INTIGRITI
ETHICAL HACKING PLATFORM

TOTVS SA

Letter of Attestation

Creation Date: June 17th, 2024

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- A06:2021-Vulnerable and Outdated Components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 119 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	InviteOnly	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	Domain
`Portal Smartclientprotheus`	http://bugbountysmartclientprotheus.totvsbugbounty.com.br:8088/rest
`Fluig`	https://bugbountyfluig.totvsbugbounty.com.br/
`Fluig`	https://bugbountyfluig.totvsbugbounty.com.br/api
`PortalDoProfessor+PortalGestaoEducacional`	https://bugbountyrm.totvsbugbounty.com.br/FrameHTML/web/app/Cmp/PortalDoFornecedor/#/login
`PortalDoProfessor+PortalGestaoEducacional`	https://bugbountyrm.totvsbugbounty.com.br/FrameHTML/web/app/Edu/PortalBiblioteca/#/?c=1&f=1&b=1
`PortalDoProfessor+PortalGestaoEducacional`	https://bugbountyrm.totvsbugbounty.com.br/FrameHTML/web/app/Edu/PortalDoProfessor/#/login
`PortalDoProfessor+PortalGestaoEducacional`	https://bugbountyrm.totvsbugbounty.com.br/FrameHTML/web/app/Edu/PortalEducacional/
`PortalDoProfessor+PortalGestaoEducacional`	https://bugbountyrm.totvsbugbounty.com.br/FrameHTML/web/app/Edu/PortalGestaoEducacional/#/login
`PortalDoProfessor+PortalGestaoEducacional`	https://bugbountyrm.totvsbugbounty.com.br/FrameHTML/web/app/Imb/PortalCliente/#/
`PortalDoProfessor+PortalGestaoEducacional`	https://bugbountyrm.totvsbugbounty.com.br/FrameHTML/web/app/Imb/PVI/#/login
`PortalDoProfessor+PortalGestaoEducacional`	https://bugbountyrm.totvsbugbounty.com.br/FrameHTML/web/app/Prj/MinhasInspecoes/login
`PortalDoProfessor+PortalGestaoEducacional`	https://bugbountyrm.totvsbugbounty.com.br/FrameHTML/web/app/Prj/PortalTopWeb/login
`PortalDoProfessor+PortalGestaoEducacional`	https://bugbountyrm.totvsbugbounty.com.br/FrameHTML/web/app/RH/PortalMeuRH/#/home
`PortalDoProfessor+PortalGestaoEducacional`	https://bugbountyrm.totvsbugbounty.com.br/FrameHTML/web/app/Sau/PEP/#/login
`PortalDoProfessor+PortalGestaoEducacional`	https://bugbountyrm.totvsbugbounty.com.br/framehtml/Web/App/Sau/PortalFarmacia/
`Portal Smartclientprotheus`	https://bugbountysmartclientprotheus.totvsbugbounty.com.br:8081/webapp/

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.

INTIGRITI
ETHICAL HACKING PLATFORM

Contact us | Visit intigriti.com | Request a demo