Triskele Labs Offensive Team

Web Application and API Penetration Test Report

Triskele Labs

go1

Triskele Labs

go1

Web Application and API Penetration Test Report

Version 2.0

Released Date: 20 July 2023

Prepared for:

Kyle Jackson

Information Security Manager

kyle.jackson@go1.com

Go1

2904 Logan Rd

Underwood QLD 4119

Australia

Submitted By:

William Davy

Offensive Consultant

william.davy@triskelelabs.com

Triskele Labs Global Pty Ltd

Level 14, 60 Albert Rd

South Melbourne VIC 3205

Australia

1. ENGAGEMENT OVERVIEW

1.1. BACKGROUND

The outcome of this assessment was to provide an insight into the potential attack vectors and risk landscape of the Go1 web application. This assessment was carried out to meet Go1 due diligence requirements. It was discovered that, while the web application follows many security best practices, there are areas of risk and therefore further opportunities for improvement. During testing, the following issues were identified:

- 0 Critical risks
- 1 High risk
- 9 Medium risks
- 5 Low risks
- 2 Informational risks

This report provides both a technical and business summary of the identified risks. For further, in-depth information, please refer to the body of this report, or contact Triskele Labs for more details.

Please Note: Aside from the Executive Summary, this document is intended for a technical audience with knowledge of Go1, supporting systems and related technologies. The information recorded within this report should be considered sensitive and restricted distribution is strongly advised as the information contained within this report would be a valuable tool to any would-be attacker.

1.2. SCOPE

This engagement was completed in accordance with the Triskele Labs proposal “Web Application and API Penetration Testing”, dated 27 October 202227 October 2022. The scope was subsequently confirmed during the kick-off meeting between Go1 stakeholders and Triskele Labs on 10 March 2023. Testing activities for this engagement were conducted between 08 May 2023 and 19 May 2023. All network-based testing was conducted from the following Triskele Labs primary remote IP addresses:

- 52.64.23.92/32

As part of this engagement, the following components were tested:

- Portal: https://pentesting.qa.go1.cloud/login
- Public API: https://api.go1.com
- Private API: https://api.go1.co
- Public website: https://website.qa.go1.cloud

1.3. RULES OF ENGAGEMENT

Strict rules of engagement were defined for the penetration testing:

- The continuity of the Go1 business was paramount. At no time was penetration testing to impact business continuity.
- Denial of service (DoS) attacks were not permitted or acceptable.
- The locking of valid customer accounts was not permitted or acceptable.
- The manipulation of data which could cause damage to Go1 systems was not permitted or acceptable.
- All findings rated critical or high had to be announced and detailed on the day of discovery.

1.4. ASSESSMENT ASSUMPTIONS

The following assumptions are relevant when considering the results presented in this report:

- Although several vulnerabilities were only exploitable with authentication, an attacker may gain access to a valid account using techniques outside the scope of this engagement, such as phishing or account compromise through a data breach of an unrelated service wherein shared credentials were utilised.

1.5. ASSESSMENT LIMITATIONS

The following limitations affecting the findings in this report were present during the assessment:

- In a modern threat environment, attackers targeting an organisation often have unlimited time to gather information, discover vulnerabilities, launch phishing campaigns, and perform social engineering and other attacks. In contrast, a penetration test is time- and scope-constricted engagement and as such, it is a best effort security assessment of the systems and networks at a specified time.
- Certain aspects of the application could not be tested due to technical issues preventing a full flowthrough of these items. The following list lists all aspects of the application considered untested at the end of this engagement:
  - Portal theme settings
  - LTI integrations

SUMMARY OF FINDINGS

The assessment has identified that there are several attack vectors that could be utilised against the Go1 web application, primarily exploitation through various types of Cross-Site Scripting vulnerabilities. *Figure 1 Risk Outline* summarises the number of findings identified during testing.

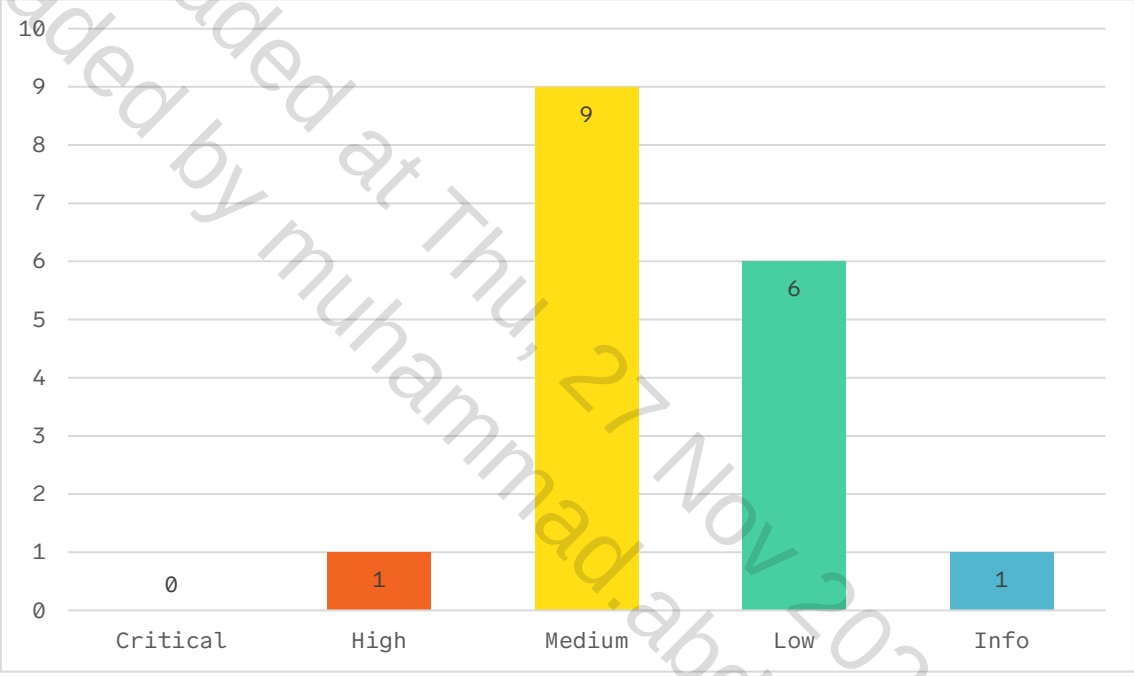

Figure 1 Risk Outline