Web App Penetration Test Summary Report

10 December 2020

Prepared for:

Information Delivery Statement

The information presented in this document summarizes the security testing services that were performed by CyberHunter Solutions Inc. (CyberHunter) for the Client named in the Executive Summary.

CyberHunter warrants that the information contained in this report is complete and accurate. We have used all reasonable care to test, collect, analyze and document, and we ascertain the accuracy of the information data within.

Authorized by:

Chris Dodunski, CEO
CyberHunter Solutions, Inc.
900-251 Laurier Avenue W.
Ottawa, Ontario, Canada K1P 5J6
www.cyberhunter.solutions

Dated: 10 December, 2020

All test procedures, findings and collected data used in the creation of this report were produced by:

Alex Lopyrev, OSCP, CRTP, CISSP (Associate)
Senior Penetration Tester
CyberHunter Solutions, Inc.

Executive Summary

CyberHunter Solutions was contracted by HELLO UMI S.L. (dba Landbot.io) to perform a manually executed, credentialed application penetration test against their web platform. The penetration testing was conducted between 21 September and 30 September 2020 by certified experts to verify the security of the following targets:

- app.landbot.io
- messages.landbot.io
- chats.landbot.io

A second round of targeted retesting was conducted on 10 December 2020 to verify that discovered issues had been successfully remediated by the Client. The report below outlines the state of security as of this date as assessed by CyberHunter Solutions Inc.

Testing Methodology & Standards

Throughout an external penetration testing engagement, CyberHunter uses methodologies based on NIST SP 800-1151 (The Technical Guide to Information Security Testing and Assessment), OWASP Top 10 Most Critical Web Application Security Risks, OWASP Testing Guide v4, CWE/SANS TOP 25 Most Dangerous Software Errors and the Penetration Testing Execution Standard (PTES), all of which can be summarized into the following high-level steps:

1. **Intelligence gathering**: In the first step of a penetration test, CyberHunter looks for as much information about the targets as possible. This includes identification of used devices, services and applications as well as the discovery of valid possible user accounts and other actions associated with the testing target.
2. **Vulnerability analysis**: Once all systems and applications are properly identified, CyberHunter performs analysis of found misconfigurations, design flaws, etc.
3. **Exploitation**: In this phase, CyberHunter attempts to exploit any weaknesses or vulnerabilities identified in discovered assets that are part of the penetration test scope.
4. **Post-exploitation**: After gaining access to a compromised device/application, we attempt to establish full control of it, determine the usefulness of this device/application for next attacks and optionally make lateral movement further into a network.
5. **Reporting**: We provide a description of all discovered attack vectors along with their severity (based on complexity, probability, user interaction, …) and possible remediation steps.

Testing Coverage

ID	Test Area	
CTG 1	Information Gathering	✔
CTG 2	Configuration and Deployment	✔
CTG 3	Authentication	✔
CTG 4	Authorization	✔
CTG 5	Session Management	✔
CTG 6	Input Validation	✔
CTG 7	Cryptography	✔
CTG 8	Business Logic	✔
CTG 9	Client-Side	✔

Severity Level Definitions

Findings severity levels used in this report are the following (starting with the most severe):

- Critical: Non-theoretical security issues that should be addressed as soon as possible. Such issues, for example, expose very sensitive data, allow a threat actor control over remote systems or their exploitation is very trivial.
- High: Non-theoretical security issues that should be promptly addressed as they pose high security risk on the organization.
- Medium: Non-theoretical security issues that should be addressed. These issues have only limited effect on the organization or the exploitation is not trivial.
- Low: Mostly theoretical issues or notices to provide further hardening tips.
- Info: Informative findings that do not need to be addressed but should be mentioned.

Findings - Summary

As of 9 December, 2020, the following findings remain outstanding in the tested platform:

- Zero **CRITICAL** severity findings
- Zero **HIGH** severity findings
- One **MEDIUM** severity finding. This issue remains outstanding as it is derived from the functionality provided by the application. Landbot is planning on deprecating this feature in a planned software release.
- Two **LOW** severity findings.