TATA CONSULTANCY SERVICES
Experience certainty.

API Penetration Testing Report

ZeroFinalBill-Mobile INTX

Cyber Security Practice

Issued by
Security Consulting Practice,
Tata Consultancy Services Limited,
July,2025

Disclaimer

Document Version Control

Document Control

Document Name	API Penetration Testing for **"ZeroFinalBill-Mobile INTX"**				
Document Version	Final v1.0	**Date**	03/07/2025	**Notes**	NA
Document Version	Final v2.0	**Date**	04/07/2025	**Notes**	NA
Document Version		**Date**		**Notes**	NA
Security Classification	Commercial in Confidence.				
Testing Team	Anon Ngauviriyasiripong, Palepu Gyana Suma Sree				
Distribution List					

Contact

Name	Anon Ngauviriyasiripong
Address	TCS Thailand
Phone	+66(0)914914556
Email	VDTCS01394@truecorp.co.th

Contents

1. EXECUTIVE SUMMARY

Tata Consultancy Services was asked to undertake API Penetration Testing on **ZeroFinalBill-Mobile INTX** (APIs to identify security vulnerabilities of application). The API Penetration Testing was performed at TCS Thailand location.

API Penetration Testing was limited to the Pre-Prod Environment as agreed prior to the commencement of the test cycle. The aim of such testing was to establish whether the application may be compromised in any way to allow unauthorized access to sensitive data or systems. To assist **ZeroFinalBill-Mobile INTX** achieve their purpose, TCS adopted an API Penetration Testing Methodology Framework which has been derived from the OWASP and other industry best practices.

It is fair to assume that experienced hackers in the wild have access to similar techniques and exploits and therefore we must reiterate that the vulnerabilities identified are real - not just hypothetical or academic theories.

This report presents the findings of the API Penetration Testing with an aim of comprehending the current security posture of the **ZeroFinalBill-Mobile INTX** Application Security and recommendations for improving the application security level.

Finally, it must be remembered that security is an ongoing process, and that this report will provide an idea of the current vulnerabilities we were able to detect. There is no guarantee that new vulnerabilities will not be found and exploited in the future.

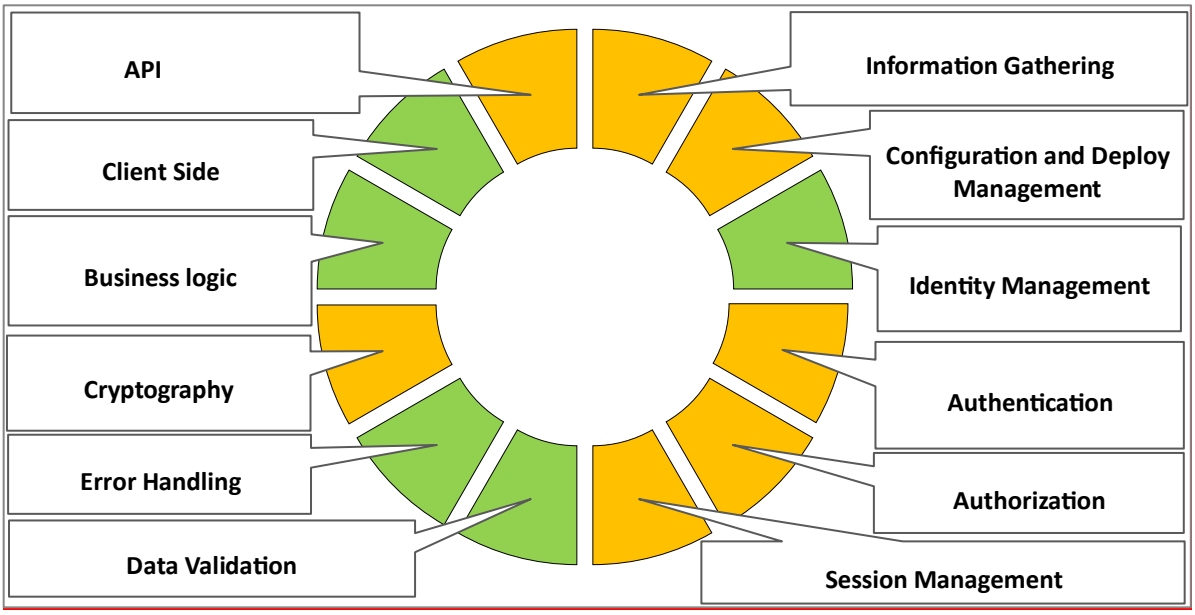
1.1 CURRENT SECURITY POSTURE

The TCS security testing team conducted a comprehensive API Penetration Testing of the **ZeroFinalBill-Mobile INTX** application on Test environment.

Telecom Client API Testing:

To determine the current security posture, TCS followed a structured checklist-based testing methodology in line with OWASP. Each domain listed below was thoroughly assessed through various attacks, with the objective of identifying security weaknesses in the target application with varying degree of attack sophistication and intent. All attack categories are assigned corresponding risks and threats specific to the application based on the relative findings.

The following doughnut chart is a graphic representation of the overall current security posture of the External API Penetration Testing Report for client in terms of the vulnerability severity of each applicable test domains.



**A detailed checklist has been included in Appendix A of this document.

Red	If a domain has been evaluated as RED, it contains at least one HIGH severity vulnerability. For RED domains, there is a strong need for corrective measures. The API may continue to operate at high risk. However, a corrective action plan must be put in place as soon as possible.
Amber	If a domain has been marked AMBER, it contains at least one MEDIUM/LOW or INFO but no HIGH severity vulnerability. For all AMBER domains, corrective actions are needed, and a plan must be developed to incorporate these actions within a reasonable period of time.
Green	If a domain is evaluated as GREEN, the target was not found to be susceptible to any major threats / vulnerabilities at this point in time.

1.2 VULNERABILITIES OBSERVATION

The following table shows a comparison of observed vulnerabilities mapped with OWASP Top 10 (2023) vulnerabilities identified in the **ZeroFinalBill-Mobile INTX** API Penetration Testing findings.

API1:2023 - Broken Object Level Authorization: APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface of Object Level Access Control issues. Object level authorization checks should be considered in every function that accesses a data source using an ID from the user.	Not Found
API2:2023 - Broken Authentication: Authentication mechanisms are often implemented incorrectly, allowing attackers to compromise authentication tokens or to exploit implementation flaws to assume other user's identities temporarily or permanently. Compromising a system's ability to identify the client/user, compromises API security overall.	**Found [RESOLVED]**
API3:2023 - Broken Object Property Level Authorization: The lack of or improper authorization validation at the object property level. This leads to information exposure or manipulation by unauthorized parties.	Not Found
API4:2023 - Unrestricted Resource Consumption: Satisfying API requests requires resources such as network bandwidth, CPU, memory, and storage. Other resources such as emails/SMS/phone calls or biometrics validation are made available by service providers via API integrations and paid for per request. Successful attacks can lead to Denial of Service or an increase of operational costs.	**Found [FIXED]**
API5:2023 - Broken Function Level Authorization: Complex access control policies with different hierarchies, groups, and roles, and an unclear separation between administrative and regular functions, tend to lead to authorization flaws. By exploiting these issues, attackers can gain access to other users' resources and/or administrative functions.	Not Found
API6:2023 - Unrestricted Access to Sensitive Business Flows: APIs vulnerable to this risk expose a business flow - such as buying a ticket, or posting a comment - without compensating for how the functionality could harm the business if used excessively in an automated manner. This doesn't necessarily come from implementation bugs.	Not Found
API7:2023 - Server-Side Request Forgery: Server-Side Request Forgery (SSRF) flaws can occur when an API is fetching a remote resource without validating the user-supplied URI. This enables an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall or a VPN.	Not Found

API8:2023 - Security Misconfiguration: APIs and the systems supporting them typically contain complex configurations, meant to make the APIs more customizable. Software and DevOps engineers can miss these configurations, or don't follow security best practices when it comes to configuration, opening the door for different types of attacks.	**Found**
API9:2023 - Improper Inventory Management: APIs tend to expose more endpoints than traditional web applications, making proper and updated documentation highly important. A proper inventory of hosts and deployed API versions are also important to mitigate issues such as deprecated API versions and exposed debug endpoints.	Not Found
API10:2023 - Unsafe Consumption of APIs: Developers tend to trust data received from third-party APIs more than user input, and so tend to adopt weaker security standards. To compromise APIs, attackers go after integrated third-party services instead of trying to compromise the target API directly.	Not Found

1.3 OWASP CHECKLIST

The TCS security testing team has been evaluated as per Open API Security Project Testing guide v4.2 as given in below attachment.

