Coupa Security Assessment - Enterprise

Executive Summary – R27

May 2020

Table of Contents

Observations Summary

Based on the manual vulnerability assessment and penetration testing performed, there were certain known security vulnerabilities found on the in-scope Web Applications. However, no sensitive data related to Coupa or its customers were exfiltrated.

Testing Team

The Coupa Internal security team, Crowdsourced testers, and Third-party teams have carried out the assessment.

Testing Environment

The testing environment is hosted on the following URL.

https://hackme5.coupadev.com

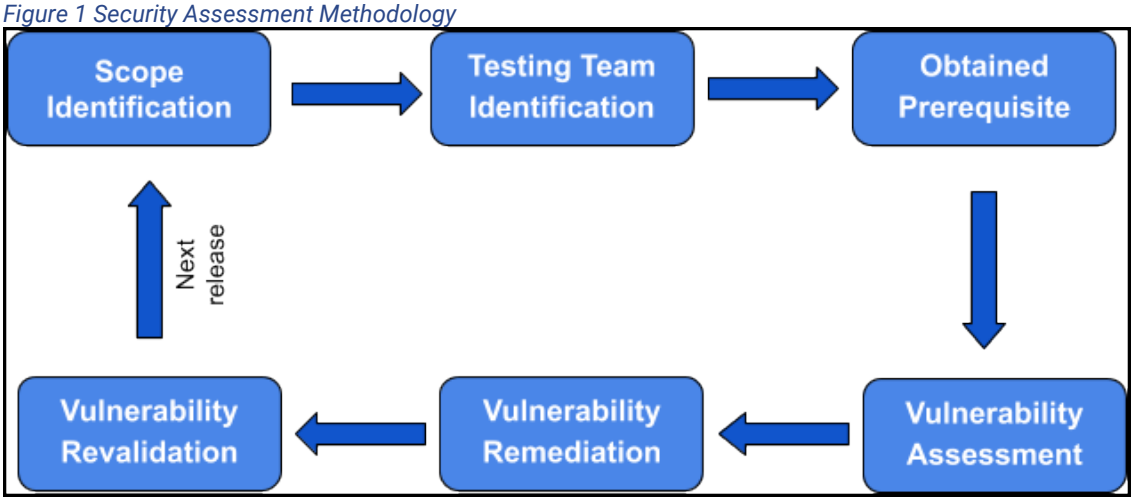
Assessment Dates

The 8-week assessment was performed from March 09, 2020 to May 01, 2020.

Coupa Security Assessment Methodology

The Coupa security team has developed a customized approach which is structured into six phases as described in Figure 1.

Figure 1 Security Assessment Methodology



Phase 1 – Scope Identification

Multiple stakeholders including, but not limited to, product managers and the security team schedule the annual security testing program. Depending on product criticality and the number of features developed, products are tested per release or on an on-demand basis.

Phase 2 – Testing Team Identification

Based on product criticality and testing team capacity, the testing team is chosen from one of the resources listed below:

1. Internal Security Team
2. Crowdsourced Testers
3. Third-Party Vendors

Phase 3 – Obtained Prerequisite

This phase includes gathering the following information from the respective development team:

- Understanding and walkthrough of the application
- Design documents
- In-scope product URLs (Development environment)
- Different user roles

Note: Coupa uses the development environment for the security assessment and not the production environment.

Phase 4 – Vulnerability Assessment

This phase includes vulnerability identification, risk rating, and JIRA ticket creation.

Vulnerability Identification

Coupa incorporates industry best practices to identify vulnerabilities which include the following methodologies:

- OSSTMM
- CREST
- OWASP
- PTES
- SANS
- NIST

These methodologies help ensure that the most recent and common web application vulnerabilities are identified in the most time and cost-efficient manners. However, testing varies based on the scope, timeline, nature of the application, and business logic flaws.

Common tested vulnerabilities include security misconfiguration, code injection, cross-site request forgery, cross-site scripting, insecure storage of sensitive data, authorization/authentication vulnerabilities, and business logic vulnerabilities, and more.

Risk Rating

After vulnerabilities are identified, risk levels are assigned to each finding.

Coupa evaluates risks by determining the likelihood and consequence of each vulnerability. An understanding of the nature of the vulnerability and its potential to affect technical and business objectives are developed by Coupa.

Additionally, Coupa evaluates vulnerabilities on a 4-level security scale which includes; Low, Medium, High, and Critical categories as described in Table 3 of Appendix 1.

Issue Tracker

For tracking, Coupa creates tickets which includes all observations and vulnerability details. Each vulnerability is tracked with a unique ID.

Phase 5 – Vulnerability Remediation

The Coupa Security Team prepares remediation plans for all issues found during penetration testing which are assigned to the appropriate development team.

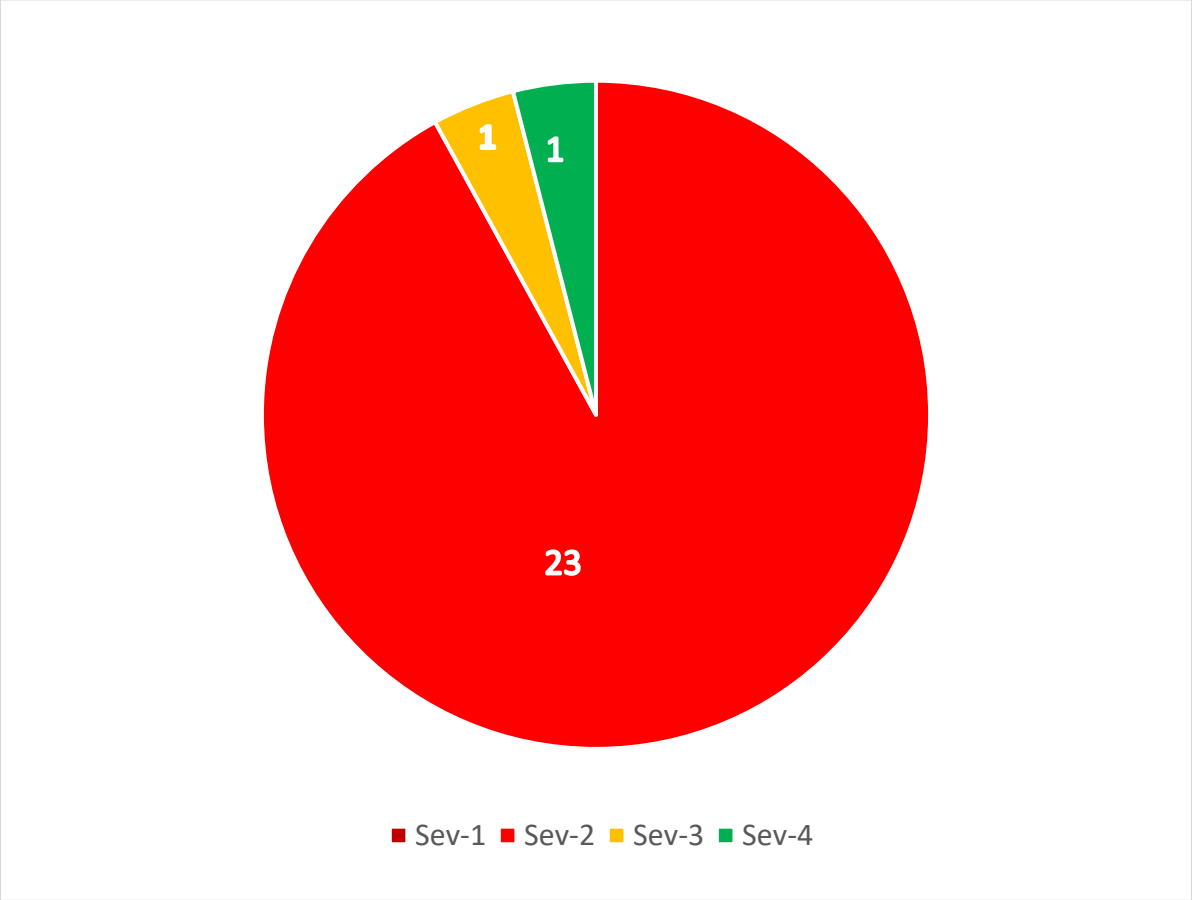
Phase 6 – Vulnerability Revalidation

After confirmation from the development team that an issue has been remediated, a retest on the updated environment is performed.

Vulnerability Summary

The chart displayed in Figure 2 gives the count of observations recorded during the execution of the assessment, along with the respective severity.

Figure 2 Vulnerability Severity and Count



Status of Findings

The post remediation assessment status is displayed in Table 2.

Table 1 Status of Findings

Sr. No.	Title	Severity	Status	Target Fixed Version	Module	Target Fixed Date DD/MM/YY	ID
1	Stored XSS - Invoice Billing Account	High	Not Fixed	NA	Invoicing	06/04/20	CD-188273
2	Second Order IDOR at https://pentestcpay.coupadev.com/requisition_headers/	High	Fixed	v28.0.0, v27.1.0	Requisitions	NA	CD-188737
3	XSS on profile photo	High	Not Fixed	NA	Users	09/04/20	CD-188739
4	Stored XSS in create/Edit global alerts in setup on https://hackme5.coupadev.com	High	Fixed	v28.0.0, v27.0.3	Contracts	NA	CD-192468
5	Stored XSS in create/edit order list in setup on hackme5 account	High	Fixed	No Code Change	Services Procurement	NA	CD-192475
6	Reflected XSS on 'authenticate' via error and error_description parameter	High	Fixed	ccc27.0.0	Contracts	NA	CD-192477
7	Files uploaded are available without any authentication	High	Fixed	master	Requisitions	NA	CD-192489
8	Stored XSS - Contracts History through Tag	High	Fixed	v28.0.0, v27.0.5	Contracts	NA	CD-192502
9	Stored XSS - Contracts custom_fields to History tab	High	Fixed	v27.0.0	Custom Fields	NA	CD-192662
10	Stored XSS - Contracts Comment XSS which leads to account takeover	High	Fixed	v27.0.0	Contracts	NA	CD-192663
11	Stored XSS in purchased order edit on hackme account	High	Fixed	v28.0.0, v27.1.0	Purchase Orders	NA	CD-193015
12	Stored XSS in user first name parameter executing on hackme-ccc	High	Fixed	ccc27.1.0	Contracts	NA	CD-193075

Sr. No.	Title	Severity	Status	Target Fixed Version	Module	Target Fixed Date DD/MM/YY	ID
13	Stored XSS through supplier name in contract sign documents	High	Fixed	ccc27.1.0	Contracts	NA	CD-193076
14	Stored XSS in setup -- > create/edit category on https://hackme5.coupadev.com	High	Fixed	v28.0.0, v27.1.0	Contracts	NA	CD-193257
15	Stored XSS on https://hackme5.coupadev.com/invoices/ - Tag to History which leads to account takeover	High	Fixed	027_release	Invoicing	NA	CD-193289
16	Site-Wide Stored XSS through Custom Field name parameter	High	Fixed	v28.0.0	Custom Fields	NA	CD-193596
17	Reflected XSS using search bar on hackme5.coupadev.com	High	Fixed	v28.0.0, v27.1.0	Search	NA	CD-193603
18	Stored XSS - Supplier Name to Items History	High	Fixed	No Code Change	Supplier	NA	CD-193757
19	Stored XSS in https://hackme-ccc.coupadev.com document edit in new field name	High	Fixed	ccc27.1.0	CLMS	NA	CD-193758
20	IDOR: Expense Report Artifacts	High	Fixed	No Code Change	Expenses	NA	CD-194077
21	Stored XSS at Sourcing - Event Watcher	High	Not Fixed	NA	Sourcing	09/04/20	CD-199066
22	Stored XSS in contract show alert create section	High	Not Fixed	NA	Contracts	09/04/20	CD-199102
23	Stored XSS at Billing Allocation	High	Not Fixed	NA	Application Platform	09/05/20	CD-199236
24	Less secure password min length can be set by parameter manipulation	Medium	Not Fixed	NA	Platform Security	14/07/20	CD-194105
25	AP has access via URL to invoices they should not be able to edit	Low	Not Fixed	NA	Invoicing	02/05/21	CD-198386

Appendix 1 – Vulnerability Evaluation

Coupa evaluates and ranks the vulnerability by determining the risk magnitude by the level of likelihood and consequence. Vulnerabilities are evaluated on a 4-level severity; Low, Medium, High, and Critical.

The likelihood and impact estimates are composed to calculate an overall severity for the risk. The is done by determining whether the likelihood is Low, Medium, or High. The same analysis is also performed for the impact.

The 0 to 10 scale is split into four sections as described in Table 3.

Table 2 Vulnerability Scale

Priority	Severity	CVSS Score	Description
1	**Sev 1 – Critical**	9 – 10.0	Vulnerabilities that affect all users of the platform, and/or affect the security of the platform or host system(s). Vulnerability is Critical that requires minimal or no technical skills and can easily be exploited with very minimal knowledge if discovered.
2	**Sev 2 – High**	7.0 – 8.9	Vulnerabilities that affect more than one user of the platform, and that require little or no user interaction to trigger. Vulnerability is High that requires little knowledge about the application and its workings and if discovered, an attacker can easily exploit the issue.
3	**Sev 3 – Medium**	4.0 – 6.9	Vulnerabilities that affect more than one user but may also require interaction or a specific configuration. Vulnerability is Medium that requires some scripting skills and familiarity of the application, it also depends on another security control which is currently implemented and if discovered needs some tools and manual techniques to exploit the issue.
4	**Sev 4 – Low**	0.1 – 3.9	Vulnerabilities that affect singular users and require interaction or significant prerequisites (MITM) to trigger. Also, leaking very basic information which might lead to information disclosure. Vulnerability is Low that is not exploitable and depends on multiple security controls that are in place and hence, cannot be exploited and is a best practice to have a multi layered security approach.

Appendix 2 – Coupa Security Assessment Tracker

The Coupa Security Assessment tracker for reported vulnerabilities is available from the following link:

Coupa Security Assessment Tracker - R27

Appendix 3 – References

- CVSS V3.1 specification document: https://www.first.org/cvss/specification-document
- OWASP testing guide: https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
- SANS Top 25: https://www.sans.org/top25-software-errors/
- WASC Threat Classification v2.0: http://projects.webappsec.org/w/page/13246978/Threat%20Classification