjY2M0YmNlNC040DljLTRhNTctYjIwMS1h0WY2N2FhYzA3NjciLCJtZW
FucyI6W3sidHlwIjoibWvhbnNUeXBliiwiaWQiOjItZWFuc0lkIn1dLCJsb2Ei0jUsInR5cCI6ImN1c3Rvb
WVyiOsInB0eSI6ImNvb2tpZSiIsInB2ZSI6InNly3VyZV9yYW5kb21fdmFsdWUiLCJzaWQiOjKzTc3ZjY3
ZC00Y2U5LTQ4ZmYtODViZS1j0WjkYmVkJZWMiLCJ2ZXIiOiIxLjQiLCJqdGkiOjI4NzI4MTYwMi1LZDm
mLTrjNDAtOTg5Zi05YVvjZDA3YTjMzcilCJ0eXAiOjJhY2Nlc3MiLCJleHAIoje3NTkzNjg2NzYsIm5iZi
I6MTc10TMw0DY3NiwiawF0IjoxNzU5MzA4Njg1LCJpc3Mi0iJhcGkuZG9tYVluLmNvbSJ9.Jgx5zH6Pc85P
U_u657hS-mt6P0zk729WPxerxxtMCYkQxm20XiPlrMVSq9WBaHZNRR2HdTbVHPYdJM-
J7hbCgjdQ5i0xBFFdfsWLmn0PM9ZzMLvebzGFwfNOMXpr3r-
FfcfJaFemd_bYbYief3x9mS2RANEqN03RNnzsC75d75U0VZ0_VRCV65__GKHYzMuBHY2j0Go3uPriWEUhT
b2weGaVJ5JPPT80p7CFW0XF6oxW0AV-_7z0wUT7wCMRHRMvUPLYQut-6bFummLGeG_LCM9-
velWzLRoHWuG48mu_g00hhTxYkY0U4zHlpXezNgi3P9Rb7gFrbNIRnPv2rf7g
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
X-Ing-Request-Id: 11
Sec-Ch-Ua-Mobile: ?0

```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
Accept: application/json
Content-Type: application/json
Origin: https://localhost:1234
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://localhost:1234/swagger-ui/index.html
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
  "ingEntity": "string",
  "productType": "string",
  "cardPointerId": "OTZmZGRkNzAtOTA1Mi00NjlmLTk3NGEtNzQyMWIwZTU2Njk0"
}
```

Verbose Error Messages (/adapter05/card/details)

5. Informational Findings

An informational is an issue of interest that was discovered during the testing and was determined not to have direct implication for the level of security. An issue described as a note should be investigated as it might be the source of vulnerabilities in the future or should further information be revealed to an attacker.

5.1. Missing HTTP Strict-Transport-Security Header (23704)

INFO	Attack Vector:	Scope:
	Attack Complexity:	Confidentiality:
	Privileges Required:	Integrity:
	User Interaction:	Availability:

5.1.1. Assets

<https://localhost:1234/v1/>;
<https://sd80tssad12:8095/v1/>;

5.1.2. Description

During the test it has been discovered that server does not utilize HTTP Strict Transport policy. This feature introduces additional security layer for the HTTPS connections. For web applications using HSTS, browsers will be instructed to not perform attempts of unencrypted connections to particular domain even if they find URL-s for such. This feature also prevents the browser from allowing to ignore certificate warnings (like when self-signed certificate is detected).

5.1.3. Recommendation

Include HTTP Strict-Transport-Security-Header into each server's HTTP response.

5.1.4. Additional Information

5.1.5. Evidence

The HSTS Security header is missing from all APIs in scope.

Missing HSTS from Riba Administration API

```
[*] Analyzing headers of https://localhost:1234/v1/riba-admin/tech-services/health/check
[*] Effective URL: https://localhost:1234/v1/riba-admin/tech-services/health/check
[!] Missing security header: X-Content-Type-Options
[!] Missing security header: Strict-Transport-Security
[!] Missing security header: Content-Security-Policy

[*] No information disclosure headers detected
[*] No caching headers detected
[!] Headers analyzed for https://localhost:1234/v1/riba-admin/tech-services/health/check
[+] There are 0 security headers
[-] There are not 3 security headers
```

Missing HSTS from Current Account Selling Solution APIs

```
[*] Analyzing headers of https://127.0.0.1:1234/v1/current-account/solution-selling/techServices/healthCheck
[*] Effective URL: https://127.0.0.1:1234/v1/current-account/solution-selling/techServices/healthCheck
[!] Missing security header: X-Content-Type-Options
[!] Missing security header: Strict-Transport-Security
[!] Missing security header: Content-Security-Policy

[*] No information disclosure headers detected
[*] No caching headers detected
```

Missing HSTS header from Oracle Adapter Card APIs

```
[*] Analyzing headers of https://sd80tsssad12:8095/v1/oracle-card/health/check
[*] Effective URL: https://sd80tsssad12:8095/v1/oracle-card/health/check
[!] Missing security header: X-Content-Type-Options
[!] Missing security header: Strict-Transport-Security
[!] Missing security header: Content-Security-Policy

[*] No information disclosure headers detected
```

Missing HSTS from Debit Card Administration APIs

```
[*] Analyzing headers of https://localhost:1234/v1/debit-card/tech-services/health/check
[*] Effective URL: https://localhost:1234/v1/debit-card/tech-services/health/check
[!] Missing security header: X-Content-Type-Options
[!] Missing security header: Strict-Transport-Security
[!] Missing security header: Content-Security-Policy

[*] No information disclosure headers detected
```

5.2. Missing HTTP X-Content-Type-Options Header (29537)

INFO 0.0	Attack Vector: NETWORK	Scope: UNCHANGED
	Attack Complexity: HIGH	Confidentiality: NONE
	Privileges Required: LOW	Integrity: NONE
	User Interaction: NONE	Availability: NONE
CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:N/CR:M/IR:H/AR:H		

5.2.1. Assets

<https://localhost:1234/v1/>;

<https://sd80tsssd12:8095/v1/>;

5.2.2. Description

During the test it has been discovered that server does not utilize HTTP X-Content-Type-Options. The lack of this header causes that certain browser, try to determine the content type and encoding of the response even when these properties are defined correctly. This can make the web application vulnerable against Cross-Site Scripting (XSS) attacks.

5.2.3. Recommendation

Include HTTP X-Content-Type-Options Header with value nosniff into each server's HTTP response.

5.2.4. Additional Information

OWASP

https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html#x-content-type-options

5.2.5. Evidence

The X-Content-Type security header was missing from all APIs in scope.

Please note that the vulnerability has been classified as "Info", as per agreements, since the security header is missing only in test environment, but it is correctly configured in production one.

Missing X-Content-Type from Riba Administration API

```
[*] Analyzing headers of https://localhost:1234/v1/riba-admin/tech-services/health/check
[*] Effective URL: https://localhost:1234/v1/riba-admin/tech-services/health/check
[!] Missing security header: X-Content-Type-Options
[!] Missing security header: Strict-Transport-Security
[!] Missing security header: Content-Security-Policy

[*] No information disclosure headers detected
[*] No caching headers detected
[!] Headers analyzed for https://localhost:1234/v1/riba-admin/tech-services/health/check
[+] There are 0 security headers
[-] There are not 3 security headers
```

Missing X-Content-Type from Current Account Selling Solution APIs

```
[*] Analyzing headers of https://127.0.0.1:1234/v1/current-account/solution-selling/techServices/healthCheck
[*] Effective URL: https://127.0.0.1:1234/v1/current-account/solution-selling/techServices/healthCheck
[!] Missing security header: X-Content-Type-Options
[!] Missing security header: Strict-Transport-Security
[!] Missing security header: Content-Security-Policy

[*] No information disclosure headers detected
[*] No caching headers detected
```

Missing X-Content-Type from Oracle Adapter Card APIs

```
[*] Analyzing headers of https://sd80tsssad12:8095/v1/oracle-card/health/check
[*] Effective URL: https://sd80tsssad12:8095/v1/oracle-card/health/check
[!] Missing security header: X-Content-Type-Options
[!] Missing security header: Strict-Transport-Security
[!] Missing security header: Content-Security-Policy

[*] No information disclosure headers detected
```

Missing X-Content-Type from Debit Card Administration APIs

```
[*] Analyzing headers of https://localhost:1234/v1/debit-card/tech-services/health/check
[*] Effective URL: https://localhost:1234/v1/debit-card/tech-services/health/check
[!] Missing security header: X-Content-Type-Options
[!] Missing security header: Strict-Transport-Security
[!] Missing security header: Content-Security-Policy

[*] No information disclosure headers detected
```

5.3. Missing HTTP Content-Security-Policy Header (29538)

INFO 0.0	Attack Vector: NETWORK	Scope: UNCHANGED
	Attack Complexity: HIGH	Confidentiality: NONE
	Privileges Required: NONE	Integrity: NONE
	User Interaction: NONE	Availability: NONE
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:N/CR:M/IR:H/AR:H		

5.3.1. Assets

https://localhost:1234/v1/*;

https://sd80tsssd12:8095/v1/*;

5.3.2. Description

During the test it has been discovered that server does not utilize HTTP Content-Security-Policy. CSP is a browser security mechanism that aims to mitigate XSS and some other attacks. It works by restricting the resources that a page can load and restricting whether a page can be framed by other pages. To enable CSP, a response needs to include an HTTP response header called Content-Security-Policy with a value containing the policy. The policy itself consists of one or more directives, separated by semicolons.

5.3.3. Recommendation

Include HTTP Content-Security-Policy Header into each server's HTTP response.

5.3.4. Additional Information

OWASP

https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

5.3.5. Evidence

The CSP security header was missing from all APIs in scope.

Please note that the vulnerability has been classified as "Info", as per agreements, since the security header is missing only in test environment, but it is correctly configured in production one.

Missing CSP header from Riba Administration API

```
[*] Analyzing headers of https://localhost:1234/v1/riba-admin/tech-services/health/check
[*] Effective URL: https://localhost:1234/v1/riba-admin/tech-services/health/check
[!] Missing security header: X-Content-Type-Options
[!] Missing security header: Strict-Transport-Security
[!] Missing security header: Content-Security-Policy

[*] No information disclosure headers detected
[*] No caching headers detected
[!] Headers analyzed for https://localhost:1234/v1/riba-admin/tech-services/health/check
[+] There are 0 security headers
[-] There are not 3 security headers
```

Missing CSP from Current Account Solution Selling APIs

```
[*] Analyzing headers of https://127.0.0.1:1234/v1/current-account/solution-selling/techServices/healthCheck
[*] Effective URL: https://127.0.0.1:1234/v1/current-account/solution-selling/techServices/healthCheck
[!] Missing security header: X-Content-Type-Options
[!] Missing security header: Strict-Transport-Security
[!] Missing security header: Content-Security-Policy

[*] No information disclosure headers detected
[*] No caching headers detected
```

Missing CSP from Oracle Adapter Card APIs

```
[*] Analyzing headers of https://sd80tsssad12:8095/v1/oracle-card/health/check
[*] Effective URL: https://sd80tsssad12:8095/v1/oracle-card/health/check
[!] Missing security header: X-Content-Type-Options
[!] Missing security header: Strict-Transport-Security
[!] Missing security header: Content-Security-Policy

[*] No information disclosure headers detected
```

Missing CSP from Debit Card Administration APIs

```
[*] Analyzing headers of https://localhost:1234/v1/debit-card/tech-services/health/check
[*] Effective URL: https://localhost:1234/v1/debit-card/tech-services/health/check
[!] Missing security header: X-Content-Type-Options
[!] Missing security header: Strict-Transport-Security
[!] Missing security header: Content-Security-Policy

[*] No information disclosure headers detected
```

G. Appendixes

1. Testing Limitation - Missing Data

During the Penetration Testing activity, it was not possible to carry out a full assessment of certain API endpoints, as the data required to execute and validate the related functionalities was not available at the time of testing. This limitation prevented meaningful verification of security controls, such as authorization, input validation, on those specific endpoints.

In agreement with ING CISO team, these APIs have been tested using a black-box approach, due to the unavailability of data required to properly invoke them.

ITA Debit Card Administration API

- <https://localhost:1234/v1/debit-card/suspension>
- <https://localhost:1234/v1/debit-card/suspension/approved>
- <https://localhost:1234/v1/debit-card/restricted-detail>
- <https://localhost:1234/v1/debit-card/restricted-detail/approved>
- <https://localhost:1234/v1/debit-card/replacement/end-flow>
- <https://localhost:1234/v1/debit-card/reactivation>
- <https://localhost:1234/v1/debit-card/reactivation/approved>
- <https://localhost:1234/v1/debit-card/mastercard/3ds>
- <https://localhost:1234/v1/debit-card/mastercard/3ds/approved>
- <https://localhost:1234/v1/debit-card/limits/manage>
- <https://localhost:1234/v1/debit-card/limits/approved>
- <https://localhost:1234/v1/debit-card/geo-blocking/area/validation>
- <https://localhost:1234/v1/debit-card/geo-blocking/area/enable>
- <https://localhost:1234/v1/debit-card/geo-blocking/area/enable/approved>
- <https://localhost:1234/v1/debit-card/geo-blocking/area/disable>
- <https://localhost:1234/v1/debit-card/geo-blocking/area/disable/approved>
- <https://localhost:1234/v1/debit-card/change-pin>
- <https://localhost:1234/v1/debit-card/change-pin/approved>
- <https://localhost:1234/v1/debit-card/activation/end-flow>
- <https://localhost:1234/v1/debit-card/restricted-detail/status-data>
- <https://localhost:1234/v1/debit-card/request/{UUID}>
- <https://localhost:1234/v1/debit-card/replacement/start-flow>
- <https://localhost:1234/v1/debit-card/mastercard/3ds/info>
- <https://localhost:1234/v1/debit-card/limits>
- <https://localhost:1234/v1/debit-card/geo-blocking>
- <https://localhost:1234/v1/debit-card/geo-blocking/pricing/info>
- <https://localhost:1234/v1/debit-card/details>
- <https://localhost:1234/v1/debit-card/assisted/{productUUID}/details>

ITA Oracle Adapter Card API

- https://sd80tsssad12:8095/v1/oracle-card/req_request/insert
- https://sd80tsssad12:8095/v1/oracle-card/mobile_tvn
- https://sd80tsssad12:8095/v1/oracle-card/mobile_token
- https://sd80tsssad12:8095/v1/oracle-card/mobile_tcn
- <https://sd80tsssad12:8095/v1/oracle-card/contract/insert>
- https://sd80tsssad12:8095/v1/oracle-card/ba_cards_property/update_property_value
- https://sd80tsssad12:8095/v1/oracle-card/ba_cards/prepaid/recharge/insert
- https://sd80tsssad12:8095/v1/oracle-card/ba_cards/lookup
- https://sd80tsssad12:8095/v1/oracle-card/ba_cards/insert
- https://sd80tsssad12:8095/v1/oracle-card/req_request/update
- <https://sd80tsssad12:8095/v1/oracle-card/products/{productId}/update>
- https://sd80tsssad12:8095/v1/oracle-card/mobile_token/{correlationId}
- <https://sd80tsssad12:8095/v1/oracle-card/coownership>
- https://sd80tsssad12:8095/v1/oracle-card/cdc_installment_plans_name
- https://sd80tsssad12:8095/v1/oracle-card/ba_cards_services/{cardId}
- https://sd80tsssad12:8095/v1/oracle-card/ba_cards/{cardId}/update
- https://sd80tsssad12:8095/v1/oracle-card/req_request
- https://sd80tsssad12:8095/v1/oracle-card/req_request/{requestId}/req_item_kits
- https://sd80tsssad12:8095/v1/oracle-card/req_request/{requestId}/req_item_cards
- https://sd80tsssad12:8095/v1/oracle-card/mobile_tar
- https://sd80tsssad12:8095/v1/oracle-card/ba_overdraft_blocks
- https://sd80tsssad12:8095/v1/oracle-card/ba_cards_property/{cardId}
- https://sd80tsssad12:8095/v1/oracle-card/ba_cards
- https://sd80tsssad12:8095/v1/oracle-card/ba_cards/{productId}/read
- https://sd80tsssad12:8095/v1/oracle-card/ba_cards/prepaid/recharge/{cardId}

ITA Payment Administrator API

- </v1/internal/payments/order-preview>
- </v1/payments/delete/operations>
- </v1/payments/delete/sepa>
- </v1/payments/delete/giro/{paymentId}>

ITA WalletDebitCard API

- </v2/adapter06/card/list>
- </adapter06/card/details>
- </adapter06/card/digitizable>
- </adapter06/card/partyinfo>
- </adapter06/card/notify>
- </adapter06/card/digitizable>

ITA WalletCreditCard API

- /adapter05/card/partyinfo
- /adapter05/card/details
- /adapter05/card/notify
- /v2/adapter05/card/list
- /adapter06/card/digitizable
- /adapter05/card/{digitizedCardId}

2. Rules of Engagement

- All testing activities are in line with Vulnerability Management PCS v1.0, Global Security Testing Strategy and underlying documents.
- All tests are conducted in 8-18 - ING Business Hours.
- Targeted environment should be stable, no changes allowed during the penetration test.
- As a part of penetration test, dynamic scan (DAST) against application will be executed. Please be aware that due the nature of such scan some data may be saved on the underlying database. It's strongly recommended to perform backup.
- There is no specific scenario to achieved for penetration test. Offensive Cyber Security team adopted the best industry standards of testing like OWASP and worked out own techniques and methodologies based on own experiences from other penetration testing services delivered already to other ING Business Units.
- During the penetration test no changes in the targeted system configuration will be done.
- Data related to the penetration test are not stored on the pentester's laptops. Report is uploaded to the SHP and deleted after 1 year (due the data retention).
- Penetration test reports do not describe risk levels, only technical severity. Residual risk should be assessed by ING (asset owner or delegate).
- The AO, representative IT-C, has confirmed that the test/acceptance environment and the production environment are sufficiently identical in security-related aspects to ensure a meaningful penetration test.
- All web application roles need to be tested, to do so all roles/permissions should to be added to the separate accounts.