Worksheet in API

PT_Assessment_ Rep

1.4 CONCLUDING REMARKS

TCS recommends that all suggested measures in this document be performed to ensure the overall security of the application.

The High / Medium vulnerabilities should be addressed as a matter of urgency. The low / Info risk vulnerabilities should also be addressed to raise the level of security of the Customer application to the highest levels. We wish to thank **DTAC** for giving us the opportunity to conduct API Penetration Testing. We hope that the information contained in this document is of benefit to your organization. As security-related needs arise again in the future, it would be our pleasure to assist you again.

2. PROJECT SCOPE

The following target applications were identified by **ZeroFinalBill-Mobile INTX** for the scope of this testing.

No.		Target URL / IP's	Observation
1	**ZeroFinalBill-Mobile INTX**	http://apigw.intx-uat5.true.th/MGBillingProfileInfo/MGBillingProfileInfo/getFinalChargeInfo http://apigw.intx-uat5.true.th/MGOfferInfo/MGOfferInfo/getFuturePromotionList http://apigw.intx-uat5.true.th/MGBillingProfileInfo/MGBillingProfileInfo/getTotalObligationInfo http://apigw.intx-uat5.true.th/CampaignBundling/CampaignBundling/getATSValidationInfo	**Vulnerable**

Below are the applicable domains tested for above URL:

- Information Gathering
- Configuration and Deploy Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Data Validation Testing
- Error Handling
- Cryptography
- Business logic Testing
- Client-Side Testing

The following steps were considered out of scope for this engagement.

- Denial of Service tests
- Intrusive Tests and Exploitation
- Social Engineering
- Implementation of Vulnerability fixes
- Application Code review from security perspective.
- Configuration review of the infrastructure.

2.1 PENETRATION TESTING

TCS's methodology for API Penetration Testing is based on industry best practices & methodologies such as OWASP, OSSTMM & NIST. API security assessment involves intrusion techniques leading to identification of potential vulnerabilities, which may compromise the APIs. TCS assessed the APIs with no prior knowledge of the application, to identify potential security vulnerabilities that may exist, which makes them vulnerable to being exploited through the internet. The testing comprised of under mentioned steps:

2.2 SECURITY TESTING TOOLS

For various phases in the API Penetration Testing Methodology, TCS security testing team uses open-source tools and manual techniques accompanied by custom scripts to ensure optimum results.

Arrays of multiple tools are deployed in a phased manner to eliminate false-positives and false negatives. Realistic information security intelligence goes into the generation of our reports with a focus on being as specific as possible about the existence of vulnerabilities and the right solution or workaround for their mitigation.

The following is a brief list of open-source tools which have been used during this penetration testing:

Activity	Open-Source Tools	Licensed Tools
WAPT	Postman	Burp Suite Professional

2.3 VULNERABILITY SEVERITY RATING

TCS rates the impact of individual vulnerabilities on a four-point scale High, Medium, Low and Info. The scale considers the potential risk of a flaw based on a technical analysis of the exact flaw and its type.

Level	Description
HIGH	Based on the existing controls and information processed, there is a certainty that sensitive information will be susceptible to disclosure, tampering and/or disruption to critical infrastructure. **High level vulnerabilities** are categorized as the most dangerous, which put a site at maximum risk for hacking and data theft.
MEDIUM	Risk exposure that does not directly compromise the confidentiality, integrity, and/or availability of the areas tested. However, there is a likelihood of intrusion given the current controls, and recommended controls should be implemented to further minimize the risks, and constant monitoring should be performed to respond to malicious activities. **Medium level vulnerabilities** are generally caused by server miss-configuration and site coding flaws, which facilitate server disruption and directory intrusion
LOW	Risk exposure that impacts insignificant business processes/information, or the likelihood of occurrence is negligible. The recommended measures may be implemented to enhance the security posture of the overall infrastructure/processes. **Low Level Vulnerabilities** are generally caused by server miss-configuration, or directory path disclosures, etc....
INFO	Information about a host that does not represent a security threat. However, some of the information could be used to assess the security of the API at large.

3. SUMMARY OF VULNERABILITIES AND RECOMMENDATIONS

3.1 VULNERABILITY SEVERITY DISTRIBUTION

The table and Pie chart below represents the vulnerabilities identified in the API penetration testing.

Vulnerabilities				Total
High	Medium	Low	Info	2
0	0	2	0