IT BANK - ITA DAILYBANKING API

Dynamic Pentest Report

CISO/ASM/CYBER OFFSEC COE

A. Document Information

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

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	Target: • 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 Methodology: GRAYBOX Facing: INTERNAL	3	4	4

IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	Target: • 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 Methodology: GRAYBOX Facing: INTERNAL	3	4	4

IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	Target: • https://localhost:1234/v1/debit-card/action/{UUID}/status Methodology: GRAYBOX Facing: INTERNAL	3	4	4
IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	Target: • 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 Methodology: GRAYBOX Facing: INTERNAL	3	4	4

IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	Target: • https://sd80tsssad12:8095/v1/oracle-card/scoring/{scoringId} • 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/health/check • https://sd80tsssad12:8095/v1/oracle-card/cdc_installment_plans • 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/{personId}/search • https://sd80tsssad12:8095/v1/oracle-card/ba_cards/prepaid/recharge/{cardId} Methodology: GRAYBOX Facing: INTERNAL	3	4	4

IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	Target: • 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 Methodology: GRAYBOX Facing: INTERNAL	3	4	4

IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	Target: • 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} Methodology: GRAYBOX Facing: INTERNAL	3	4	4
IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	Target: • /v1/riba-admin/tech-services/health/check Methodology: GRAYBOX Facing: INTERNAL	3	4	4
IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	Target: • /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 Methodology: GRAYBOX Facing: INTERNAL	3	4	4

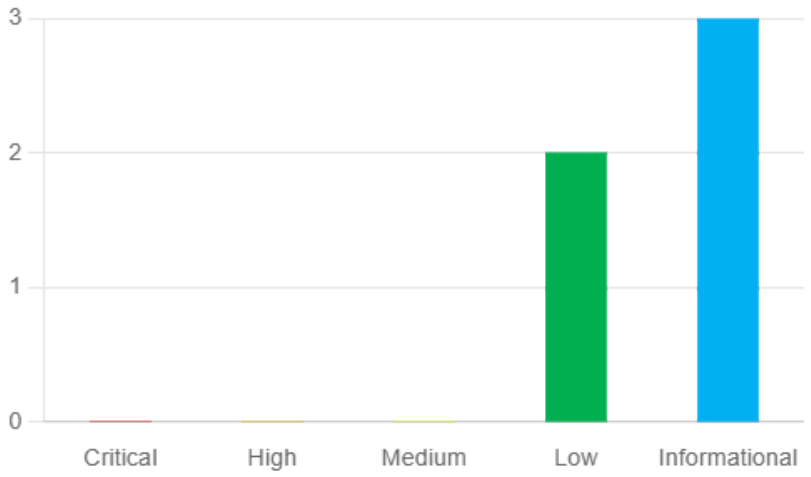
IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	Target: • /adapter05/card/phonenumber/{party-uuid} • /adapter05/card/{digitizedCardId} • /adapter05/tech-services/health/check • /adapter05/tech-services/keepalive • /v2/adapter05/card/list • /adapter05/card/details • /adapter05/card/digitizable • /adapter05/card/notify • /adapter05/card/partyinfo Methodology: GRAYBOX Facing: INTERNAL	3	4	4
IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	Target: • /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 Methodology: GRAYBOX Facing: INTERNAL	3	4	4
IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	Target: • /v1/domestic-payments/technical-services/health/check Methodology: GRAYBOX Facing: INTERNAL	3	4	4

IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	Target: • /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 Methodology: GRAYBOX Facing: INTERNAL	3	4	4
IT BANK - ITA DAILYBANKING API TST	02.09.2025 - 08.09.2025	Target: • /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) Methodology: GRAYBOX Facing: INTERNAL	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/card/details; /adapter05/card/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://localhost:1234/v1/; https://sd80tsssad12:8095/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	Recommendation	Status
F 4.1 Offsec: 30612	LOW **3.7**	/adapter05/card/phonenumber/{party-uuid}; /adapter06/card/phonenumber/{party-uuid}; /v1/payments/iban/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://localhost:1234/v1/; https://sd80tsssad12:8095/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://localhost:1234/v1/*; https://sd80tsssad12:8095/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.

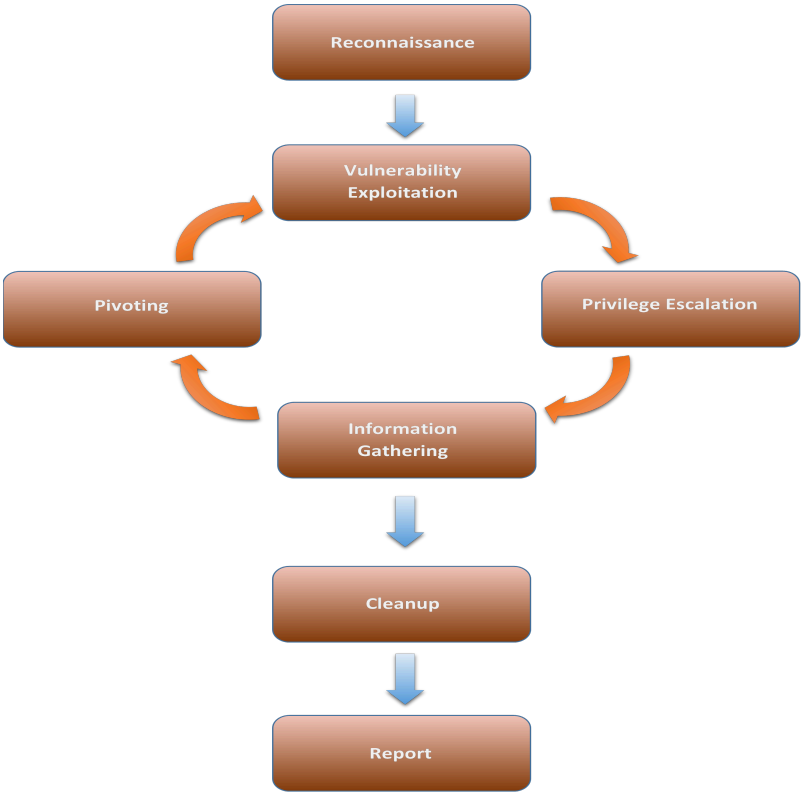
Offensive Cyber Security team uses the following main methodologies depending on the requirements:

- **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 past 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 disclosure 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	• Initial calls with the Customer • Initial exchange of required information
Testing	• Information gathering • Scanning, vulnerability assessment • Manual testing of components • Exploitation of findings
Reporting (Draft)	• Draft report • Draft presentation
Finalization of the report	• Amendments • Retesting if required (in case of errors or Customer's remarks)
Final report	• Final report and presentation
Remediation support	• Support with remediation process
Retesting	• 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/phonenumber/{party-uuid};

/adapter06/card/phonenumber/{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

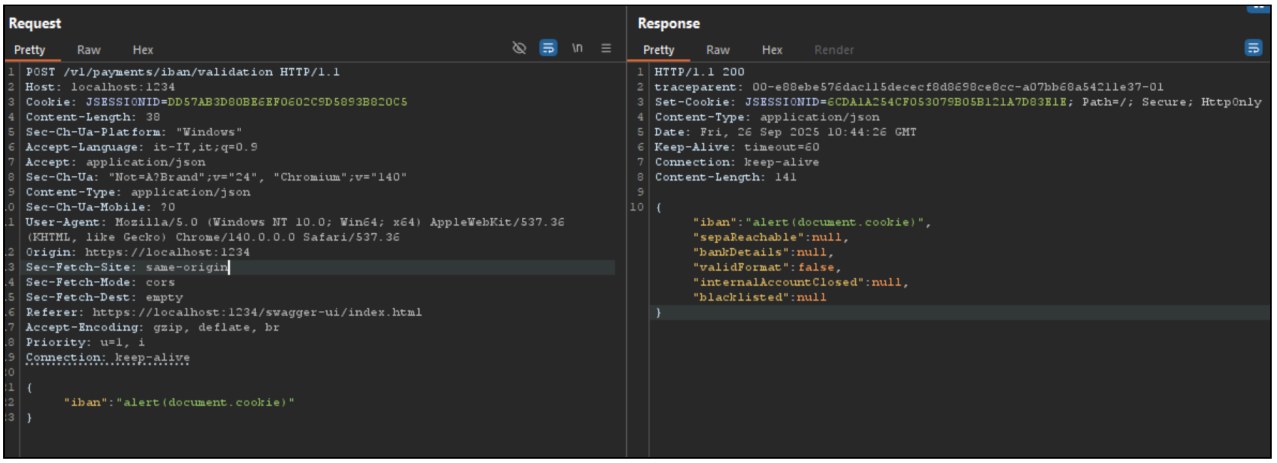
The tested endpoints do not enforce proper input validation on several parameters.

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.

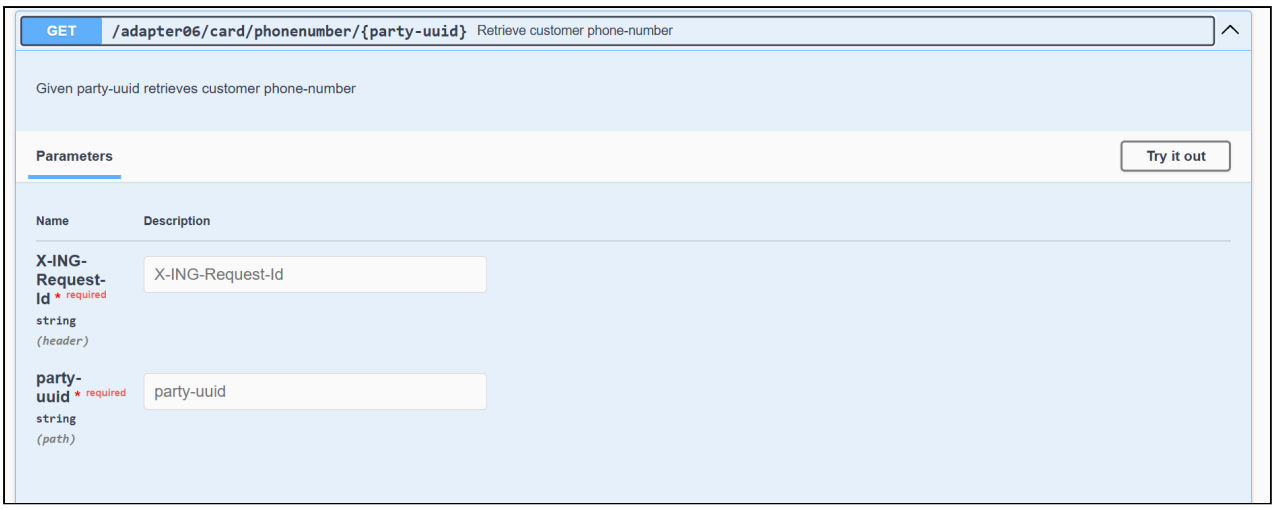
```
POST /v1/payments/iban/validation HTTP/1.1
Host: localhost:1234
Cookie: JSESSIONID=DD57AB3D80BE6EF0602C9D5893B820C5
Content-Length: 38
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: it-IT,it;q=0.9
Accept: application/json
Sec-Ch-Ua: "Not=A?Brand";v="24", "Chromium";v="140"
Content-Type: application/json
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)



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}.

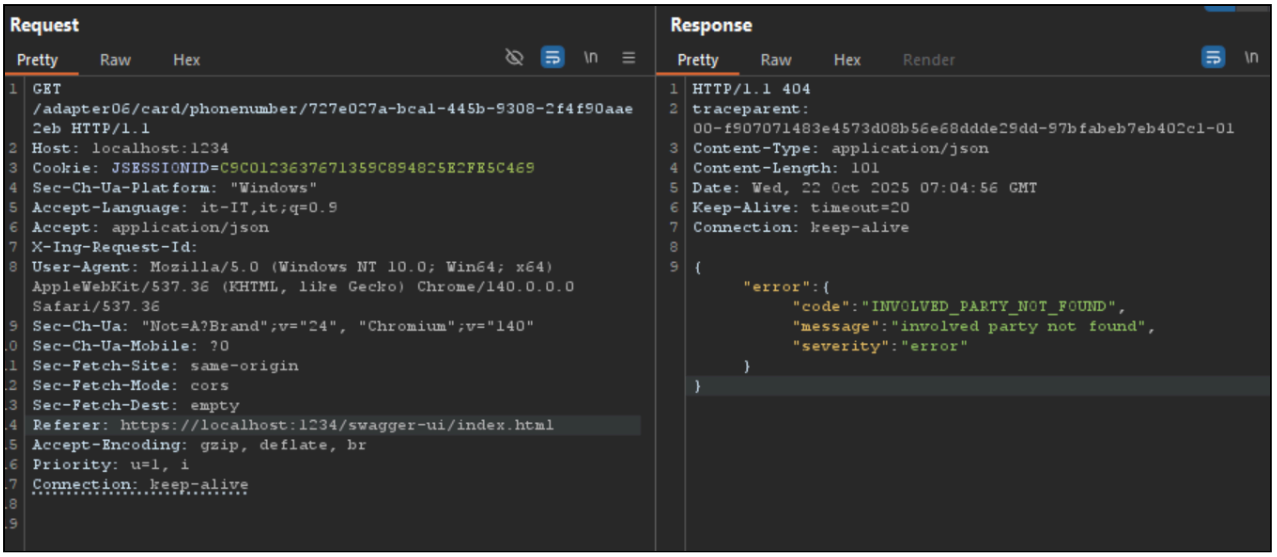
Required header X-ING-Request-Id



Even if the header is marked as required value, it is possible to perfom 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})



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://sd80tsssad12:8095/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

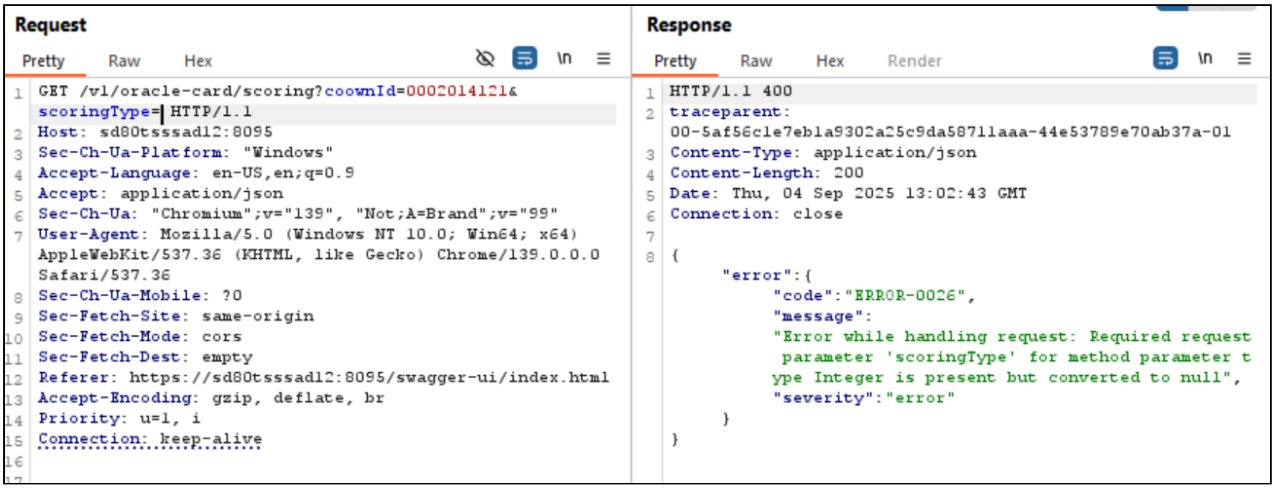
Verbose errors should not be provided to end users. Friendly static error pages should be provided instead. Error cause should be investigated within the code.

4.2.4. Additional Information

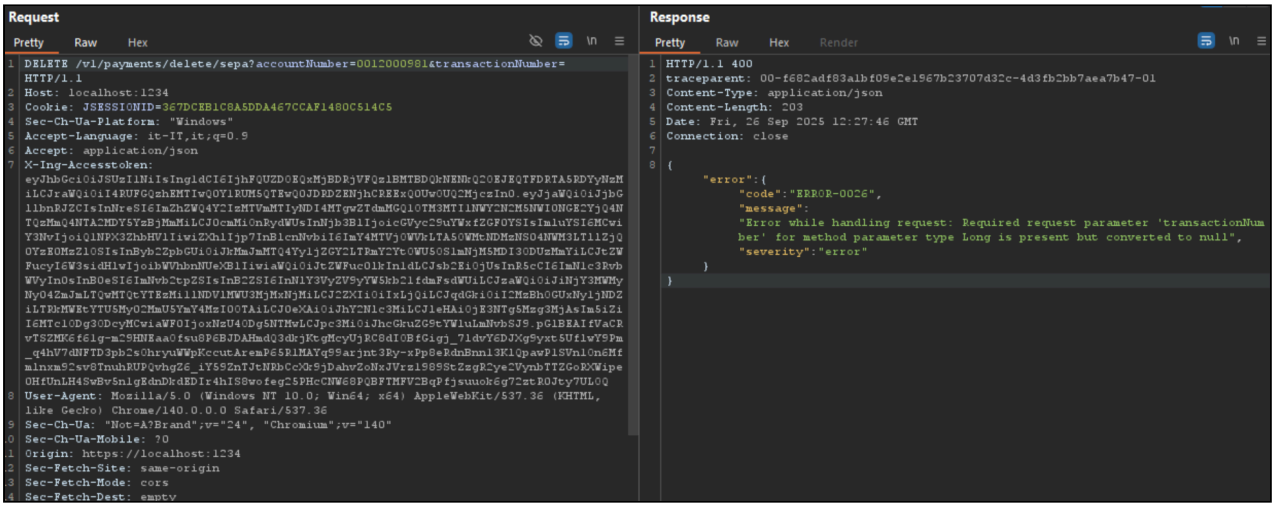
4.2.5. Evidence

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)



Verbose Error Messages (/v1/payments/delete/sepa)



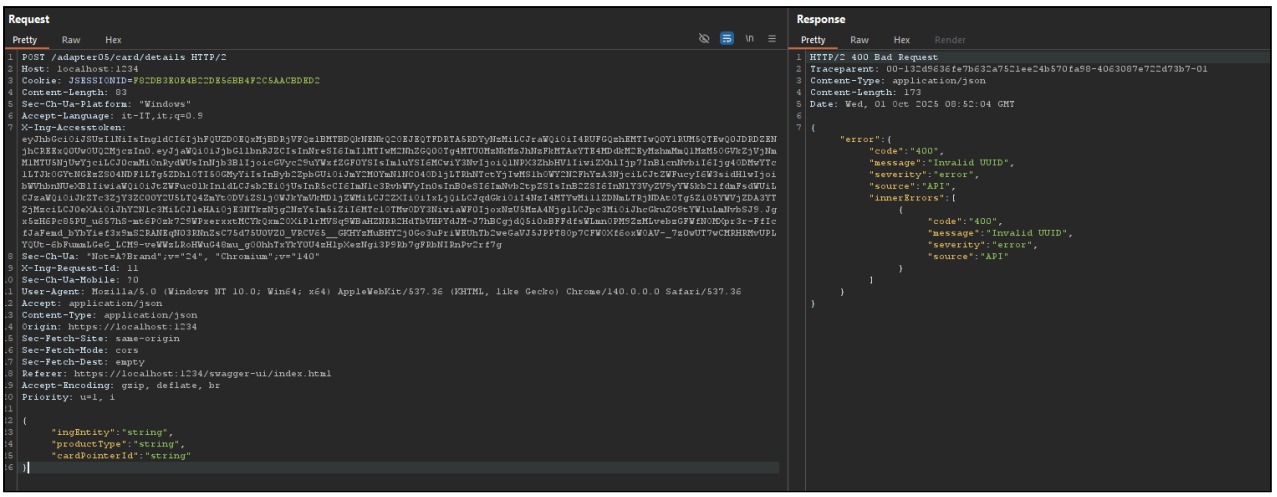
The evidence below shows that response returned allowed the attacker to reconstruct part of the request based on message error.

1. The inizial request sent with generic string value allowed to discover that one of the parameter must be an UUID
2. Once inserted in cardPointerId a generic UUID, the response reveals that the id should be encoded in base64
3. Based on the analysed responses, the last request was performed by passing an encoded UUID in the cardPointerId parameter and - as a result - the problems related on it value were solved.

```
POST /adapter05/card/details HTTP/2
Host: localhost:1234
Cookie: JSESSIONID=F82DB3E0E4B22DE56BB4F2C5AACBDED2
Content-Length: 83
```

```
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: it-IT,it;q=0.9
X-Ing-Accesstoken:
eyJhbGciOiJSUzI1NiIsIng1dCI6IjhFQUZDOEQxMjBDRjVFQzlBMTBDQkNENkQ2OEJEQTFDRTA5RDYyNzM
iLCJraWQiOiI4RUFGQzhEMTIwQ0Y1RUM5QTEwQ0JDRDZENjhCREExQ0UwOUQ2MjczIn0.eyJjaWQiOiJjbG
llbnRJZCIsInNreSI6ImI1MTIwM2NhZGQ0OTg4MTU0MzNkMzJhNzFkMTAxYTE4MDdkM2EyMzhmMmQ1MzM5O
GVkZjVjNmM1MTU5NjUwYjciLCJ0cmMiOnRydWUsInNjb3BlIjoicGVyc29uYWxfZGF0YSIsImluYSI6MCwi
Y3NvIjoiQ1NPX3ZhbHVlIiwiZXhlIjp7InBlcnNvbiI6Ijg4ODMwYTc1LTJkOGYtNGEzZS04NDFlLTg5ZDh
lOTI5OGMyYiIsInByb2ZpbGUiOiJmY2M0YmNlNC04ODljLTRhNTctYjIwMS1hOWY2N2FhYzA3NjciLCJtZW
FucyI6W3sidHlwIjoibWVhbnNUeXBlIiwiaWQiOiJtZWFuc0lkIn1dLCJsb2EiOjUsInR5cCI6ImN1c3Rvb
WVyIn0sInB0eSI6ImNvb2tpZSIsInB2ZSI6InNlY3VyZV9yYW5kb21fdmFsdWUiLCJzaWQiOiJkZTc3ZjY3
ZC00Y2U5LTQ4ZmYtODViZS1jOWJkYmVkMDljZWMiLCJ2ZXIiOiIxLjQiLCJqdGkiOiI4NzI4MTYwMi1lZDN
mLTRjNDAtOTg5Zi05YWVjZDA3YTZjMzciLCJ0eXAiOiJhY2Nlc3MiLCJleHAiOjE3NTkzNjg2NzYsIm5iZi
I6MTc1OTMwODY3NiwiaWF0IjoxNzU5MzA4Njg1LCJpc3MiOiJhcGkuZG9tYWluLmNvbSJ9.Jgx5zH6Pc85P
U_u657hS-mt6POzk729WPxerxxtMCYkQxm2OXiPlrMVSq9WBaHZNRR2HdTbVHPYdJM-
J7hBCgjdQ5i0xBFFdfsWLmnOPM9ZzMLvebzGFWfNOMXpr3r-
FfIcfJaFemd_bYbYief3x9mS2RANEqN03RNnZsC75d75U0VZ0_VRCV65__GKHYzMuBHY2j0Go3uPriWEUhT
b2weGaVJ5JPPT8Op7CFWOXf6oxWOAV-_7z0wUT7wCMRHRMvUPLYQUt-6bFummLGeG_LCM9-
veWWzLRoHWuG48mu_gO0hhTxYkY0U4zHlpXezNgi3P9Rb7gFRbNIRnPv2rf7g
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"
}
```

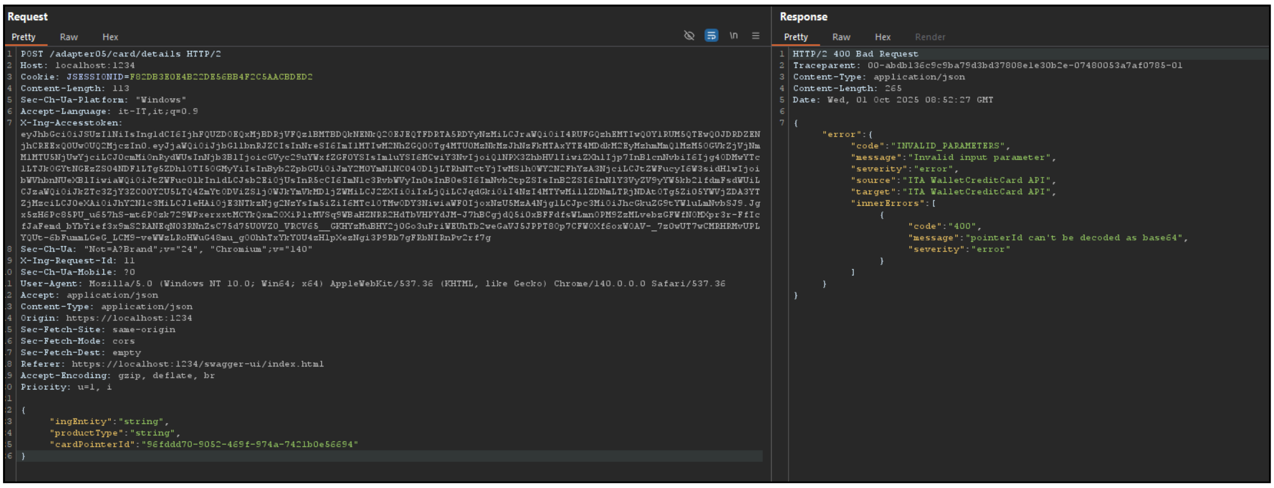
Verbose Error Messages (/adapter05/card/details): UUID type missing




```
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:
eyJhbGciOiJSUzI1NiIsIng1dCI6IjhFQUZDOEQxMjBDRjVFQzlBMTBDQkNENkQ2OEJEQTFDRTA5RDYyNzM
iLCJraWQiOiI4RUFGQzhEMTIwQ0Y1RUM5QTEwQ0JDRDZENjhCREExQ0UwOUQ2MjczIn0.eyJjaWQiOiJjbG
llbnRJZCIsInNreSI6ImI1MTIwM2NhZGQ0OTg4MTU0MzNkMzJhNzFkMTAxYTE4MDdkM2EyMzhmMmQ1MzM5O
GVkZjVjNmM1MTU5NjUwYjciLCJ0cmMiOnRydWUsInNjb3BlIjoicGVyc29uYWxfZGF0YSIsImluYSI6MCwi
Y3NvIjoiQ1NPX3ZhbHVlIiwiZXhlIjp7InBlcnNvbiI6Ijg4ODMwYTc1LTJkOGYtNGEzZS04NDFlLTg5ZDh
lOTI5OGMyYiIsInByb2ZpbGUiOiJmY2M0YmNlNC04ODljLTRhNTctYjIwMS1hOWY2N2FhYzA3NjciLCJtZW
FucyI6W3sidHlwIjoibWVhbnNUeXBlIiwiaWQiOiJtZWFuc0lkIn1dLCJsb2EiOjUsInR5cCI6ImN1c3Rvb
WVyIn0sInB0eSI6ImNvb2tpZSIsInB2ZSI6InNlY3VyZV9yYW5kb21fdmFsdWUiLCJzaWQiOiJkZTc3ZjY3
ZC00Y2U5LTQ4ZmYtODViZS1jOWJkYmVkMDljZWMiLCJ2ZXIiOiIxLjQiLCJqdGkiOiI4NzI4MTYwMi1lZDN
mLTRjNDAtOTg5Zi05YWVjZDA3YTZjMzciLCJ0eXAiOiJhY2Nlc3MiLCJleHAiOjE3NTkzNjg2NzYsIm5iZi
I6MTc1OTMwODY3NiwiaWF0IjoxNzU5MzA4Njg1LCJpc3MiOiJhcGkuZG9tYWluLmNvbSJ9.Jgx5zH6Pc85P
U_u657hS-mt6POzk729WPxerxxtMCYkQxm2OXiPlrMVSq9WBaHZNRR2HdTbVHPYdJM-
J7hBCgjdQ5i0xBFFdfsWLmnOPM9ZzMLvebzGFWfNOMXpr3r-
FfIcfJaFemd_bYbYief3x9mS2RANEqN03RNnZsC75d75U0VZ0_VRCV65__GKHYzMuBHY2j0Go3uPriWEUhT
b2weGaVJ5JPPT8Op7CFWOXf6oxWOAV-_7z0wUT7wCMRHRMvUPLYQUt-6bFummLGeG_LCM9-
veWWzLRoHWuG48mu_gO0hhTxYkY0U4zHlpXezNgi3P9Rb7gFRbNIRnPv2rf7g
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"
}
```

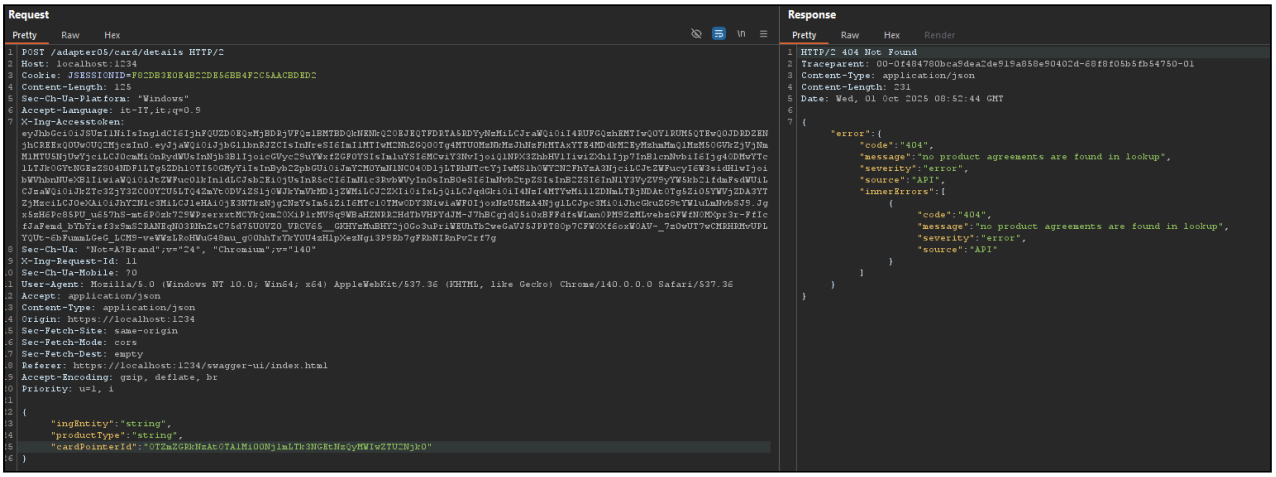
Verbose Error Messages (/adapter05/card/details): base64 encoding missing




```
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:
eyJhbGciOiJSUzI1NiIsIng1dCI6IjhFQUZDOEQxMjBDRjVFQzlBMTBDQkNENkQ2OEJEQTFDRTA5RDYyNzM
iLCJraWQiOiI4RUFGQzhEMTIwQ0Y1RUM5QTEwQ0JDRDZENjhCREExQ0UwOUQ2MjczIn0.eyJjaWQiOiJjbG
llbnRJZCIsInNreSI6ImI1MTIwM2NhZGQ0OTg4MTU0MzNkMzJhNzFkMTAxYTE4MDdkM2EyMzhmMmQ1MzM5O
GVkZjVjNmM1MTU5NjUwYjciLCJ0cmMiOnRydWUsInNjb3BlIjoicGVyc29uYWxfZGF0YSIsImluYSI6MCwi
Y3NvIjoiQ1NPX3ZhbHVlIiwiZXhlIjp7InBlcnNvbiI6Ijg4ODMwYTc1LTJkOGYtNGEzZS04NDFlLTg5ZDh
lOTI5OGMyYiIsInByb2ZpbGUiOiJmY2M0YmNlNC04ODljLTRhNTctYjIwMS1hOWY2N2FhYzA3NjciLCJtZW
FucyI6W3sidHlwIjoibWVhbnNUeXBlIiwiaWQiOiJtZWFuc0lkIn1dLCJsb2EiOjUsInR5cCI6ImN1c3Rvb
WVyIn0sInB0eSI6ImNvb2tpZSIsInB2ZSI6InNlY3VyZV9yYW5kb21fdmFsdWUiLCJzaWQiOiJkZTc3ZjY3
ZC00Y2U5LTQ4ZmYtODViZS1jOWJkYmVkMDljZWMiLCJ2ZXIiOiIxLjQiLCJqdGkiOiI4NzI4MTYwMi1lZDN
mLTRjNDAtOTg5Zi05YWVjZDA3YTZjMzciLCJ0eXAiOiJhY2Nlc3MiLCJleHAiOjE3NTkzNjg2NzYsIm5iZi
I6MTc1OTMwODY3NiwiaWF0IjoxNzU5MzA4Njg1LCJpc3MiOiJhcGkuZG9tYWluLmNvbSJ9.Jgx5zH6Pc85P
U_u657hS-mt6POzk729WPxerxxtMCYkQxm2OXiPlrMVSq9WBaHZNRR2HdTbVHPYdJM-
J7hBCgjdQ5i0xBFFdfsWLmnOPM9ZzMLvebzGFWfNOMXpr3r-
FfIcfJaFemd_bYbYief3x9mS2RANEqN03RNnZsC75d75U0VZ0_VRCV65__GKHYzMuBHY2j0Go3uPriWEUhT
b2weGaVJ5JPPT8Op7CFWOXf6oxWOAV-_7z0wUT7wCMRHRMvUPLYQUt-6bFummLGeG_LCM9-
veWWzLRoHWuG48mu_gO0hhTxYkY0U4zHlpXezNgi3P9Rb7gFRbNIRnPv2rf7g
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: Attack Complexity: Privileges Required: User Interaction:	Scope: Confidentiality: Integrity: Availability:

5.1.1. Assets

https://localhost:1234/v1/;
https://sd80tsssad12:8095/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://sd80tsssad12:8095/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

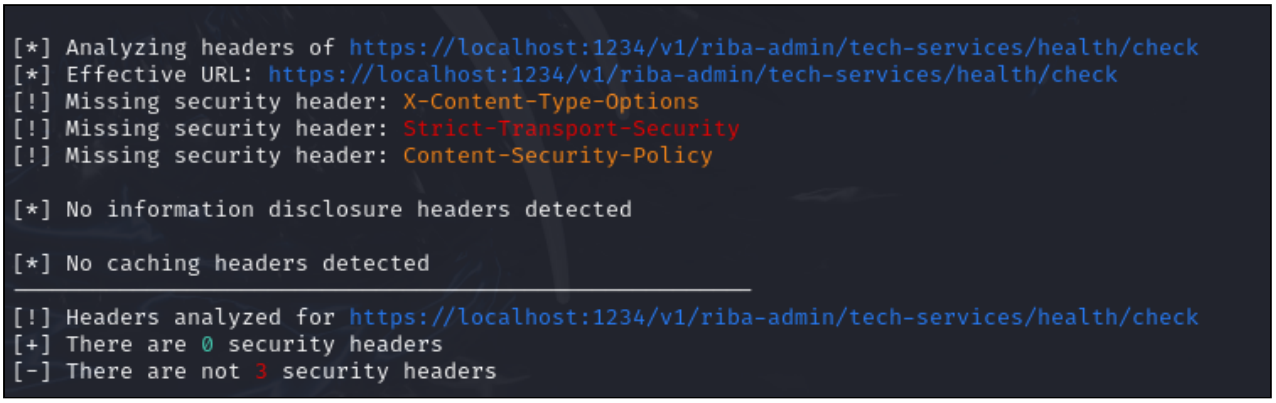
https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html#x-content-type-options

5.2.5. Evidence

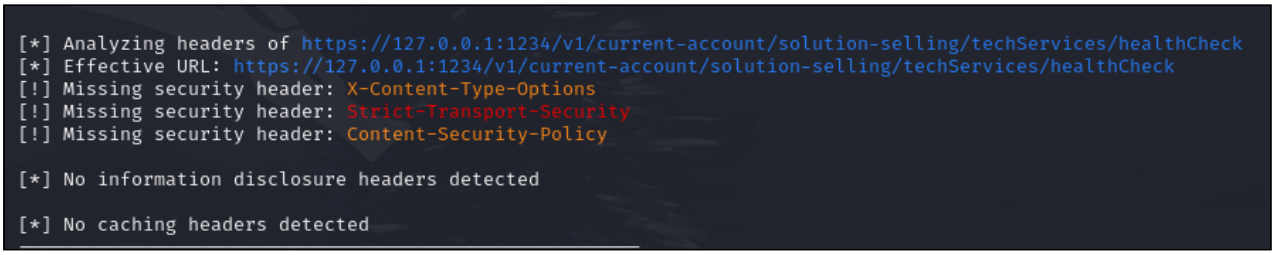
The X-Content-Type security header was missing from all APIs in scope.

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 correctely configured in production one.

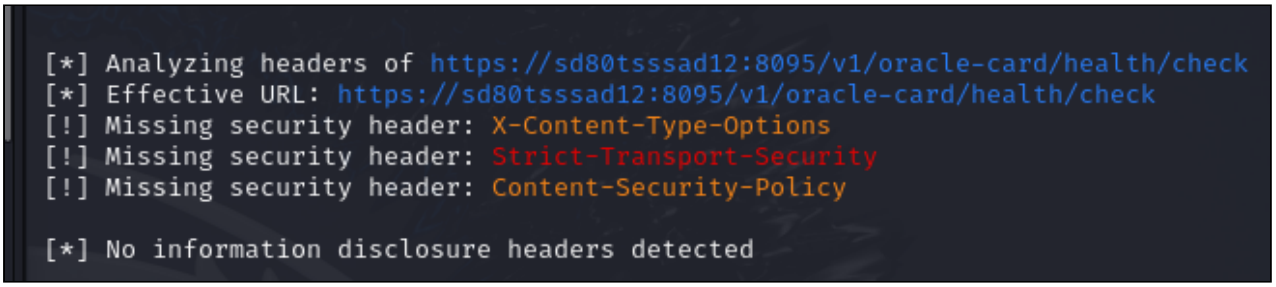
Missing X-Content-Type from Riba Administration API



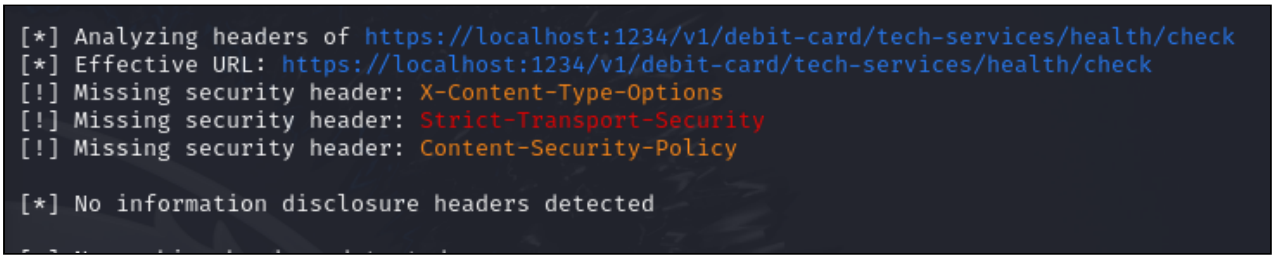
Missing X-Content-Type from Current Account Selling Solution APIs



Missing X-Content-Type from Oracle Adapter Card APIs



Missing X-Content-Type from Debit Card Administration APIs



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://sd80tsssad12:8095/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

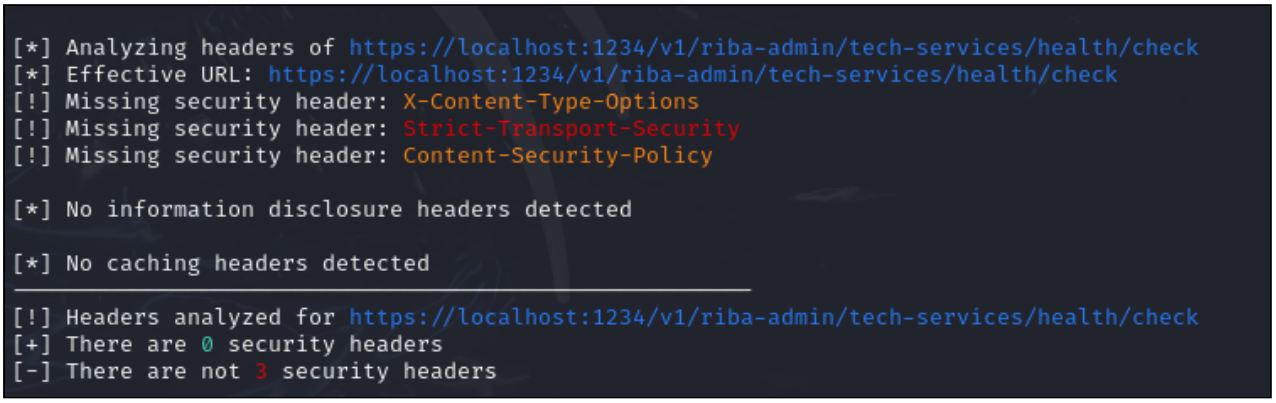
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

5.3.5. Evidence

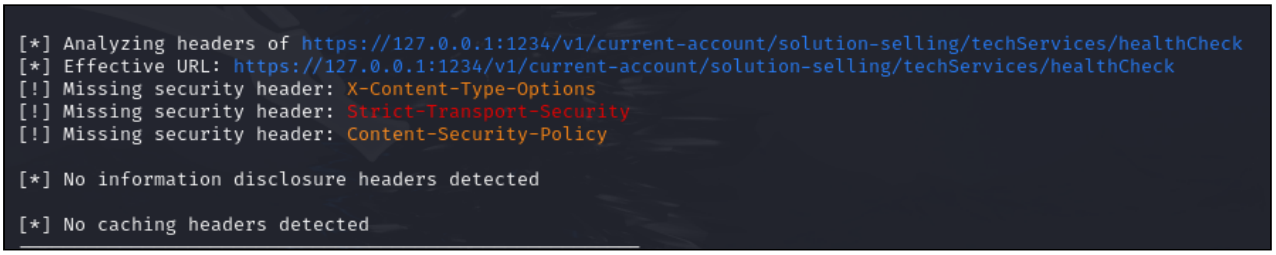
The CSP security header was missing from all APIs in scope.

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 correctely configured in production one.

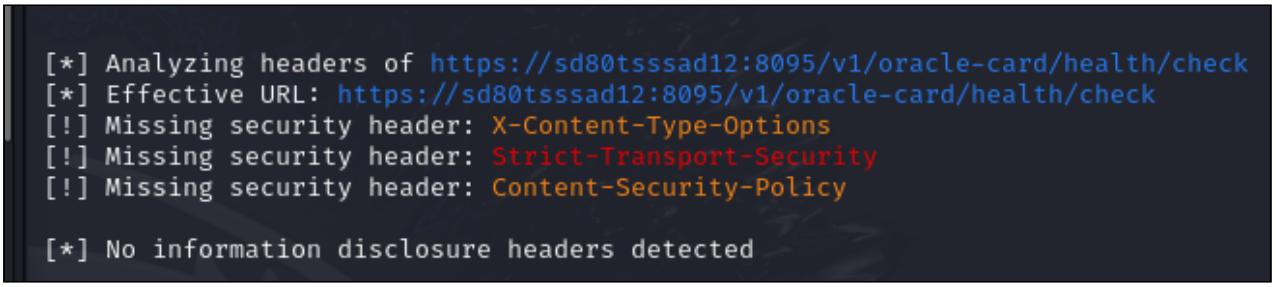
Missing CSP header from Riba Administration API



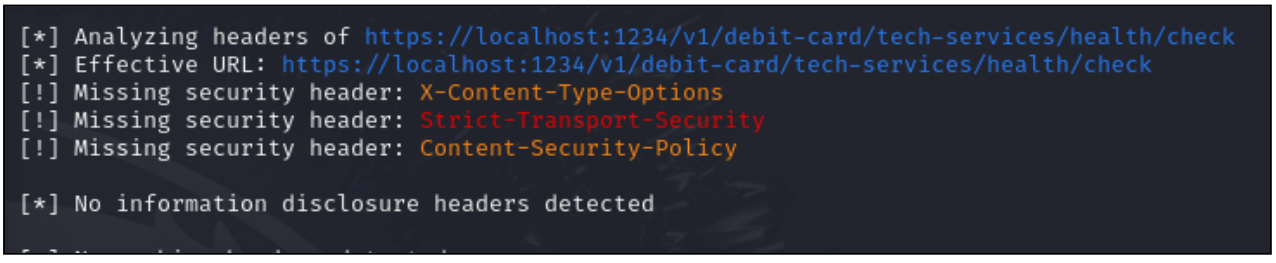
Missing CSP from Current Account Solution Selling APIs



Missing CSP from Oracle Adapter Card APIs



Missing CSP from Debit Card Administration APIs



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