HackerOne Coupa
Security Assessment

APRIL 11TH, 2019 • CONFIDENTIAL

Version
1.0

Author
Joaquin Silva Jr. (Program Manager, HackerOne)
joaquin@hackerone.com

Reviewers
Zach Dando (Manager of Triage, HackerOne)
Eduardo Cervantes (Technical Program Manager, HackerOne)

Table of Contents

1 - Executive Summary

Coupa engages HackerOne to perform continuous security testing on their applications and services via their ongoing bug bounty program hosted on HackerOne. Coupa's program launched on May 17th, 2018 on HackerOne. This report summarizes all security testing that occurred from February 22nd, 2019 to April 11th, 2019. During this timeframe, 25 vulnerabilities were identified by eight security researchers.

During the assessment, five vulnerabilities were found that had a CVSS score of 7.0 or higher, rating either high or critical. These vulnerabilities represent the greatest immediate risk to Coupa and should be prioritized for remediation. Table 1 shows the in scope assets and breakdown of findings by severity per asset. Section 2.4 contains more information on how severity is calculated.

	Critical	High	Medium	Low	None	Σ
R24 Contract Collaboration	0	0	**2**	0	0	**2**
R24 CLM application	0	**2**	**6**	0	0	**8**
R24 Enterprise Application & CoupaPay application	0	**2**	**7**	**3**	0	**12**
R24 Supplier portal	0	0	0	0	0	0
	0	**4**	**15**	**3**	0	**22**

Table 1: findings per asset

The security assessment was conducted using a crowd-sourced penetration testing methodology. From its community of over 200,000 hackers, HackerOne curated a set of top-tier researchers to focus on identifying vulnerabilities in Coupa's scope during the agreed upon testing window, while abiding by the policies set forth by Coupa. Section 2.2 contains more information about the methodology.

2 - Introduction

Coupa engages HackerOne to perform continuous security testing on their applications and services via their ongoing bug bounty program hosted on HackerOne. This report summarizes all security testing that occurred from February 22nd, 2019 to April 11th, 2019.

2.1 - Scope

The in-scope assets are outlined in Table 2.

In Scope Assets
R24 Contract Collaboration
R24 CLM application
R24 Enterprise Application & CoupaPay application
R24 Supplier portal

Table 2: in scope assets

2.2 - Methodology

HackerOne works with Coupa to continuously maintain a scope for their ongoing bug bounty program, as well to determine what types of vulnerabilities are most important to Coupa. This information is published on a Security Page, also known as the rules of engagement, for Coupa's program. This page outlines the targets in scope for the program, reward structure, and other parameters of the testing. It is designed to incentivize and enable testing by a broad community of security talent with diverse experience and specializations. HackerOne has a community of over 200,000 hackers, and any and all of them have access to Coupa's program at any time. Each security researcher is incentivized through a bounty structure published on the Security Page where the reward for identifying a vulnerability goes up the higher the severity of the identified vulnerability is. Please refer to Appendix B for a copy of the bounty structure that was used in this assessment. HackerOne and Coupa make regular updates to the Security Page to communicate expansions of scope, new areas of interest as well as ensure security researchers continue to be incentivized as Coupa's applications become more hardened.

HackerOne encourages the use of individual tools and methods by each security researcher. This ensures diversity in the testing. It also ensures that new tools and techniques can be used in the testing. While individuality in testing methodology is encouraged, researchers ascribe to OWASP's (Open Web Application Security Project) standard testing techniques to uncover issues (e.g. OWASP Top 10) within Coupa's applications and services. Additionally, HackerOne's security analysts triage and categorize all identified vulnerabilities against the CWE(Common Weakness Enumeration) standard, as well as assign a severity ranking based on the CVSS v3.0 (Common Vulnerability Scoring System) standard, providing consistent, easy to understand guidelines on the severity of each vulnerability.

2.3 - Classification

HackerOne uses a vulnerability taxonomy based on the industry-standard Common Weakness Enumeration (CWE). CWE is a community-developed list of common software security weaknesses. It serves as a common language, a measuring stick for software security tools, and as a baseline for weakness identification, mitigation, and prevention efforts. More information can be found on MITRE's website: https://cwe.mitre.org/.

2.4 - Framework

HackerOne uses the industry-standard CVSS to calculate severity for each identified security vulnerability. CVSS provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly

assess and prioritize their vulnerability management processes. More information can be found on the Forum for Incident Response and Security Teams' (FIRST) website: https://www.first.org/cvss.

2.6 - Team

2.6.1 - HackerOne Staff

This engagement was delivered by a combination of HackerOne staff and security researchers of the HackerOne community.

- **Joaquin Silva Jr., Technical Program Manager**
  bensdp@hackerone.com
- **Zachary Dando, Security Analyst Manager**
  zach@hackerone.com

Please feel free to contact these individuals with any questions or concerns you have around the engagement or this report.

2.6.2 - HackerOne Researchers

A full list of researchers that participated in this program during the reporting window are available in Appendix A.

3 - Remediation Status

After the completion of the Coupa campaign, all seven (7) reported vulnerabilities were remediated. Table 3 shows the number of remediated reports based on severity per asset. The Coupa ensured the vulnerabilities were patched properly. Coupa has ensured that the vulnerabilities are not only fixed but are fixed thoroughly and a mitigation can't be bypassed.

	Critical	High	Medium	Low	None	Σ
R24 Contract Collaboration	0	0	**2**	0	0	**2**
R24 CLM application	0	**1**	**3**	0	0	**4**

R24 Enterprise Application & CoupaPay application	0	**2**	0	**1**	0	**3**
R24 Supplier portal	0	0	0	0	0	0
	0	**3**	**5**	**1**	0	**9**

Table 3: Remediated reports

Appendix A - HackerOne Researchers

The following individuals were curated to participate in this bug bounty program from HackerOne's community of over 300,000 hackers:

Hackers' Usernames
hackerone.com/bugbountyhunter555
hackerone.com/sandeep_hodkasia
hackerone.com/tolo7010
hackerone.com/toannc123
hackerone.com/foobar7
hackerone.com/todayisnew
hackerone.com/neema
hackerone.com/balis0ng

Appendix B - Bounty Structure

Reward amounts are based on the severity of a vulnerability. HackerOne uses CVSS 3.0 (Common Vulnerability Scoring Standard) to calculate severity.

The following bounty structure was published on the Security Page at the time of reporting: