IT BANK - FakeAsset

Penetration Test Report

CISO/ASM/CYBER OFFSEC COE

A. Document Information

Responsible department	CISO/ASM/CYBER OFFSEC COE
Report owner	()
Pentesters	faketester@ing.fake (1FAKE2)
Last update date	30.01.2026
Version	1.3
Version status	Draft

1. Version History

Version	Date	Author	Status	Note
0.1	27.01.2026	fakeautor@ing.fake	Statement of Work	—
1.0	27.01.2026	fakeautor@ing.fake	Draft	—
1.1	27.01.2026	fakeautor@ing.fake	Draft	—
1.2	30.01.2026	fakeautor@ing.fake	Draft	—
1.3	30.01.2026	fakeauthor@ing.fake	QA	—

B. Table of Contents

C. Executive Summary

1. Overview

Offensive Cyber Security team was tasked to perform Penetration Test against IT BANK - FakeAsset. The security assessment was conducted over the period - .

During the assessment no risk was identified.Following risks were identified during previous assesments:

- Critical: 1
- High: 1
- Medium: 1
- 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.

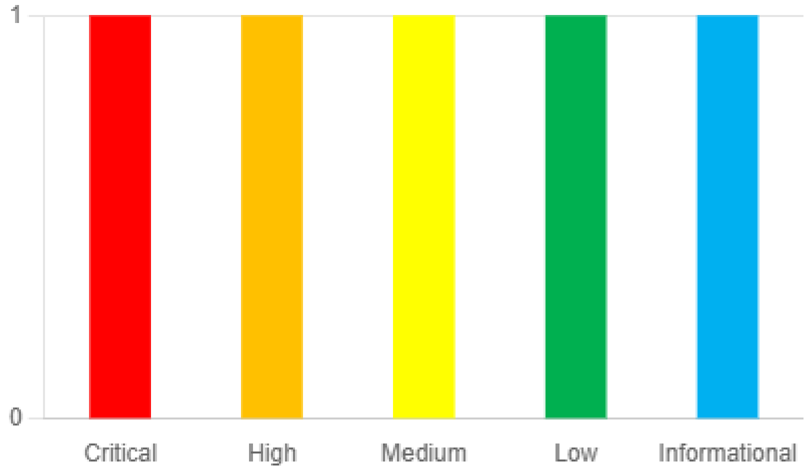
2. Penetration Test Scope

Asset	Date	Details	CIA Rating		
			C	I	A
IT BANK - FakeAsset ACC	-	Target: • www.fakeasset.fake Methodology: GRAYBOX Facing: INTERNAL	1	1	1

3. Customer Contact Information

Name	Role	Asset	Contact information
Fake Person 1	Asset Owner	IT BANK - Fake Asset	fakeperson1@ing.fake
Fake Person 2	IT Custodian	IT BANK - Fake Asset	fakeperson2@ing.fake
Fake Person 3	Security Officer	IT BANK - Fake Asset	fakeperson3@ing.fake
Fake Person 4	SPOC	IT BANK - Fake Asset	fakeperson4@ing.fake

4. Vulnerabilities chart



5. 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
Offsec: 9996	CRITICAL **9.8**	https://intra-app-gateway.fakecorp.local/admin/InternalService	Oracle HTTP Server Authentication Bypass	A critical authentication bypass vulnerability in Oracle HTTP Server and WebLogic Proxy Plug-in allows unauthenticated remote attackers to craft malicious HTTP requests that bypass proxy-layer access controls. This can lead to unauthorized data access, modification, or full compromise of backend WebLogic services.	Apply Oracle's January 2026 Critical Patch Update immediately to eliminate the vulnerability, and restrict network exposure to proxy components. Implement WAF protections and monitor for suspicious HTTP traffic targeting WebLogic endpoints.	New

Offsec: 9995	HIGH **7.5**	https://docs-hub.fakecorp.local/office/preview/render	Microsoft Office Security Feature Bypass	A critical security feature bypass in Microsoft Office allows attackers to craft malicious documents that bypass OLE protection mechanisms, tricking Office into executing unsafe embedded content. Successful exploitation requires only that the user opens a specially crafted file	Apply Microsoft's out-of-band patches for Office 2016/2019 and ensure Office 2021/Microsoft 365 instances are restarted so the server-side fix activates. Advise users to avoid unsolicited attachments and strengthen anti-phishing controls.	New
Offsec: 9904	MEDIUM **5.8**	https://api.fakecorp.local/user/profile?id=102	Insecure Direct Object References (IDOR)	The application grants direct access to objects based on user-supplied input without proper authorization checks.	Ensure that only authorized users can access sensitive resources, implement robust access control mechanism, use indirect references and implement server-side authorization check.	New

Offsec: 9906	LOW **2.4**	https://legacy-auth.fakecorp.local	TLS/SSL Server Supports Weak Cipher Algorithms	The server supports deprecated or cryptographically weak TLS/SSL ciphers (e.g., RC4, 3DES, EXPORT-grade), allowing attackers to exploit downgrade attacks or decrypt captured traffic. This significantly weakens the confidentiality and integrity of communications.	Disable all weak and deprecated cipher suites and enforce strong modern TLS configurations such as TLS 1.2+ with AES-GCM or CHACHA20-POLY1305. Regularly audit SSL configurations using automated scanners and industry best practices.	New
Offsec: 9994	INFO **0.0**	https://app.fakecorp.local/api/orders?order_id=abc	SQL Error Message	The application returns SQL error message that contains sensitive information like executed SQL statements. This information may help an attacker for example to build successful SQL Injection attacks.	All SQL errors of the application should be collected in the application logs, no errors should be returned to the application user	Not To Be Fixed

D. Introduction

1. Terminology

The goal of this document is to describe the results of Penetration Test.

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. Vulnerabilities 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).

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.

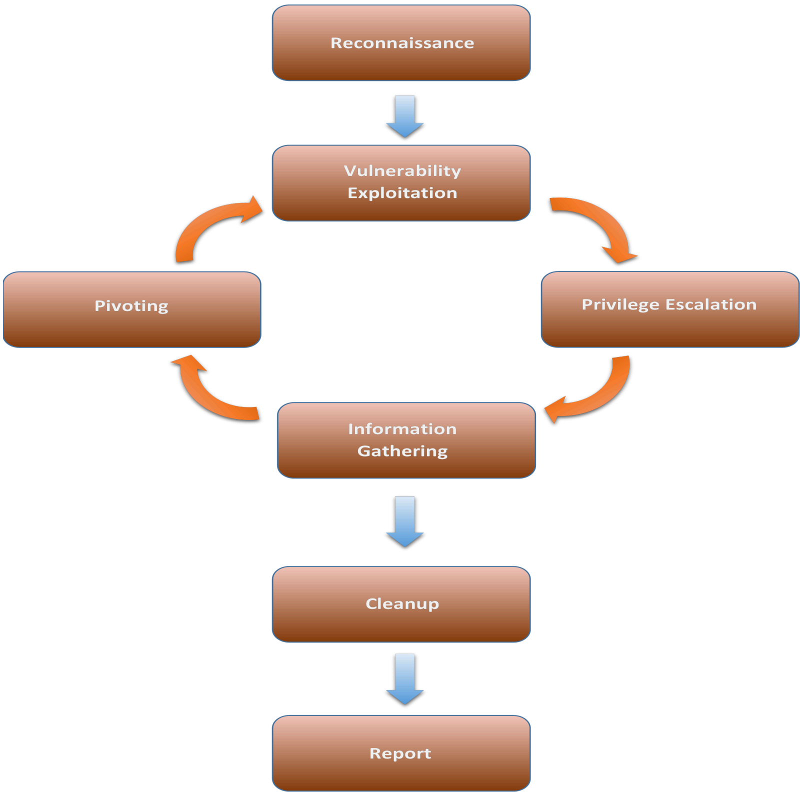
Offensive Cyber Security team uses the following main methodologies depending on the requirements:

- **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. 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.

1.1. Oracle HTTP Server Authentication Bypass (9996)

CRITICAL 9.8	Attack Vector:	NETWORK	Scope:	UNCHANGED
	Attack Complexity:	LOW	Confidentiality:	HIGH
	Privileges Required:	NONE	Integrity:	HIGH
	User Interaction:	NONE	Availability:	HIGH
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H				

1.1.1. Assets

https://intra-app-gateway.fakecorp.local/admin/InternalService;

1.1.2. Description

The Oracle HTTP Server Authentication Bypass vulnerability refers to a critical flaw in the Oracle HTTP Server and the WebLogic Server Proxy Plug-in that allows a remote attacker to bypass authentication mechanisms through crafted HTTP-based protocol exploitation. Because the attack requires only low privileges and no user interaction, a successful exploit could grant unauthorized access to protected resources and potentially enable full compromise of systems relying on the affected proxy components.

1.1.3. Recommendation

Apply Oracle CPU (January 2026) to all affected Oracle HTTP Server and WebLogic Proxy Plug-in versions, as this is the official fix. [sangfor.com], [fieldeffect.com] Limit external network reachability to the proxy layer using segmentation and firewall rules. [fieldeffect.com] Deploy or enhance WAF protections to detect crafted traversal paths and header manipulation; Imperva confirms their WAF blocks related patterns. [imperva.com] Monitor logs for abnormal WebLogic-related paths, malformed headers, and traversal sequences associated with exploitation attempts. [fieldeffect.com] Review backend WebLogic security posture (auth settings, admin interface exposure, credential hygiene) in case proxy bypass occurred. Conduct vulnerability scanning to ensure no unpatched or exposed instances remain

1.1.4. Additional Information

1.1.5. Evidence

Reproduction steps in retest findings.

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.

2.1. Microsoft Office Security Feature Bypass (9995)

HIGH 7.5	Attack Vector:	NETWORK	Scope:	UNCHANGED
	Attack Complexity:	LOW	Confidentiality:	HIGH
	Privileges Required:	NONE	Integrity:	NONE
	User Interaction:	NONE	Availability:	NONE
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N				

2.1.1. Assets

https://docs-hub.fakecorp.local/office/preview/render;

2.1.2. Description

This high-severity vulnerability in Microsoft Office allows an unauthorized attacker to bypass a security feature locally due to reliance on untrusted inputs in a critical security decision. Although it cannot be exploited remotely, a local attacker with limited access could leverage the flaw to circumvent Office’s built-in security controls, potentially enabling further compromise depending on the environment. Organizations are advised to apply the vendor-provided mitigations or discontinue affected versions until patches are available

2.1.3. Recommendation

Install official security updates (Office 2016 KB5002573, Office 2019 build 10417.20095+, Microsoft 365 via server-side update). [blackswan-...curity.com], [bleepingcomputer.com] Force restart Office applications on Office 2021 / LTSC / Microsoft 365 so ECS mitigation activates. [blackswan-...curity.com] Notify users and raise phishing awareness, as exploitation requires document opening. [blackswan-...curity.com] Apply registry-based temporary mitigation for legacy Office deployments via COM Compatibility key hardening. [blackswan-...curity.com], [bleepingcomputer.com] Keep Office builds updated and discourage enabling macros/OLE content in unknown files.

2.1.4. Additional Information

2.1.5. Evidence

Reproduction steps in retest findings.

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.

3.1. Insecure Direct Object References (IDOR) (9904)

MEDIUM 5.8	Attack Vector:	NETWORK	Scope:	CHANGED
	Attack Complexity:	LOW	Confidentiality:	LOW
	Privileges Required:	NONE	Integrity:	NONE
	User Interaction:	NONE	Availability:	NONE
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N				

3.1.1. Assets

https://api.fakecorp.local/user/profile?id=102;

3.1.2. Description

Insecure Direct Object References (IDOR) occurs when an application grants direct access to objects based on user-supplied input without proper authorization checks. This vulnerability allows attackers to bypass access controls and retrieve sensitive resources, such as database records, files, or other protected data.By modifying request parameters that reference an object (e.g., changing a numerical ID in a URL or API call), an attacker can gain unauthorized access to data belonging to other users or manipulate system resources. This is caused by the fact that the application takes user supplied input and uses it to retrieve an object without performing sufficient authorization checks.

3.1.3. Recommendation

Remediating the Insecure Direct Object References (IDOR) vulnerability requires a combination of technical measures and secure coding practices. By following the next steps, the risk of Insecure Direct Object References vulnerabilities in the web application can be significantly reduced and the overall security posture enhanced:- Identify and authenticate users: ensure that only authorized users can access sensitive resources. This could include using strong passwords, multi-factor authentication, or integrating with a trusted identity provider.- Implement access control: use role-based access control (RBAC) or attribute-based access control (ABAC) to determine what actions and resources each user is allowed to access. Avoid relying solely on client-side access controls, as they can be easily manipulated.- Use indirect references: instead of directly referencing sensitive objects or resources with direct identifiers related to IDs on the database or disk, perform an indirect mapping by using indirect references or surrogate identifiers. This means that rather than using predictable or sequential identifiers, unique tokens or random identifiers should be generated, since they cannot be easily guessed or manipulated by an attacker.- Implement server-side authorization checks: verify that the authenticated user has the necessary permissions to access or modify requested resources, regardless of any client-side controls.- Apply least privilege principle: ensure to grant users only the minimum level of access required to perform their tasks.- Secure API endpoint: ensure that application's API endpoints are protected against IDOR vulnerabilities. Implement proper authorization checks and validation of input coming to API requests.

3.1.4. Additional Information

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

3.1.5. Evidence

It is possible to generate report by iterating the numeric value passed through the id parameter. As proof of concept, please consider the request below performed with id 123.

```
POST /v1/investment-reporting/report/pdf/base64 HTTP/1.1
Host: localhost:1234
Cookie: JSESSIONID=223sddsdds22332
Content-Length: 175
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: it-IT,it;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="141", "Not?A_Brand";v="8"
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/141.0.0.0 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

{
  "id": 123,
  "ownershipKey": "fake",
  "referenceDate": "2020-10-17T13:54:00.591Z",
  "fromDate": "2020-10-17T13:54:00.591Z",
  "hiddenElements": [
    "string"
  ]
}
```

By changing the id from 123 to 234, it was possibile to generate report associated to that id

```
POST /v1/investment-reporting/report/pdf/base64 HTTP/1.1
Host: localhost:1234
Cookie: JSESSIONID=971F417D1FE8A31BD8627FE236F3DB63
Content-Length: 175
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: it-IT,it;q=0.9
Accept: application/json
Sec-Ch-Ua: "Chromium";v="141", "Not?A_Brand";v="8"
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/141.0.0.0 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
{
  "id": 234,
  "ownershipKey": "fake",
  "referenceDate": "2020-10-17T13:54:00.591Z",
  "fromDate": "2020-10-17T13:54:00.591Z",
  "hiddenElements": [
    "string"
  ]
}
```

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. TLS/SSL Server Supports Weak Cipher Algorithms (9906)

LOW 2.4	Attack Vector:	PHYSICAL	Scope:	UNCHANGED
	Attack Complexity:	LOW	Confidentiality:	NONE
	Privileges Required:	NONE	Integrity:	LOW
	User Interaction:	NONE	Availability:	NONE
CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N				

4.1.1. Assets

https://legacy-auth.fakecorp.local;

4.1.2. Description

The TLS/SSL server supports cipher suites based on weak algorithms. This may enable an attacker to launch man-in-the-middle attacks and monitor or tamper with sensitive data. In general, the following ciphers are considered weak: - So called ""null"" ciphers, because they do not encrypt data. - Export ciphers using secret key lengths restricted to 40 bits. This is usually indicated by the word EXP/EXPORT in the name of the cipher suite. - Obsolete encryption algorithms with secret key lengths considered short by today's standards, eg. DES or RC4. - CBC mode of operation

4.1.3. Recommendation

To mitigate the use of deprecated or weak TLS/SSL cipher suites, the organization should harden the server's cryptographic configuration to align with modern industry standards (NIST, OWASP, ENISA, CIS Benchmarks). Weak ciphers such as RC4, 3DES, EXPORT-grade ciphers, and NULL/Anonymous suites should be disabled entirely, as they expose encrypted traffic to attacks such as BEAST, POODLE, SWEET32, RC4 Bias, and downgrade exploits. A secure TLS posture must enforce contemporary algorithms that offer confidentiality, integrity, forward secrecy, and resistance to known cryptographic weaknesses.

4.1.4. Additional Information

4.1.5. Evidence

Reproduction steps in retest findings.

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. SQL Error Message (9994)

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

5.1.1. Assets

https://app.fakecorp.local/api/orders?order_id=abc;

5.1.2. Description

All SQL errors of the application should be collected in the application logs, no errors should be returned to the application user

5.1.3. Recommendation

To mitigate SQL Error Message Disclosure, the organization should implement a robust error-handling strategy that prevents sensitive backend information from leaking through application responses. Raw SQL errors often reveal database engine type, schema details, table and column names, or full query fragments — all of which significantly aid attackers performing SQL Injection reconnaissance. Proper remediation requires changes at both application and infrastructure layers.

5.1.4. Additional Information

CWE-209 http://cwe.mitre.org/data/definitions/209.html CWE-200 http://cwe.mitre.org/data/definitions/200.html

5.1.5. Evidence

```
Query: SELECT * FROM orders WHERE order_idd = 'abc'

SQLSTATE[42S22]: Column not found: 1054 Unknown column 'order_idd' in 'where clause'
```

G. Appendixes

1. 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.

2. Original request

```
{"spocEmails":["sania.dutta.ext@ing.com"],"firstLoDOfficerEmail":
["sania.dutta.ext@ing.com"]}
```

END OF REPORT