



TOTVS SA

Letter of Attestation

Creation Date: June 17th, 2024

MODELO



Introduction

This document is created as evidence and audit proof for our customer TOTVS SA explaining the results of their ongoing security testing via the Intigriti platform.

Intigriti is a cloud solution, providing an ethical hacking platform to companies that desire a structured bug bounty program or hybrid Pentest.

Intigriti is a **crowdsourced security platform** where security researchers meet and communicate with companies in a coordinated way. Based on the defined scope of the projects launched by the participating companies, the researchers will search for vulnerabilities and report them back. Researchers are only paid in case of a new and in scope vulnerability, which has not been reported on before. If no vulnerabilities are found, no bounties will be paid. Based on the customer's predefined scope in their program details, researchers from Intigriti's security community have searched for vulnerabilities and reported their findings through Intigriti's platform.

The security assessments from our crowd include testing for an extensive range of vulnerabilities, including those defined in the [OWASP top 10 - 2021](#):

- [A01:2021-Broken Access Control](#)
- [A02:2021-Cryptographic Failures](#)
- [A03:2021-Injection](#)
- [A04:2021-Insecure Design](#)
- [A05:2021-Security Misconfiguration](#)
- [A06:2021-Vulnerable and Outdated Components](#)
- [A07:2021-Identification and Authentication Failures](#)
- [A08:2021-Software and Data Integrity Failures](#)
- [A09:2021-Security Logging and Monitoring Failures](#)
- [A10:2021-Server-Side Request Forgery](#)



Executive Summary

This document provides a summary of the testing conducted on the Intigriti platform. Further details can be shared at the discretion of TOTVS SA

Up to June 17th, 2024 there were 02 vulnerabilities reported by security researchers on the Intigriti platform, of which 61 vulnerabilities were unique and accepted. The reported vulnerabilities and their status are detailed in **Table 5**.

The programs for which this testing was conducted are:

Program Name	Launch date	Confidentiality Level	ID Check Required
TOTVS	28/02/2023	Invite Only	1

(Table 1)

There are a variety of program types available:

Public Program, where any member of our security researcher community can access the program. Public Programs are advertised on our website and the testing details as well as bounty amounts are publicly available.

Responsible Disclosure, where any member of our security researcher community can access the program. Responsible Disclosure Programs are advertised on our website, however there is no bounty paid for vulnerabilities found.

Invite Only (Private) Program, where the program details are kept private except for a select group of specialist security researchers, who are invited to participate in the program.

Registered Program, where researchers who have registered their account on the Intigriti platform can find the program details and access the program. The program details are not publicly available on the website, and testing can be limited to researchers who have already been verified on our platform.

Application Program, where researchers need to submit an application to participate in testing on the program, and the company needs to accept the application in order for testing to commence.



Scope

The scope against which testing was conducted and vulnerabilities were reported is defined as:

Product name	Version
Product 1	Version 1.0
Product 2	Version 2.0
Product 3	Version 3.0
Product 4	Version 4.0
Product 5	Version 5.0
Product 6	Version 6.0
Product 7	Version 7.0
Product 8	Version 8.0
Product 9	Version 9.0
Product 10	Version 10.0
Product 11	Version 11.0
Product 12	Version 12.0
Product 13	Version 13.0
Product 14	Version 14.0
Product 15	Version 15.0
Product 16	Version 16.0
Product 17	Version 17.0
Product 18	Version 18.0
Product 19	Version 19.0
Product 20	Version 20.0
Product 21	Version 21.0
Product 22	Version 22.0
Product 23	Version 23.0
Product 24	Version 24.0
Product 25	Version 25.0
Product 26	Version 26.0
Product 27	Version 27.0
Product 28	Version 28.0
Product 29	Version 29.0
Product 30	Version 30.0
Product 31	Version 31.0
Product 32	Version 32.0
Product 33	Version 33.0
Product 34	Version 34.0
Product 35	Version 35.0
Product 36	Version 36.0
Product 37	Version 37.0
Product 38	Version 38.0
Product 39	Version 39.0
Product 40	Version 40.0
Product 41	Version 41.0
Product 42	Version 42.0
Product 43	Version 43.0
Product 44	Version 44.0
Product 45	Version 45.0
Product 46	Version 46.0
Product 47	Version 47.0
Product 48	Version 48.0
Product 49	Version 49.0
Product 50	Version 50.0
Product 51	Version 51.0
Product 52	Version 52.0
Product 53	Version 53.0
Product 54	Version 54.0
Product 55	Version 55.0
Product 56	Version 56.0
Product 57	Version 57.0
Product 58	Version 58.0
Product 59	Version 59.0
Product 60	Version 60.0
Product 61	Version 61.0
Product 62	Version 62.0
Product 63	Version 63.0
Product 64	Version 64.0
Product 65	Version 65.0
Product 66	Version 66.0
Product 67	Version 67.0
Product 68	Version 68.0
Product 69	Version 69.0
Product 70	Version 70.0
Product 71	Version 71.0
Product 72	Version 72.0
Product 73	Version 73.0
Product 74	Version 74.0
Product 75	Version 75.0
Product 76	Version 76.0
Product 77	Version 77.0
Product 78	Version 78.0
Product 79	Version 79.0
Product 80	Version 80.0
Product 81	Version 81.0
Product 82	Version 82.0
Product 83	Version 83.0
Product 84	Version 84.0
Product 85	Version 85.0
Product 86	Version 86.0
Product 87	Version 87.0
Product 88	Version 88.0
Product 89	Version 89.0
Product 90	Version 90.0
Product 91	Version 91.0
Product 92	Version 92.0
Product 93	Version 93.0
Product 94	Version 94.0
Product 95	Version 95.0
Product 96	Version 96.0
Product 97	Version 97.0
Product 98	Version 98.0
Product 99	Version 99.0
Product 100	Version 100.0

MODELO



Methodology

Depending on the scope of the assessment, Intigriti's vetted researcher base is following the methodologies and standards discussed in this chapter.

Web application

During the security assessment of a web application, an extensive range of vulnerabilities is tested for, including those defined in the OWASP Top 10 – 2021:

- [A01:2021-Broken Access Control](#)
- [A02:2021-Cryptographic Failures](#)
- [A03:2021-Injection](#)
- [A04:2021-Insecure Design](#)
- [A05:2021-Security Misconfiguration](#)
- [A06:2021-Vulnerable and Outdated Components](#)
- [A07:2021-Identification and Authentication Failures](#)
- [A08:2021-Software and Data Integrity Failures](#)
- [A09:2021-Security Logging and Monitoring Failures](#)
- [A10:2021-Server-Side Request Forgery](#)

A common methodology that is followed is the [OWASP Web Security Testing Guide](#).

API

For the security assessments of API's, the focus of testing lies on the security vulnerabilities defined in the [OWASP API Top 10 - 2019](#):

- [API1:2019-Broken Object Level Authorization](#)
- [API2:2019-Broken User Authentication](#)
- [API3:2019-Excessive Data Exposure](#)
- [API4:2019-Lack of Resources & Rate Limiting](#)
- [API5:2019-Broken Function Level Authorization](#)
- [API6:2019-Mass Assignment](#)
- [API7:2019-Security Misconfiguration](#)
- [API8:2019-Injection](#)
- [API9:2019-Improper Assets Management](#)
- [API10:2019-Insufficient Logging & Monitoring](#)



Mobile application

During the security assessment of mobile applications, the [OWASP MAS checklist](#) and the [OWASP Mobile Application Security Testing Guide](#) play a predominant role in test coverage. These include vulnerabilities out of the following categories:

- Architecture, Design and Threat Modelling
- Data Storage and Privacy
- Cryptography
- Authentication and Session Management
- Network Communication
- Platform Interaction
- Code Quality and Build Setting
- Resilience

Submissions

Each submission gets triaged by Intigriti's in-house team to validate the proof of concept and ensure that the submission can be replicated.

Scoring the severity of submissions:

Intigriti's severity scoring system is based on the CVSSv3 scoring system together with business impact factors that are determined during the scoping phase of the engagement.