3. Original request

```
{  
  "spocEmails": [  
    "stefano.cascella@ing.com",  
    "teresa.giuseffi@ing.com"  
,  
  "assetOwnerEmail": "Matthias.Neuner@ing.com",  
  "firstLoDOfficerEmail": [  
    "edvin.jazaj@ing.com"  
,  
  "typeOfTarget": [  
    "Web API",  
    "Infrastructure"  
,  
  "webApplicationDetails": null,  
  "webApiDetails": {  
    "documentationUrl": "A Postman collection file that contains raw HTTP requests  
for all endpoints, with required headers and sample valid testing data.",  
    "methodology": "Gray Box",  
    "roles": [  
      "ask to:\nL. Roscini\nT. Giuseffi\nS. Cascella\nA. Mangoni\nM. Rigiroli\nV.P.  
Montaruli\n"  
,  
    "scopeRemarks": null,
```

```

        "url": "/v1/payments/iban/validation; /v1/internal/payments/order-preview;
/v1/internal/payments/{accountNumber}/receipt; /v1/payments/delete/operations;
/v1/payments/delete/sepa;
/v1/payments/delete/giro/{paymentId}\n/v1/limitations/technical-
services/health/check; /v3/limitations/limitations/{businessFunctionType};
/v1/internal/limitations/{businessFunctionType};
/v1/limitations/user/threshold\n/v1/domestic-payments/technical-
services/health/check\n\"Tutti gli endpoint menzionati a questo
link:\nhttps://touchpoint.ing.net/asm/resources/OpenApiDocument/ITA_OracleAdapterPr
icing_API?itProduct=P10905\"\n\"Tutti gli endpoint menzionati a questo
link:\nhttps://touchpoint.ing.net/asm/resources/OpenApiDocument/ITA_Profile7Adapter
PaymentAdministration_API?itProduct=P10905\"\n\"Tutti gli endpoint menzionati a
questo
link:\nhttps://touchpoint.ing.net/asm/resources/OpenApiDocument/ITA_Profile7Adapter
Restrictions_API?itProduct=P10905\"\n\"Tutti gli endpoint menzionati a questo
link:\nhttps://touchpoint.ing.net/asm/resources/OpenApiDocument/ITA_ThirdPartyAdapt
er_API?itProduct=P10905\"\n\"Tutti gli endpoint menzionati a questo
link:\nhttps://touchpoint.ing.net/asm/resources/OpenApiDocument/ITA_Profile7Adapter
CurrentAccount_API?itProduct=P10905\"\n\"Tutti gli endpoint menzionati a questo
link:\nhttps://touchpoint.ing.net/asm/resources/OpenApiDocument/ITA_OracleAdapterCa
rd_API?itProduct=P10905\"\n\"Tutti gli endpoint menzionati a questo
link:\nhttps://touchpoint.ing.net/asm/resources/OpenApiDocument/ITA_OracleAdapterPa
ymentAdministration_API?itProduct=P10905\"\n\"Tutti gli endpoint menzionati a
questo
link:\nhttps://touchpoint.ing.net/asm/resources/OpenApiDocument/ITA_Profile7Adapter
Order_API?itProduct=P10905\"\n\"Tutti gli endpoint menzionati a questo
link:\nhttps://touchpoint.ing.net/asm/resources/OpenApiDocument/ITA_WalletCreditCar
d_API?itProduct=P10905\"\n\"Tutti gli endpoint menzionati a questo
link:\nhttps://touchpoint.ing.net/asm/resources/OpenApiDocument/ITA_WalletDebitCard
_API?itProduct=P10905\"\n\"Tutti gli endpoint menzionati a questo
link:\nhttps://touchpoint.ing.net/asm/resources/OpenApiDocument/ITA_WalletPrepaidCa
rd_API?itProduct=P10905\"\n\"Tutti gli endpoint menzionati a questo
link:\nhttps://touchpoint.ing.net/asm/resources/OpenApiDocument/ITA_Tax_Engine_API?
itProduct=P10905\"\n\"Tutti gli endpoint menzionati a questo
link:\nhttps://touchpoint.ing.net/asm/resources/OpenApiDocument/ITA_AccountSwitchMa
nager_API?itProduct=P10905\"\n\"Tutti gli endpoint menzionati a questo
link:\nhttps://touchpoint.ing.net/asm/resources/OpenApiDocument/ITA_RiBa_API?
itProduct=P10905\"\n"
},
"androidApplicationDetails": null,
"iosApplicationDetails": null,
"thickClientDetails": null,
"infrastructureDetails": {
    "excludedProductionHosts": null,
    "excludedProductionHostsJustification": null,
    "excludedSecondaryTestingEnvironmentHosts": null,
    "excludedSecondaryTestingEnvironmentHostsJustification": null,
    "methodology": "Gray Box",
    "scopeRemarks": "ACC IP
addresses:\nsd80tsadpt12\nsd80tsssad01\nsd80tsssad02\nsd80tsssad11\nsd80tsssad12\nP
RD IP addresses:\n- \n- \nAdditional remarks:\n- "
}

```

}

END OF REPORT